

The background of the slide features a complex network of glowing blue nodes connected by thin lines, creating a web-like pattern that suggests data connectivity and analysis.

BIA

BOSTON
INSTITUTE OF
ANALYTICS

®

Create a Report on tools and methods that are used for Reconnaissance (Information Gathering).

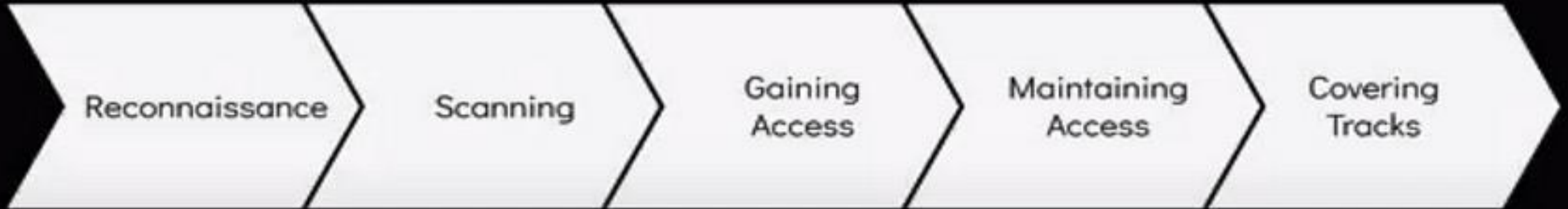
Project By :Varun Sharma

Agenda

- A. Reconnaissance in [cybersecurity](#) refers to the preliminary phase of an attack where an attacker gathers information about a target system or network to identify vulnerabilities and plan a potential breach
- B. The goal of recon is to gather as much information about the target as you can. More the information, more beneficial it will be for further phases of pen testing.
- C. Most of new learners underestimates this phase and ignore it but recon is most important phase of pen testing.
- D. This phase involves collecting data on **network architecture, system configurations, IP addresses, and domain names**, as well as understanding the target's security measures and personnel.
- E. Techniques used in reconnaissance include **scanning for open ports, analyzing network traffic**, and searching for publicly available information on social media or company websites.

This Phase explains the 5 steps of Hacking taking an example of a Hacker trying to hack a company's server and gaining access to all the data.

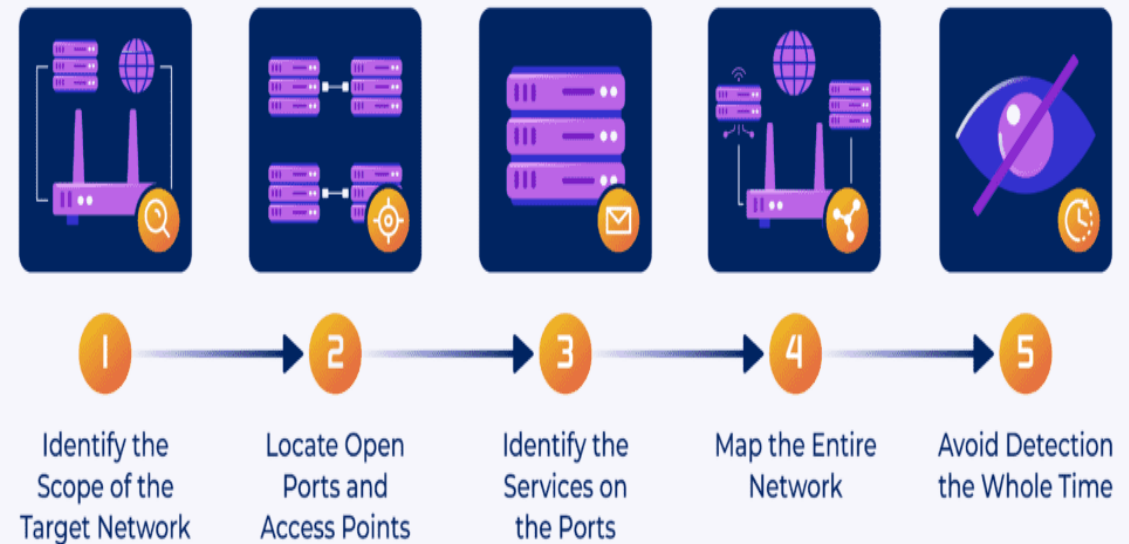
5 phases of Hacking



Reconnaissance

- ❑ Reconnaissance, mainly referred to as "recon" or "exploration", refers to gathering information about an adversary before engaging with it as your potential target.
- ❑ It is a crucial step in acquiring in-depth insights essential for preparing strategies, whether for enhancing network security or successfully competing in corporate initiatives.
- ❑ To perform reconnaissance before carrying out an attack, hackers must determine how far the target network extends and collect data like open network ports, services running on the ports, and an overall map of the network.
- ❑ At the same time, the hackers also try to stay unnoticed during the entire reconnaissance process

How Hackers Perform Reconnaissance



eSecurity Planet

CONFIDENTIAL: The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

Types of Reconnaissance Techniques

- To successfully launch an attack, threat actors need plenty of information beforehand so they don't go in blind and avoid detection as long as possible.
- Popular reconnaissance techniques include collecting data, performing social engineering experiments, scanning network ports, and fingerprinting operating system activities.

❑ Data Aggregation

Data aggregation is a broad term that encompasses all the methods a hacker gathers information about businesses, networks, computers, users, and physical premises. Common methods of aggregating data include:

1. **Studying the company website:** One of the easiest methods of gathering data is exploring a company's main web page and even public-facing documentation.
2. **Conducting employee research:** LinkedIn profiles reveal data about business operations and org charts, including employee contact information.
3. **Exploring physical premises:** Sometimes hackers will snoop around office buildings or data centers to find weak spots or observe traffic.
4. **Studying open-source intelligence:** Open-source feeds are useful for security, but they're also a tool for attackers to study existing vulnerabilities.

❑ Social Engineering

Often, the process of social engineering is a form of reconnaissance because it involves gathering information like email addresses to target and learning details about an organization's operations. Examples of social engineering include:

1. **Phishing:** Victims receive emails or phone calls with requests for money or login credentials or receive malicious links that they're urged to click.
2. **Smishing:** A form of phishing sent through SMS or text, smishing is designed to trick users into making rapid decisions on their phones.

❑ Port Scanning

When hackers explore a network to gauge its security controls, they'll often scan the network ports by sending data packets to the port and seeing what happens.

Sometimes, they'll find that the packet makes it through to the destination, but sometimes the preconfigured firewall rules will block the traffic. By performing a port scan, hackers can observe:

1. **Any existing firewalls:** This tells them whether they'll have to bypass an initial firewall.
2. **Potential network users:** Attackers might be able to determine which users are in charge of a particular network service.
3. **Current port statuses:** They'll want to know whether each port is open or closed to traffic or if it's filtering and blocking traffic.

❑ OS Fingerprinting

Hackers use operating system fingerprinting by reading packets that come from the computer system and trying to determine the OS's security policies and vulnerabilities from that. While not always a reliable method of determining the system's current status, it can be useful for observing.(TOS-type of service, DF-data fragment)

1. **Any system weaknesses:** In some cases, data packets can reveal places where an attacker could stage a successful breach.
2. **Potential network security policies:** If attackers observe certain packets being permitted but don't see others, they might guess that certain policies are in effect.
3. **Typical traffic patterns:** Hackers may be able to tell when the computer system receives more traffic and when it's more dormant.

