VULNERABILITY ASSESSMENT REPORT

Zero Health Corp

Melvin Baird

Cyber Security Analyst

3rd July, 2025

Table of Contents

1 Executive Summary.....Error! Bookmark not defined.

2. Methodology ……..3

4. Endpoint detection and Ports scanning ……..……..4

5. Enumeration of Web application ……..13

6. Risk assessment ,……15

7. Recommendations ……17

10. Conclusion ……..18

11. References ……..1

Executive Summary

Zero Health Corp is experiencing reported slow system performance and unexpected failed

login attempts on their admin portal. A vulnerability assessment was conducted by me on

the organization`s network and many vulnerabilities were found ranging from easy access to

gain root/admin user privilege, to weak webpages which allows an attacker to gain

unauthorized access to the server and tweak the system or upload payloads onto your

server and web applications, having access to sensitive files and having the power to move,

modify or delete same. These vulnerabilities were classified according to different levels of

severity (High, Medium, and Low), and recommendations to mitigate them.

Methodology

I adopted an approach where information about the target is obtained from available

information exposed from scanning the ports with running services on the targets servers

and also, their webpage. I used tools like Nmap and Nikto for scanning the ports for

vulnerabilities, searchsploit and Metasploit to gain root access, and carried out webpage

enumeration to gain more information to aid my access. Also used national vulnerability

database(NVD) of National institute of Standard technology (NIST) to obtain the CVE and

CVSS ratings for the vulnerabilities found

Endpoints detection and Ports scanning

- Identification of the endpoints on the network by running command
  sudo netdiscover -r 192.168.X.0/24
  the 0/24 mandates the system range check for the different hosts on the network.

```
File  Actions  Edit  View  Help
Currently scanning: Finished!   |   Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 540
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.[redacted]    78:8d:af:6c:6a:43      3     180  Unknown vendor
192.168.[redacted]    f8:e4:e3:e7:e3:b6      1      60  Intel Corporate
192.168.[redacted]    36:3b:3c:cc:f9:0c      1      60  Unknown vendor
192.168.[redacted]    b6:88:27:24:97:a9      1      60  Unknown vendor
192.168.[redacted]    96:54:8e:a1:d2:79      1      60  Unknown vendor
192.168.[redacted]    08:00:27:ed:15:1d      1      60  PCS Systemtechnik GmbH
192.168.[redacted]    08:fb:ea:3f:14:c8      1      60  AMPAK Technology,Inc.
```

I was able to identify the target IP from the MAC vendor/hostname as PCS Systemtechnik GmbH in the list above. Also identified other vendors to ascertain there is no unauthorized endpoint on the network

- Run Nmap scan to check for open ports with running services on the target network,
  Command - Nmap target IP

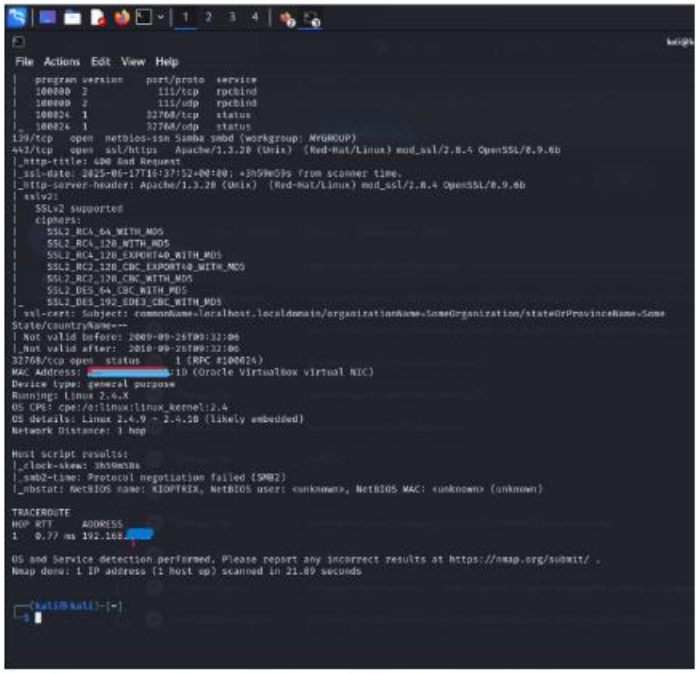
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.[redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-22 15:57 EDT
Nmap scan report for 192.168.[redacted]
Host is up (0.00011s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
32768/tcp open  filenet-tms
MAC Address: [redacted]:1D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

┌──(kali㉿kali)-[~]
└─$
```

From the above screenshot, it shows that 1000 ports were scanned and 994 ports were closed, there were 6 open ports with different services running on them. (ssh on port 22,

http on port 80, rpcbind on port 111, netbios-ssn on port 139, https on Port 443 and filenet-tms on port 32768).

To get a more indepth information on the services running on the open ports, a deeper Nmap scan is executed with command - Nmap -A -p- -T4 target IP

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap -A -p- -T4 192.168.0.[redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-17 08:37 EDT
Nmap scan report for 192.168.[redacted]
Host is up (0.00077s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_sshv1: Server supports SSHv1
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1          32768/tcp   status
|_  100024  1          32768/udp   status
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: 400 Bad Request
|_ssl-date: 2025-06-17T16:37:52-00:00; +3h59m59s from scanner time.
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=Some
State/countryName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
32768/tcp open  status     1 (RPC #100024)
MAC Address: [redacted] (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
```



```
File  Actions  Edit  View  Help
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1          32768/tcp   status
|_  100024  1          32768/udp   status
139/tcp   open  netbios-ssn Samba smbd (workgroup: WYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: 400 Bad Request
|_ssl-date: 2025-06-17T16:37:52+00:00; +3h59m59s from scanner time.
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=Some
State/countryName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
32768/tcp open  status    1 (RPC #100024)
MAC Address: [redacted]:10 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_clock-skew: 3h59m59s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   0.77 ms 192.168.[redacted]

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 21.89 seconds

┌──(kali㉿kali)-[~]
└─$
```

This scan gave a similar report as the first scan but with more details. 65,535 ports were scanned, and 65,529 were closed, showing more details on services running on same 6 open ports as the prior scan.

- **Port 22** is open with ssh service running on version Open SSH 2.9p2 (protocol 1.99) . It also revealed 3 host keys which can be used to verify the identity of a server when a client connects.
- **Port 80** is open with http services running on it. The server version also revealed as Apache httpd 1.3.20 mod ssl/2.8.4 open SSL/0.9,6b
- **Port 111** is open with remote procedure call services, (RPCBind), port used for communication between programs on different machines.
- **Port 139** is open with netbios-ssn service. Service Message block protocol is used here for file and printer sharing on windows network.
- **Port 443** is open with https services running, on same server version as port 80. The SSL certificate directory is shown in the Nmap scan.

- **Port 32768** is an open and dynamic port that binds with RPC services like port 139, peer to peer applications for gaming consoles and so on.

  The operating system version of our target IP is equally revealed at the end of the scan as **Linux 2.4.x**, falling within the version ranges of **Linux 2.4.9 to 2.4.18.**

To further get more information before i go in-depth into my assessment, I ran a broader scan using **Nmap** to scan each port individually. Also, i used another tool – **Nikto** to give more information on ports 80 and 443.

