Main Page

Minimize

Week 1C - Initial Penetration Testing

User: e0540252 e0540252 (GUEST)
e0540252@u.nus.edu
Registered Account
Log off Account Links
Machine State: **RUN**
Refresh in: 0:00.
Time left: 7 mins
Boot progress: complete

control **connect** *stats* *useful*

Home IP:	137.132.84.43
VM IP:	10.0.1.113
Direct:	telnet or ssh to linuxzoo.net
SSH:	unavailable
VM Web:	http://host-1-113.linuxzoo.net/
JScript Telnet:	Network / ~~Console~~
Java Telnet:	Auto
JavaScript SSH:	SSH
JavaScript VNC:	VNC
URI telnet:	linuxzoo.net
Connect:	Username: root, Password: secure

SHARED IP MODE

Initial Pen Testing

A gentle introduction to some elemental command used when performing penetration testing.

To reset all the check buttons from a previous attempt click here

Question 1: Using Locate

"locate" searches through the filesystem looking for things which match the command line. It does this very quickly using a file database. The command "updatedb" refreshes the database.

Use the locate command to find the full path name of the nmap file with "stun-version" in its title.
file location: /usr/share/nmap/scripts/stun-version.nse

Check
Tests: Complete
Location search PASSED

Locate finds all locations which contains information related to the search parameter. Try

```
locate zenmap
```

Pipe the output through grep and locate the part of nmap which involves copyright. Use locate with zenmap and then pipe this into a grep for copyright.
file location: /usr/share/doc/zenmap/copyright

Check
Tests: Complete
Copyright location PASSED

Use locate and grep to find the full pathname where the nmap executable lives. This will be a directory with "bin/" somewhere in its name.
file location: /usr/bin/nmap

Check

Tests: Complete
nmap binary location PASSED

Use locate and grep to find the full pathname where the locate database lives. Hint: database files usually end with ".db".
file location: /var/lib/mlocate/mlocate.db

Check

Tests: Complete
locate db location PASSED

Question 2: Network commands

Make sure you are logged into your virtual machine using at least 1 telnet or ssh session.

The ss command can be used to check network sessions running. Use the ss command and identify the remote endpoint ip number used when you ssh or telnet to a virtual machine.
Proxy IP: 10.0.1.217

Check

Tests: Complete
Proxy ssh/telnet IP PASSED

The ss command with "-a" shows all current network connections. Services which are using ports will be in the LISTEN state.

How many ports are being used by services?
Service ports used: 3

Check

Tests: Complete
Ports used PASSED

Use the service command to start the apache2 service.

Check

Tests: Complete
Start apache2 PASSED

Use the ss command, find out which port number apache2 is running on.

Hint. Use the man page of ss to help. Look for how to see the port numbers numerically, as well as to see what processes are using which entry in ss.
Service port: 80

Check

Tests: Complete
Port of apache2 PASSED
apache2 still running PASSED

Use iceweasel, browse to 127.0.0.1, and fill in the blank below.

Iceweasel can be found in the application menu, Internet>Iceweasel.

Fill in the blank:
The webserver software is running but no content has been added

Check

Tests: Complete

Start apache2	PASSED
apache2 seems to respond	PASSED
blank correct	PASSED

Use nano and edit the default webpage.

Use locate to find "index.html", and then pipe and greps to locate an instance with "www" and "var" in their names.

In the appropriate index.html, change "It works!" to "It does not work!". Remember to save!

Check

Tests: Complete

apache2 seems to respond	PASSED
file edited	PASSED
running apache2	PASSED

Use the service command to stop the apache2 service.

Check

Tests: Complete

Stop apache2	PASSED

Question 3: Networking

Use the ifconfig command. What is the interface which is connected to the local network? This will be the interface with relates to the 10.x.x.x network.
Device: eth0

Check

Tests: Complete

Main network device	PASSED

Again using ifconfig, what is the IP number of this machine in terms of the device identified above.
IP: 10.0.1.217

Check

Tests: Complete

IP number	PASSED

Question 4: Netcat

Netcat is a command for basic client/server command line configuration.

Use netcat to make a web request to linuxzoo.net on the http port. Basic netcat configuration puts the server name in parameter 1 and the port number in paramater 2. Once connected, type "GET /index.html" then type CTRL-V CTRL-M then the return key. Note when connected you dont get any

message, just a blank line... HTTP requests need to end with carriage return then a line feed, thus the need for CTRL-V CTRL-M.

Look through the resulting web document. What is on the last line?
Last line: </body>

Check

Tests: Complete

Network working	PASSED
Last	PASSED

Use netcat for a chat client. Make sure you either have two terminal sessions or two command windows in your virtual machine.

In command window 1, do

```
netcat -l 127.0.0.1 -p 666
```

In command window 2, connect to this localhost service with netcat on port 666, and type some messages.

Now have a third command window. Use the ss command and find the established entry for this chat session. What is the local endpoint port number used at the client end of this network connection?
Client port number: 48709

Once passed press CTRL-C in the chat session to quit.

Check

Tests: Complete

Client port number	PASSED

Use

```
-e 'cat /etc/passwd'
```

at the end of the nc (which is an alias to netcat) command and run a listening server on port 777. Try connecting to this, but note that each time you do the end of the connection (when ended with CTRL-C) closes the server too.

Introduce the flag "--continuous" and restart the nc listener. Now when you end the client with CTRL-C, you can connect again without problems.

When finished, terminate the listener with a CTRL-C in that window. NOTE: Sometime in vnc mode pressing CTRL-C results in autorepeat. If it looks like a key is held down, just press any other key to fix this. This is a bug in the java vnc client.

Check

Tests: Complete

Listener gives /etc/passwd	PASSED
Listiner gives /etc/passwd (repeated for continuous)	PASSED

Use your new knowledge to create a backdoor on port 789. This should be a listening port in continuous mode which runs /bin/bash when someone connects. Run this and connect to it, and try "ls"...

When finished, terminate the listener with a CTRL-C in that window.

Check

Tests: Complete	
Listener gives a shell	PASSED
Listener gives a shell and continuous	PASSED

Use your new knowledge to create a server on port 790. This should be a listening port in continuous mode which runs something which tell you how many files and directories (not including hidden files) can be found in /root. When you are counting you should ignore hidden files.

When finished, terminate the listener with a CTRL-C in that window.

Check

Tests: Complete	
Listener gives a count	PASSED
Listener gives a count and continuous	PASSED
Count seems right test1	PASSED
Count seems right test2	PASSED

Centos 7 intro:	Paths | BasicShell | Search
Linux tutorials:	intro1 intro2 wildcard permission pipe vi essential admin net SELinux1 SELinux2 fwall DNS diag Apache1 Apache2 log Mail
Caine 10.0:	Essentials | Basic | Search | Acquisition | SysIntro | grep | MBR | GPT | FAT | NTFS | FRMeta | FRTools | Browser | Mock Exam |
CPD:	Cygwin | Paths | Files and head/tail | Find and regex | Sort | Log Analysis
Kali:	1a | 1b | 1c | 2 | 3 | 4a | 4b | 5 | 6 | 7a | 8a | 8b | 9 | 10 |
Useful:	Quiz | Forums | Privacy Policy | Terms and Conditions
Site Links:	XMLZoo ActiveSQL ProgZoo SQLZoo