Module 05

Vulnerability Analysis

Learning Objectives

01 Summarize Vulnerability Assessment Concepts

02 Use Vulnerability Assessment Tools

03 Analyze Vulnerability Assessment Reports

Objective 01

Summarize Vulnerability Assessment Concepts

Vulnerability Classification

Vulnerability Type	Description	Examples
Misconfigurations/Weak Configurations	• Misconfigurations occur when systems, applications, or devices are not configured correctly, leaving them susceptible to exploitation • It allows attackers to **break into a network** and gain unauthorized access to systems	**Network Misconfigurations** • Insecure protocols, open ports and services, errors, and weak encryption **Host Misconfigurations** • Open permissions and unsecured root accounts
Application Flaws	• Application flaws are vulnerabilities in applications that are exploited by attackers • Flawed applications pose security threats such as **data tampering** and **unauthorized access** to configuration stores	• Buffer overflows, memory leaks, resource exhaustion, integer overflows, null pointer/object dereference, DLL injection, race conditions, improper input handling, improper error handling, and code signing weakness
Poor Patch Management	• Software vendors provide patches that **prevent exploitations** and reduce the probability of threats exploiting a specific vulnerability • Unpatched software can make an application, server, or device **vulnerable to various attacks**	• Unpatched servers, unpatched firmware, unpatched OS, and unpatched applications
Design Flaws	• Logical flaws in the functionality of the system are exploited by the attackers to **bypass the detection mechanism** and acquire access to a secure system	• Incorrect encryption and poor validation of data
Third-Party Risks	• Third-party services can have access to privileged systems and applications, through which financial information, customer and employee data, and processes in the enterprise's supply chain can be compromised	• Vendor management, supply-chain risks, outsourced code development, data storage, and cloud-based vs. on-premises risks

Vulnerability Scoring Systems and Databases

Common Vulnerability Scoring System (CVSS)

- CVSS helps capture the principal characteristics of a vulnerability and produces a numerical score to reflect its severity

https://www.first.org

CVSS Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

National Vulnerability Database (NVD)

- NVD is the U.S. government repository of standards-based vulnerability management data
- NVD performs an analysis on CVEs that have been published to the CVE Dictionary

https://nvd.nist.gov

Common Weakness Enumeration (CWE)

- CWE is a category system for software vulnerabilities and weaknesses
- CWE's over 600 categories of weaknesses provide an effective baseline for the community's identification, mitigation, and prevention efforts

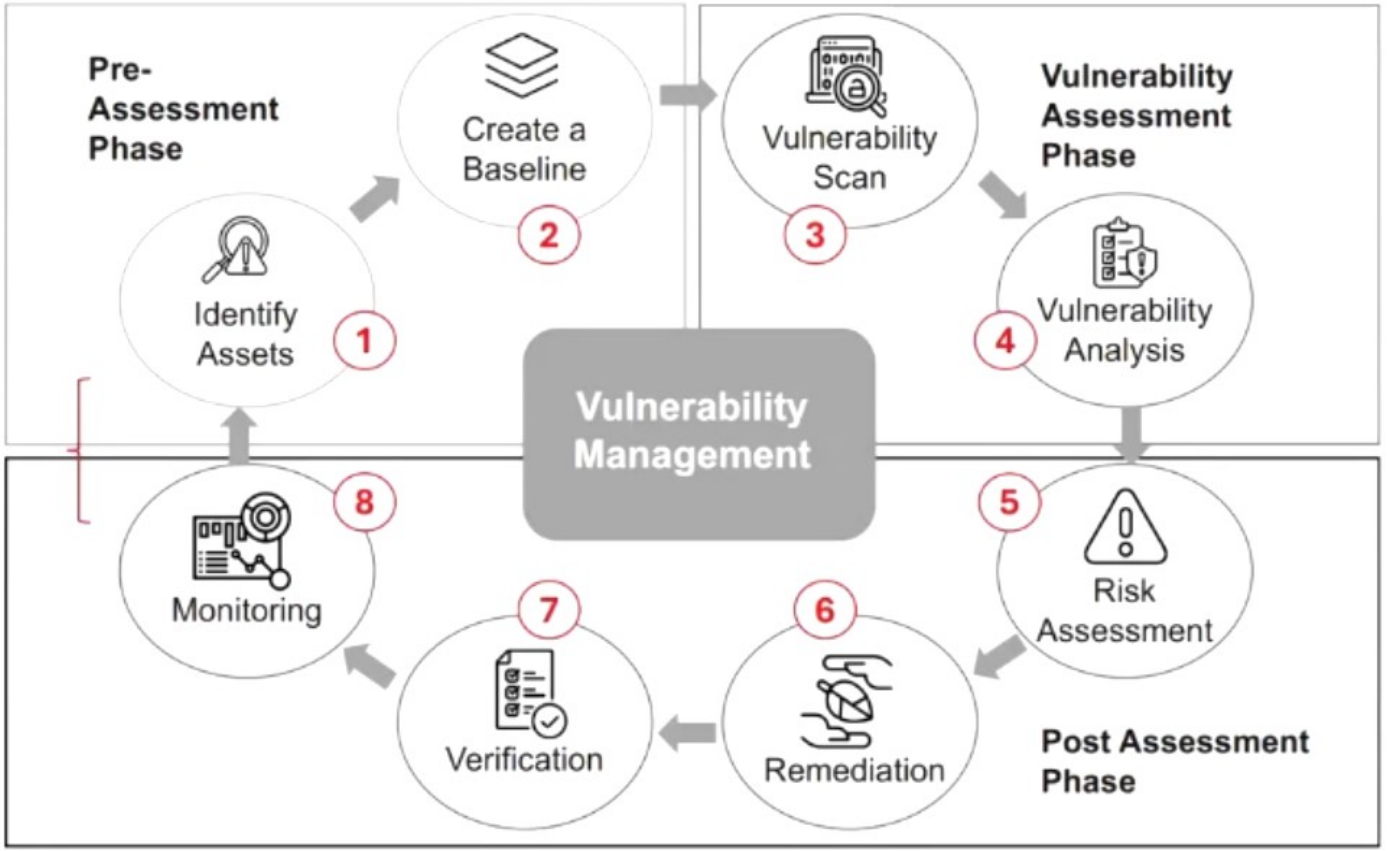
https://cwe.mitre.org

Common Vulnerabilities and Exposures (CVE)

- CVE® is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures

https://cve.mitre.org

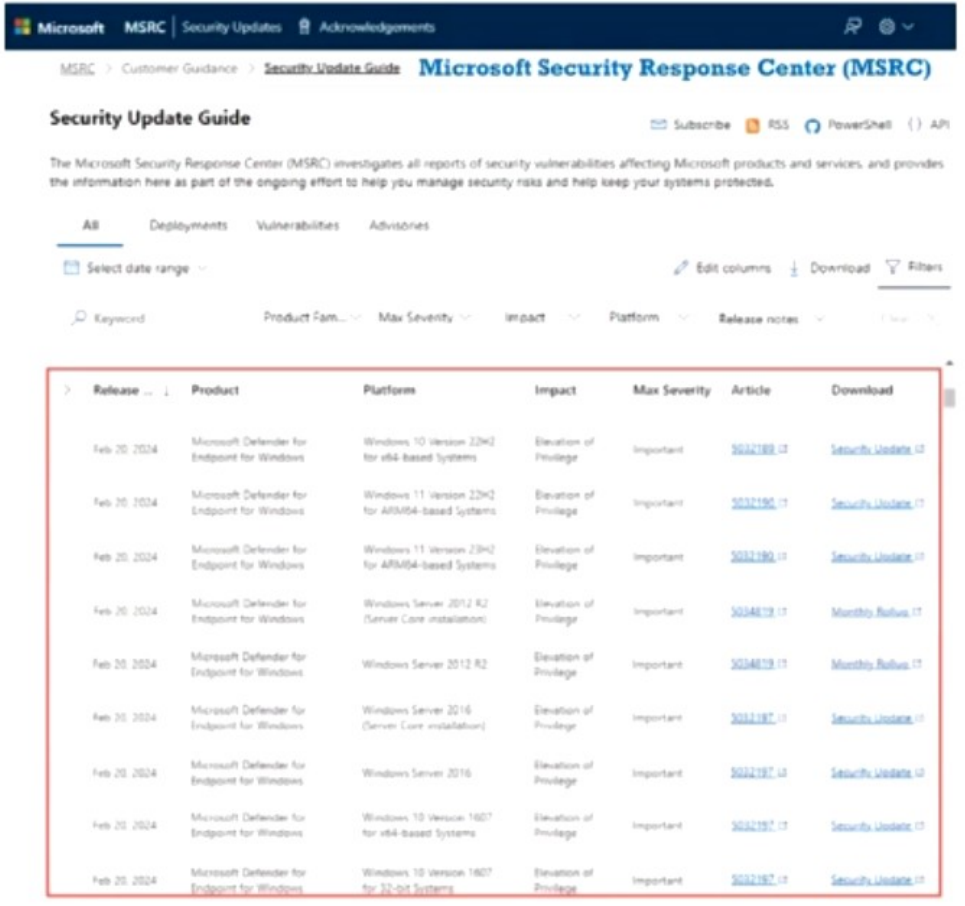
Vulnerability-Management Life Cycle



Vulnerability Research

An administrator needs vulnerability research:

