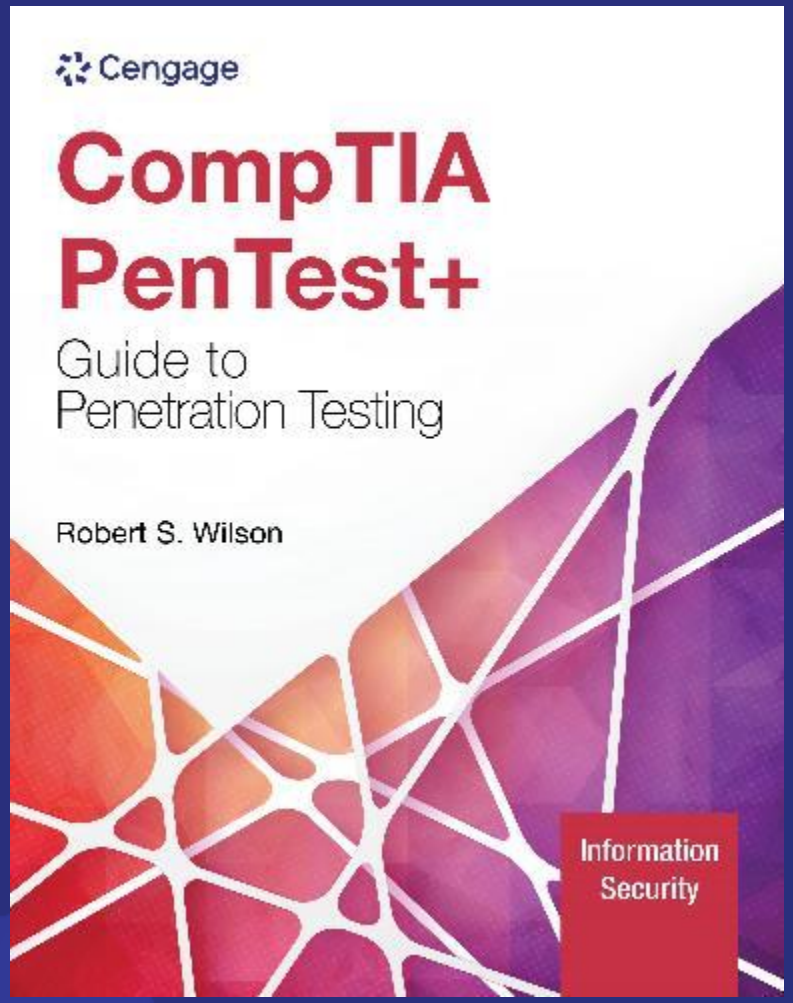


CompTIA PenTest+ Guide to Penetration Testing, 1e

Module 5: Performing Vulnerability Scanning

Module Objectives

By the end of this module, you should be able to:

1. Describe vulnerability scanning and its purposes
2. Describe methods and tools to discover targets for vulnerability scanning
3. Describe different types of vulnerabilities and vulnerability scans
4. Describe additional considerations when performing vulnerability scans
5. Execute vulnerability scans using different tools
6. Analyze the results of vulnerability scans

Understanding Vulnerability Scanning (1 of 26)

Key Terms

Vulnerability Scanning – looking for vulnerabilities in targets and weaknesses in services that can be exploited to circumvent security

Understanding Vulnerability Scanning (2 of 26)

Purpose of Vulnerability Scanning

Ultimate goal – to discover target vulnerabilities and weaknesses so they can be repaired before threat actors can exploit them

Clients may request penetration testing in the following scenarios:

- Proactive decision – check computing environment before cyber attack
- Reactive decision – reaction to security breach; need help fixing flaws
- Corporate policy – client organization has mandated testing and remediation; may include regulatory component
- Regulatory requirements – Legal or industry requirements such as PCI-DSS

Understanding Vulnerability Scanning (3 of 26)

Federal Information Security Management Act (FISMA)

- FISMA refers to two U.S. laws:
  - Federal Information Security Management Act of 2002
  - Federal Information Security Modernization Act of 2014
    - Amended original 2002 act
- Requires federal agencies to place security controls commensurate with risk and potential impact
- Federal Information Processing Standard (FIPS) 199 outlines these requirements

Understanding Vulnerability Scanning (4 of 26)

Federal Information Security Management Act (FISMA)

NIST SP 800-53 Vulnerability Scanning Requirements

- FISMA requires U.S. agencies to require scanning to NIST 800-53
  - Vulnerability scanning outlined in section “Security and Privacy Controls for Federal Information Systems and Organizations”
  - Guidance on vulnerability scans starting on page 242

Understanding Vulnerability Scanning (5 of 26)

Federal Information Security Management Act (FISMA)

NIST SP 800-53 Vulnerability Scanning Requirements (Examples)

- Scans for vulnerabilities in the information system and in hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported
- Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the process
- Analyzes vulnerability scan reports and results
- Remediates vulnerabilities in accordance with risk assessment

Understanding Vulnerability Scanning (6 of 26)

Determining Targets for Vulnerability Scanning

Potential sources of targets on which to conduct vulnerability scans:

- Statement of work (SOW)
- Rules of engagement (ROE)
- White box information
- Nmap and network discovery tools
- Assessment management and inventory tools
- Asset discovery scans via vulnerability scans

Understanding Vulnerability Scanning (7 of 26)

Determining Targets for Vulnerability Scanning

- Statement of work (SOW) – test only targets covered in scope of test
- Rules of engagement (ROE) – may forbid testing types and targets
- White box information – details provided to pen tester by client

Understanding Vulnerability Scanning (8 of 26)

Determining Targets for Vulnerability Scanning

- Nmap and network discovery tools – scanning tools using standard port scans or specialized tools like SNMP scanners can locate targets
- Assessment management and inventory tools – tools like Lansweeper can discover and inventory hosts on a target network
- Asset discovery scans via vulnerability scans – vulnerability scanners with Nessus perform inventory of hosts as part of vulnerability assessment and discovery

Understanding Vulnerability Scanning (9 of 26)

Types of Vulnerabilities

Vulnerability scanners can be categorized into software flaws and failure to follow best practices

Common vulnerability types

- Missing software patches
- Administrative accounts
- Default configurations
- Default permissions
- SSL/TLS certification issues
- Web application vulnerabilities

Understanding Vulnerability Scanning (10 of 26)

Types of Vulnerabilities

Specialized systems can be affected by less common vulnerabilities

Examples of specialized systems

- Industrial control systems (ICSs)
- Supervisory control and data acquisition systems (SCADA)
- Mobile devices
- Internet of Things (IoT) devices
- Embedded systems
- Point of sale (POS) systems
- Biometric devices
- Application containers
- Real-time operating systems RTOSs)

Understanding Vulnerability Scanning (11 of 26)

Types of Vulnerability Scans

Vulnerability scanning programs may offer preconfigured scan types or templates to chose from based on several factors:

- Type of target
- Need for scan to remain undetected
- Scans for compliance (PCI DSS, GDPR)
- Scans that may limit potential effect or impact on production type hosts
- White box scans with provided credentials or black box with no info

Understanding Vulnerability Scanning (12 of 26)

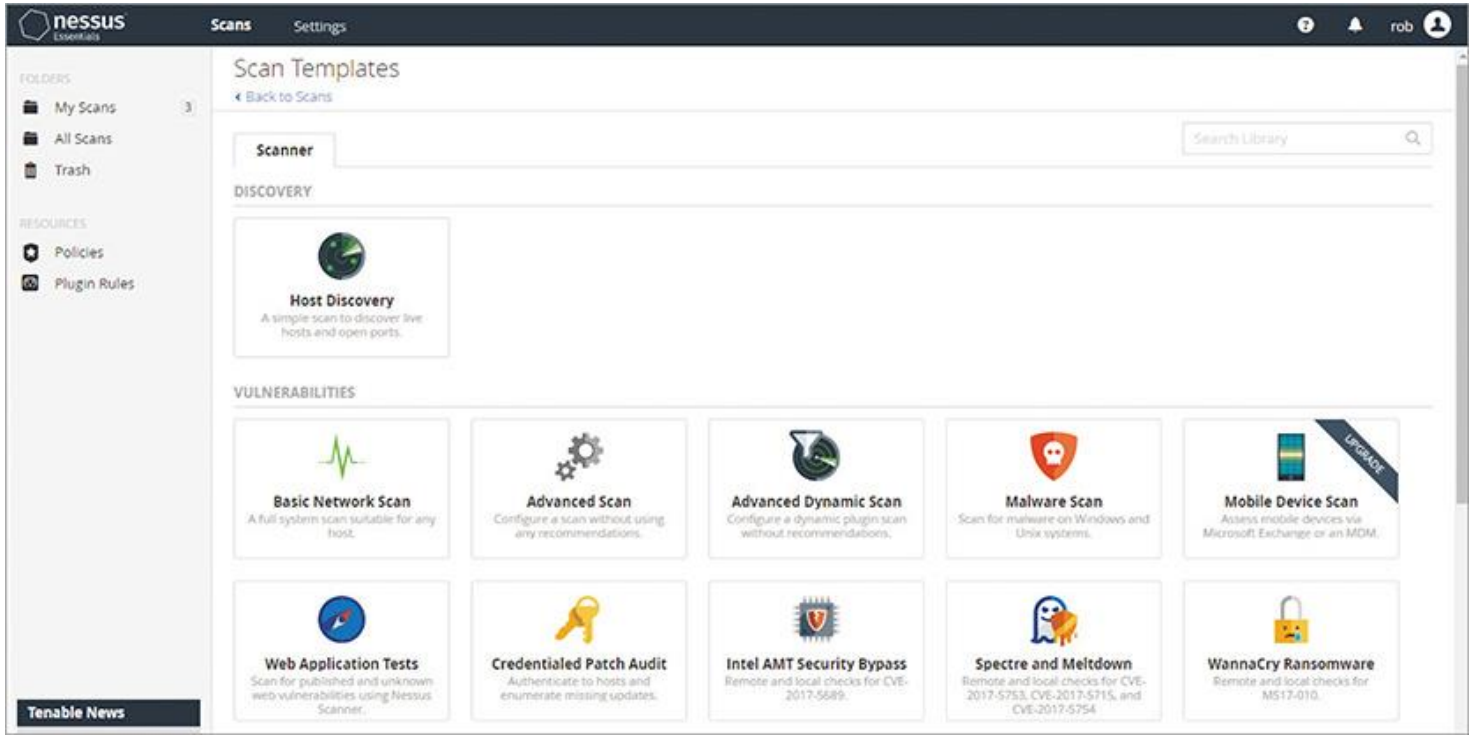
Types of Vulnerability Scans

- Discovery – locates hosts to follow up with a different scan
- Full – employs many scan methods and techniques; considered “noisy”
- Stealth – attempts to generate little traffic and remain undetected
- Compliance – custom scans to meet requirements of regulation (PCI DSS)
- Web application – targets web servers and apps for vulnerabilities
- Many other scan types available in vulnerability scanning tools
  - Some tools offer enhanced options for paid versions

Understanding Vulnerability Scanning (13 of 26)

Types of Vulnerability Scans

- Tenable's Nessus is a well-known vulnerability scanning tool
- Offers a wide range of scan types and templates for use
- Over 100k plug-ins for testing



Nessus scan templates

Understanding Vulnerability Scanning (14 of 26)

Types of Vulnerability Scans

- Credentialed scans
  - Use known account name and password during scan
    - Credentials may be provided by client or discovered during recon
    - Administrative credentials more useful than standard user account
  - Able to retrieve a large amount of information from target
- Noncredentialed scans
  - Performed in black box approach with no username or password
  - Less information typically discovered during this scan type

Discussion Activity 5-1

The state of computing and networks has evolved dramatically in the last ten years. Today, remote work is commonplace at organizations where it did not exist even just a few years ago.

Think about the modern computing landscapes at organizations that might seek penetration test services.

In small groups, discuss the challenges associated with pen testing organizations today that are associated with modern computing environments. How are those challenges different than five or ten years ago?

Understanding Vulnerability Scanning (15 of 26)

Application Vulnerabilities

- Web applications are a very common type of hacked application
- Web apps must reside on an accessible servers; easy targets
- Compromise of a web application can lead to host compromise
- Large variety of programming languages and platforms for web apps
  - Each has advantages and disadvantages
  - Easy app development or in-depth programming knowledge needed
  - Freely available, open-source, commercial or proprietary types

Understanding Vulnerability Scanning (16 of 26)

Application Vulnerabilities

- Application security (AppSec) overlooked as many security professionals have networking experience but little programming knowledge
- Programming sometimes overlooked in network security courses
- Best perimeter firewall and defenses circumvented with web or application vulnerabilities
- Network layer protection may not provide protection for applications
- Basic programming or scripting concepts can allow application exploits

Understanding Vulnerability Scanning (17 of 26)

Web Application Test Execution

Web application testing falls into two main techniques:

- Static application security testing (SAST) uses analysis of source code
  - Reliable way to enumerate vulnerabilities from software coding errors
  - “White box testing”
- Dynamic application security testing (DAST) necessary if no source code
  - “Black box testing”
- Interactive application security testing (IAST) combines both techniques
  - “Gray box testing”

Understanding Vulnerability Scanning (18 of 26)

Application Vulnerabilities and Countermeasures

- Open Web Application Security Project (OWASP)
  - Maintains a list of “Ten Most Critical Web Application Security Risks”

1. Injection vulnerabilities
2. Authentication flaws and weaknesses
3. Sensitive data exposure
4. XML External Entities (XXE)
5. Broken access control
6. Security misconfigurations
7. Cross-site scripting (XSS)
8. Insecure deserialization
9. Using components with known vulnerabilities
10. Insufficient logging and monitoring

Understanding Vulnerability Scanning (19 of 26)

