Vulnerability Audit and Assessment Report (Results and Executive Summary)

Table of Contents

Executive Summary

The current report contains information about the scanning methodology, results, and recommendations as a part of the vulnerability audit and assessment for www.ehr-online.co.uk web application.

The assessment process was conducted based on the methodology described by McNab (2016) with a combination of internal and external scans, in addition to social engineering, analysis, and risk assessment (Tunggal, 2021; Cyber Today Academy, 2021). Scanning was performed using Nmap and Nessus followed by an investigation of vulnerabilities, then some penetration tests.

Six vulnerabilities were found (1 high, and 5 medium severity), and 7-8 unnecessarily open ports. All the issues found can be easily mitigation by updates or closure of unnecessary ports.

Further recommendations were presented to ensure compliance with ISO 27001 standard and the GDPR regulation.

Methodology

The assessment was organized into different stages as suggested by McNab (2016). First, the ***reconnaissance stage*** was completed using *Nmap, Hping3, and Nessus.* Open TCP and UDP ports were explored using the following Nmap commands:

```
nmap -sT -F ehr-online.co.uk > open_tcp.txt

nmap -sU -F ehr-online.co.uk > open_udp.txt
```

Then, different ***OS detection*** methods were used:

1. *Nmap* OS detection:

```
nmap -A -F -O -oN os_detection.txt ehr-online.co.uk
```

2. *Nmap* OS fingerprinting:

```
nmap -open -sS -A -d -oN tcp_fast ehr-online.co.uk
```

3. *Hping* OS fingerprinting using TTL:

```
hping3 -c 3 -S -p 443 ehr-online.co.uk
```

Next, the Nmap ***service detection*** command was used:

```
nmap -sV -T4 -F -oA service_detection ehr-online.co.uk

nmap -A -T4 -F -oA service_detection2 ehr-online.co.uk
```

After that, Nessus basic and advanced network scans were performed. Last, Wireshark was theoretically used as no access to internal network assessment was possible.

The ***vulnerability scanning stage*** was done using *Nmap* and *Nessus* Basic and Advanced Network Scans, Web Application Tests, and 2021 Threat Landscape Retrospective (TLR). The following *Nmap* commands were used:

```
nmap -Pn -sSC -oN vul_scan ehr-online.co.uk

nmap -p<port_num> --script vul -oN port_<port_num>_ul ehr-online.co.uk
```

Last, the following additional tests were performed*:*

- Checking if the HTTPS protocol is used.
- SQL injection test using " ' or 1=1 – ".

During the ***investigation of the vulnerabilities*** **stage,** the type of vulnerability, severity, according to the Common Vulnerability Scoring System (CVSS-SIG) (Forum of Incident Response and Security Teams, 2019), and the risks were evaluated.

The ***exploitation and circumvention stage*** included:

- Attempt to exploit detected vulnerabilities.
- Social engineering attacks by sending the system users phishing emails aiming to obtain their credentials (only theoretical) after arranging with the administrative personnel.

Scan Results

Open ports detection

Fifteen open ports were identified along. However, the scans failed to reveal the exact version of some of the services (Table1).

Table 1 List of open ports discovered

Port	Service	Version
21/tcp	ftp	Pure-FTPd
80/tcp	http	Apache httpd (PHP 7.4.32)
53/tcp	domain	ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
110/tcp	pop3	Dovecot pop3d
143/tcp	imap	Dovecot imapd
443/tcp	https	Apache httpd (W3 Total Cache/0.9.4.6.4)
465/tcp	smtps	Exim smtpd 4.95
587/tcp	smtp	Exim smtpd 4.95
993/tcp	imaps	Dovecot imapd
995/tcp	pop3s	Dovecot pop3d
2083/tcp	ssl/radsec?	?
2086/tcp	gnunet?	?
2525/tcp	smtp	Exim smtpd 4.95
3306/tcp	mysql	MySQL 5.5.5-10.3.36-MariaDB-cll-lve
5432/tcp	postgresql	PostgreSQL DB 9.6.0 or later
53/udp	domain	ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)

Firewall detection

A Fortinet FortiGate 200B firewall was detected.

Operating system detection

The operating system of the server couldn't be directly identified. However, the TTL value received by using the *hping3* tool was 128 suggesting a Windows operating system with no version information.

```
hping3 -c 3 -S -p 443 ehr-online.co.uk

HPING 68.66.247.187 (eth0 68.66.247.187): S set, 40 headers + 0 data bytes
len=48 ip=68.66.247.187 ttl=128 id=4919 sport=443 flags=SA seq=0 win=32768 rtt=4.5 ms
len=48 ip=68.66.247.187 ttl=128 id=4920 sport=443 flags=SA seq=1 win=32768 rtt=6.7 ms
len=48 ip=68.66.247.187 ttl=128 id=4921 sport=443 flags=SA seq=2 win=32768 rtt=3.7 ms

--- 68.66.247.187 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3.7/5.0/6.7 ms
```

Figure 1. OS fingerprinting using hping3

HTTPs protocol check

The web application is using HTTPs with a valid certificate.

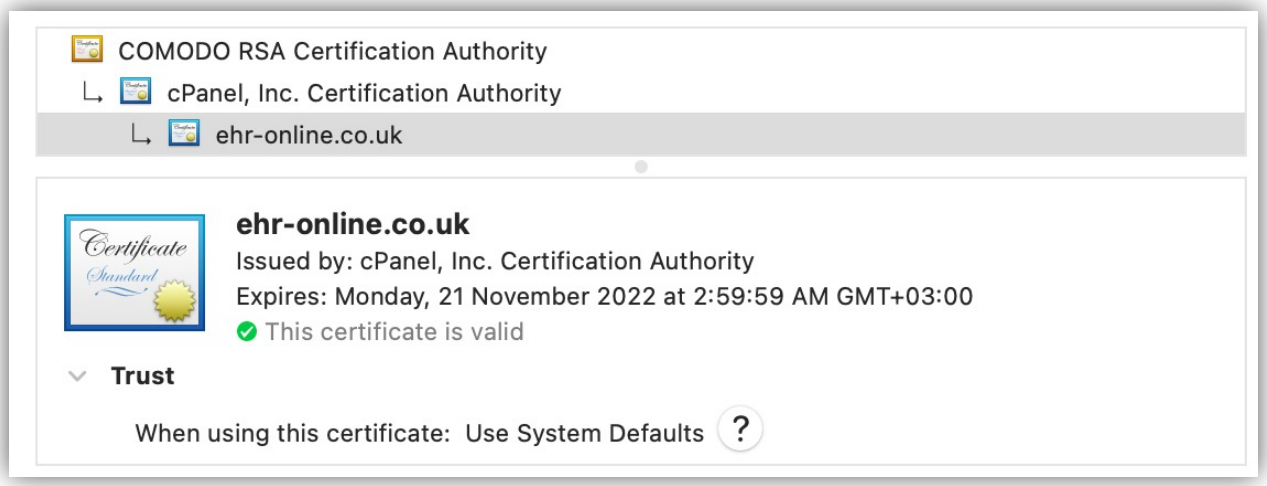

Figure 2. Ehr-online.co.uk shows a valid digital certificate

Investigations of Vulnerabilities

After using *Nmap and Nessus* vulnerability scans, the following vulnerabilities were found.

Table 2 List of vulnerabilities discovered

Vulnerability Type	CVE	Port	Description	Detection Tool	Severity	CVSS	Risk
SSL Medium Strength Cipher	CVE-2016-2183	143	3DES encryption using 64 – 112 bits keys	Nessus Advanced Network Scan	High	7.5 (CVSS 3.0)	Exploitable medium strength encryption to expose sensitive information
TLS v1.0 Protocol Detection	N/A	143	TLS v1.0 is enabled on port 143/tcp	Nessus Advanced Network Scan	Medium	6.5 (CVSS 3.0)	Exploitable by man-in-the-middle attacks due to cryptographic design flaws that
TLS v1.0 Protocol Detection	N/A	143	TLS v1.1 is enabled on port 143/tcp	Nessus Advanced Network Scan	Medium	6.5 (CVSS 3.0)	Exploitable by man-in-the-middle attacks due to cryptographic design flaws that
Anonymous Diffie-Hellman Key Exchange MitM Vulnerability	N/A	21	TLS uses	Nmap NSE Scripts	Estimated to by Medium – High	Estimated to be >= 6.5 compared with the above	Exploitable by man-in-the-middle attacks that affect date privacy and integrity
Vulnerable Firewall model found (Fortinet Fortigate 900B)	CVE-2012-4948	N/A	Improper Certificate Validation	NIST NVD search after Nmap OS / Version Detection	Medium	5.3 (CVSS 2.0)	Exploitable by man-in-the-middle attacks to Spoof SSL Servers
PostgreSQL before 10.X	CVE-2017-15099		Information disclosure using INSERT ... ON CONFLICT DO UPDATE	NIST NVD search after Nmap OS / Version Detection	Medium	6.5 (CVSS 3.0)	Table content disclosure by attackers with no read access.

No vulnerabilities were found in the following service versions:

- Apache httpd (PHP 7.4.32).
- Apache httpd (W3 Total Cache/0.9.4.6.4).
- Exim smtpd 4.95
- MySQL 5.5.5-10.3.36

Exploitation of Vulnerabilities

Brute Force Attacks:

The brute force attack using *Hydra* on the login page was stopped after 31 minutes and 1207 trials. According to that, it was assumed that a good password policy was implemented for the web application (Fig.3).

```
┌──(root㉿kali)-[~]
└─# hydra 68.66.247.187 http-form-post "/interface/login/login.php:authUser=^USER^&clearPass=^PASS^&Login=submit:Login Inval
id username or pass phrase" -L /home/mohammad/Desktop/top-usernames-shortlist.txt -P /home/mohammad/Desktop/rockyou.txt
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f
or illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-29 20:03:31
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to pr
event overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 243854783 login tries (l:17/p:14344399), ~15240924 tries per task
[DATA] attacking http-post-form://68.66.247.187:80/interface/login/login.php:authUser=^USER^&clearPass=^PASS^&Login=submit:L
ogin Invalid username or pass phrase
[STATUS] 18.00 tries/min, 18 tries in 00:01h, 243854779 to do in 225791:28h, 2 active
[STATUS] 30.33 tries/min, 91 tries in 00:03h, 243854706 to do in 133986:07h, 2 active
[STATUS] 35.57 tries/min, 249 tries in 00:07h, 243854548 to do in 114255:49h, 2 active
[STATUS] 38.07 tries/min, 571 tries in 00:15h, 243854226 to do in 106766:18h, 2 active
[STATUS] 38.94 tries/min, 1207 tries in 00:31h, 243853590 to do in 104383:37h, 2 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Figure 3. Burte Force Attack on the Login Page using Hydra on Kali Linux

Also, the brute force attacks on the MySQL and PostgresSQL servers failed. This means that default passwords and usernames were changed (Fig.4-7).