1. To gather information concerning **security trends**, **threats**, **attack surfaces**, attack vectors and techniques
2. To discover **weaknesses** in the OS and applications, and alert the network administrator before a **network attack**
3. To **gather information** to aid in the prevention of security issues
4. To know **how to recover** from a network attack



https://msrc.microsoft.com

Vulnerability Scanning and Analysis

1. Vulnerability scanning involves analyzing protocols, services, and configurations to **discover vulnerabilities and design flaws** that may expose an operating system and its applications to exploitation, attack, or misuse

2. Vulnerability analysis is the systematic process of **identifying**, **evaluating**, and **prioritizing** security weaknesses in systems, networks, applications, or protocols

3. Vulnerabilities are classified based on **severity level** (low, medium, or high) and **exploit range** (local or remote)

4. The goal of this analysis is to understand the **nature of these vulnerabilities**, assess their **potential impact**, and develop strategies to mitigate or eliminate them

Types of Vulnerability Scanning

1 External Scanning

Scans the network from a hacker's perspective to discover exploits and vulnerabilities that are accessible to the outside world

2 Internal Scanning

Scans the **internal infrastructure** to discover exploits and vulnerabilities

3 Host-based Scanning

Conducts a **configuration-level check** to identify system configurations, user directories, file systems, registry settings, etc., to evaluate possibility of compromise

4 Network-based Scanning

Determines possible **network security attacks** that may occur on the organization's systems

5 Application Scanning

Tests and analyzes all elements of the **web infrastructure** for any **misconfiguration, outdated content**, or **known vulnerabilities**

6 Credentialed Scanning

Scanner logs into the target system **using valid credentials** to perform a more thorough and comprehensive scan

7 Non-Credentialed Scanning

A security testing method that assesses systems, networks, and applications without using valid credentials to log into the target system

8 Manual Scanning

Manually **identifying, evaluating,** and **validating** security vulnerabilities in systems, networks, and applications

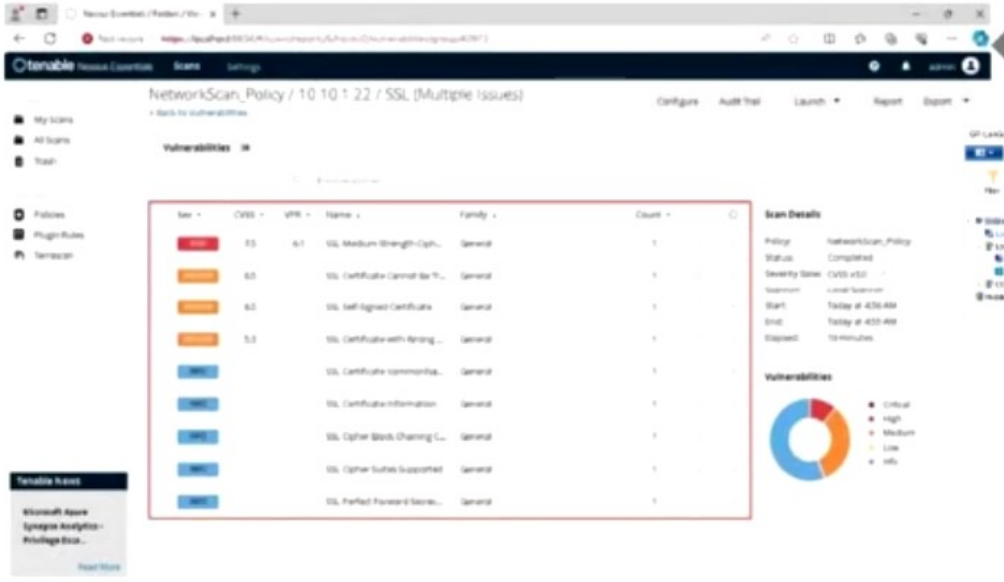
9 Automated Scanning

Uses automated software tools such as **Nessus, Qualys**, and **GFI LanGuard** to systematically identify, evaluate, and report security vulnerabilities