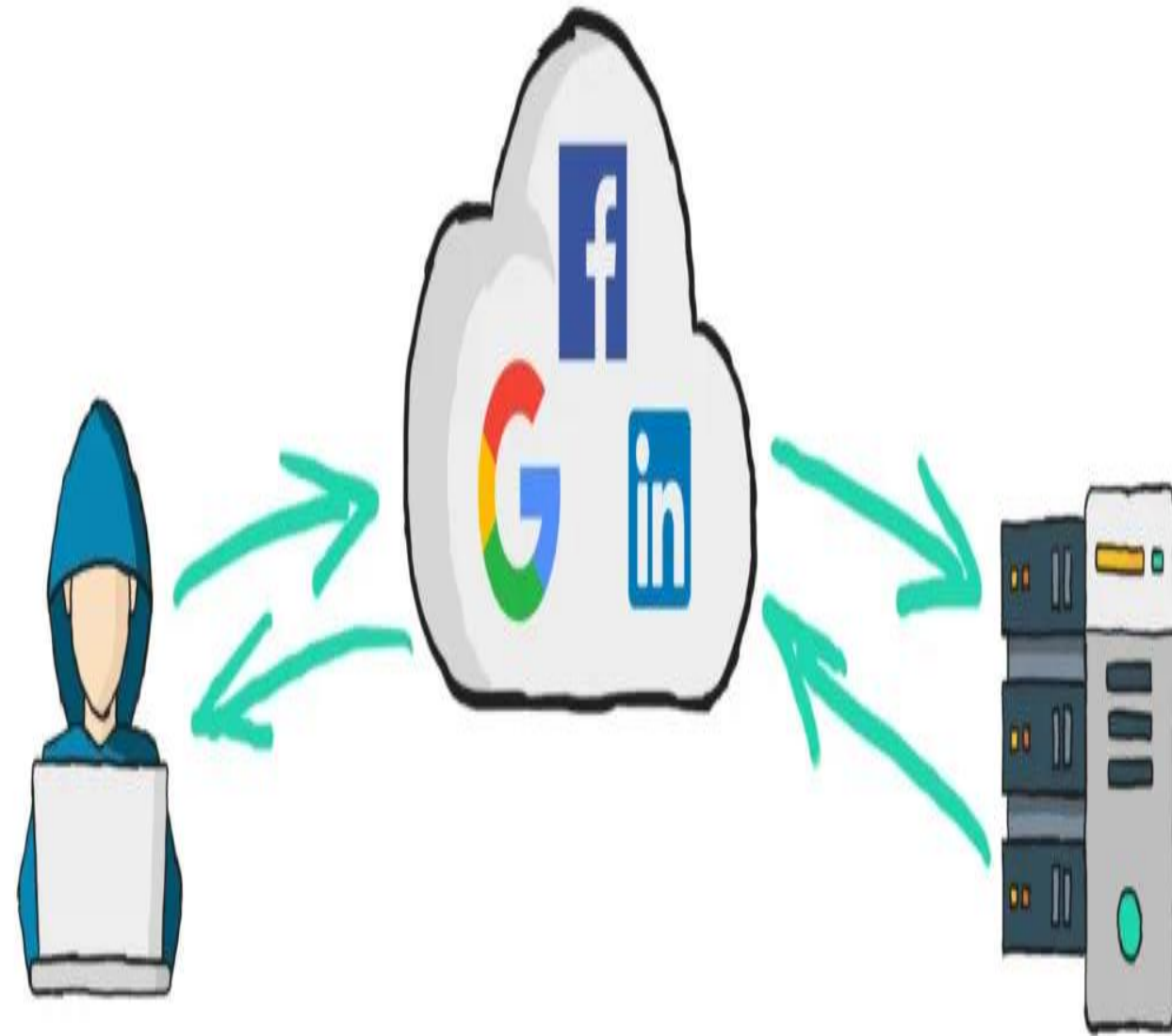
Active Reconnaissance

- ❑ Here, the attacker directly connects or interacts with the target and tries to get some information by engaging with it. They might opt for social engineering (making a call and asking for some information while pretending to be someone else or using other social engineering techniques).
- ❑ The attacker here exposes themselves to the target; it is an intrusive approach.
- ❑ A perfect and famous example of active reconnaissance is the
 - ❑ “**watering hole attack**”. In this technique, as the name suggests, the attacker will infect the websites that the targets would like to use by profiling their interests
 - ❑ when they visit those sites, the attacker will gain access to their systems through the loopholes they created.
- ❑ It's just like an animal who wants to attack its prey, so instead of chasing them, they know the prey will come to the water hole to drink water. So, when they visit the watering hole, the animal will take over its prey.



Passive Reconnaissance

- ❑ Passive reconnaissance involves collecting information about a target without directly interacting with its systems, making it a non-intrusive approach that Minimise the risk of detection.
- ❑ In this technique, attackers gather data available through public sources or intercept traffic without alerting the target to their presence.(WHOIS)
- ❑ For instance, an attacker might monitor social media posts or public databases to gather information about an organization's employees, systems, or operational details without making direct contact or triggering security systems.

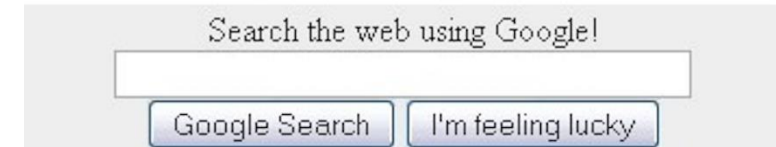


Reconnaissance tools:

- WIRESHARK
- SEARCHENGINE(GOOGLE).
- FINDSUBDOMAIN.COM
- OSINT.
- SHODAN
- NMAP
- NESSUS
- OPENVAS
- NIKTO
- METASPLOIT



Metasploit



CONFIDENTIAL: The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

TOP PASSIVE RECON TOOLS

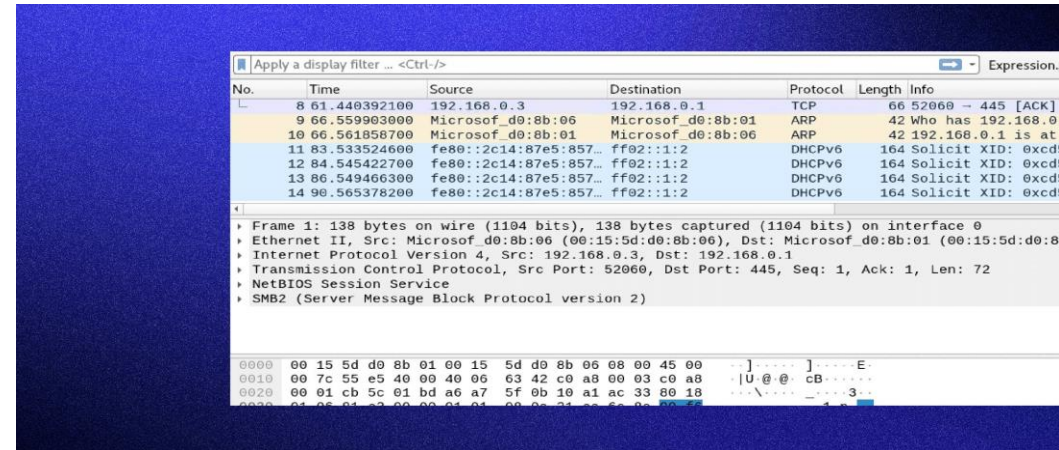
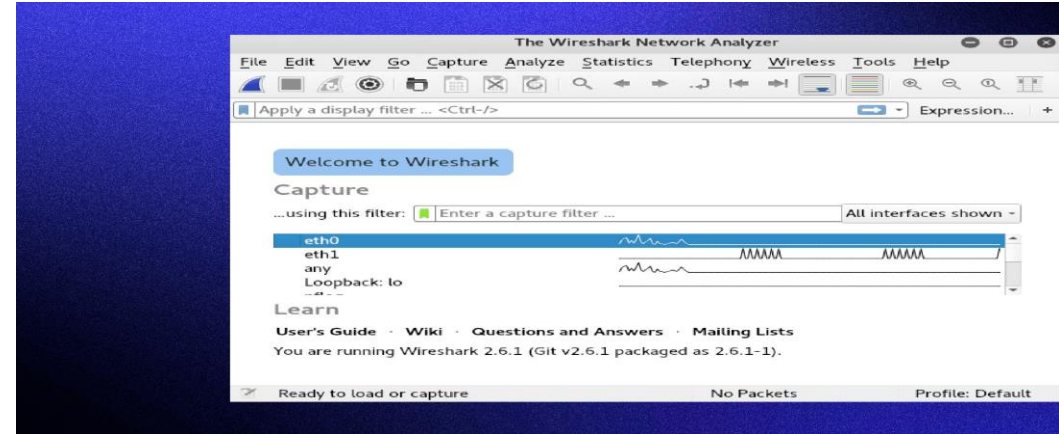
In passive reconnaissance, the hacker never interacts directly with the target's network.

