

CompTIA PenTest+ Guide to Penetration Testing, 1e

Module 4: Information Gathering

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

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

Passive Reconnaissance Techniques (2 of 27)

Gathering High-Level Organizational Information Geographic Locations and Organizational Structure

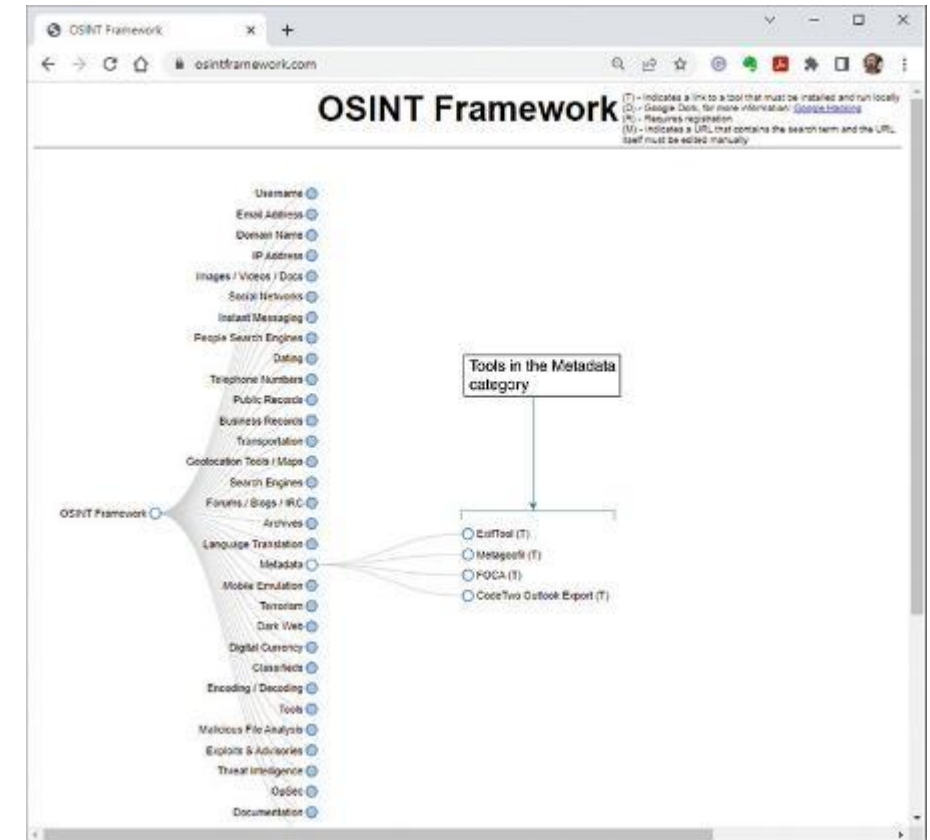
- Knowing physical location can be important during a pen test
- Some pen tests target physical security
- Sources for physical location information
 - Target organization websites
 - Social media postings about target
 - Public records, including business licenses and tax information

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

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

Passive Reconnaissance Techniques

(5 of 27)

Gathering High-Level Organizational Information

Document Metadata

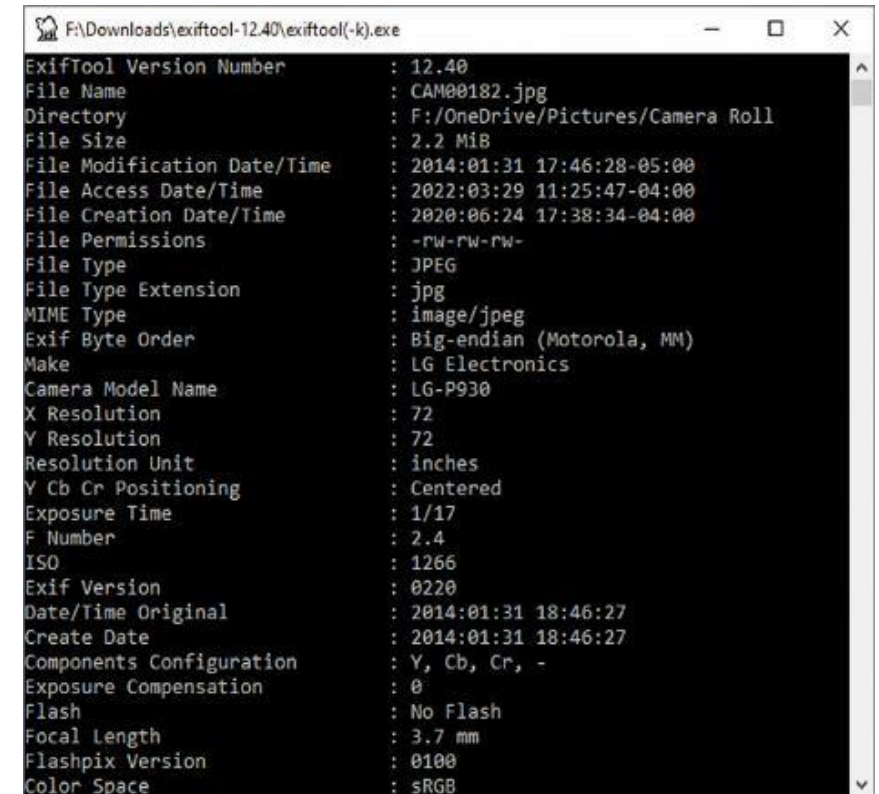
- Metadata is “data about data”
- Details about files, beyond the main info within a file
 - File creation date
 - Author
 - Servers related to document
 - Users
 - Email addresses
 - Operating system
 - GPS coordinates

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



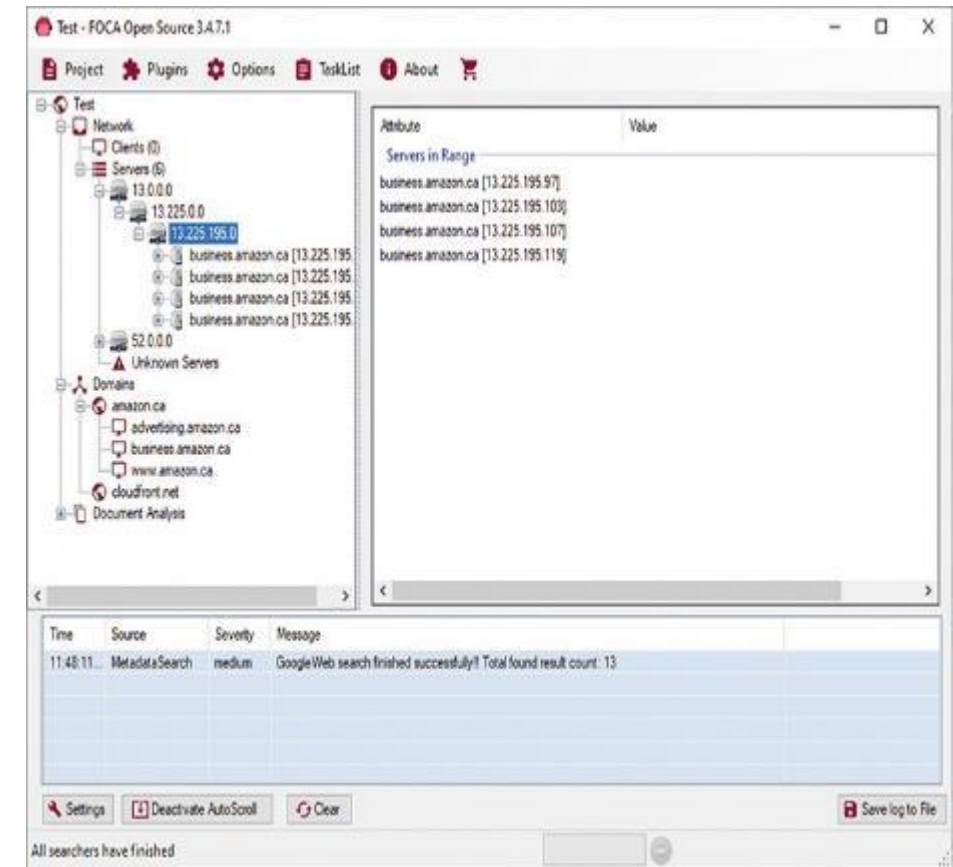
```
F:\Downloads\exiftool-12.40\exiftool(-k).exe
ExifTool Version Number      : 12.40
File Name                    : CAM00182.jpg
Directory                   : F:/OneDrive/Pictures/Camera Roll
File Size                    : 2.2 MiB
File Modification Date/Time  : 2014:01:31 17:46:28-05:00
File Access Date/Time       : 2022:03:29 11:25:47-04:00
File Creation Date/Time     : 2020:06:24 17:38:34-04:00
File Permissions             : -rw-rw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order              : Big-endian (Motorola, MM)
Make                         : LG Electronics
Camera Model Name            : LG-P930
X Resolution                 : 72
Y Resolution                 : 72
Resolution Unit              : inches
Y Cb Cr Positioning         : Centered
Exposure Time                : 1/17
F Number                     : 2.4
ISO                           : 1266
Exif Version                 : 0220
Date/Time Original           : 2014:01:31 18:46:27
Create Date                  : 2014:01:31 18:46:27
Components Configuration    : Y, Cb, Cr, -
Exposure Compensation       : 0
Flash                       : No Flash
Focal Length                 : 3.7 mm
Flashpix Version             : 0100
Color Space                  : sRGB
```

