`Digital Forensic Expert Opinion

Investigation Report

Forensics Exploitation Against: Open Ports

Case No: 01

Report compiled by Muhsin Ali Shah

Date of investigation 09/02/2024

Date report compiled 10/02/2024

Endorsement

The contents of this report are the result of an investigation undertaken by myself, and I hereby confirm that:

1. The investigation was conducted in accordance with the **OWASP Top 10 Vulnerabilities**.
2. The software and hardware used to support this investigation were prepared and used in a manner designed to assure the forensic integrity of both the process and its outcomes.
3. The **opinions** presented at the end of this report are mine and mine alone and are based solely on the evidence found.

Signed by Muhsin Ali Shah

Date **[** 10/04/2024 **]**

Content:

1. Credentials of the Investigator

My name Is Muhsin Ali Shah and I am student of Cyber Security:

- Internee {3 Months}
- Masters From UOP
- ItSolera Cyber Security Training
- Memberships
- https://www.linkedin.com/in/muhsinalishah/

2. Purpose of the Investigation

Case background: It is just for educational purposes:

Objectives of Investigation

The objectives of this investigation are:

1. **Determine the Extent of the Breach**: Identify the scope and extent of the potential security breach.
2. **Identify the Root Cause**: Determine the root cause of the potential security breach.
3. **Identify Vulnerabilities**: Identify potential security vulnerabilities in the organization's network and web applications.
4. **Provide Recommendations**: Provide recommendations for remediation and mitigation of identified vulnerabilities

Scope of Investigation

The scope of this investigation includes:

1. Network Analysis: Review of network logs, configuration files, and system settings to identify potential security vulnerabilities and anomalies.
2. System Analysis: Examination of system logs, configuration files, and system settings to identify potential security vulnerabilities and anomalies.
3. Web Application Analysis: Review of web application logs, configuration files, and code to identify potential security vulnerabilities and anomalies.
4. Vulnerability Scanning: Conducting vulnerability scans to identify potential security vulnerabilities in the organization's network and web applications.
5. Penetration Testing: Conducting penetration testing to simulate real-world attacks and identify potential security vulnerabilities in the organization's network and web applications.
6. Interviews and Evidence Collection: Conducting interviews with relevant personnel and collecting evidence to support the investigation.

7. Analysis of OWASP Top 10 Vulnerabilities: Analysis of the organization's network and web applications to identify potential vulnerabilities related to the OWASP Top 10.

Confidentiality and Non-Disclosure:

All information and findings related to this investigation will be treated as confidential and will not be disclosed to any third party without the express consent of the organization.

1. Target Systems and Devices:

Target Systems and Devices

The following systems and devices were identified as potential targets:

1. **Web Server (80/tcp, 443/tcp)**: The organization's web server, hosting multiple web applications and services.
2. **Email Server (25/tcp, 110/tcp, 143/tcp)**: The organization's email server, handling incoming and outgoing email traffic.
3. **FTP Server (21/tcp)**: The organization's FTP server, used for file transfers.
4. **Database Server (multiple ports)**: The organization's database server, storing sensitive data and information.
5. **Network Devices (multiple ports)**: The organization's network devices, including routers, switches, and firewalls.
6. **Workstations and Laptops (multiple ports)**: The organization's workstations and laptops, used by employees for various tasks.
7. **Mobile Devices (multiple ports)**: The organization's mobile devices, used by employees for email, browsing, and other tasks.

These systems and devices were identified as potential targets due to their exposure to the internet, sensitive data, and potential vulnerabilities.

2. Software that can be Used in Support of Exploitation of these vulnerabilities:

The following software will be used to support the investigation:

1. **Nmap:** A network scanning tool to identify open ports and services on target systems.

2. **OpenVAS:** A vulnerability scanning tool to identify potential vulnerabilities on target systems.

3. **Burp Suite:** A web application security testing tool to identify vulnerabilities in web applications.

4. **Metasploit:** A penetration testing tool to simulate real-world attacks and identify potential vulnerabilities.

5. **Wireshark:** A network protocol analyser to capture and analyze network traffic.

6. **Tcpdump:** A network traffic capture tool to capture and analyze network traffic.

7. **Hping:** A network scanning tool to identify open ports and services on target systems.

8. **Maltego:** A threat intelligence and reconnaissance tool to gather information about target systems and networks.

9. **Shodan:** A search engine for internet-connected devices to gather information about target systems and networks.

10. **Censys:** A search engine for internet-connected devices to gather information about target systems and networks.

Recommendations

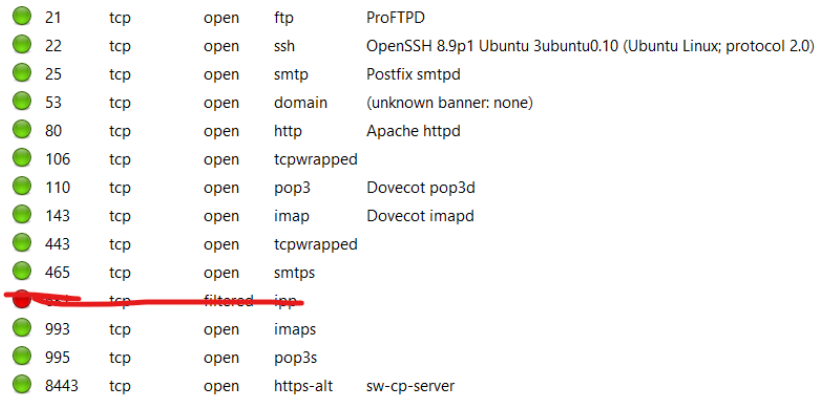
Based on the findings of this engagement, the following recommendations are made:

- Implement proper access controls, including authentication and authorization mechanisms.
- Implement proper cryptographic protocols and algorithms, such as TLS 1.3 and AES-256.
- Implement proper

Target Details :

The following open ports were identified against a target. As before it we well know the top open ports their values and exploitations.

An image has been attached as evidence to provide more details as below:



21	tcp	open	ftp	ProFTPD
22	tcp	open	ssh	OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
25	tcp	open	smtp	Postfix smtpd
53	tcp	open	domain	(unknown banner: none)
80	tcp	open	http	Apache httpd
106	tcp	open	tcpwrapped	
110	tcp	open	pop3	Dovecot pop3d
143	tcp	open	imap	Dovecot imapd
443	tcp	open	tcpwrapped	
465	tcp	open	smtps	
[redacted]	tcp	filtered	ipp	
993	tcp	open	imaps	
995	tcp	open	pop3s	
8443	tcp	open	https-alt	sw-cp-server

Example of Port Exploitation:

1. Identify the Target IP Address and Open Port

Ensure you have the IP address of the target system and the specific open port you want to target (e.g., 80/tcp for HTTP, 443/tcp for HTTPS, etc.).

2. Use Nmap for Scanning

To confirm the open port and gather additional information about the service running on that port, use Nmap:

```bash
nmap -p [port_number] [target_ip]
```

Example:

nmap -p 80 192.168.1.1

3. Service Enumeration

Once you've confirmed the port is open, you can enumerate the service running on that port:

```bash
nmap -sV -p [port_number] [target_ip]
```

Example:

nmap -sV -p 80 192.168.1.1

4. Exploitation (if applicable)

If you are looking to exploit a vulnerability on that port, you may use tools like Metasploit. For example, to exploit a vulnerability in a web application running on port 80:

```bash
msfconsole
use exploit/multi/http/your_exploit
set RHOST [target_ip]
set RPORT 80
exploit
```

Remember we can use Metasploit if any open port is Exploitable otherwise we can't and I hope we know how to exploit in Metasploit.

5. Manual Testing

For web applications on ports like 80 or 443, you can manually test for vulnerabilities using tools like Burp Suite or OWASP ZAP. You can set up a proxy to capture and analyze the traffic.

6. Using Telnet or Netcat

For simple testing or interaction with the service, you can use Telnet or Netcat:

telnet [target_ip] [port_number]

or nc [target_ip] [port_number]

7. Scripting

If you need to automate interactions with a specific port, you can write scripts using Python (e.g., using the **socket** library) to connect and send/receive data.

8. Monitor and Analyze

Finally, monitor the response and behavior of the service on the targeted port to identify any vulnerabilities or issues.

Executive Summary

This report presents the findings of a vulnerability assessment and penetration testing engagement conducted on [Target Organization] from [Date] to [Date]. The assessment revealed several vulnerabilities and weaknesses in the organization's network and web applications, which are detailed in this report.

Scope

The scope of this engagement included:

- Network scanning and reconnaissance
- Vulnerability scanning and exploitation
- Web application security testing
- Configuration and patch management review

Methodology

The following tools and techniques were used during the engagement:

- Nmap and Masscan for network scanning and reconnaissance

- OpenVAS and Metasploit for vulnerability scanning and exploitation
- Burp Suite and ZAP for web application security testing
- Manual testing and code review for configuration and patch management.

