Lab 8: Introduction to Pen Testing (HPING)

Aim:

To provide a foundation in understanding of email with a focus on hping to provide security assessments and in understanding the trails of evidence produced.

Time to complete: Up to 30 minutes.

Activities:

- **Complete Lab 8**: hping.
- **Complete Test 8**.

Leaning Activities:

At the end of these activities, you should understand:

- How to determine key details related to basic pen testing.
- Craft hping scans.

Reflective statements (end-of-exercise):

You should reflect on these questions:

- How might an intruder determine if a host was on if ping is blocked, using hping?

Lab 8: Intro to Pen Testing (hping)

1 Details

Aim: To provide a foundation in understanding HPING.

In this lab (Figure 1), we will use the **Ubuntu instance** to scan the Windows 2003 virtual machine. The addresses we will use are:

- [Windows2003 IP] which is the IP address of the Windows 2003 virtual image.
- [Ubuntu IP] which is the IP address of the Ubuntu virtual image.

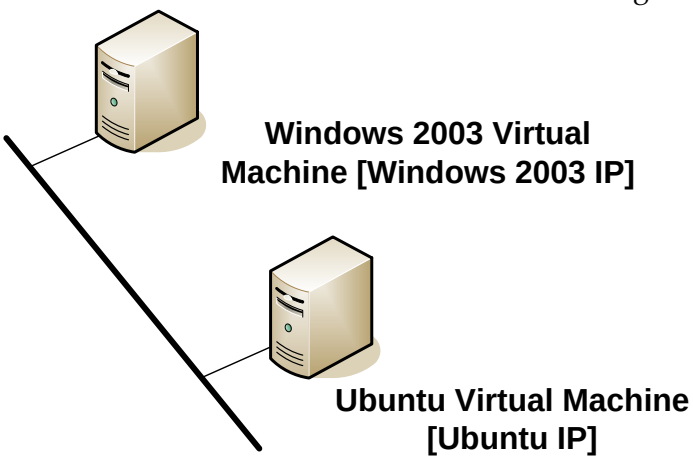

Figure 1: Network setup

2 Crafting packets

For all of the following, within the Ubuntu virtual instance, open two Terminal windows and in one capture your data packets with:

sudo tcpdump -i eth3

L1.1 Start Wireshark on the Windows 2003 virtual machine, and start Wireshark within it. Next go to your Ubuntu virtual machine, and run the command of:

sudo hping [Windows 2003 IP]

Let it run for a few seconds, and the stop it with the Ctrl-C keystroke. Next go back to your Windows 2003 instance and stop the trace. What can you observe from the trace:

Which TCP ports have been used:

L1.2 Start Wireshark on the Windows 2003 virtual machine, and start Wireshark within it. Next go to your Ubuntu virtual machine, and run the command of:

sudo hping –S [Windows 2003 IP]

Let it run for a few seconds, and the stop it with the Ctrl-C keystroke. Next go back to your Windows 2003 instance and stop the trace. What can you observe from the trace: **Which TCP flags and ports have been used:**

L1.3 Investigate the following:

sudo hping –S [Windows 2003 IP] –p 80

How might an intruder use this command:

L1.4 Investigate the following:

sudo hping –1 [Windows 2003 IP]

How might an intruder use this command:

L1.5 View the options for hping with **hping –help**, and create a scan with a spoof address of 10.0.0.1.

What can you identify on the scanned host:

L1.6 We can use **hping** to perform a security assessment for servers and firewalls. If Ping is blocked on a network, we can do an **Ack Scan**. For this scan we scan port 80, and if the port is open it returns a RST response back if the port is open, else it may not respond. Run the following and examine:

sudo hping -c 1 -V -p 80 -s 5050 -A [Windows 2003 IP]

Did it return a RST: **What happens if you scan a port which is not open (such as port 777):**

L1.7 For a Null Scan, we set the sequence number to zero and have no flags set in the packet. For a closed TCP port, the target sends back TCP RST packet, else it sends no reply:

sudo hping -c 1 -V -p 80 -s 5050 -Y [Windows 2003 IP]

Run the command and analyse how the packets are created:

What happens if you scan a port which is not open (such as port 777):

L1.8 The DOS Land attack sends special poisoned spoofed packets:

sudo hping -V -c 1000000 -d 120 -S -w 64 -p 445 -s 445 --rand-source [Windows 2003 IP]

Run the command and analyse how the packets are created:

Now repeat L.6 and L.7 using the **Metasplotiable instance** as a target (Username: user, Password: user).

L1.9 We can use **hping** to perform a security assessment for servers and firewalls. If Ping is blocked on a network, we can do an **Ack Scan**. For this scan we scan port 80, and if the port is open it returns a RST response back if the port is open, else it may not respond. Run the following and examine:

sudo hping -c 1 -V -p 80 -s 5050 -A [Metasploitable 2003 IP]

What is the response for Port 80:

What is the response for Port 77:

L1.10 For a Null Scan, we set the sequence number to zero and have no flags set in the packet. For a closed TCP port, the target sends back TCP RST packet, else it sends no reply:

sudo hping -c 1 -V -p 80 -s 5050 -Y [Metasploitable 2003 IP]

What is the response for Port 80:

What is the response for Port 77: