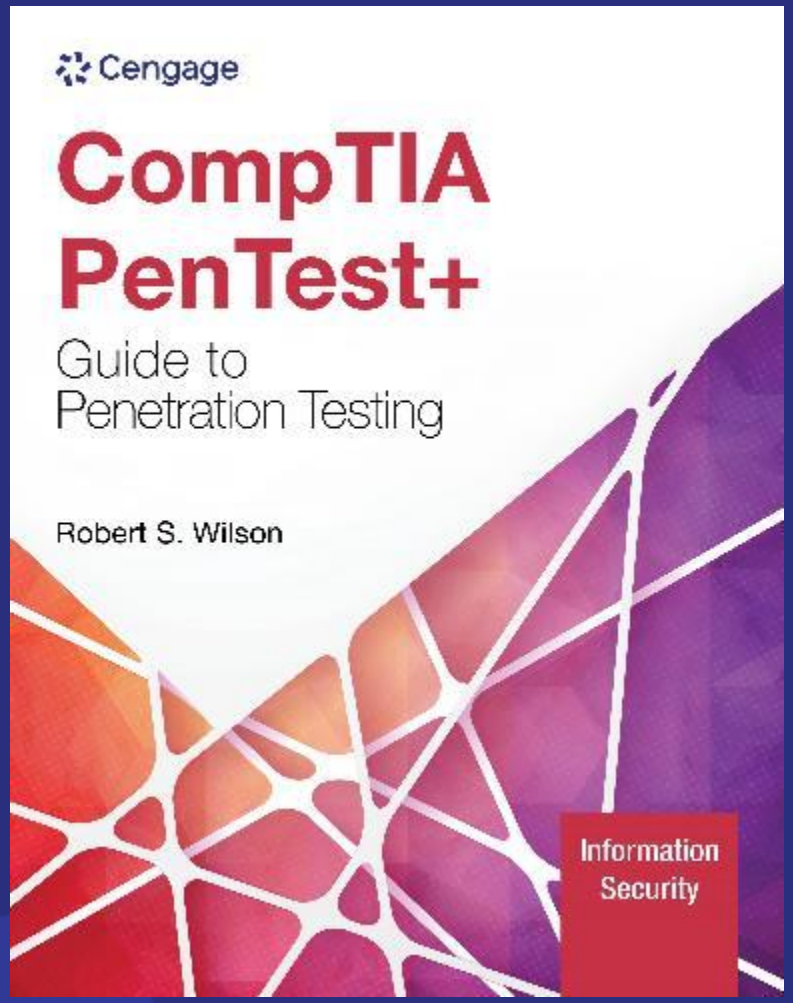


CompTIA PenTest+ Guide to Penetration Testing, 1e

Module 4: Information Gathering

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Module Objectives

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

1. Apply passive reconnaissance techniques
2. Apply active reconnaissance techniques
3. Analyze the results of reconnaissance
4. Use active and passive reconnaissance tools

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (1 of 27)

Key Terms

Passive Reconnaissance – Using reconnaissance techniques openly shared with the public with little chance of alerting the target organization

Open Source Intelligence (OSINT) – Open and freely available sources of information and processes used during passive reconnaissance

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (2 of 27)

Gathering High-Level Organizational Information

Geographic Locations and Organizational Structure

- Knowing physical location can be important during a pen test
- Some pen tests target physical security
- Sources for physical location information
  - Target organization websites
  - Social media postings about target
  - Public records, including business licenses and tax information

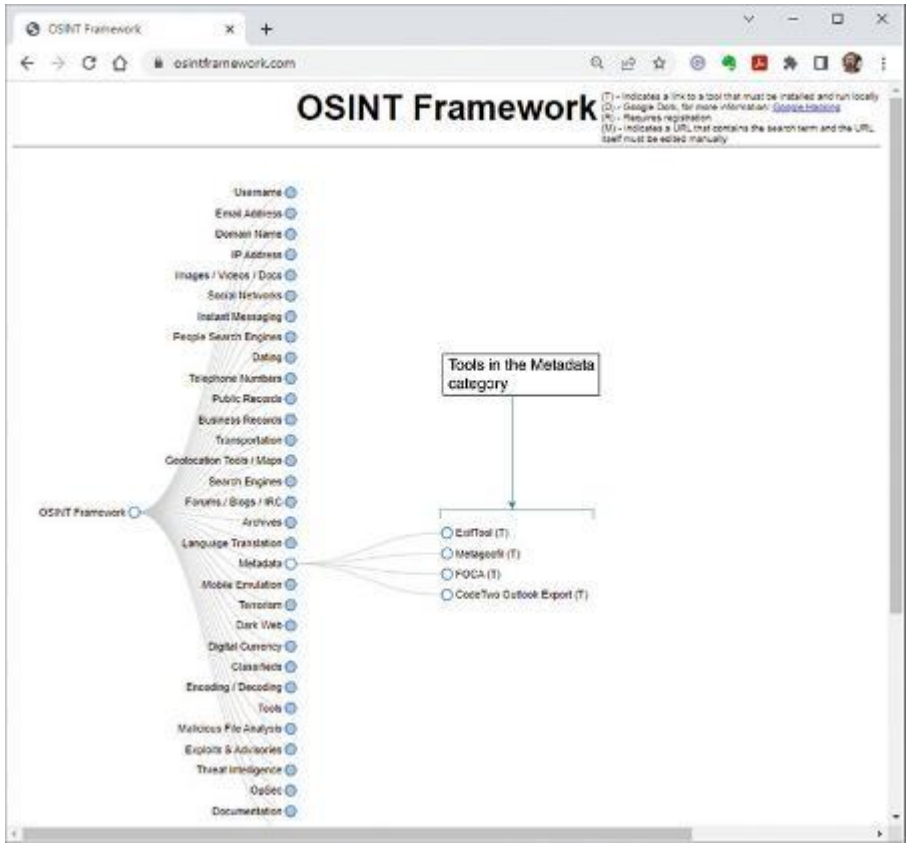
Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (3 of 27)

Gathering High-Level Organizational Information

- OSINT Framework website is built in a tree structure with nodes that link to public records
- Many other resources are useful for data gathering



OSINT Framework Website

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (4 of 27)

Gathering High-Level Organizational Information

Passive Reconnaissance at Target Physical Location

- Armed with physical location(s) of target organization, several tactics for passive recon are possible to gather information
  - Visit locations for in-person info gathering and observation
    - Keycard secured doors, security desks, man-traps, etc.
  - Dumpster diving, *or* searching through a target's trash, can result in finding documents or other resources
- Location knowledge can support planning for social engineering

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (5 of 27)

Gathering High-Level Organizational Information

Document Metadata

- Metadata is “data about data”
- Details about files, beyond the main info within a file
  - File creation date
  - Author
  - Servers related to document
  - Users
  - Email addresses
  - Operating system
  - GPS coordinates

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (6 of 27)

Gathering High-Level Organizational Information

- Photos and similarly created image files may contain Exif data
  - Exchangeable image file format
- Exif metadata can be very useful
- Exif metadata is often removed if file is uploaded to an image sharing site
- Special tools can strip metadata, or cameras and editors can save without Exif details

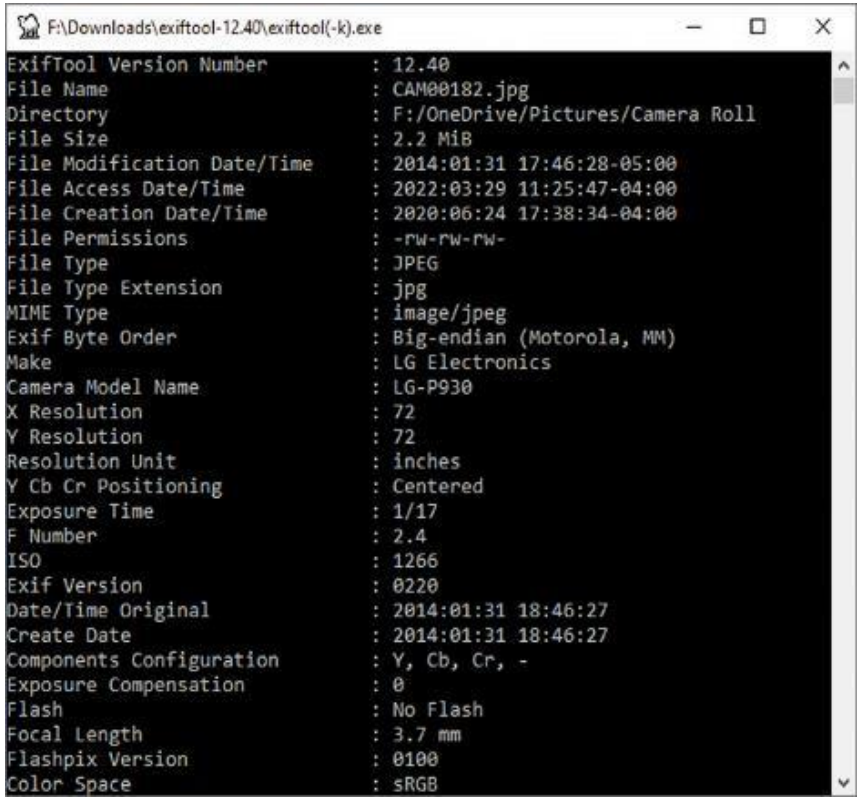


Image file metadata in ExifTool

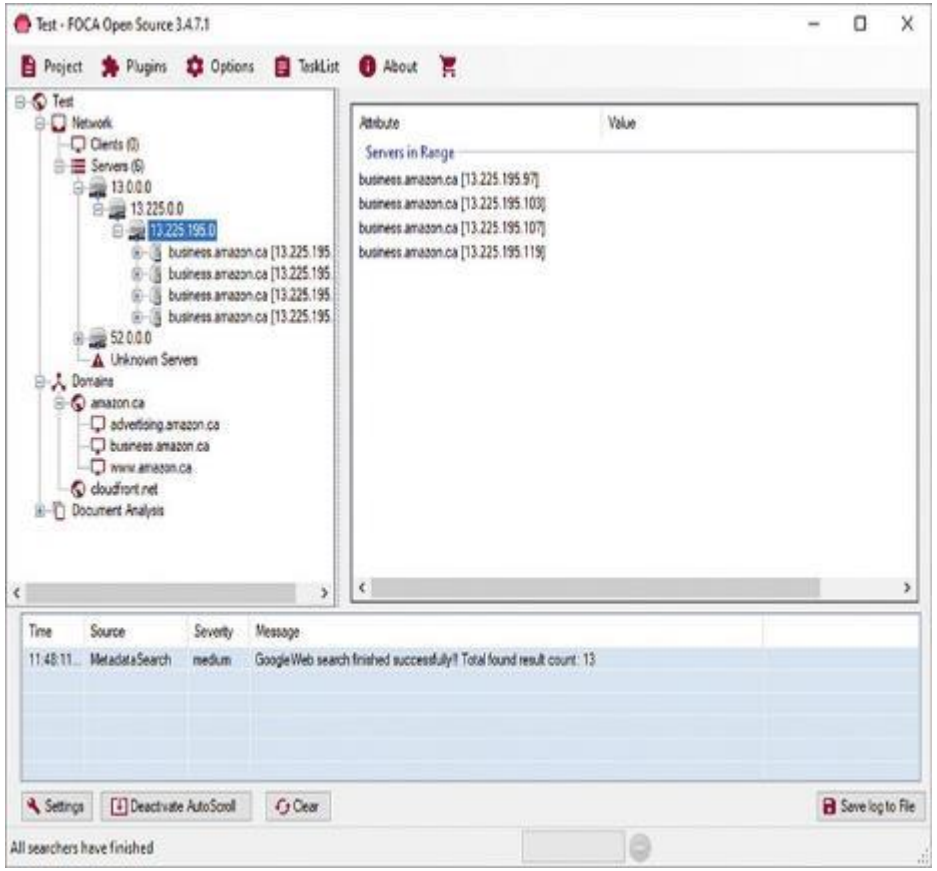
Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (7 of 27)

Gathering High-Level Organizational Information

- The possibilities for open-source intelligence gathering is only limited by the pen tester's imagination
- Way Back Machine (archive.org) stores snapshots of websites from years past
- FOCA identifies server metadata
- Many additional OSINT tools available



Server metadata in FOCA

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (8 of 27)

Gathering High-Level Organizational Information

Technical and Administrative Contacts - People are targets too!

- Technical contacts may provide info on systems and processes
- Administrative contacts can give target details and other contact access
- Social media can be a treasure trove of OSINT
  - Official posts on sites like LinkedIn, Twitter, or YouTube
  - Employee's personal posts on Facebook and Instagram
- Social media scraping is the process of analyzing posts for intelligence

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (9 of 27)

Gathering High-Level Organizational Information

Domains and Networks

- Domain registrar is an accredited organization that sells domain names
  - Details about the domain owner can be found from registrars
  - Domain registrars are assigned authority over geographic regions
- Domain info and IP data can help determine if potential target servers and IP addresses are local or cloud-based

Cengage

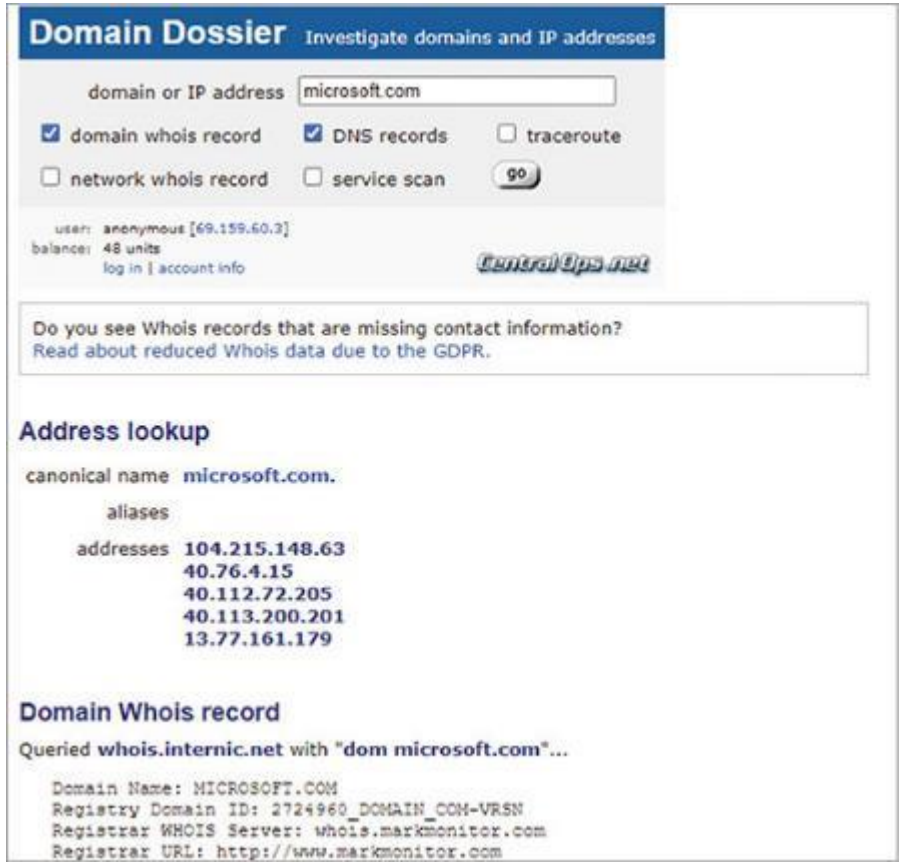
Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (10 of 27)

Gathering High-Level Organizational Information

Domains and Networks

- Domain Name System (DNS) – translates computer host and domain names to IP addresses
- Internet Assigned Numbers Authority (IANA) – central DNS authority
- Whois service – tool for gathering domain info such as ownership, IP addresses, registrar, and more



Domain Dossier tool with whois info

Cengage

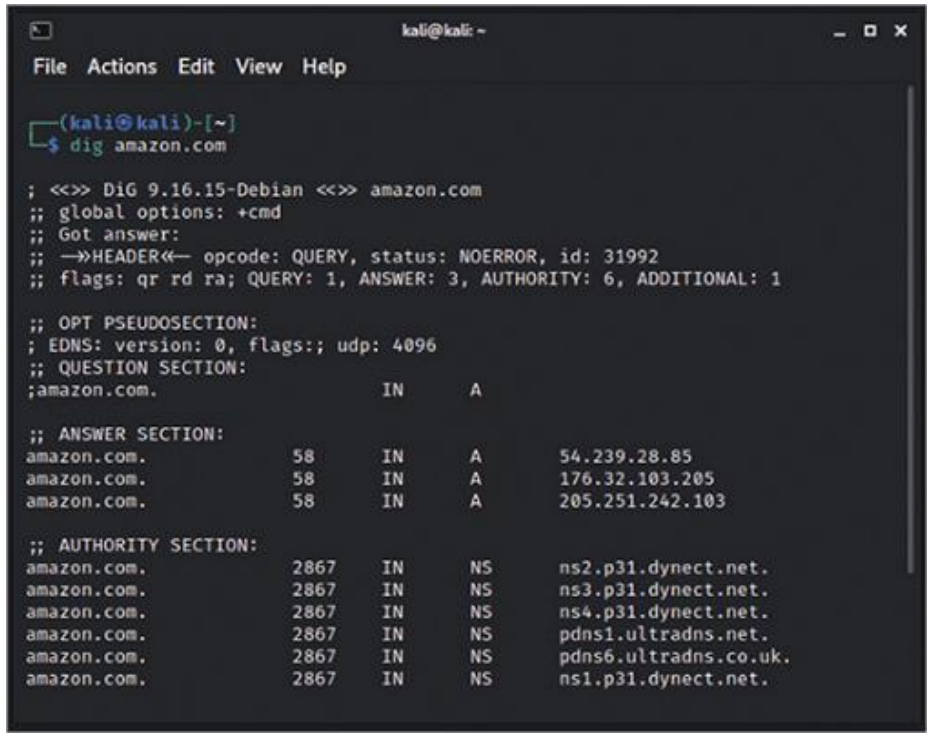
Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (11 of 27)

Gathering High-Level Organizational Information

DNS Lookups

- Native OS tools can be used to query DNS servers, Nslookup, and dig
- Query results vary widely by target
- DNS zone transfer request to server may return all known info about a particular zone, the domain, or subdomain of a target



Using dig to look up DNS info

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (12 of 27)

Gathering High-Level Organizational Information

Routers and Routing Information

- Knowing the IP addresses of network infrastructure can be valuable
- Routers and firewall IP data help pen testers determine or make guesses about:
  - The ISP and data network the target is using
  - The names and IP addresses of routers to target
  - Whether infrastructure is on-premise or hosted/owned elsewhere

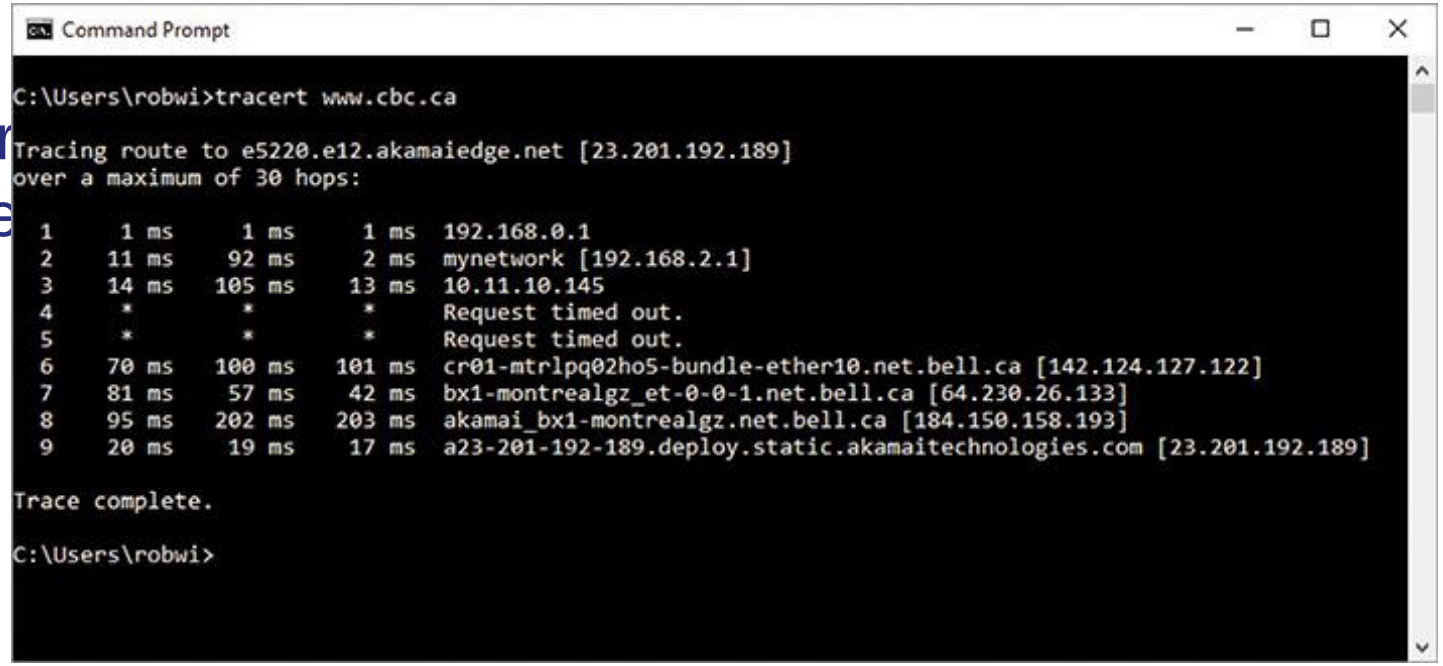
Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (13 of 27)

Gathering High-Level Organizational Information

Traceroute tool uses ICMP to deter
routers or “hops” between a source
target



Using the tracert command

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (14 of 27)

Gathering High-Level Organizational Information

War Driving

- Act of discovering wireless networks by walking or driving around using a Wi-Fi device and special software for detection
- Identifying whether discovered devices or systems are target owned or third-party hosted is important
  - Pen testing cloud-hosted wireless networks require additional authorization
  - Public and guest networks commonly use cloud management hosts
  - Use whois, traceroute, SSL/TLS certification info to make distinction

Cengage

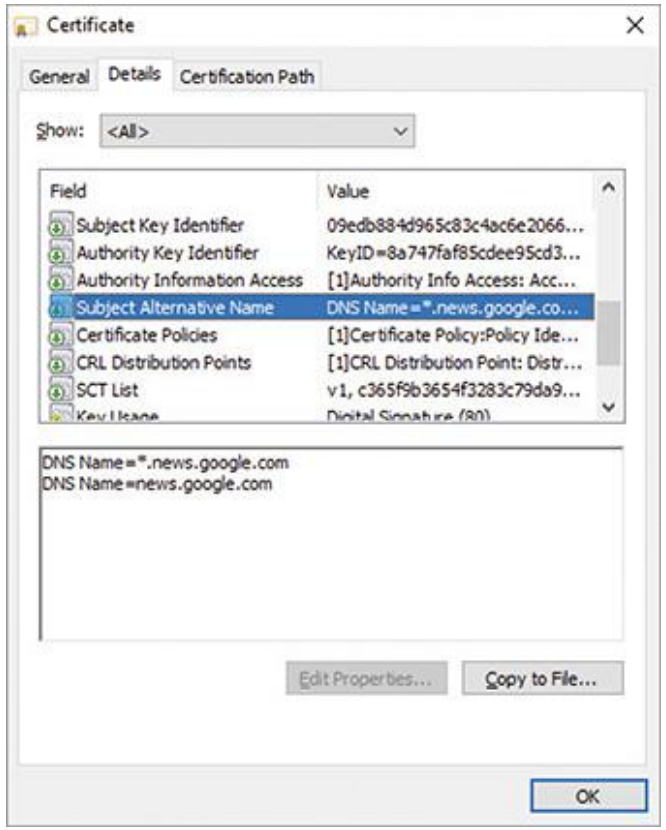
Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (15 of 27)

Company Reputation and Security Posture Data

SSL/TLS Certificates

- Identifies and verifies the integrity of websites and other systems and services
- Mechanism for browser to show site as secure
- Encryption performed using keys in certificates
- Other useful information such as DNS server names, organization info, keys, and more are contained in SSL/TLS digital certificates



Certificate details

Cengage

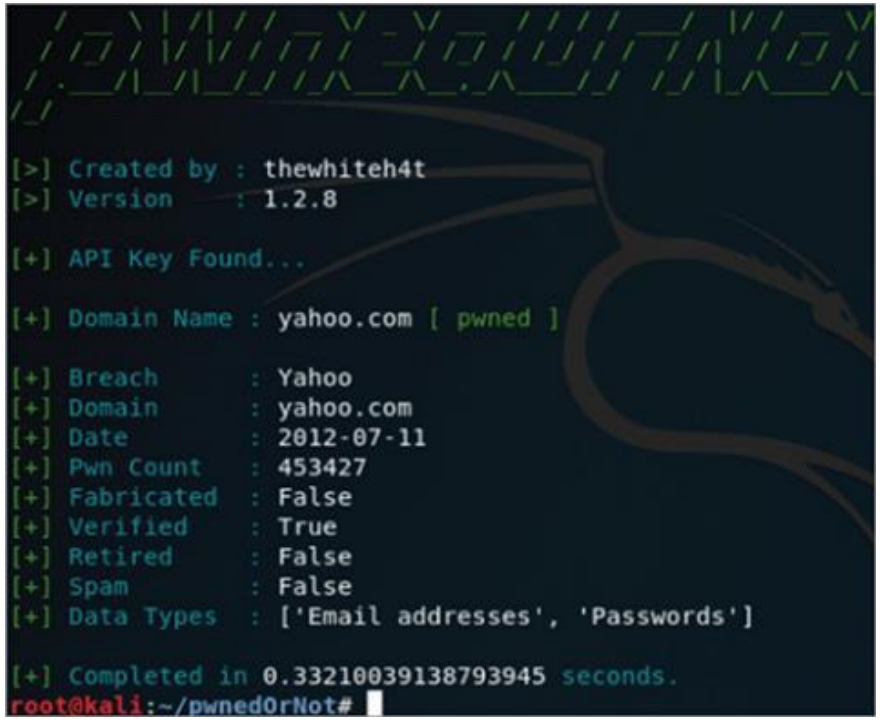
Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (16 of 27)

Company Reputation and Security Posture Data

Password Dumps

- Online databases of passwords from breaches can be useful to pen tester
- Large lists useful to automate brute-force logins or other attacks
- Stick to reputable sites and be wary of sales of password dumps



PwnedOrNot password dump info

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (17 of 27)

Company Reputation and Security Posture Data

Public-Facing Cloud Storage

- Cloud data services used by organizations to store data of all types
- Unsecured public-facing storage can unintentionally expose sensitive information
- Amazon Web Services (AWS) S3 and other cloud-storage management tools help targets identify public storage instances
- Search engine for public cloud storage is also useful

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (18 of 27)

Strategic Search Engine Analysis

Google Hacking Database (GHDB)

- Google search can be one of most useful tools for pen testers
- GHDB lists terms and tactics for pen testers to best Google targets

Shodan

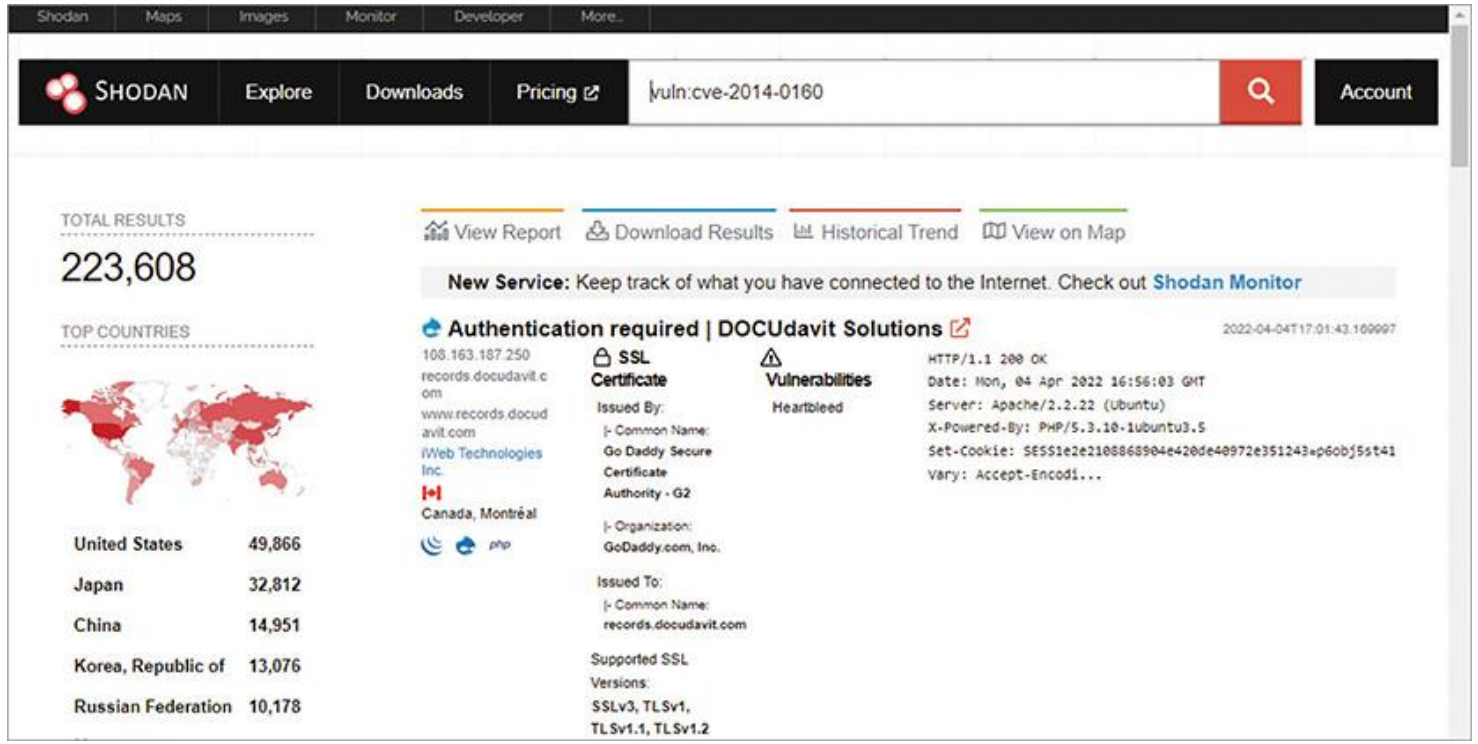
- Search engine for Internet of Things (IoT) devices
- Hosts discovered running non-standard protocols
- Specific vulnerabilities can be searched as well

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (19 of 27)

Strategic Search Engine Analysis

Shodan.io



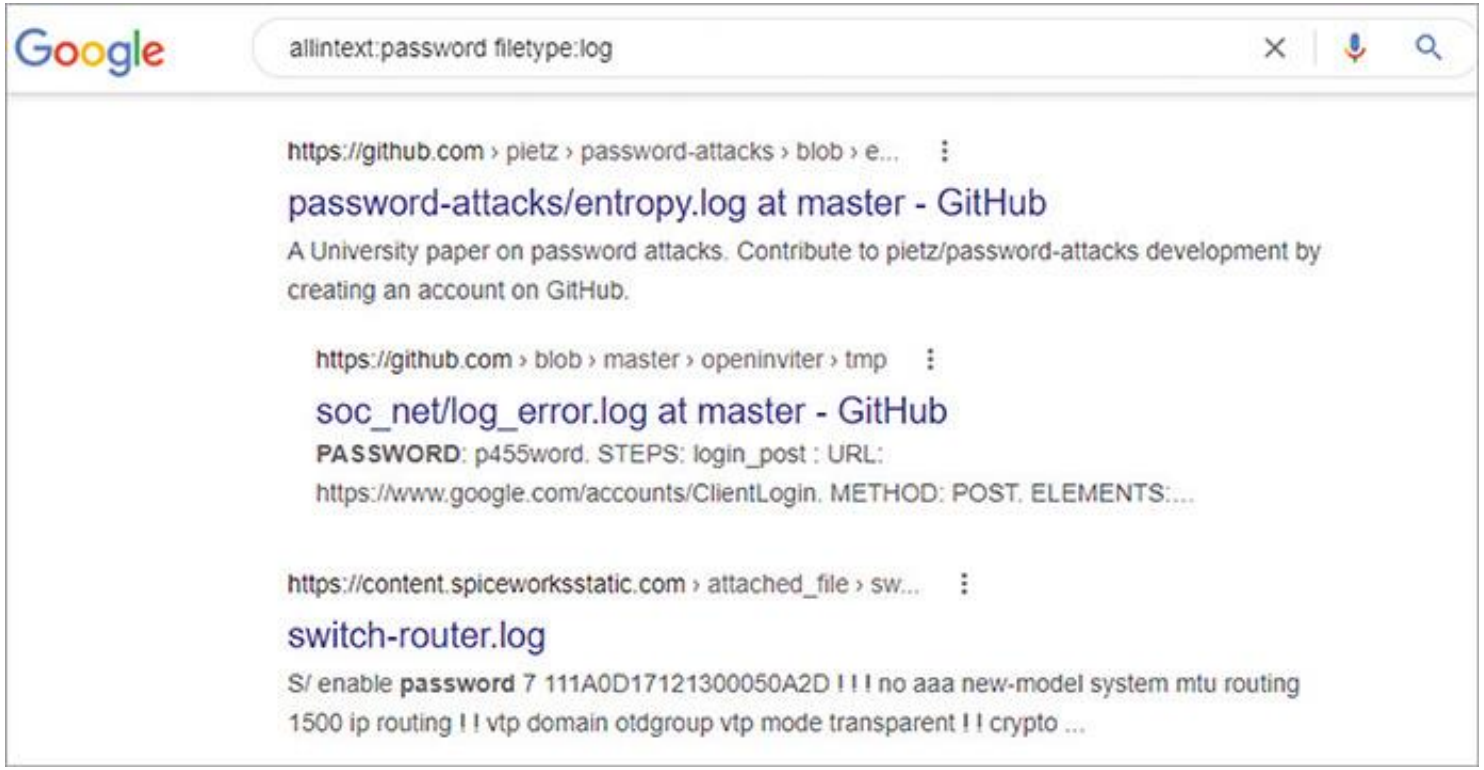
Shodan SSL Heartbleed vulnerability information

