



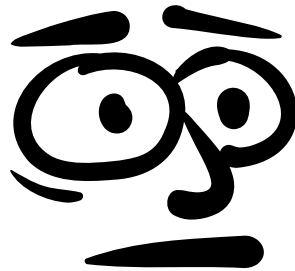
PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Assessing Vulnerability



Objectives

In continuation to our earlier lectures, this tutorial helps in providing you an overview of tools used to scan network vulnerabilities.

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should contact me prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Use various tools to do a vulnerability scanning and analyse the vulnerabilities within the network

Task 1: Use Nessus tool in Windows to scan for network vulnerabilities
--

Task 2: Use Nessus tool in Kali Linux to scan for network vulnerabilities

Task 3: Use Nikto in Kali Linux to scan Web vulnerabilities

Task 4: Use NMAP to scan vulnerabilities
--

Task 5: Use the Wireshark Captured network traffic to analyse the network and identify security details.
--

Task 6: Use Tools of your choice to scan for network, identify vulnerabilities, assess the vulnerabilities and enumerate
--

Why to use these tools? These tools are used to scan the networks and identify hosts, ports, and services. It is one of the components of intelligence gathering that can be used by attackers to gather information and create a profile of their targets

Task 1: Use Nessus tool in Windows to scan for network vulnerabilities

Install and assess from: Windows Server 2022

Network: VM Machines

The network scan will help to check live systems, its port status, perform banner grabbing and OS Fingerprinting, list out its vulnerabilities, and map the network based on vulnerable hosts

Download Nessus.

1. Install Nessus. Select appropriate options while installing. When it says your connection is not private, select proceed to local host.
2. Set user credentials and log in to Nessus.
3. Register and activate using the activation code received in your email.
Checkpoint: After activation, it will download and instal plugins.
4. Login
5. Create a new Policy with Advanced Scan option.
6. Configure name of the policy and add a description (add your student id) under basic settings.
7. Select Host Discovery under discovery option. Turn off – Ping the remote host
Why would we turn off ping the remote host option?
8. Customize the port scanning by verifying open TCP Ports. (*Hint: under Local port enumerators in Port scanning*). Leave other options with default settings.
9. Under advanced settings, make maximum number of concurrent TCP sessions per host and per scan unlimited.
Why would we set them to unlimited?
10. Set credentials to the policy and save.
11. Create new scan. Select the policy you have created.
12. Give a name for the scan with description and enter the target IP Address. (It may be any machine as per your choice. However, to get listed more known vulnerabilities under lab environment, it is recommended to scan lower Windows OS (XP/ 7/8).
13. Launch the scan.
14. After completing the scan, analyse the results.
15. Click the vulnerabilities and view all the vulnerabilities associated to the target.
16. Download and Export the report.
17. Use the report and classify action plan/ mitigation steps to overcome the vulnerabilities.
 - a. To do that, categorize all the listed vulnerabilities based on its severity.
 - b. Select one of the vulnerability and propose a mitigation/ action plan.
- 18. Document your report and Mitigation plan with proper/adequate citations.**

