HANDS-ON CYBERSECURITY CAPSTONE PROJECT

This project aims to test your assimilation of the Cybersecurity training based on different categories covered during the course. Areas you will be tested upon include Networking setup, Penetration testing, Malware/Malicious file Analysis and OSINT/Linux Command Essentials.

INSTRUCTIONS: Install the following chrome extension – scre.io, a screen-recording software extension for making pre-recorded videos of your screen and your camera at any time.

You are required to do a screen recording/recorded video of the Penetration tests, Malicious file analysis and OSINT/Linux command exercises which will be submitted as proof of your project.

NETWORKING

You will begin by downloading Ubuntu Operating System – the ISO file. Download the Ubuntu OS from the Ubuntu website. Direct link https://ubuntu.com/download/desktop

File link: https://releases.ubuntu.com/24.04.3/ubuntu-24.04.3-desktop-amd64.iso

Once downloaded, install Ubuntu inside virtualbox (oracle) as a virtual machine. Make sure it is in the same subnet 192.168.56.X as your other virtual machines in your local network. It must have two adapters/adapter interfaces and must be able to browse/access the internet.

PENETRATION TESTING

With your kali linux OS, generate a linux-based payload which can compromise your Ubuntu machine. Your payload should be able to establish a reverse-shell connection to your kali linux machine.

Move the generated payload into your Ubuntu machine.

Using any listener of your choice (***meterpreter*** or ***netcat***) exploit/hack into your new ubuntu system from kali.

MALWARE/MALICIOUS FILE ANALYSIS

Examine/Analyze the payload using any malware analysis tool of your choice and establish the following:

- How high/low risk is this payload based on percentage OR percentage-wise?
- How many security vendors in total flag it as malicious ?

- What is the SHA-256 file hash of the payload you used in Ubuntu hack?
- What is the MD-5 hash of the payload you used in your Ubuntu hack ?

OSINT/LINUX COMMAND ESSENTIALS

DXYTECH has a website with URL/web address dxytechub.com.

Run full **OSINT/Reconnaissance** on https://dxytechub.com and answer/extract the following information

- What hosting provider does dxytechub.com use?
- When was this website hosted?
- What is the IP address of the hosting server which hosts this website?
- How many ports are open on this server and what ports are these?
- Is there any email associated with dxytech's website? What is the email address?

NOTE: Submit screen recordings, and also a written report with screenshots + answers.

ASSESSMENT

Networking setup – **20%,** Pentest – **30%**, Malware analysis – **25%,** OSINT/Linux – **25%**