Fuzzing

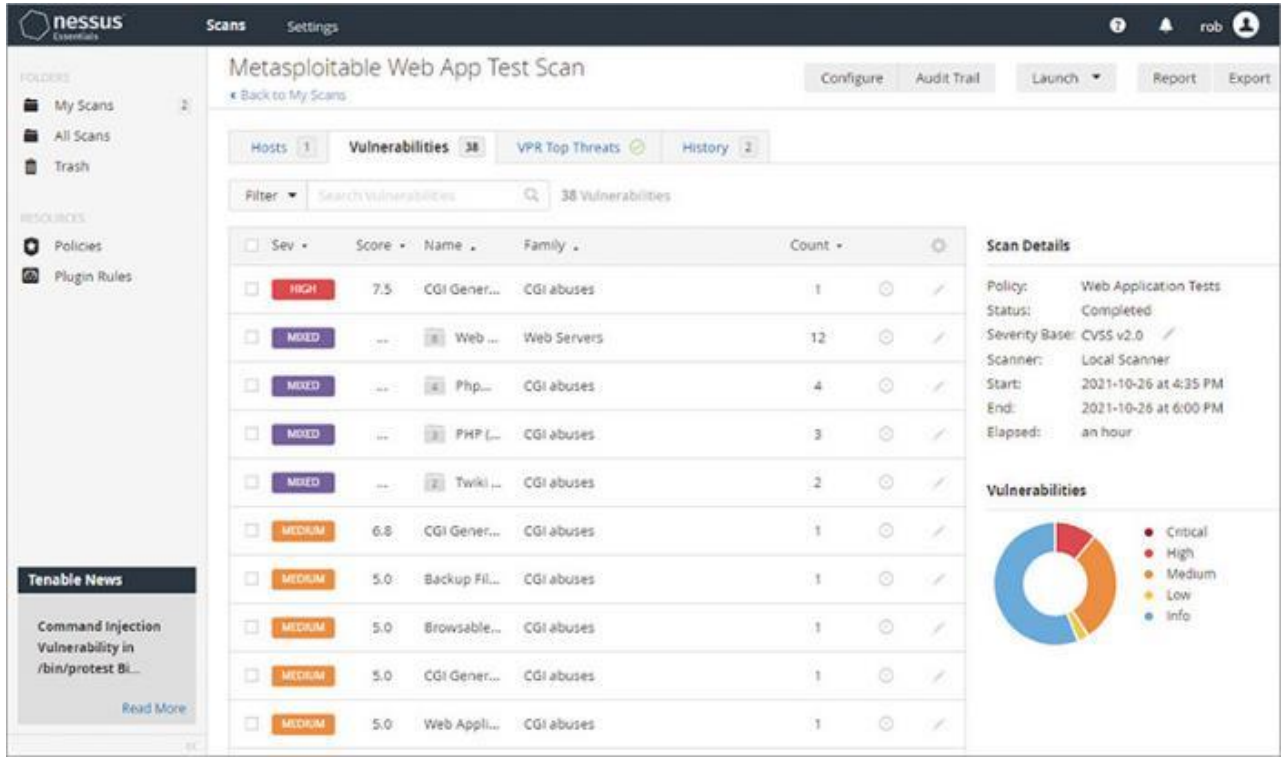
- Top OWASP application security risk “injection vulnerabilities” can be tested with “fuzzing” technique
  - Entering random information into all application input fields
  - Results can indicate potential vulnerabilities or potential to crash app
- Fuzzing with SQL input can determine potential SQL injection flaws

Understanding Vulnerability Scanning (20 of 26)

Web Application Vulnerability Scanning

Tenable Nessus

- Offers web application tests and templates
- Several commercial and free home editions



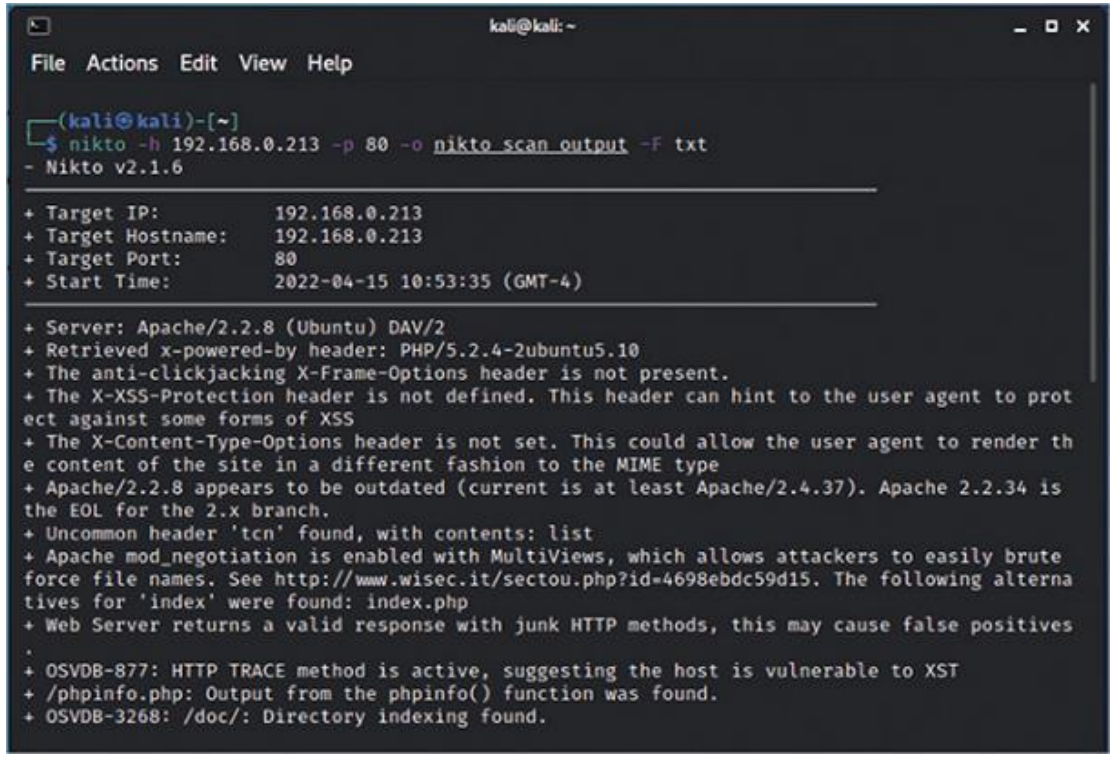
Nessus scan results

Understanding Vulnerability Scanning (21 of 26)

Web Application Vulnerability Scanning

Nikto

- Open source CLI web app scanner
- Supports many custom options for scans



Nikto example

Understanding Vulnerability Scanning (22 of 26)