This Page is
intentionally left blank

Task 2: Use Nessus tool in Kali Linux to scan for network vulnerabilities

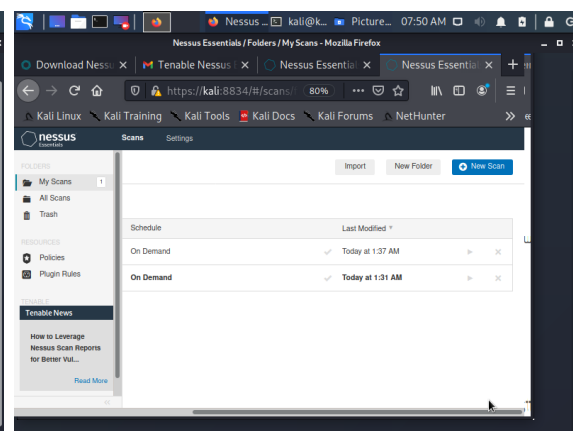
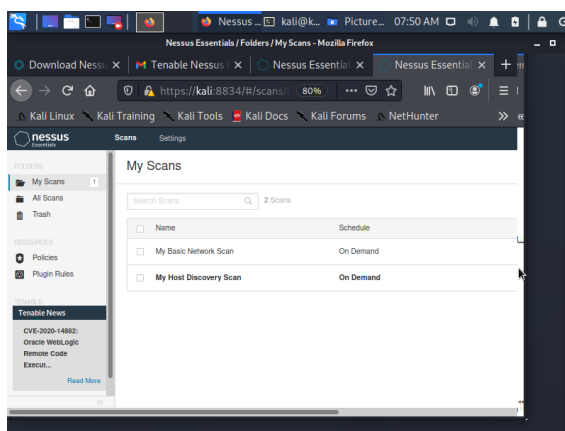
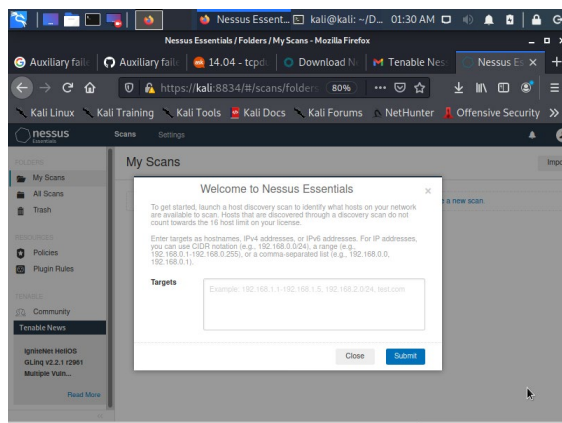
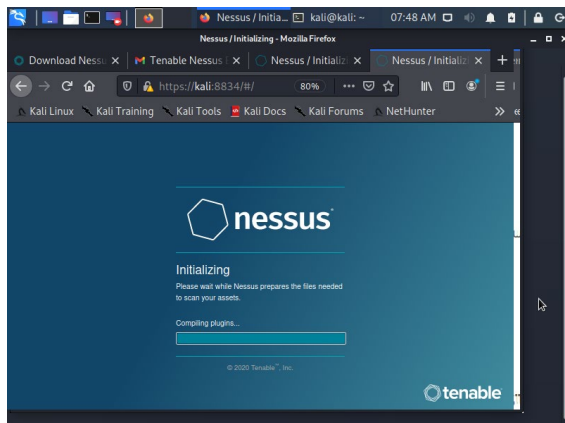
Install and assess from: Kali Linux

