Penetration Testing
Implementation Plan

Azhar Ghafoor

Fall-2022

Department of Cyber Security, FCAI
Air University, Islamabad

Network Penetration Testing

Network Penetration Testing

1. Network penetration testing involves detecting security weaknesses in the network infrastructure of the target organization
2. Network penetration test can be conducted from inside or outside of the organization
3. It is recommended that organizations should perform both internal and external network penetration testing for better results

Network penetration test commonly includes the following type of tests against target network infrastructure:

- Detecting unnecessary open ports, services running, sensitive information exposed through default banners
- Firewall bypass testing
- IDS evasion testing
- Testing switching or routing issues

External and Internal Penetration Testing

- External penetration testing involves security evaluation of:
  - All publicly available network applications such as websites/applications, FTP, etc.
  - Network infrastructure devices such as firewall, IDS, routers, switches, etc.
  - Wireless networks
- Internal penetration testing involves security evaluation of:
  - All internal networks, infrastructure devices and applications including servers, end points, etc.

Network Penetration Testing Process

White, Black or Grey Box Network Penetration Testing?

White-Box Penetration Testing:

- In case of white-box network penetration testing assignment, the organization may provide you with the following information in advance about their network infrastructure:
  - Network diagrams
  - IP addresses
  - Domain names
  - Device type
  - Applications and their versions
  - Security defenses such as IDS, IPS
  - OS details
  - Other infrastructure details
- Generally, organization may provide you with network administrator level knowledge, excluding passwords

White, Black or Grey Box Network Penetration Testing? (Cont'd)

Black-Box Penetration Testing:

- In case of black-box network penetration testing assignment, the organization will not provide any information about their network infrastructure
- You need to gather target network information such as domain names, IP range, live hosts, OS details, network map, device types, security defenses, etc., on your own by applying various information gathering and reconnaissance techniques

Gray-Box Penetration Testing:

- In case of gray-box network penetration testing assignment, the organization may provide you some of the information about their network infrastructure

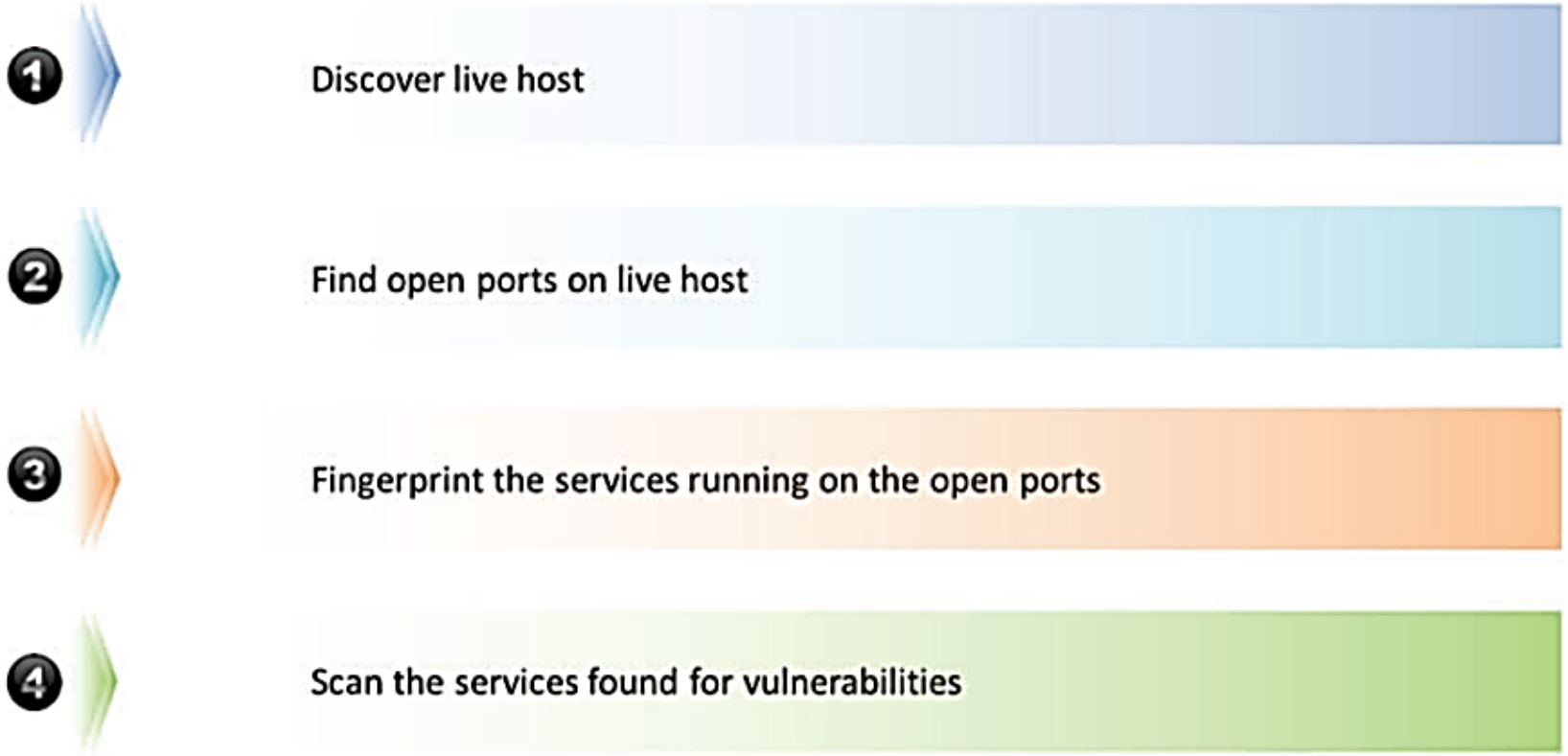
Step 1: Information Gathering (OSINT)

Topics Discussed in the Previous Lecture

Step 2: Port Scanning

2. Port Scanning

- **The information obtained in reconnaissance phase is used in port scanning phase to:**



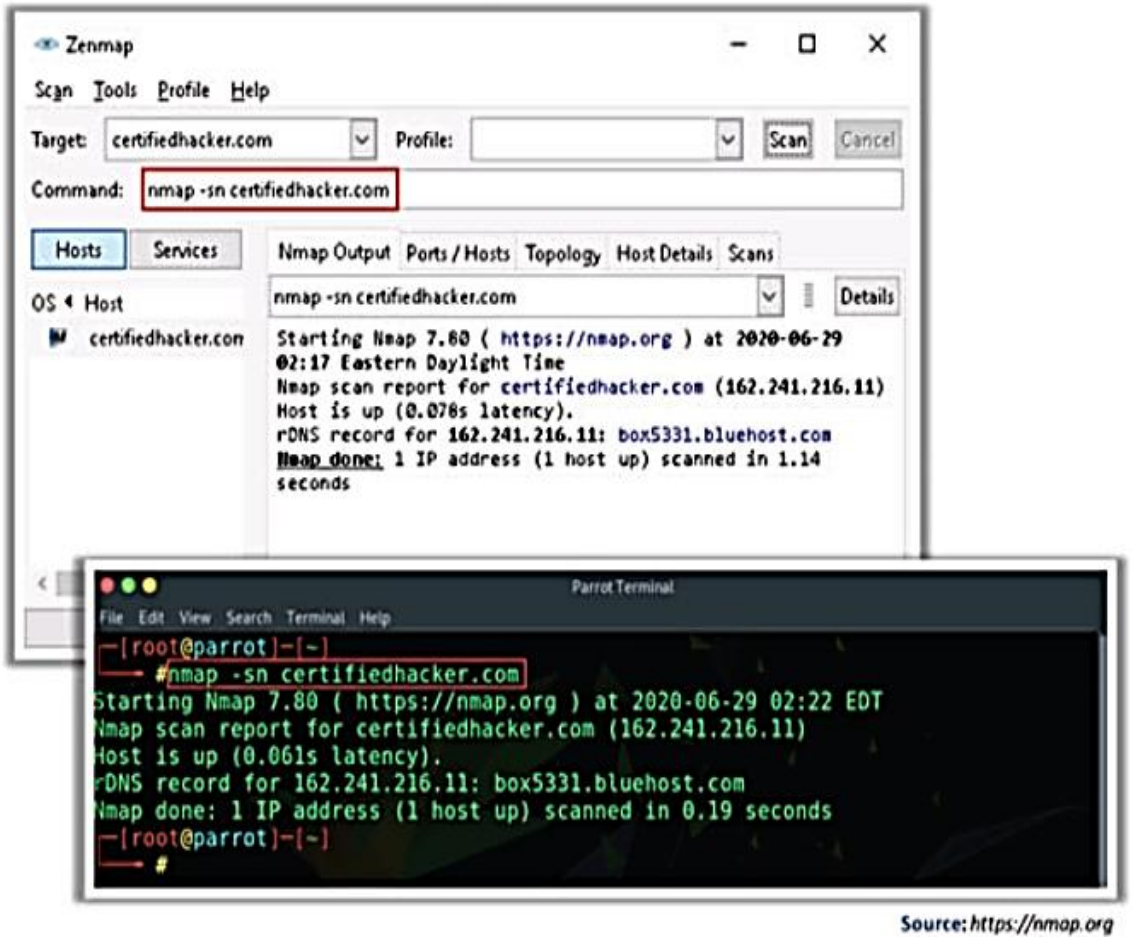
Check for Live Systems – ICMP Scanning

ICMP scanning involves sending ICMP ECHO requests to a host. An ICMP ECHO reply will indicate that the host is live

This scan is useful for locating active devices or determining if ICMP is passing through a firewall

Perform ICMP scanning using Nmap and check the response

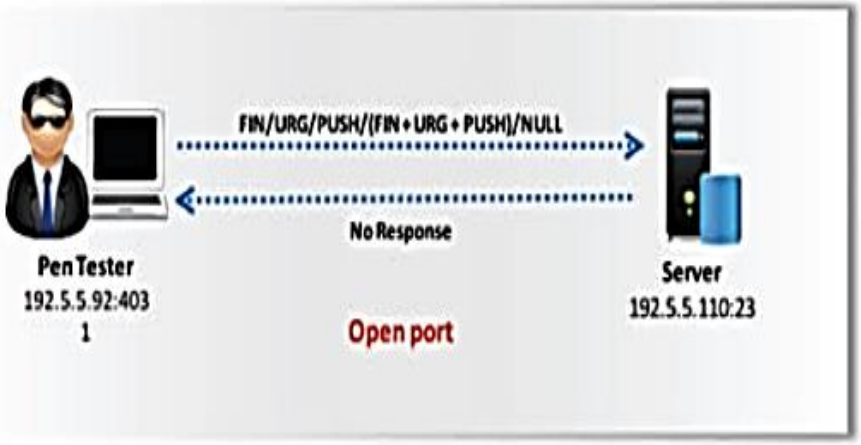
You can also use tools such as Angry IP Scanner, Ping Sweep, Colasoft Ping Tool, SolarWinds Engineer Toolset's Ping Sweep, etc. to check live systems

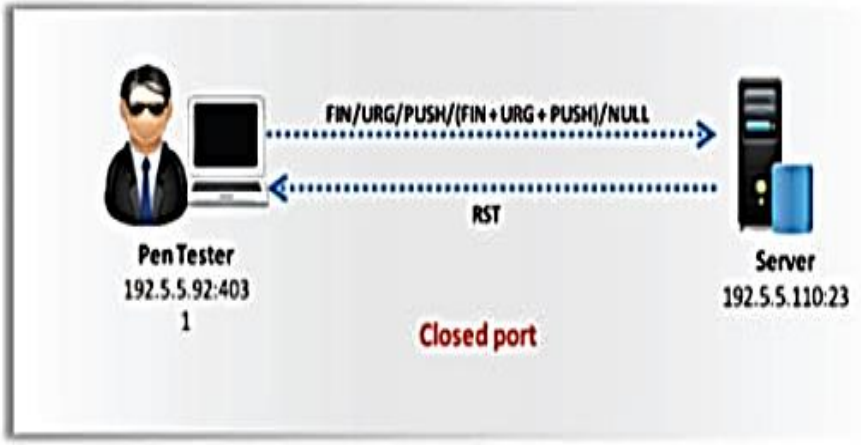


Source: https://nmap.org

Use Illegal Flag Combinations to Scan the Targets

- Refers to the use of FIN, URG, PUSH, a combination of these or no flags to scan a target for open ports
- These scans work only on OSes with **RFC 793-compliant** TCP/IP implementations
- These scans do not work against any **current version** of Microsoft Windows



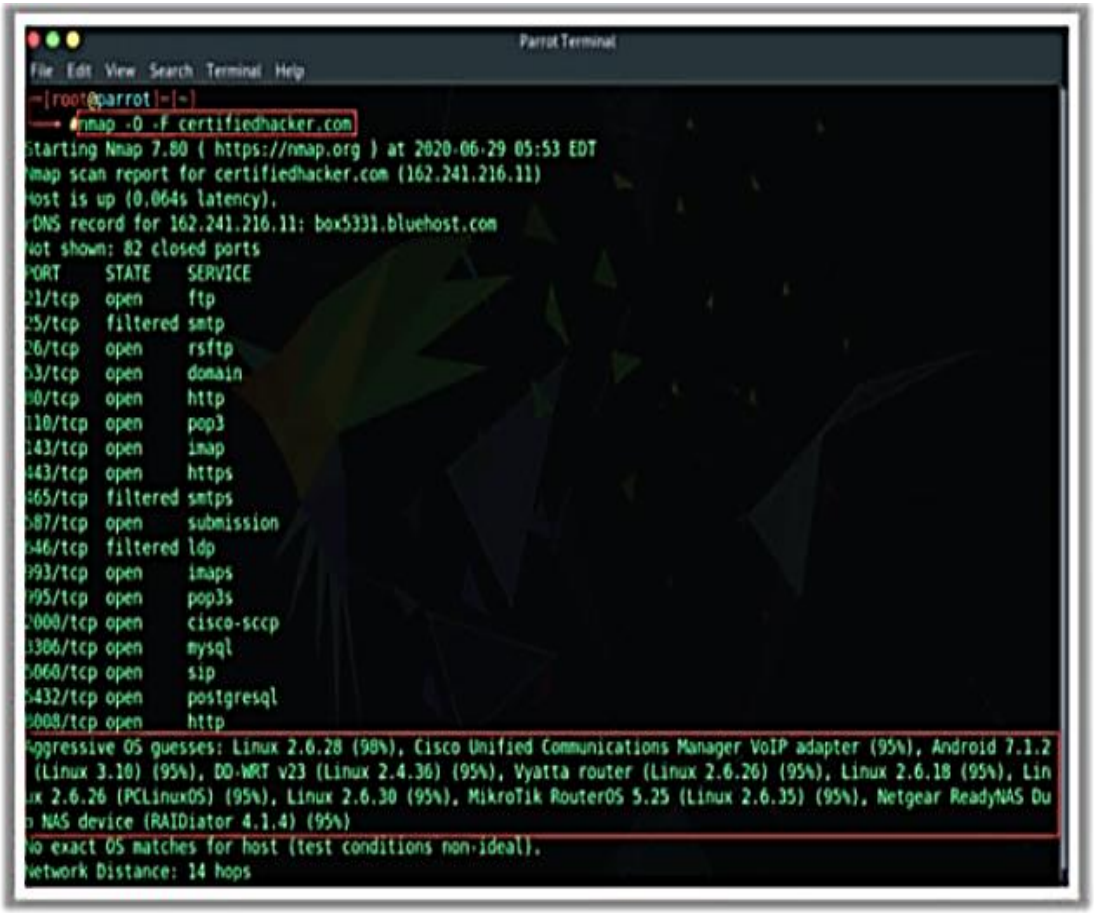


Step 3: OS and Service Fingerprinting

Fingerprint the OS

Active OS Fingerprinting:

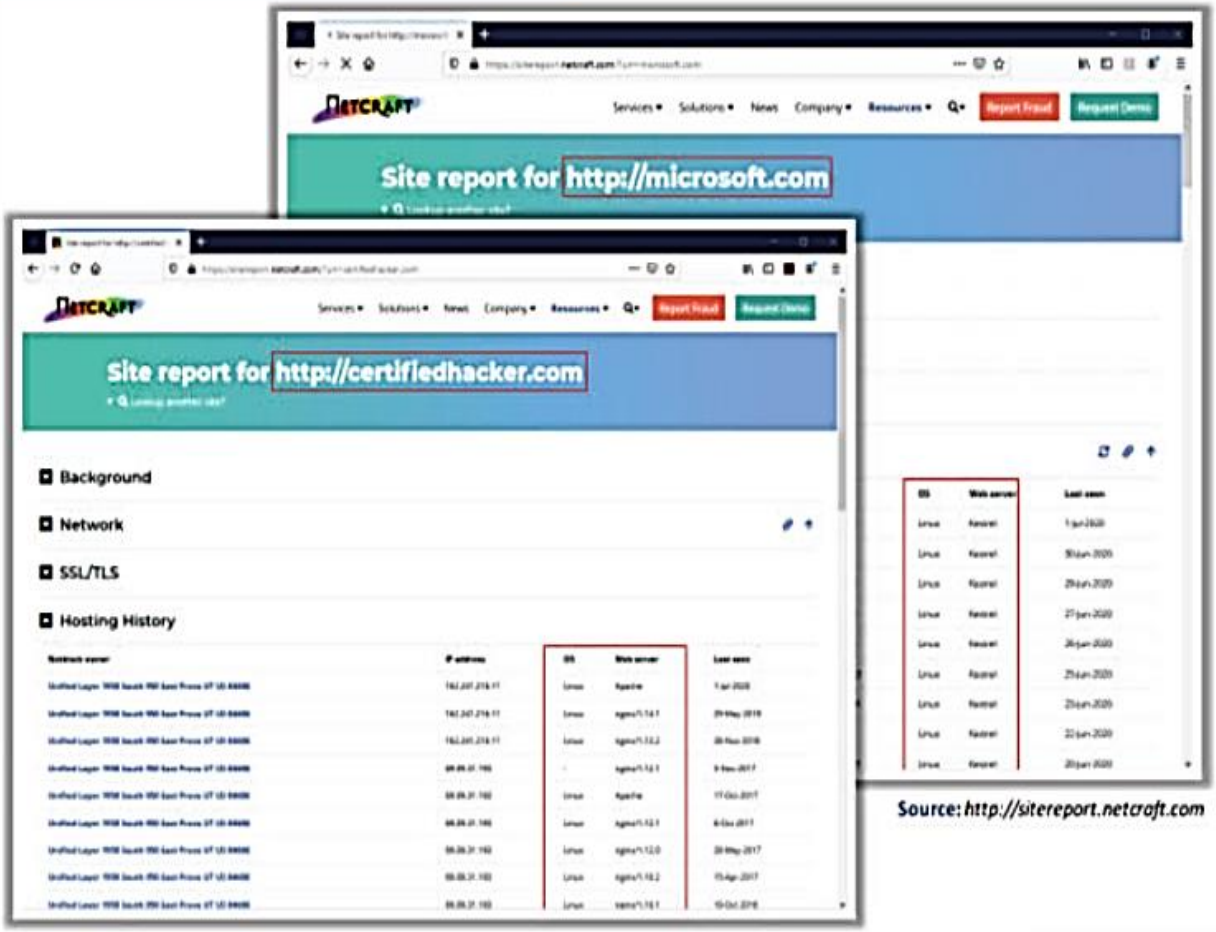
- It refers to gathering OS information about the target with direct interaction
- To fingerprint target OS details, use following Nmap command
  - Nmap –O <Target>



Fingerprint the OS (Cont'd)

Passive OS Fingerprinting:

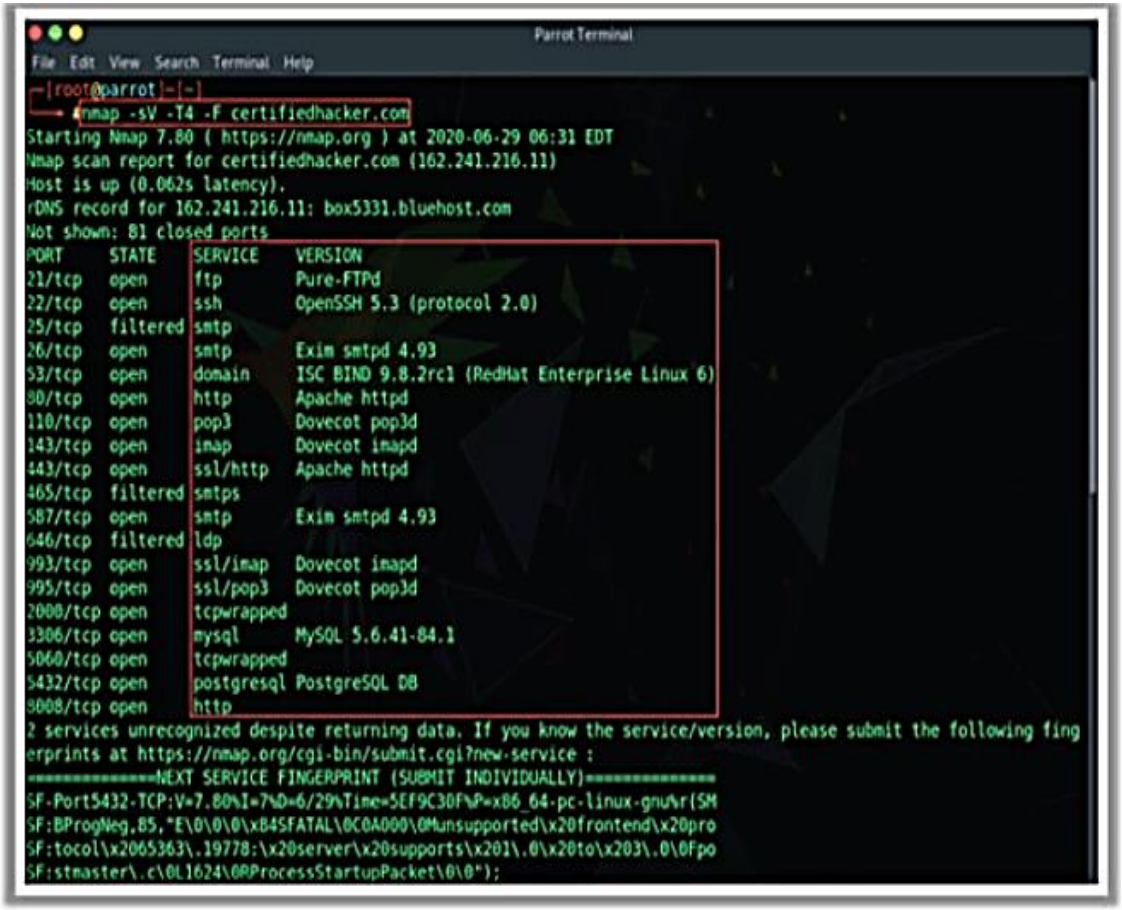
- It refers to gathering OS information about a target without direct interaction
- Use *Netcraft* to find information about **OSes of web servers**



Source: http://sitereport.netcraft.com

Fingerprint the Services

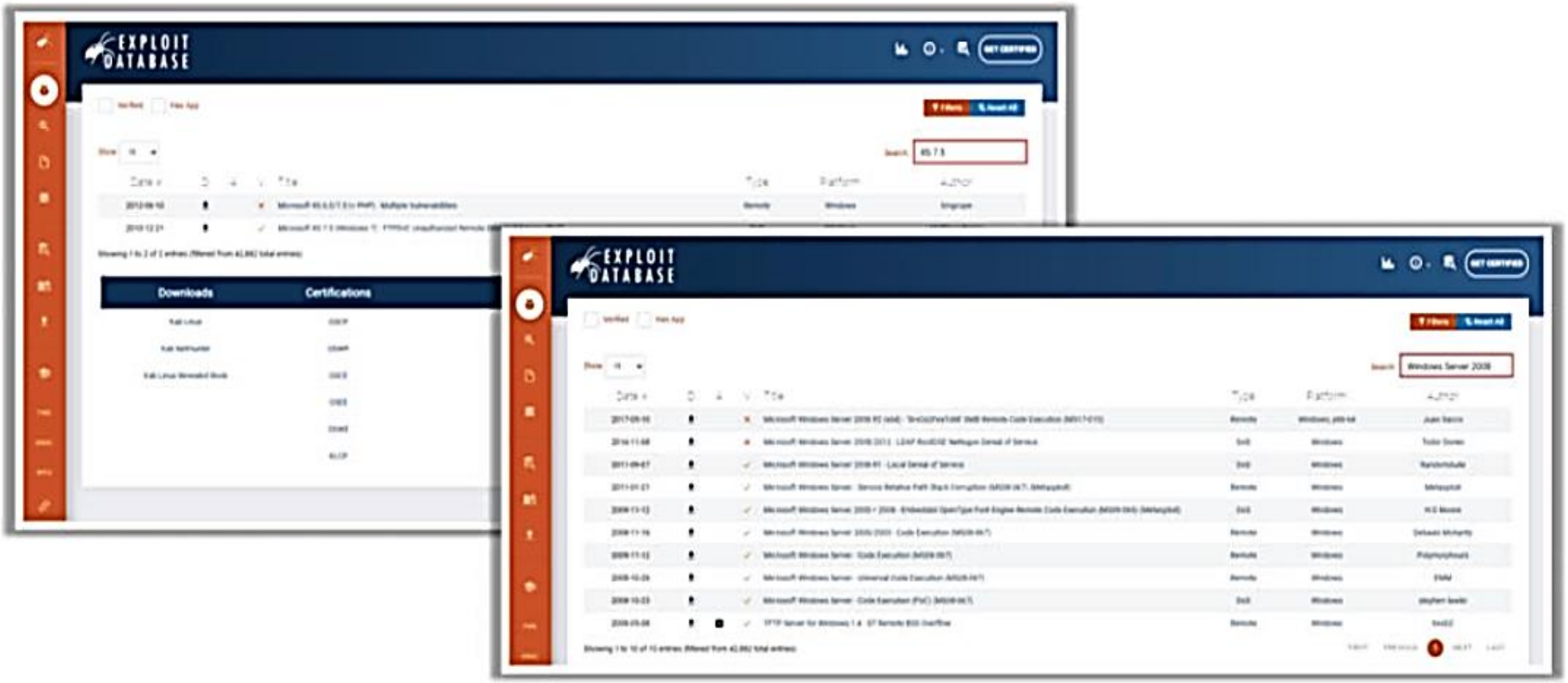
- Service fingerprinting is performed to determine services running on various port and their versions
- To perform service fingerprint, use following Nmap command
  - Nmap –sV <Target>



Step 4: Vulnerability Research

Find out the Security Vulnerability Exploits

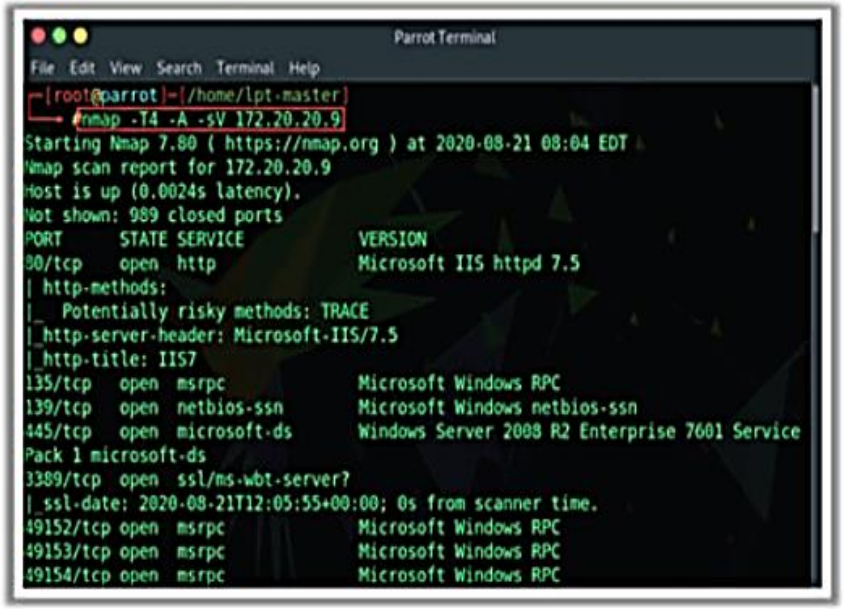
- Find out the exploits related to specific security vulnerability in the Exploit Database or using searchsploit

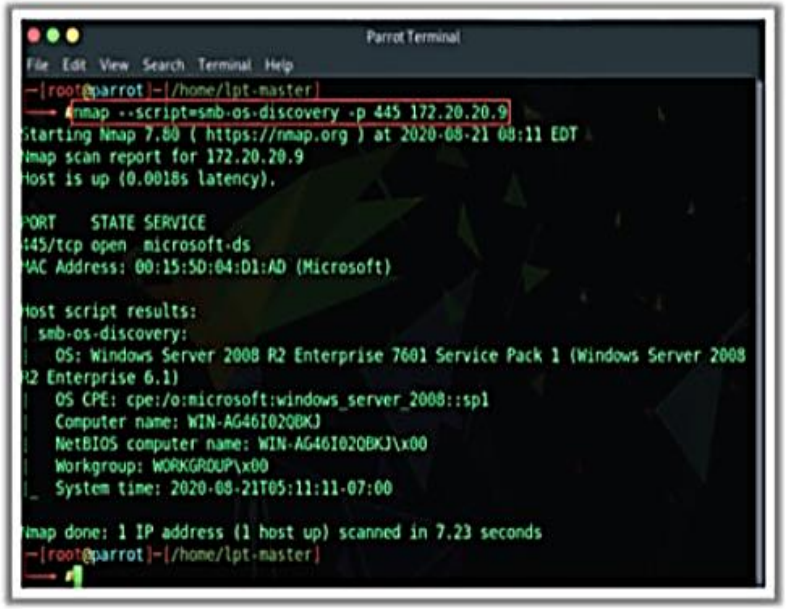


Source: https://www.exploit-db.com

Run the Exploits Against Identified Vulnerabilities

- Execute the exploits against vulnerabilities found in services, OS or devices
- For example,
  - Exploiting SMB vulnerability in Windows 7 Ultimate





The Server Message Block protocol (SMB protocol) is a client-server communication protocol used for **sharing access to files, printers, serial ports and other resources on a network**.

Step 5: Exploit verification

Overview of Exploit Verification

Initial Assessment:

The process begins with identifying potential vulnerabilities through techniques such as vulnerability scanning, code review, or using automated tools.

Test Environment Setup:

A controlled environment (sandbox or test lab) is set up to safely conduct exploitation attempts without affecting production systems.

Exploitation Attempt:

Testers use various methods and tools to attempt to exploit the identified vulnerabilities, observing whether they can gain unauthorized access or execute arbitrary code.

Validation:

If the exploit is successful, further analysis is conducted to assess the potential impact, severity, and possible mitigations.

Methods of Exploit Verification:

Manual Testing:

Security professionals manually attempt to exploit vulnerabilities, often using scripting and programming skills.

Automated Tools:

Various tools (e.g., Metasploit, Burp Suite) can automate the exploitation process, quickly testing multiple vulnerabilities.

Fuzzing:

This technique involves inputting unexpected or random data into the system to find security flaws that could be exploited.

Proof of Concept (PoC):

Creating PoC exploits that demonstrate the vulnerability's exploitation can provide validation of the risk.

Step 6: Reporting

Reporting

- *Document findings from assessments and tests (e.g., vulnerabilities, incidents).*
- *Guide decision-making for technical teams and management.*

Types of Reports:

Vulnerability Assessment Report:

Highlights system weaknesses and provides remediation steps.

Penetration Testing Report:

Details security test findings, exploited vulnerabilities, and impact.

Incident Response Report:

Covers the analysis and resolution of security incidents.

Key Components of a Report

Executive Summary:
Brief overview for management.

Technical Findings:
Detailed vulnerabilities, exploits, or issues.

Risk Ratings:
Severity levels (high, medium, low).

Recommendations:
Actions for mitigating identified risks.

Timeline:
Chronology of testing or incidents.

Case Study: XYZ Corporation Network Penetration Test

Background:

XYZ Corporation, a mid-sized financial services firm, was concerned about the security of its network infrastructure due to a recent surge in cyberattacks targeting financial institutions. To identify potential vulnerabilities, they hired a penetration testing team to simulate an attack on their network and assess the security posture.

Step 1: Information Gathering (OSINT)

- *The penetration testers began by collecting public information about XYZ Corporation using tools like* ***Recon-ng and Maltego etc****.*
- *These tools helped them gather data from the internet, including details from* ***job postings, social media profiles, and breached databases.***
- *For instance, they discovered employee emails that had been exposed in* ***past breaches****, as well as some technical details about the company's internal systems.*

Step 2: Port Scanning

- *After gathering information, the team used **Nmap or Zenmap** to scan XYZ Corporation's external network for open ports.*
- *They found multiple open ports, including port 21 (FTP), port 22 (SSH), and port 80 (HTTP), **which could potentially serve as entry points for attackers.***
- *These services needed to be evaluated further for **vulnerabilities**.*

Step 3: OS and Service Fingerprinting

- *The team used **Nmap's** advanced features and **Netcat** to identify the operating systems and services running on the open ports they discovered.*
- *They learned that XYZ's web server was using an **outdated version of Apache**, and one of their internal servers was running an older version of **Windows Server.***
- *Both systems were missing important **security patches, making them potentially vulnerable.***

Step 4: Vulnerability Research

- *Using vulnerability databases such as **CVE Details and ExploitDB,** the testers researched known vulnerabilities related to the software and systems they identified.*

- *The outdated Windows Server was found to be vulnerable to the **EternalBlue exploit (CVE-2017-0144),** while the Apache web server was at risk of an **SQL injection vulnerability** that could allow an attacker to retrieve sensitive data from the company's database.*

Step 5: Exploit Verification

- *To verify the discovered vulnerabilities, the team used Metasploit to exploit the* ***EternalBlue vulnerability on XYZ's Windows Server.***

- *They were able to gain access to the internal network, showing that an attacker could* ***easily breach the system.***

- *Additionally, they* ***used SQLMap to exploit the SQL injection*** *vulnerability on the* ***Apache web server****, confirming that they could extract sensitive information from the company's database.*

https://gist.github.com/05t3/7d5925e6a4585abe2a48cc4a978aea87

Step 6: Reporting

- *After completing the penetration test, the team created a detailed report using* ***Dradis or other tools*** *to organize and document their findings.*
- *The report included all the vulnerabilities they discovered,* ***how they exploited them, and the potential impact on XYZ Corporation's network.***
- *It also provided actionable recommendations, such as* ***applying security patches, updating firewall configurations, and enhancing employee security awareness.***

Hacking Web Server

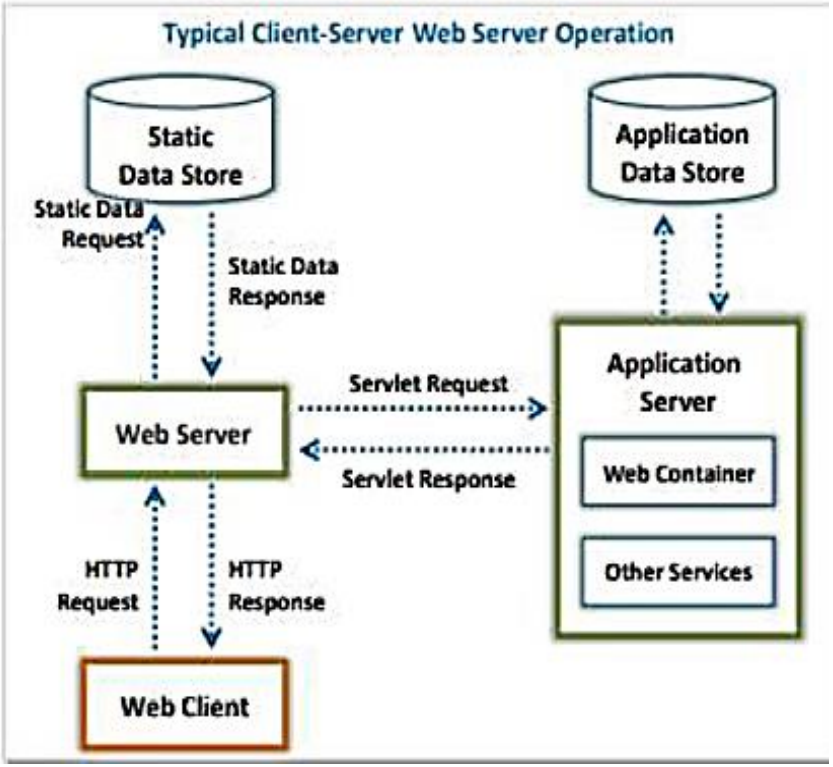
Module Flow:-

Web Server Operations

- A web server is a computer system that **stores**, **processes**, and **delivers web pages** to clients via HTTP

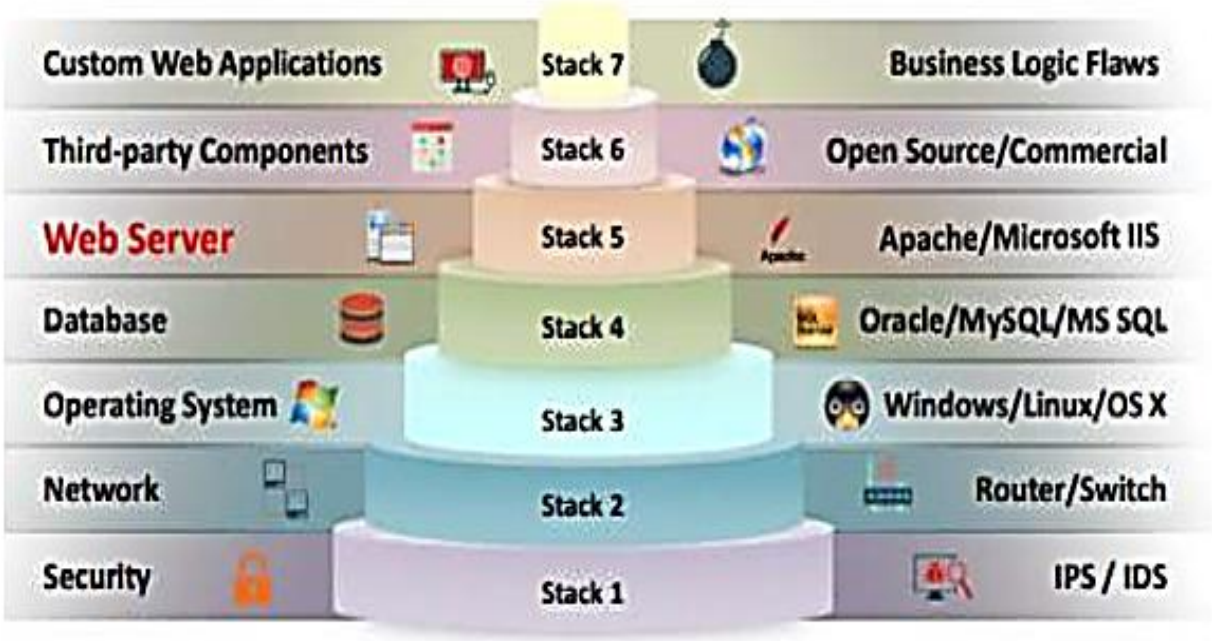
Components of a Web Server

- **Document Root:** Stores critical HTML files related to the web pages of a domain name that will be served in response to the requests
- **Server Root:** Stores server's configuration, error, executable, and log files
- **Virtual Document Tree:** Provides storage on a different machine or disk after the original disk is filled up
- **Virtual Hosting:** Technique of hosting multiple domains or websites on the same server
- **Web Proxy:** Proxy server that sits between the web client and web server to prevent IP blocking and maintain anonymity



Web Server Security Issues

- Attackers usually target **software vulnerabilities** and configuration errors to compromise web servers
- **Network** and **OS level attacks** can be well defended using proper network security measures such as firewalls, IDS, etc. However, web servers can be accessed from anywhere via the Internet, which renders them **highly vulnerable** to attacks



Impact of Web Server Attacks

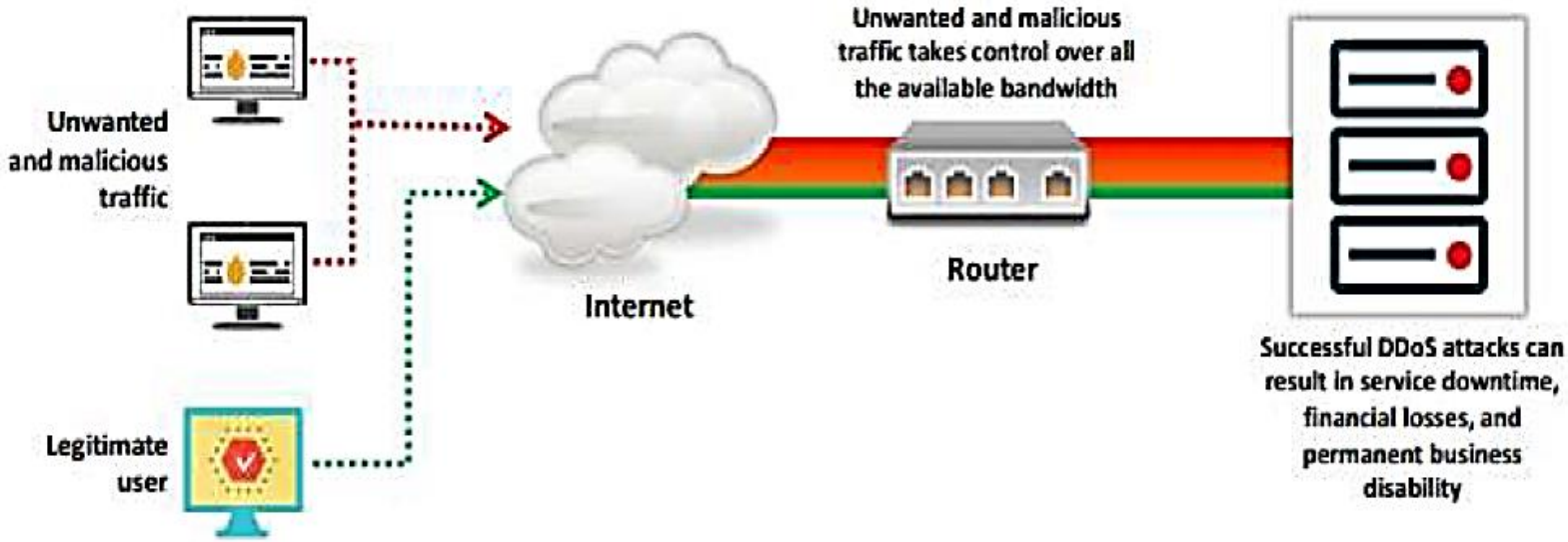
- Compromise of user accounts
- Website defacement
- Secondary attacks from the website
- Root access to other applications or servers
- Data tampering and data theft
- Reputational damage of the company

Why Are Web Server Compromised?

- **Improper** file and directory **permissions**
- Server installation with **default settings**
- Enabling of **unnecessary services**, including content management and remote administration
- **Security conflicts** with business ease-of-use case
- **Lack of proper security policies**, procedures, and maintenance
- **Improper authentication** with external systems
- **Default accounts** having default passwords, or no passwords
- **Unnecessary** default, backup, or sample **files**
- **Misconfigurations** in web server, operating systems, and networks
- **Bugs** in server software, OS, and web applications
- **Misconfigured SSL certificates** and encryption settings
- Administrative or **debugging functions** that are **enabled** or accessible on web servers
- Use of **self-signed certificates** and default certificates

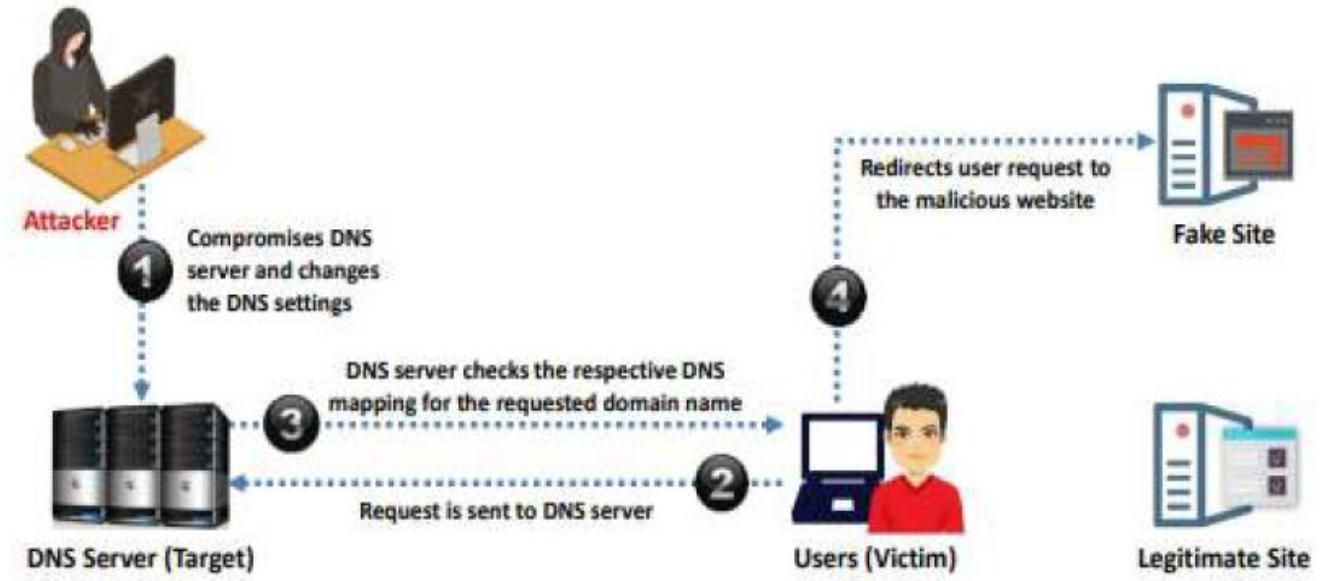
Web Server DoS\DDoS Attack

- Attackers may send numerous **fake requests** to the web server, which causes **web server crashing** or makes it unavailable to the legitimate users
- Attackers may target **high profile web servers** such as banks, credit card payment gateways, and government owned services to **steal user credentials**



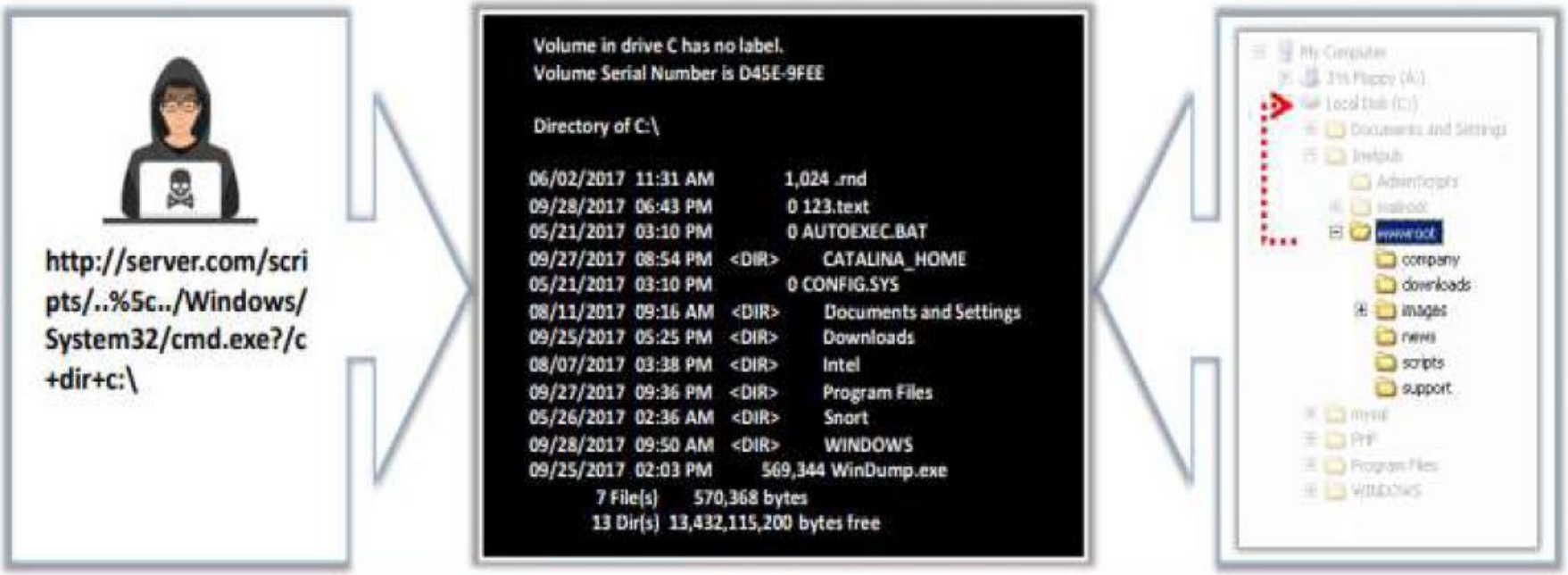
DNS Server Hijacking Attack

- Attacker compromises the DNS server and **changes the DNS settings** so that all the requests coming towards the target web server are redirected to his/her own malicious server



Directory Traversal Attack

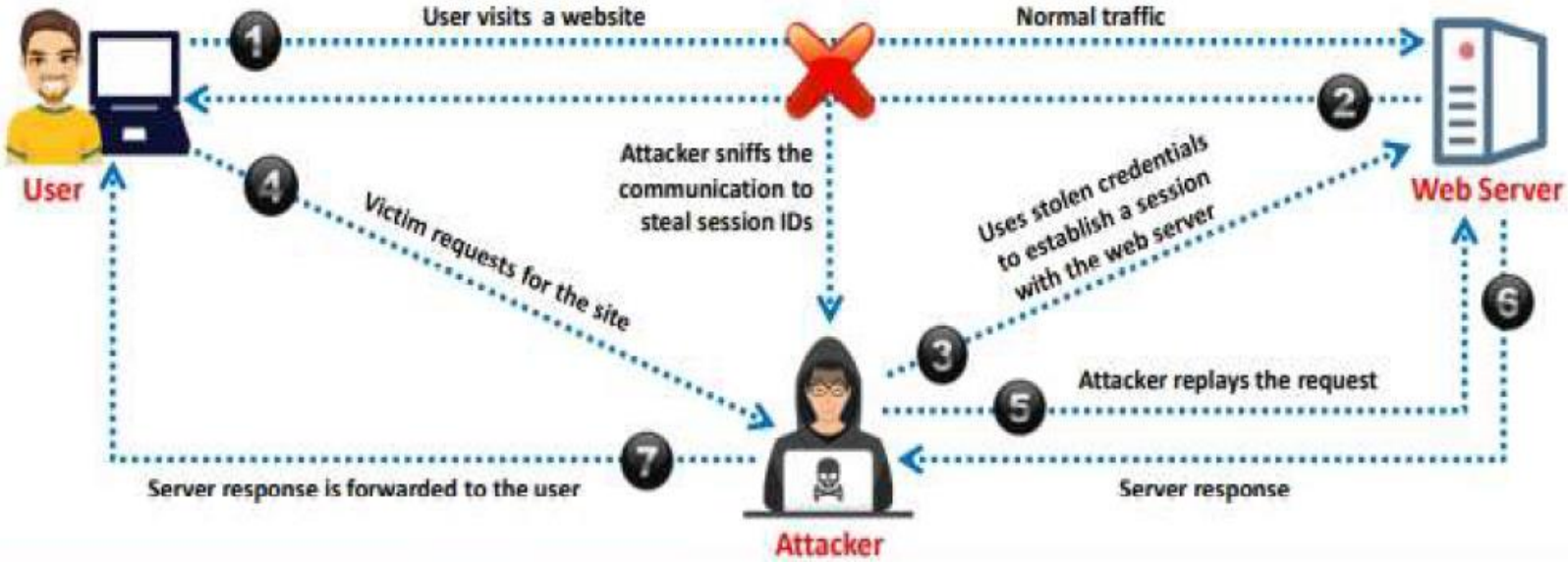
- In directory traversal attacks, attackers use the **../ (dot-dot-slash)** sequence to access restricted directories outside the web server root directory
- Attackers can use the **trial and error method** to navigate outside the root directory and access sensitive information in the system



Man-in-the-middle / Sniffing Attack

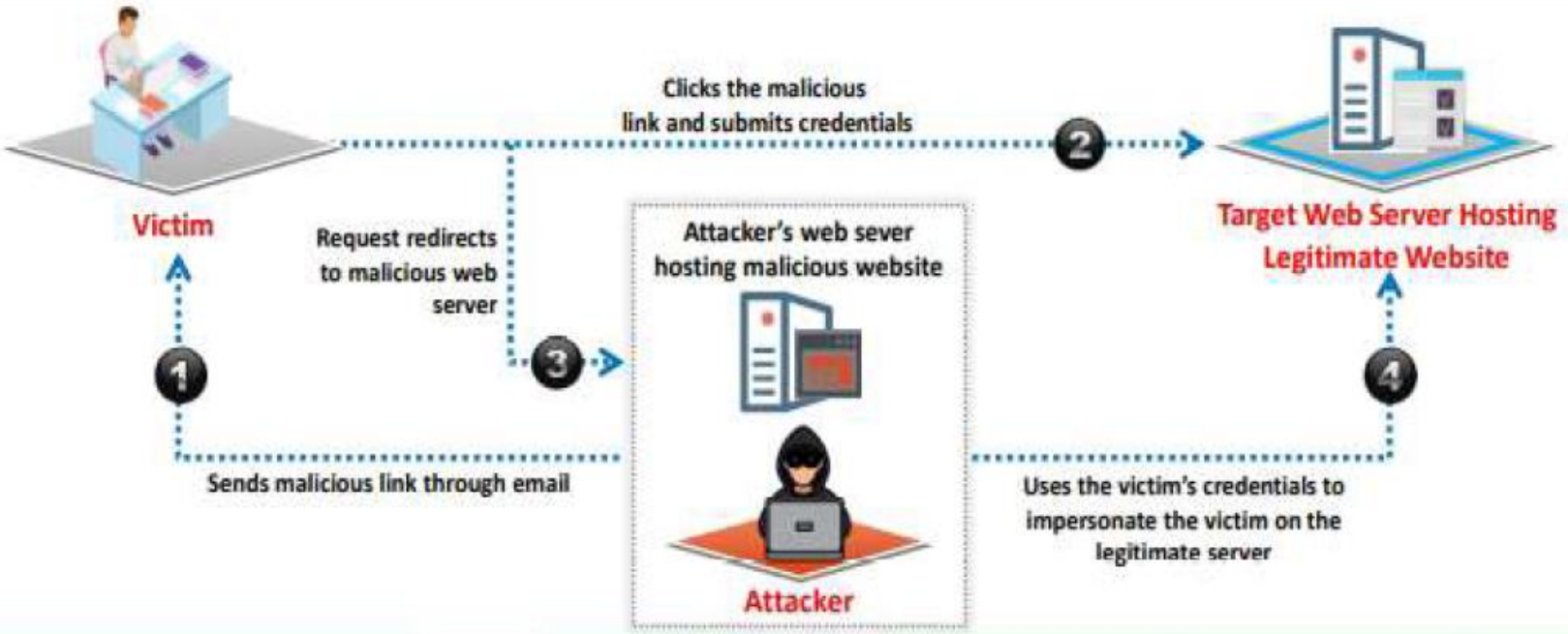
1. Man-in-the-Middle (MITM) attacks allow an attacker to access sensitive information by **intercepting and altering communications** between an end-user and web servers

2. An attacker **acts as a proxy** such that all communications between the user and web server passes through him



Phishing Attack

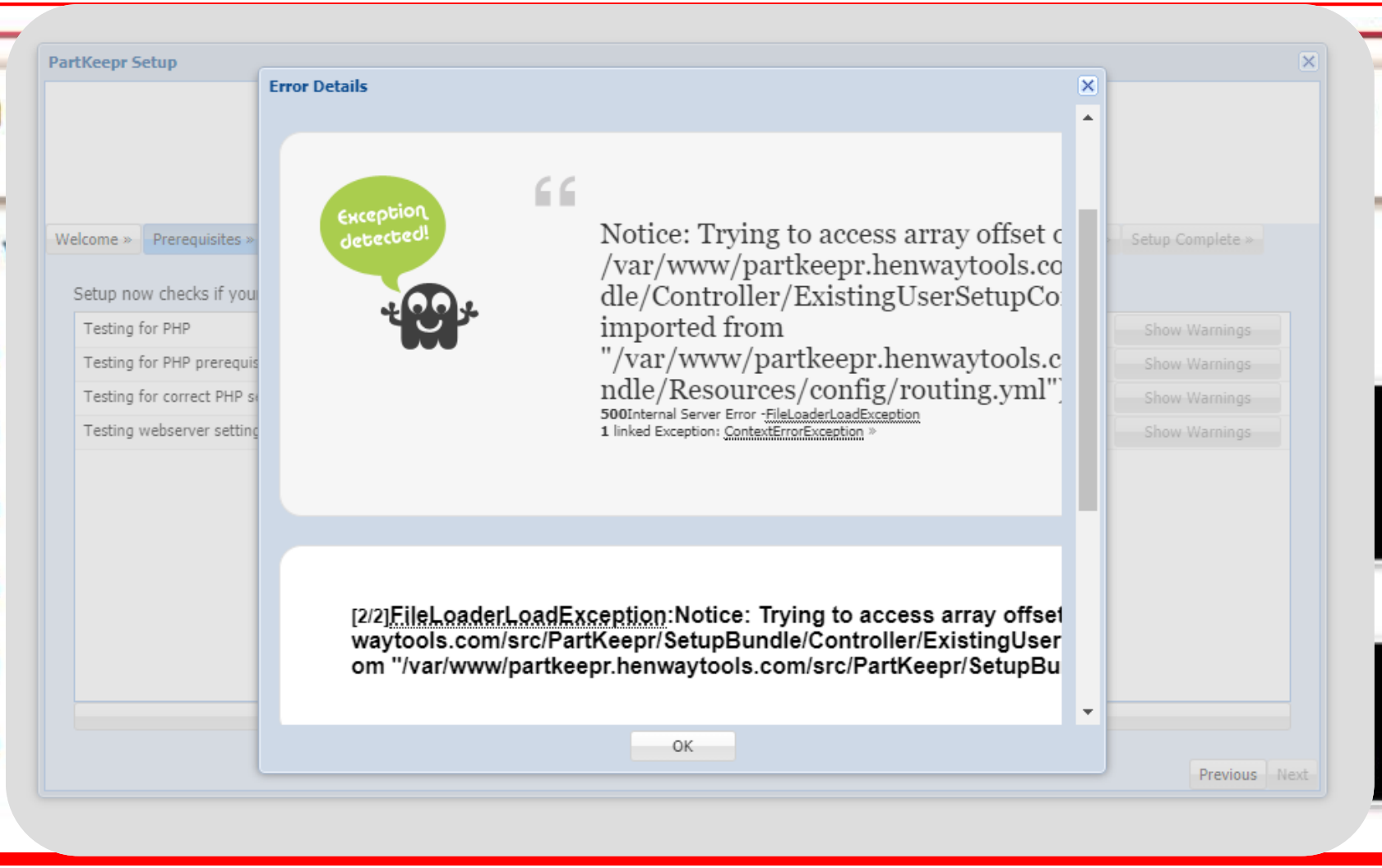
- The attacker tricks the user to submit **login details** for a website that looks legitimate, and redirects them to the malicious website hosted on the attacker's web server
- The attacker then **steals the credentials** entered and uses them to impersonate the user with the website hosted on the legitimate target server
- Attacker can then perform **unauthorized** or **malicious operations** on the target legitimate website



Website Defacement Attack

- Web defacement occurs when an intruder **maliciously alters the visual appearance of a web page** by inserting or substituting provocative, and frequently, offending data
- **Defaced pages expose visitors to some propaganda** or misleading information until the unauthorized changes are discovered and corrected
- Attackers use a variety of methods such as **MYSQL injection** to access a site in order to deface it

Web Server Misconfiguration Attack



Web Cache Poisoning Attack

What is it?

- Attackers manipulate the cache (a system used to store web pages for faster loading) to store harmful content instead of legitimate data.

How does it work?

