Lab 11: Enumeration

Aim:

To provide a foundation in enumeration.

Time to complete: Up to 45 minutes.

Activities:

- Complete Lab 11: Enumeration.
- Complete Test 11.

Leaning Activities:

At the end of these activities, you should understand:

• How to enumerate hosts.

Reflective statements (end-of-exercise):

You should reflect on these questions:

- How might you stop someone from enumerating your host from outside a corporate network?
- Initially, why might an intruder compromise a host on the network, rather than a domain controller?

Lab 11: Pen Testing (Enumeration)

1 Details

Aim: To provide a foundation in a Pen Testing using enumeration methods.

2 Activities (Enumeration)

L1.1 On you host computer, open a console and run the following commands and note the results:

net share

Which are the main shares on your host:

L1.2 On you host computer, open a console and run the following commands and note the results:

net view /domain

Which domains are present on the network:

net view /domain:napier-mail

Outline a few of the computers with this domain:

- L1.3 Ask your neighbour to share their TEMP folder (right click on the folder, and then select the Sharing tab, and select Advanced Sharing (see Figure 1). Next go to the Start button, and enter Error! Hyperlink reference not valid. Address> into the Run box, and see if you can access the share.
- **L1.4** On your Windows desktop, download Superscan, and start up the Ubuntu, Windows 2003 and Metasploitable images. Run Superscan and determine the following:

The hosts which are connected to the network (IP and MAC addresses):

The TCP ports which are open:

The network shares on the virtual machines:

No. 146.176.164.159 - Remote Des	ktop Connection	
JE C372	04/07/2012 12:40 File1	older
📔 Intel	12/11/2012 12:33 File f	older
📔 PerfLogs	14/07/2009 03:37 File f	older
📔 Program Files	25/04/2013 15:33 File f	older
📔 Quarantine	14/09/2012 20:16 File f	older
📙 Temp	07/05/2013 17:23 File f	older
📕 Users	30/08/2013 11:16 File f	older
📔 Windows	10/04/2013 10:44 File j	jolder
.rnd	10/04/2013 10:45 RND	Advanced Sharing
APPCONF_29-06-12_17.26	🚴 Temp Properties	
🖏 Dropbox 1.4.11		Share this folder
🗋 msexp	General Sharing Security Previous	Settings
MSPrinters	Network File and Folder Sharing	Share name:
🗋 vs2010	Temp	Temp
winconf_29-06-12_17.24	Vot Shared	Add Remove
📄 ziswin.hst	Network Path:	Limit the number of simultaneous users to:
	Not Shared	
	Share	Comments:
dified: 07/05/2013 17:23		
	Advanced Sharing	
	Set custom permissions, create multip	2
	advanced sharing options.	Permissions Caching
	🕞 Advanced Sharing	
	L L	Support nours.
		Website: O
		Computer name domain and wo
		Computer name, domain, and wo
	Close	Cancel Apply
•		

Figure 1:

L1.5 On your Windows host, use the command **nbstat** –**n** to show your NetBIOS table.

What information does it show:		
Can you determine the name of the primary and secondary controllers for your domain:		
Which TCP ports on your computer are related to NetBIOS:		

L1.6 The Metasploitable image has a NULL share vulnerability. Start it up, and then re-run your NESSUS scan against it, and identify the NULL share vulnerability. Read the information on it, and see if you can exploit it with a command something like:

Net use \\[Metasploitable IP]\\$IPC /user:""

L1.7 Download:

http://asecuritysite.com/sid.zip

And extract it to a folder on your desktop. Open a command line and then use the USER2SID command to determine the SID for the guest account on your Windows 2003 virtual machine.

What information does it show:

L1.8 Download:

http://asecuritysite.com/enum.zip

And extract it to a folder on your desktop. Open a command line and then use the **enum** command to enumerate your Windows 2003 host.

What information does it show: