Nmap – Scanning tool

About Nmap

Nmap is a robust, open-source tool that is frequently used for penetration testing, security audits and network discovery. It allows users to find running operating systems, firewalls, hosts and services on a network. Nmap uses a number of scanning methods, including FTP, TCP SYN (half-open), UDP and others, to give comprehensive information about network devices.

Process

Step 1: Enter IP Address or Hostname

- Provide the target IP address or hostname that you want to scan.

Example: 192.168.1.1

Step 2: Enter Port Number

- Specify the target port(s). Leave blank to scan all common ports.

Example: 22,80,443 or leave empty for default ports.

Step 3: Select Scan Speed

Select a scan timing template based on the requirements for stealth and network conditions:

- T0 – paranoid (Slowest speed, highly stealthy and quiet on the network)
- T1 – sneaky (Very slow scan, reduces chances of being detected)
- T2 – polite (Balanced speed, careful with network resources)
- T3 – normal (Standard speed, provides reliable and balanced results)
- T4 – aggressive (Faster scans, best for reliable and stable networks)
- T5 – insane (Extremely fast, needs a strong and stable network)

Example: T3

Step 4: Select Scan Type Choose the type of Nmap scan to perform, such as:

- Operating System (OS) Detection
- Service/Version Detection
- TCP SYN Scan
- UDP Scan
- Firewall Detection
- Comprehensive Scan

Example: Operating System

Step 5: Commence Scan

- Click Scan to initiate the operation. Example: 192.168.1.1

Step 6: View Results

- The output portion provides a clear display of the scan's results, which include open ports, service information, OS details, and probable vulnerabilities.

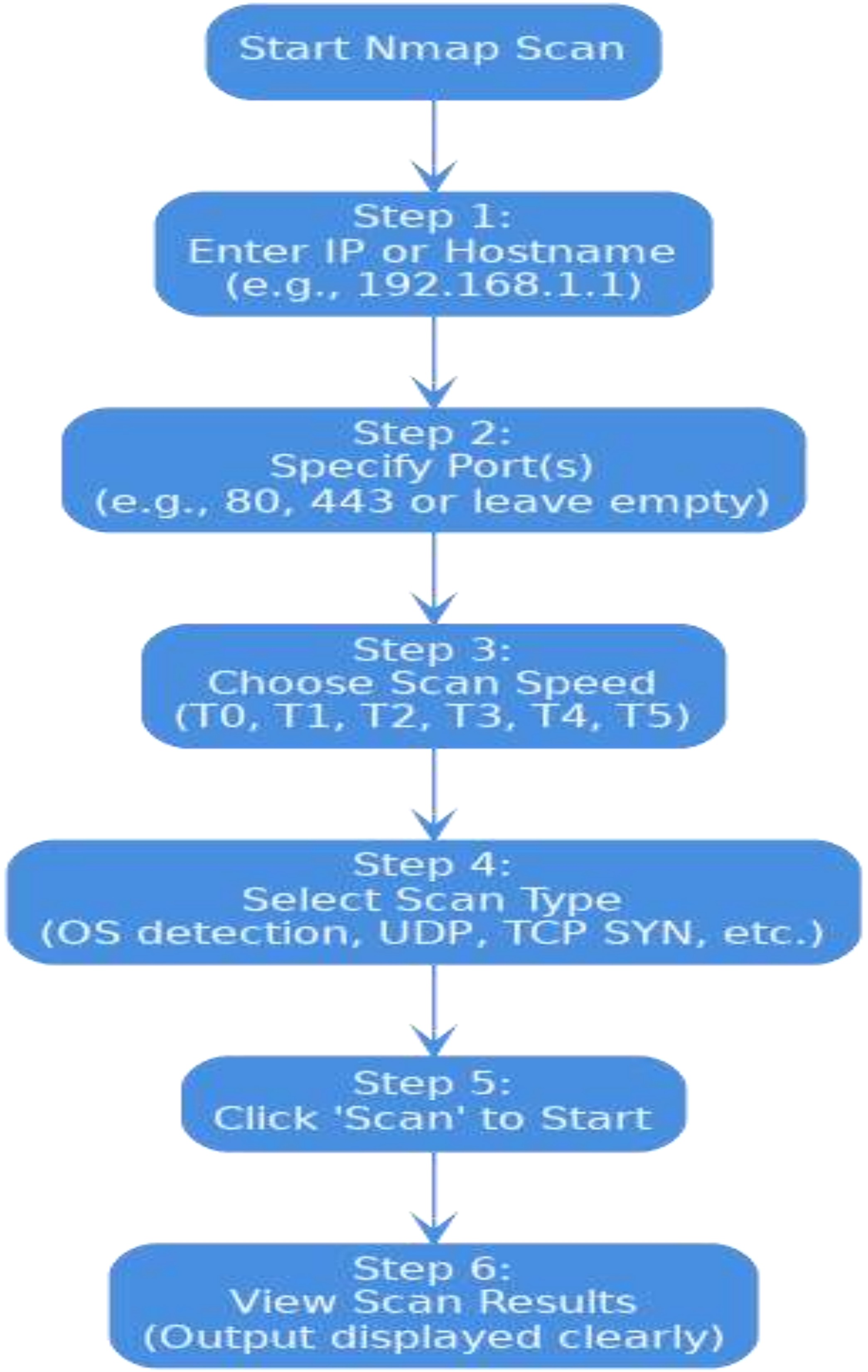
Let's look at an output example:

- nmap -T3 -O -p 22,80,443 192.168.1.1

Now lets breakdown the command-

- -T3: Normal speed
- -O: Operating System detection
- -p 22,80,443: Scanning ports 22 (SSH), 80 (HTTP) and 443 (HTTPS)
- 192.168.1.1: The IP address of the target host.

Flowchart



Start Nmap Scan

Step 1:
Enter IP or Hostname
(e.g., 192.168.1.1)

Step 2:
Specify Port(s)
(e.g., 80, 443 or leave empty)

Step 3:
Choose Scan Speed
(T0, T1, T2, T3, T4, T5)

Step 4:
Select Scan Type
(OS detection, UDP, TCP SYN, etc.)

Step 5:
Click 'Scan' to Start

Step 6:
View Scan Results
(Output displayed clearly)

Key Features

- **Host Discovery:**
Checks which devices are active on a network.

- **Port Scanning:**
Finds open or closed ports on a device and identifies the services running on those ports.

- **OS Detection:**
Identifies the operating system (e.g., Windows, Linux) on a target device.

- **Service Detection:**
Discovers specific services and their version numbers running on target systems.

- **Firewall and IDS Detection:**
Detects if a firewall or intrusion detection system (IDS) is protecting a network or device.

- **Scriptable Interaction (NSE):**
Allows advanced scanning and customization through scripts for specific scanning tasks.

Testing tutorial link- https://youtu.be/W0KRYkZppIw?si=faxiyQPjO8KUX-gU

Nikto

About Nikto:

Nikto is an open-source web server scanner utilized in penetration testing for finding vulnerabilities in websites and web applications. It scans for outdated software, malicious files, misconfigurations and other security issues that can be exploited by attackers.

Nikto is a fast and reliable way to test web servers for known problems, and it's especially good at identifying issues that are not obvious just by visiting the website.

Key Features

- **Vulnerability Detection:**
Scans for over 6000 known vulnerabilities like outdated software and insecure files.

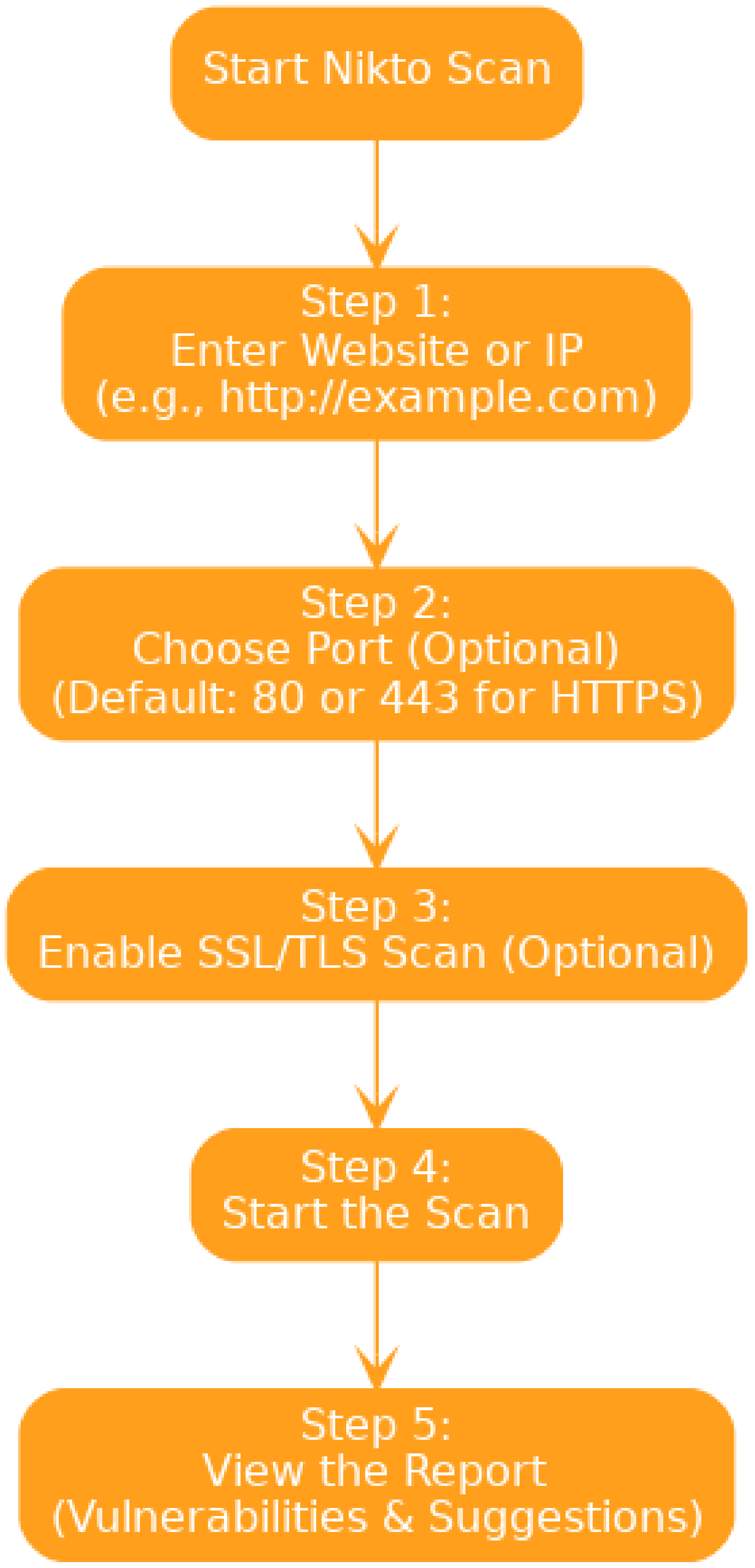
- **Checks Web Server Configs:**
Identifies misconfigurations that can lead to attacks.

- **SSL Testing:**
Can scan for weak SSL/TLS ciphers and certificate issues.

- **Custom Tests:**
Supports plugins and test customization for advanced scans.

- **Reporting Options:**
Exports results in plain text, HTML or CSV formats.

Flowchart



Start Nikto Scan

Step 1:
Enter Website or IP
(e.g., http://example.com)

Step 2:
Choose Port (Optional)
(Default: 80 or 443 for HTTPS)

Step 3:
Enable SSL/TLS Scan (Optional)

Step 4:
Start the Scan

Step 5:
View the Report
(Vulnerabilities & Suggestions)

Process

Step 1: Enter Target Website or IP

- Type in the web address or IP of the site you want to scan.

Example: http://xyz.com or 192.168.1.100

Step 2: Choose Port (Optional)

- Nikto will scan port 80 (HTTP) by default, but if needed you can specify an alternative port.

Example: 443 for HTTPS.

Step 3: Set SSL Option (Optional)

- If the site is accessed via HTTPS, you can use the SSL/TLS scan option to detect problems with it.

Step 4: Start the Scan

- Click Start to run the Nikto scan on the target. The tool will begin checking for known web vulnerabilities.

Testing tutorial link- https://youtu.be/0qZXewloIU0?si=XQCci_GxsMALY_gp

Step 5: View the Report

- After the scan, you will see a report with all discovered issues, including security risks and recommendations for fixing them.