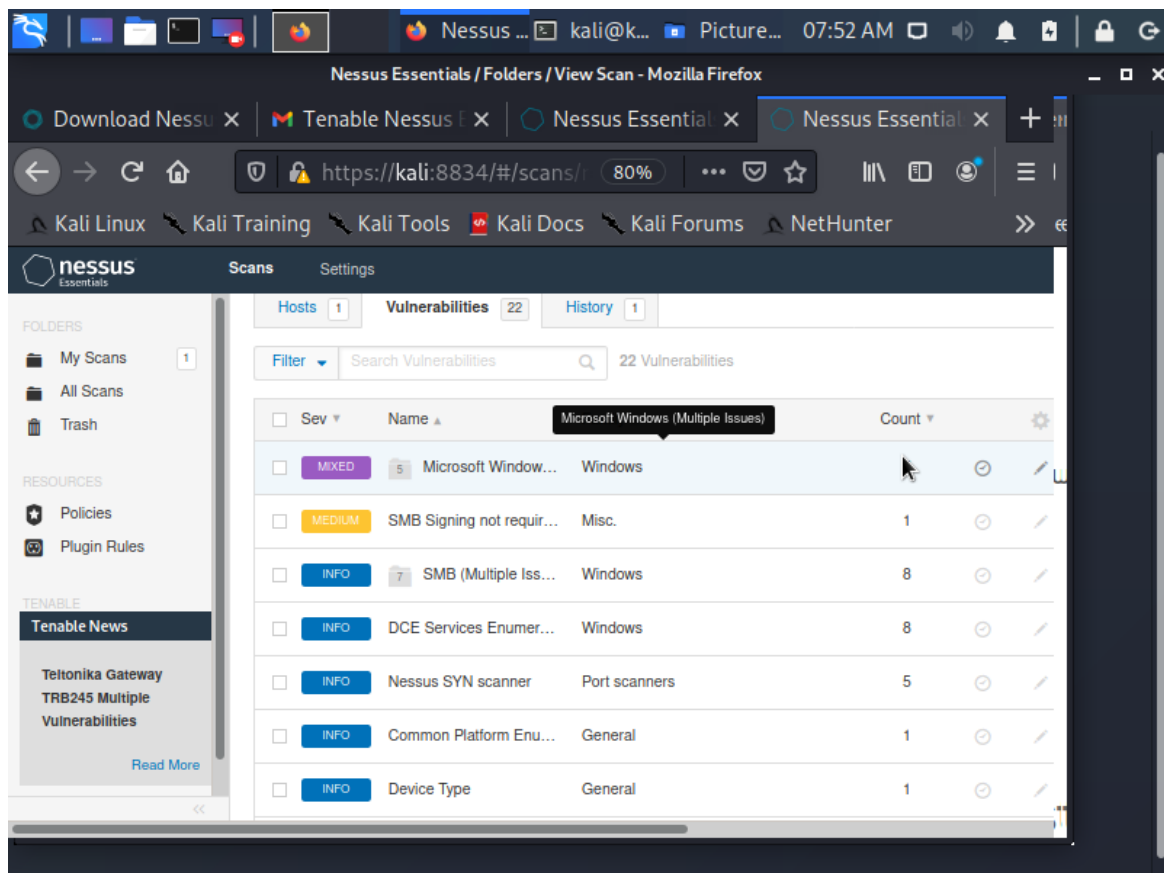
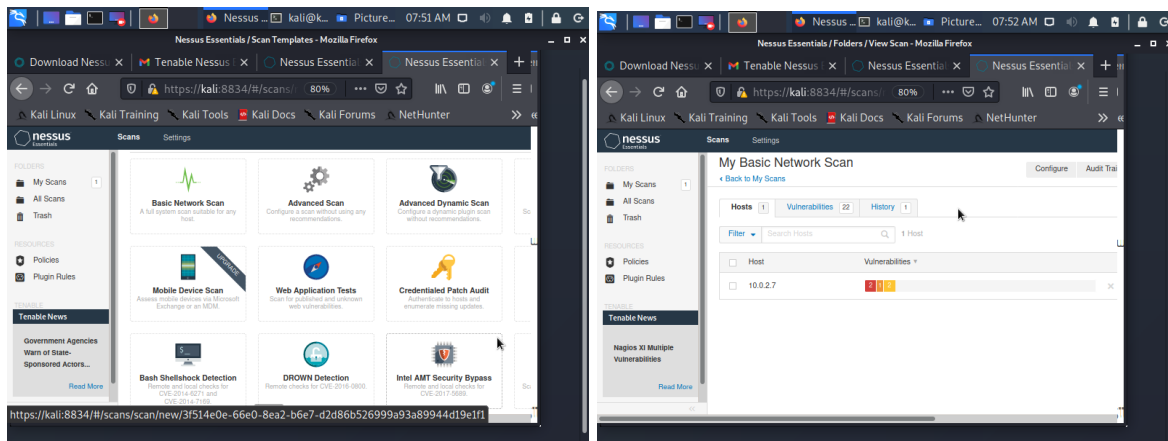
Network: VM Machines

The network scan will help to check live systems, its port status, perform banner grabbing and OS Fingerprinting, list out its vulnerabilities, and map the network based on vulnerable hosts

Download Nessus.

