Lab 1: Lab 03: Reconnaissance with Nmap, Zenmap, and Masscan and Lab 04:

Reconnaissance with Hping– Start with Lab 03, Section 1, “Reconnaissance Using Nmap,” and capture screenshots of the following:

• Step 11 output

Graphical user interface, text, application

Description automatically generated

• Step 12 output

A screenshot of a computer

Description automatically generated with medium confidence

• Step 13 output

Graphical user interface, text

Description automatically generated

– Continue with Lab 03, Section 2, “Using Amap for Reconnaissance,” and capture screenshots of the following:

• Step 3 output

A screenshot of a computer

Description automatically generated

• Step 8 output

A screenshot of a computer

Description automatically generated with medium confidence

• Step 9 output

A screenshot of a computer

Description automatically generated with medium confidence

– Continue with Lab 03, Section 3, "Reconnaissance Using Masscan,” and capture a screenshot of the following:

• Step 4 output

Graphical user interface, text

Description automatically generated

– Continue with Lab 04, Section 1, "Using Hping as an ICMP utility,” and capture screenshots of the following:

• Step 7 output

A screenshot of a computer

Description automatically generated with medium confidence

• Step 8 output

A screenshot of a computer

Description automatically generated with medium confidence

• Step 9 output

Graphical user interface, text

Description automatically generated

– Continue with Lab 04, Section 2, “Using Hping for Port Scanning,” and capture screenshots of the following:

• Step 5 output

Graphical user interface, text

Description automatically generated

• Step 7 output

A screenshot of a computer

Description automatically generated with medium confidence

• Step 8 output

A screenshot of a computer

Description automatically generated with medium confidence

– Summary and Reflection: In a few paragraphs, reflect on what you learned through this lab

assignment. Was there anything surprising or unexpected? Was there anything worth investigating

further?

Through the labs we can get a lot of information from computer and on the network that the virtual system is running on. I thought it was interesting that with a couple of commands we can get a lot of information like how nmap will tell us the different ports and whether they are open or closed. Limiting it let us look at the standard ports where we took off port 5001. My question is that if a hacker it using the ports to find a service that is more likely to contain vulnerabilities are they more likely to look at all ports or just the more standard ports? I did enjoy using the zenmap as I am a more visual person so seeing it through that compared to nmap was quite interesting. Masscan was interesting with how it is called the fastest port scanner and how it goes back to the command prompts with nmap. The hping was fun to look at but the lines began to get overwhelming with how many different sections there were. I think I will need to go back and look more into the meanings behind the letters in the commands like -c and -T. Overall, I think the content of the labs were very informative and fun to look into.