Let's look at an example Command (Nikto CLI)::

-
  ```
  nikto -h http://192.168.1.100 -p 80
  ```

Now lets breakdown the command:-

- -h: Target host (website or IP)
- -p 80: Port number (80 is the default for HTTP)

If scanning HTTPS:

```
nikto -h https://192.168.1.100 -p 443
```

Tcpdump tool

About Tcpdump :

The main purpose of the powerful command line network analysis program tcpdump is to record, examine and troubleshooting network packets. By intercepting and showing packet contents as they pass through network interfaces, it offers insights into network traffic.

Process

Step 1: Select Network Interface
• Choose the network interface you wish to monitor.
Example: eth0, wlan0

Step 2: Enter Host/IP Address (Optional)
• Specify a specific host/IP to filter traffic.
Example: 192.168.1.5 (leave empty for all traffic)

Step 3: Specify Port (Optional)
• Filter traffic by port number.
Example: 80 (HTTP), 443 (HTTPS) (leave empty for all ports)

Step 4: Select Protocol (Optional)
• Choose a specific protocol to filter packets.
TCP, UDP, ICMP (or leave empty to capture all protocols)

Step 5: Start Capture

- Click Capture to begin packet collection.

Step 6: View and Analyze Output

- Captured packet data is displayed clearly for immediate analysis.

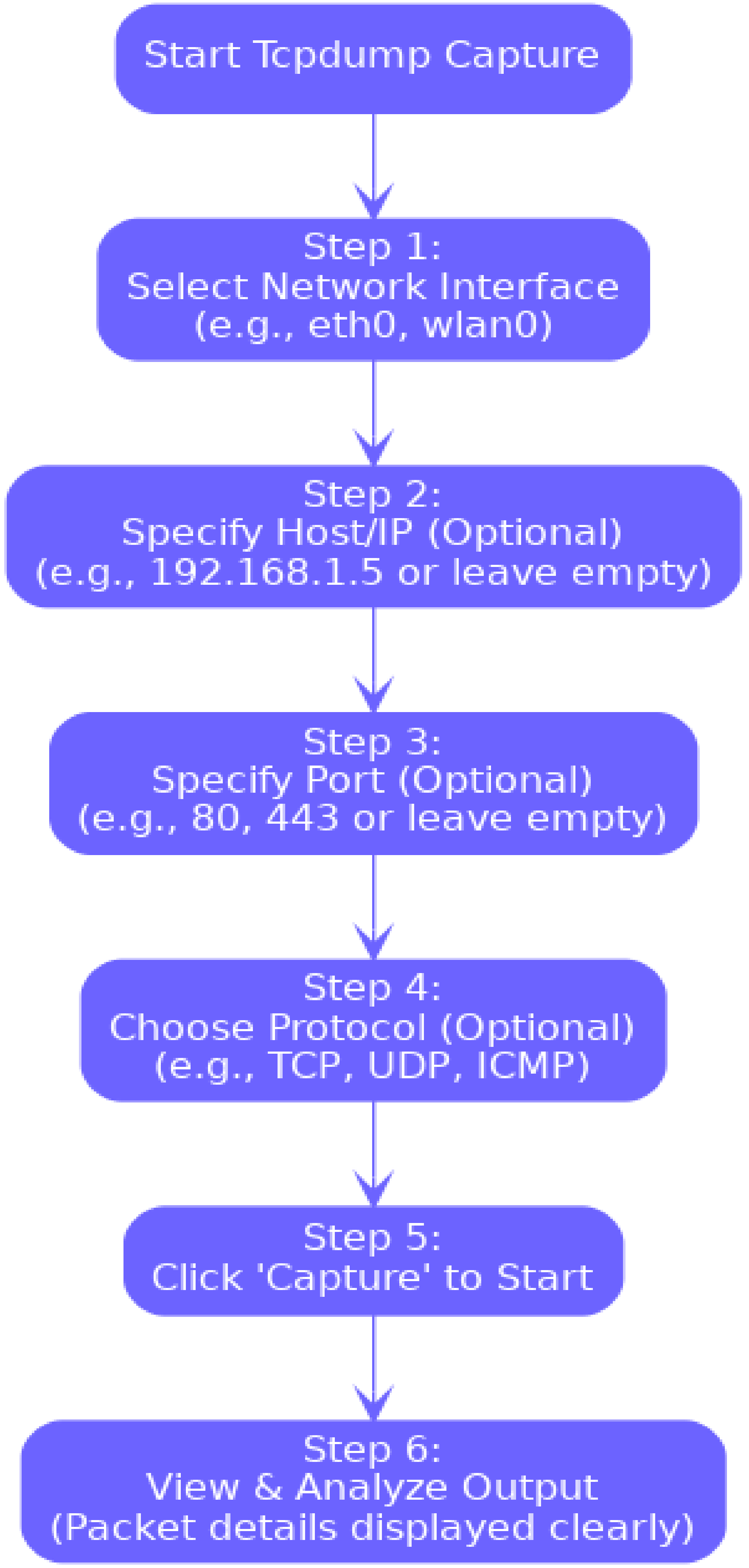
Let's look at an output example:

- tcpdump -i eth0 host 192.168.1.5 and port 80 -vv

Now lets breakdown the command-

- -i eth0: Specifies capturing packets on the eth0 network interface.
- host 192.168.1.5: Filters the captured network traffic to include only packets sent to or received from the specified IP address (192.168.1.5).
- port 80: Further narrows the captured traffic to only those packets involving port 80, typically associated with HTTP traffic.
- -vv: Produces highly detailed (verbose) output, providing comprehensive information about each captured packet.

Flowchart



Start Tcpdump Capture
Step 1:
Select Network Interface
(e.g., eth0, wlan0)
Step 2:
Specify Host/IP (Optional)
(e.g., 192.168.1.5 or leave empty)
Step 3:
Specify Port (Optional)
(e.g., 80, 443 or leave empty)
Step 4:
Choose Protocol (Optional)
(e.g., TCP, UDP, ICMP)
Step 5:
Click 'Capture' to Start
Step 6:
View & Analyze Output
(Packet details displayed clearly)

Key Features

- **Packet Capture:**
Records network traffic by intercepting data packets transmitted across networks.