1. Open Kali Linux.
2. You can start Nessus Scanner by typing `/bin/systemctl start nessusd.service`
3. Then go to <https://kali:8834/> to configure your scanner (*Note: Port may differ if you configured it differently*)
4. Create username and password
5. Update the plugins
6. Perform a vulnerability scan to the attack machine (*Any machine in your VM other than the one you did earlier*)





- Click on the vulnerabilities and look at all the vulnerabilities listed for the target machine. View the detailed report about all the listed vulnerabilities and create a list based on High, Medium categories.
- Based on your categorization, select the Top listed vulnerability, and propose your mitigation steps/ strategies. Refer to websites/ databases which we have covered during our lectures to list out the necessary mitigation steps, citations etc.
- Generate the Report.

10. Use the report and classify action plan/ mitigation steps to overcome the vulnerabilities.
 - a. To do that, categorize all the listed vulnerabilities based on its severity.
 - b. Select one of the vulnerabilities and propose a mitigation/ action plan.
11. Document your report and Mitigation plan with proper/adequate citations.

This Page is
intentionally left blank

Task 3: Use Nikto in Kali Linux to scan Web vulnerabilities

Install and assess from: Kali Linux

The web scanners will do a comprehensive test against web servers to look for harmful files, CGIs, Versions etc

1. Open Kali Linux.

Download and install Nikto in Kali Linux.

```

$ nikto
- Nikto v2.1.6
-----
+ ERROR: No host or URL specified

-config+      Use this config file
-Display+     Turn on/off display outputs
-dbcheck      check database and other key files for syntax errors
-Format+      save file (-o) format
-Help         Extended help information
-host+        target host/URL
-id+          Host authentication to use, format is id:pass or id:pass:realm
-list-plugins  List all available plugins
-output+      Write output to this file
-nossl        Disables using SSL
-no404        Disables 404 checks
-Plugins+     List of plugins to run (default: ALL)
-port+        Port to use (default 80)
-root+        Prepend root value to all requests, format is /directory
-ssl          Force ssl mode on port
-Tuning+      Scan tuning
-timeout+     Timeout for requests (default 10 seconds)
-update       Update databases and plugins from CIRT.net
-Version      Print plugin and database versions
-vhost+       Virtual host (for Host header)

```

Observe the options of nikto

```

(ethical@ SC-205-03) ~
$ nikto -H

Options:
-ask+      Whether to ask about submitting updates
           yes   Ask about each (default)
           no   Don't ask, don't send
           auto Don't ask, just send
-Cgidirs+  Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
-config+   Use this config file
-Display+  Turn on/off display outputs:
           1    Show redirects
           2    Show cookies received
           3    Show all 200/OK responses
           4    Show URLs which require authentication
           D    Debug output
           E    Display all HTTP errors
           P    Print progress to STDOUT
           S    Scrub output of IPs and hostnames
           V    Verbose output
-dbcheck   Check database and other key files for syntax errors
-evasion+  Encoding technique:
           1    Random URI encoding (non-UTF8)
           2    Directory self-reference (./)
           3    Premature URL ending
           4    Prepend long random string
           5    Fake parameter
           6    TAB as request spacer
           7    Change the case of the URL

```

2. Use tuning option to pursue a deep scan on the target. In my case, the target is itsecgames.com. You may try a different vulnerable website for Educational

purpose (like the BeeBox Machine in our Network, www.certifiedhacker.com).

Donot try in production environment or unauthorized websites.

```
(ethical@ SC-205-03) ~
$ nikto -h http://www.itsecgames.com -Tuning x
- Nikto v2.1.6
```

3. What vulnerability did you observe?

```
(ethical@ SC-205-03) ~
$ nikto -h http://www.itsecgames.com -Tuning x
- Nikto v2.1.6
-----
+ Target IP: 31.3.96.40
+ Target Hostname: www.itsecgames.com
+ Target Port: 80
+ Start Time: 2022-03-07 07:56:53 (GMT0)
-----
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: e43, size: 5d7959bd3c800, mtime: gzip
+ Uncommon header 'link' found, with contents: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink"
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7901 requests: 7 error(s) and 8 item(s) reported on remote host
+ End Time: 2022-03-07 08:03:28 (GMT0) (395 seconds)
-----
+ 1 host(s) tested
```

In this above screenshot, I have OSVDB – 3233 (Apache default file found).