The tools used for passive reconnaissance take advantage of unintentional data leaks from an organization to provide the hacker with insight into the internals of the organization's network.

- 1. Wireshark.**
- 2. SearchEngine(google).**
- 3. findsubdomain.com**
- 4. OSINT.**
- 5. Shodan**

Wireshark

- ❑ Wireshark is best known as a network traffic analysis tool, but it can also be invaluable for passive network reconnaissance.
- ❑ If an attacker can gain access to an organization's Wi-Fi network or otherwise eavesdrop on the network traffic of an employee (e.g., by eavesdropping on traffic in a coffee shop), analyzing it in Wireshark can provide a great deal of useful intelligence about the target network.
- ❑ By passively eavesdropping on traffic, a hacker may be able to map IP addresses of computers within the organization's network and determine their purposes based on the traffic flowing to and from them.
- ❑ Captured traffic may also include version information of servers, allowing a hacker to identify potentially vulnerable software that can be exploited.



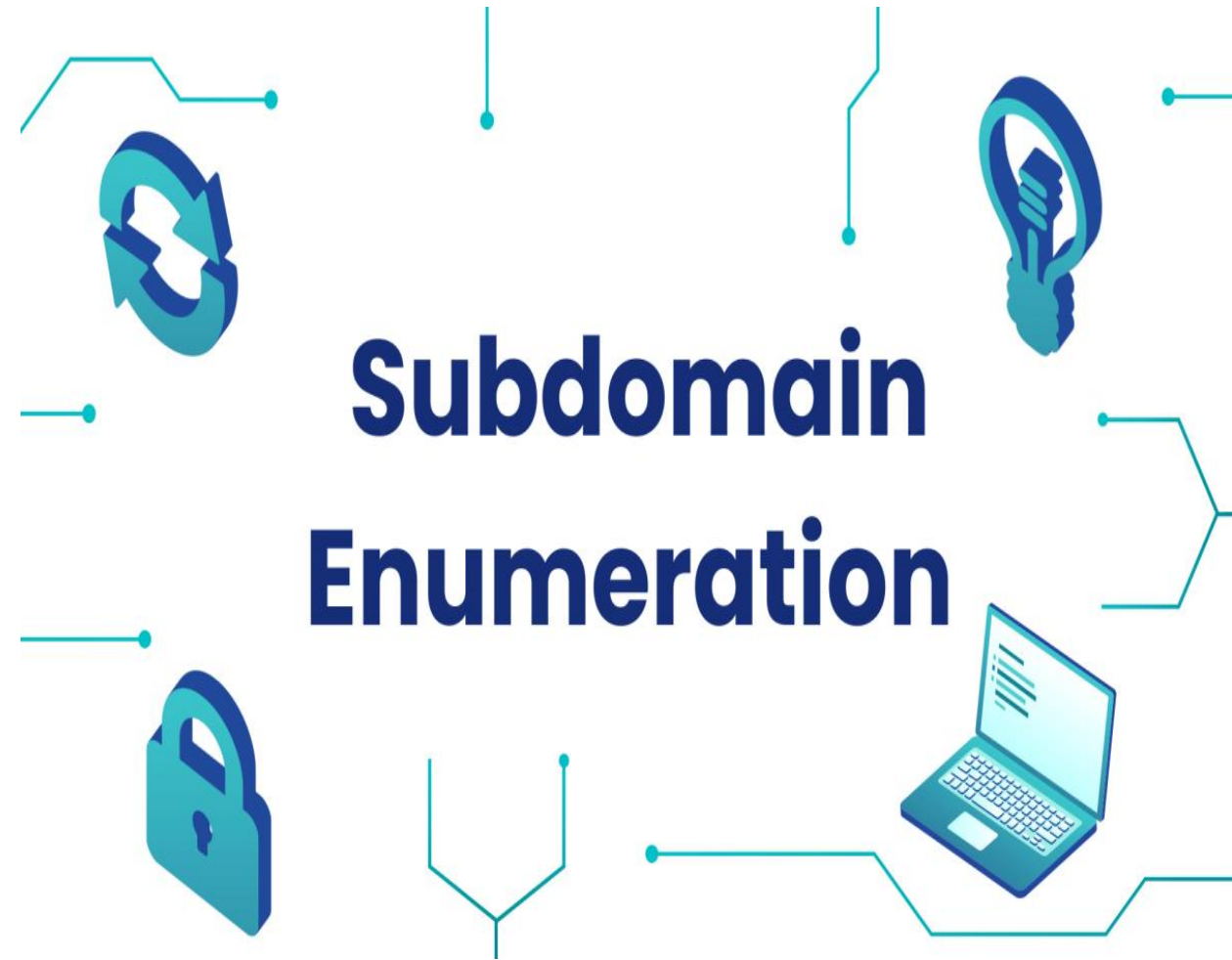
Search-Engine(Google)

- ❑ Google. Google can provide a vast amount of information on a variety of different topics. One potential application of Google is for performing passive reconnaissance about a target. The information that an organization posts online can provide a massive amount of information about their network(footprinting).
- ❑ The information that an organization posts online can provide a massive amount of information about their network.
- ❑ The organization's website, especially its career page, can provide details of the types of systems used in the network. By using specialized Google queries (Google Dorking), it's also possible to search for files that were not intentionally exposed to the internet but still publicly available as well.
- ❑ Sometimes a misconfiguration web server might show in directory.
 - ❑ This would show all the files within a directory.
 - ❑ Include HTML, CSS, PHP.



Findsubdomain

- FindSubDomains.com is one example of a variety of different websites designed to help identify websites that belong to an organization.
- While many of these sites may be deliberately intended for public consumption and others may be protected by login pages, the possibility exists that some are unintentionally exposed to the internet.
- Subdomains can be found using passive reconnaissance tools like **NETCRAFT** **SUBFINDER**. These tools use passive DNS to find subdomains.



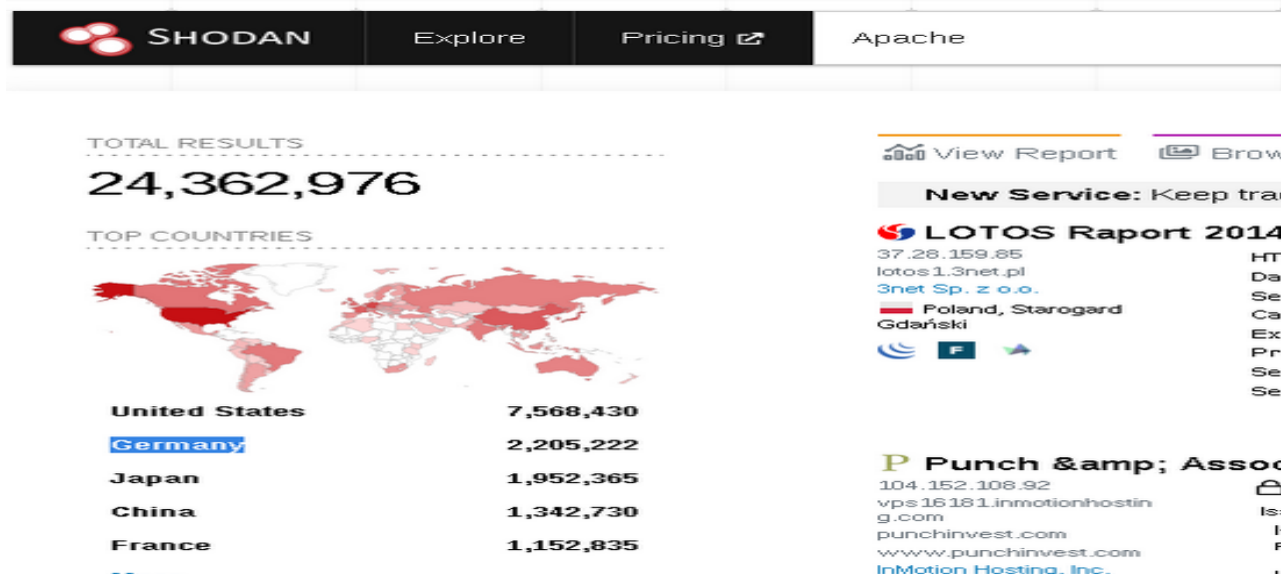
OSINT

- ❑ OSINT (Open Source Intelligence) assists in acquiring data from openly accessible sources. As the name implies, open source platforms including websites, publications, blogs, social media, public records, etc. are used for reconnaissance. Considering how crucial reconnaissance is, OSINT plays a vital role. It is commonly known that hackers dedicate approximately 50 to 60 percent of their time and effort into this phase.
- ❑ OSINT helps in gathering, analysing, and applying the data gathered from websites and open resources. It can be used for hacking purposes as well as general information gathering which is required in corporations. OSINT is used by various entities including security experts, defenders, national intelligence agencies, and cybercriminals as the primary users of this technique..
- ❑ Basically, OSINT involves three phases of information gathering: gathering, processing, and exploitation.
 - ❖ In the initial stage, various tools are employed to gather information about the target from sources like websites, subdomains, and publications. Once information is collected, it is analysed because there might be redundant information and false positives.
 - ❖ Processing is crucial, as the raw information collected might create confusion in the next phases. Additionally, the information is structured and understood by hackers.
 - ❖ Lastly, an exploit is carried out to predict the attacks and their effects on the system. This phase may also help in the examination of attack patterns and motives.



SHODAN

- Shodan.io is used to learn more about our target network. Shodan is like a search engine for devices online, and just because we are not directly connecting to the devices, it will give us a lot of information during the passive research. (network connected devices like server, router)



[View Report](#) [View on Map](#)

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

301 Moved Permanently

54.220.229.192
ec2-54-220-229-192.eu-west-1.compute.amazonaws.com
Amazon.com, Inc.
Ireland, Dublin

cloud

HTTP/1.1 301 Moved Permanently
Server: nginx/1.14.0 (Ubuntu)
Date: Tue, 05 Apr 2022 07:32:52 GMT
Content-Type: text/html
Content-Length: 194
Connection: keep-alive
Location: https://54.220.229.192/
X-Frame-Options: ALLOW-FROM https://tryhackme.com

CONFIDENTIAL: The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

TOP ACTIVE RECON TOOLS

- Tools for active reconnaissance are designed to interact directly with machines on the target network in order to collect data that may not be available by other means.
 - Active reconnaissance can provide a hacker with much more detailed information about the target but also runs the risk of detection.
1. NMAP
 2. Nessus
 3. OpenVAS
 4. Nikto
 5. Metasploit

NMAP (Network Mapping)