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (20 of 27)

Strategic Search Engine Analysis

Google Hacking Database (GHDB)



GHDB search for log files containing the keyword "password"

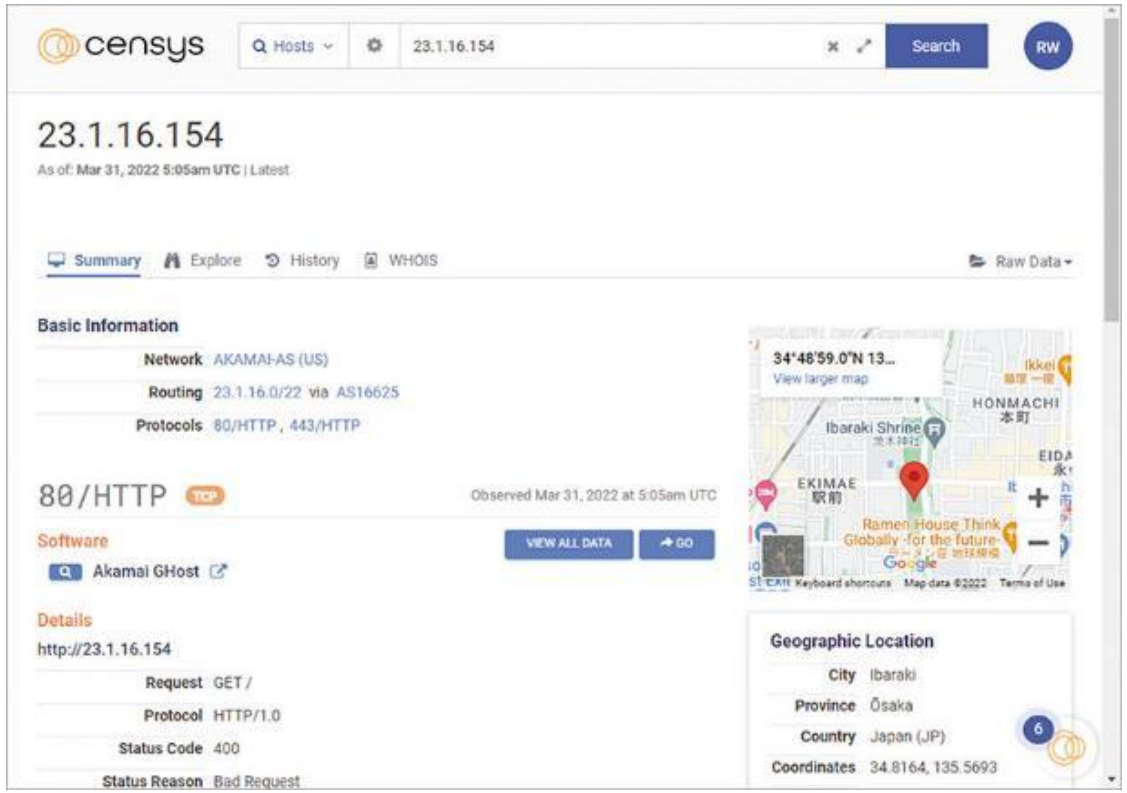
Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (21 of 27)

Strategic Search Engine Analysis

Censys

- Search engine similar to Shodan
- Includes geographic and device details



Censys details for specific host IP address

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (22 of 27)

Strategic Search Engine Analysis

Recon-Ng – web recon framework that pairs with Metasploit Framework

theHarvester – command-line tool to discover subdomains, email addresses, open ports, banners, and more from public sources

Maltego – gathers intelligence and displays results graphically

Cengage

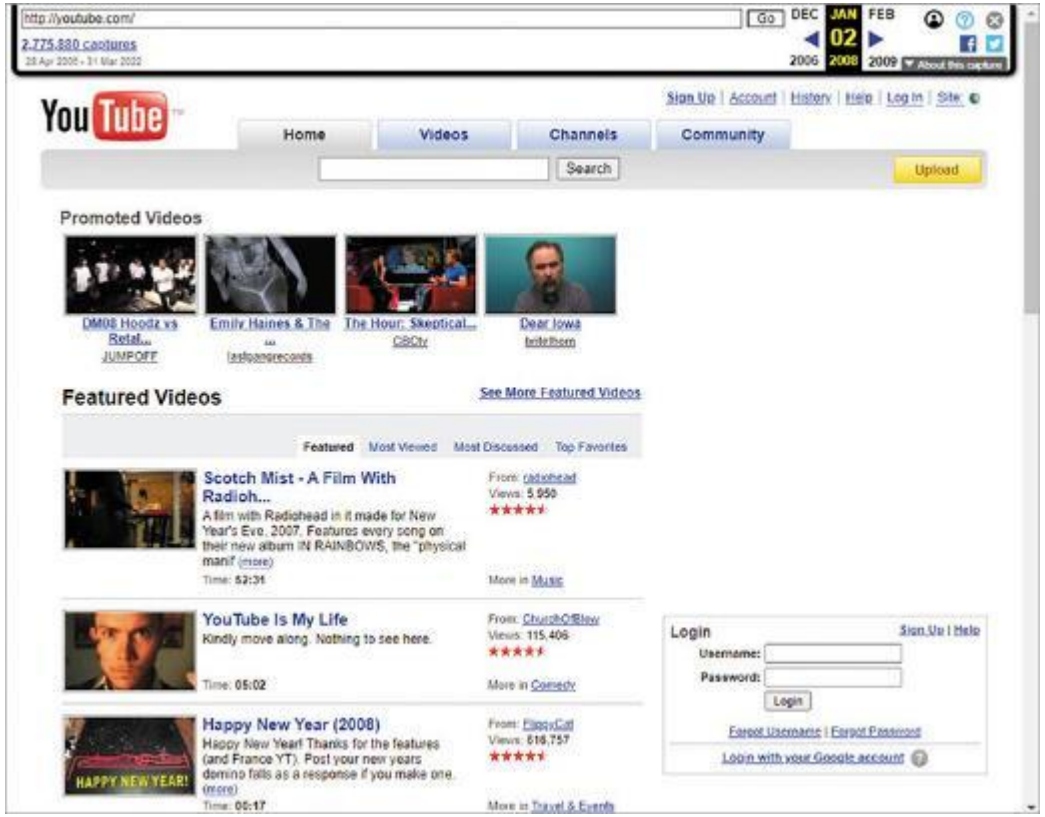
Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (23 of 27)

Strategic Search Engine Analysis

Website Archiving and Caching Databases

- The Internet Archive's "Way Back Machine"
- Snapshots of websites from years before
- Some sites may have many archive pages, others have few, or none



2008 YouTube on Way Back Machine

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (24 of 27)

Strategic Search Engine Analysis

Public Source-Code Repositories

- Source code available at public repositories can be invaluable
- Analyzing code in repositories such as GitHub and Ansible may contain very useful information shared both intentionally and inadvertently
  - Version info
  - Credentials and passwords
  - Configuration details
  - IP addresses of hosts
  - Proprietary code accidentally shared
  - Domains and subdomains
  - Contact data
  - Exploitable software code flaws

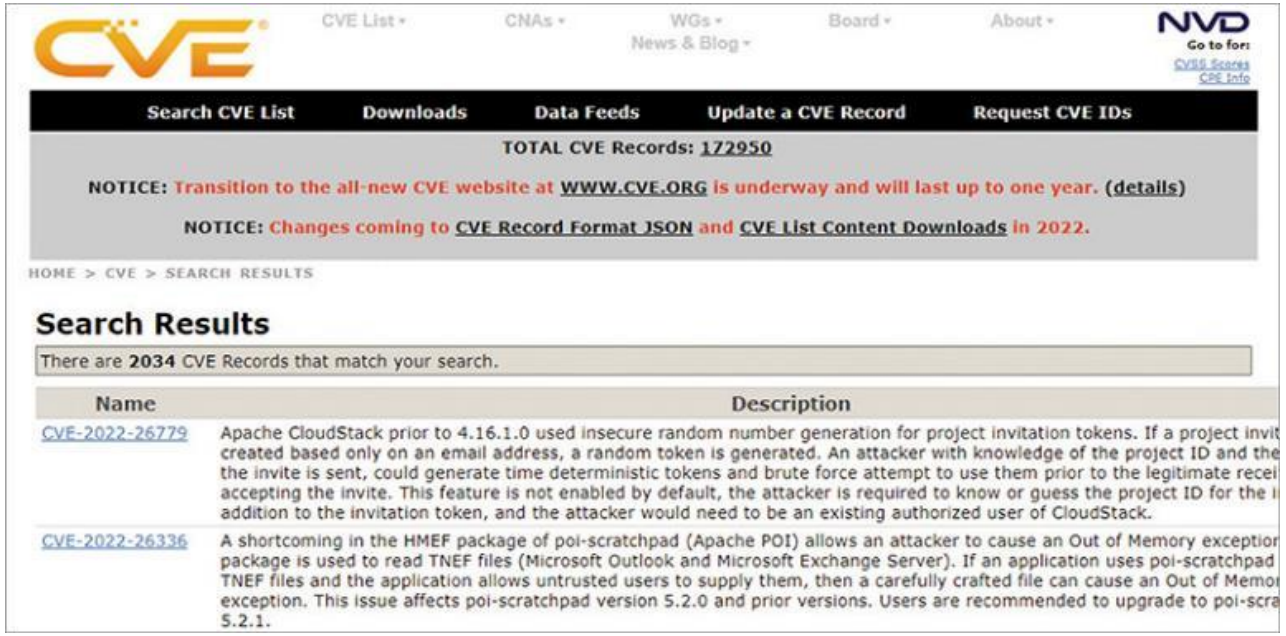
Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (25 of 27)