4. Do a detailed research (with reference to our lectures) on the identified vulnerability and propose mitigation actions. Document it.
5. Let us now check the CGI Directories. What vulnerability did you observe?

```
$ nikto -h http://www.itsecgames.com -Cgdirs all
- Nikto v2.1.6
-----
+ Target IP: 31.3.96.40
+ Target Hostname: www.itsecgames.com
+ Target Port: 80
+ Start Time: 2022-03-07 08:04:46 (GMT0)
-----
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /, inode: e43, size: 5d7959bd3c800, mtime: gzip
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ Uncommon header 'link' found, with contents: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink"
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 26516 requests: 7 error(s) and 8 item(s) reported on remote host
+ End Time: 2022-03-07 08:19:56 (GMT0) (910 seconds)
-----
+ 1 host(s) tested
```

6. Use other commands to scrutinize the target network. List out the commands you used, and the vulnerabilities identified.
7. **Write a report to provide your thoughts and observation on your target's security posture and exposure. Submit in Moodle**

This Page is
intentionally left blank

Task 4: Use NMAP to scan vulnerabilities

Install and assess from: Kali Linux

Target: All Victim Machines (Recommended) - *bee-box v1.6*

1. Open Kali Linux.
 - a. Check your IP Address
Ifconfig
 - b. Do a nmap scan on the available target range
Nmap 192.168.137.0-254
 - c. Do an nmap to list the available targets.
nmap 192.168.137.0/24 -sL
 - d. Do an nmap ARP discovery on the entire subnet
nmap 192.168.137.0/24 -PR
 - e. Do an nmap Host discovery – disable port scanning
nmap 192.168.137.0/24 -sn
 - f. Do an nmap Port Scan – disable Host discovery
nmap 192.168.137.0/24 -Pn
 - g. Do a TCP Syn Port Scan
nmap 192.168.137.131 -sS
 - h. Do a TCP Connect Port Scan
nmap 192.168.137.131 -sT
 - i. Do a TCP ACK Port Scan
nmap 192.168.137.131 -sA
 - j. Do a TCP Window Port Scan
nmap 192.168.137.131 -sW
 - k. Do a UDP Port Scan
nmap 192.168.137.131 -Su
 - l. Do a complete port scan (65535)
nmap 192.168.137.131 -p-65535
nmap 192.168.137.131 -p-

Analyse the outcomes from the above scans.

What information did you gather from ARP Discovery?

Try to identify the services running on the port!

- m. Do a nmap scan to identify the version of the services running on port
nmap 192.168.137.131 -sV
- n. Do a intense nmap scan to identify the version
nmap 192.168.137.131 -sV -version- intensity all (or instead of all give an number between 0 – 8)
- o. Do a nmap scan to identify the version of the services running on port
nmap 192.168.137.131 -sV

- p. Do a nmap scan to identify the OS, version and script scanning
nmap 192.168.137.131 -A
- q. Do a nmap scan to identify the OS, version and script scanning enabling Nmap script scanning and specifying the output in a text file?
nmap 192.168.137.132 -sV -A -sC -o ~/Desktop/nmap.txt

Analyse the outcomes from the above scans.

D. 2 Discuss with your classmates/ Team to find out and try other nmap scans that help you to get more information on the Operating System, Services and other valuable information. List them in the discussion forum and enable a strong argument.

Understand Nmap Scripting Engine.

Group Activity: Discuss with your classmates/ team about Nmap Scripting Engine (NSE). Address what NSE is?

How to effectively use Nmap as a lightweight vulnerability scanner?

NSE scripts extend basic functionality of Nmap to do a variety of networking tasks. They are grouped into categories around cases such as vulnerability detection, brute forcing, network discovery etc. NSE is an extension of version detection and information gathering capabilities of Nmap.

Refer to <https://nmap.org/book/nse.html>

- 2. Have a look at the Nmap scripts
 - cd /usr/share/nmap/scripts
 - cat script.db
 - a. Look at the scripts and discuss about the available script categories
Eg: Entry { filename = "afp-path-vuln.nse", categories = { "exploit", "intrusive", "vuln", } }
What is this category?
How does this script help you to test?
What script will help you to assess the vulnerability of the existing target machines?
 - b. Based on the above scans try to deep dive and focus on exploring more vulnerabilities on the target machine using nmap scripts on any specific port. In my case, I will be using port 443 and category "vuln"
nmap -sV -p 443 --script "vuln" 192.168.137.132
- Q. 8.** What vulnerabilities did you find out?

