Scenario

As a key member of the Digital Guardian Corp, you are identified by your codename 'Archon'. You belong to the Arch Angel team, renowned in the industry for their unparalleled skills in the realm of cybersecurity, specifically, pentesting and security audits.

Your latest assignment is a challenging one, you have been hired by an infamous conglomerate, Evil Co and Associates. Your mission is to conduct an initial reconnaissance of their digital fortress, to identify and report any potential vulnerabilities that may exist within their complex network.

Day 1 begins with the gathering of as much publicly available information on Evil Co and Associates as possible. This process, known as Open Source Intelligence (OSINT), involves looking into employee profiles on LinkedIn, scanning social media for any posts by or about the company, and scouring their website for potential loopholes. The objective is to build a digital footprint of the company without alerting them of your activities.

Meanwhile, you also kickstart the Network Enumeration process, mapping out Evil Co's systems, identifying live hosts, IP addresses, and open ports. This will serve as the blueprint for the next stages of the operation.

Your actions are monitored and guided by your wise supervisor, Professor Magneto. A veteran in the field of cybersecurity, Professor Magneto not only provides technical expertise but also keeps the team's morale high with his witty remarks and encouraging words.

By the end of the week, you have amassed a significant amount of data. You start classifying them according to relevance and potential exploitability. With your team's help, you conduct preliminary analysis, noting down potential weak points that could be utilized for the actual penetration testing.

As the week comes to a close, it's time for the crucial task: writing a comprehensive report to Professor Magneto. The report includes an overview of Evil Co and Associates, the methods used for information gathering, the blueprint of their network systems, potential vulnerabilities identified, and recommendations for the next steps.

However, the journey has just begun. With Professor Magneto's approval, Arch Angel will prepare for the next phase, ready to expose the darkest secrets hidden within Evil Co's digital fortress, and strengthen their fortifications against cyber threats lurking in the shadows. The mission is risky, but for the Arch Angel team, it's all in a day's work.

Assignment Objectives

Setup VMWare or select Hypervisor in a network with the following virtual machines:

a. PFSense or OPNSense
b. Windows Server 2019/2022
c. Parrot or Kali Linux
d. OWASP Broken Application
e. Windows 10/11 Enterprise

Configure the Network Gateway

f. Setup PFSense/OPNSense as a firewall/network gateway
g. Configure DHCP
h. Configure Firewall
i. Configure 2 NICS (NAT & LAN)
j. Passthrough networking from all VMs through the Network Gateway

Perform all the stages up-to Enumeration

Screenshot each stage with your name in it (kali/parrot user should be your name ie. Travis Lothar Czech & Student Number: 1234567890 – tczech890)

k. Usernames should be your initial, name, last three of student number
l. Screenshot your process

