**INFORMATION SECURITY**



**Session 2023 - 2027**

**Submitted by:**

Sumaira Hafeez 2023-CS-1

**Supervised by:**

Mam Faiza Iqbal

**Course:**

Information Security

Department of Computer Science

**University of Engineering and Technology**

**Lahore Pakistan**

Contents

[**RISK MANAGEMENT AND DDOS ATTACK** 2](#_Toc195183310)

[ **Vulnerability scanning and Risk Evaluation:** 2](#_Toc195183311)

[**1.** **Discover Network Hosts:** 2](#_Toc195183312)

[**2.** **Host Discovery:** 2](#_Toc195183313)

[**3.** **Scan targets for open ports:** 3](#_Toc195183314)

[**4.** **Web Vulnerability Scan:** 3](#_Toc195183315)

[Vulnerabilities Found 4](#_Toc195183316)

[1. Missing X-Frame-Options Header 4](#_Toc195183317)

[2. Missing X-Content-Type-Options Header 4](#_Toc195183318)

[3. Server Banner Changed (AkamaiNetStorage → AkamaiGHost) 4](#_Toc195183319)

[4. Login Attempt with Common Credentials 4](#_Toc195183320)

[6. Error Limit Reached / DNS Failure 4](#_Toc195183321)

[ **Distributed Denial of Service Attack** 5](#_Toc195183322)

[**1.** **XERSES Compilation** 5](#_Toc195183323)

[**2.** **DDOS attack** 6](#_Toc195183324)

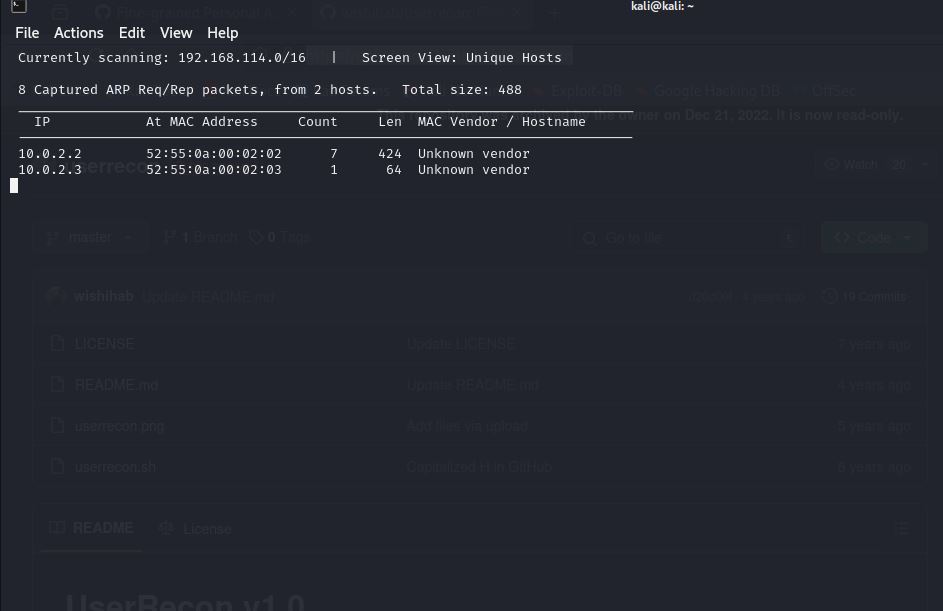
[ **Reflection:** 6](#_Toc195183325)

# **RISK MANAGEMENT AND DDOS ATTACK**

# **Vulnerability scanning and Risk Evaluation:**

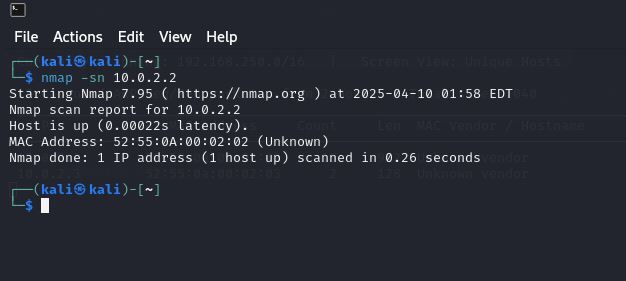
## **Discover Network Hosts:**

Netdiscover command is used to discover Network hosts for scanning and and vulnerability assessment. The host address this command discovered are 10.0.2.2 and 10.0.2.3



