Chapter 6: Reconnaissance

In this chapter, you'll learn:

- About reconnaissance goals and passive reconnaissance tools
- How to perform active reconnaissance to attack or protect a network
- How to analyze vulnerability scan output

Module A: Reconnaissance techniques

In this module, you'll learn:

- About reconnaissance goals and types
- How to gather open-source intelligence
- How to harvest DNS and WHOIS data

Reconnaissance goals

- Footprinting or cybersecurity reconnaissance encompasses just about any technique you can use to gather information about any target from an individual host up to an entire organization.
  - Network structure and addresses
  - Hosts and network devices
  - Active network services
  - Network security systems, such as IDS and IPS
  - Business details, such as locations, contact information, and organizational structure
  - Names and other details about individual employees

Footprinting techniques

- Passive reconnaissance is anything that doesn't require direct contact with the target
- Active reconnaissance requires direct or intrusive contact that could raise suspicion if it's noticed, so you need to proceed more carefully and plan for defensive countermeasures
- Semi-passive reconnaissance is a "softer" form of active reconnaissance that is designed to avoid drawing attention

Continued...

Footprinting techniques

- Gathering open-source intelligence from public sources
- Using social engineering to gather information
- Performing topology discovery of a network to identify its attack surface
- Performing service discovery to identify open ports and network services on a given host
- Identifying specific operating systems and versions used by hosts by using more detailed network scans
- Gathering network conversations between two hosts using passive packet sniffers
- Reviewing logs, ACLs, and system or device configuration details
- Access to software binaries or source code to find vulnerabilities or useful metadata

Environmental reconnaissance variables

- Network scans are more effective from inside the network and most effective in the same segment
- Wireless networks can be scanned and sniffed from anywhere within range, especially with a directional antenna
- Virtual hosts and networks can have logical topologies quite different from their physical topologies, and both are relevant for an attacker to learn
- Cloud services can be challenging to scan without the proper tools, and your service agreement with a CSP might limit the scans you can perform on your own cloud-based services

OSINT sources

- Open-source intelligence (OSINT) is a term that's long been used by intelligence agencies to refer to any information about a target that isn't secret and is available to anyone who just knows where to look.
- Public information
- Official (government) information
- Third-party sources

OSINT gathering methods

- Email harvesting
- Web footprinting
- DNS harvesting
- WHOIS harvesting

Exercise: Probing a site

Assessment: Reconnaissance techniques

As a penetration tester, you want to get a username and password for a critical server, but lockout and monitoring systems mean you'll be detected if you try brute force guessing. What techniques might directly find the credentials you need? Select all that apply.

A. DNS harvesting
B. Packet capture
C. Phishing
D. Service discovery
E. Social engineering

B, C, and E

Assessment: Reconnaissance techniques

For an outside attacker, what reconnaissance method is much easier on wireless networks than wired ones? Choose the best response.

A. DNS harvesting
B. Log review
C. Packet capture
D. Service discovery

C

Assessment: Reconnaissance techniques

For business reasons, your company isn't at all secretive about its WHOIS information. What reconnaissance type might attackers find easier as a result? Choose the best response.

A. OS fingerprinting
B. Packet capture
C. Social engineering
D. Topology discovery

C

Assessment: Reconnaissance techniques

You're targeting a DNS server during a penetration test, as part of network mapping. What kind of attack could you attempt to get all the server's data with a single request? Choose the best response.

A. Digging
B. Google hacking
C. Topology discovery
D. Zone transfer

D

Module B: Active reconnaissance

In this module, you'll learn:

- How to perform network scans
- About vulnerability analyzers
- How to perform packet captures

Planning a scan

1. Recognize that your scan will likely be noticed and that there can be severe professional or legal consequences for unauthorized network probes.
   - Ensure you have written permission for the type and scope of the plan and verify that the scan is unlikely to disrupt production networks.
   - If you're a red team member in a penetration test, determine stealth techniques that make your scan, or at least its point of origin, harder to discover.
2. Perform an initial network scan to find responsive hosts and network infrastructure devices.
3. Perform network service enumeration by scanning for open ports or monitoring network traffic.
4. Scan active services in-depth to determine more about them. Banner grabbing and OS fingerprinting are useful at this stage.
5. Analyze vulnerabilities based on the results of the scan.
6. Update your network map based on your findings.

Scanning tools

- Vulnerability scanner
  - Methodically searches for documented vulnerabilities in a host or service.
- Compliance scanner
  - Analyzes host or service configurations and compares them to a policy or regulatory baseline.
- Exploit framework
  - Bundles exploits and other attack tools for use by a penetration tester.
- Cracker
  - Attempts to break encryption keys, crack hashed passwords, or gain access to an account without a password. Sometimes euphemistically called password auditing or password recovery tools, when used defensively.

Nmap

- Host discovery across specified IP ranges or subnets
- Port scanning using TCP or UDP
- Fingerprinting of host operating systems and service versions
- Multiple scan types that can discover additional information or avoid firewall/IDS rules that block default scans
- Traceroute scans that help to map out network ranges
- Extensibility via scripts to perform more specialized communications with or attacks on targets

Nmap scan types

- The basic syntax of Nmap is simple:
  nmap scantype options target
- To scan a subnet, use CIDR notation, such as 10.10.10.0 /24
- To scan an IP range, use -, such as 10.10.10.1-100
- To scan a list of IPs from a text file, use -iL filename
- To scan a range of ports, use -p <ports>
- To quickly scan the 100 most common ports, use -F
- To scan all 65535 ports, use -p-

Zenmap scan presets

- Quick scan
- Ping scan
- Intense scan
- Intense scan, no ping
- Intense scan plus UDP
- Slow comprehensive scan
- Quick traceroute

Hping

- Examining firewall rulesets
- Advanced port scanning and OS fingerprinting
- Detailed network mapping (traceroute, MTU)
- Spoofing or relaying packets
- Arbitrary file transfer through strict firewalls
- Studying the inner workings of TCP/IP for educational purposes

Exercise: Scanning the network

Vulnerability analyzers

- Vulnerability analyzers can only detect vulnerabilities against known threats, or at least known types of threats.
- Finding specific vulnerabilities
- Verifying regulatory compliance
- Auditing against a user-defined security baseline
- Performing automatic vulnerability remediation
- Output to reporting, logging, and security systems
- Integration into a CI/CD or vulnerability management workflow

Assessment tools

- Infrastructure vulnerability scanners
  - Nessus
  - OpenVAS
  - Nexpose
  - Qualys
- Web application scanners
  - Nikto
  - BrowserCheck
  - OWASP Zed Attack Proxy (ZAP)
  - Arancini
  - Burp Suite
  - SQL Map

Continued...

Assessment tools

- Cloud infrastructure assessment tools
  - ScoutSuite
  - Prowler
  - Pacu

Packet analyzers

- Examining network problems at the packet level
- Finding active services by their traffic
- Viewing overall traffic flow patterns
- Isolating traffic based on source, destination, protocol, or contents
- Gathering or auditing the security of sensitive information, such as authentication processes and encryption
- Verifying the status of network security controls such as firewalls, filters, and proxies
- Logging network traffic for later use

Wireless packet capture

- The most basic requirement is that the application must support the Layer 2 protocols used by your network interface
- Wi-Fi has an entirely different (and more complex) set of management and control protocols it uses for authentication, collision avoidance, and other features needed for normal network function in a wireless environment
- Most wireless networks not intentionally open to the public use encryption to prevent eavesdropping and unauthorized access

Packet capture applications

- tcpdump
  - A free and open-source packet analyzer that runs at the command line. It's simple and writes the packets it captures to standard output or a file. tcpdump is available for most Unix-like operating systems, including macOS and Android. The Windows port is slightly different and is called WinDump.
- Wireshark
  - Another free and open-source packet analyzer for a variety of operating systems, formerly known as Ethereal. Unlike tcpdump, it runs in a GUI that allows you to sort, filter, and otherwise present captured data more easily without a separate analysis tool.
- Sniffer
  - One of the original packet sniffer programs designed by Network General. It's now been acquired by NetScout, who uses it in enterprise products such as their InfiniStream network appliances.

Wireless assessment tools

- Aircrack-ng
  - A software suite designed to analyze and attack Wi-Fi networks.
- Kismet
  - A passive wireless sniffer which can also function as a network detector and IDS.
- Reaver
  - A brute force cracking tool designed to attack Wi-Fi networks with WPS enabled.
- oclHashcat
  - A high-speed password recovery tool, available for many platforms.