To scan individual ports, run command – Nmap -p22 -script=vuln 192.168.x.x and do same for all other open ports replacing the port number for each run.

```
└─$ sudo su
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -p22 -script=vuln 192.168.[redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-21 12:50 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.[redacted]
Host is up (0.00054s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: [redacted] (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 35.04 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p80 -script=vuln 192.168.[redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-21 12:51 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:01:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.49% done; ETC: 12:53 (0:00:03 remaining)
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.12% done; ETC: 12:53 (0:00:01 remaining)
Nmap scan report for 192.168.[redacted]
Host is up (0.00053s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|   /test.php: Test page
|   /icons/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|   /manual/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|_  /usage/: Potentially interesting folder
```

/home/kali

File Actions Edit View Help

```
|   /icons/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|   /manual/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|_  /usage/: Potentially interesting folder
MAC Address: [redacted]:1D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 132.95 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p111 -script=vuln 192.168.[redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-21 12:53 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.[redacted]
Host is up (0.00049s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
MAC Address: [redacted]:1D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.89 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p443 -script=vuln 192.168.[redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-21 12:54 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.49% done; ETC: 12:55 (0:00:00 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.49% done; ETC: 12:55 (0:00:00 remaining)
Stats: 0:01:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.49% done; ETC: 12:56 (0:00:03 remaining)
Stats: 0:03:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.49% done; ETC: 12:58 (0:00:06 remaining)
Nmap scan report for 192.168.[redacted]
Host is up (0.00039s latency).

PORT    STATE SERVICE
443/tcp open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| ssl-dh-params:
|   VULNERABLE:
```

```
File  Actions  Edit  View  Help
Nmap scan report for 192.168.[redacted]
Host is up (0.00039s latency).

PORT    STATE SERVICE
443/tcp open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| ssl-dh-params:
|   VULNERABLE:
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2015-4000  BID:74733
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: mod_ssl 2.0.x/512-bit MODP group with safe prime modulus
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://www.securityfocus.com/bid/74733
|       https://weakdh.org
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: mod_ssl 2.0.x/1024-bit MODP group with safe prime modulus
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

Nikto -h 192.1668.x.x .ssl

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.[redacted]
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.[redacted]
+ Target Hostname:    192.168.[redacted]
+ Target Port:        80
+ Start Time:         2025-06-18 17:59:50 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ /: Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2898, mtime: Wed Sep  5 23:
12:46 2001. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/
Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
ilities/missing-content-type-header/
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ OpenSSL/0.9.6b appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branc
h and will be supported until Nov 11 2023.
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x
 branch.
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2
006-3918
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-commun
ity/attacks/Cross_Site_Tracing
+ Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution.
+ Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to ki
ll any process on the system.
+ Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote sh
ell.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
^[[@^[[@^[[@+ /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scriptin
g (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0835
+ /manual/: Directory indexing found.
+ /manual/: Web server manual found.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsread
me/
+ /test.php: This might be interesting.
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was
found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file ma
nager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was f
ound.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
```

```
1  2  3  4