Image file metadata in ExifTool

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

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

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

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

The screenshot displays the 'Domain Dossier' web application. At the top, it says 'Investigate domains and IP addresses'. A search bar contains 'microsoft.com'. Below the search bar, there are checkboxes for 'domain whois record' (checked), 'DNS records' (checked), 'network whois record' (unchecked), and 'service scan' (unchecked). There are also links for 'traceroute' and a 'go' button. Below this, user information is shown: 'user: anonymous [69.159.60.3]', 'balance: 48 units', and 'log in | account info'. A notice states: 'Do you see Whois records that are missing contact information? Read about reduced Whois data due to the GDPR.' The 'Address lookup' section shows the canonical name 'microsoft.com.' and a list of aliases: '104.215.148.63', '40.76.4.15', '40.112.72.205', '40.113.200.201', and '13.77.161.179'. The 'Domain Whois record' section shows the queried whois.internic.net with 'dom microsoft.com'... and the following details: 'Domain Name: MICROSOFT.COM', 'Registry Domain ID: 2724960_DOMAIN_COM-VRSN', 'Registrar WHOIS Server: whois.markmonitor.com', and 'Registrar URL: http://www.markmonitor.com'.

Domain Dossier tool with whois info

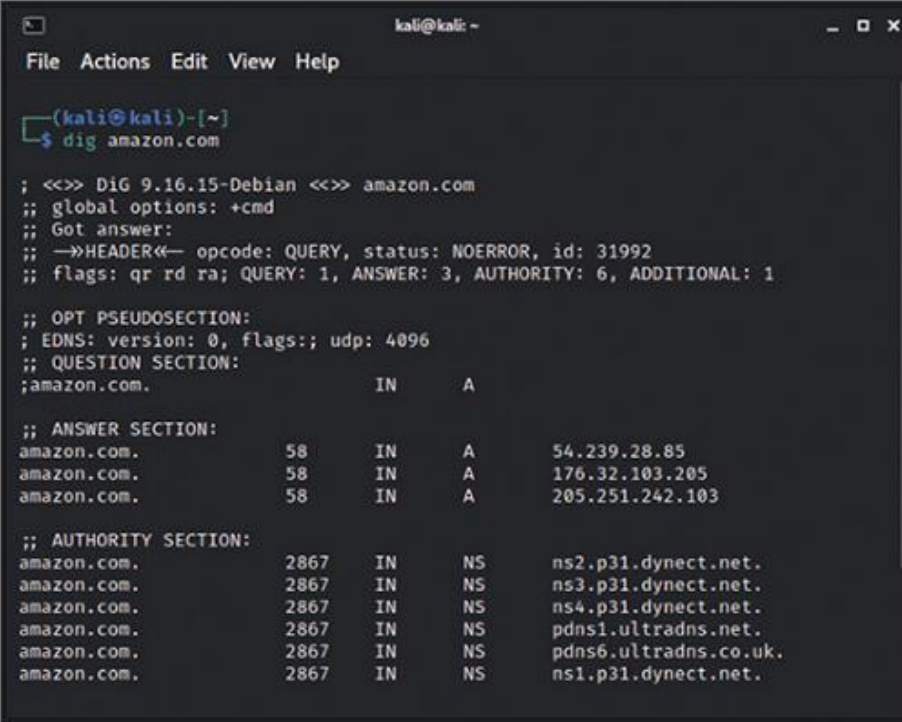
Passive Reconnaissance Techniques

(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



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ dig amazon.com  
  
; <<>> DiG 9.16.15-Debian <<>> amazon.com  
;; global options: +cmd  
;; Got answer:  
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 31992  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 6, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;amazon.com. IN A  
  
;; ANSWER SECTION:  
amazon.com. 58 IN A 54.239.28.85  
amazon.com. 58 IN A 176.32.103.205  
amazon.com. 58 IN A 205.251.242.103  
  
;; AUTHORITY SECTION:  
amazon.com. 2867 IN NS ns2.p31.dynect.net.  
amazon.com. 2867 IN NS ns3.p31.dynect.net.  
amazon.com. 2867 IN NS ns4.p31.dynect.net.  
amazon.com. 2867 IN NS pdns1.ultradns.net.  
amazon.com. 2867 IN NS pdns6.ultradns.co.uk.  
amazon.com. 2867 IN NS ns1.p31.dynect.net.
```

Using dig to look up DNS info

Passive Reconnaissance Techniques (12 of 27)

Gathering High-Level Organizational Information

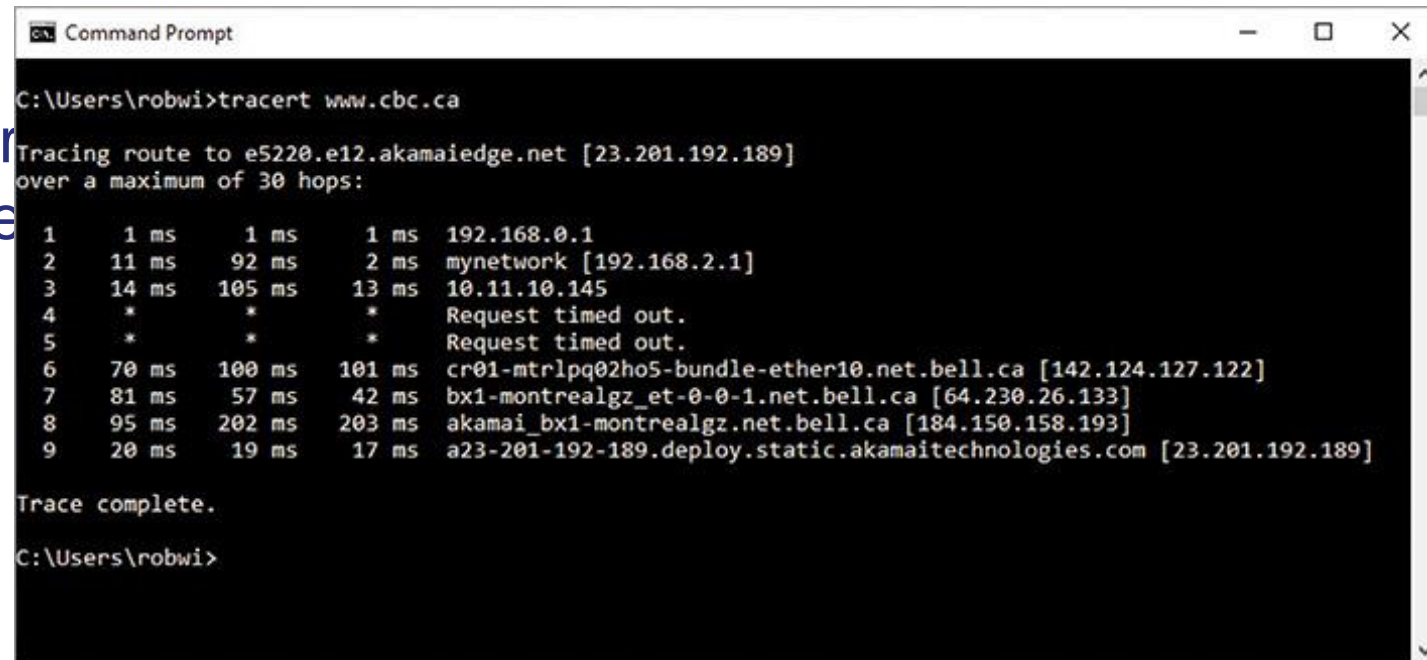
Routers and Routing Information

- 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

Passive Reconnaissance Techniques (13 of 27)

Gathering High-Level Organizational Information

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



```
Command Prompt
C:\Users\robwi>tracert www.cbc.ca

Tracing route to e5220.e12.akamaiedge.net [23.201.192.189]
over a maximum of 30 hops:
  0  0 ms  0 ms  0 ms  192.168.0.1
  1  11 ms  92 ms  2 ms  mynetwork [192.168.2.1]
  2  14 ms  105 ms  13 ms  10.11.10.145
  3  *      *      *      Request timed out.
  4  *      *      *      Request timed out.
  5  70 ms  100 ms  101 ms  cr01-mtrlpq02ho5-bundle-ether10.net.bell.ca [142.124.127.122]
  6  81 ms  57 ms  42 ms  bx1-montrealgz_et-0-0-1.net.bell.ca [64.230.26.133]
  7  95 ms  202 ms  203 ms  akamai_bx1-montrealgz.net.bell.ca [184.150.158.193]
  8  20 ms  19 ms  17 ms  a23-201-192-189.deploy.static.akamaitechnologies.com [23.201.192.189]

Trace complete.

C:\Users\robwi>
```

Using the tracert command

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

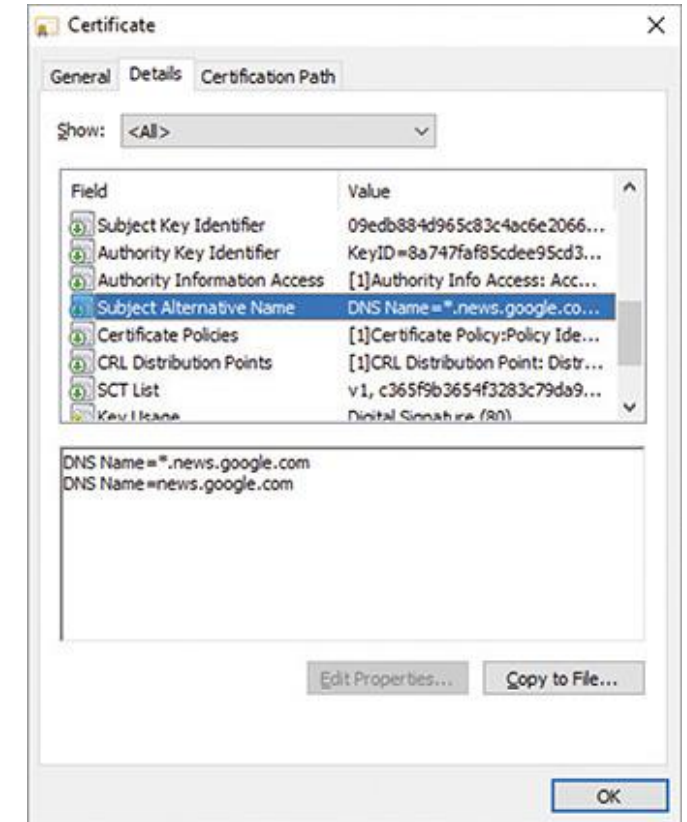
Passive Reconnaissance Techniques

(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

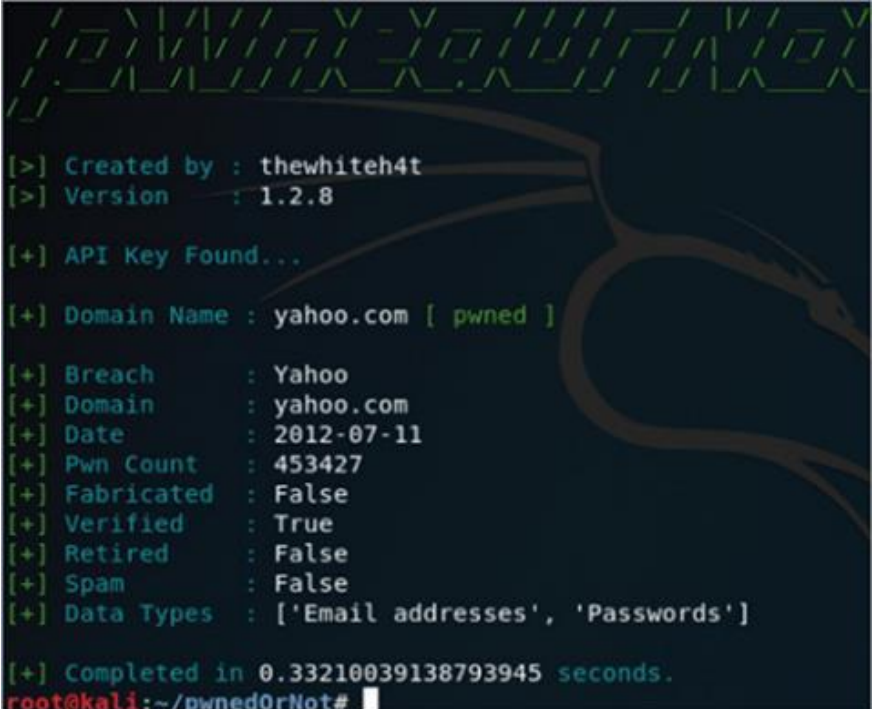
Passive Reconnaissance Techniques

(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



```
[>] Created by : thewhiteh4t
[>] Version : 1.2.8

[+] API Key Found...

