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:

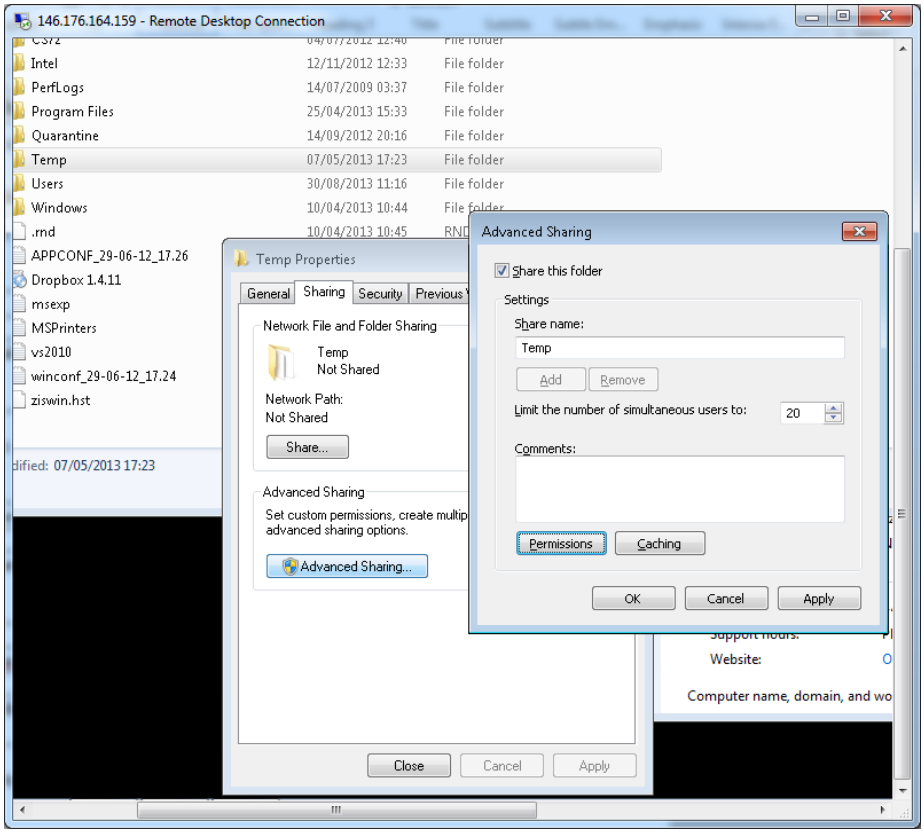

Figure 1:

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: