Lab 02: Scanning the Network on the LAN

Lab report template Name: Kevin Ubilla

This Lab is required for Unit 2. It is worth 15 points. The Challenge flags are worth 2.5 Extra Credit points.

**( 1/1 [name] + 6/9 [questions] = 7/10 [total] , 10.5/15 rescaled, 2.5/2.5 [Flags])**

1. **Scanning, Step 5:** In this step, you are asked to carry out the command **arp** **- scan 192.168.1.0/24**. Please explain why the ‘**0/24**’ has been used in this command (please research it if you are unsure) and place your answer below:

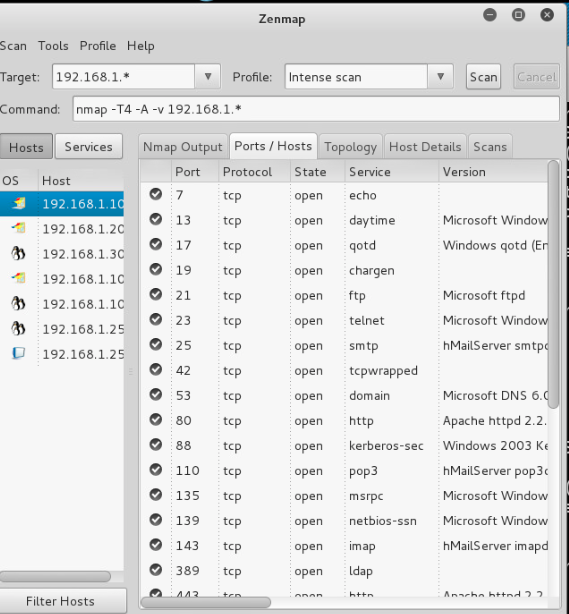
**→ ‘0/24’ is the interface range. It is used to configure multiple interfaces.** **(****I don’t understand what you mean by “interface range”. There are many interfaces for any one host in general. If you mean an Internet/network interface, do you mean that a host can have many? The /24 means “use the first 24 (binary) characters in the address as the subnet mask”. Therefore, the final portion [8 bits] is the “wild card” in the search [numbers 0-255]. I think that you knew the answer, but just didn’t hone in on the right one to put in the report.).←**

1. **Scanning – The whole section:** You have seen the guesses as to what the various OSs are for these hosts. **Where is the firewall**, and what are the most likely OSs for the firewall? (Look at the nMap reports and use your own text to answer.) Please write your answer below:

**→ The Firewall will probably be either Windows Vista or OpenBSD.** **(The firewall is at 192.168.1.254 [on the network, IP addresses are the locations]** **as shown on the picture of the network topology in the lab.** **The OS of 192.168.1.254 as determined by nMap is one of several possible:** **Comau embedded [92%], FreeBSD 8.X [85%] and OpenBSD 4.X [85%].)**

**(←**

1. **Scanning Step 19:**  Please capture the result of the Zenmap intense scan of **192.168.1.254** and paste it below (“in line with text,” please): **The target machine has on 3 ports open.**

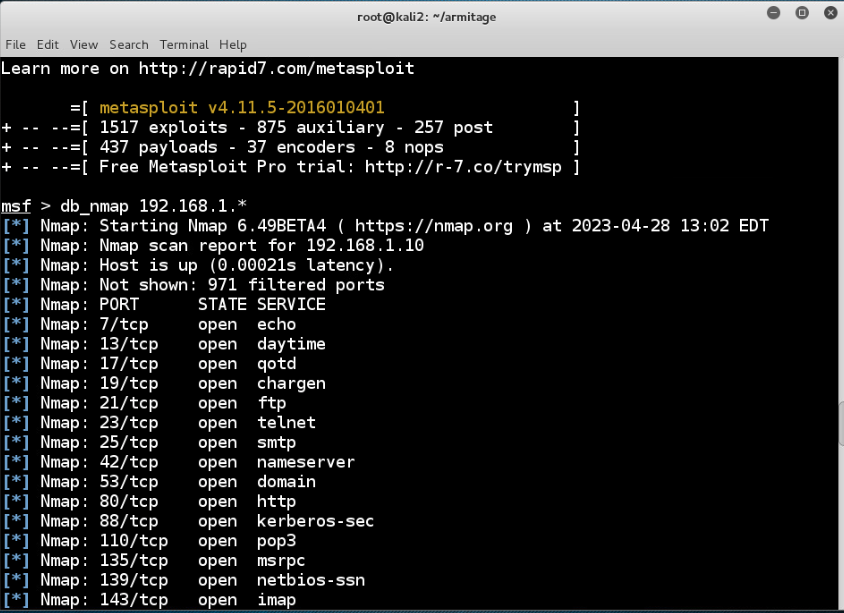
**→ ** Graphical user interface, text, application