Web Application Vulnerability Scanning

Wapiti

- Open source CLI web app scanner

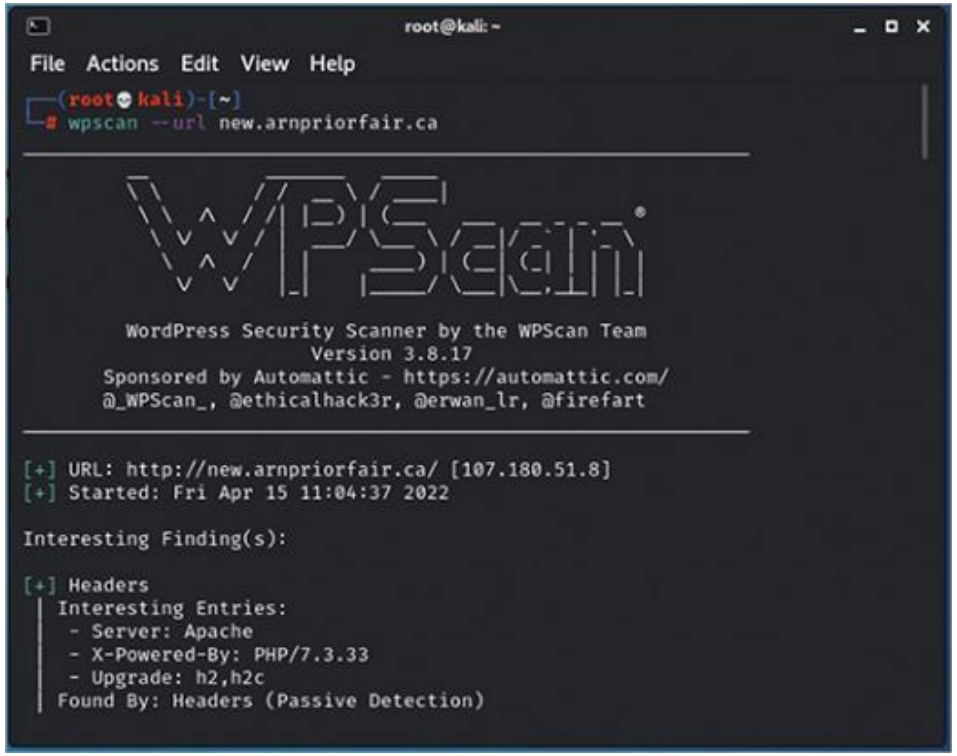
Wapiti example

Understanding Vulnerability Scanning (23 of 26)

Web Application Vulnerability Scanning

WPScan

- Targets WordPress platform
- WordPress is extremely popular web platform and content management system (CMS)
- WordPress sites often use many different plug-ins that can lack security and have exploitable flaws



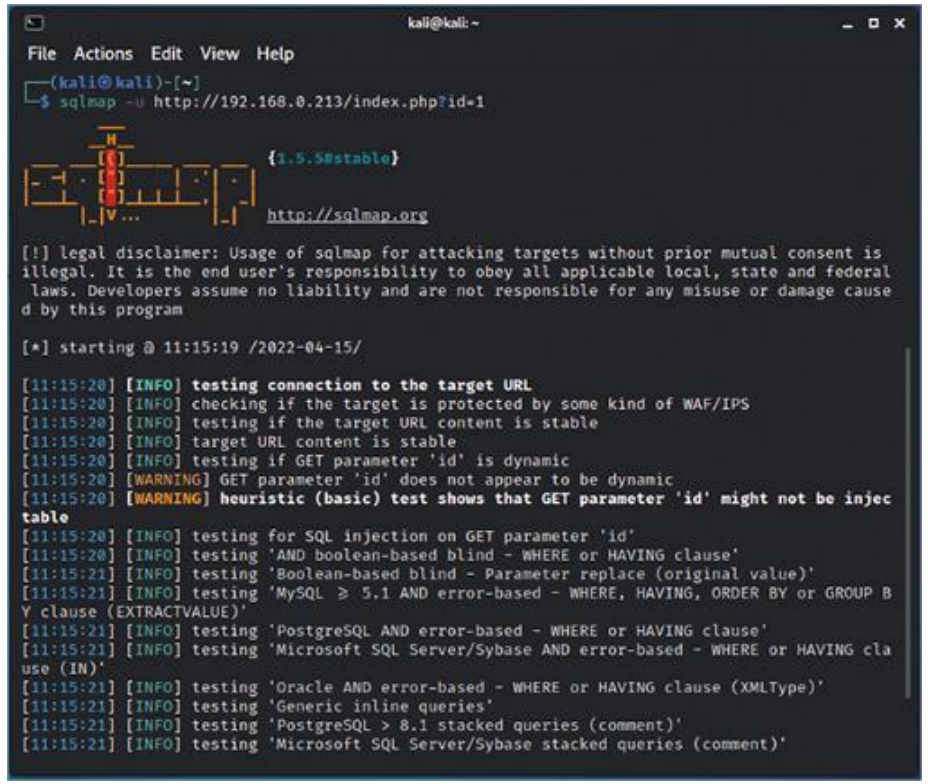
WPScan example

Understanding Vulnerability Scanning (24 of 26)

Web Application Vulnerability Scanning

SQLmap

- Structured Query Language (SQL) used by web apps to communicate with back-end databases
- Database breach may result in sensitive information disclosure
- SQL injection very common flaw
- Scans for SQL injection flaws and other SQL problems



SQLmap example

Understanding Vulnerability Scanning (25 of 26)

Vulnerability Scan Considerations

Important factors to consider before conducting a scan:

- Timing – when the target is to be tested
  - Off hours, during production or workday, over weekends
- Protocols – port numbers discovered may indicate protocol chosen
- Network topology – can influence possible scans or tools to use or avoid
- Bandwidth – scans may affect low bandwidth links or networks

Understanding Vulnerability Scanning (26 of 26)

Vulnerability Scan Considerations

Important factors to consider before conducting a scan:

- Query throttling – reduce rate of scan tool interactions with targets
- Fragile systems – scanning certain hosts can disrupt or crash them
  - Systems operating near capacity or older hardware and OSs
- Nontraditional systems – IoT devices and other similar systems may be discovered during active recon
  - not all may be known by client; notify client and seek approval to test
  - Smart TVs
  - Medical devices
  - Employee-owned smartphones

Knowledge Check Activity 5-1

Which of the following penetration testing tools or projects provides a list of top ten web application vulnerabilities?

a. Tenable Nessus

b. Nmap

c. OpenVAS

d. OWASP

Knowledge Check Activity 5-1: Answer

Which of the following penetration testing tools or projects provides a list of top ten web application vulnerabilities?

Answer: OWASP

The Open Web Application Security Project publishes the “Ten Most Critical Web Application Security Risks” paper. The OWASP nonprofit foundation and associated community consists of security professionals finding and fighting the causes of web application vulnerabilities.

Executing Vulnerability Scans (1 of 7)

Important factors to consider before conducting scans:

- Scope of the scans
- Configuration steps
- Credentialed or noncredentialed scans
- Internal and external scans
- Scanner and plug-in updates

Executing Vulnerability Scans (2 of 7)

Scope of Vulnerability Scans

- SOW and ROE key to determine scope of vulnerability scans and tests
- Types and specific tools can be allowed or restricted
- White box test may limit scans to specific host provided by client
- Scoping can help break large networks into more manageable segments
- Dividing scans by types of targets for vulnerability scans can also be a good approach

