

NISM Executive Summary

1. Introduction

Through penetration testing, the underlying E-Health website is vetted according to applicable regulations and security standards. The E-Health website under consideration offers consultation and information for users provided by medical specialists. Within the project's scope, a list of vulnerabilities will be provided, together with an evaluation of conformity to standards and recommendations to resolve issues found.

2. Applied Methodology

As a foundation, the extended CIA triad was used to evaluate the project's conformity to security. STRIDE was applied to identify potential threats. For the evaluation, a DREAD analysis was conducted to triage identified threats and rate them on an ordinal scale.

Due to the current circumstances and travel restrictions, the project's penetration testing scope had to be confined to an off-shore model. The team could not conduct the testing from within the company's location and instead ran a full suite of tests through the external network. This made the testing of certain attack vectors, such as a local area network Man-in-the-Middle (MITM) attack, impossible. Instead, the focus was shifted towards the security of the web application itself.

Furthermore, conducting penetration testing in the healthcare sector offers its own set of risks and issues. Patients need to be able to access the application at all times, meaning that the production system cannot experience any downtime. It is also critical to preserve the integrity of sensitive user data due to its highly private nature and strict compliance adherence. Therefore, the main components of the penetration test were run against the application's User Acceptance Testing (UAT) environment with additional stress testing done

on a production-like environment to simulate the impact of availability attacks, e.g., a Denial-of-Service (DOS) attack.

3. Sequence of Applied Tools

The penetration test can be split into four phases that are run through in sequence. A complete list of outputs from applied tools can be found in the appendix of the report.

3.1 Reconnaissance

- Footprinting, Scanning and Enumeration of target
- Information gathering such as OS fingerprint, open ports and running services
- Gathering of WHOIS, DNS, and SMTP records
- **Tools used:** NMAP, Metasploit and Open-source intelligence (OSINT)

3.2 Web Application Scanning

- Automated web scanners are used to find potential vulnerabilities and attack vectors
- Common attacks such as SQL injections and XSS are tested against
- Ensure validity of findings by use of multiple sources and tools
- **Tools used:** Zed Attack Proxy, Nikto, Nessus and Metasploit (WMAP)

3.3 Vulnerability Analysis

- Search for common vulnerabilities and exploits for running services
- Use of CVE databases and Metasploit Framework to identify prevalent issues
- **Tools used:** Metasploit, Mitre CVE and NIST NVD

3.4 Availability Attack

- Denial-of-Service attack to stress test application
- Evaluation of website loading times while under load of HTTP DoS attack
- **Tools used:** Slowloris

4. List of Security Issues

Challenges specific to E-Health are as follows:

- Any alteration to patient data can result in incorrect diagnosis, causing severe injuries or even death.
- Use of sensitive information (i.e. diagnoses and diseases) for blackmailing.
- Alteration of the health care professionals' work schedules can lead to confusion and denial of health care services.
- Any ransomware attack on health care records leading to denial or delay of services to the patients.
- Any disclosure of patient / healthcare professionals' personal sensitive data (name, telephone, address, social security) can lead to identity theft.

The technical findings are in the below section.

5. Findings

Summary

The health care site provided are susceptible to the following attacks resulting in the mentioned security findings:

NESSUS

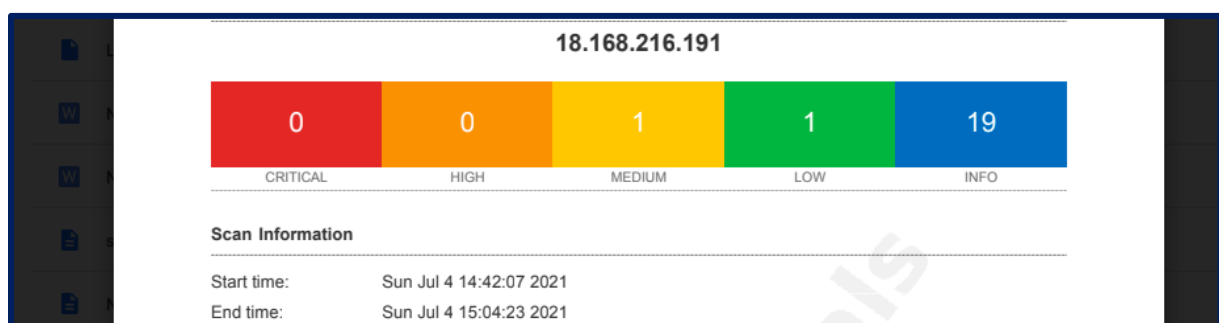



Figure 1: Nessus Security Findings

Zed Attack Proxy (ZAP)



ZAP Scanning Report

Summary of Alerts

Generated on Sun, 4 Jul 2021 15:51:00

Risk Level	Number of Alerts
High	0
Medium	1
Low	3
Informational	1

Alerts

Name	Risk Level	Number of Instances
X-Frame-Options Header Not Set	Medium	4
Absence of Anti-CSRF Tokens	Low	2
Cross-Domain JavaScript Source File Inclusion	Low	8
X-Content-Type-Options Header Missing	Low	10
Information Disclosure - Suspicious Comments	Informational	1

Figure 2: ZAP Security Findings

FND 1: The site is currently missing a Load Balancer or Intrusion Prevention System (IPS), resulting in a successful D-DoS attack. This weakness in the system can result in service disruption.

FND 2: This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target if the network is loaded.

FND 3: The website is susceptible to Man In The Middle attack, and the data transferred is not encrypted since it has HTTP port 80 open.

FND 4: The SSH port number, SSH version, the Apache webserver version, the Fully Qualified Domain Name of the system, and the Operating System type is visible can result in targeted D-Dos and Brute force attack. The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

FND 5: The system is susceptible to Cross-Site Request Forgery and can lead to unauthorised privileged access to the attacker

a. Data Protection Act

As a framework for data protection law, Data Protection Act seeks to empower individuals to take control of their personal information while supporting organisations with the lawful processing of private data (Information Commissioner's Office, 2021a).

Protecting personal data can be a complex challenge in E-health. There is a tendency to store information far more than necessary, including duplicated or out-dated personal data, which adds unnecessary challenges to privacy, data protection and data security. Therefore, additional care must take when transferring patient health information across countries during implementation and adaptation.

The laws and regulations underpinning patient health information remain highly dynamic on a country-by-country basis forming more robust legal protection for more sensitive information.

For an example, the DPA 2018 the amended-on 01 January 2021, sets out the data protection framework in the UK, alongside the UK GDPR (Information Commissioner's Office, 2021b). Especially relates to E-health, the UK's Medicines and Healthcare Products Regulatory Agency (regulating apps, smartphone-connected devices and wearable technologies) also play a key role (Bodulovic et al., 2020).

Inability to demonstrate that good data protection is a cornerstone of the E-Health policy and practices may lead the E-Health opens to enforcement actions by countries that can damage reliability and reputation, even for significant penalties threatening the existence of the application.

Thus, data protection is a boardroom issue and ensuring a level of security “appropriate to the risk” to a country’s rights/ freedoms is crucial when it comes to personal data.

b. General Data Protection Regulation (GDPR)

The GDPR significantly altered how personal data must be legitimately processed. The E-Health industry is notably impacted by the new legislation, which establishes even tougher restrictions for so-called "special categories" of personal data, including all genetic, biometric, and health data (Burgess, 2020). As a result, under the new data protection legislation, the whole E-Health industry is crucial, and legal requirements must be thoroughly assessed.

Moreover, data processing in the E-Health sector includes data collection, organisation, and deletion. Our application aims to gather patient data and publish it on the website as medical history for doctors to review. Thus, every entity that handles personal data must verify that they comply with the GDPR's standards. The GDPR's primary obligations are as follows:

- Use of personal data in accordance with standards of integrity. Processing, for example, must have a specific function. As a result, one cannot gather personal information "just in case". Patients, in other words, have a right to know how their data is used and a say in the process.
- Breached personal data must be notified within 72 hours. If sensitive data, such as health history, is lost, it must be notified to the authorities and each affected individual within 72 hours (Burgess, 2020).

The following checklist outlines the application's objectives in relation to the GDPR directive's regulations (Burgess, 2020).

- The privacy policy includes detailed information on data processing and its legal implications.
- Users are informed about why and how their data is collected. It is explained to them how the data is processed, who has access to it, and how it is safeguarded.
- Data Subject and authorities are notified in the case of a data breach.
- In case of alteration of patient data, the supervisory authority in the jurisdiction is notified within 72 hours to prevent incorrect diagnosis of the patient.

In a nutshell, GDPR highlights the need for safeguarding the security of personal data processing at early stages as stated in Article 35 of the GDPR as “prior to the processing, carry out an assessment of the impact of envisaged processing operations on the protection of personal data” (IT Governance Ltd, 2017: 3) .

Considering the UK as an example, measures to safeguard personal information within an E-health application may include:

In the UK, any information relates to an identified or identifiable individual (for example, information as simple as a name or a number or an IP address or a cookie identifier, or other factors), then the information may be personal data (Information Commissioner's Office, 2021c).

- ✓ **Ensuring secure and resilient processing systems and service based the on Article 32 (1) (b) of the UK GDPR - [FND1](#)** highlights missing a Load Balancer or Intrusion Prevention System(IPS), which leads to a successful ‘denial of service ‘attack causing service disruptions.
- ✓ **Encrypting personal data based on Article 32 (1) (a) of the UK GDPR - [FND3](#)** highlights the open HTTP port 80. Thus, communication is made over unsecured,

unencrypted HTTP and allows an attacker who manages to intercept communication at the network level to access data.

- ✓ **DPA 2018 and Article 4(11) & Recital 32 of the UK GDPR requires websites to obtain explicit consent in collecting personal data** (Bird & Bird LLP, 2021) - **FND5** highlights the system susceptibility to Cross-Site Request Forgery, which can lead to unauthorised privileged access to an attacker. For both cookies and third-party plugins, user consent is crucial for personal data processing.

Remediation Plan (Recommendations):

Finding (FND) Number	Recommendation	Priority
FND 1	Use a Load balancer or IPS	High
FND 2	Protect your target with an IP filter.	High
FND 2	Implement a hardware/software Firewall.	High
FND 3	Block port 80	High
FND 5	Enable X-Framework Option	High
FND 5	Implementing Content Security Policy's "frame-ancestors" directive	High
FND 5	Change FRAMESET to "DENY"	High
FND 5	X-XSS-Protection header to be defined	High
FND 5	Anti-MIME-Sniffing header X-Content-Type-Options to be set as 'nosniff'	High
FND 5	Block access to the following pages to ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end-users of the application. <ul style="list-style-type: none">• http://www.123easyinvite.com/assets/css/bootstrap.min.css• http://www.123easyinvite.com/assets/css/bootstrap-responsive.min.css• https://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js?s=2	High
FND 4	Change SSH configuration and update Apache to the latest version.	Medium
FND 4	Contact the vendor or consult product documentation to disable CBC mode cypher encryption, and enable CTR or GCM cypher mode encryption.	Medium

6. Conclusions

The system assessed contains a high threat related to clickjacking and CSRF can result in unauthorised access, thus violating user confidentiality.

The system should be PCI/DSS, along with NIST, ISO27001, GDPR and DPA compliant, so a Network Load Balancer along with IPS/IDS needs to be implemented. The JavaScript and the bootloader need to be configured behind the firewall to avoid exposed APIs.

The system seems to have weak security measures and needs recommendations/remediation plans to be implemented.

Please refer to the APPENDIX section for the details of the findings.

7. Appendix

a. Code Visible:

- **bootstrap_min**



- **bootstrap-responsive**



- **jquery_min_js**



b. Scanning Results

- **Nessus**



- **ZAP**



ZAP Scanning Report

c. Summary of Alerts

- **Generated on Sun, 4 Jul 2021 15:51:00**

Risk Level	Number of Alerts
High	0
Medium	1
Low	3
Informational	1

- **Alerts**

Name	Risk Level	Number of Instances
X-Frame-Options Header Not Set	Medium	4
Absence of Anti-CSRF Tokens	Low	2
Cross-Domain JavaScript Source File Inclusion	Low	8
X-Content-Type-Options Header Missing	Low	10
Information Disclosure - Suspicious Comments	Informational	1

▪ Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

URL	http://www.123easyinvite.com/add
Method	POST
Parameter	X-Frame-Options
URL	http://www.123easyinvite.com
Method	GET
Parameter	X-Frame-Options
URL	http://www.123easyinvite.com/
Method	GET
Parameter	X-Frame-Options
URL	http://www.123easyinvite.com/add

Method	GET
Parameter	X-Frame-Options
Instances	4
Solution	<p>Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.</p>
Reference	<p>https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</p>
CWE Id	1021
WASC Id	15
Source ID	3

Low (Medium)	Absence of Anti-CSRF Tokens
Description	<p>No Anti-CSRF tokens were found in a HTML submission form.</p> <p>A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF</p>

attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

- * The victim has an active session on the target site.
- * The victim is authenticated via HTTP auth on the target site.
- * The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

URL	http://www.123easyinvite.com/add
Method	POST
Evidence	<form action="/add" method="post" class="form-horizontal" enctype="multipart/form-data">
URL	http://www.123easyinvite.com/add
Method	GET
Evidence	<form action="/add" method="post" class="form-horizontal" enctype="multipart/form-data">

Instances

2

Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Solution

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

	<p>This control includes a component for CSRF.</p> <p>Do not use the GET method for any request that triggers a state change.</p> <p>Phase: Implementation</p> <p>Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.</p>
Other information	<p>No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF] was found in the following HTML form: [Form 1: "thoughtAuthor"].</p>

Reference	<p>http://projects.webappsec.org/Cross-Site-Request-Forgery</p> <p>http://cwe.mitre.org/data/definitions/352.html</p>
CWE Id	352
WASC Id	9
Source ID	3

Low (Medium)	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.

URL	http://www.123easyinvite.com/add
Method	GET
Parameter	http://html5shim.googlecode.com/svn/trunk/html5.js<script
Evidence	src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script>
URL	http://www.123easyinvite.com
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js<script
Evidence	src="//ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js"></scrip >
URL	http://www.123easyinvite.com/add
Method	POST
Parameter	http://html5shim.googlecode.com/svn/trunk/html5.js<script
Evidence	src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script>
URL	http://www.123easyinvite.com/
Method	GET
Parameter	http://html5shim.googlecode.com/svn/trunk/html5.js<script
Evidence	src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script>
URL	http://www.123easyinvite.com
Method	GET
Parameter	http://html5shim.googlecode.com/svn/trunk/html5.js<script
Evidence	src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script>
URL	http://www.123easyinvite.com/add

Method	POST
Parameter	//ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js<script
Evidence	src="//ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js"></script>
URL	http://www.123easyinvite.com/
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js<script
Evidence	src="//ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js"></script>
URL	http://www.123easyinvite.com/add
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js<script
Evidence	src="//ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js"></script>
Instances	8
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Source ID	3

Low (Medium)

X-Content-Type-Options Header Missing

Description	<p>The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.</p>
-------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

URL	http://www.123easyinvite.com/assets/css/bootstrap-responsive.min.css
Method	GET
Parameter	X-Content-Type-Options
URL	http://www.123easyinvite.com/add
Method	POST
Parameter	X-Content-Type-Options
URL	http://www.123easyinvite.com/
Method	GET
Parameter	X-Content-Type-Options
URL	http://www.123easyinvite.com/assets/img/background.png
Method	GET
Parameter	X-Content-Type-Options
URL	http://www.123easyinvite.com/assets/css/bootstrap.min.css
Method	GET

Parameter	X-Content-Type-Options
URL	http://www.123easyinvite.com
Method	GET
Parameter	X-Content-Type-Options
URL	http://www.123easyinvite.com/assets/img/glyphicons-halflings-white.png
Method	GET
Parameter	X-Content-Type-Options
URL	http://www.123easyinvite.com/assets/img/glyphicons-halflings.png
Method	GET
Parameter	X-Content-Type-Options
URL	http://www.123easyinvite.com/assets/js/bootstrap.min.js
Method	GET
Parameter	X-Content-Type-Options
URL	http://www.123easyinvite.com/add
Method	GET
Parameter	X-Content-Type-Options
Instances	10
Solution	<p>Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.</p> <p>If possible, ensure that the end user uses a standards-compliant and</p>

Other information	modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.
	At "High" threshold this scan rule will not alert on client or server error responses.

Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
	https://owasp.org/www-community/Security-Headers
CWE Id	693
WASC Id	15
Source ID	3

Informational (Low)	
Information Disclosure - Suspicious Comments	
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://www.123easyinvite.com/assets/js/bootstrap.min.js

Method	GET
Evidence	query
Instances	1
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to. The following pattern was used: \bQUERY\b and was detected in the element starting with: "!function(\$){use
Other information	strict";\$(function(){\$.support.transition=function(){var transitionEnd=function(){var name,el=document.createElement", see evidence field for the suspicious comment/snippet.

Reference	
CWE Id	200
WASC Id	13
Source ID	3

d. NMAP

```
root@kali:~# nmap www.123easyinvite.com
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-04 11:58 EDT
```

```
Nmap scan report for www.123easyinvite.com (18.168.216.191)
```

```
Host is up (0.022s latency).
```

```
rDNS record for 18.168.216.191: ec2-18-168-216-191.eu-west-
```

```
2.compute.amazonaws.com
```

```
Not shown: 998 filtered ports
```

```
PORT      STATE SERVICE
```

22/tcp open ssh

80/tcp open http

▪ TCP

```
root@kali:~# sudo nmap -sT -p80,443,22 18.168.216.191
```

Starting Nmap 7.91 (<https://nmap.org>) at 2021-07-04 12:02 EDT

Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com
(18.168.216.191)

Host is up (0.00061s latency).

PORT	STATE	SERVICE
------	-------	---------

22/tcp	filtered	ssh
--------	----------	-----

80/tcp	filtered	http
--------	----------	------

443/tcp	filtered	https
---------	----------	-------

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds

▪ UDP

```
root@kali:~# sudo nmap -sU -p80,443,22 18.168.216.191
```

Starting Nmap 7.91 (<https://nmap.org>) at 2021-07-04 12:06 EDT

Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com
(18.168.216.191)

Host is up (0.00065s latency).

PORT	STATE	SERVICE
------	-------	---------

22/udp	open filtered	ssh
--------	---------------	-----

80/udp	open filtered	http
--------	---------------	------

443/udp	open filtered	https
---------	---------------	-------

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds

▪ OS

```
root@kali:~# sudo nmap -O 18.168.216.191
```

Starting Nmap 7.91 (<https://nmap.org>) at 2021-07-04 12:12 EDT

Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com
(18.168.216.191)

Host is up (0.10s latency).

Not shown: 998 filtered ports

PORT	STATE	SERVICE
------	-------	---------

22/tcp	open	ssh
--------	------	-----

80/tcp	open	http
--------	------	------

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: 2N Helios IP VoIP doorbell (98%), Grandstream GXP1105 VoIP phone (98%), Garmin Virb Elite action camera (94%), Advanced Illumination DCS-100E lighting controller (93%), Enlogic PDU (FreeRTOS/lwIP) (93%), Smart Mirage CX06 satellite receiver (93%), Ocean Signal E101V emergency beacon (FreeRTOS/lwIP) (93%), AzBox Bravissimo Twin satellite TV decoder (92%), Cognex DataMan 200 ID reader (lwIP TCP/IP stack) (92%), DTE Energy Bridge (lwIP stack) (92%)

No exact OS matches for host (test conditions non-ideal).

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

Nmap done: 1 IP address (1 host up) scanned in 18.20 seconds

▪ **Host Key, Servertype**

root@kali:~# sudo nmap -A 18.168.216.191

Starting Nmap 7.91 (<https://nmap.org>) at 2021-07-04 12:16 EDT

Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com
(18.168.216.191)

Host is up (0.026s latency).

Not shown: 998 filtered ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	tcpwrapped	
--------	------	------------	--

| ssh-hostkey:

| 2048 27:bf:d1:ec:34:d9:26:cf:34:65:fc:7d:99:97:4e:76 (RSA)

| 256 ba:df:47:d1:e1:0e:5d:ea:43:d3:c5:e9:41:a8:38:fe (ECDSA)

|_ 256 8c:68:d5:6d:47:fa:0f:72:f2:01:5b:28:f0:e9:59:1d (ED25519)

80/tcp	open	tcpwrapped	
--------	------	------------	--

|_http-server-header: Apache

|_http-title: Your Thoughts

Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port

Device type: specialized|VoIP phone|webcam|general purpose

Running (JUST GUESSING): 2N embedded (93%), Grandstream embedded
(92%), Garmin embedded (89%), Advanced Illumination embedded (85%), IBM
OS/2 4.X (85%)

OS CPE: cpe:/h:2n:helios cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite
cpe:/h:advanced_illumination:dcs-100e cpe:/o:ibm:os2:4

Aggressive OS guesses: 2N Helios IP VoIP doorbell (93%), Grandstream
GXP1105 VoIP phone (92%), Garmin Virb Elite action camera (89%), Advanced
Illumination DCS-100E lighting controller (85%), IBM OS/2 Warp 2.0 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 0.22 ms ec2-18-168-216-191.eu-west-2.compute.amazonaws.com
(18.168.216.191)

OS and Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 35.78 seconds

▪ Vulnerability

```
root@kali:~# sudo nmap --script vuln 18.168.216.191
```

Starting Nmap 7.91 (<https://nmap.org>) at 2021-07-04 12:22 EDT

Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com
(18.168.216.191)

Host is up (0.028s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)

| http-csrf:

| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=ec2-18-168-
216-191.eu-west-2.compute.amazonaws.com

| Found the following possible CSRF vulnerabilities:

|

| Path: http://ec2-18-168-216-191.eu-west-2.compute.amazonaws.com:80/add

```
|   Form id: thoughtmessage
|_  Form action: /add
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
```

Nmap done: 1 IP address (1 host up) scanned in 82.37 seconds

e. NIKTO

```
root@kali:~# nikto -h 18.168.216.191 -p 80 -o shirazNikto -F txt
- Nikto v2.1.6
```

```
-----
+ Target IP:      18.168.216.191
+ Target Hostname: 18.168.216.191
+ Target Port:    80
+ Start Time:     2021-07-04 13:54:23 (GMT-4)
-----
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent
to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to
render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause
false positives.
```

+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Configure Apache to ignore this file or upgrade to a newer version.

+ 7922 requests: 7 error(s) and 5 item(s) reported on remote host

+ End Time: 2021-07-04 14:23:08 (GMT-4) (1725 seconds)

f. LBD

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.

Written by Stefan Behte (<http://ge.mine.nu>)

Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND

Checking for HTTP-Loadbalancing [Server]:

Apache

NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 11:52:13, 11:52:13, 11:52:14, 11:52:14, 11:52:14, 11:52:15, 11:52:15, 11:52:16, 11:52:16, 11:52:17, 11:52:17, 11:52:18, 11:52:18, 11:52:19, 11:52:19, 11:52:20, 11:52:20, 11:52:20, 11:52:21, 11:52:21, 11:52:22, 11:52:22, 11:52:23, 11:52:23, 11:52:24, 11:52:24, 11:52:24, 11:52:25, 11:52:25, 11:52:26, 11:52:26, 11:52:27, 11:52:27, 11:52:27, 11:52:28, 11:52:28, 11:52:29, 11:52:29, 11:52:30, 11:52:30, 11:52:31, 11:52:31, 11:52:31, 11:52:32, 11:52:32, 11:52:33, 11:52:33, 11:52:34, 11:52:34, 11:52:34, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND

< Date: Mon, 24 May 2021 11:52:22 GMT

< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:23 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:23 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:24 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:24 GMT

< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:25 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:25 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:26 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:26 GMT

< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:26 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:27 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:27 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:28 GMT

< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:28 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:29 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:29 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:29 GMT

< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:30 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:30 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:31 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:31 GMT