```
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /home/mohammad/Desktop/mysql_default_user.txt
USER_FILE ⇒ /home/mohammad/Desktop/mysql_default_user.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /home/mohammad/Desktop/mysql_default_pass.txt
PASS_FILE ⇒ /home/mohammad/Desktop/mysql_default_pass.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set BLANK_PASSWORDS True
BLANK_PASSWORDS ⇒ True
msf6 auxiliary(scanner/mysql/mysql_login) > run
```

Figure 4, Metasploit settings for MySQL brute force login.

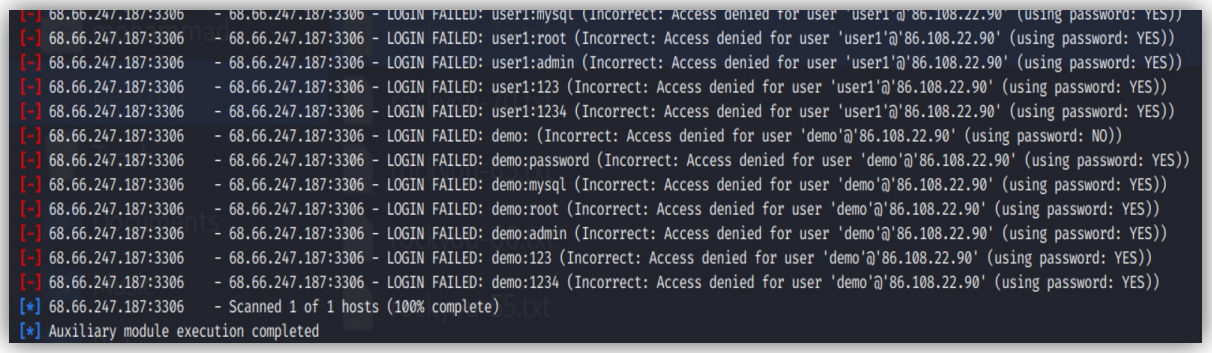

Figure 5, Sample from failed brute force login attempt on the MySQL server.

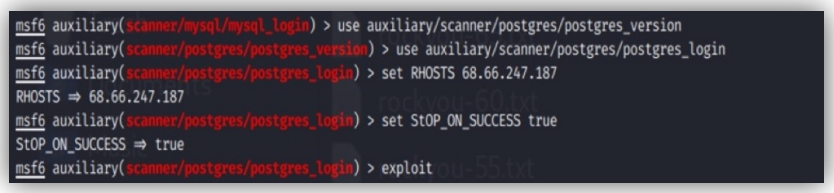

Figure 6, Metasploit settings for PostgresSQL brute force login.

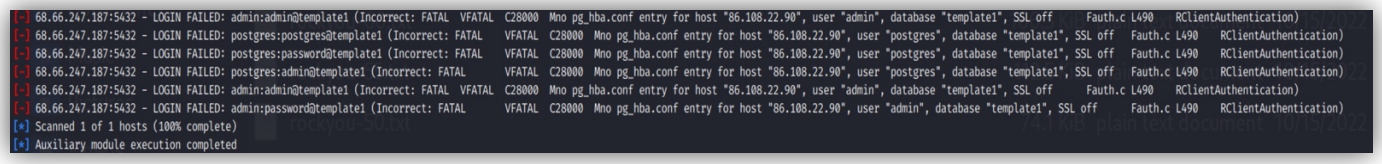

Figure 7 Sample form the failed brute force login attempt on the PostgresSQL server.

Compliance with Information Security Standards and GDPR

It appears from the scan results that access to online health records by care providers is through HTTPs. However, further information is needed to verify full compliance with GDPR and ISO 27001 (International Organization for Standardization, 2013) as follows:

- Are user accounts secured by a 2FA or MFA?
- Is data stored in an encrypted form?
- Will patients be able to access their records or request a copy downloaded, or forwarded to a third party?

Mitigations & Recommendations

Mitigations and recommendations are presented in the following tables (Table 3-4). In addition, it is advisable to implement the following as well:

- Strong password policy.
- Security education of the healthcare staff.
- 2FA or MFA for the system login.

Table 3 List of vulnerabilities and mitigations

Vulnerability	Mitigation
SSL Medium Strength Cipher	Adjust the configurations of the service to use only advanced encryption standard (AES) or close the port
TLS 1.0 protocol	Disable support for TLS 1.0 and enable TLS 1.2 and 1.3
Anonymous Diffie-Hellman Key Exchange	Enable TLS1.2 and 1.3 that used ephemeral Diffie-Hellman instead
CVE-2012-4948 (Firewall)	Verify that the default configurations have been changed
CVE-2017-15099 (PostgreSQL)	Upgrade to PostgreSQL 10.1 or later

Table 4 List of recommended port closure

Port	Recommendation
21/tcp	Close or enforce more secure TLS1.2/1.3
80/tcp	Close as https is more secure
110/tcp	Close and keep the secure pop3s on port 995
143/tcp	Close and keep the secure imaps on port 993
587/tcp	Close and keep the secure smtps on port 465
2086/tcp	Close
2525/tcp	Close
3306/tcp	Close if only PostgreSQL is needed
5432/tcp	Close if only MySQL is needed

Challenges

A couple of challenges were faced during the scanning process. First, scans had to be run individually to avoid temporary blocks. Second, internal scans or deactivation of IPS and firewalls were not feasible, hence some vulnerabilities have been likely overlooked.

References

Cyber Today Academy (2021) vulnerability assessment tutorial for beginners. Available from: https://www.youtube.com/watch?v=hIbkwnOteTc [Accessed 10 October 2022].

Forum of Incident Response and Security Teams (2019) Common Vulnerability Scoring System SIG. Available from: https://www.first.org/cvss/ [Accessed 30 October 2022].

International Organization for Standardization (2013) ISO/IEC 27001 Information security management. Available from: https://www.iso.org/isoiec-27001-information-security.html [Accessed].

Mcnab, C. (2016) *Network security assessment : know your network*. Third edition. ed. Sebastopol, CA ;: O'Reilly.

Tunggal, A. (2021) What Is a Vulnerability Assessment? And How to Conduct One. Available from: https://www.upguard.com/blog/vulnerability-assessment [Accessed 10 October 2022].