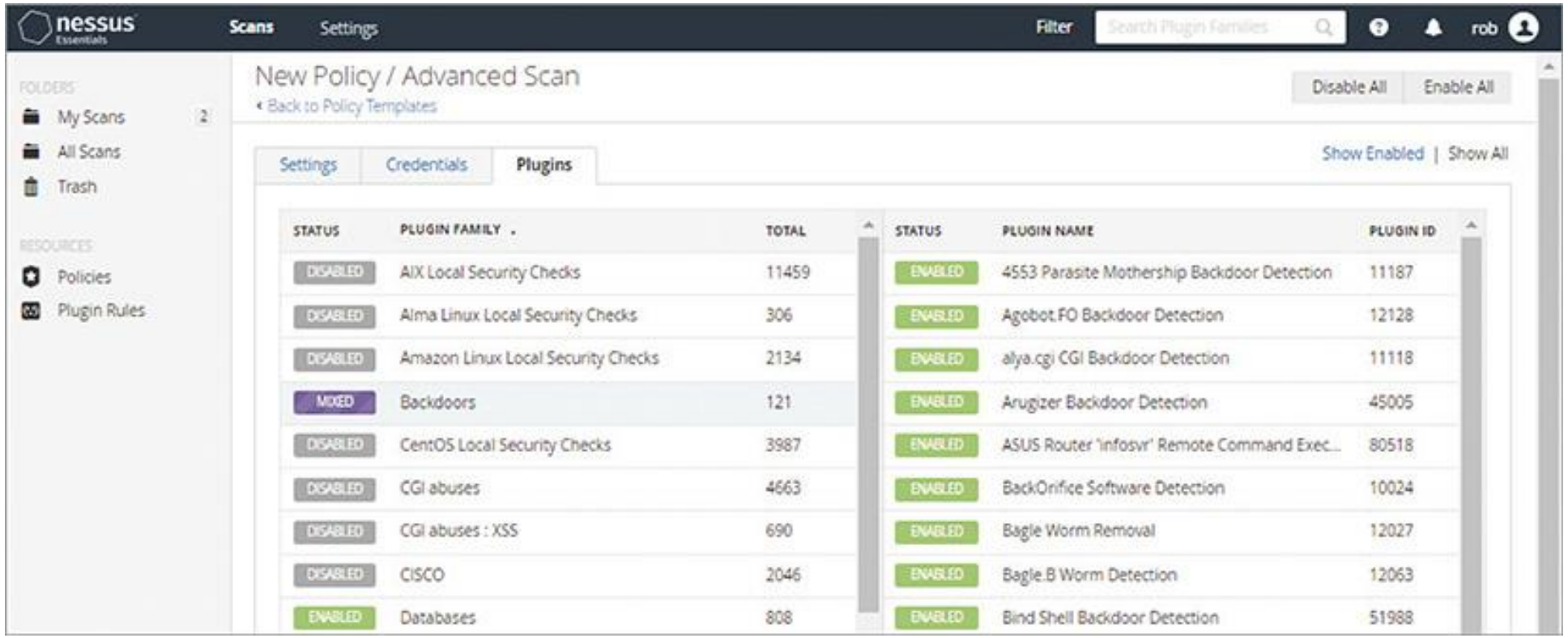
Executing Vulnerability Scans (3 of 7)

Configuring Vulnerability Scans

- Nessus and OpenVAS vulnerabilities offer similar configuration options
  - Nessus has many more plug-ins and scanning capabilities
  - OpenVAS is free, open source, and community-supported
- Type of scan – may start with one of available scan templates
- Plug-ins to use – plug-ins are individual vulnerability test components
  - Contain intelligence to discover specific vulnerabilities

Executing Vulnerability Scans (4 of 7)

Configuring Vulnerability Scans

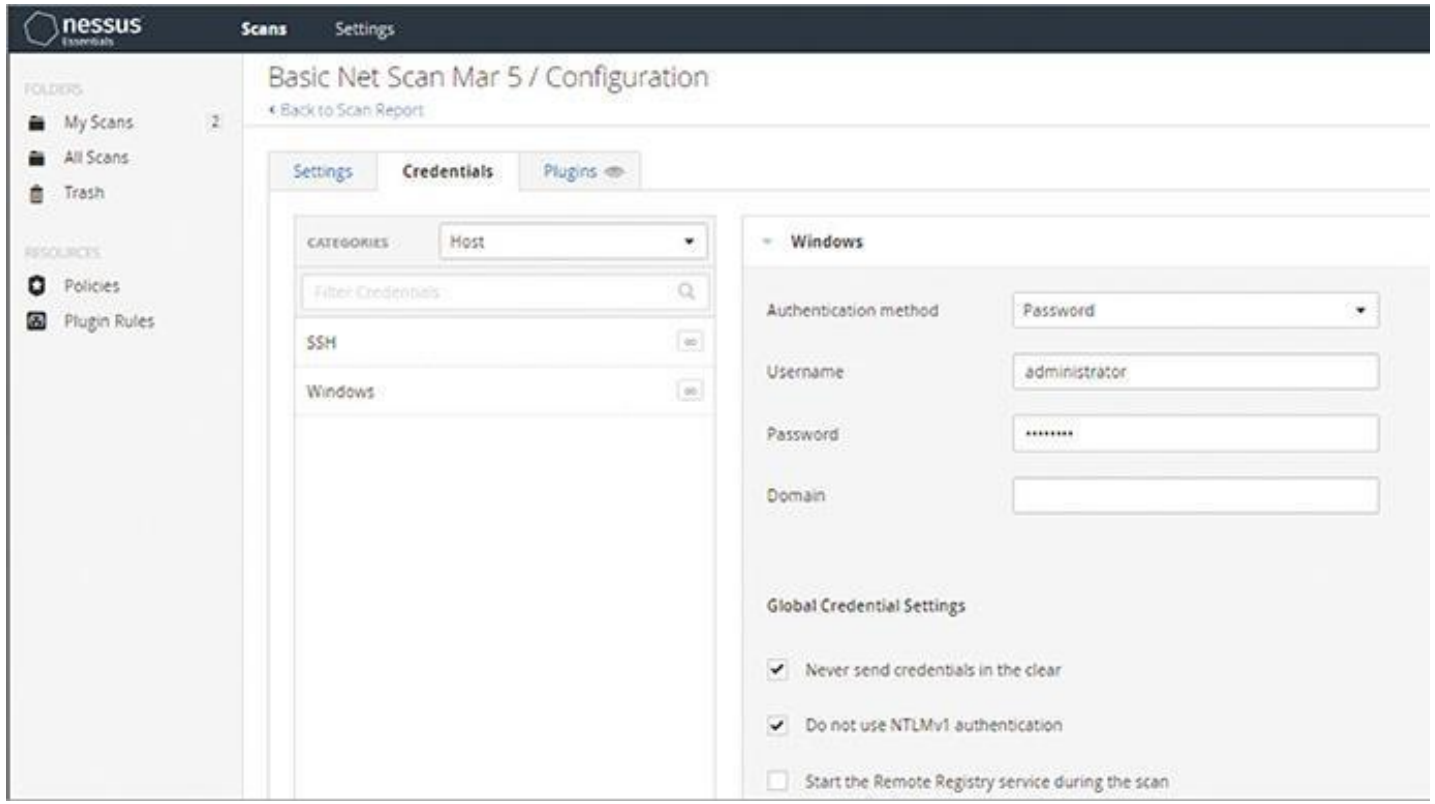


Enabling and disabling plugins in Nessus

Executing Vulnerability Scans (5 of 7)

Credentialed or Noncredentialed Scans

- Credentialed scan uses valid account and password on target
- Noncredentialed scan more realistic to threat actor
  - No account info is available to use



Specifying credentials for scan in Nessus

Executing Vulnerability Scans (6 of 7)

Internal and External Scans

- Results of scans will vary widely depending on whether scan source is internal or external to the target host's network
  - Internal scan may emulate insider threat
  - External scan more closely resembles black hat, outside threat actor