[+] Domain Name : yahoo.com [ pwned ]

[+] Breach : Yahoo
[+] Domain : yahoo.com
[+] Date : 2012-07-11
[+] Pwn Count : 453427
[+] Fabricated : False
[+] Verified : True
[+] Retired : False
[+] Spam : False
[+] Data Types : ['Email addresses', 'Passwords']

[+] Completed in 0.33210039138793945 seconds.
root@kali:~/pwnedOrNot#
```

PwnedOrNot password dump info

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

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

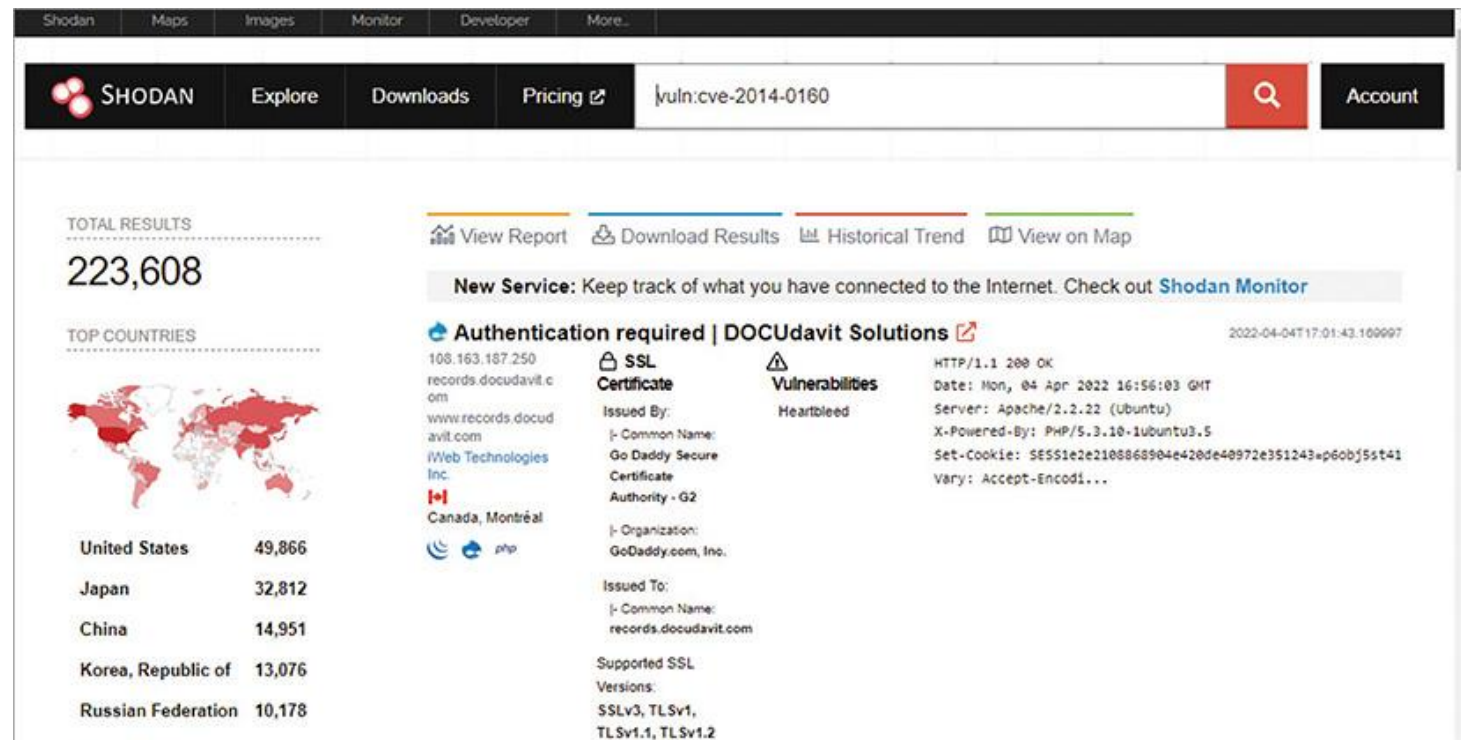
Shodan

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

Passive Reconnaissance Techniques (19 of 27)

Strategic Search Engine Analysis

Shodan.io

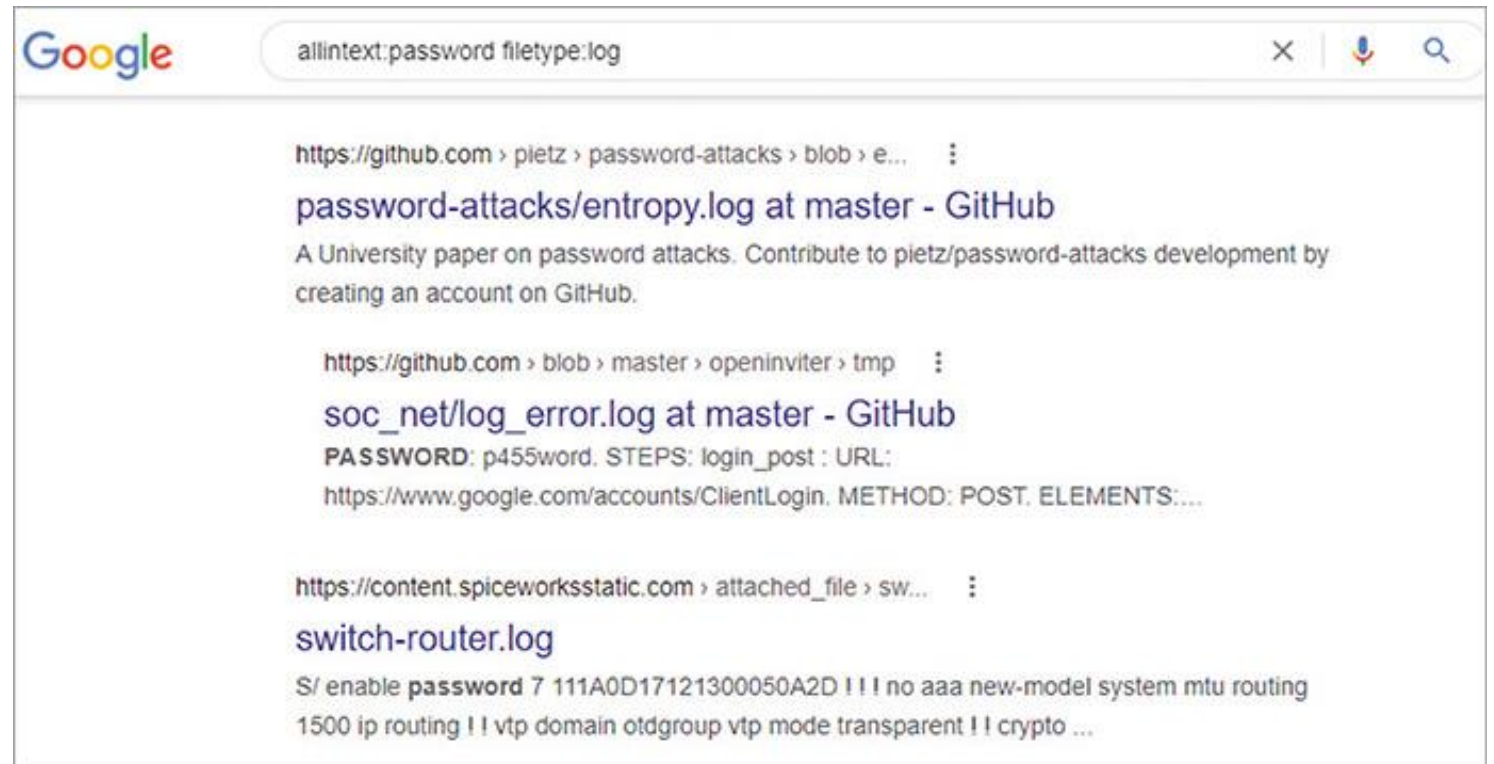


Shodan SSL Heartbleed vulnerability information

Passive Reconnaissance Techniques (20 of 27)

Strategic Search Engine Analysis

Google Hacking Database (GHDB)



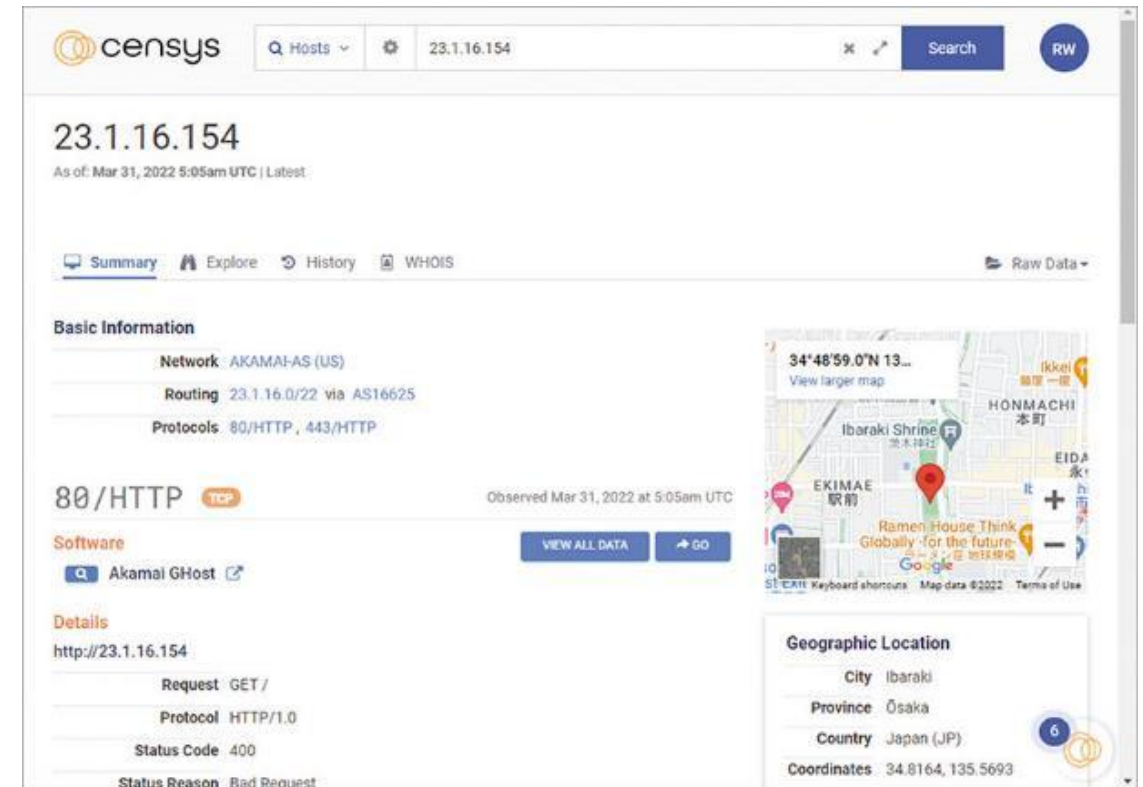
GHDB search for log files containing the keyword "password"

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

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

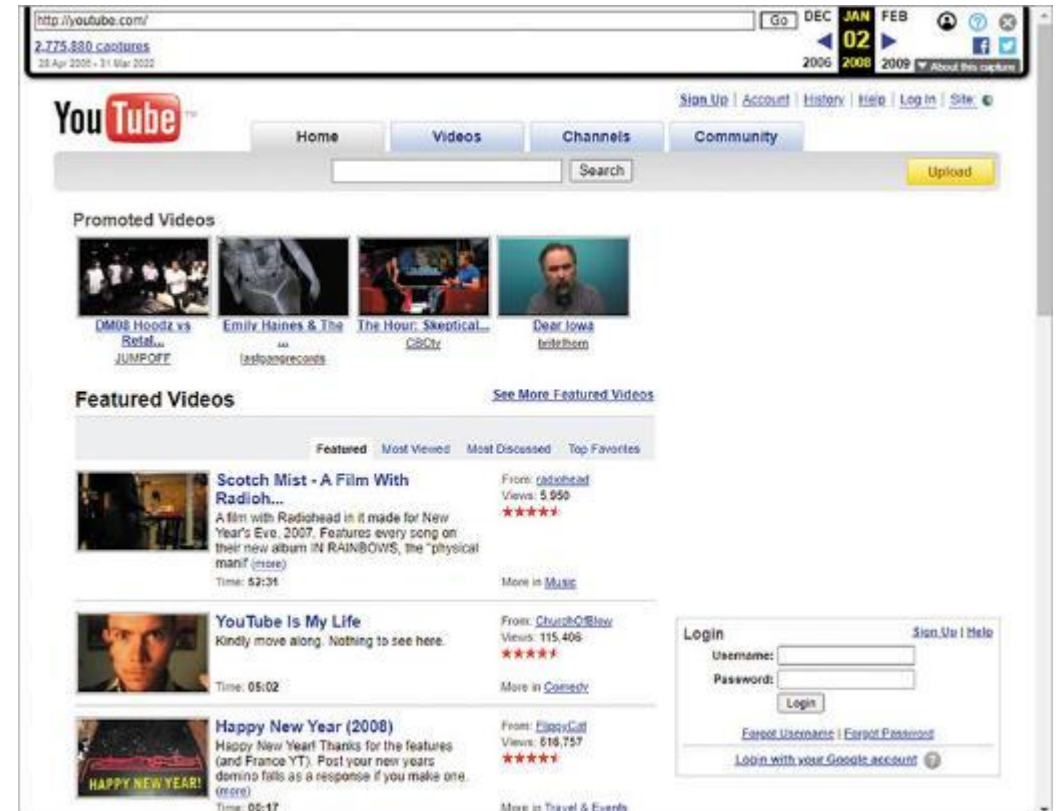
Maltego – gathers intelligence and displays results graphically

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

Passive Reconnaissance Techniques (24 of 27)

Strategic Search Engine Analysis

Public Source-Code Repositories

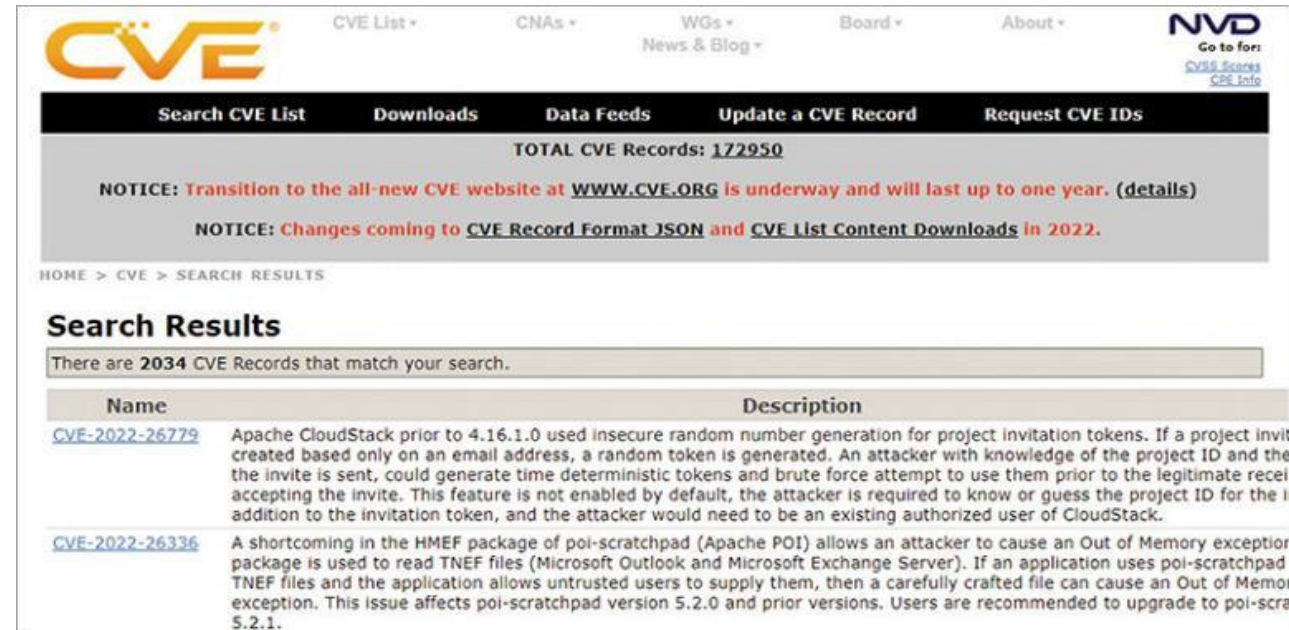
- Source code available at public repositories can be invaluable
- Analyzing code in repositories such as GitHub and Ansible may contain very useful information shared both intentionally and inadvertently
 - Version info
 - Credentials and passwords
 - Configuration details
 - IP addresses of hosts
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

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