Objective 02

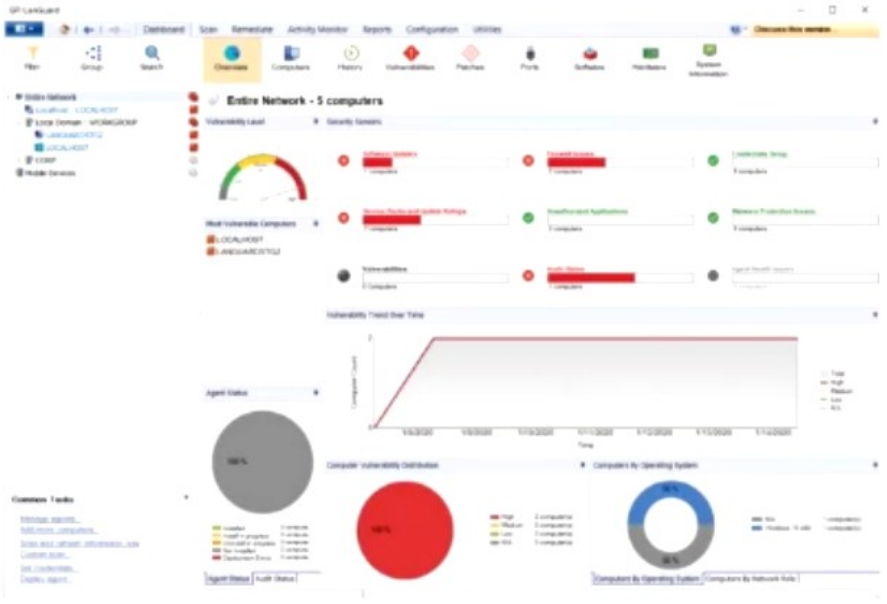
Use Vulnerability Assessment Tools

Vulnerability Assessment Tools: Nessus Essentials and GFI LanGuard



Nessus Essentials is an assessment solution for identifying **vulnerabilities**, **configuration issues**, and **malware**, which can be used to penetrate networks

https://www.tenable.com



GFI LanGuard scans, detects, assesses, and rectifies **security vulnerabilities** in a network and connected devices

https://www.gfi.com

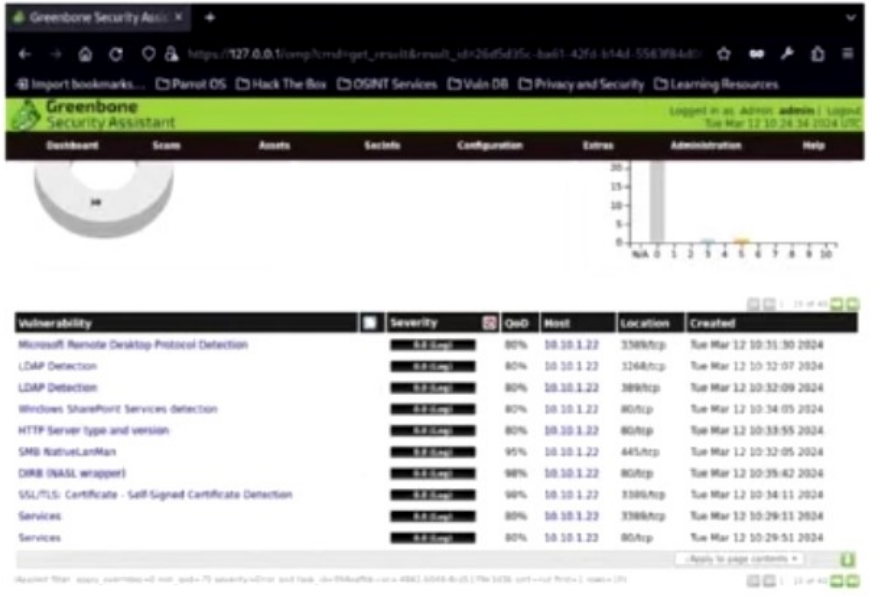
Vulnerability Assessment Tools: OpenVAS and Nikto

OpenVAS

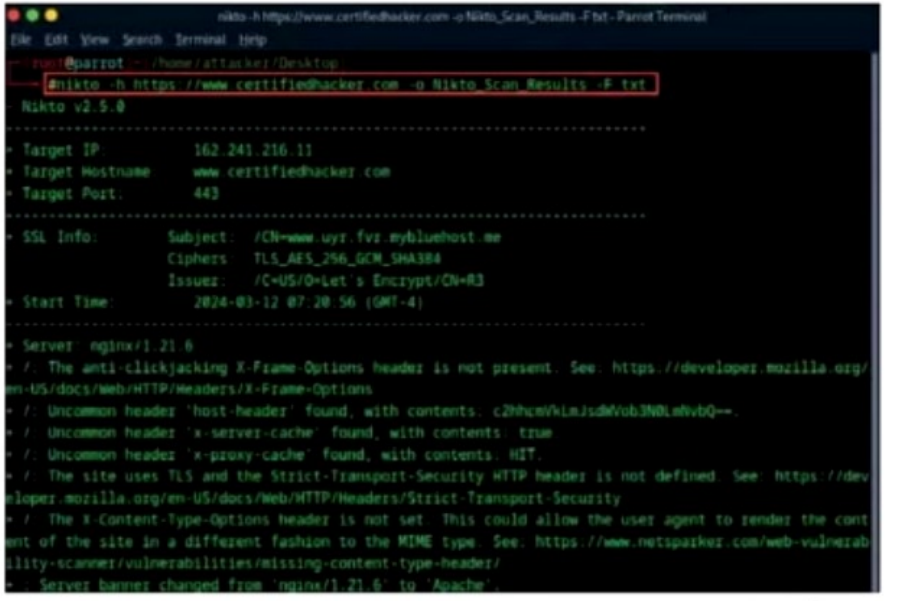
A framework of several services and tools offering a comprehensive and powerful **vulnerability scanning** and **vulnerability management solution**