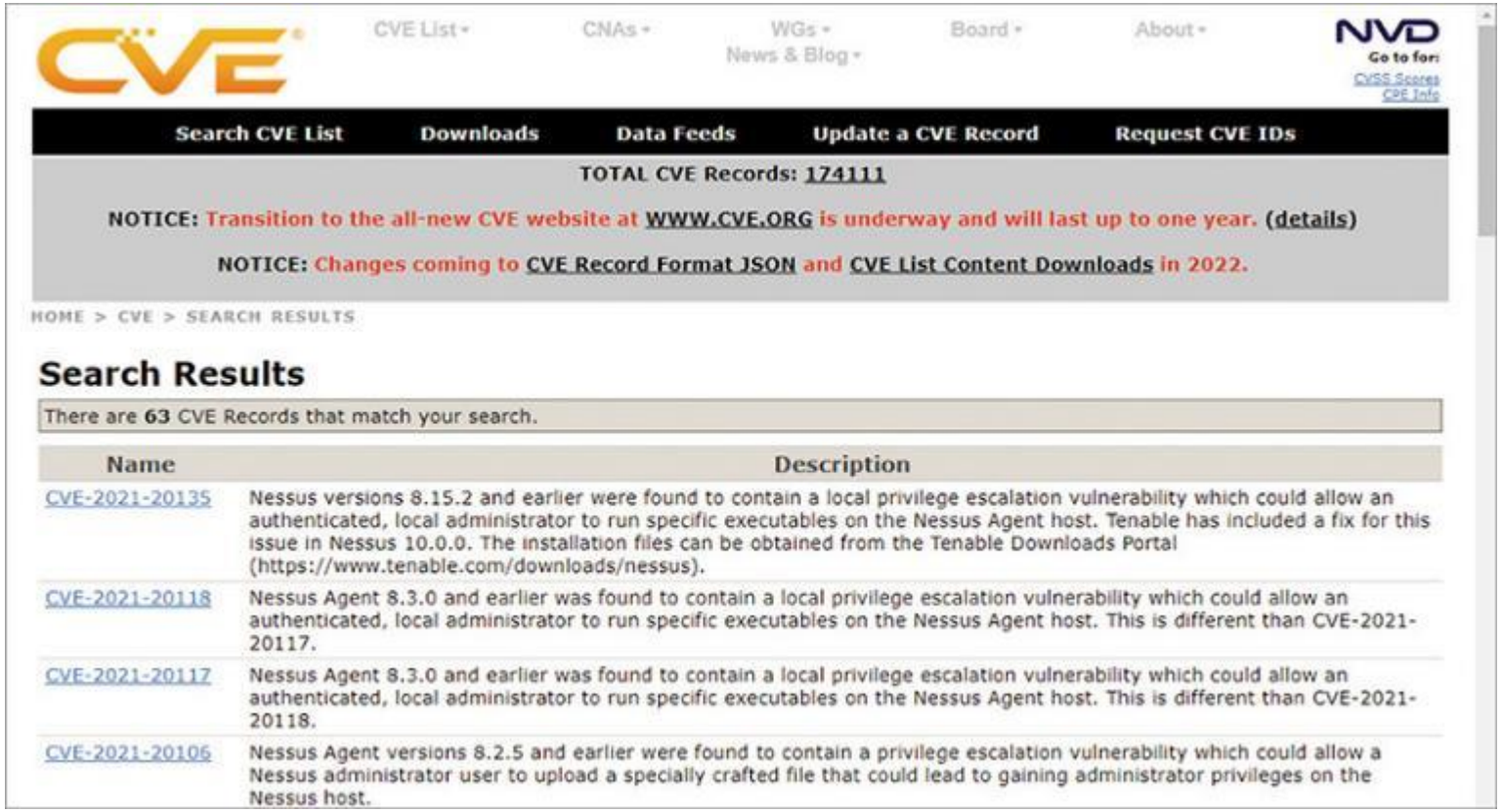
Scanner and Plug-in Updates

- Vulnerability scanners are types of software that require update
  - Tools can be flawed and vulnerable to exploits too
  - Compromised scan server can be treasure trove for pen test or threat actor

Executing Vulnerability Scans (7 of 7)

Scanner and Plug-in Updates

- CVE records exist for vulnerability scanners too
- Important to ensure tools are updated regularly
- Ensure systems that run scans and store results are secure



Nessus CVE

Discussion Activity 5-2

Two vulnerability scanners stand out as all-in-one tools for scanning networks and target hosts of varying platforms and system types.

Examine the features of Tenable Nessus and the open-source OpenVAS vulnerability scanners. Discuss differences in feature sets and scanning capabilities and capacities. How does the licensing available to the pen tester affect their pen testing capabilities?

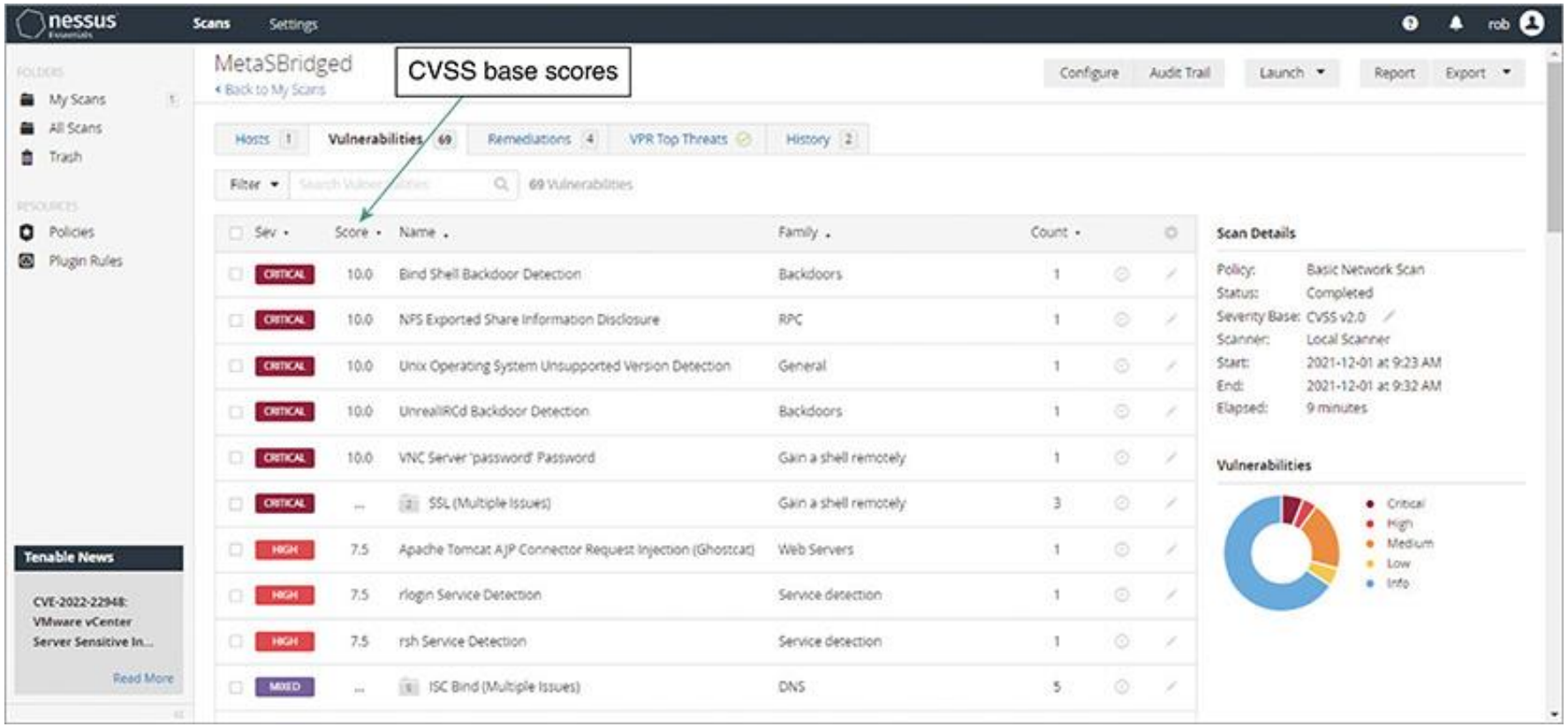
Analyzing Vulnerability Scan Results (1 of 9)

