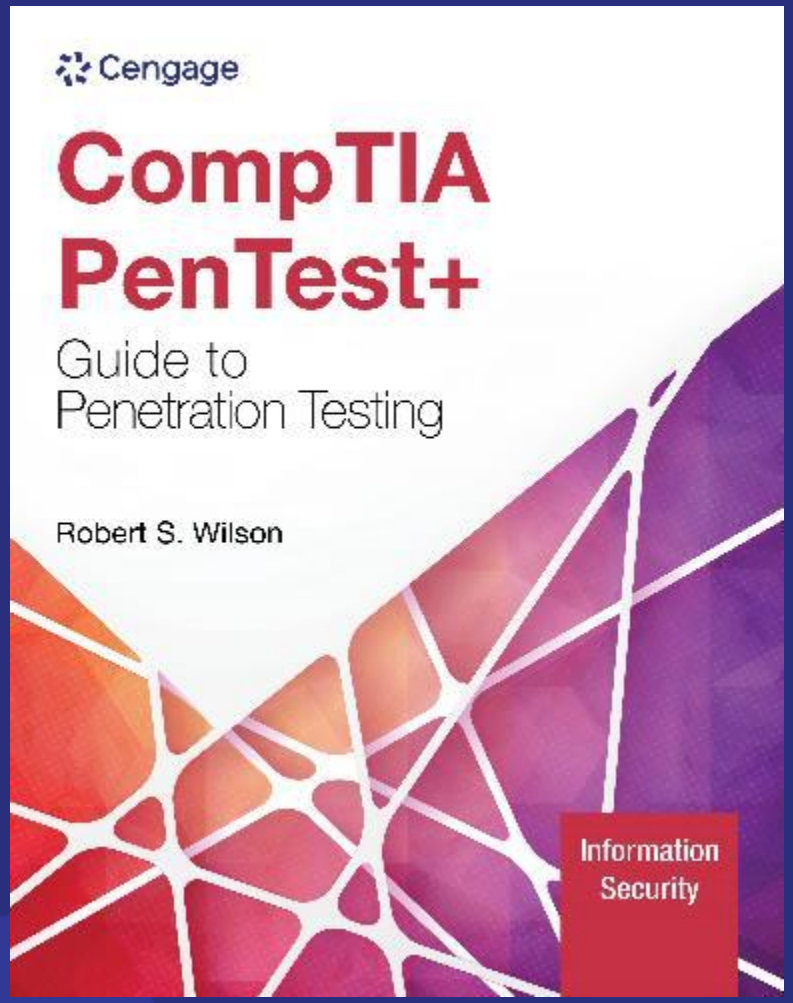


CompTIA PenTest+ Guide to Penetration Testing, 1e

Module 14: The Final Penetration-Testing Project

Preparing for Pen Testing

- Welcome to the final project
- This project consists of hands-on activities to be performed on the pen-testing environment
- Tools used are covered throughout this course in the various modules
- Results of the pen-testing project should be communicated using reporting format and methodology described in Module 12

Performing the Penetration Testing (1 of 4)

Using the `nmap` command

- `Nmap` is a useful command-line tool for discovering target devices and open ports on a network
- Using `nmap` can discover targets to use with other scanning tools like Nessus
- Ports identified on targets indicate what services are most likely running on the host
- Those services may provide clues as to the type or purpose of the system discovered

Performing the Penetration Testing (2 of 4)

Using the `netcat` Command and HTTP Methods

- The `netcat` or `nc` command and HTTP methods can extract information from web servers
- The info obtained using `netcat` to query HTTP servers may reveal vulnerabilities to target with exploits or additional scan tools
- The `nc` command can identify web server software or version info

Performing the Penetration Testing (3 of 4)

Using the `wget` Command

- The `wget` command can be used to extract information from web servers
- It can also download files from web servers