Strategic Search Engine Analysis

Common Vulnerabilities and Exposures (CVE)

- Mitre.org hosts web database of software vulnerabilities
- Each unique flaw given a CVE number
- Searchable site allows for finding known flaws in specific software



CVE search for Apache vulnerabilities

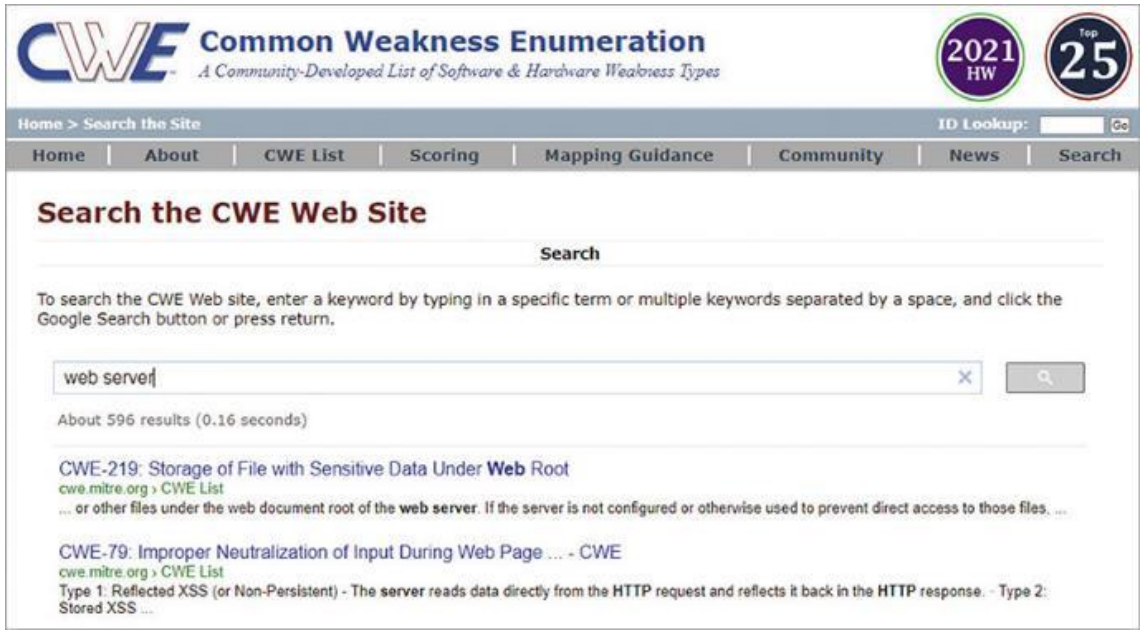
Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (26 of 27)

Strategic Search Engine Analysis

Common Weakness Enumeration (CWE)

- Database of hardware and software weaknesses
- General list of potential flaws rather than specific instances like CVE
- Useful to help developers prevent flaws being built into hardware and software



CWE web server weakness search

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Passive Reconnaissance Techniques (27 of 27)

Strategic Search Engine Analysis

Computer Emergency Response Team (CERT)

- Many CERT groups share a wide range of info useful to pen testers

National Institute of Standards and Technology (NIST)

- U.S. standards organization that publishes cybersecurity resources
- SP 800-115 Technical Guide to Information Security Testing and Assessment

Full Disclosure Lists

- Free and commercial lists and services sharing vulnerability and exploits

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Discussion Activity 4-1

Passive reconnaissance techniques are often the first actions taken during a penetration-testing engagement. Much of the information that can be gathered during web searches of useful resources and with other open-source intelligence sources could be used in social engineering.

In small groups, think about the types of information that are available and that can be located using the OSINT tools discussed in this module. Create three separate social engineering scenarios that consider what may be found. Consider what pieces of info are most useful to a pen tester or social engineer. What particular people (targets) would be most likely to help a pen tester further develop a pen-testing plan of action?

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (1 of 17)

Key Terms

Active Reconnaissance – tools and techniques that directly engage targets

- Many tools are available in Kali and elsewhere to perform active recon
  - Scanners probe networks for hosts and listening services

Enumeration – act of counting things and making lists. Pen testers enumerate many things in active reconnaissance:

- Hosts
- Ports
- Services
- Data files
- Vulnerabilities
- Networks

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (2 of 17)

Enumeration - Hosts

Make sure authorization to perform active reconnaissance is obtained prior to performing any active recon activities

- Nmap is by far most common scanning tool; pen tester's best friend
- Pen-testing targets can be people and processes, usually computers
- Ping sweep often one of first active recon activities for host discovery
  - Tool scans a target network or IP and listens for response
  - Response reply indicates host is up at that IP address

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (3 of 17)

Enumeration - Hosts

- White box testing may provide a list of host IP addresses to pen tester
  - Can eliminate the need for host discovery scan
  - Tools such as Nmap, Nessus, and many others perform host discovery
- Other tools and resources can help locate host IP addresses, if available
  - Logs and config files – DHCP logs, router/firewall logs, system configs
  - Network management tools – may contain detailed host data

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (4 of 17)

Enumeration - Hosts

- Pen-testing targets can be people, processes; usually computers
- Ping sweep is often one of first activities for host discovery
  - Tool scans a target
  - Replies indicate host is “up”
  - Host discovery often uses ICMP
  - TCP, ARP, and other protocols can be used for host discovery

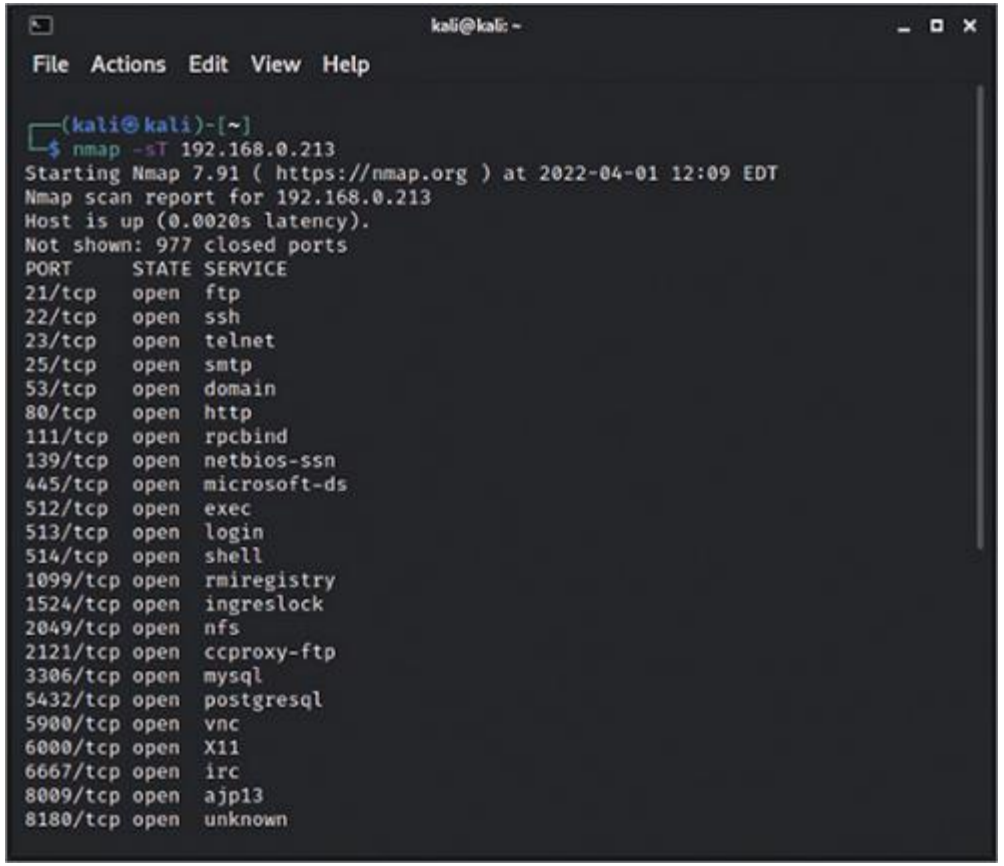
Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (5 of 17)