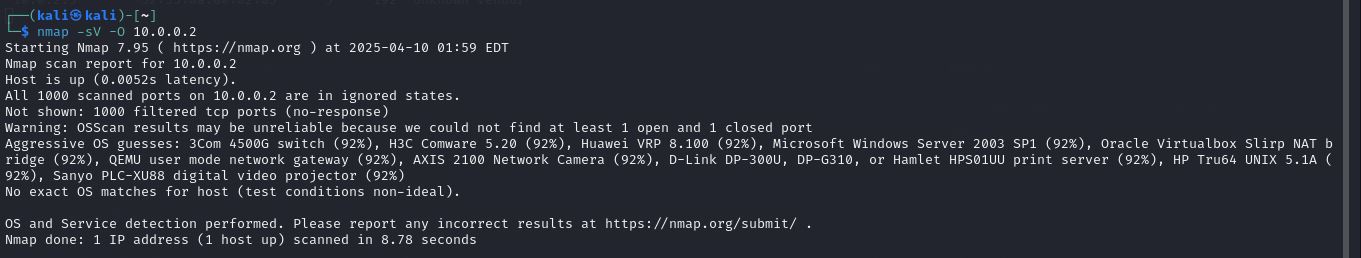
## **Host Discovery:**

Host discovery is performed using nmap scan which scans the entire subnet sends ping requests and identify hosts which are online. This command provided for how long this host was online and the MAC address of the given IP address.



## **Scan targets for open ports:**

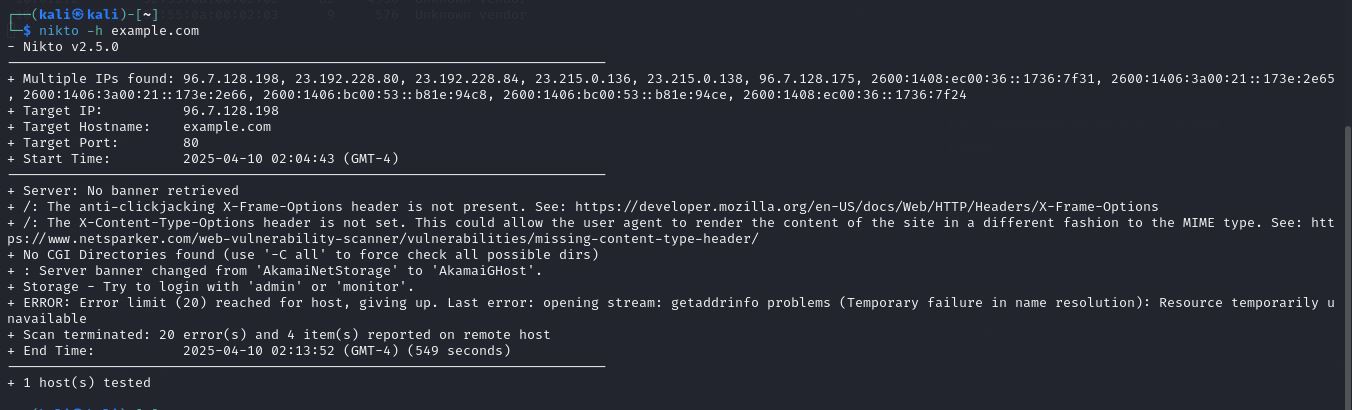
nmap -sV -O <target-IP> command is used to determine open ports in a specific target. The results it provided are that the host is up but its ports are not responding but still OS detection provided multiple guesses which are not reliable and no services like http, htttps are identifiable.



