Lab 5 – Scanning

*Please clearly number your responses.* ***Unnumbered or random responses will not be grade.*** *Your screenshot should be* ***cropped*** *to show the requested content; do not use a screenshot of the entire desktop. Make sure your first name is visible in the screenshots done in Kali. This could be having you name open in terminal in the background.*

**Part 1**

Make a copy of Kali in VMware. Additionally, you may use a VM of another OS as a target, if

you have access to them. Or, you may set up your own Kali and targets with vApps in the Projects section of the IA Lab.

1. Use IP Gen script from chapter 3 in your basics book to set up IP address randomization for the victim machine. Provide a screenshot showing you have run it successfully.

2. Turn on or off different services on the victim machine. Provide a screenshot indicating you

have turned on or off at least six services.

3. Run 4 scans from the lecture and explain in your own words what each does, how it works,

and if the output is what you would anticipate. Why or why not? Provide a screenshot from the

output and explain your analysis. Clearly label each belonging to what scan.

**Part 2**

*All of the questions below must be answered with Nmap command line if it involves port*

*scanning.*

*For the following, you may use a VM that you set up (and selectively set it up so ports are in us), Metasploitable, scanme.nmap.org, or (with permission), an employee network.* ***Please select one that gives results.*** *If all else fails, try Metasploitable.*

2.1. What ports are open on the scanme.nmap.org test server? Use a TCP connect scan. Your

answer must include only the port numbers. Do not include other parts of nmap output. nmap -sT scanme.nmap.org

2.2. Using a TCP SYN scan, what ports do you find open on scanme.nmap.org? What do your

enter in terminal to get your result?

2.3. Looking at the output of the two scans outside the ports listed, what differences do you find between the TCP connect and SYN scans? If there is no difference, then just write “None”

below. If there is a difference, how do you account for it?

2.4. Some machines are behind a firewall, which filters connections to some ports, preventing

nmap from receiving any response from those ports. Blocked ports may be listed as either

“filtered” or “closed”. To see an example of such a scan, perform a TCP connect scan on

www.example.com. Your answer must include port numbers for both closed and open ports. Do not include other parts of nmap output. nmap -sT www.example.com

2.5. To determine why a scan returns the results that it does, use the --reason option. Explain the reasons that ports are listed as open, closed, or filtered in the scan of www.example.com. Nmap --reason -sT www.example.com

2.6. Try the scan on scanme.nmap.org again and determine the reasons why.

**For the following questions, you may use Kali and another VM on your machine. Try to use one that gives some results, so that might mean you might explicitly set it up to make sure some ports are open. Provide screenshot of result.**

3.1. What is the syntax if you want to do a TCP Connect port scan on google.com ports 1-1000?

3.2. What is the syntax if you want to do an Ack scan on 192.168.3.2 ALL ports?

3.3. What is the syntax if you want to do a port scan on 192.168.3.2 scanning UDP ports? Do

only ports for http, ftp, telnet.

3.4. What is the syntax if you want to do an Xmas port scan on 192.168.3.2 at insane speed?

3.5. What is the syntax if you want to do a port scan on 192.168.3.2 to find out what OS and

services are running?

3.6. Create a file of targets and use that to do an UDP scan on your target.

3.7 Pick out a scan that you want to test, explain why, and do it.

**For the following questions, you need not do any scans. Simply provide the necessary syntax, as if you were doing the scan.**

3.7. What is the syntax if you want to do a UDP port scan on 192.168.3.0 – the whole subnet?

With cidr of 24?

3.8. What is the syntax if you want to do an idle scan on 192.168.3.2 and your zombie is

192.168.3.23?

**Deliverable** : Word document or PDF with requested screenshots.