Enumeration – Services

- Determining if TCP or UDP ports are open
- Open port usually indicates a software service is “listening” for clients to connect and send network traffic
- Well-known ports numbers – commonly low-numbered TCP or UDP ports most often used by systems for network communication



Scanning for open ports with Nmap

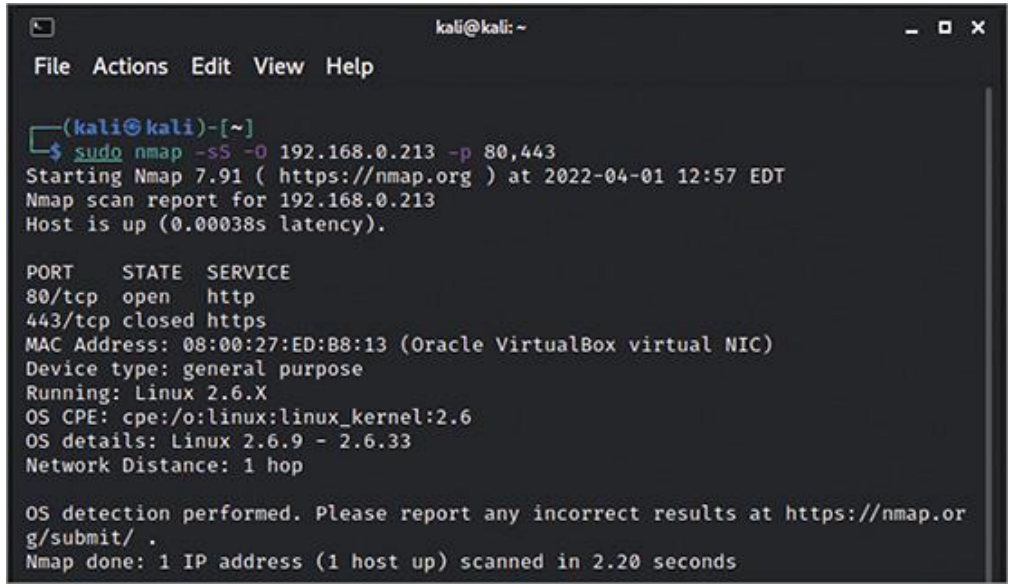
Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (6 of 17)

Enumeration – Nmap

- Nmap most widely known and used tool for enumerating services
- Zenmap is GUI for nmap
- Proficiency with command line nmap may make scanning more efficient
- Large community of users and experts
- Many features well beyond just simple host discovery and port scanning



Nmap scan for operating system

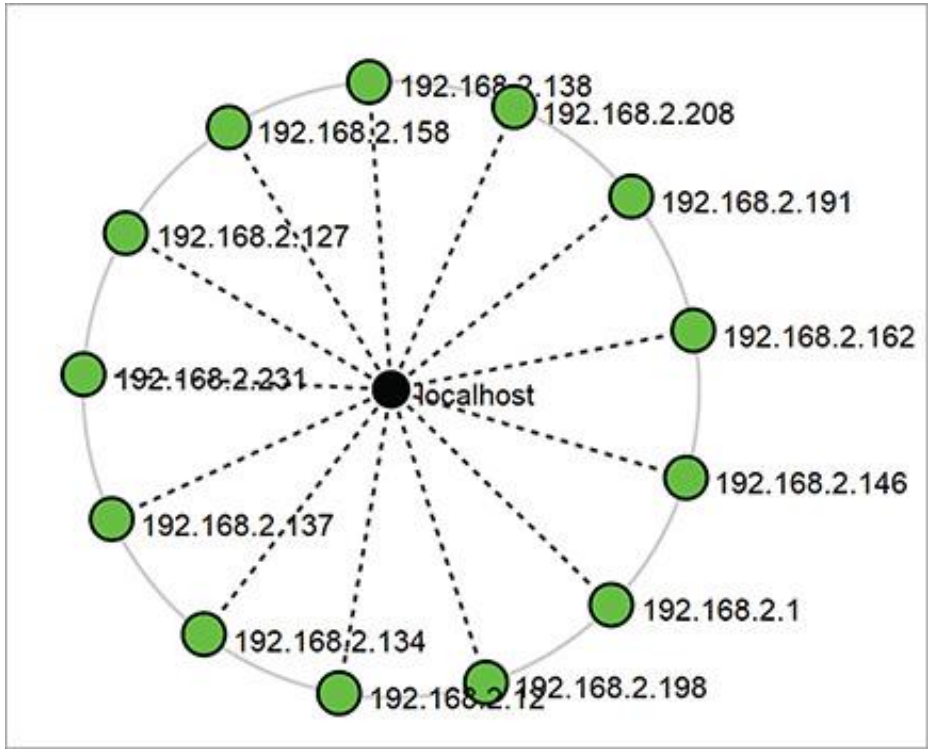
Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (7 of 17)

Enumeration - Network Topology

- Understanding the topology of a network helps understand how systems connect
- Free and commercial tools help develop diagram of network topology
- Knowledge of connections can further direct pen-test activities
- SNMP and other tools or protocols can assist in topology discovery and mapping



Zenmap network topology diagram

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (8 of 17)

Enumeration – Users and User Groups

- Determining valid user accounts or login identifiers
- Network protocol enumeration tools may discover usernames
- Security groups facilitate the distribution of permissions
- Distribution groups consist of email accounts for message distribution
- Microsoft's Active Directory (AD) is the management and security cornerstone for Windows domains
  - AD has tools for administration of users and groups

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (9 of 17)

Enumeration – Email Addresses

- Email addresses used in social engineering and phishing
- Frequently used as an account name
- Possible use in password attacks
- OSINT tools and directories to search
- theHarvester and Metasploit Framework have email address harvesting capability

theHarvester searching for email

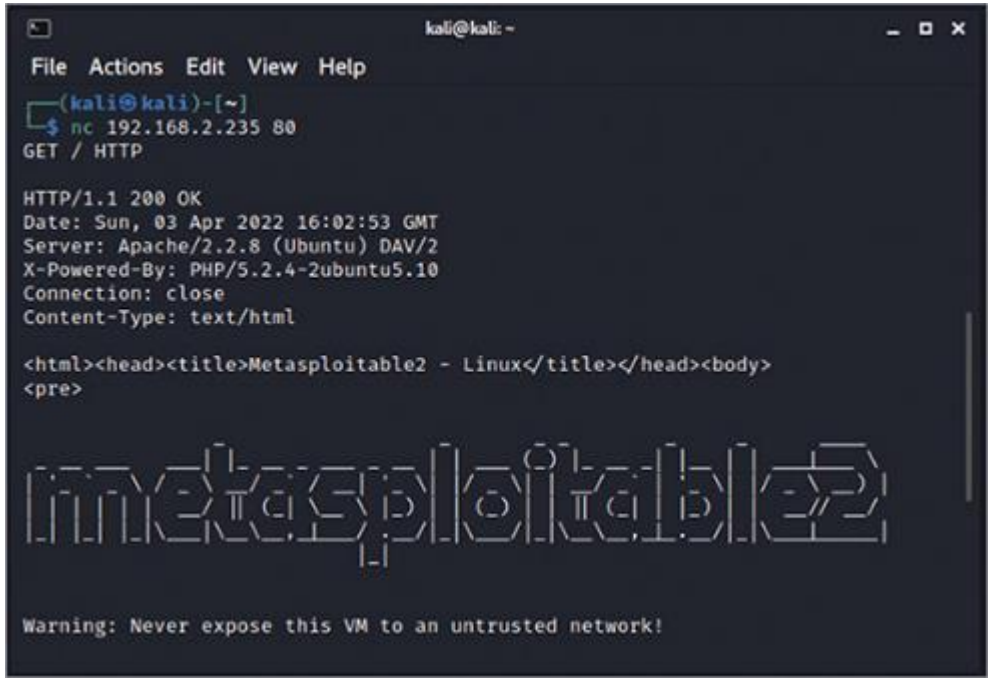
Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (10 of 17)

Enumeration – Shares and Applications

- Shares are file directories accessible to users on other remote systems
- Tools scan using sharing protocols like SMB and NFS
- Application running on remote systems may have critical or remote vulnerabilities
- Version information of running applications can be retrieved by “banner grab,” or capture of a network service or protocol sharing useful info, like the version used



Netcat (nc) banner grab

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (11 of 17)