Using the `enum4linux` Command

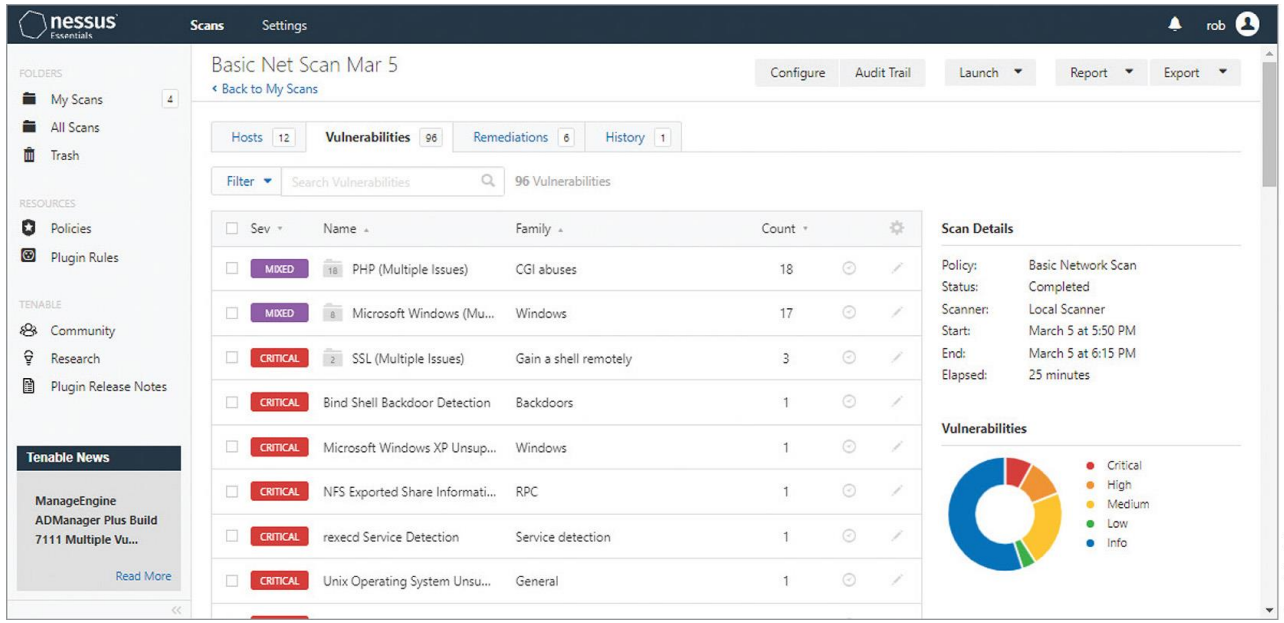
- The `enum4linux` is a powerful tool for enumerating SMB details from Windows and Linux target systems
- With this information, vulnerabilities may be discovered as well as targets for additional testing tools

Performing the Penetration Testing (4 of 4)

Using Nessus

Nessus is a powerful vulnerability scanning tool

- Scan all VMs with Nessus starting with Host Discovery
- Scan each VM with the “Basic Network” and “Web Application Scan” types
- Save the results for the final pen test report



Vulnerability information from a Nessus scan

Pen Testing Exploitable Vulnerabilities

- Vulnerabilities on various targets should have been discovered during this final project
- Pen testing involves attempting to exploit vulnerabilities in a nondestructive way
- Use Metasploit or other exploitation tool to exploit a vulnerability

Completing the Report

- After the penetration concludes, it is time to finalize the report
- Follow the methods and suggestions in Module 12 in order to create a pen-test report containing the results of the pen-test final project

Pen Testing Revisited

- This module's activities use only a few of the tools and methods presented throughout this course
- Value may be found in reflecting on the progression through this course
  - Consider what has been learned and what may be revisited
- The author encourages continued research and intelligence gathering from different viewpoints

With great power comes great responsibility, so remember to always wear your white hat when exercising some the newly acquired penetration testing abilities.

Self-Assessment 14-1

Now that the pen-testing course modules have been completed, learners should have a good understanding of the pen-testing process an ethical hacker or pen-test team will undergo. Briefly discuss and summarize each of the following steps in a penetration test.

- Planning and scoping
- Information gathering
- Vulnerability scanning
- Exploiting targets
- Social engineering
- Physical attacks
- Reporting and communication