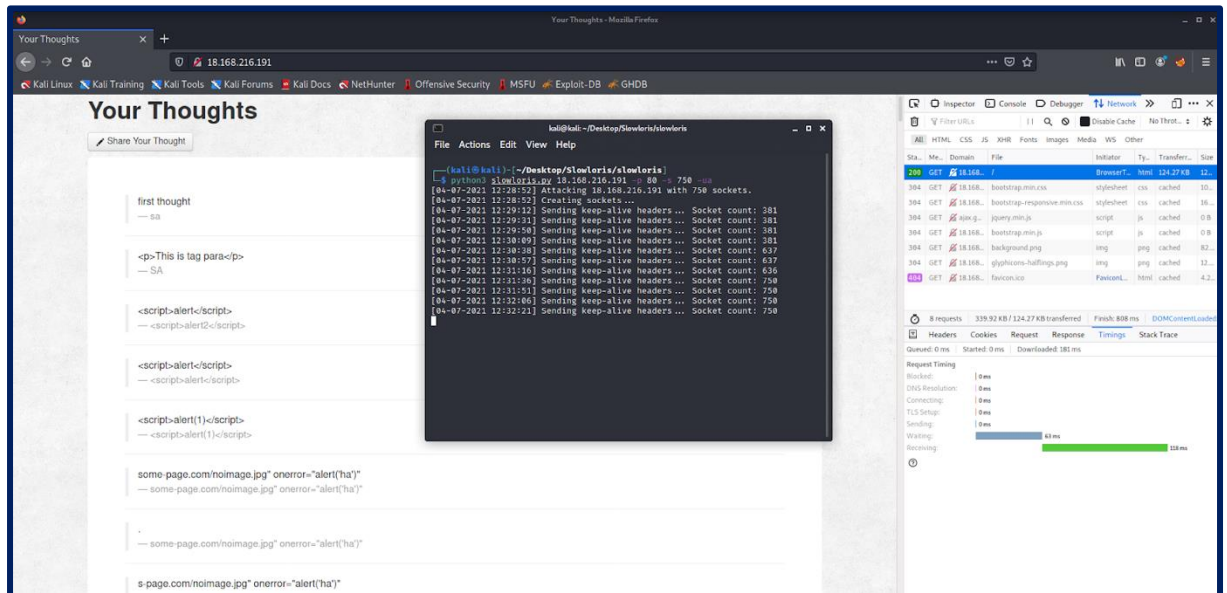
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:32 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:32 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:32 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:33 GMT

< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:33 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:34 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:34 GMT
< Server: Apache
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
< HTTP/1.1 200 OK
< Date: Mon, 24 May 2021 11:52:35 GMT

nismgroupb-env.eba-3ytnmtgq.us-east-1.elasticbeanstalk.com does Load-balancing.

Found via Methods: HTTP[Diff]

g. DOS Attack using Slowloris



Slowloris is basically an HTTP Denial of Service attack that affects threaded servers. It works like this:

- We start making lots of HTTP requests.
- We send headers periodically (every ~15 seconds) to keep the connections open.
- We never close the connection unless the server does so. If the server closes a connection, we create a new one keep doing the same thing.
- This exhausts the servers thread pool and the server can't reply to other people.

Ran Slowloris against target IP on Port 80 (HTTP). The DOS attack was using 750 sockets and I have added randomized user-agents for each request ("ua" flag on command).

As you can see on the right side, the request timings of the website have only been impacted slightly. The usual waiting time was at around 40-50ms, and while running

the attack, the timing only increased slightly to 60ms. The DOS attack overall only had a minor impact on the application.

Full command:

```
python3 slowloris.py 18.168.216.191 -p 80 -s 750 -ua
```

Github Repo for Script:

<https://github.com/gkbrk/slowloris>

- Metasploit Framework - Testing against Target

TARGET: 18.168.216.191

URL: www.123easyinvite.com

#####

h. SSH Version:

SSH-2.0-OpenSSH_7.4 (service.version=7.4 service.vendor=OpenBSD

service.family=OpenSSH service.product=OpenSSH

service.cpe23=cpe:/a:openbsd:openssh:7.4 service.protocol=ssh

fingerprint_db=ssh.banner)

#####

i. WMAP:

msf6 auxiliary(scanner/ssh/ssh_version) > wmap_run -t

[*] Testing target:

[*] Site: 18.168.216.191 (18.168.216.191)

[*] Port: 80 SSL: false

=====

[*] Testing started. 2021-07-04 12:04:53 -0400

[*] Loading wmap modules...