The screenshot shows the CVE website interface. At the top, there's a navigation bar with links like 'CVE List', 'CNAs', 'WGs', 'Board', and 'About'. Below this is a search bar and a 'Search CVE List' button. The main content area displays 'TOTAL CVE Records: 172950' and two notices regarding the transition to the new CVE website and changes to the CVE Record Format JSON and CVE List Content Downloads in 2022. Below the notices, there's a 'Search Results' section showing 'There are 2034 CVE Records that match your search.' A table lists the results, with the first entry being CVE-2022-26779, which describes a vulnerability in Apache CloudStack related to insecure random number generation for project invitation tokens. The second entry is CVE-2022-26336, which describes a shortcoming in the HMEF package of poi-scratchpad (Apache POI) that allows an attacker to cause an Out of Memory exception.

Name	Description
CVE-2022-26779	Apache CloudStack prior to 4.16.1.0 used insecure random number generation for project invitation tokens. If a project invite is created based only on an email address, a random token is generated. An attacker with knowledge of the project ID and the invite is sent, could generate time deterministic tokens and brute force attempt to use them prior to the legitimate recipient accepting the invite. This feature is not enabled by default, the attacker is required to know or guess the project ID for the addition to the invitation token, and the attacker would need to be an existing authorized user of CloudStack.
CVE-2022-26336	A shortcoming in the HMEF package of poi-scratchpad (Apache POI) allows an attacker to cause an Out of Memory exception. The package is used to read TNEF files (Microsoft Outlook and Microsoft Exchange Server). If an application uses poi-scratchpad TNEF files and the application allows untrusted users to supply them, then a carefully crafted file can cause an Out of Memory exception. This issue affects poi-scratchpad version 5.2.0 and prior versions. Users are recommended to upgrade to poi-scratchpad 5.2.1.