- **Packet Analysis:**
Offers comprehensive insights into captured packets, detailing their contents and network behavior.

- **Advanced Filtering:**
Enables precise filtering of network traffic through customizable filter expressions.

- **Protocol Inspection:**
Capable of analyzing diverse protocols, including TCP, UDP, ICMP, among others.

- **Data Management:**
Facilitates saving captured packet data into files for convenient later review and analysis.

Testing tutorial link- https://www.youtube.com/watch?v=1lDfCRM6dWk

SMB Enumeration

About SMB Enumeration:

SMB Enumeration is a method used to collect information from a system that uses the SMB (Server Message Block) protocol. SMB is mostly used in Windows systems for sharing files, folders and printers across a network. By running an SMB enumeration scan you can find out what resources are being shared and get useful details like usernames, groups and even the system's OS info.

This is a really useful step in penetration testing because it can reveal misconfigurations or open shares that an attacker might take advantage of.

Key Features

- **List Shared Resources:**
Shows folders, printers and drives shared over the network.

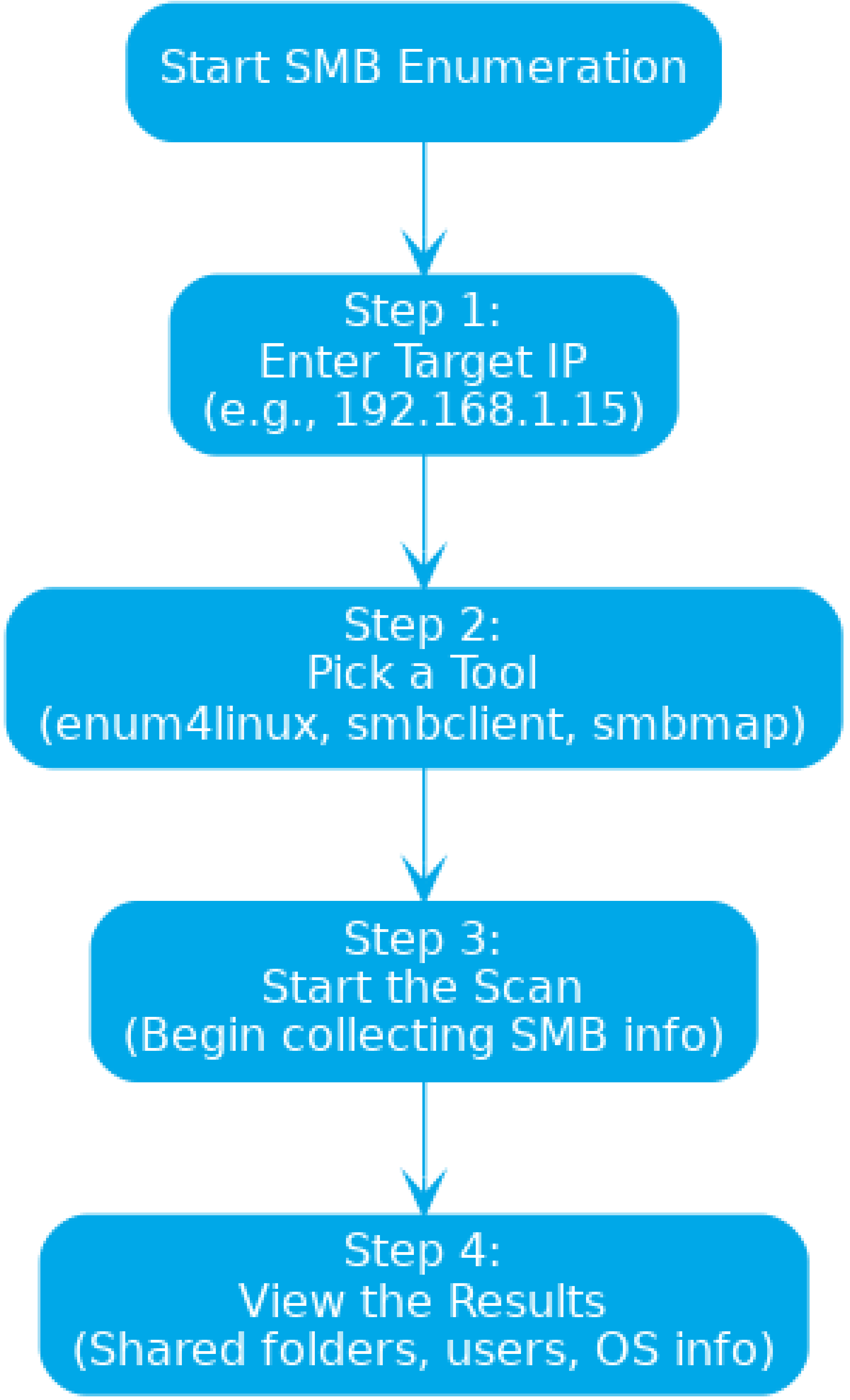
- **User and Group Info:**
Lists usernames and group names from the system.

- **OS and Host Details:**
Gives info like the hostname and operating system.

- **Detect Vulnerabilities:**
Helps identify if there are any security issues with SMB.

- **Access Control Testing:**
Lets you see if shared files are protected properly.

Flowchart



Start SMB Enumeration

Step 1:
Enter Target IP
(e.g., 192.168.1.15)

Step 2:
Pick a Tool
(enum4linux, smbclient, smbmap)

Step 3:
Start the Scan
(Begin collecting SMB info)

Step 4:
View the Results
(Shared folders, users, OS info)

Process

Step 1: Enter the Target IP Address

- Input the IP address of the system you want to scan for SMB data.

Example: 192.168.1.15

Step 2: Choose the Tool or Method

- Select the enumeration tool or technique you want to use, such as:
  - smbclient
  - enum4linux
  - smbmap
  - nbtscan

Step 3: Start the Enumeration

- Click Start to begin scanning the target system for SMB-related information.

Step 4: View the Output

- The results will show available shares, user accounts, OS version and any other accessible information.

Let's look at an example:

- enum4linux -a 192.168.1.15

Now lets breakdown the command:-

- -a: Runs all enumeration options available.
- 192.168.1.15: Target IP address to scan.
- 192.168.1.1: The gateway or router being spoofed.

Another example with smbclient:

- smbclient -L //192.168.1.15 -N

Now lets breakdown the command:-

- -L: Lists the shares
- -N: Tells it to connect without asking for a password

Testing tutorial link- https://www.youtube.com/watch?v=SGXWXpWvaRc

OpenVAS (Greenbone)

About OpenVAS :

A powerful open source tool for locating and controlling security flaws in networks and systems is OpenVAS (Open Vulnerability Assessment Scanner), which is now frequently linked to Greenbone. It identifies possible security flaws, does automated vulnerability scans and provides thorough remedial guidance.

Process

Step 1: Enter Target or Hostname

• Enter the IP address or hostname of the system you want to analyze.
Example: 192.168.1.10

Step 2: Choose a Scan Profile

• Select an appropriate scan profile depending on the level of assessment needed:

- Quick Scan for faster, lighter checks
- Full and Deep Scan for thorough security analysis
- Web Application Scan for testing websites
- Custom Profile for user-specific configurations

Step 3: Set Scan Schedule (Optional)

• Decide whether to run the scan immediately or schedule it for a later date and time.
Example: "Run Immediately" or "Schedule for Later"

Step 4: Launch the Scan

- Click the Start Scan button to begin the vulnerability assessment.

Step 5: Observe Scan Progress

- Monitor the scan's status and progress in real time through the interface.

Step 6: Review and Analyze the Report

- Once the scan is complete, examine the detailed report, which includes discovered vulnerabilities, their severity and recommended remediation steps.

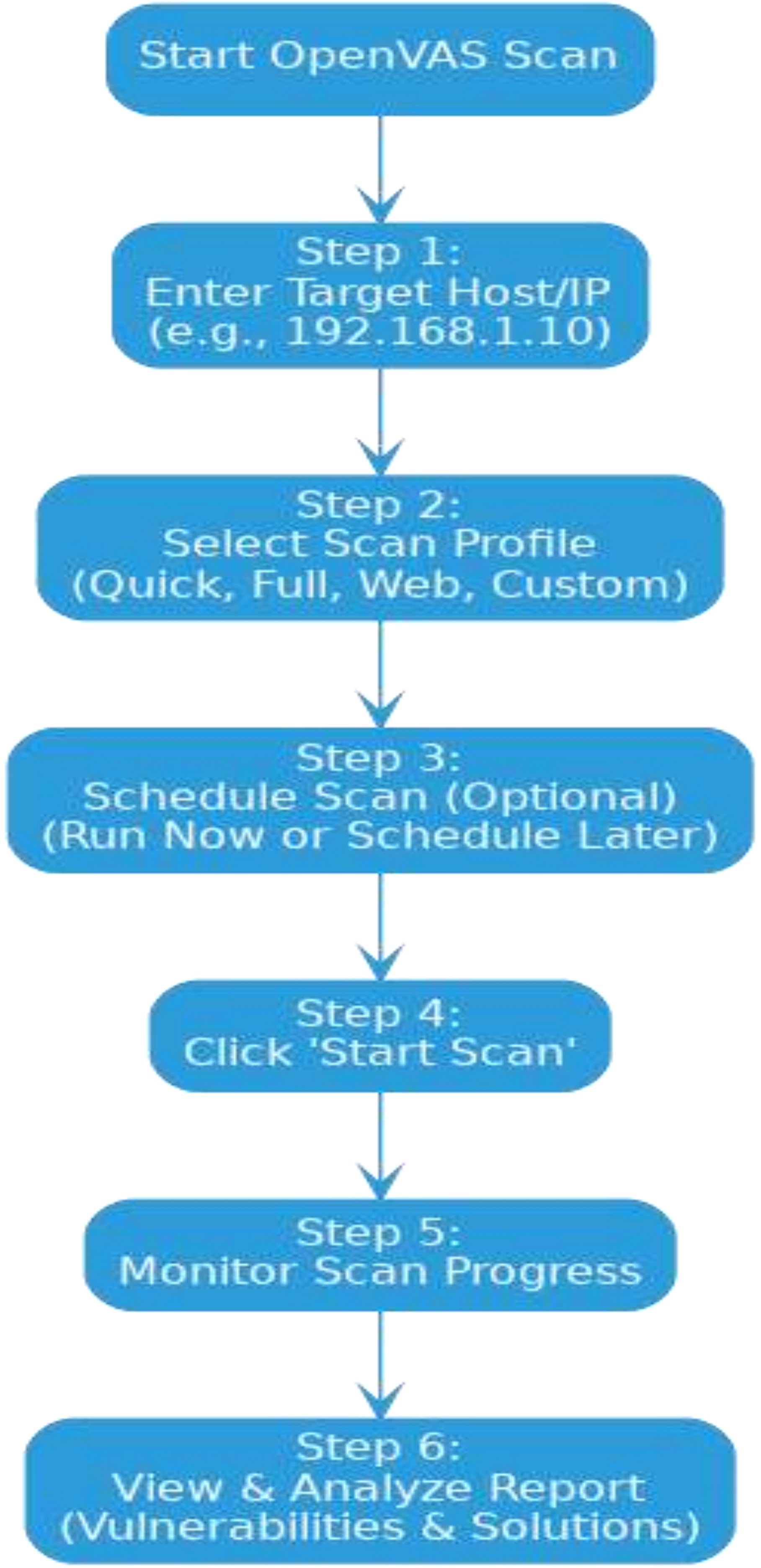
Let's look at an output example:

- openvas -T 192.168.1.10 --profile=Full_and_Deep --report=html

Now lets breakdown the command-

- -T 192.168.1.10: Specifies the IP address or hostname of the target system to be scanned.
- --profile=Full_and_Deep: Selects the "Full and Deep" scan profile for an in depth vulnerability assessment.
- --report=html: Generates the scan results in an HTML format for easy viewing and sharing.

Flowchart



Start OpenVAS Scan

Step 1:
Enter Target Host/IP
(e.g., 192.168.1.10)

Step 2:
Select Scan Profile
(Quick, Full, Web, Custom)

Step 3:
Schedule Scan (Optional)
(Run Now or Schedule Later)

Step 4:
Click 'Start Scan'

Step 5:
Monitor Scan Progress

Step 6:
View & Analyze Report
(Vulnerabilities & Solutions)

Key Features

- **Threat Identification:**
Detects and flags a broad spectrum of recognized security vulnerabilities across systems.