Nikto

A **web server assessment tool** that examines a web server to discover potential problems and security vulnerabilities



https://www.openvas.org

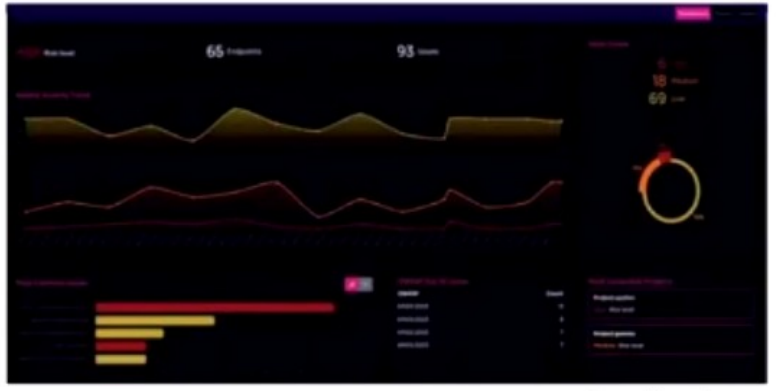


https://cirt.net

AI-Powered Vulnerability Assessment Tools

Equixly

- Equixly is a SaaS platform that integrates API security testing into the development workflow
- It leverages machine learning to **automate vulnerability assessments** and provide developers with actionable remediation plans



https://equixly.com

SmartScanner

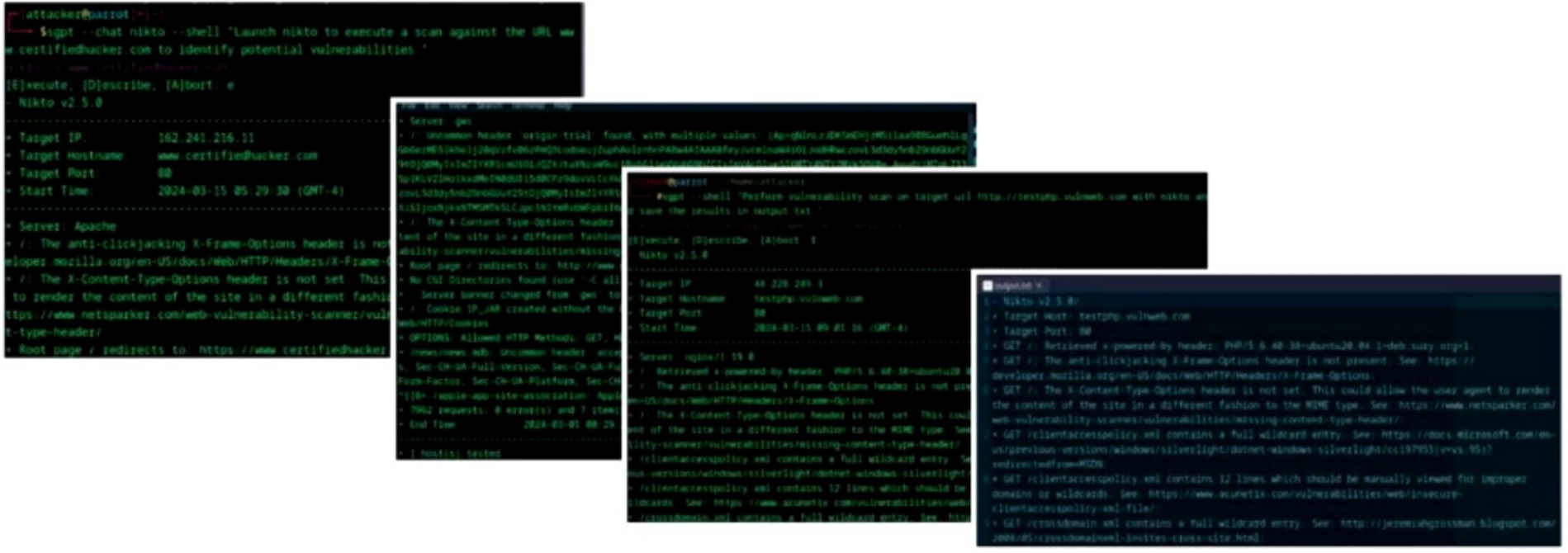
- SmartScanner an automated vulnerability scanner designed to **identify and mitigate potential vulnerabilities in websites** utilizes AI and machine learning (ML) to enhance its threat detection capabilities

