Lab 01: Performing Reconnaissance from the WAN

Lab 01 report Name: Kevin Ubilla

This Lab is required for Unit 1. It is worth 15 points. The Challenge Flags are worth 2.5 Extra Credit points total.

**1/1 (name) + 4/8 (lab items) = 5/9 (total), rescaled to 8.33/15 , Flags = 1.0/2.5**

1. **Banner Grabbing Step 1.0:** In your own words, please explain why the IP addresses beginning with 192.168.1.x shown in this portion of the Lab differ from the 203.0.113.100 address in the specific machine(s) they refer to and place your text between the arrow points below:

**→The 203.0.113.100 is the firewall that masks their true IP address. (Actually, that is the one “true” IP address as all the rest are “private” addresses and not unique.)←**

1. **Banner Grabbing Step 14.0**: Capture the result of the banner grab **nc** [www.campus.edu](http://www.campus.edu) 80 and place it below: (Please paste it as “in line with text”, make the text large enough to read clearly, and place it precisely between the arrow points. If it is text from a command prompt exchange, capture the command(s) as well as the response.)

**→** Text

Description automatically generated **←**

1. **Banner Grabbing Step 14.0:** Please report – in your own words - the name of operating system used by the machine managing Port 80 at www.campus.edu, the web server used for port 80 at [www.campus.edu](http://www.campus.edu), and also note the scripting languages used at that site (Google them to be certain that they are web scripting languages, web servers, etc.) and place it below:

**→ OS: Windows; Web Server: Apache; Scripting Languages: PHP, Perl ←**

1. **Banner Grabbing – The whole section:** Please type the names of the two tools you used for banner grabbing:

**→ Nmap, Metasploit Telnet & Netcat (nc)←**

1. **Advanced Scanning with NMAP Step 2:** Please tell me **(1) exactly how many ports were scanned** at 203.0.113.100 and also (2) tell me how many of these were open and place the numbers in that order below:

**→11 scanned, 989 open** **1000 ports were scanned and only 11 were open ←**

1. **Advanced Scanning with NMAP Step 17:** Please report nMap’s estimate of the name and version of the Operating System running on the machine that was managing port 3306 (again, if you aren’t certain, it’s best to make certain it is an OS by Googling it) and place the name and version below:

**→ 5.0.51a-3 Ubuntu5** **(That’s not an OS. Ubuntu 5 is the OS: the programmers did not have space for any characters for punctuation or spacing here, so they are jammed together.) ←**

1. **Advanced Scanning with NMAP - The whole section:** Please tell me exactly what the -sC and -sV “switches” do in nmap (finding a good nMap “cheat sheet” can help. Please give me a sentence for each.):

**→-sC: executes scripted scan using scripts in default category. Used for discovery and is safe.**

**-sV: attempts to find version of service running on a given port.←**

1. **Analysis and Exploitation Step 12:** You are using John the Ripper in KALI Linux. Please summarize, in your own words, how the program “cracks” passwords (as always, I encourage you to use Google or Wikipedia to help).

**→John the Ripper uses the rainbow table approach which consists of using its internal dictionaries to compare against the hashed password in order to find a match. ←**

*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.*

**→ ←**