- **Extensive Scanning Coverage:**
Performs in depth scans across entire networks, including hosts, devices and services.

- **Continuous Database Updates:**
Maintains an up to date vulnerability feed to stay aligned with the latest threat intelligence.

- **Risk Based Prioritization:**
Assesses and ranks vulnerabilities based on their potential impact and severity.

- **In-Depth Reporting:**
Delivers detailed, actionable reports to help security teams understand issues and apply fixes effectively.

Testing tutorial link- https://www.youtube.com/watch?v=9fLp1VGNHIs

ARP Spoofing

About ARP Spoofing

ARP Spoofing also called ARP Poisoning is a type of network attack where a hacker sends fake ARP messages on a local network. The goal is to trick devices into thinking the attacker’s MAC address belongs to another device, like the router or gateway. This way, the attacker can control the flow of network traffic and see or change data being sent between two devices.

It’s mostly used in Man-in-the-Middle (MITM) attacks, where the attacker can read, change, or block data between a user and the network.

Key Features

- **Traffic Sniffing:**

Lets the attacker see network traffic between the victim and the router.

- **Session Hijacking:**

The attacker can take over active sessions.

- **Stealing Credentials:**

Can be used to grab usernames, passwords and other private data.

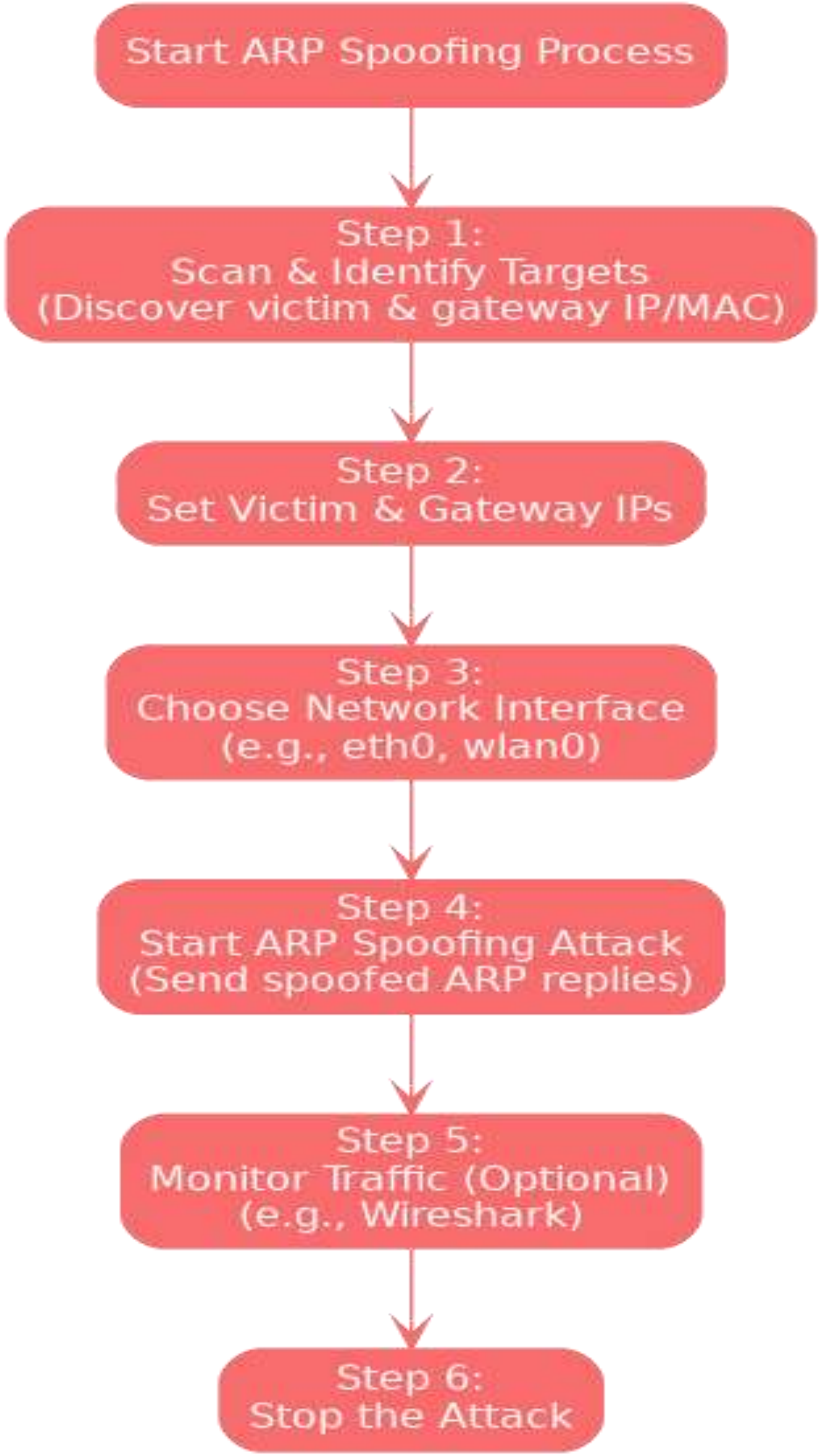
- **Data Manipulation:**

Allows the attacker to add or change information in the data being sent.

- **Network Disruption:**

Can break communication between devices or cause a denial of service(DoS).

Flowchart



Start ARP Spoofing Process

Step 1:
Scan & Identify Targets
(Discover victim & gateway IP/MAC)

Step 2:
Set Victim & Gateway IPs

Step 3:
Choose Network Interface
(e.g., eth0, wlan0)

Step 4:
Start ARP Spoofing Attack
(Send spoofed ARP replies)

Step 5:
Monitor Traffic (Optional)
(e.g., Wireshark)

Step 6:
Stop the Attack

Process

Step 1: Find Your Targets :

- First, use a tool like Nmap to find the IP and MAC addresses of devices on your network.

Example: 192.168.1.10, Gateway - 192.168.1.1

Step 2: Enter Ips :

- Enter the IP addresses of the victim device and the default gateway.

Step 3: Choose Your Network Interface :

- Select the interface that will be used for the spoofing, such as eth0 or wlan0.

Step 4: Start ARP Spoofing Attack :

- Click start to begin spoofing. The tool will send fake ARP replies to redirect the traffic through your system.