[*] 39 wmap enabled modules loaded.

[...]

+++++

Launch completed in 4553.764599323273 seconds.

+++++

[*] Done.

msf6 auxiliary(scanner/ssh/ssh_version) > wmap_vulns -l

[*] + [18.168.216.191] (18.168.216.191): scraper /

[*] scraper Scraper

[*] GET Your Thoughts

[*] + [18.168.216.191] (18.168.216.191): directory /git/

[*] directory Directory found.

[*] GET Res code: 200

[*] + [18.168.216.191] (18.168.216.191): file /index.php

[*] file File found.

[*] GET Res code: 404

[*] + [18.168.216.191] (18.168.216.191): file /assets

[*] file File found.

[*] GET Res code: 301

msf6 auxiliary(scanner/ssh/ssh_version) > vulns

Vulnerabilities

=====

Timestamp Host Name References

Metasploit was able to identify the SSH version used on the server. Although some information was leaked (see directories/files that were found in WMAP output), the WMAP module was not able to find any vulnerabilities within the Web Application itself.

No CVEs found for OpenSSH 7.4 either:

The screenshot shows the CVE Details website interface. At the top, there's a search bar with a 'Search' button and a 'View CVE' button. Below the search bar, the page title is 'CVE Details' with the tagline 'The ultimate security vulnerability datasource'. The main content area shows a search for 'Openbsd » Openssh » 7.4 P1: Security Vulnerabilities'. The search results are empty, displaying a message: 'Could not find any vulnerabilities matching the requested criteria'. The page also includes a sidebar with navigation links like 'Home', 'Browse', 'Reports', and 'Search'. The bottom of the page shows 'Total number of vulnerabilities : 0' and 'Page : 1'.

Source: https://www.cvedetails.com/vulnerability-list/vendor_id-97/product_id-585/version_id-228285/Openbsd-Openssh-7.4.html

Reference List

Bird & Bird LLP (2021) *Cookies: impact of UK GDPR and DPA 2018*. Available from:

[https://uk.practicallaw.thomsonreuters.com/w-016-7485?transitionType=Default&contextData=\(sc.Default\)#co_anchor_a935319](https://uk.practicallaw.thomsonreuters.com/w-016-7485?transitionType=Default&contextData=(sc.Default)#co_anchor_a935319) [Accessed 16 July 2021].

Bodulovic, G., Wang, S., de Morpurgo, M. and Saunders, E. (2020) *Telehealth around the world: A global guide*. Available from:

<https://www.dlapiper.com/en/italy/insights/publications/2020/11/telehealth-around-the-world-global-guide/> [Accessed 15 July 2021].

Information Commissioner's Office (2021) *An overview of the Data Protection Act 2018*.

Available from: <https://ico.org.uk/media/for-organisations/documents/2614158/ico-introduction-to-the-data-protection-bill.pdf> [Accessed 15 July 2021].

Information Commissioner's Office (2021) *Guide to the General Data Protection Regulation*

(GDPR). Available from: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf> [Accessed 15 July 2021].

Information Commissioner's Office (2021) *What is personal data?* Available from:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/> [Accessed 15 July 2021].

IT Governance Ltd (2017) *Penetration Testing and the GDPR*. Available from:

<https://www.itgovernance.co.uk/green-papers/penetration-testing-and-the-gdpr> [Accessed 18 July 2021].

Burgess, M (2020). What is GDPR? The summary guide to GDPR compliance in the UK. [online] WIRED UK. Available from: <<https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018> [Accessed 15 July 2021].

The National Archives (2021) *Data Protection Act 2018*. Available from: <https://www.legislation.gov.uk/ukpga/2018/12/section/94/enacted> [Accessed 15 July 2021].