web.compass.lighthouselabs.ca /projects/network-admin

Compass | Network Administration

10-12 minutes

This project can be completed in two phases, Part 1 and Part 2, as described below:

Instruction

This project will make use of a variety of tools and techniques you have seen throughout this course. Read and understand all requirements before starting, to determine which tools you will need to use.

Part 1 Network Scans and Information Collection

The first part of the project will focus on scanning networks and collecting information, and can be completed in three steps as described below.

For students using the EVE Environment

Warning

For this project, you will need to have your EVE Main Lab open and all the machines turned on so you can scan and collect information from each of them. However, you will be running all your Nmap scans, and Wireshark captures from the Jump Host machine.

Students using VirtualBox/VMWare

Warning

For this project, you will need all of your virtual machines turned on so you can scan and collect information from each of them. However, you will be running all your Nmap scans, and Wireshark captures from the Kali OpenVas VM.

Part 1A Turning on Machines

For students using the EVE Environment

In EVE, open your Main Lab and turn on all of your machines (WinServer, Windows1, Linux, & KaliOpenVAS). Make sure you have booted up successfully before moving on to the next step.

Students using VirtualBox/VMWare

In VirtualBox/VMWare, turn on all of your machines (Windows11, Linux Server, and KaliOpenVAS). Ensure you have booted up successfully before proceeding to the next step.

Part 1B Performing Scans & Collecting Information

For students using the EVE Environment

Open Wireshark: On your Jump Host, open Wireshark. You want to make sure you are using it to capture all network traffic while using Nmap to scan your Main Lab network.

Students using VirtualBox/VMWare

Open Wireshark: On your Kali OpenVas, open Wireshark. You want to make sure you are using it to capture all network traffic while using Nmap to scan your Virtual Lab network.

Use Nmap to Perform Scans: Use Nmap to perform scans of the Main Lab network to collect information about each of your machines. You can either use the command line Nmap, or the GUI (Graphical User Interface) Zenmap to complete your scans, the decision is up to you. They are both available on your Jump Host.

Record in Wireshark: Start recording in Wireshark on Ethernet0.

For students using the EVE Environment

Discover & Collect Information: With Wireshark capturing all traffic on Ethernet0, use Nmap/Zenmap on your Jump Host to discover and collect the following information about each of the five machines on your Main Lab network (IP addresses 172.16.14.50 through 172.16.14.54). You should ignore any and all information related to the devices with the IP addresses 172.16.14.1 through 172.16.14.3.

Students using VirtualBox/VMWare

Discover & Collect Information: With Wireshark capturing all traffic on Ethernet0, use Nmap/Zenmap on your Kali OpenVAS machine to discover and collect the following information about each of the machines on your Virtual Network (IP addresses 10.0.2.4, 10.0.2.5 & 10.0.2.15).

Warning

Remember to stop the Wireshark scan after the Nmap scan finishes!

Note

Hint: You should be able to collect the following information except the Machine Designation from the output of an Intense scan. You can get the command for this from one of your cheat sheets, or by using Zenmap to set up your scan.

- Machine designation (ex. Windows1, Windows2, etc)
- Device Host Name (ex. DESKTOP-JE9II55, etc)
- IP address
- MAC address
- Operating System & version
- Open ports with associated services
- ARP Ping Scan elapsed time

Zenmap Samples

Here is an example of what you would expect to see if you use Zenmap:

Note

Some information, like the MAC address, you may have to get from your Wireshark capture.

```
nmap -T4 -A -v 172.16.14.100

Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 22:46 Coordinated Universal Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:46
Completed NSE at 22:46, 0.00s elapsed
Initiating NSE at 22:46
Completed NSE at 22:46, 0.00s elapsed
Initiating NSE at 22:46
Completed NSE at 22:46, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 22:46
Completed Parallel DNS resolution of 1 host. at 22:46, 0.47s elapsed
Initiating SYN Stealth Scan at 22:46
Scanning 172.16.14.100 [1000 ports]
Discovered open port 135/tcp on 172.16.14.100
Discovered open port 139/tcp on 172.16.14.100
Discovered open port 445/tcp on 172.16.14.100
Discovered open port 3389/tcp on 172.16.14.100
Discovered open port 5357/tcp on 172.16.14.100
Completed SYN Stealth Scan at 22:46, 0.39s elapsed (1000 total ports)
Initiating Service scan at 22:46
Scanning 5 services on 172.16.14.100
Completed Service scan at 22:47, 11.03s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against 172.16.14.100
NSE: Script scanning 172.16.14.100.
Initiating NSE at 22:47
Completed NSE at 22:47, 14.31s elapsed
Initiating NSE at 22:47
Completed NSE at 22:47, 0.34s elapsed
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Nmap scan report for 172.16.14.100
Host is up (0.0014s latency).
```

```
nmap -T4 -A -v 172.16.14.100

Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DESKTOP-WIN10PRO
| Issuer: commonName=DESKTOP-WIN10PRO
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-07-12T20:01:04
| Not valid after:  2024-01-11T20:01:04
| MD5:   ec23:d567:e68a:7d91:9bca:0d67:3bde:a6dd
|_SHA-1: 0400:95c2:1a53:712d:9427:1c0e:f3ab:cb80:1aa1:8436
| rdp-ntlm-info:
|   Target_Name: DESKTOP-WIN10PR
|   NetBIOS_Domain_Name: DESKTOP-WIN10PR
|   NetBIOS_Computer_Name: DESKTOP-WIN10PR
|   DNS_Domain_Name: DESKTOP-WIN10PRO
|   DNS_Computer_Name: DESKTOP-WIN10PRO
|   Product_Version: 10.0.19041
|_  System_Time: 2023-09-25T22:47:07+00:00
|_ssl-date: 2023-09-25T22:47:21+00:00; 0s from scanner time.
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 2004
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
nmap -T4 -A -v 172.16.14.100

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-09-25T22:47:09
|_  start_date: N/A

NSE: Script Post-scanning.
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.82 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2045 (87.250KB)
```