Step 5: Watch the Traffic (Optional) :

- You can use tools like Wireshark or Tcpdump to look at the captured traffic.

Step 6: Stop the Attack :

- Once you’re done testing, stop the spoofing to return everything to normal.

Let's look at an example:

- arpspoof -i eth0 -t 192.168.1.10 192.168.1.1

Now lets breakdown the command:-

- -i eth0: Use the eth0 network interface.
- -t 192.168.1.10: The target device (victim).
- 192.168.1.1: The gateway or router being spoofed.

To spoof both directions (victim and router), you can run another command with the IPs reversed.

Testing tutorial link- https://www.youtube.com/watch?v=4s3Z9eFyKnA

Burp Suite

About Burp suit:

Burp Suite is one of the best tools used to conduct web application penetration testing. It is a go between between your browser and website you are checking out, allowing you to see and make changes to everything that is being sent or received. It is really great for catching things like broken authentication, insecure inputs or hidden flaws.

Burp Suite is comprised of a set of tools that act together and it is convenient for both beginner and advanced testers.

Key Features

- **Proxy Tool:**
Intercepts traffic between your browser and the target site so you can inspect or manipulate it.

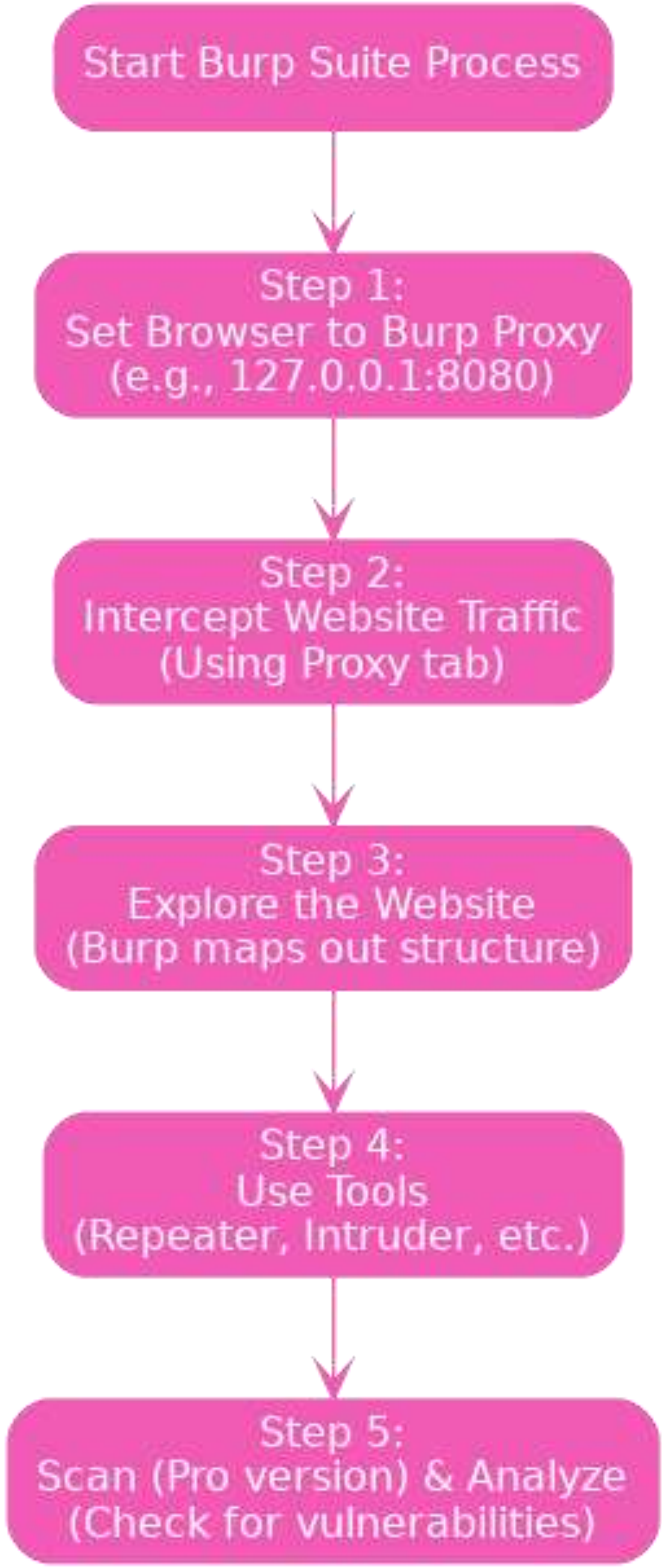
- **Scanner (Pro version):**
Automatically scans sites for vulnerabilities like XSS, SQLi, etc.

- **Repeater:**
Enables you to manually manipulate and resend requests to see how the server will react.

- **Intruder:**
Used for automatic attacks like brute force or fuzzing inputs.

- **Decoder & Comparer:**
Helps you inspect encoded data and compare request/response data.

Flowchart



Start Burp Suite Process

Step 1:
Set Browser to Burp Proxy
(e.g., 127.0.0.1:8080)

Step 2:
Intercept Website Traffic
(Using Proxy tab)

Step 3:
Explore the Website
(Burp maps out structure)

Step 4:
Use Tools
(Repeater, Intruder, etc.)

Step 5:
Scan (Pro version) & Analyze
(Check for vulnerabilities)

Process

Step 1: Set Up Your Browser

- Make your browser use the Burp Suite proxy (usually 127.0.0.1:8080). Burp will then be able to intercept and listen to the traffic.

Step 2: Intercept Requests

- With Burp running, go to the target website. Burp will intercept requests and responses, which you can view in the Proxy tab.

Step 3: Explore the Site

- Click the site. Burp will graph the site topology and intercept traffic.

Step 4: Use Tools like Repeater and Intruder

- Repeater: Select a request and manually modify it to attempt different inputs.
- Intruder: Execute attacks like brute force or fuzzing automatically.

Step 5: Scan for Vulnerabilities (Pro)

- If you have Pro, you can run an automated scan to determine security vulnerabilities.

Step 6: Analyze the Results

- Scan the output for vulnerabilities or anything out of the ordinary. You can also export the results for a report.

Example Use Case:

You open a login page in your browser, Burp intercepts the request. You send that request to Repeater, try different passwords and see how the site responds. This tells you if the site is vulnerable to brute force or weak authentication.