Vulnerability scanners can return a variety of information in scan results:

- Names and types of vulnerabilities detected
- Scores associated with severity or criticality of vulnerability
- Detailed vulnerability technical information
- Remediation steps may be included with some scan tools
- Exploit details and links to working exploits for further action
- References to other sources of information or resources

Analyzing Vulnerability Scan Results (2 of 9)

- Vulnerability scanners present flaws discovered in reports
- Rankings common based on severity of vulnerabilities identified

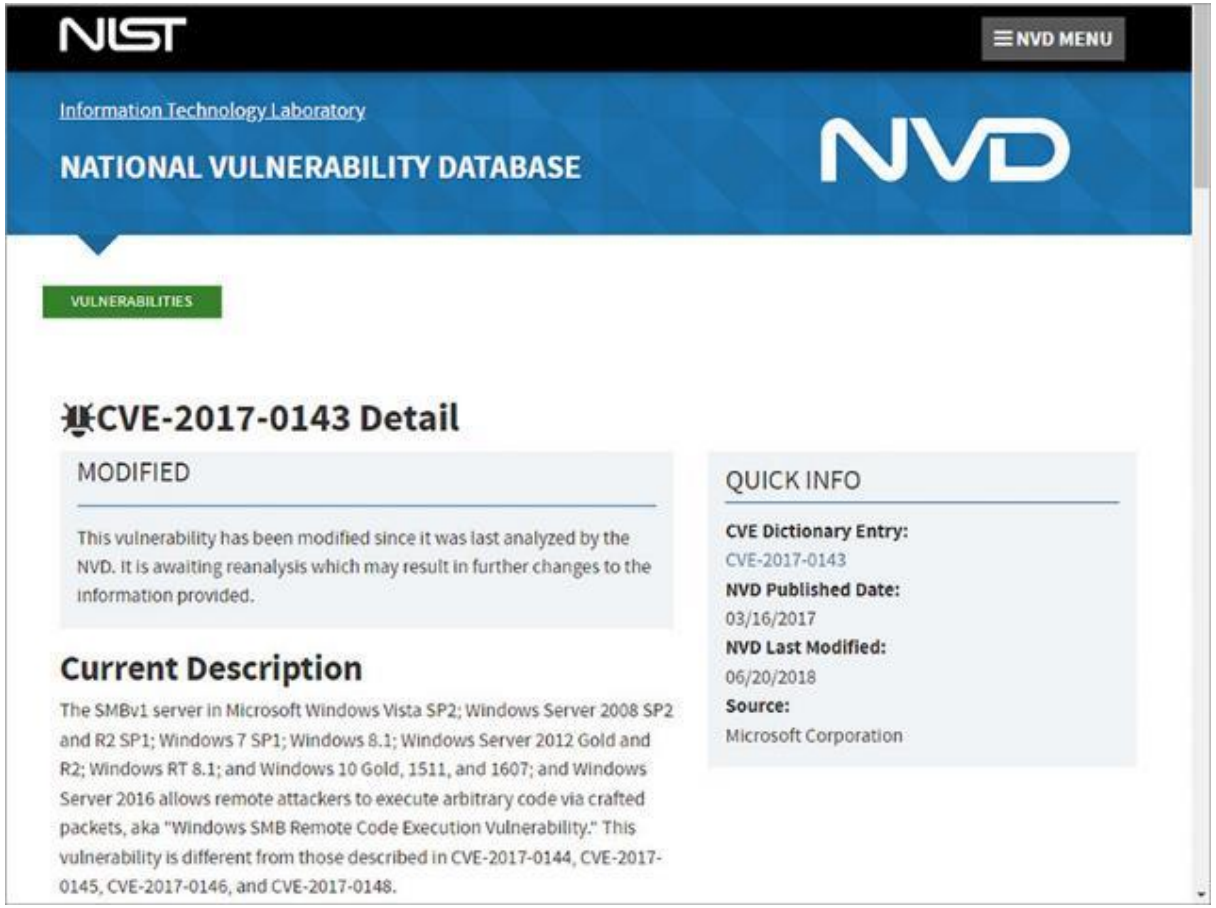


Vulnerability CVSS base scores

Analyzing Vulnerability Scan Results (3 of 9)

CVSS Base Scores

- Common Vulnerability Scoring System (CVSS) from NIST
- NIST supported metric
- Method used to supply a qualitative measure of vulnerability severity
- Measured on 0 – 10 scale and severity label: Low, Medium, High, and Critical