Website Reconnaissance – Crawling and Scraping Websites

Crawling – exploring a site's structure by checking all links and folders

Scraping – extracting useful info from webpages, files, and crawling

- Network hosts may run a web service for management or configuration
- Crawling and scraping can identify info for social engineering
- Crawling by hand possible, but other tools are more efficient and thorough
  - Wget, msfcrawler, Black Widow, w3af, Burp Suite Spider
- Robots.txt – file on web server contain IP of hosts not to crawl, can be ignored by attackers or used to advantage of pen tester

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

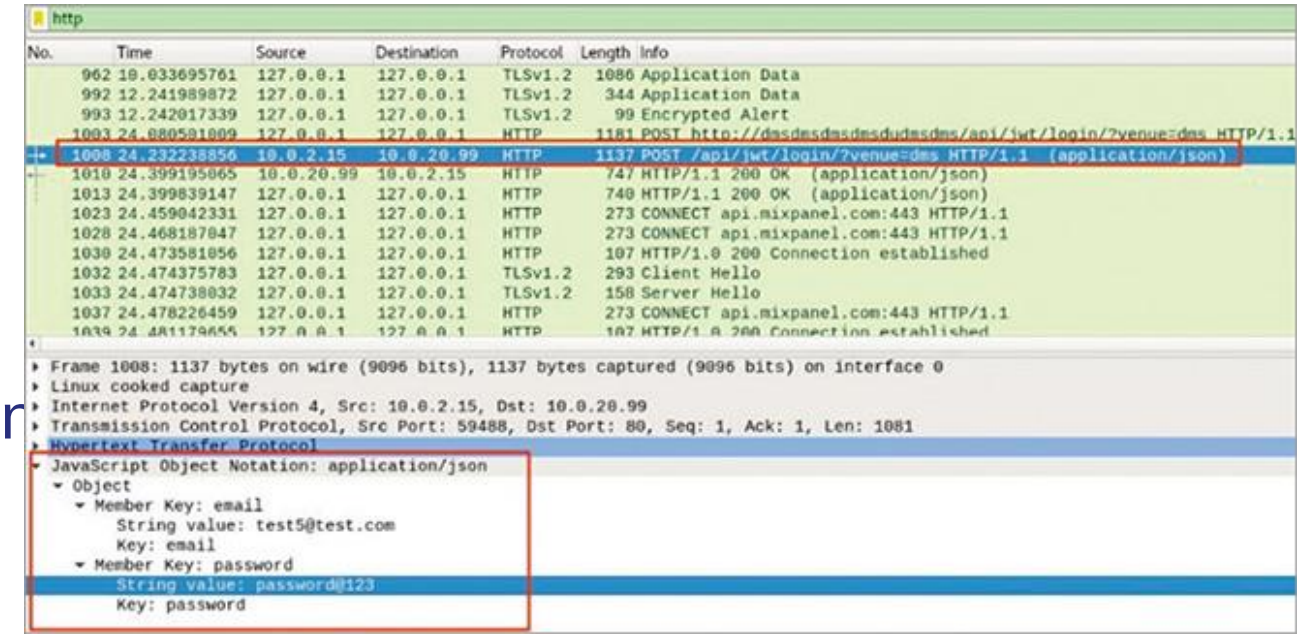
Active Reconnaissance Techniques (12 of 17)

Packet Interception and Crafting

Packet sniffing – taking copies of messages passed by network interface

Wireshark – most well- known packet interception and network analyzer tool

- GUI displays packets
- Protocols are parsed and displayed in format readable by humans



Wireshark intercepting unencrypted password

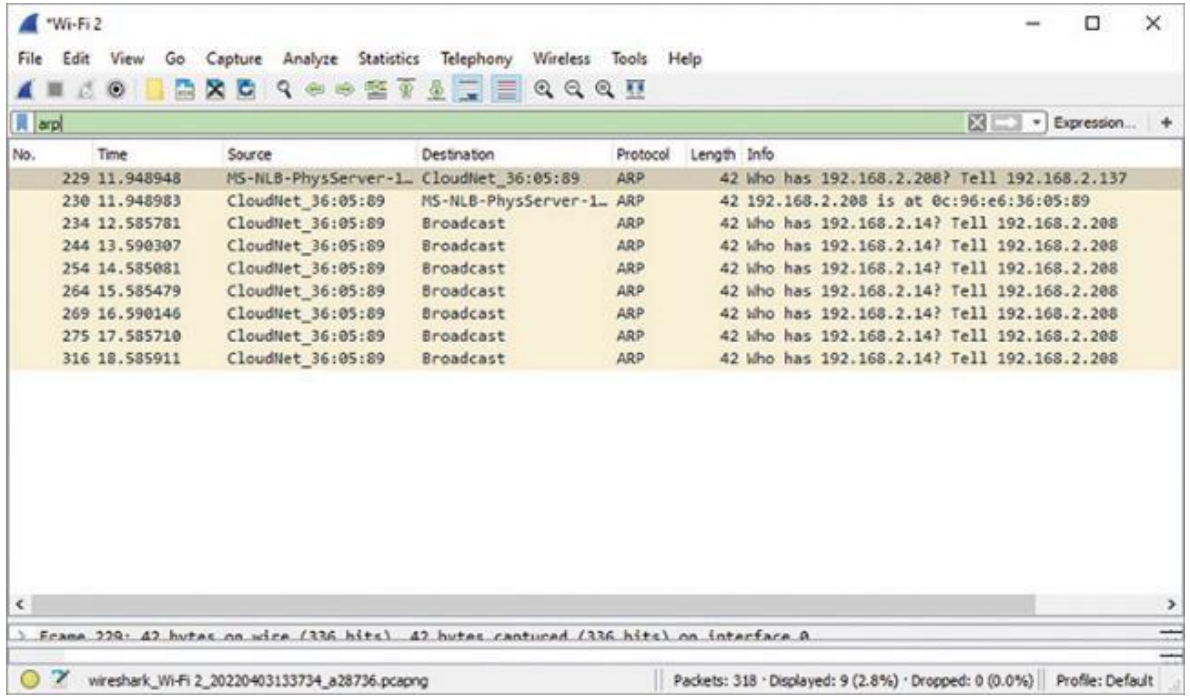
Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (13 of 17)

Packet Interception and Crafting

- Network protocol headers in captured frames may contain unencrypted passwords
- Address Resolution Protocol (ARP) traffic contains MAC addresses of network hosts
- Captured traffic can be replayed in more active pen- test techniques, Man In The Middle (MITM) attack



Wireshark intercepting unencrypted password

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (14 of 17)

Packet Interception and Crafting – Tokens

Tokens are data elements in networks, systems, and applications to help with authentication and authorization

- Tokens may be intercepted or acquired; used to gain access
- Token attacks are complex and vary by type of token
- Token concepts on the PenTest+
  - Scoping tokens to see if they contain user info; access level details
  - Issuing tokens created by pen tester to provide system access
  - Revoking tokens effectively destroys access session created

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (15 of 17)

Defense Detection

Active recon may involve detecting defensive security devices on network

PenTest+ exam covers four types of defensive devices:

- Load balancer – software or hardware to distribute network workload
- Web application firewall (WAF) –protects web apps and servers
- Antivirus software –can interfere with pen-testing attempts, block files
  - Tools can modify pen-test files and applications to evade antivirus
- Firewall – use rules to intercept and block traffic
  - The software tool Firewalk detects traffic paths that are allowed through

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (16 of 17)

Cloud Asset Discovery and Third-Party Hosted Services

- Organizations may host all or part of infrastructure in the cloud
  - Virtual servers
    - Web servers
  - Virtual storage
    - AWS S3 buckets
  - Applications
    - Office 365

- Permission from third party must be acquired before any cloud-testing activities begin
- Cloud vendors likely will have Rules of Engagement and other acceptable-use policies for pen testers working with the cloud provider's customers

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Active Reconnaissance Techniques (17 of 17)

Detection Avoidance

- Passive reconnaissance is rarely detectable by a target
- Active reconnaissance may be detectable by target, target's network provider, or cloud service provider
- Pen test may require avoiding detection
- Tests requested by the target may not require avoiding detection
- Scanning and enumeration tools may employ tactics to limit detection
  - Limiting scan to a few targets
  - Reducing number of ports to scan
  - Faking or changing IP or MAC address regularly
  - Increasing time between scans

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Discussion Activity 4-2

Pen testers will employ many different resources available to them during the reconnaissance phase of a pen-test engagement. The more information about the target the tester can gather, the more options are available to the tester once the more involved steps of the test are underway. Passive reconnaissance is extremely useful, but there are results needed for success that only active recon can provide.

Discuss with other learners the active reconnaissance tools and techniques in this module, and create a “Top 5” list. Discuss the types of information to be found in each and how it is valuable to a pen tester.

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Summary

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

1. Apply passive reconnaissance techniques
2. Apply active reconnaissance techniques
3. Analyze the results of reconnaissance
4. Use active and passive reconnaissance tools

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.