Part 1C Verifying Collected Information

Make sure you double check that the information you collected using Nmap is correct by verifying it against what is actually on each machine as much as possible.

Part 2 Creating Report

In the second part of the project, you need to create a report that documents all the information that you captured in the first part of the project.

Here are some examples of what a Cyber Security Esecutive Summary: * https://www.bitsight.com/glossary/cybersecurity-executive-summary-example * https://www.upguard.com/blog/writing-a-cybersecurity-executive-summary

Part 2A Documenting Devices Information

Create documentation for the devices in your Lab. Ensure that it is clear, easy to read and interpret, and includes all the information you have collected and verified from each device. Use your space wisely and organize the information for quick and efficient reference and use (including point form notes and tables to organize information for each machine).

You can document the following information:

- Machine designation (ex. Windows1, Windows2, etc)
- Device Host Name (ex. DESKTOP-JE9II55, etc)
- IP address
- MAC address
- Operating System & version
- Open ports with associated services
- ARP Ping Scan elapsed tim
- List what OSI Layer header each of the addresses and port #’s is found in and include screen captures showing the information captured using Wireshark
- A fully labeled topology diagram that includes your recommendation on how network segmentation (both IP address ranges & VLANs) should be added to the network in order to improve the network security posture. Make your decisions based on what services are on each machine.

Part 2B Documenting Information Collection Process

- Document how you collected your information.
- Analyze the Wireshark capture(s) you took to see where you can see each of the scans you did being performed.
- Take screen captures of each portion/type of scan and document how you know that was the scan that you completed.

Part 2C Creating Report

Organize all the information you have collected and put together in a 3-5 pager report. In your report:

- Include your documentation of the network devices
- Share details of your information collection methodologies
- Present the information in your report in the following (suggested) format:
    - Table of contents
    - Introduction section
    - Network Devices Information
    - Information Collection Methodology
    - References and Citation

Note

Report Recommendation: You should utilize half a page per device for documentation, one page for your topology diagram showing network segmentation recommendations, and maximum 2 pages for your methodology documentation.

Project Learning Outcomes

In completing this project, learners will be able to:

- Explore what processes and software are running on Windows and Linux systems
- Select appropriate virtual machine connectivity to other virtual machines and the outside world given a scenario
- Interpret captured network traffic using packet sniffing software
- Plan an IPv4 addressing scheme and basic network segmentation approach given a scenario

Submission Guidelines

- Submit a link to a Google doc that contains your report. This report will be evaluated according the evaluation rubric.
- Make sure you change the share settings to the doc to allow and access to all.
- To submit your project, use the *Project Submission* button given at the top and follow the instructions.
- your project should follow an Executive Summary format

Note

There is more than one way to approach this problem.

After you have submitted your workflow, you may also want to share it with your peers on Discord, and take a look at the various approaches your peers used.

Evaluation Guidelines

- Familiarize yourself with the Eval Rubric tab so you can read about the competencies you will be evaluated on for this particular project, and review what the different levels of each competency require.
- If you receive Unsatisfactory for any competency, your project will be given feedback to implement before it is accepted. Review the feedback provided, make changes to your project, and aim to resubmit your updated project within 48 hours.

This is not a bad thing; having to resubmit is an opportunity for you to improve and it is common for students to need to implement feedback on their projects before being accepted.

Project Requirements

- Documentation of the network devices discovered through network scans and direct device exploration
- Includes table of contents, introduction, network devices information, and references
- Evidence of findings with labels with labeled screenshots that are tied to description within report
- Details of information collection methods
- Performed wireshark transfers and scans

References

References are crucial for credibility, validating arguments, and avoiding plagiarism. References enable readers to verify information; build on existing knowledge, and uphold ethical standards while promoting transparency. All the resources you access should be listed in a References List at the end of your work.

You may use tools, like Citation Machine, to generate citations for your work.

Instruction

The widely accepted citation format in the cyber security industry is the APA format. Use this format for all projects in the program. Once you enter the industry, you may follow a different citation style if instructed by your organization.

Note

Examples: A guide to digital forensics and cybersecurity tools. Forensics Colleges. (2022, May 19). https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools

Whitman, M., & Mattord, H. (2017). Principles of information security (6th ed.). CENGAGE Learning Custom Publishing.