Since it is not providing any answer I am using sudo nmap -Pn -sS -p- 10.0.0.2 command to scan all ports and bypass any check.

## **Web Vulnerability Scan:**

Nikto is used to determine ay vulnerability in the website. I used the provided example.com site



In the above command following result can be generated:

### Vulnerabilities Found

### 1. ****Missing X-Frame-Options Header****

* **Description**: This allows **clickjacking** attacks, where an attacker tricks users into interacting with invisible or disguised elements.
* **Mitigation**: Add X-Frame-Options: SAMEORIGIN or DENY.
* **Estimated CVSS v3 Score**: **6.5 (Medium)**

### 2. ****Missing X-Content-Type-Options Header****

* **Description**: Allows **MIME sniffing**, which could lead to browsers interpreting files as executable content.
* **Mitigation**: Add X-Content-Type-Options: nosniff.
* **Estimated CVSS v3 Score**: **5.3 (Medium)**

### 3. ****Server Banner Changed (AkamaiNetStorage to AkamaiGHost)****

* Also **informational**, not a direct vulnerability.
* Nikto is just noting the change in the server banner that is useful for fingerprinting.

### 4. ****Login Attempt with Common Credentials****

* Storage – Try to login with 'admin' or 'monitor'
* **Possible brute-force or misconfigured login portals**.
* **Mitigation**: Ensure login panels are protected with strong credentials and hidden from public access (or IP-restricted).
* **Estimated CVSS v3 Score**: **7.5 (High)**

### 6. ****Error Limit Reached / DNS Failure****

* Nikto reported: getaddrinfo problems (Temporary failure in name resolution)
* This is **not a vulnerability**, but a **network/host issue** (probably DNS or firewall block).
* Here's a clean and organized summary table along with recommended **mitigation techniques** for each item:

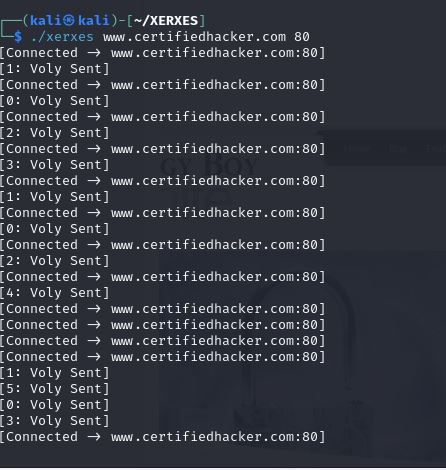
| **Vulnerability** | **Severity** | **CVSS Score** | **Notes** | **Mitigation Techniques** |
| --- | --- | --- | --- | --- |
| Missing X-Frame-Options Header | Medium | 6.5 | Susceptible to clickjacking | Set the X-Frame-Options header to DENY or SAMEORIGIN to prevent clickjacking attacks. |
| Missing X-Content-Type-Options Header | Medium | 5.3 | Risk of MIME-sniffing | Add the X-Content-Type-Options: nosniff header to prevent browsers from MIME-type sniffing. |
| Login with 'admin' / 'monitor' attempt | High | 7.5 | Indicates weak/default credentials could be present | Disable or change default credentials, enforce strong password policies, use account lockout mechanisms. |
| No CGI directories, banner change, DNS error | Info | - | Not vulnerabilities | Ensure CGI directories are not used or are secured, suppress server version banners, and configure DNS securely. |

# **Distributed Denial of Service Attack**

## **XERSES Compilation**



## **DDOS attack**



This attack was carried out at certifiedhacker.com port 80 and in the output the website stopped responding.

# **Reflection:**

Ethical hacking is important because it helps organizations identify and fix security vulnerabilities before malicious hackers exploit them. It strengthens cybersecurity defenses and protects sensitive data. Real-world DDoS attacks can crash websites, disrupt services, cause financial loss, and damage reputations. They can also lead to data breaches and customer trust issues. Ethical hackers simulate such attacks to prepare systems against them.