Minimize all open windows and show the desktop
File  Actions  Edit  View  Help
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file ma
nager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was f
ound.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was
found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ /wp-config.php#: wp-config.php# file found. This file contains the credentials.
+ 8908 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time:           2025-06-18 18:05:56 (GMT-4) (366 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.[redacted] .ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.[redacted]
+ Target Hostname:    192.168.[redacted]
+ Target Port:        80
+ Start Time:         2025-06-18 18:10:03 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ /: Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep  5 23:
12:46 2001. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/
Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
ilities/missing-content-type-header/
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x
 branch.
```

```
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x
 branch.
+ OpenSSL/0.9.6b appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branc
h and will be supported until Nov 11 2023.
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2
006-3918
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-commun
ity/attacks/Cross_Site_Tracing
+ Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution.
+ Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to ki
ll any process on the system.
+ Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote sh
ell.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). See
: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0835
+ /manual/: Directory indexing found.
+ /manual/: Web server manual found.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsread
me/
+ /test.php: This might be interesting.
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was
found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file ma
nager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was f
ound.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was
found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ /Wwp-config.php#: Wwp-config.phpE file found. This file contains the credentials.
+ 8908 requests: 0 error(s) and 38 item(s) reported on remote host
+ End Time:           2025-06-18 18:10:40 (GMT-4) (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

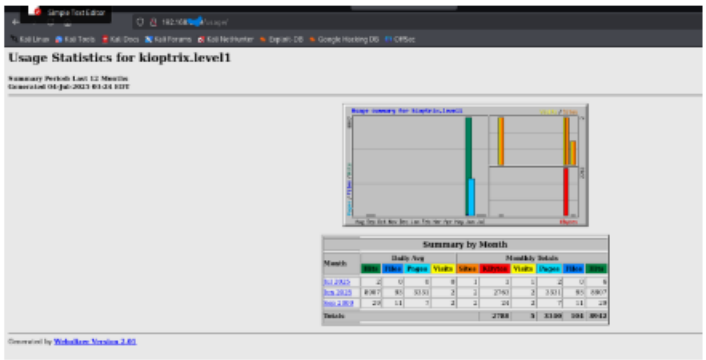
Enumeration of the web application

The screenshot below shows the webpage of our target (192.168.x.x) and the different types of information exposed online that attackers can easily use to gain access and exploit.

The webpage is verbose, exposing too much information ranging from

- The operating OS (Linux version), Red-hat Linux 6.2
- DocumentRoot
- The target server (Apache/1.3.20 Server) at 127.0.0.1
- The port its running on, (Port 80)
- Path Traversal/Directory Traversal
- Source code

Also, the URL on the webpage allows for SQL injection to gain access to other information within the server. For example, /usage/ was added to the URL and it took me to a page where information on the data on frequency of visits by users to this website, the number files accessed, file size, number of pages, and number of sites at a given period. Such information become very useful to attackers who may be planning a DDoS attack, as it helps them to gather information about the target.



Ports	Vulnerability	Description	CVSS score
22	Broadcast-avahi DoS. avahi packet DoS CVE-2011-1002	avahi-core/socket's in avahi-daemon in Avahi before 0.6.29 allows remote attackers to cause a denial of service	5.0 (medium)

		(infinite loop) via an empty mDNS (1) IPv4 or (2) IPv6 UDP packet to port 5353. NOTE: this vulnerability exists because of an incorrect fix for CVE 201	
80	Apache mod_ssl < 2.8.4 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) CVE-2002-0082 Mod_ssl/2.8.4, Apache/1.3.20 and Open SSL/0.9.6b are outdated Apache HTTP Server 1.3.22 through 1.3.27 CVE-2003-1418 HTTP trace is active CVE-2006-3918	A critical security flaw in the session caching feature of mod_ssl (before version 2.8.7-1.3.23) and Apache-SSL (before 1.3.22+1.46) could allow an attacker to take control of the server. An attacker can trigger this by connecting with a specially crafted large client certificate. If the certificate is signed by a trusted authority, the server	7.5 (high) 4.3 (medium) 4.3 (medium)

		mishandles its data, causing a "buffer overflow," which can be exploited to execute malicious code. -Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod rewrite and mod_cgi. Apache HTTP Server 1.3.22 through 1.3.27 on OpenBSD allows remote attackers to obtain sensitive	**4.3 (medium**

		information via (1) the ETag header, which reveals the i-node number, or (2) multipart MIME boundary, which reveals child process IDs (PID) Apache HTTP server does not sanitize the Expect header from an HTTP request when it is reflected back in an error message, which	