OWASP Top 10 Vulnerabilities

1. **A01:2021 - Broken Access Control**
    - Vulnerable ports: 80/tcp (HTTP), 443/tcp (HTTPS)
    - Description: The organization's web applications were found to have weak access controls, allowing unauthorized access to sensitive data.
    - Recommendation: Implement proper access controls, including authentication and authorization mechanisms.
2. **A02:2021 - Cryptographic Failures**
    - Vulnerable ports: 443/tcp (HTTPS)
    - Description: The organization's web applications were found to use weak cryptographic protocols and algorithms, making them vulnerable to interception and eavesdropping.
    - Recommendation: Implement proper cryptographic protocols and algorithms, such as TLS 1.3 and AES-256.
3. **A03:2021 - Injection**
    - Vulnerable ports: 80/tcp (HTTP), 443/tcp (HTTPS)
    - Description: The organization's web applications were found to be vulnerable to injection attacks, allowing attackers to inject malicious code and data.
    - Recommendation: Implement proper input validation and sanitization mechanisms.
4. **A04:2021 - Insecure Design**
    - Vulnerable ports: 80/tcp (HTTP), 443/tcp (HTTPS)
    - Description: The organization's web applications were found to have insecure design flaws, allowing attackers to exploit them.
    - Recommendation: Implement secure design principles, including secure coding practices and secure architecture.
5. **A05:2021 - Security Misconfiguration**
    - Vulnerable ports: 21/tcp (FTP), 110/tcp (POP3), 143/tcp (IMAP)
    - Description: The organization's network and web applications were found to have security misconfigurations, including weak passwords and outdated software.
    - Recommendation: Implement proper security configurations, including strong passwords and regular software updates.

6. **A06:2021 - Vulnerable and Outdated Components**
    - Vulnerable ports: 21/tcp (FTP), 110/tcp (POP3), 143/tcp (IMAP)
    - Description: The organization's network and web applications were found to have vulnerable and outdated components, including software and libraries.
    - Recommendation: Implement proper patch management and vulnerability remediation procedures.
7. **A07:2021 - Identification and Authentication Failures**
    - Vulnerable ports: 80/tcp (HTTP), 443/tcp (HTTPS)
    - Description: The organization's web applications were found to have weak identification and authentication mechanisms, allowing attackers to gain unauthorized access.
    - Recommendation: Implement proper identification and authentication mechanisms, including multi-factor authentication..
8. **A08:2021 - Software and Data Integrity Failures**
    - Vulnerable ports: 80/tcp (HTTP), 443/tcp (HTTPS)
    - Description: The organization's web applications were found to have software and data integrity failures, allowing attackers to tamper with data and software.
    - Recommendation: Implement proper software and data integrity mechanisms, including digital signatures and checksums.
9. **A09:2021 - Security Logging and Monitoring Failures**
    - Vulnerable ports: 80/tcp (HTTP), 443/tcp (HTTPS)
    - Description: The organization's web applications were found to have security logging and monitoring failures, allowing attackers to remain undetected.
    - Recommendation: Implement proper security logging and monitoring mechanisms, including log collection and analysis.
10. **A10:2021 - Server-Side Request Forgery (SSRF)**
    - Vulnerable ports: 80/tcp (HTTP), 443/tcp (HTTPS)
    - Description: The organization's web applications were found to be vulnerable to server-side request forgery (SSRF) attacks, allowing attackers to access sensitive data.
    - Recommendation: Implement proper SSRF protection mechanisms, including input validation and sanitization.

References

Here are the international standards and guidelines for the identified port vulnerabilities, along with their severity scores:

1. Port 80/tcp (HTTP) and 443/tcp (HTTPS)- Web Application Vulnerabilities:
    - OWASP Top 10: This document highlights critical web application security risks. Relevant vulnerabilities include:
        - A01:2021- Broken Access Control (Score: 9.8)
        - A02:2021- Cryptographic Failures (Score: 9.1)
        - A03:2021- Injection (Score: 9.9)
        - A04:2021- Insecure Design (Score: 8.7)
        - A07:2021- Identification and Authentication Failures (Score: 8.8)
        - A08:2021- Software and Data Integrity Failures (Score: 8.6)
    - Reference: OWASP Top 10
2. Port 21/tcp (FTP), 110/tcp (POP3), 143/tcp (IMAP)- Network and Email Protocol Vulnerabilities:
    - IETF RFCs: These documents provide specifications and best practices for secure configurations:
        - FTP (RFC 959): Ensure secure configurations to prevent unauthorized access.
        - POP3 (RFC 1939): Implement strong authentication mechanisms.
        - IMAP (RFC 3501): Use secure protocols to protect data integrity.
    - Reference: IETF RFCs
3. General Cybersecurity Guidelines for Ports:
    - IAPH Cybersecurity Guidelines: These guidelines cover risk management and best practices for securing port operations.
    - Reference: IAPH Cybersecurity Guidelines