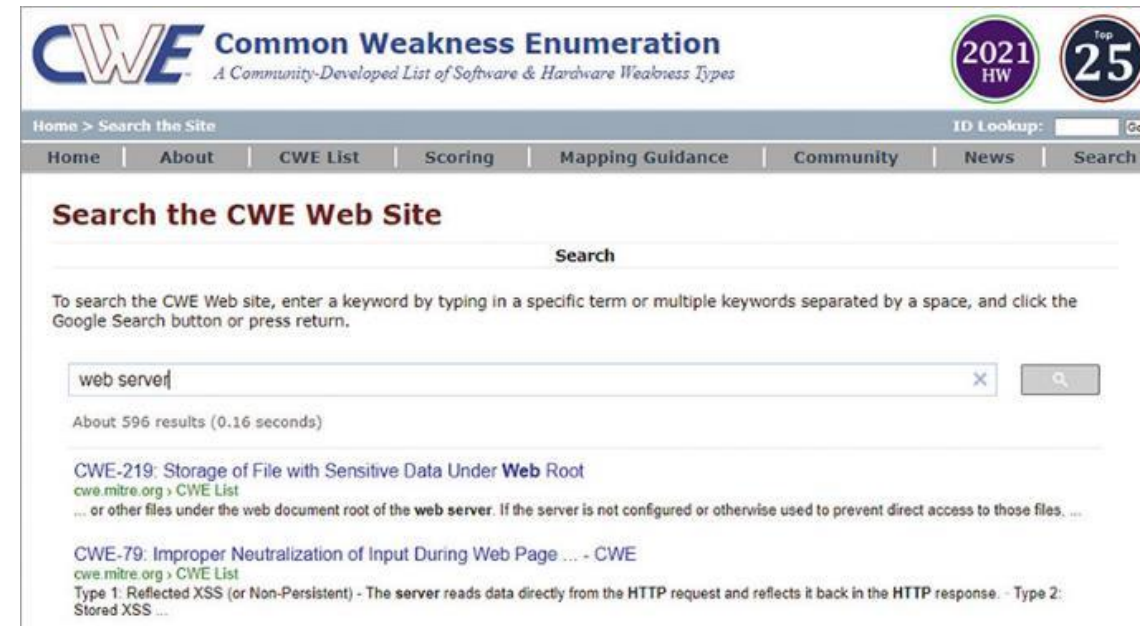
CVE search for Apache vulnerabilities

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

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

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?

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 | – Services | – Vulnerabilities |
| – Ports | – Data files | – Networks |

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

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

Active Reconnaissance Techniques (4 of 17)

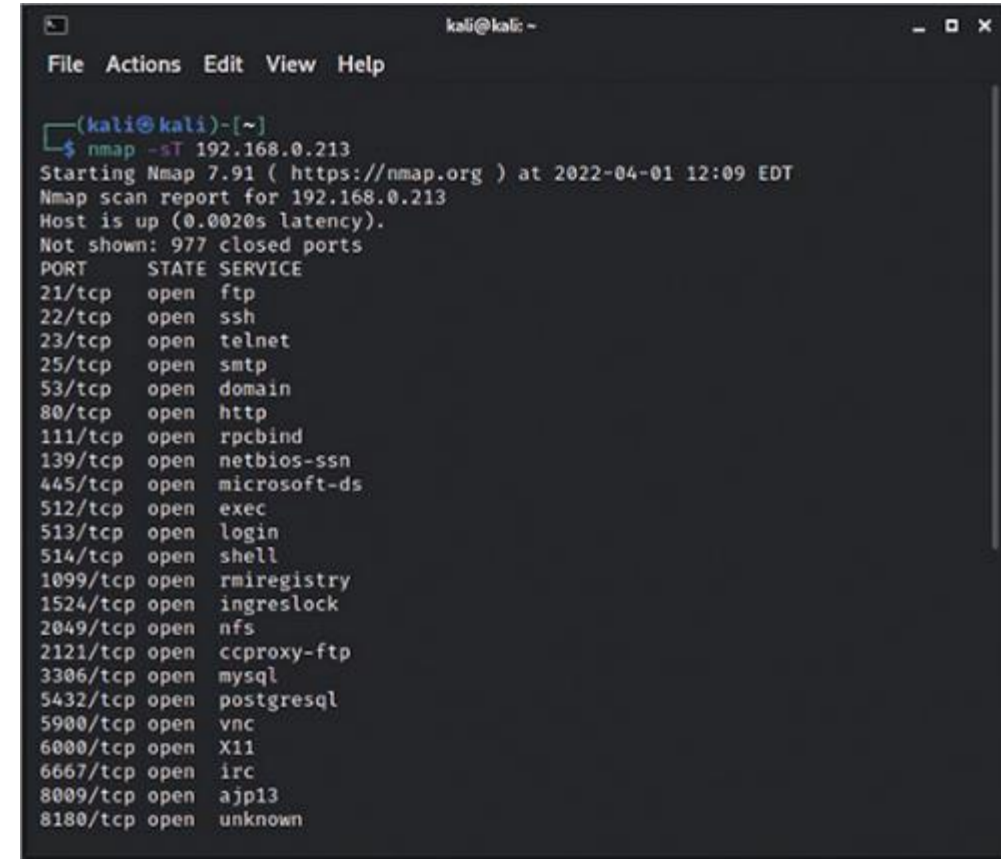
Enumeration - Hosts

- 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

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

A terminal window titled 'kali@kali' showing the output of an Nmap scan. The command executed is 'nmap -sT 192.168.0.213'. The output indicates the host is up and lists 20 open TCP ports with their corresponding services. The services listed include ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn, microsoft-ds, exec, login, shell, rmiregistry, ingreslock, nfs, ccproxy-ftp, mysql, postgresql, vnc, X11, irc, and ajp13.

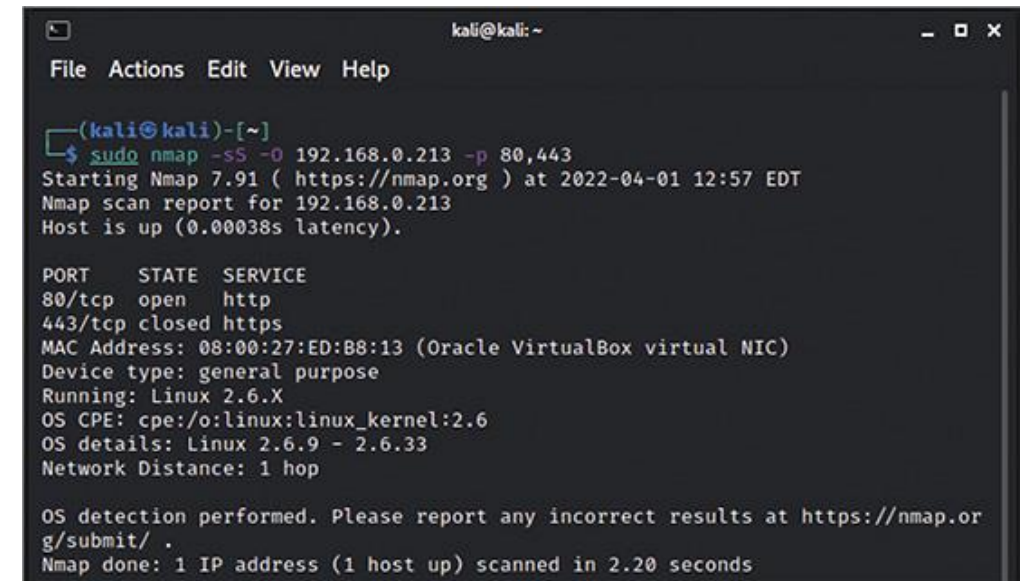
```
(kali@kali)-[~]
$ nmap -sT 192.168.0.213
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-01 12:09 EDT
Nmap scan report for 192.168.0.213
Host is up (0.0020s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
```

Scanning for open ports with Nmap

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



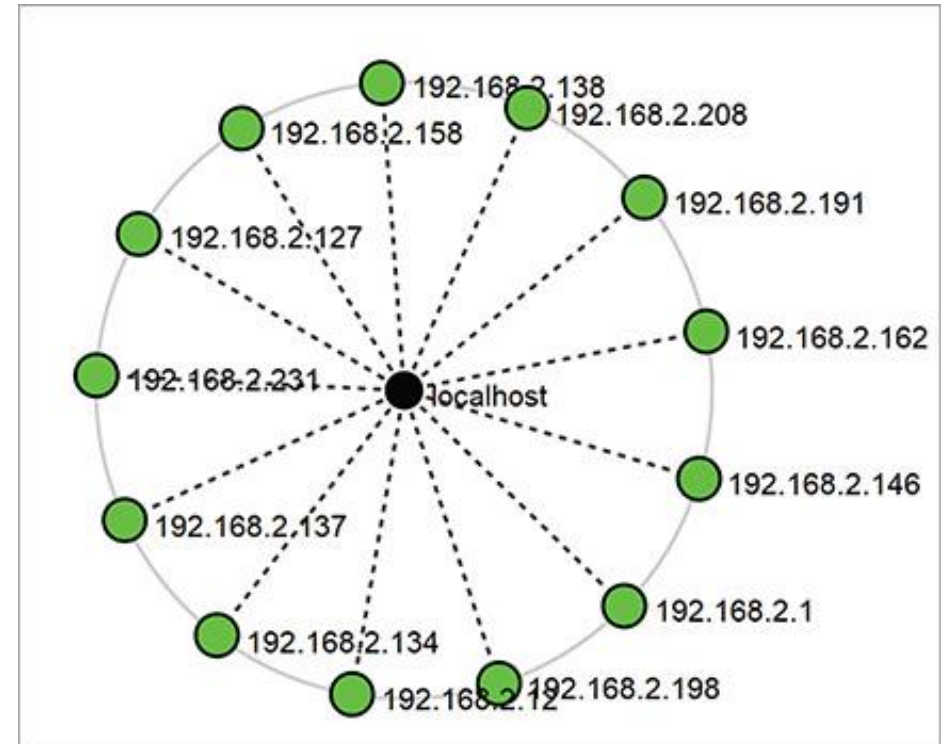
```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -sS -O 192.168.0.213 -p 80,443  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-01 12:57 EDT  
Nmap scan report for 192.168.0.213  
Host is up (0.00038s latency).  
  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp    closed https  
MAC Address: 08:00:27:ED:B8:13 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