		might allow cross-site scripting (XSS) style attacks using web client components that can send arbitrary headers in requests, as demonstrated using a Flash SWF fil	
111	RPCbind - DoS CVE-2017-8779 Privilege escalation CVE-2010-2064,	Specially crafted UDP packets to port 111 can trigger large and un-freed memory allocations. This can lead to the rpcbind service, or even the	7.5high

	CVE 2010-2061	**entire system, running out of memory and crashing, resulting in a denial of service. Local users could exploit symlink attacks on temporary files (/tmp/portmap.xdr, /tmp/rpcbind.xdr) to write to arbitrary files or potentially gain elevated privileges**	
139	**Samba smbd 3.x – 4.x vulnerability CVE-2009-3103**	**Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location, aka "SMBv2 Negotiation Vulnerability." NOTE: some of these**	**10.0high**

		details are obtained from third party information	
443	**TSL protocol DHE_EXPORT ciphers downgrade MitM (logjam) CVE-2015-4000**	**The TLS protocol 1.2 and earlier, when a DHE_EXPORT cipher suite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a Client Hello with DHE replaced by DHE_EXPORT and then rewriting a Server Hello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue**	**3.7(low)**
	SSL POODLE information leak CVE-2014-3566	**The SSL protocol 3.0, as used in OpenSSL through 1.0.11 and other products, uses nondetermiatic CBC padding, which makes it easier for MiTM attackers to obtain clear text data via a padding-oracle attack, aka the "POODLE" issue**	**3.4(low)**
32768		**Services could potentially be susceptible to DoS if it has flaws that allow it to be overwhelmed.**	**5.0 (medium)**

		avahi-core/socket's in avahi-daemon in Avahi before 0.6.29 allows remote attackers to cause a denial of service (infinite loop) via an empty mDNS (1) IPv4 or (2) IPv6 UDP packet to port 5353. NOTE: this vulnerability exists because of an incorrect fix for CVE 2010-2244	

Recommendations

All the vulnerabilities found need to be addressed irrespective of the classification, high,

medium or low. But the high-risk vulnerabilities should be prioritized, followed by addressing

the medium risk, and finally the low-risk vulnerabilities.

Following my findings, here are my recommendations

1. Strong authentication methods: password authentication should be disabled,

generate strong SSH keys using ssh-keygen to create strong passphrase protected

keys. secure private keys and have periodic key review and rotation. Be sure to

implement MFA, strong passwords if password authentication is necessary.

2. SSH server configuration hardening: disable root login, limit user access, disable

unnecessary modules/features, set session timeouts, increase log, ing level and

alerts of suspicious access, and enable strict modes.

3. Network and Firewall Security: Set firewall rules to only allow SSH connections from

trusted IP addresses or networks. Have Intrusion Prevention/Detection Systems

(IPS/IDS) on the server with proper monitoring and audit of logs, perform

vulnerability scans regularly. Also web application firewall (WAF)

4. Software maintenance: regular software updates and patch management

5. Enforce HTTPS and Strong TLS Configuration: configure web server to redirect HTTP

to HTTPS on the server to ensure secure connection. Implement HSTS (HTTP Strict

Transport Security, use Strong TLS Protocols and Ciphers. Obtain Reputable SSL/TLS

Certificates.

6. Limit Information Disclosure: Delete default web pages, sample scripts, and

documentation files that could expose information or vulnerabilities. Disable Server

Banners, Implement custom error pages to avoid revealing internal system details

through default error messages

7. Input Validation and Sanitization: Rigorously validate and sanitize all user input to

prevent common attacks like unauthorised SQL Injection, Cross-Site Scripting (XSS),

Command Injection, Path Traversal/Directory Traversal

8. Network segmentation: Separate network segments from internal resources to limit

lateral movement in case of a breach

9. Disable NetBIOS over TCP/IP (NBT) and SMBv1: Ensure no critical legacy applications

or devices rely solely on NetBIOS for name resolution or file sharing before doing

this. Enable SMB Encryption, signing and utilize modern SMB versions

Conclusion

Zero Health Corp runs on a network structure that has vulnerabilities easily exploitable by

attackers as shown in this assessment. High-risk Vulnerabilities found as at the time of this

report are 3, Medium-risk vulnerabilities 5, while vulnerabilities of low risk are 2. The

management of Zero Health is advised to quickly address these vulnerabilities in order of

priority to prevent attackers from gaining access to exploiting these vulnerabilities with the

intention to harm the Corp, which may lead to financial losses, data breach and loss, loss of

confidentiality, legal issues among others. The mitigation steps are listed in the

recommendation for necessary ACTi

REFERENCE:

https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/securing_networks/securing-network-services_securing-networks