Description automatically generated**←**

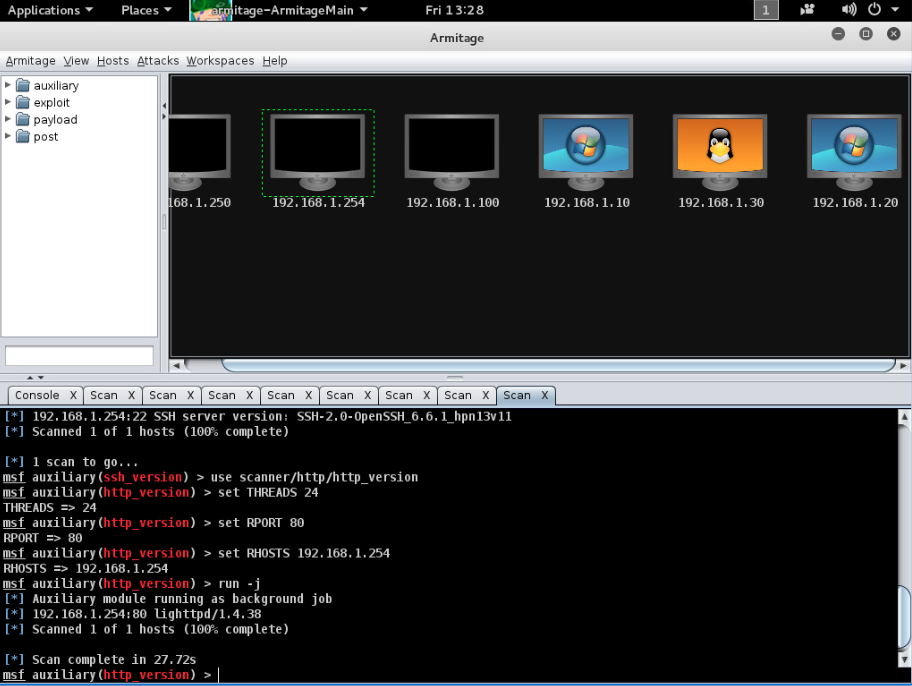
1. **Scanning Discussion Questions:**  What is the nmap option(/flag) for doing only an OS scan?:

**→ For OS scan we use the -O flag. ←**

1. **Scanning with Metasploit and Armitage Step 8-9:**  Please capture the command **db\_nmap 192.168.1.\*** when you get the **msf>** prompt along with the first dozen or so ports discovered (you’ll have to scroll back up the screen to get this) and paste it below:

**→ ←**

1. **Scanning with Metasploit and Armitage Step 23:** You have now used the “Armitage” GUI for Metasploit. Please capture the graphic which shows the OSs it has determined is being run at each of the four **192.168.1.\*** sites, showing a portion of the command prompt box history and the day and time at the top and paste it below. **(The “bonus” system was added recently by InfoSecLearning. No doubt it will appear in the instructions later.)**

**→ ←**

1. **Exploitation Step 5:** You have just successfully exploited **192.168.1.30** by crashing the host. Please capture the screen that displays the graphic of the four host OSs plus the panel that shows “**Server stopped**”.

**→ Graphical user interface, website

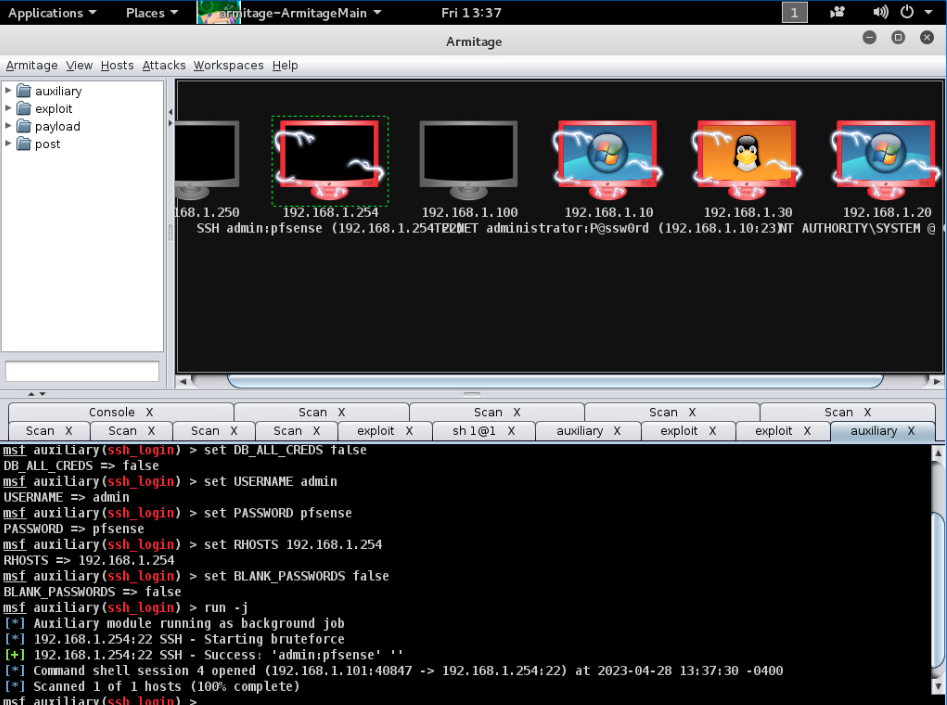
Description automatically generated ←**

1. **Exploitation Step 15:** Capture the command prompt text beginning with the “**john pass.txt**” command and all the lines until the next prompt (including it, too) and paste it in below.

**→ Text

Description automatically generated←**

1. **Exploitation Step 25:** At this stage, you have successfully compromised all of the **192.168.1.\*** hosts using Armitage and are showing all four hosts’ OS graphics. Please capture the panel that shows all four graphics as having been compromised along with the day/time at the top and a few lines of the command prompt box at the bottom and paste it in below.

**→ ←**

*If you encountered any issues, either positive or negative, with this Lab, please let me know by commenting here. I am tuning this according to what you say.*

**→The FreeBSD icon {red daemon} did not appear even after running the command several times. Oh well, at least I am lucky to know one of the BSD founders, Marshall Kirk McKusick who has advised me on several occasions and even signed my patent journal as a witness for my smart headphones invention. (Cool. It is a cute demon, and I think that the graphic may have been corrupted when they shifted to the new cloud at the start of the quarter. )←**