Using Wireshark

- When you open Wireshark, it shows a list of available network interfaces along with an activity graph for each.
- Captured packets are displayed in the top pane and are color-coded according to their nature.
- Select a packet in the list to view its details.
- Since network traffic involves massive numbers of packets, use filtering tools to find what you're looking for.

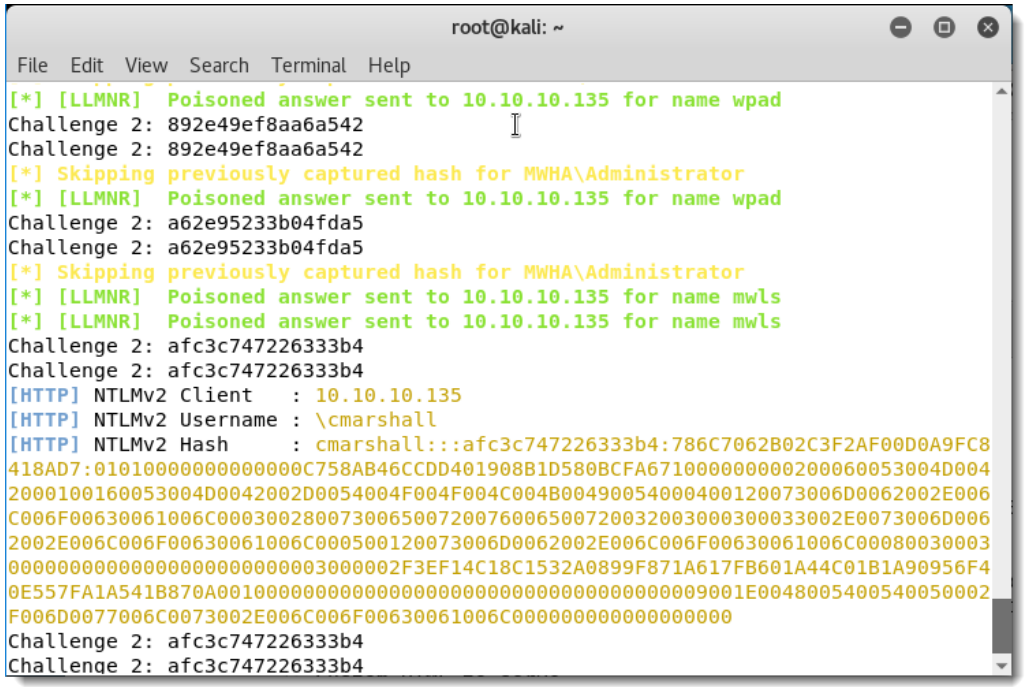
Continued...

Using Wireshark

- To view an entire conversation, such as a TCP session, right-click any packet in it and choose Follow > TCP stream. You can also similarly follow UDP or SSL streams.
- To perform further analysis on overall traffic statistics, use the Statistics menu, or the Telephony and Wireless menus for those sorts of traffic.
- You can save and load traffic captures.

Using Responder

- Responder is a command-line script, and you can control its precise operation through command-line options and by editing the /etc/responder/responder.conf file. The -help option will show syntax, but the following options are helpful.



Exercise: Packet capture

Assessment: Active reconnaissance

You're mapping a network and looking for rogue devices and services. Which tool are you most likely to use? Choose the best response.

A. MBSA
B. Nessus
C. Nikto
D. Nmap

D

Assessment: Active reconnaissance

You're scanning the local subnet with Zenmap. When you're about to try an Intense scan, a coworker suggests you run Intense scan, no ping instead. If you take that advice, what will the likely result be? Choose the best response.

A. It will complete faster but probably find fewer hosts and services.
B. It will complete faster and probably find more hosts and services.
C. It will take longer but probably find more hosts and services.
D. It will take longer and probably find fewer hosts and services.

C

Assessment: Active reconnaissance

You want to perform a vulnerability scan on a web application with a SQL backend. Which tool would be most appropriate? Choose the best response.

A. Arachni
B. Nexpose
C. Prowler
D. ScoutSuite

A

Assessment: Active reconnaissance

You think attackers are using packet sniffers on your Wi-Fi network. The network is using secure WPA2 encryption, but what can the attackers still learn without the key? Select all that apply.

A. Active applications
B. IP addresses
C. MAC addresses
D. Most active hosts
E. SSIDs

C, D, and E

Assessment: Active reconnaissance

Your organization is expanding its use of AWS cloud infrastructure. After your team scans and hardens it, a red team will perform a penetration test while you defend it. Which of the following tools would be more useful to a red team member than to your blue team? Choose the best response.