Nmap scan for operating system

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

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

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



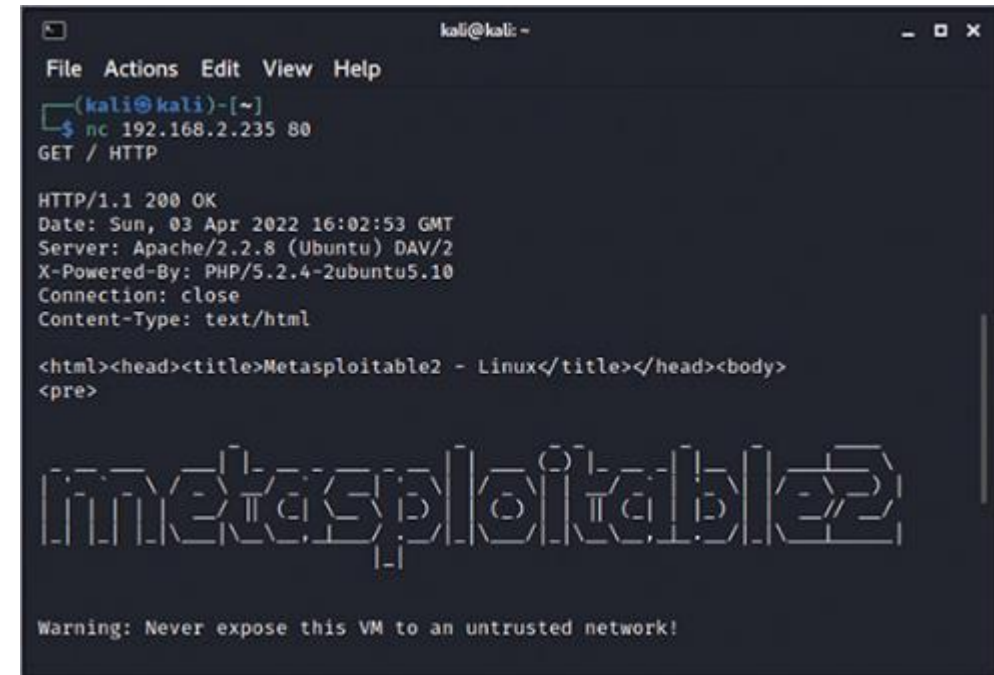
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ theHarvester -d cbc.ca -l 200 -b google  
  