https://www.thesmartscanner.com

Other Tools: **CodeDefender** https://codedefender.ro | **DryRun Security** *https://www.dryrun.security* | **Hackules** https://hackules.com | **Corgea** *https://corgea.com* | **Pentest Copilot** *https://copilot.bugbase.ai*

Vulnerability Assessment using AI

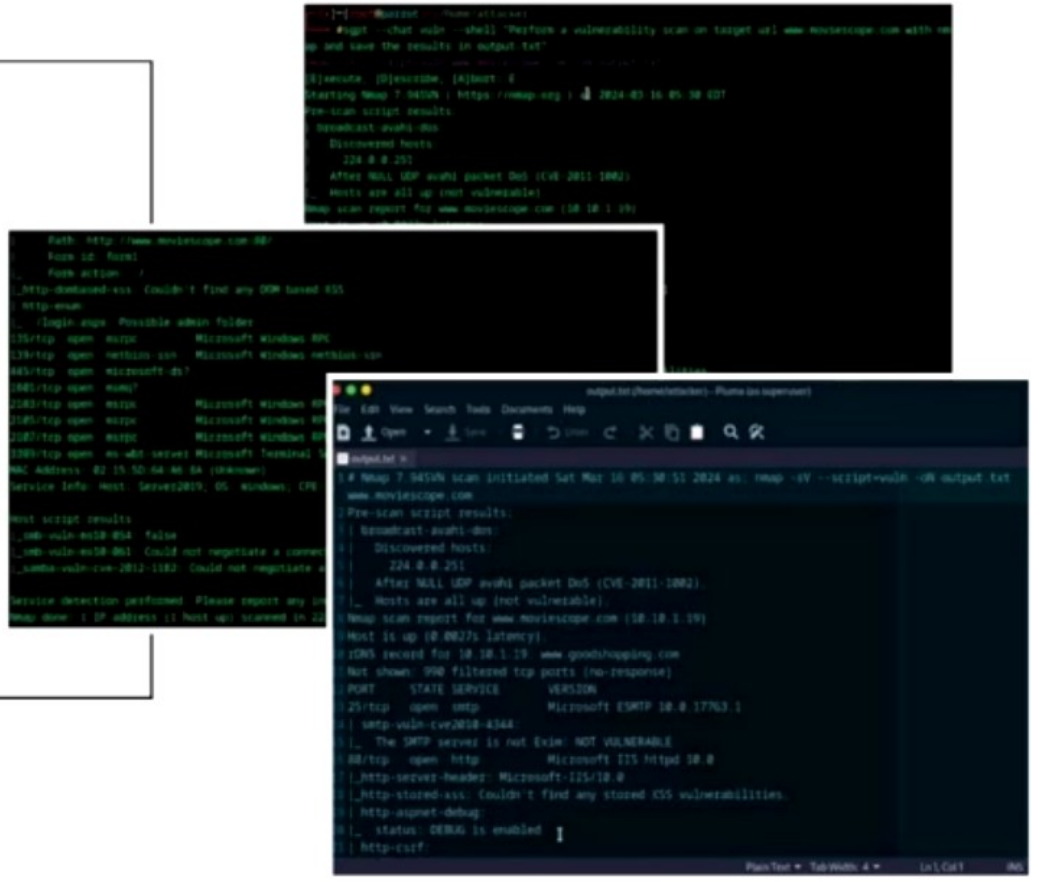
- An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as
  - ***"Launch nikto to execute a scan against the URL www.certifiedhacker.com to identify potential vulnerabilities."***
  - ***"Perform vulnerability scan on target url http://testphp.vulnweb.com with nikto and save the results in output.txt."***



