**Lab Report**

**Lab Completed: Using Active and Passive Techniques to Enumerate Network Hosts**

**Objective:** Complete the lab presented. Using your textbook, the written lab, and the hands-on activity, use the lab report to demonstrate understanding of the concept presented.

**Part 1: Lab Activity**

Directions: Complete the lab assigned in Netlab. Take 2 screenshots (or more) that demonstrate completion of the lab. Answer the following:

**Q1:** Provide a synthesis of the activity you completed in your own words.

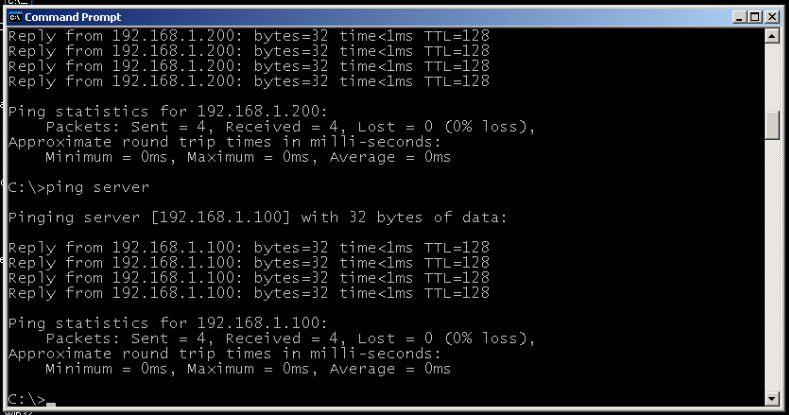
Answer Here: We used various network reconnaissance tools across Linux and Windows to enumerate hosts and filter captured packets sent by the hosts on the network scanned.

**Q2:** Provide 2 screenshots that demonstrate lab completion. For each screenshot, include 1-2 sentences explaining what the screenshot is demonstrating.

Answer Here:



This is a screenshot of the metasploit framework enumerating the ip addresses, associated netbios names, operating systems, and mac addresses for machines on the network.



This is a screenshot of a ping request from the Windows XP machine to the machine with a hostname of server

**Part 2: Critical Thinking**

**Directions**: Complete the following questions. Provide an explanation of your reasoning for each answer.

The answers should address the lab you just completed.

Suggested length for Part 2: 1-2 pages

**Q1**: What vulnerability(s) are demonstrated or found in this lab? Vulnerabilities may occur during the lab as part of the lab activity.

Answer Here: In this lab it seemed like we were just using fundamental network protocols to return information that should likely be available for the network to function. However, the amount and accuracy of the information returned to devices outside of the network could possibly be considered a vulnerability.

**Q2:** How might this (these) attack(s) be utilized during a penetration test?

Answer Here: You might use these attacks to map the network and identify potential targets.

**Q3:** Explain your reasoning as to what phase of the attacker methodology this lab falls under.

Answer Here: Scanning because we are scanning the network to see which machines respond and what further information we can exfiltrate from those machines.

**Q4:** Research how the attack(s) in this lab can be mitigated or prevented. Cite any sources used. (APA)

Answer Here: Per the NMAP website, “Possible defenses include blocking the probes, restricting information returned, slowing down the Nmap scan, and returning misleading information.”

Rackspace gives numerous suggestions for mitigating sniffers:

“

* *Restrict the physical access to the network media to ensure that a packet sniffer cannot be installed.*
* *Use encryption to protect confidential information.*
* *Permanently add the MAC address of the gateway to the ARP cache.*
* *Use static IP addresses and static ARP tables to prevent attackers from adding spoofed ARP entries for their machines to the network.*
* *Turn off network identification broadcasts, and if possible, restrict the network to authorized users in order to protect the network from being discovered with sniffing tools.*
* *Use the IPv6 instead of the IPv4 protocol.*
* *Use encrypted sessions such as Secure Shell (ssh) instead of Telnet.*
* *Use Secure Copy (scp) instead of a file transfer protocol (ftp).*
* *Use Secure Socket Layer (SSL) for email connections.*

*“*

*Chapter 11. defenses against nmap*. Chapter 11. Defenses Against Nmap | Nmap Network Scanning. (n.d.). Retrieved January 16, 2022, from https://nmap.org/book/defenses.html

Jaishwal, P. (2019, October 30). *Packet sniffers and how to protect yourself from them*. Packet sniffers and how to protect yourself from them -. Retrieved January 16, 2022, from https://docs.rackspace.com/blog/packet-sniffers-and-how-you-protect-yourself/

**Q5:** What ethical or potentially problematic issues should a penetration tester consider if they plan on implementing this (these) attack(s) by exploiting a vulnerability?

Answer Here: The tester should ask if they are in the scope of the pentest.