Testing tutorial link- https://youtu.be/JkJLZ4NYISQ?si=5aPBYPeC3yvWOek2

Gobuster

About Gobuster:

ARP Spoofing also called ARP Poisoning is a type of network attack where a hacker sends fake ARP messages on a local network. The goal is to trick devices into thinking the attacker’s MAC address belongs to another device, like the router or gateway. This way, the attacker can control the flow of network traffic and see or change data being sent between two devices.

It’s mostly used in Man-in-the-Middle (MITM) attacks, where the attacker can read, change, or block data between a user and the network.

Key Features

- **Directory Scanning:**
Scans websites to uncover hidden directories or files using wordlists.

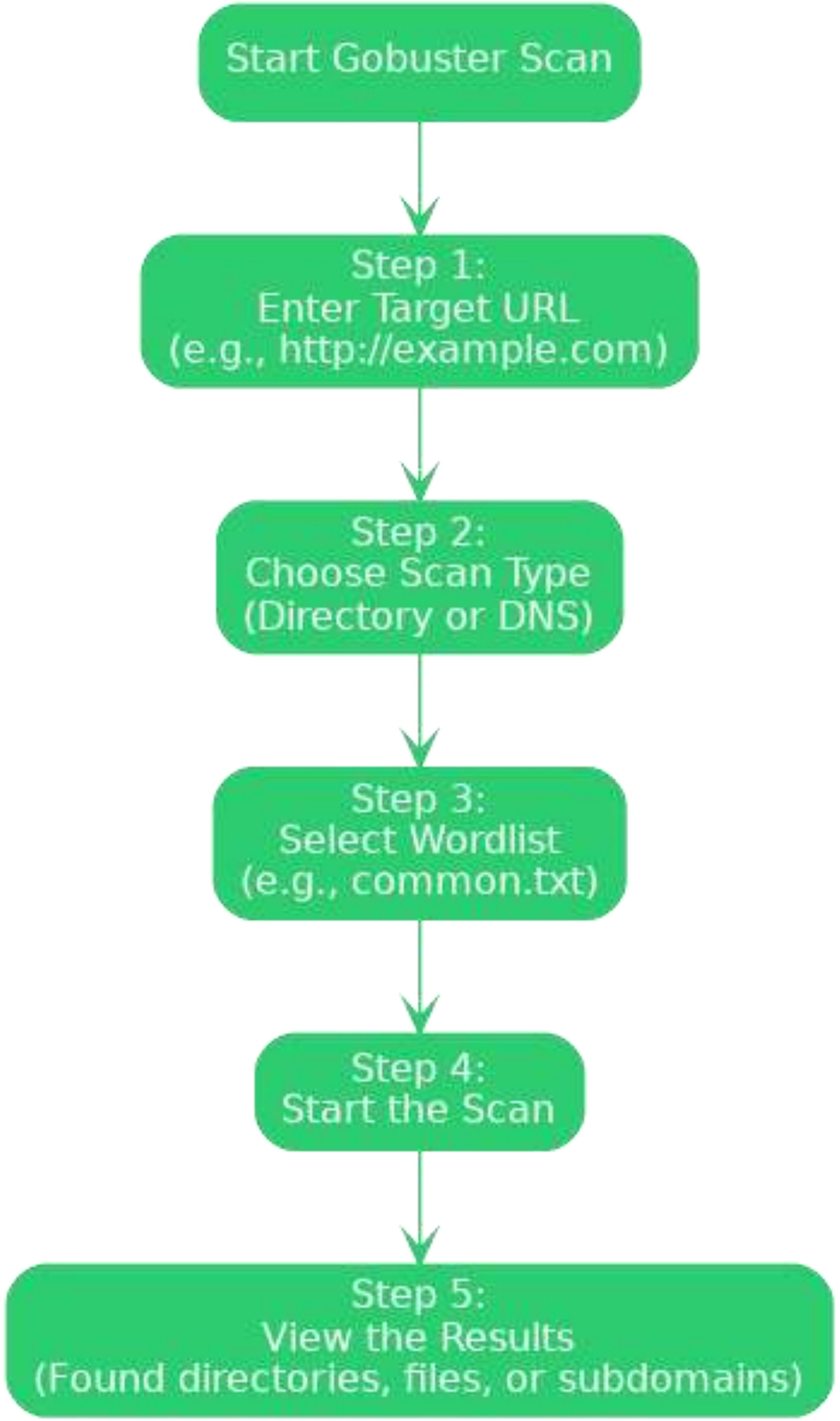
- **DNS Subdomain Bruteforce:**
Tries common names to find subdomains that are not normally visible.

- **Fast Performance:**
Runs super quick because it is built with the Go programming language.

- **Custom Wordlists:**
You can use any wordlist for custom scans.

- **Simple CLI Output:**
Gives results in a clean and easy to read format.

Flowchart



Start Gobuster Scan

Step 1:
Enter Target URL
(e.g., http://example.com)

Step 2:
Choose Scan Type
(Directory or DNS)

Step 3:
Select Wordlist
(e.g., common.txt)

Step 4:
Start the Scan

Step 5:
View the Results
(Found directories, files, or subdomains)

Process

Step 1: Enter the Target URL :

- Enter the address of the website you want to scan.

Example: http://xyz.com

Step 2: Choose Scan Type :

- Decide what kind of scan you want to run:
  - Directory Scan (to look for hidden folders or files)
  - DNS Scan (to find subdomains of the site)

Step 3: Choose a Wordlist :

- Select a wordlist that Gobuster will use to guess file, folder or subdomain names.

Example: abc.txt

Step 4: Start the Scan

- Hit the Start button and Gobuster will begin testing each word from the list against the site.

Testing tutorial link- https://www.youtube.com/watch?v=HjXNK-mYwDQ

Step 5: View the Results

- Once the scan finishes you will see any directories, files or subdomains it found, these might lead to interesting or vulnerable parts of the site.

Let's look at an example Command (Directory Scan):

- gobuster dir -u http://example.com -w /usr/share/wordlists/dirb/common.txt

Now lets breakdown the command:-

- dir: Tells Gobuster to run a directory scan
- -u: Sets the target URL
- -w: Points to the wordlist you want to use

For DNS subdomain scan:

```
gobuster dns -d example.com -w /usr/share/wordlists/dns/common.txt
```