OFFENSIVE SECURITY PORTFOLIO

Student Number: STU234412

Module Name : Offensive Security

Word Count: 3129 words

Part 1 : Mini Project

Discovering vulnerabilities in IP : 10.10.3.12

Gathering Phase

The Gathering Phase, also known as Footprinting or Reconnaissance, begins with verifying host activity as a crucial initial step in collecting information about potential vulnerabilities. Host discovery, a fundamental part of this phase in security testing, lists live hosts and removes unwanted targets, enabling focused scans and penetration tests (Jetty & Rahalkar, 2019).

To verify host availability, the following command is performed:

sudo nmap -sn 10.10.3.12

Figure 1. Initial step

```
root@ip-10-10-169-18:~# sudo nmap -sn 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:01 BST
Nmap scan report for 10.10.3.12
Host is up (0.00033s latency).
MAC Address: 02:AB:22:30:0C:19 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
root@ip-10-10-169-18:~#
```

The presence of an active host can be identified using the Nmap command, as it enables the detection of a target host's online status. Host discovery is a primary function of Nmap (based on the context of Jetty & Rahalkar, 2019 from the previous turn).

Liao et al. (2020) highlight Nmap as a widely used technique for scanning target hosts. Despite the existence of alternatives like Hping or Scanner, Nmap's firewall evasion methods and comprehensive scan types make it a primary choice for effective results. Following initial information gathering, the next step involves investigating firewall rules on the target IP address. A TCP ACK Scan is used to determine the presence of a firewall and identify which ports are not blocked.

The following command is used:

sudo nmap -sA 10.10.3.12

Figure 2. Unfiltered Ports

```
root@ip-10-10-169-18:~# sudo nmap -sA 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:03 BST
Nmap scan report for 10.10.3.12
Host is up (0.00032s latency).
Not shown: 991 filtered ports
PORT     STATE      SERVICE
21/tcp   unfiltered ftp
22/tcp   unfiltered ssh
80/tcp   unfiltered http
445/tcp  unfiltered microsoft-ds
631/tcp  unfiltered ipp
3000/tcp unfiltered ppp
3306/tcp unfiltered mysql
8080/tcp unfiltered http-proxy
8181/tcp unfiltered intermapper
MAC Address: 02:AB:22:30:0C:19 (Unknown)
```

The findings suggest the potential openness of the following ports, given the lack of configured firewall rules.

Port	State	Service
Port 21/tcp	unfiltered	ftp
Port 22/tcp	unfiltered	ssh
Port 80/tcp	unfiltered	http
Port 445/tcp	unfiltered	microsoft-ds
Port 631/tcp	unfiltered	ipp
Port 3000/tcp	unfiltered	ppp
Port 3306/tcp	unfiltered	mysql
Port 8080/tcp	unfiltered	http-proxy
Port 8181/tcp	unfiltered	intermapper

As Chandel (2018) notes, an unfiltered state implies port availability. Despite providing information about the port's state, Nmap cannot conclude whether it is open or closed in this scenario. Consequently, further scans are necessary to determine the port's status.

As the gathering phase continues, the next objective is to determine which ports are open and the associated services.

For it, the command to execute is :

sudo nmap -sV 10.10.3.12

Figure 3. Discovering open ports and its services

```
root@ip-10-10-169-18:~# sudo nmap -sV 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:05 BST
Nmap scan report for 10.10.3.12
Host is up (0.00024s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE     VERSION
21/tcp   closed ftp
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol
2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 02:AB:22:30:0C:19 (Unknown)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OS: Linux; CPE: cpe:/o:linux:li
nux_kernel
```

The figure 3 represents the following opened ports and its services:

PORT	STATE	SERVICE	VERSION
Port 22/tcp	Open	ssh	OpenSSH 6.6.1p1 Ubuntu 2Ubuntu2.13
Port 80/tcp	Open	http	Apache httpd 2.4.7
Port 445/tcp	Open	netbios-ssn	Samba smbd 3.X - 4.X(workgroup: workgroup)
Port 631/tcp	Open	ipp	CUPS 1.7
Port 3306/tcp	Open	Mysql	MYSQL unauthorized
Port 8080/tcp	Open	http	Jetty 8.17.v20120910

Following an initial TCP ACK scan that identified unfiltered ports, a subsequent version detection scan confirmed that ports 22, 80, 445, 631, 3306, and 8080 have no firewall rules blocking connection attempts. The absence of these rules exposes the network to unauthorized access, increasing the risk of data breaches, malware infections, illegitimate intrusions, and potential control of systems by cybercriminals. This can lead to the exfiltration of classified data, network destabilization, loss of productivity, and significant recovery costs (Joshua, 2024).

It is also important to discover which operating system is using our target IP address and it is main information.

For it the command to execute is :

sudo nmap -sS -O 10.10.3.12

Figure 4. Discover information about OS

```
root@ip-10-10-169-18:~# sudo nmap -sS -O 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:08 BST
Nmap scan report for 10.10.3.12
Host is up (0.00057s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 02:AB:22:30:0C:19 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.10 - 3.13
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit
```

The findings indicate that the Operating System is **Linux Kernel version 3**.

The following open ports, identified in the initial steps, are relevant to the four vulnerabilities that will be investigated further

- Port 22/tcp open ssh
- Port 80/tcp open http
- Port 445/tcp open microsoft-ds
- Port 631/tcp open ipp

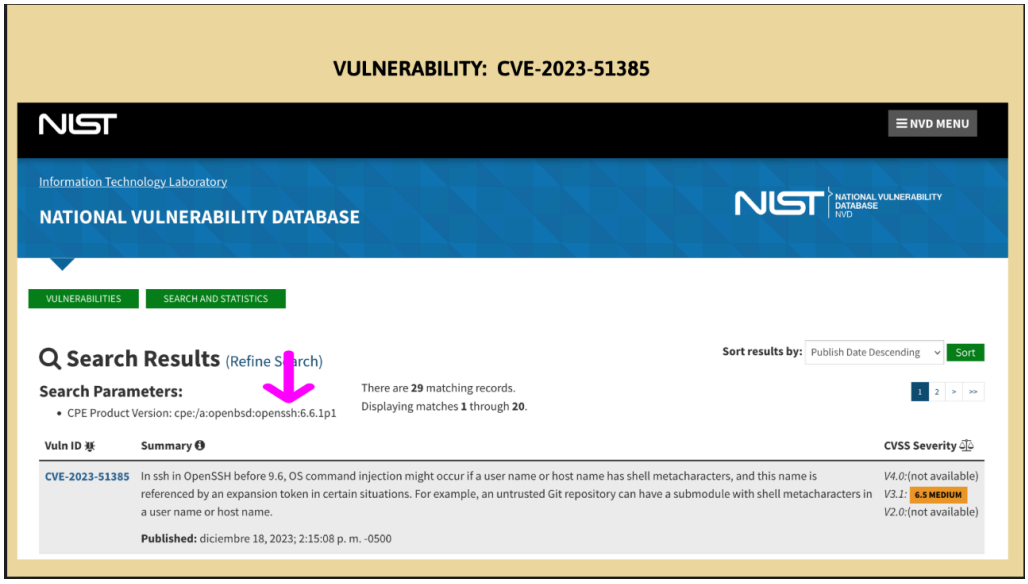
```
root@ip-10-10-169-18:~# sudo nmap -sS -O 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:08 BST
Nmap scan report for 10.10.3.12
Host is up (0.00057s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 02:AB:22:30:0C:19 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.10 - 3.13
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit
```

Port 22

Among the vulnerabilities detected in Port 22/tcp which its state is unfiltered, and it is an open port with a ssh service and an OpenSSH 6.6.1p1 version, the following vulnerabilities are the most remarkable:

a) In relation to its outdated version OpenSSH 6.6.1p1



CVE-2023-51385:

According to CVE (2023), a serious OS command injection vulnerability likely affects older OpenSSH versions like 6.6.1p1 and persists in versions before 9.6. This can occur if a username or hostname contains shell metacharacters that are referenced by an expansion token in specific situations, such as in an untrusted Git repository's submodule.

Vulnerabiliy: CVE-2023-38408

CVE-2023-38408	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009. **Published:** julio 19, 2023; 11:15:10 p. m. -0400	*V4.0:*(not available) *V3.1:* 9.8 CRITICAL *V2.0:*(not available)

CVE-2023-38408:

The Public-key Cryptography Standards # 11 highlighted in
ssh-agent in OpenSSH before 9.3p2 has a potentially insecure search path, conducting to remote execution if an agent is directed to an attacker-controlled system.

A search path which employs an unquoted element, in which the element incorporates whitespace or other separators, causing the product to retrieve resources in a parent path. Therefore, the possibility to elevate privileges is a solution against the circumstance in which a malicious attacker has access to the file system. (CWE, 2006)

b) In relation to cryptographic algorithms that the SSH service on port 22 supports, the use of the Nmap Scripting Engine (NSE): ssh2-enum-algos script is crucial.

The following command is used:

sudo nmap - -script ssh2-enum-algos -p 22 10.10.3.12

Weak Exchange Algorithms & Weak Encryption Algorithms

```
root@ip-10-10-169-18:~# sudo nmap --script ssh2-enum-algos -p 22 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:10 BST
Nmap scan report for 10.10.3.12
Host is up (0.00011s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (8)
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (4)
|       ssh-rsa
|       ssh-dss
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (16)
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       arcfour256
```

Weak Mac Algorithms

```
      aes128-gcm@openssh.com
      aes256-gcm@openssh.com
      chacha20-poly1305@openssh.com
      aes128-cbc
      3des-cbc
      blowfish-cbc
      cast128-cbc
      aes192-cbc
      aes256-cbc
      arcfour
      rijndael-cbc@lysator.liu.se
  mac_algorithms: (19)
      hmac-md5-etm@openssh.com
      hmac-sha1-etm@openssh.com
      umac-64-etm@openssh.com
      umac-128-etm@openssh.com
      hmac-sha2-256-etm@openssh.com
      hmac-sha2-512-etm@openssh.com
      hmac-ripemd160-etm@openssh.com
      hmac-sha1-96-etm@openssh.com
      hmac-md5-96-etm@openssh.com
      hmac-md5
      hmac-sha1
      umac-64@openssh.com
      umac-128@openssh.com
      hmac-sha2-256
      hmac-sha2-512
      hmac-ripemd160
      hmac-ripemd160@openssh.com
```

Weak Exchange Algorithms: Diffie-Hellman-group1-sha1

The ssh2-enum-algos script identifies weak key exchange algorithms, including the outdated and vulnerable diffie-hellman-group1-sha1, which can be susceptible to pre-computation attacks, potentially allowing attackers to compromise future sessions if sufficient traffic is collected. This algorithm uses weak 768-bit keys and lacks forward secrecy, creating a security risk (Villanueva, no date).

Weak Encryption algorithms aes128-cbc

Furthermore, the weak encryption algorithm aes128-cbc (Advanced Encryption Standard with a 128-bit key in Cipher Block Chaining mode) has been detected. As a symmetric encryption algorithm supported by SSH implementations like OpenSSH 6.6.1p1, its CBC mode has known weaknesses. According to Dell Technologies (2023), the CBC ciphers aes128-cbc, aes192-cbc, and aes256-cbc are considered insecure for use.

c) In relation to enumerating SSH authentication method, ssh-auth-methods script is performed.

The following command is used:

sudo nmap - -script ssh-auth-methods -p 22 10.10.3.12

```
root@ip-10-10-169-18:~# sudo nmap --script ssh-auth-methods -p 22 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:17 BST
Nmap scan report for 10.10.3.12
Host is up (0.000096s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
MAC Address: 02:AB:22:30:0C:19 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

The findings reveals that the SSH server on open port 22 permits client authentication using both Password and Publickey methods.

Password Authentication

Password authentication poses vulnerabilities to brute-force and dictionary attacks, as well as keylogging and the exploitation of weak passwords. According to Schrader (2025), OpenSSH servers are easily discoverable, allowing attackers to attempt common password combinations and username guessing.

Publickey Authentication

Publickey authentication is generally considered more secure than password authentication because it uses cryptographic keys instead of passwords for verification.

Port 80

The following notable vulnerabilities were detected in the unfiltered and open Port 80/ http, which is running an Apache httpd 2.4.7 version:

a) Missing security headers which expose the target Ip to various web attacks.

The following command is used:

sudo nmap - -script http-security-headers -p 80 10.10.3.12

```
root@ip-10-10-169-18:~# sudo nmap --script http-security-headers -p 80 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:20 BST
Nmap scan report for 10.10.3.12
Host is up (0.000083s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-security-headers:
MAC Address: 02:AB:22:30:0C:19 (Unknown)
```

The Nmap script http-security-headers revealed that the web server on port 80 does not implement security-related HTTP response headers, creating a gap in defense and potentially increasing the web application's vulnerability to client-side attacks. Strong (2024) emphasizes that this lack of headers can reduce the application's resistance to man-in-the-middle attacks, facilitating the interception of communication and potential theft of sensitive data.

The OWASP Top Ten list (2021) identifies security misconfigurations as a significant risk, including missing security protocols, incorrectly set cloud permissions, insecure default configurations in various components, and the failure to implement or properly configure security headers.

b) Outdated version Apache httpd 2.4.7 :

The following command is used:

sudo nmap - -script http-server-header -p 80 10.10.3.12

```
root@ip-10-10-169-18:~# sudo nmap --script http-server-header -p 80 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:22 BST
Nmap scan report for 10.10.3.12
Host is up (0.00012s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-server-header: Apache/2.4.7 (Ubuntu)
MAC Address: 02:AB:22:30:0C:19 (Unknown)
```

In this figure, open port 80/tcp http service has a version named Apache/2.4.7 which confirms the exact version associated with this particular release:

CVE-2021-44224

Apache HTTP Server 2.4.7 is vulnerable to a crash caused by a crafted URI sent to an httpd configured as a forward proxy. Configurations mixing forward and reverse proxy declarations can allow requests to be directed to a declared Unix Domain Socket endpoint, leading to the dereferencing of a null pointer (CWE, 2006).

c) Directory and File enumeration Scan and vulnerabilities found:

The following command is used:

sudo nmap - - script http-enum -p 80 10.10.3.12

```
root@ip-10-10-169-18:~# sudo nmap --script http-enum -p 80 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:24 BST
Nmap scan report for 10.10.3.12
Host is up (0.000089s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /: Root directory w/ listing on 'apache/2.4.7 (ubuntu)'
|   /phpmyadmin/: phpMyAdmin
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
MAC Address: 02:AB:22:30:0C:19 (Unknown)
```

The File Enumeration Scan revealed several vulnerabilities: the enabled directory listing in the root directory (/) exposes sensitive files and server structure; the presence of /phpmyadmin/ suggests a potential security risk due to outdated or misconfigured installations; and the identification and enabled directory listing of the /uploads/ directory on the Apache server (version 2.4.7 on Ubuntu) is a high-risk vulnerability, allowing attackers to view and potentially exploit uploaded files, including malicious scripts.

Port 445

Port 445/tcp has an unfiltered state, it is an open port with a netbios-ssn service and Samba smbd 3.X - 4.X (Workgroup: Workgroup) version. The most remarkable vulnerabilities are the following:

a) Vulnerabilities related to its version:
In a previous scan of the target IP, its version detected does not provide a complete information. Information about the SMB service can be found using nmap scripts.

The following command is used:

sudo nmap - -script smb-os-discovery -p 445 10.10.3.12

```
root@ip-10-10-169-18:~# sudo nmap --script smb-os-discovery -p 445 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:25 BST
Nmap scan report for 10.10.3.12
Host is up (0.000085s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:AB:22:30:0C:19 (Unknown)

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: metasploitable3-ub1404
|   NetBIOS computer name: METASPLOITABLE3-UB1404\x00
|   Domain name: \x00
|   FQDN: metasploitable3-ub1404
|_  System time: 2025-05-08T10:25:52+00:00
```

In this figure, open port 445/tcp netbios-ssn service has a version named Samba 4.3.11- Ubuntu which confirms the exact version associated with this particular release:

CVE-2016-2119

Samba versions prior to 4.4.5 contain a vulnerability that allows Man-in-the-Middle (MITM) attacks to bypass client-signing protection, enabling attackers to originate spoofed SMB2 and SMB3 servers.

Additionally, an attacker can downgrade the required signing for an SMB2/3 client connection by injecting the SMB2_SESSION_FLAG_IS_GUEST or SMB2_SESSION_FLAG_IS_NULL flags, allowing an attacker connected to a Samba server to impersonate it and provide malicious output (Samba, 2016).

b) In relation to its nature: unfiltered Port 445

```
PORT     STATE      SERVICE
21/tcp   unfiltered ftp
22/tcp   unfiltered ssh
80/tcp   unfiltered http
445/tcp  unfiltered microsoft-ds
```

Port 445 is the main communication channel for the SMB protocol, enabling file and printer sharing, and inter-process communication in Windows and Samba networks. The lack of filtering on this port exposes the SMB service to network attacks and facilitates lateral movement, where attackers gain initial access through a less critical system to target valuable resources within the network (ISDecisions, n.d).

c) In relation to the security mode of the SMB server, the script named smb-security-mode.nse depicts user-level, share-level and authentication level.

The following command is used:

sudo nmap - -script smb-security-mode -p 445 10.10.3.12

```
root@ip-10-10-169-18:~# sudo nmap --script smb-security-mode -p 445 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:28 BST
Nmap scan report for 10.10.3.12
Host is up (0.00013s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:AB:22:30:0C:19 (Unknown)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

The findings revealed a high-severity vulnerability: SMB message signing is disabled, a dangerous default configuration that makes the system susceptible to Man-in-the-Middle (MITM) attacks. Without message signing, attackers can intercept and alter SMB traffic undetected, leading to data manipulation, command injection, and session hijacking. The combination of an open and unfiltered port 445 with the identified Samba version (smbd 4.3.11) further exacerbates this vulnerability by allowing easy connection to SMB services, facilitating MITM attacks.

Port 631

Port 631/tcp is unfiltered and open, running the IPP service with CUPS version 1.7. A significant vulnerability associated with CUPS 1.7 can be detected using the vulners Nmap script.

The following is the command used:

sudo nmap -sV - -script vulners -p 631 10.10.3.12

```
root@ip-10-10-169-18:~# sudo nmap -sV --script vulners -p 631 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:31 BST
Nmap scan report for 10.10.3.12
Host is up (0.00017s latency).

PORT    STATE SERVICE VERSION
631/tcp open  ipp     CUPS 1.7
|_http-server-header: CUPS/1.7 IPP/2.1
| vulners:
|   cpe:/a:apple:cups:1.7:
|       CVE-2014-5031   5.0     https://vulners.com/cve/CVE-2014-5031
|       CVE-2014-2856   4.3     https://vulners.com/cve/CVE-2014-2856
|       CVE-2014-5030   1.9     https://vulners.com/cve/CVE-2014-5030
|       CVE-2014-3537   1.2     https://vulners.com/cve/CVE-2014-3537
|_      CVE-2013-6891   1.2     https://vulners.com/cve/CVE-2013-6891
MAC Address: 02:AB:22:30:0C:19 (Unknown)
```

This process queries the Vulners database for vulnerabilities associated with "CUPS 1.7" and the "ipp" service, revealing notable vulnerabilities, including the following:

CVE-2014-5031

A vulnerability exists in CUPS web interfaces prior to version 2.0 due to the failure to verify the existence of world-readable files controlling access permissions and security settings, allowing remote attackers to obtain confidential information.

Part 2 : Report

Vulnerability Assessment Report

Date: May 7, 2025
Target: 10.10.3.12
Conducted By: Ivonne Benites

Executive Summary

Assessment Scope and Objectives:

This vulnerability assessment involved an initial information gathering phase to identify active hosts, firewall configurations, open ports, services, and operating systems on the target network. The primary objective is to identify potential vulnerabilities that could be exploited.

Purpose of the Vulnerability Scanning:

Map the attack surface of the target network, and detect potential entry points.

Scope of the Scanning:

The scope of the scanning included host discovery on 10.10.3.12,
firewall analysis on 10.10.3.12, service and version detection on 10.10.3.12 and 10.10.3.12, operating system detection on 10.10.3.12, and initial vulnerability scanning on specific ports (22, 80, 445, 631).

The assessment began with host discovery using `nmap -sn`.
Then, firewall rules were investigated using a TCP ACK scan `nmap -sA`.
Open ports and services were identified using version detection scans `nmap -sV`.
Operating system detection was performed using a SYN scan `nmap -sS -O`.
Finally, initial vulnerability analysis was conducted on identified open ports using Nmap scripts: `ssh2-enum-algos`, `http-security-headers`, `http-server-header`, `http-enum`, `smb-os-discovery`, `smb-security-mode`, `vulners`.

Findings Summary:

The initial gathering phase revealed several potential areas of concern.
An active host was identified at 10.10.3.12
The TCP ACK scan on 10.10.3.12 indicated several unfiltered ports
(22, 80, 445, 631, 3306, 8080), suggesting a lack of restrictive firewall rules.

The operating system for 10.10.3.12 was identified as Linux Kernel version 3.

Further investigation into specific open ports revealed:

Port 22 (SSH):
An outdated OpenSSH version 6.6.1p1 which has vulnerabilities known as CVE-2023-51385 and CVE-2023-38408.

The port 22 shows Weak Key Exchange Algorithms such as **diffie-hellman-group1-sha1**, Weak Encryption Algorithms such as **aes128-cbc**, and enabled password authentication.

Port 80 (HTTP):
Missing security headers were found, an outdated Apache httpd version (2.4.7 potentially vulnerable to CVE-2021-44224), and enabled directory listing with exposed sensitive directories like `/phpmyadmin/` and `/uploads/`.

Port 445 (SMB):
An identified Samba version (4.3.11-Ubuntu) vulnerable to CVE-2016-2119,
an unfiltered port exposing the SMB service, and disabled SMB message signing.

Port 631 (IPP/CUPS):
CUPS version 1.7, potentially vulnerable to CVE-2014-5031.

The overall risk level based on these initial findings is **Medium-High**, requiring further in-depth vulnerability analysis and potential exploitation attempts.
The lack of firewall rules and outdated software versions are critical issues that need to be addressed.

Remediation Summary:

Enforce strong firewall rules to restrict access to non-essential ports.
Upgrade all identified outdated software (OpenSSH, Apache httpd, Samba, CUPS)
Implement strong security headers on the web server.
Disable directory listing where not necessary and secure sensitive directories.
Enable SMB message signing.
Disable password authentication for SSH.
Enforce public key authentication.

Vulnerability Assessment Walkthrough

Target: 10.10.3.12
Date: May 7, 2025
Assessor: Ivonne Benites
Objective: To identify potential vulnerabilities on the target system 10.10.3.12

Phase 1: Reconnaissance and Information Gathering

Objective: To gather initial information about the target system, including port filtering status, vulnerabilities caused by outdated versions,

Steps:

1. Port Filtering Scan:

Performed a TCP SYN scan to determine the filtering status of common port on the target.

The following command is used :

sudo nmap -sA 10.10.3.12

Evidence Collected:

```
root@ip-10-10-169-18:~# sudo nmap -sA 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:03 BST
Nmap scan report for 10.10.3.12
Host is up (0.00032s latency).
Not shown: 991 filtered ports
PORT     STATE      SERVICE
21/tcp   unfiltered ftp
22/tcp   unfiltered ssh
80/tcp   unfiltered http
445/tcp  unfiltered microsoft-ds
631/tcp  unfiltered ipp
3000/tcp unfiltered ppp
3306/tcp unfiltered mysql
8080/tcp unfiltered http-proxy
8181/tcp unfiltered intermapper
MAC Address: 02:AB:22:30:0C:19 (Unknown)
```

2. Basic Port Scan:

Performed an initial TCP SYN scan to identify open ports on the target.

The following command is used:

sudo nmap -sV 10.10.3.12

Evidence Collected:

```
root@ip-10-10-169-18:~# sudo nmap -sV 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:05 BST
Nmap scan report for 10.10.3.12
Host is up (0.00024s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE     VERSION
21/tcp   closed ftp
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol
2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 02:AB:22:30:0C:19 (Unknown)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OS: Linux; CPE: cpe:/o:linux:li
nux_kernel
```

Nmap scan report showing port 445/tcp as open and 631/tcp as open.

3. Service Version Detection:

Performed service version detection to identify the services running on the open ports.

Command Used:

sudo nmap -sV - - script vulnerable -p 631 10.10.3.12
sudo nmap - -script smb-os-discovery -p 445 10.10.3.12

Evidence Collected:

631/tcp open ipp CUPS 1.7

```
root@ip-10-10-169-18:~# sudo nmap -sV --script vulners -p 631 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:31 BST
Nmap scan report for 10.10.3.12
Host is up (0.00017s latency).

PORT    STATE SERVICE VERSION
631/tcp open  ipp     CUPS 1.7
|_http-server-header: CUPS/1.7 IPP/2.1
| vulners:
|   cpe:/a:apple:cups:1.7:
|       CVE-2014-5031   5.0     https://vulners.com/cve/CVE-2014-5031
|       CVE-2014-2856   4.3     https://vulners.com/cve/CVE-2014-2856
|       CVE-2014-5030   1.9     https://vulners.com/cve/CVE-2014-5030
|       CVE-2014-3537   1.2     https://vulners.com/cve/CVE-2014-3537
|_      CVE-2013-6891   1.2     https://vulners.com/cve/CVE-2013-6891
MAC Address: 02:AB:22:30:0C:19 (Unknown)
```

445/tcp open netbios-ssn Samba 4.3.11 - Ubuntu

```
root@ip-10-10-169-18:~# sudo nmap --script smb-os-discovery -p 445 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:25 BST
Nmap scan report for 10.10.3.12
Host is up (0.000085s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:AB:22:30:0C:19 (Unknown)

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: metasploitable3-ub1404
|   NetBIOS computer name: METASPLOITABLE3-UB1404\x00
|   Domain name: \x00
|   FQDN: metasploitable3-ub1404
|_  System time: 2025-05-08T10:25:52+00:00
```

Nmap scan report showing:

The nmap scan report depicts that about 6 ports are unfiltered and its state is open. Additionally, port 631 presents an outdated version CUPS 1.7 with CVE vulnerabilities related to it. Moreover, port 445 shows a version which is vulnerable to several type of attacks such as man-in-the-middle attacks and network attacks.

Phase 2: Vulnerability Scanning and Analysis

Objective: To identify potential vulnerabilities related to the identified services.

Steps Undertaken:

1. SMB Vulnerability Scanning (Initial - Specific CVE):
Attempted to scan for CVE-2017-7494 (SambaCry) using the specific Nmap script.

Command Used:

```
sudo nmap --script smb-vuln-cve-2017-7494.nse  -p  445  10.10.3.12
```

Evidence Collected:

```
root@ip-10-10-169-18:~# sudo nmap --script smb-vuln-cve-2017-7494.nse -p 445 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:42 BST
Nmap scan report for 10.10.3.12
Host is up (0.000085s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:AB:22:30:0C:19 (Unknown)
```

Nmap output indicating that the script ran but did not report the target as vulnerable.

2. SMB Vulnerability Scanning:

A broader scan using all SMB vulnerability scripts was executed.

Command Used:

```
sudo nmap --script smb-vuln* -p 445 10.10.3.12
```

Evidence Collected:

```
root@ip-10-10-169-18:~# sudo nmap --script smb-vuln* -p 445 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:46 BST
Nmap scan report for 10.10.3.12
Host is up (0.00013s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:AB:22:30:0C:19 (Unknown)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of
 service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerabi
lity was discovered by Ron Bowes
|       while working on smb-enum-sessions.
```

3. General Vulnerability Scanning:

A general vulnerability scan using the vuln category of Nmap scripts was executed.

Command Used:

sudo nmap --script vuln -p 445 10.10.3.12

Evidence Collected:

```
root@ip-10-10-169-18:~# sudo nmap --script vuln -p 445 10.10.3.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 11:48 BST
Nmap scan report for 10.10.3.12
Host is up (0.00022s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 02:AB:22:30:0C:19 (Unknown)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of
 service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerabi
lity was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_
```

Impact & Remediation advice and countermeasures to improve the security posture for each vulnerability mentioned

Port 22

Vulnerability: CVE-2023-51385

Attackers exploiting OS Command Injection (CWE-78) can execute unauthorized system commands by injecting shell meta characters, leading to product disablement, unauthorized data access and modification, system crashes, and instability. Injected commands can also be used for persistence and to conceal malicious activity, making it appear as if actions originated from the application or its owner.

Countermeasures:

Upgrade to OpenSSH 9.6+ to fix this vulnerability; temporary measures include limiting username/hostname sources, using reliable libraries, encoding output, validating input characters, reducing error details, applying firewalls, and minimizing SSH daemon privileges.

Vulnerability: CVE-2023-38408

The impact of this vulnerability is the execution of unauthorized code or commands which damage the principles of confidentiality, integrity, and availability.

Countermeasures:

Preventing OS Command Injection involves properly quoting search paths, implementing strict input validation with an allowlist (checking length, category, range, syntax, consistency, business rules), and decoding/canonicalizing inputs once.

Vulnerability: Diffie-Hellman-group1-sha1

The weak key size of diffie-hellman-group1-sha1 in older OpenSSH versions like 6.6.1p1 allows MITM attackers to potentially record and decrypt SSH sessions by computing the shared and session keys, resulting in insecure communication.

Countermeasures:

Disabling unsafe key exchange algorithms like diffie-hellman-group1-sha1 on SSH port 22/tcp is the most effective security measure (Villanueva, no date).

Vulnerability: aes128-cbc

Using aes128-cbc can lead to Padding Oracle Attacks, potentially allowing attackers to decrypt ciphertext and steal sensitive information like passwords and tokens, compromising web application security (confidentiality, integrity, availability).

Countermeasures:

An effective mitigation strategy is to set up the use of CTR mode rather than CBC mode. According to IBM (2025), a GCM cipher mode encryption can be configured instead of using CBC mode.

Vulnerability: Password Authentication & Publicly Authentication

Password authentication is vulnerable to brute-force and dictionary attacks, often automated by bots (IBM, 2025).

Disabling password authentication and using public key authentication can prevent these attacks.

Countermeasures:

Security measures include disabling password authentication and root login, enabling public key authentication, reloading SSH, regularly monitoring logs for attacks and suspicious logins, and changing the default SSH port (IBM, 2025).

Port 80

Vulnerability: Impact of missing security headers:

The absence of security headers negatively impacts website security, increasing vulnerability to attacks like HTTPS downgrade exploits. Additionally, it can lower search engine rankings, as major search engines such as Google favor secure websites (Strong, 2024).

Countermeasures:

Regular security scans are crucial for finding missing security headers, like HSTS (identified via browser tools), which protects against MITM. Other measures include segmented architecture, patch updates, cloud permission checks, and removing unused features (Strong, 2024; OWASP, 2021).

Vulnerability: CVE-2021-44224

Apache httpd 2.4.7 has multiple security vulnerabilities (CVE, 2017) including DoS, unauthorized code execution, memory manipulation, XSS, CSRF, privilege escalation, information leakage, and authentication bypass.

Countermeasures:

The main security recommendation is to upgrade Apache HTTP Server and implement pointer validation, proper locking, safer language consideration, and rigorous input validation (CWE, 2006).

Vulnerability: Directory and File Enumeration Scan

During reconnaissance, attackers gather network infrastructure details like IP addresses and open ports to target systems and identify exploitable vulnerabilities for infiltration (Hariharasubramanian, 2025).

Countermeasures:

Mitigation of enumeration attacks involves understanding their methods and implementing protective measures like firewalls, strong passwords with MFA, least privilege, IDS for detection, network segmentation, and encryption (Meritshot, n.d.).

Port 445

Vulnerability: outdated Samba 4.3.11

CVE-2016-2019 enables security bypass via code injection affecting authentication, potentially leading to remote exploitation, unauthorized access, control flow modification, and data compromise; detection is hard due to concealed actions (CWE, 2006).

Countermeasures:

Mitigating CVE-2016-2019 code injection involves avoiding dynamic code generation, using sandboxes, employing input allowlists, and utilizing static analysis and taint propagation prevention (CWE, 2006).