Vulnerability Scan using Nmap with AI

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as

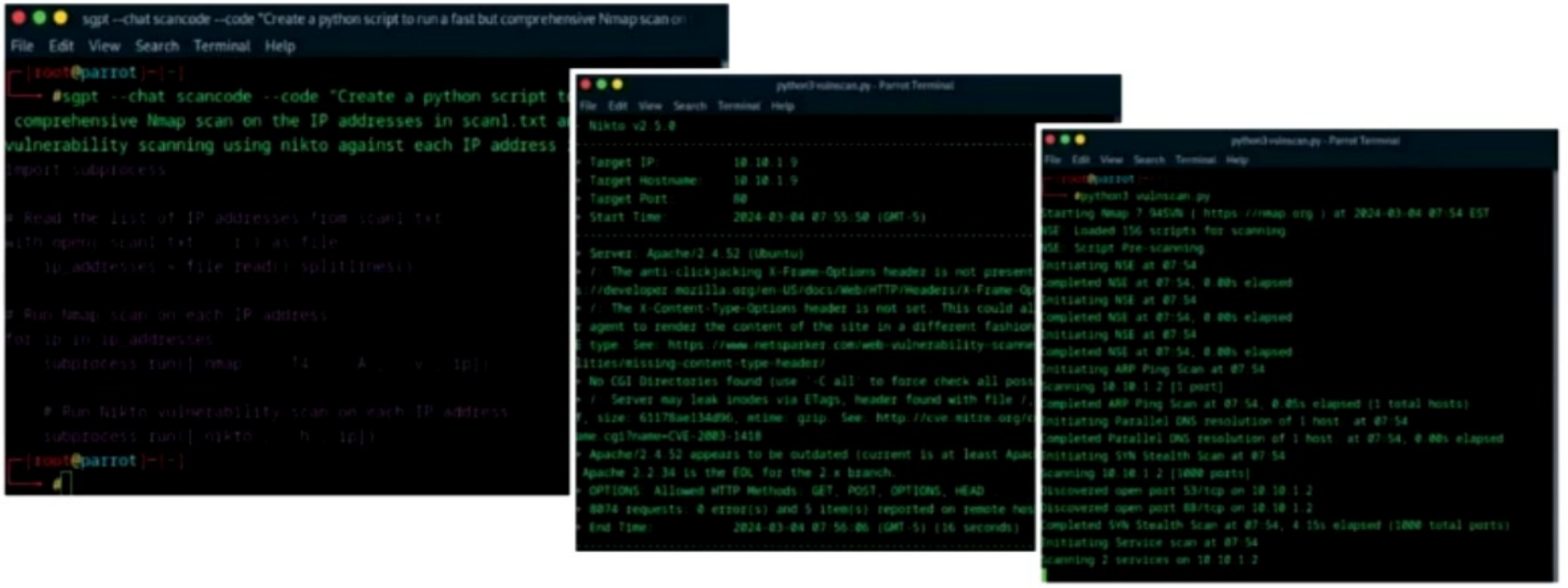
- ***"Perform a vulnerability scan on target url www.moviescope.com with nmap and save the results in output.txt"***



Vulnerability Assessment using Python Script with AI

- An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as

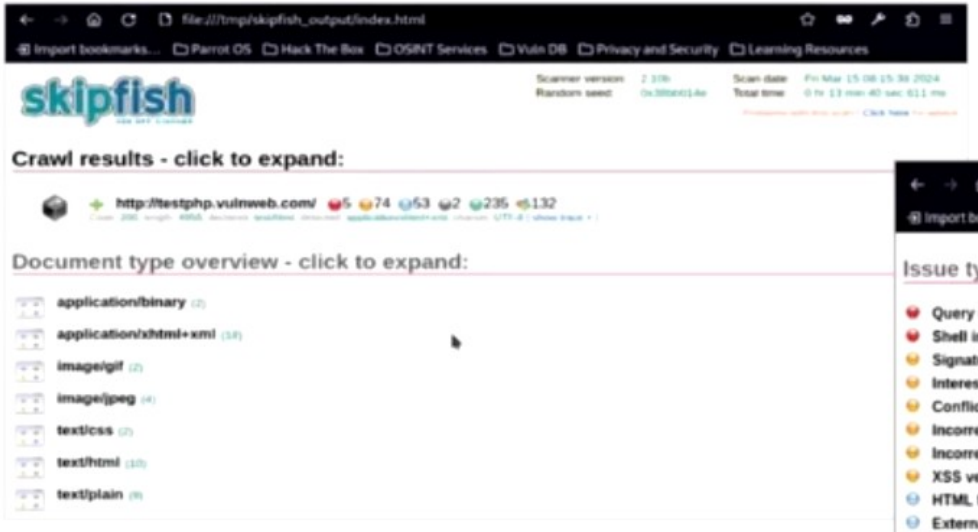
  sgpt --chat scancode --code "*Create a python script to run a fast but comprehensive Nmap scan on the IP addresses in scan1.txt and then execute vulnerability scanning using nikto against each IP address in scan1.txt*"