A. Nessus
B. Nikto
C. Pacu
D. Prowler

C

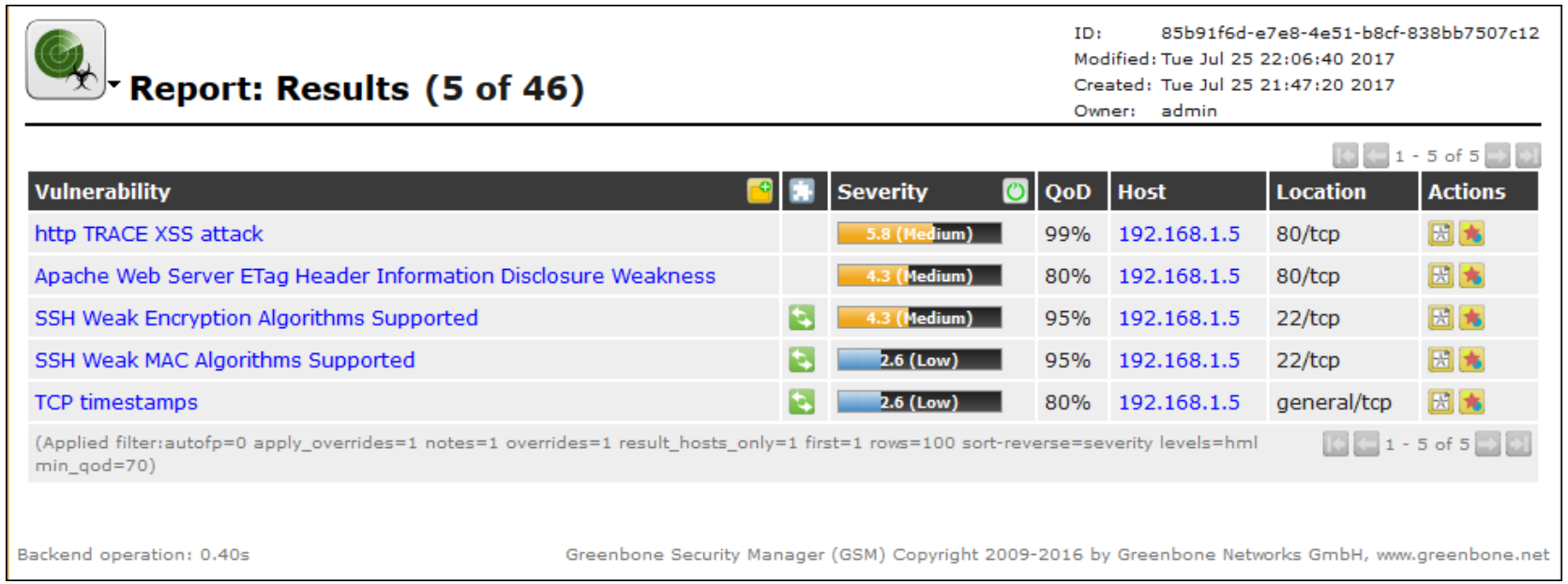
Module C: Analyzing scan results

In this module, you'll learn:

- How to interpret scan results
- About the Common Vulnerability Scoring System
- How to identify false positives and exceptions
- How to reconcile multiple data sources

About scan interpretation

- Filtered results from an OpenVAS vulnerability scan



Report: Results (5 of 46)

ID: 85b91f6d-e7e8-4e51-b8cf-838bb7507c12
Modified: Tue Jul 25 22:06:40 2017
Created: Tue Jul 25 21:47:20 2017
Owner: admin

1 - 5 of 5

Vulnerability	Severity	QoD	Host	Location	Actions
http TRACE XSS attack	5.8 (Medium)	99%	192.168.1.5	80/tcp	
Apache Web Server ETag Header Information Disclosure Weakness	4.3 (Medium)	80%	192.168.1.5	80/tcp	
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.1.5	22/tcp	
SSH Weak MAC Algorithms Supported	2.6 (Low)	95%	192.168.1.5	22/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.1.5	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

1 - 5 of 5

Backend operation: 0.40s

Greenbone Security Manager (GSM) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

The Common Vulnerability Scoring System

- An industry standard for communicating the severity of vulnerabilities
- CVSS score types
  - Base - The intrinsic qualities of the vulnerability: how hard it is to exploit and how severe its impact is.
  - Temporal - How the vulnerability might change over time: whether it is an established and practical attack, and whether there are effective countermeasures.
  - Environmental - How your individual environment affects the base risk: does your configuration change how hard it is to exploit the vulnerability or its potential impact?