*****  
* theHarvester *  
* Coded by Christian Martorella *  
* Edge-Security Research *  
* cmartorella@edge-security.com *  
*****  
  
[*] Target: cbc.ca  
    Searching 0 results.  
    Searching 100 results.  
    Searching 200 results.  
[*] Searching Google.  
  
[*] No IPs found.  
  
[*] Emails found: 1  
_____  
cbc.colocation@cbc.ca  
  
[*] Hosts found: 5  
_____  
cbchelp.cbc.ca:104.16.51.111, 104.16.53.111  
i.cbc.ca:23.201.192.189  
www.cbc.ca:23.201.192.189  
x22www.cbc.ca  
x3enwww.cbc.ca
```

theHarvester searching for email

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



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc 192.168.2.235 80  
GET / HTTP  
  
HTTP/1.1 200 OK  
Date: Sun, 03 Apr 2022 16:02:53 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Connection: close  
Content-Type: text/html  
  
<html><head><title>Metasploitable2 - Linux</title></head><body>  
<pre>  
  
metasploitable2  
  
</pre>  
</body></html>  
  
Warning: Never expose this VM to an untrusted network!
```

Netcat (nc) banner grab

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

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

The screenshot displays a Wireshark network traffic analysis. The top section lists several packets, with packet number 1008 highlighted in red. This packet is an HTTP POST request from source IP 10.0.2.15 to destination IP 10.0.20.99. The details pane below the packet list provides further information:

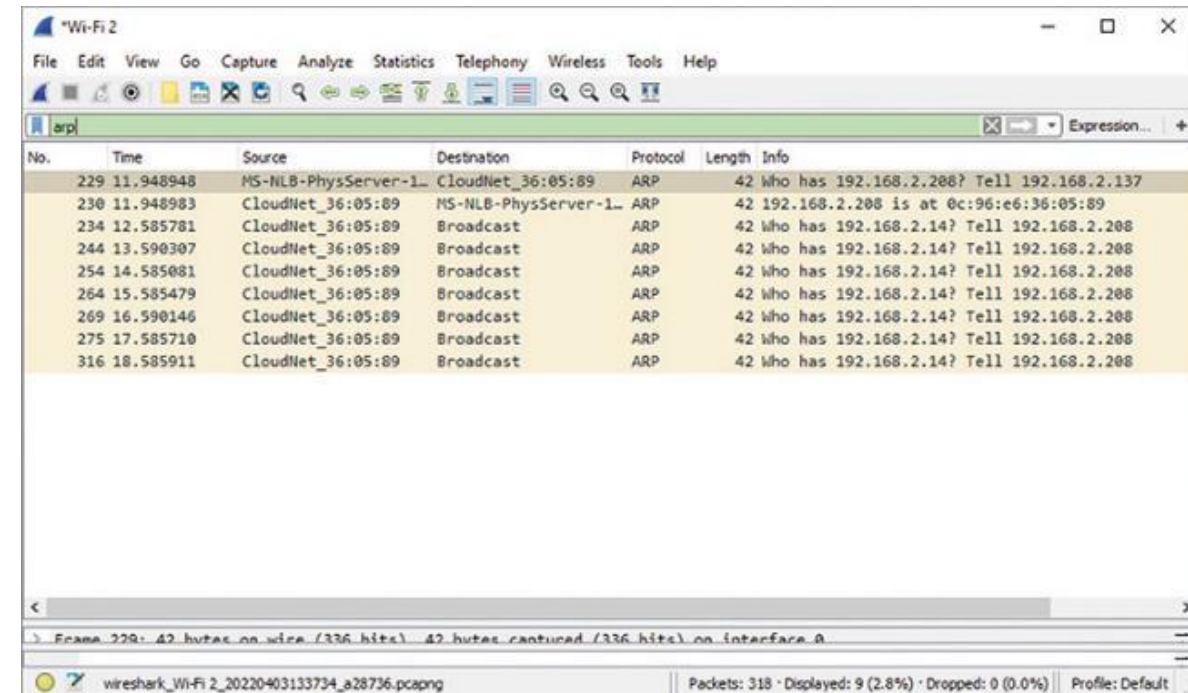
- Frame 1008:** 1137 bytes on wire (9096 bits), 1137 bytes captured (9096 bits) on interface 0
- Ethernet II, Linux cooked capture**
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.20.99**
- Transmission Control Protocol, Src Port: 59488, Dst Port: 80, Seq: 1, Ack: 1, Len: 1081**
- Hypertext Transfer Protocol**
- JavaScript Object Notation: application/json**
 - Object**
 - Member Key: email**
 - String value: test5@test.com
 - Key: email
 - Member Key: password**
 - String value: password@123
 - Key: password

Wireshark intercepting unencrypted password

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



The image shows a Wireshark packet capture window titled "Wi-Fi 2". The packet list on the left shows several ARP packets. The selected packet (No. 229) is expanded, showing the "Info" field with the text: "42 Who has 192.168.2.208? Tell 192.168.2.137". The packet details pane on the right shows the "Frame 229: 42 bytes on wire (336 bits) 42 bytes captured (336 bits) on interface 0". The status bar at the bottom indicates "Packets: 318 · Displayed: 9 (2.8%) · Dropped: 0 (0.0%) Profile: Default".

No.	Time	Source	Destination	Protocol	Length	Info
229	11.948948	MS-NLB-PhysServer-1	CloudNet_36:05:89	ARP	42	Who has 192.168.2.208? Tell 192.168.2.137
230	11.948983	CloudNet_36:05:89	MS-NLB-PhysServer-1	ARP	42	192.168.2.208 is at 0c:96:e6:36:05:89
234	12.585781	CloudNet_36:05:89	Broadcast	ARP	42	Who has 192.168.2.14? Tell 192.168.2.208
244	13.590307	CloudNet_36:05:89	Broadcast	ARP	42	Who has 192.168.2.14? Tell 192.168.2.208
254	14.585081	CloudNet_36:05:89	Broadcast	ARP	42	Who has 192.168.2.14? Tell 192.168.2.208
264	15.585479	CloudNet_36:05:89	Broadcast	ARP	42	Who has 192.168.2.14? Tell 192.168.2.208
269	16.590146	CloudNet_36:05:89	Broadcast	ARP	42	Who has 192.168.2.14? Tell 192.168.2.208
275	17.585710	CloudNet_36:05:89	Broadcast	ARP	42	Who has 192.168.2.14? Tell 192.168.2.208
316	18.585911	CloudNet_36:05:89	Broadcast	ARP	42	Who has 192.168.2.14? Tell 192.168.2.208

Wireshark intercepting unencrypted password

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

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

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

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

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.

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