**Lab Report**

**Lab Completed: Conducting Active and Passive Reconnaissance against a Target**

**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**

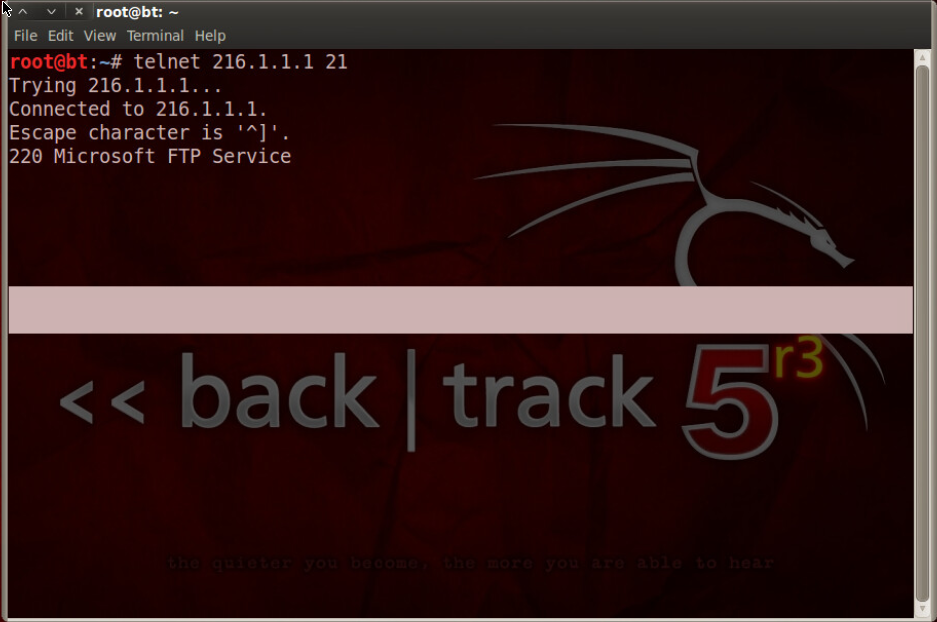
Directions: Complete the lab assigned in Netlab. Take 2 screenshots (or more) that demonstrate completion of the lab. Answer the following:

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

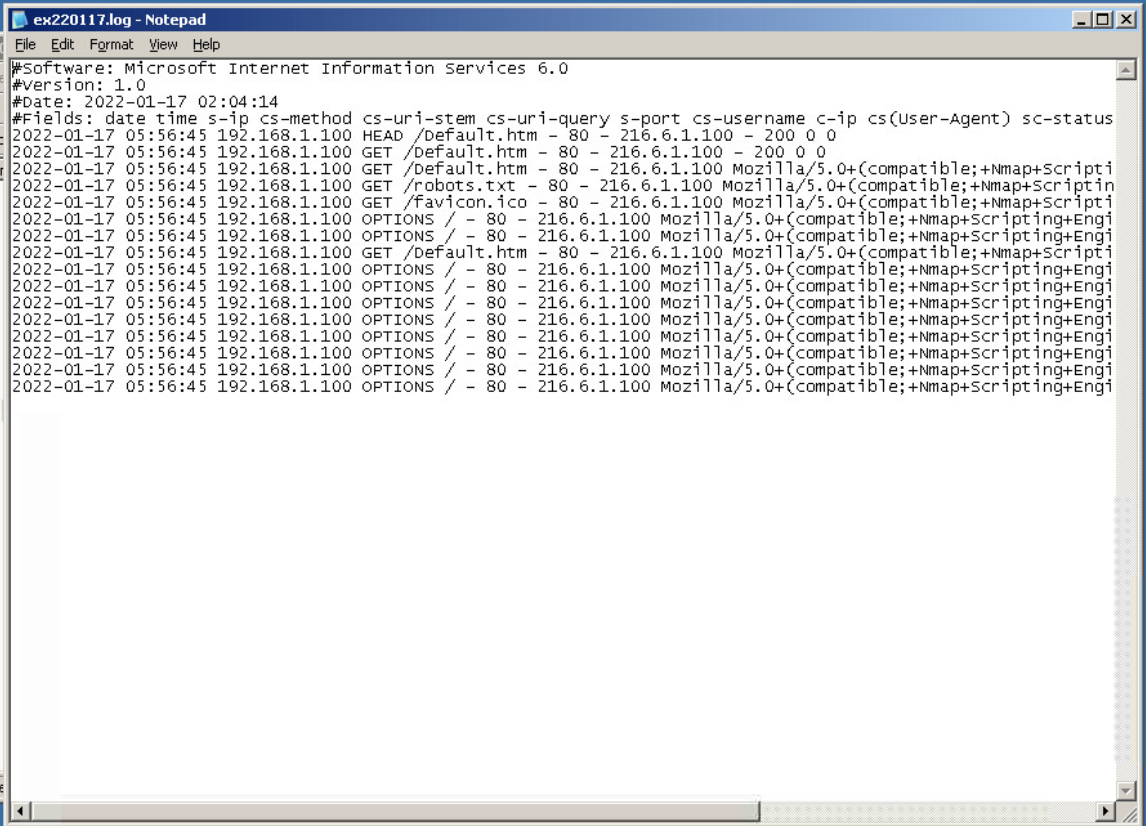
Answer Here: In this lab we conducted both internal and external active and passive reconnaissance on a network. We used tools such as telnet, nmap, and metasploit console to enumerate hosts on the network internally and grab banners to enumerate host information from the front door externally. Additionally, we went through the front door host’s log files to observe the amount of noise a tool like nmap generates vs the amount of noise that a simple banner grab will generate.

**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 from the point in the lab where we used telnet to do a banner grab externally from the ftp service running on the server running at 216.1.1.1.



This is a screenshot showing the log entries created by the above banner grab and the subsequent nmap scan we did, showing that while nmap is able to extrapolate a significant amount of information in a pretty efficient manner, it is also quite noisy and a red flag for most network admins.

**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.

Similar to the last lab, the vulnerability lies in the information released by each machine scanned and the services running on those machines.

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

While the information given up during the internal and external scans may not strictly be considered vulnerabilities, it can be used by attackers to sniff out vulnerabilities based on the service version running on a certain port or the OS version/Service Pack of the operating system running on the machines.

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

I would say that this lab could fall under both the Reconnaissance and Scanning phases. Using programs like tcpdump and wireshark to passively monitor flowing traffic might fall under reconnaissance, and using programs like nmap or msfconsole to interact with actively extrapolate information from target machines would probably fall under scanning.

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

This lab was very similar to the last lab in the techniques used, the targeted machines, and the information obtained, so I have included the same information from that lab below.

In addition to this information, I would like to add a couple of tactics from my personal experience. When I worked with OpenTable’s engineering department as a software integration coordinator, we would often see ip filtering implemented to deal with potential traffic to remote services. Internally we had ACLs that helped to restrict which services/domains we could interact with based on the VPN we connected to.

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?

As this lab fell pretty squarely in the Reconnaissance/Scanning categories, it may be worth considering whether or not the machines and services being targeted are included within the scope of the penetration test.