

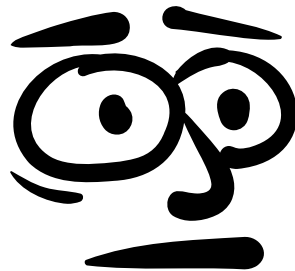


PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing
Wales Institute of Science and Art
(WISA)

Advanced Cybersecurity (ACCB6000)

Analyse, Scan and Enumerate Vulnerabilities



Objectives

In continuation to our earlier lectures, this tutorial has two parts.

Part 1 helps you to understand the flow of packets in the network, working with captured packets – give attention to details in the packets and analyse the packets to identify any security issues.

Part 2 helps you to scan a network, identify vulnerabilities and search details on the listed vulnerabilities and enumerate them if possible.

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. You are NOT allowed to use any tools listed in any of this or earlier or future activities (even for educational purposes) on an outside environment.

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 the Wireshark Captured network traffic to analyse the network and identify security details.

Task 2: Use Tools of your choice to scan for network, identify vulnerabilities, assess the vulnerabilities and enumerate

You need to complete and submit both the tasks in Moodle

ICONS Used in this document:

Find out the outcome/ Answers/ Solution



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.

Recommended Screenshot (with Timestamp) for your Coursework.

Recommended to address this part in your Coursework.

Record your Reflection

Task 1

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

Requirements: .pcap file (available in moodle – Capture_1_KuM)

Brief:

Use your knowledge, understanding, and cognitive skills, - *refer to the lecture and tutorial activities done in the last 4 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

I will show my approach in working with captured network packets and upload the files I used for your understanding after the lecture.

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)

Try this!!!

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

Try this!!!

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

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).

Try this!!!

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

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.
3. Note: Atleast 3 Questions will be in this approach for your 10% CBT marks in this module.

Task 2

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 in advance – Record your discussion beginning from your type of scan, outcomes of your scan, and your approach in detailing the vulnerabilities and enumerating them.
4. You need not submit it in Moodle, if you have done the demonstration during the lecture/ tutorials.
5. 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.