Vulnerability: Unfiltered Port 445

Unfiltered port 445 allows unrestricted SMB interaction, creating targets for exploits and credential-based attacks leading to unauthorized access and data collection; its combination with specific Samba versions is a major security risk.

Countermeasures:

Kelley (2023) states that preventing attacks on unfiltered port 445 includes blocking it at the perimeter (if safe), network segmentation, strong passwords, service inventory, strong file permissions, alert monitoring, and trusted IP access via firewalls.

Vulnerability: Security mode of SMB server

Disabling SMB message signing exposes communication to undetectable MITM attacks and potential session hijacking (based on the context of previous turns).

Counter Measures:

Implementing and enforcing strong SMB message signing on both client and server is crucial to mitigate MITM attacks and ensure SMB communication integrity.

Port 631

Vulnerability: CVE-2014-5031

Path traversal allows attackers to read/overwrite files and bypass security, potentially enabling unauthorized code execution (Red Hat, 2024).

Countermeasures:

The main mitigation strategy is to upgrade the fixed version to reduce risks. Moreover, enforce temporary workarounds can secure the system.(Vulert, 2014)

References

Chandel, R. (2018). *Nmap for Pentester: Port Status*. [online] *Hacking Articles*. Available at: https://www.hackingarticles.in/nmap-for-pentester-port-status/. Accessed 8 May 2025.

CWE (2006). CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'). [online] Available at: https://cwe.mitre.org/data/definitions/78.html.Accessed 8 May 2025.

CVE (2023). *CVE-2023-51385*. [online] Available at: https://www.cve.org/CVERecord?id=CVE-2023-51385.Accessed 8 May 2025.

Dell Technologies (2022). *PowerScale: SSH Key Exchange Algorithm is flagged by security vulnerability scanners: diffie-hellman-group1-sha1*. [online] Available at: https://www.dell.com/support/kbdoc/en-us/000195307/powerscale-ssh-key-exchange-algorithm-is-flagged-by-security-vulnerability-scanners-diffie-hellman-group1-sha1. Accessed 8 May 2025.

Dell Technologies (2022). *PowerScale: SSH Key Exchange Algorithm is flagged by security vulnerability scanners: diffie-hellman-group1-sha1*. [online] Available at: https://www.dell.com/support/kbdoc/en-us/000195307/powerscale-ssh-key-exchange-algorithm-is-flagged-by-security-vulnerability-scanners-diffie-hellman-group1-sha1. Accessed 8 May 2025.

Hariharasubramanian, N. (2025). *Understanding Network Enumeration: Essential Techniques and Tools*. [online] *Fidelis Cybersecurity*. Available at: https://fidelissecurity.com/cybersecurity-101/learn/network-enumeration/. Accessed 8 May 2025.

IBM (2025). *CBC ciphers and SSH vulnerabilities*. [online] Available at: https://www.ibm.com/docs/en/guardium-insights/3.x?topic=setup-cbc-ciphers-ssh-vulnerabilities. Accessed 8 May 2025.

Jetty, S. and Rahalkar, S. (2019). Securing Network Infrastructure: Discover practical network security with Nmap and Nessus 7. [online] Available at: https://tinyurl.com/nwatmmph. Accessed 8 May 2025.

Joshua, C. (2024). *What is a firewall? What it does? and why you need it?* [online] *Norton*. Available at: https://us.norton.com/blog/privacy/firewall. Accessed 8 May 2025.

Liao, S. et al. (2020). 'A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments'. In *2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Chongqing, China, pp. 64-71. doi: 10.1109/CyberC49757.2020.00020.

Meritshot (n.d.). *Enumeration in Cybersecurity*. [online] Available at: https://www.meritshot.com/enumeration-in-cyber-security/. Accessed 8 May 2025.

OWASP Top 10:2021 (2021). *A05:2021 – Security Misconfiguration*. [online] Available at: https://owasp.org/Top10/A05_2021-Security_Misconfiguration/ Accessed 8 May 2025.

Samba (2016). *Samba 4.3 Features added/changed*. [online] Available at: https://wiki.samba.org/index.php/Samba_4.3_Features_added/changed#Samba_4.3.11. Accessed 8 May 2025.

Strong, A. (2024). *Understanding the Missing HSTS Header Vulnerability*. [online] *Trace Security Blog*. Available at: https://www.tracesecurity.com/blog/articles/understanding-the-missing-hsts-header-vulnerability.Accessed 8 May 2025.

Villanueva, J.C. (n.d.). *Fixing SSH/SFTP client connection issues involving Diffie-Hellman-Group1-SHA1*. [online] Available at: https://www.jscape.com/blog/what-you-need-to-know-about-diffie-hellman-group1-sha1-vulnerability. Accessed 8 May 2025.