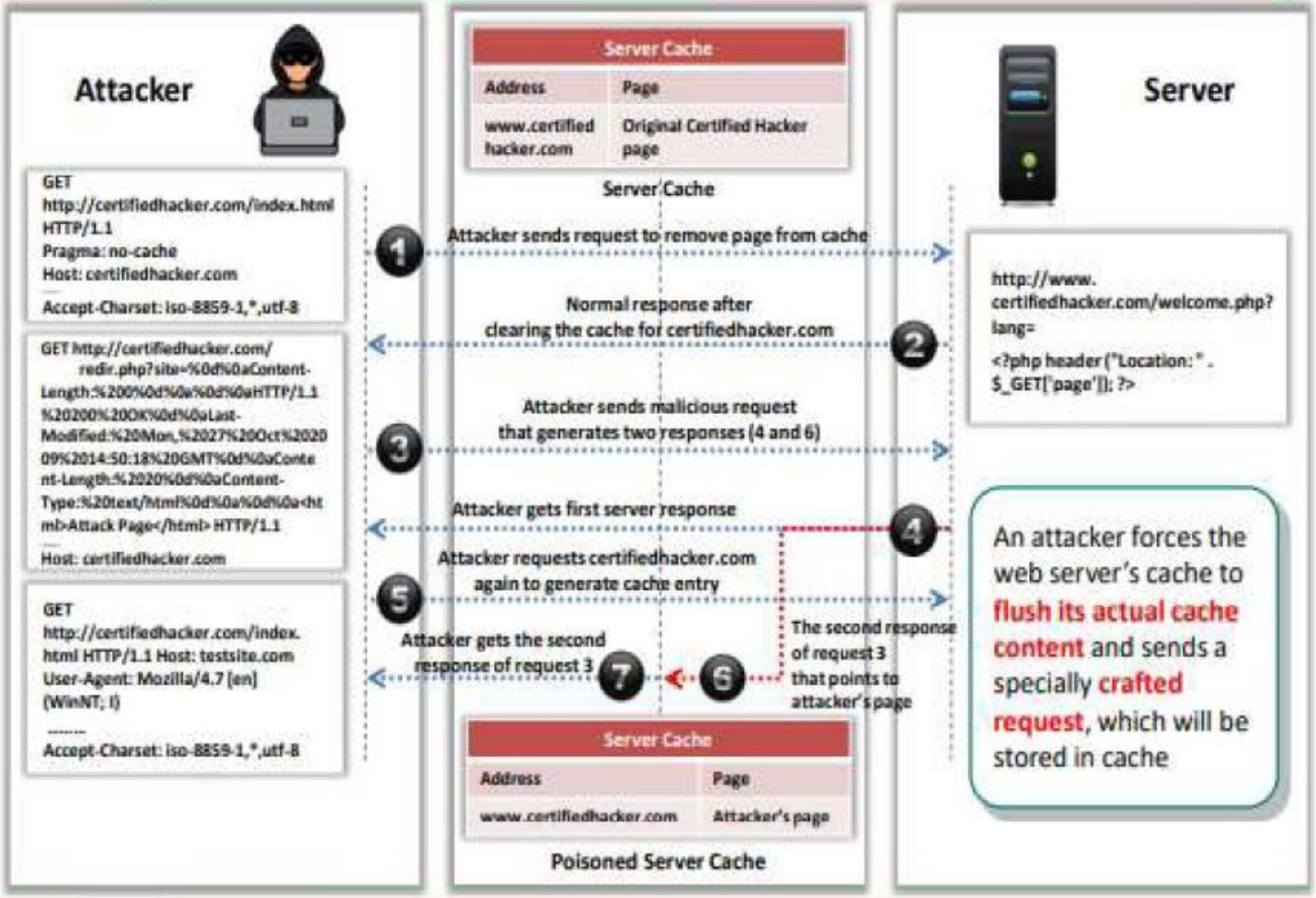
- The attacker sends a malicious request to the server. This request tricks the server into replacing the legitimate cached data with poisoned content.
- Users who access the site afterward will unknowingly receive the infected content from the cache instead of the original, secure page.

Why is it dangerous?

- It can lead to users being redirected to malicious websites, malware downloads, or other harmful actions, all without their knowledge.

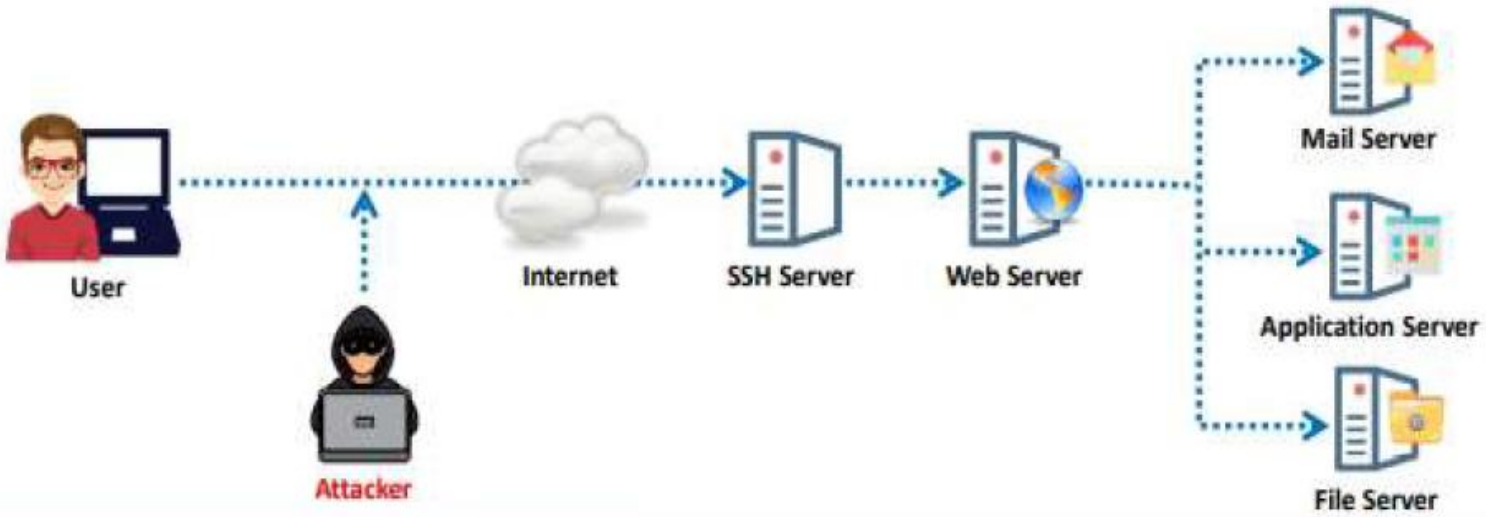
Web Cache Poisoning Attack

- Web cache poisoning attacks the **reliability of an intermediate web cache source**
- In this attack, the attackers **swap cached content** for a random URL with infected content
- Users of the web cache source can **unknowingly use the poisoned content** instead of the true and secured content when requesting the required URL through the web cache



SSH Brute Force Attack

1. SSH protocols are used to create an **encrypted SSH tunnel** between two hosts to transfer unencrypted data over an insecure network
2. Attackers can brute force SSH login credentials to gain **unauthorized access to an SSH tunnel**
3. SSH tunnels can be used to **transmit malwares** and other exploits to victims without being detected



Web Server Password Cracking

- An attacker tries to exploit weaknesses to hack well-chosen passwords
- The most common passwords found are password, root, administrator, admin, demo, test, guest, qwerty, pet names, etc.

Attacker mainly targets:

- SMTP servers
- Web shares
- SSH Tunnels
- Web form authentication cracking
- FTP servers

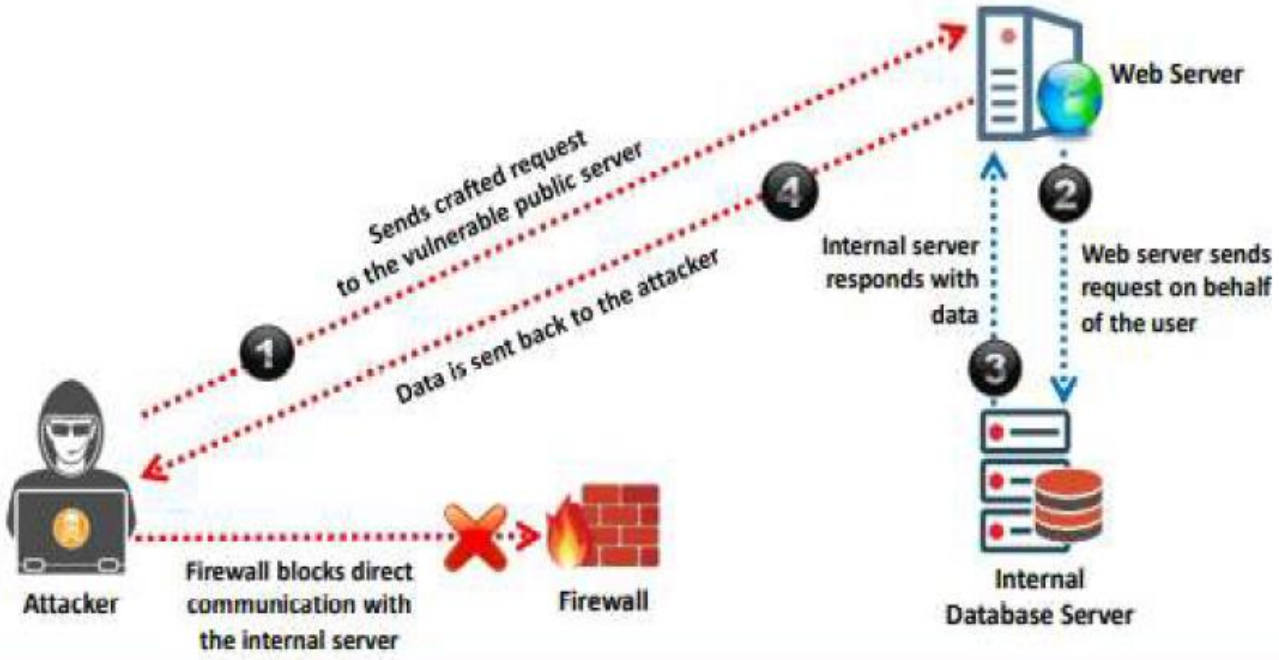
- Attackers use different methods such as social engineering, spoofing, phishing, using a Trojan Horse or virus, wiretapping, and keystroke logging

- Attackers usually begin hacking attempts with password cracking to prove to the web server that they are valid users

- Passwords can be cracked manually by guessing or by performing dictionary, brute force, and hybrid attacks using automated tools such as THC Hydra, and Ncrack

Server-Side Request Forgery (SSRF) Attack

- Attackers exploit SSRF vulnerabilities in a public web server to **send crafted requests** to the internal or back end servers
- Once the attack is successfully performed, the attackers can perform various activities such as **port scanning**, **network scanning**, **IP address discovery**, reading web server files, and bypassing host-based authentication



Q&A

Thankyou