Could you try other target machines and ports, categories to find more vulnerabilities? Document them using a report. Discuss this in moodle discussion forum.

This Page is
intentionally left blank

Task 5: Use the Wireshark Captured network traffic to analyse the network and identify security details.

Requirements: .pcap file (available in moodle – Capture_1_PublicCapture)

Brief:

Use your knowledge, understanding, and cognitive skills, - *refer to the lecture and tutorial activities done in the last 5 weeks* - to practically analyse the captured packets and present your outcomes.

This activity helps you to deep dive and analyse a network traffic to understand and identify security issues and challenges.

You are allowed to use any appropriate tools to complete this activity. I would strongly recommend you to work on/ complete any activity given to you in your virtual environment.

Remember ethical considerations at all the time.

Quiz!!! Have you ever tried tshark?

Advise:

- ✓ Patience is very important.
- ✓ Give attention to details
- ✓ Try to understand the flow of the network comprehensively
- ✓ Work based on the task given to make your life easier (avoid overwhelming!!!)
- ✓ Go back and refer to the basics (network protocols, OSI Layers, Header file etc)
- ✓ Document your findings
- ✓ Well-structured approach is the key

Refer to my lecture on working with captured network packets for your understanding. Similar kind of activities will be in your CBT.

Deliverables:

1. Answer all the 3 questions. Respond to questions with adequate explanation and include the scripts used.
2. Include the names of your classmate/ team member with whom you collaborated.

Tasks to complete

1. From the captured packets, identify all the web servers that were successfully accessed. We want to know the list of web servers, even if the website didn't work perfectly. We're only looking at regular connections, not secure or private connections (like online banking). We're not concerned with the specific problems on accessing the web servers, like errors or missing pages.

How to do?

- + Understand the protocol used by web servers and the codes associated with it.
 - + Use a tool to look at the network trace (like Wireshark).
 - + Find the web traffic in the trace.
 - + Make a list of the web server addresses.
 - + Ignore the secure or private connections.
 - + Don't worry about any issues on the websites; (refer to codes)
2. From the captured packets, find out any plain text user names and passwords. You must look at valid user names and passwords only.

How to do?

- + Understand the protocol used to send user names and passwords on a plain text.
 - + Use a tool to look at the network trace (like Wireshark).
3. From the captured packets, find out if any older versions of web servers. Trace further to get the host IP address and the web servers version

How to do?

- + Understand web servers, its versions and protocols.
- + Use a tool to look at the network trace (like Wireshark).

For all the above tasks, Try this!!!

- + Use Python to script the analysis and execute the code.

This Page is
intentionally left blank

Task 6: Use Tools of your choice to scan for network, identify vulnerabilities, assess the vulnerabilities and enumerate

1. Demonstrate a simple Network Scan on your simulated environment, pick up a vulnerability, and try to enumerate the vulnerability.
2. Demonstration Time: 10 Minutes
3. Do the scan – Record your discussion beginning from your type of scan, outcomes of your scan, and your approach in detailing the vulnerabilities and enumerating them.
4. Prepare for your demo and submit the video link (using OneDrive, Panopto, YouTube etc) in Moodle. The duration is 10 minutes, explain your topology, show you scan types and outcomes. Walkthrough your steps in detailing the vulnerabilities and enumerating the vulnerabilities.
5. If you volunteer to do the demonstration during our Tutorials/ Lecture, you need not submit your work in Moodle.

Record your Reflection:



1. Understanding on all the activities
2. Understanding about various tools used
3. New/ Similar tools you identified and used
4. Compare and Contrast the tutorial tools with your identified tools
5. Rate yourself: How confident are you to Gather Information, Assess Vulnerabilities and Enumerate the network ethically?
6. Any other Troubleshooting Steps, you need to share?