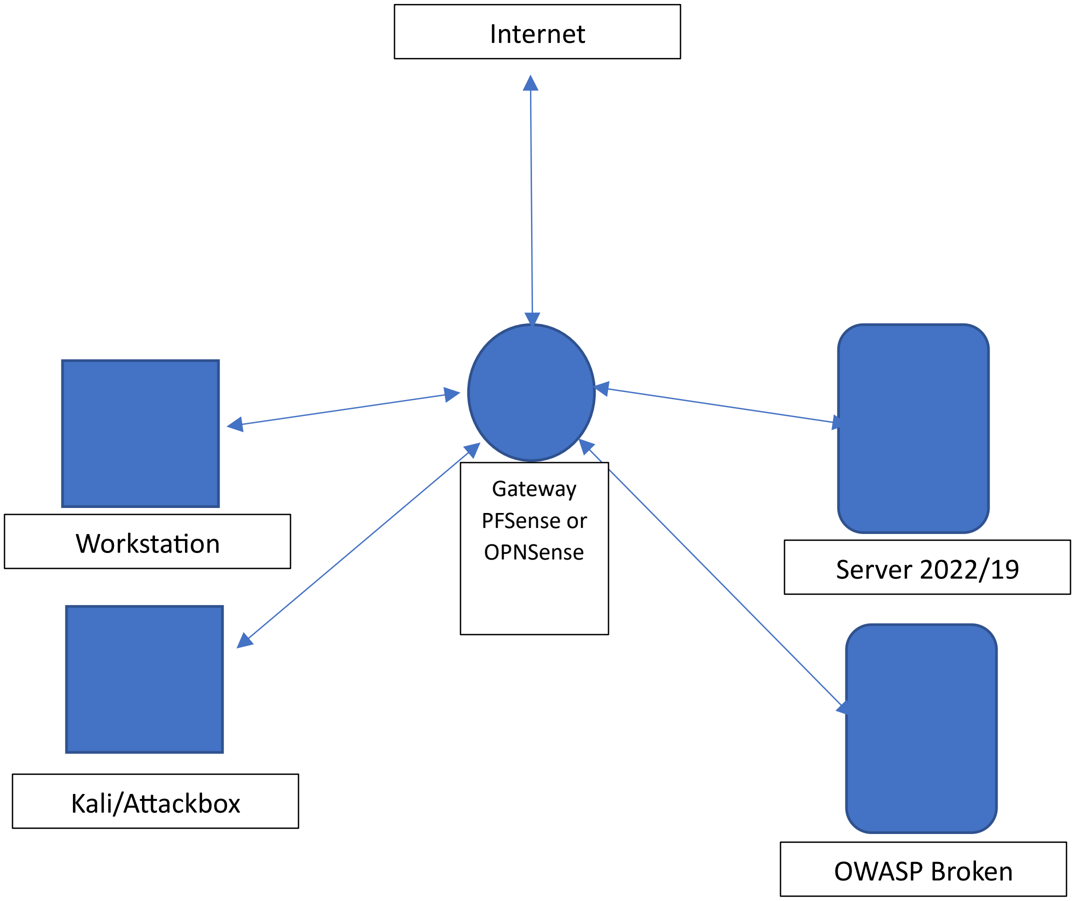
Write a report of your findings

m. Pentesting report
n. Report format
o. Annex A should be your screenshotted process

Ruberic

Objective	100%	75%	50%
Virtual Network Setup	Effectively Demonstrates an Understanding of Networking and Hypervisor Technology	Somewhat understands, and demonstrates networking, and virtualization techniques.	Utilized the required technologies, however didn't demonstrate an adequate knowledge.
Report Writing	Effectively Communicates Knowledge and Understanding of what is required in a penetration testing report while highlighting vulnerabilities, risks, mitigation strategies, and formatting.	Writes a report that communicates the steps taken, and an understanding of a pentesting report.	Wrote a report, however didn't fully demonstrate an understanding.
Stages of Security Testing	Uses an established framework to break down the stages of pentesting, and uses it to develop an effective report.	Referenced a framework, and somewhat applied it.	Loosely applied a framework.
Understanding Legal Requirements	Researches the applicable Laws, and Regulations. Communicates them, and utilizes them as part of the assignment.	Somewhat understands the legal requirements.	Loosely utilized laws or regulations.
Footprinting	Applies and Demonstrates techniques, and includes them in the report.	Somewhat demonstrates the techniques required.	Loosely demonstrated the required techniques.
Scanning	Applies and Demonstrates techniques, and includes them in the report.	Somewhat demonstrates the techniques required.	Loosely demonstrated the required techniques.
Enumeration	Applies and Demonstrates techniques, and includes them in the report.	Somewhat demonstrates the techniques required.	Loosely demonstrated the required techniques.

Network


Internet
Workstation
Gateway
PFSense or
OPNSense
Server 2022/19
Kali/Attackbox
OWASP Broken

Resources

- https://opnsense.org/download/
    - https://www.youtube.com/watch?v-5SXZnKQCgR8
    - https://atxfiles.netgate.com/mirror/downloads/
        - You can use PFSense instead of OPNSense if faced with issues
- https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/
    - Windows 11 Machine
- https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022
    - Server 2019 is acceptable
- https://www.kali.org/get-kali/#kali-platforms
    - Your Choice of Kali or Parrot
- https://www.vulnhub.com/entry/owasp-broken-web-applications-project-12,46/
    - Must be installed