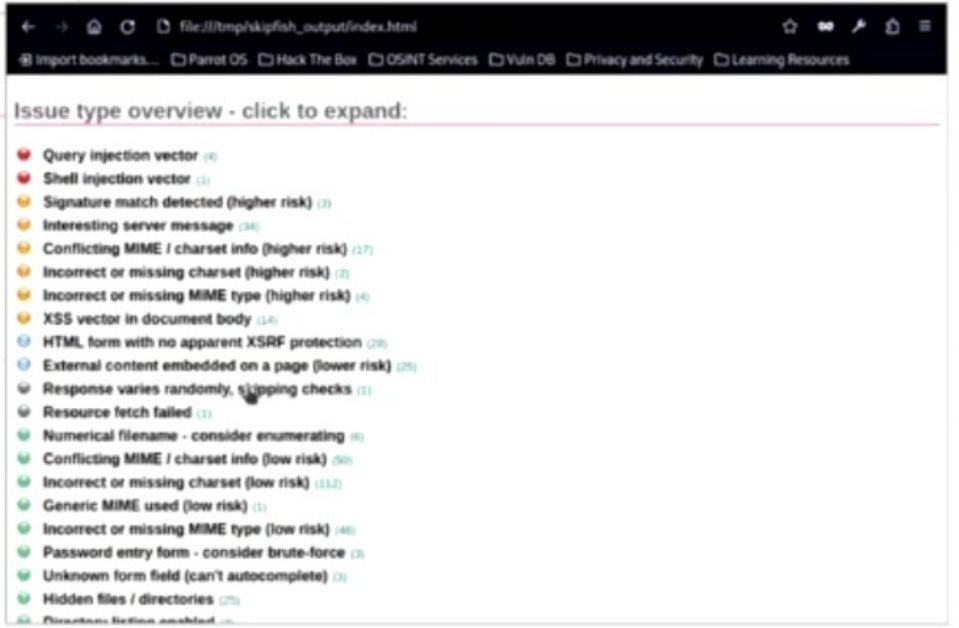


Vulnerability Scan using Skipfish with AI

- An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as
  - ***"Perform a vulnerability scan on target url http://testphp.vulnweb.com with Skipfish and display the output file index.html in Firefox "***

Vulnerability Scan using Skipfish with AI (Cont'd)





Objective 03

Analyze Vulnerability Assessment Reports

Vulnerability Assessment Reports

A vulnerability assessment report is a **comprehensive document** that details the findings of a vulnerability assessment

Executive Summary

- Assessment scope and objectives
- Testing narrative
- Findings summary
- Remediation summary
- Component compliance summary

Assessment Overview

- Assessment methodology
- Scan information
- Target information
- Tools involved

Findings

- Scanned hosts
- Affected assets
- Types of vulnerabilities identified
- Detailed information on identified vulnerabilities
- Notes describing additional details of scan results

Risk Assessment

- Classification of vulnerabilities based on the risk level
- Potential vulnerabilities that can compromise the system or application
- Critical hosts with severe vulnerabilities

Recommendations

- Prioritization of remediation based on the risk ranking
- Action plan to implement the recommendations for each identified vulnerability
- Root-cause analysis
- Application of patches/fixes
- Lessons learned
- Awareness training
- Implementation of periodic vulnerability assessment
- Implementation of policies, procedures, and controls

Appendices and Supporting Information

- Additional information that supports the report's findings such as detailed logs, configuration files, or references to external resources

Conclusion

- Summary of key findings and recommendations, reinforcing the importance of addressing the identified vulnerabilities

Follow-Up Actions and Timeline

- Timeline for re-assessment or follow-up actions to ensure vulnerabilities are addressed and to monitor the effectiveness of the remediation efforts

Glossary of Terms

- Definitions for technical terms used in the report

Module Summary

- In this module, we have discussed:
  - Various types of vulnerabilities, the CVSS vulnerability scoring system, and databases
  - The vulnerability-management life cycle and vulnerability research
  - Vulnerability scanning, vulnerability analysis, and various types of vulnerability scanning techniques
  - Various vulnerability assessment solutions, along with their characteristics
  - Various tools that are used to test a host or application for vulnerabilities, along with the criteria and best practices for selecting the tool
  - We concluded with a detailed discussion on how to analyze a vulnerability assessment report and how it discloses the risks detected after scanning the network
- In the next module, we will discuss the methods attackers, as well as ethical hackers and pen testers, utilize to hack a system based on the information collected about a target of evaluation; for example, footprinting, scanning, enumeration, and vulnerability analysis phases