- ❑ **Nmap is a network scanner utility used for port mapping, host discovery and vulnerability scanning.** Most of its functions are based on using IP packet analysis to detect and identify remote hosts, operating systems and services.
- ❑ Nmap is used by mid and large companies as well as smaller-sized organizations for semi-automated and manual port auditing, host monitoring, penetration testing, [red and blue team](#) exercises, and similar tasks.
- ❑ Even with Nmap constantly being updated with new features for decades, **its core function remains as a network scanner**, helping users gather data by sending packets to local or remote ports. This is done by waiting for packet responses to **determine if ports are closed, open or filtered.**
- ❑ The most popular method of using Nmap is via the terminal (command-line console), by performing a Nmap full scan command
- ❑ The describe link will demonstrate commands used in nmap.
<https://github.com/jasonniebauer/Nmap-Cheatsheet/>

Basic Scanning Techniques

Scan a single target	nmap [target]
• Scan multiple targets	nmap [target1,target2,etc]
• Scan a list of targets	nmap -iL [list.txt]
• Scan a range of hosts	nmap [range of IP addresses]
• Scan an entire subnet	nmap [IP address/cdir]
• Scan random hosts	nmap -iR [number]
• Excluding targets from a scan	nmap [targets] --exclude [targets]
• Excluding targets using a list	nmap [targets] --excludefile [list.txt]
• Perform an aggressive scan	nmap -A [target]
• Scan an IPv6 target	map -6 [target]

Nessus

- ❑ [Nessus](#) is a commercial vulnerability scanner.
- ❑ Its purpose is to identify vulnerable applications running on a system and provides a variety of details about potentially exploitable vulnerabilities.
- ❑ Nessus is a paid product, but the comprehensive information that it provides can make it a worthwhile investment for a hacker.

How Nessus is used in active reconnaissance

❑ Identifying live hosts

Nessus can identify live hosts, which narrows down potential targets.

❑ Discovering open ports

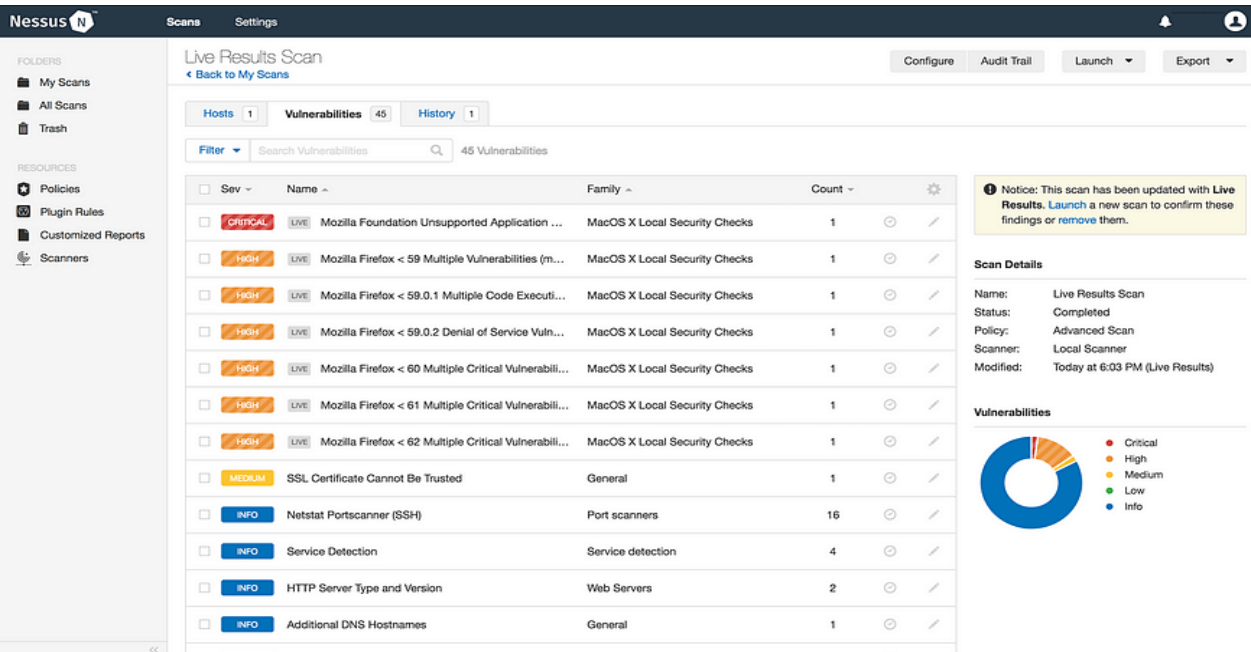
Nessus can identify open ports, which can be potential entry points for attackers.

❑ Scanning entire networks

Nessus can scan entire networks to provide an understanding of the target environment.

❑ Identifying vulnerabilities

Nessus can identify weaknesses in the target's software and configurations.

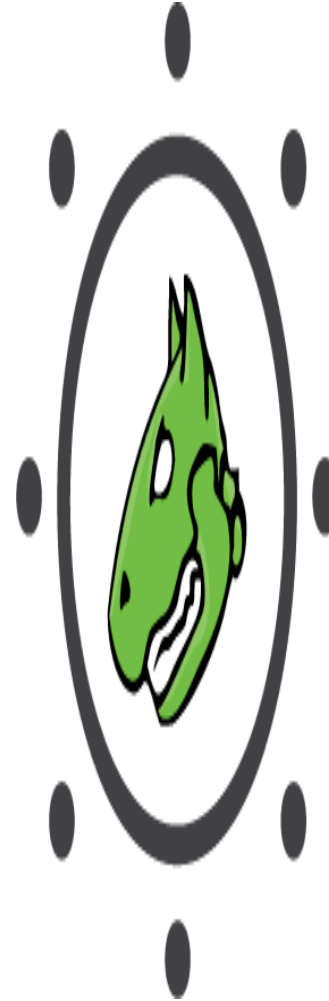


CONFIDENTIAL: The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

OpenVAS

- [OpenVAS](#) is a vulnerability scanner that was developed in response to the commercialization of Nessus.
- The Nessus vulnerability scanner was previously open-source, and, when it became closed-source, OpenVAS was created off of the last open-source version to continue to provide a free alternative.
- As a result, it provides a lot of the same functionality as Nessus but may lack some of the features developed since Nessus was commercialized.
- The describe link will demonstrate extracting information OpenVAS

<https://hackertarget.com/openvas-tutorial-tips/>



OpenVAS

Open Vulnerability Assessment Scanner

Nikto

- ❑ Nikto is a web server vulnerability scanner that can be used for reconnaissance in a manner similar to Nessus and OpenVAS.
- ❑ It can detect a variety of different vulnerabilities but is also not a stealthy scanner.
- ❑ Scanning with Nikto can be effective but is easily detectable by an intrusion detection or prevention system (like most active reconnaissance tools)
- ❑ Nikto is a free command line web server scanner that identifies vulnerabilities on web servers.
- ❑ This includes dangerous files, outdated server software, and other common problems.
- ❑ You can get the source code for Nikto from its

<https://github.com/sullo/nikto/>

The screenshot shows the output of a Nikto v2.1.5 scan. The scanner source IP is 66.175.214.247. The target IP is 65.x.x.x, target hostname is example.com, and target port is 80. The scan started on 2019-02-01 at 12:17:06 GMT. The output lists various findings, including uncommon headers, server information, and a list of allowed HTTP methods. Three annotations are present: 1. A box at the top right states 'Nikto detects security related issues in web scripts and web server configuration'. 2. A box at the bottom right states 'Unusual items are always worth investigating' with an arrow pointing to the 'Cookie PHPSESSID created without the httponly flag' finding. 3. A box at the bottom left states 'Ran 5567 tests and found 14 items of interest' with an arrow pointing to the '5567 items checked: 0 error(s) and 14 item(s) reported on remote host' line.

```
Scanner Source IP: 66.175.214.247
1 Scanner Source IP: 66.175.214.247
2 User Agent: Nikto 2.1.5
3
4 - Nikto v2.1.5
5 -----
6 + Target IP: 65.x.x.x
7 + Target Hostname: example.com
8 + Target Port: 80
9 + Start Time: 2019-02-01 12:17:06 (GMT0)
10 -----
11 + Server: Microsoft-IIS/8.5
12 + Retrieved x-powered-by header: ASP.NET
13 + Uncommon header 'x-content-security-policy' found, with contents: default-src 'self' ;
14 + Uncommon header 'content-security-policy' found, with contents: default-src 'self' 'unsafe-inline' example.com maxcdn.bootstrapcdn.com;
15 + Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN example.com
16 + Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
17 + Retrieved x-aspnet-version header: 4.0.1219
18 + Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x4e234235aed08bddd:0
19 + robots.txt contains 2 entries which should be manually viewed.
20 + RFC-1918 IP address found in the 'location' header. The IP is 10.23.1.3.
21 + OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory.
22 + Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
23 + Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
24 + Cookie PHPSESSID created without the httponly flag
25 + /login.php: Admin login page/section found.
26 + 5567 items checked: 0 error(s) and 14 item(s) reported on remote host
27 + End Time: 2019-02-01
```