CVSS metrics

- CVSS 3.0 uses the following metrics to calculate a Base score.
  - AV: Attack Vector indicates how an attacker can access the vulnerability.
  - AC: Attack Complexity refers to how repeatable the attack is.
  - PR: Privileges Required indicates the system access needed to exploit the vulnerability.
  - UI: User interaction refers to whether human interaction is required for the vulnerability to be exploited, such as by a user running a malicious program.
  - S: Scope refers to whether the impact of the vulnerability goes beyond the vulnerable component.

Continued...

CVSS metrics

- Temporal scores are simpler since there are only three metrics.
  - E: Exploit Code Maturity is the current state of attacks against the vulnerability.
  - RL: Remediation level is whether there is a way to correct the vulnerability.
  - RC: Report Confidence is whether the vulnerability's base metric can be considered accurate.
- Environmental metrics are almost identical to Base metrics since they reflect how your organization or implementation is likely to be affected if that differs from the base metrics.

Validating scan results

1. Identify false positives.
2. Identify existing security exceptions.
3. Analyze other data sources, such as related logs or other scan results.
4. Reconcile differences between conflicting reports.
5. Compare results to regulatory compliance or general best practices.
6. Review trends in the threat landscape and determine how they may change your priorities.

False positives

- Telling the difference between a genuine vulnerability and a false positive isn't always easy
- Sometimes it's just a matter of verifying that you've applied the correct patches and settings to remedy the potential issue, but other times you might need to perform detailed investigations, compare the results of multiple scanners or directly attempt exploits to verify whether the problem exists

Managing exceptions

- Security exceptions aren't something to be taken lightly, even in cases where they only introduce a negligible amount of risk.
- Exceptions must receive written approval by management before being enacted, in accordance with your organization's exception policy.
- If you're creating an exception because remediation is too difficult, explore compensating controls you can use to reduce risk.
- Compliance requirements might restrict what exceptions you can allow or specify compensating controls you need to apply instead.
- Exceptions must be documented to prevent your work from being repeated or undone by a later scan.
- Known false positives can be added to exception lists, but be careful in case a future configuration change causes the actual vulnerability to appear.
- Exceptions and their reasons should also be documented in relevant policies and procedures, including the disaster recovery plan.

Gathering additional vulnerability data

- Best practices documents and regulatory
- Reconciling the results of multiple scanners and tools
- Reviewing your network configuration
- Logs and SIEM systems
- Penetration tests and active defenses like threat hunting and honeypots
- Record and analyze trends within your vulnerability management system

Exercise: Evaluating scan results

Assessment: Analyzing scan results

You researched an authentication system vulnerability last month, and while it had a severe impact in theory, no demonstrated code could exploit it. Last week a security researcher demonstrated exploit code. How will this affect the vulnerability's CVSS score? Choose the best response.

A. It will change the Base metrics.
B. It will change the Environmental metrics.
C. It will change the Temporal metrics.
D. It will change all three metrics.
E. It won't change any metrics.

C

Assessment: Analyzing scan results

After performing a vulnerability scan on a database server, you manually verify that each reported vulnerability exists on the server. What are you looking for? Choose the best response.

A. False positives
B. False negatives
C. Both
D. Neither

A

Assessment: Analyzing scan results

A web server with access to customer PII has a severe vulnerability, which is going to be very time-consuming and expensive to fix. Fortunately, your company compliance officer verified that you could configure a WAF as a compensating control until you replace the server. In the meantime, how can you deal with the severe vulnerability appearing every time someone runs a scan? Choose the best response.

A. Mark it as a false positive.
B. Document it as a security exception.
C. Get used to reminding people.
D. Do nothing since the WAF will hide the vulnerability on the scanner, too.

B

Summary: Reconnaissance

You should now know how to:

- About environmental reconnaissance goals and techniques, including passive methods such as open-source intelligence.
- How to actively scan your own network using network mappers, vulnerability scanners, and packet analyzers.
- How to analyze results from a vulnerability scan using standard metrics, identify security exceptions and false positives, and correlate data from multiple sources.