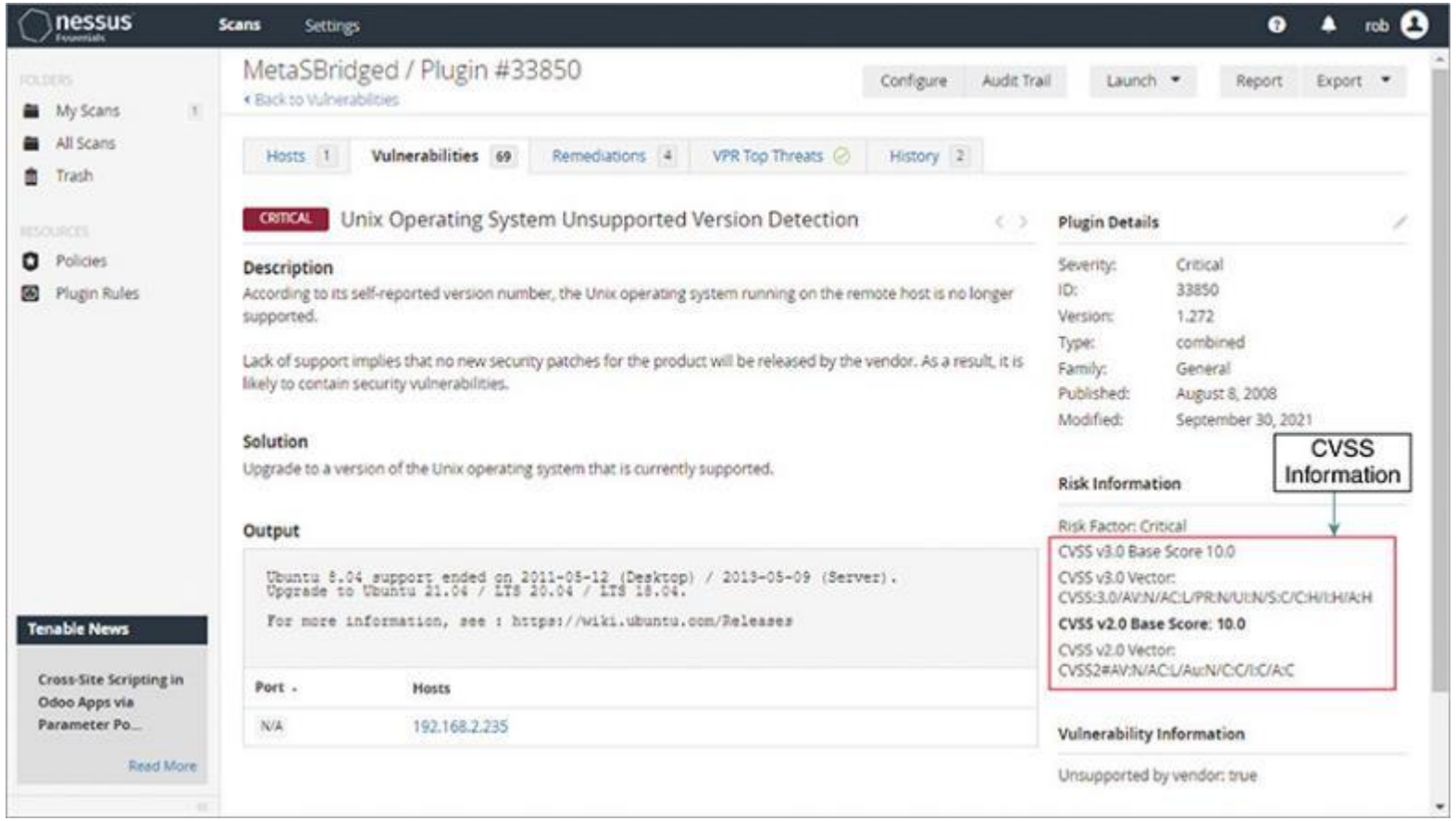


National Vulnerability Database

Analyzing Vulnerability Scan Results (4 of 9)

Exploit Information

- Vulnerability scanners may provide details on specific vulnerabilities found and links to resources to remediate or exploit

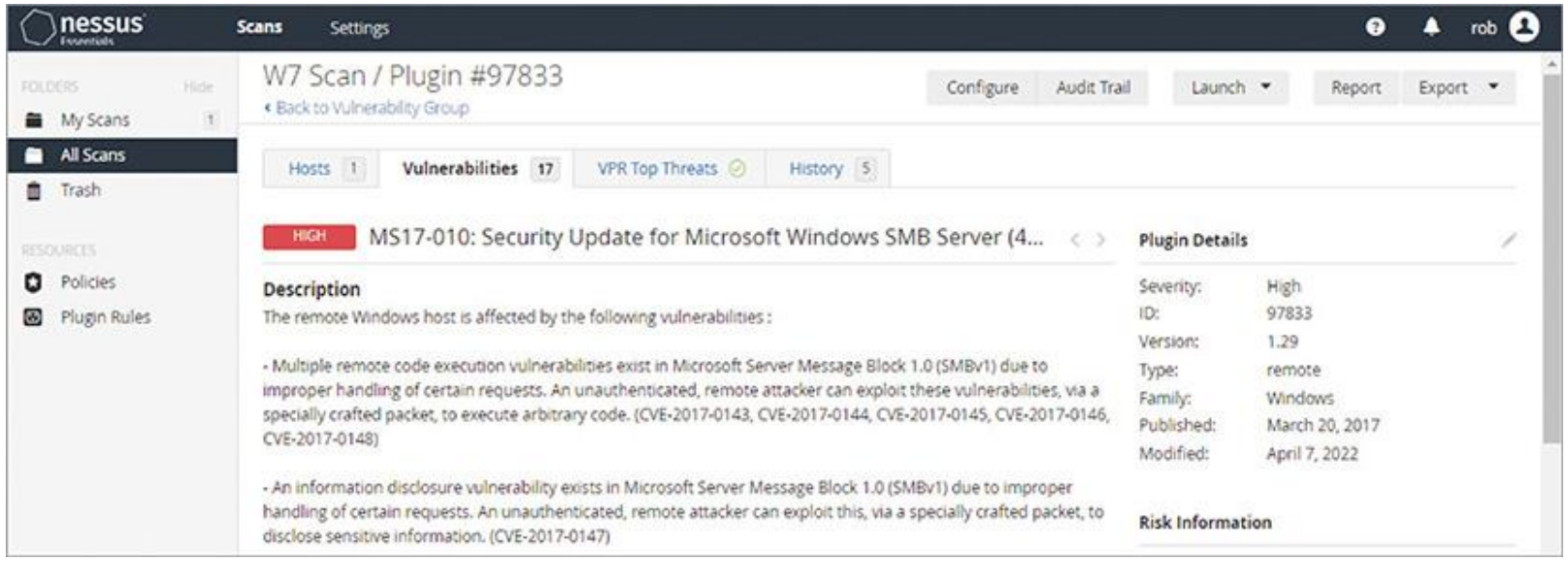


Vulnerability details

Analyzing Vulnerability Scan Results (5 of 9)

Exploit Information

- If a vulnerability exists, there is a good chance an exploit is available
- The Metasploit Framework is a common source of working exploits



SMB vulnerability information

Analyzing Vulnerability Scan Results (6 of 9)

CVSS Vector Information

- CVSS vector information provides details on how base score is calculated
- Vector metrics have a much more finely detailed vulnerability information
- CVSS Version 2.0 and 3.0 in use; slightly different expression of data
- Seven attack vectors currently in use:
  - Attack Vector (AV)
  - Attack Complexity (AC)
  - Privileges Required (PR)
  - User Interaction (UI)
  - Confidentiality (C)
  - Integrity (I)
  - Availability (A)

Analyzing Vulnerability Scan Results (7 of 9)

CVSS Vector Information

- Each vector has metric assigned, and metrics together calculate CVSS
- Attack Vector (AV) – how attacker must be positioned
  - Physical (P), Local (L), Adjacent Network (A), Network (N)
- Attack Complexity (AC) – conditions needed to exploit; attacker skill level
  - High (H), Medium (M), Low (L)
- Privileges Required (PR) – authentication level needed to exploit
  - High (L), Low (L), None (N)

Analyzing Vulnerability Scan Results (8 of 9)

CVSS Vector Information

- User Interaction (UI)– whether user other than attacker must interact
  - None (N), Required (R)
- Confidentiality (C) – what level attacker can access confidential data
  - None (N), Low (L), High (H)
- Integrity (I) – what level attacker can corrupt data
  - None (N), Low (L), High (H)
- Availability (A) - what level attacker can compromise availability
  - None (N), Low (L)

Analyzing Vulnerability Scan Results (9 of 9)

Ranking Vulnerabilities

After building a list of vulnerabilities, rank them in order of remediation, or which order to “exploit” first

Consider the following factors:

- Severity level/CVSS base score
- Network exposure level
- System importance/criticality
- Statement of work
- False positives
- CIA triad violations

Discussion Activity 5-3

Use the CVE database at Mitre.org to search for recent vulnerabilities for a specific software or application. Choose two or three vulnerabilities to examine in depth.

Look at the resources associated with the vulnerability from sites external to Mitre.org. Pay attention to any CVSS-related information and availability of exploits for the vulnerability.

Discuss the findings with other learners in this course.

Summary

By the end of this module, you should be able to:

1. Describe vulnerability scanning and its purposes
2. Describe methods and tools to discover targets for vulnerability scanning
3. Describe different types of vulnerabilities and vulnerability scans
4. Describe additional considerations when performing vulnerability scans
5. Execute vulnerability scans using different tools
6. Analyze the results of vulnerability scans