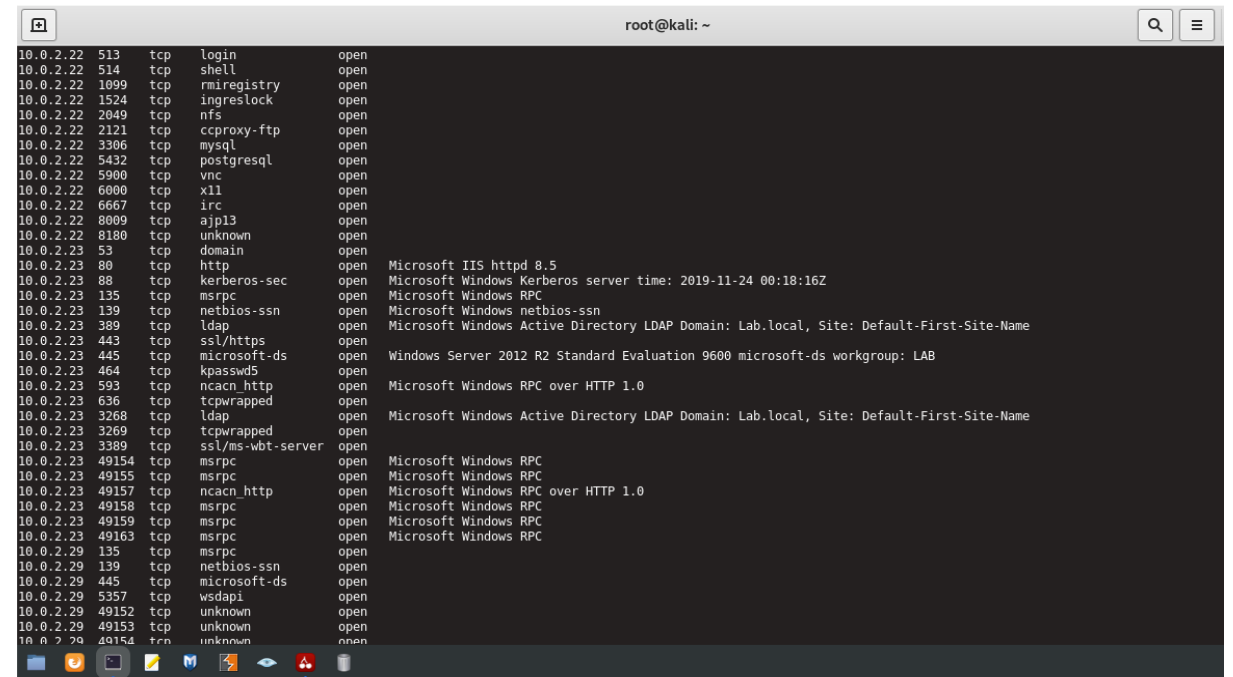
Metasploit

- ❑ [Metasploit](#) is primarily designed as an exploitation toolkit. It contains a variety of different modules that have prepackaged exploits for a number of vulnerabilities. With Metasploit, even a novice hacker has the potential to break into a wide range of vulnerable machines.
- ❑ Although it was designed as an exploit toolkit, Metasploit can also be effectively used for reconnaissance. At the minimum, using the autopawn option on Metasploit allows a hacker to try to exploit a target using any means necessary.
- ❑ A tool for penetration testing is Metasploit. White hat hackers also use it to create intrusion detection and prevention systems (IDSs/IPSSs), despite the fact that many threat actors use it to carry out attacks.
- ❑ Users can write, test, and run exploit codes that enable them to conduct targeted analyses of security vulnerabilities because it is based on Ruby.
- ❑ The describe link will demonstrate extracting information using Metasploit Framework.

<https://github.com/Samsar4/Ethical-Hacking-Labs/blob/master/1-Footprinting-and-Reconnaissance/5-Metasploit-Basics.md/>

How does Metasploit work for active reconnaissance?

- ❑ Metasploit is a framework that can be used to develop and execute exploit code against a remote target machine.
- ❑ It contains a variety of different modules that have prepackaged exploits for a number of vulnerabilities.
- ❑ Metasploit can be used to perform more targeted analysis to perform reconnaissance with more subtlety.



```
root@kali: ~  
10.0.2.22 513 tcp login open  
10.0.2.22 514 tcp shell open  
10.0.2.22 1099 tcp rmiregistry open  
10.0.2.22 1524 tcp ingreslock open  
10.0.2.22 2049 tcp nfs open  
10.0.2.22 2121 tcp ccproxy-ftp open  
10.0.2.22 3306 tcp mysql open  
10.0.2.22 5432 tcp postgresql open  
10.0.2.22 5900 tcp vnc open  
10.0.2.22 6000 tcp x11 open  
10.0.2.22 6667 tcp irc open  
10.0.2.22 8009 tcp ajp13 open  
10.0.2.22 8180 tcp unknown open  
10.0.2.23 53 tcp domain open  
10.0.2.23 80 tcp http open Microsoft IIS httpd 8.5  
10.0.2.23 88 tcp kerberos-sec open Microsoft Windows Kerberos server time: 2019-11-24 00:18:16Z  
10.0.2.23 135 tcp msrpc open Microsoft Windows RPC  
10.0.2.23 139 tcp netbios-ssn open Microsoft Windows netbios-ssn  
10.0.2.23 389 tcp ldap open Microsoft Windows Active Directory LDAP Domain: Lab.local, Site: Default-First-Site-Name  
10.0.2.23 443 tcp ssl/https open  
10.0.2.23 445 tcp microsoft-ds open Windows Server 2012 R2 Standard Evaluation 9600 microsoft-ds workgroup: LAB  
10.0.2.23 464 tcp kpasswds open  
10.0.2.23 593 tcp ncacn_http open Microsoft Windows RPC over HTTP 1.0  
10.0.2.23 636 tcp tcpwrapped open  
10.0.2.23 3268 tcp ldap open Microsoft Windows Active Directory LDAP Domain: Lab.local, Site: Default-First-Site-Name  
10.0.2.23 3269 tcp tcpwrapped open  
10.0.2.23 3389 tcp ssl/ms-wbt-server open  
10.0.2.23 49154 tcp msrpc open Microsoft Windows RPC  
10.0.2.23 49155 tcp msrpc open Microsoft Windows RPC  
10.0.2.23 49157 tcp ncacn_http open Microsoft Windows RPC over HTTP 1.0  
10.0.2.23 49158 tcp msrpc open Microsoft Windows RPC  
10.0.2.23 49159 tcp msrpc open Microsoft Windows RPC  
10.0.2.23 49163 tcp msrpc open Microsoft Windows RPC  
10.0.2.29 135 tcp msrpc open  
10.0.2.29 139 tcp netbios-ssn open  
10.0.2.29 445 tcp microsoft-ds open  
10.0.2.29 5357 tcp wsdaapi open  
10.0.2.29 49152 tcp unknown open  
10.0.2.29 49153 tcp unknown open  
10.0.2.29 49154 tcp unknown open
```

Reference

- <https://medium.com/>
- <https://www.geeksforgeeks.org/>
- <https://www.infosecinstitute.com/>
- <https://www.researchgate.net/>

Questions ?

CONFIDENTIAL: The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

The background is a dark blue gradient with a complex network of glowing blue lines and dots, resembling a molecular structure or a data network. The lines and dots are more concentrated in the lower half of the image, creating a sense of depth and connectivity.

Thank You!