# Red Team: Summary of Operations

## 

## Table of Contents

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### Exposed Services

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

**nmap -v -sV -O 192.168.1.110**

|  |
| --- |
| root@Kali:~# **nmap -v -sV -O 192.168.1.110**  Starting Nmap 7.91 ( <https://nmap.org> ) at 2020-12-12 02:57 PST  NSE: Loaded 45 scripts for scanning.  Initiating ARP Ping Scan at 02:57  Scanning 192.168.1.110 [1 port]  Completed ARP Ping Scan at 02:57, 0.09s elapsed (1 total hosts)  Initiating Parallel DNS resolution of 1 host. at 02:57  Completed Parallel DNS resolution of 1 host. at 02:57, 0.02s elapsed  Initiating SYN Stealth Scan at 02:57  Scanning 192.168.1.110 [1000 ports]  Discovered open port 139/tcp on 192.168.1.110  Discovered open port 80/tcp on 192.168.1.110  Discovered open port 445/tcp on 192.168.1.110  Discovered open port 111/tcp on 192.168.1.110  Discovered open port 22/tcp on 192.168.1.110  Completed SYN Stealth Scan at 02:57, 0.08s elapsed (1000 total ports)  Initiating Service scan at 02:57  Scanning 5 services on 192.168.1.110  Completed Service scan at 02:57, 11.02s elapsed (5 services on 1 host)  Initiating OS detection (try #1) against 192.168.1.110  NSE: Script scanning 192.168.1.110.  Initiating NSE at 02:57  Completed NSE at 02:57, 0.03s elapsed  Initiating NSE at 02:57  Completed NSE at 02:57, 0.01s elapsed  Nmap scan report for 192.168.1.110  Host is up (0.00099s 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)  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  Uptime guess: 0.034 days (since Sat Dec 12 02:09:21 2020)  Network Distance: 1 hop  TCP Sequence Prediction: Difficulty=253 (Good luck!)  IP ID Sequence Generation: All zeros  Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux\_kernel  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: 1 IP address (1 host up) scanned in 14.04 seconds             Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.298KB) |

**nmap -v -sV -O 192.168.1.115**

|  |
| --- |
| root@Kali:~# **nmap -v -sV -O 192.168.1.115**  Starting Nmap 7.91 ( <https://nmap.org> ) at 2020-12-12 03:04 PST  NSE: Loaded 45 scripts for scanning.  Initiating ARP Ping Scan at 03:04  Scanning 192.168.1.115 [1 port]  Completed ARP Ping Scan at 03:04, 0.05s elapsed (1 total hosts)  Initiating Parallel DNS resolution of 1 host. at 03:04  Completed Parallel DNS resolution of 1 host. at 03:04, 0.01s elapsed  Initiating SYN Stealth Scan at 03:04  Scanning 192.168.1.115 [1000 ports]  Discovered open port 22/tcp on 192.168.1.115  Discovered open port 445/tcp on 192.168.1.115  Discovered open port 80/tcp on 192.168.1.115  Discovered open port 139/tcp on 192.168.1.115  Discovered open port 111/tcp on 192.168.1.115  Completed SYN Stealth Scan at 03:04, 0.08s elapsed (1000 total ports)  Initiating Service scan at 03:04  Scanning 5 services on 192.168.1.115  Completed Service scan at 03:04, 11.02s elapsed (5 services on 1 host)  Initiating OS detection (try #1) against 192.168.1.115  NSE: Script scanning 192.168.1.115.  Initiating NSE at 03:04  Completed NSE at 03:04, 0.03s elapsed  Initiating NSE at 03:04  Completed NSE at 03:04, 0.02s elapsed  Nmap scan report for 192.168.1.115  Host is up (0.00075s 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)  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  Uptime guess: 0.038 days (since Sat Dec 12 02:09:33 2020)  Network Distance: 1 hop  TCP Sequence Prediction: Difficulty=259 (Good luck!)  IP ID Sequence Generation: All zeros  Service Info: Host: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux\_kernel  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: 1 IP address (1 host up) scanned in 13.42 seconds             Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.298KB) |

The scans identify the services below as potential points of entry:

**Target 1**

**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

445/tcp open  netbios-ssn Samba smbd 3.X - 4.X

**Target 2**

**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

445/tcp open  netbios-ssn Samba smbd 3.X - 4.X

### Critical Vulnerabilities

Vulnerability scans identified 68 vulnerabilities – each found on both target machines.

**Top Five Highest rated Vulnerabilities Target 1 and Target 2**

CVE Severity Reference and Description

CVE-2020-11984 7.5 <https://vulners.com/cve/CVE-2020-11984>

*mod\_proxy\_uwsgi info disclosure and possible* RCE

CVE-2017-7679 7.5 <https://vulners.com/cve/CVE-2017-7679>

*mod\_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.*

CVE-2017-7668 7.5 https://vulners.com/cve/CVE-2017-7668

*The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap\_find\_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap\_find\_token() to return an incorrect value.*

CVE-2017-3169 7.5 <https://vulners.com/cve/CVE-2017-3169>

*mod\_ssl may dereference a NULL pointer when third-party modules call ap\_hook\_process\_connection() during an HTTP request to an HTTPS port.*

CVE-2017-3167 7.5 <https://vulners.com/cve/CVE-2017-3167>

*use of the ap\_get\_basic\_auth\_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.*

Vulnerability scan results Target 1

|  |
| --- |
| root@Kali:~# nmap --script vuln -sV -p80 192.168.1.110  Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-11 01:58 PST  Nmap scan report for 192.168.1.110  Host is up (0.00063s latency).  PORT STATE SERVICE VERSION  80/tcp open http Apache httpd 2.4.10 ((Debian))  | http-csrf:  | Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.110  | Found the following possible CSRF vulnerabilities:  |  | Path: http://192.168.1.110:80/  | Form id:  | Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01  |  | Path: http://192.168.1.110:80/service.html  | Form id:  | Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01  |  | Path: http://192.168.1.110:80/wordpress/  | Form id: search-form-5fd342f437716  | Form action: http://raven.local/wordpress/  |  | Path: http://192.168.1.110:80/contact.php  | Form id: myform  | Form action:  |  | Path: http://192.168.1.110:80/contact.php  | Form id:  |\_ Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01  |\_http-dombased-xss: Couldn't find any DOM based XSS.  | http-enum:  | /wordpress/: Blog  | /wordpress/wp-login.php: Wordpress login page.  | /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'  | /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'  | /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'  | /manual/: Potentially interesting folder  |\_ /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'  |\_http-server-header: Apache/2.4.10 (Debian)  |\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  | vulners:  | cpe:/a:apache:http\_server:2.4.10:  | CVE-2020-11984 7.5 https://vulners.com/cve/CVE-2020-11984  | CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679  | CVE-2017-7668 7.5 https://vulners.com/cve/CVE-2017-7668  | CVE-2017-3169 7.5 https://vulners.com/cve/CVE-2017-3169  | CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167  | EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB 7.2 https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB \*EXPLOIT\*  | CVE-2019-0211 7.2 https://vulners.com/cve/CVE-2019-0211  | 1337DAY-ID-32502 7.2 https://vulners.com/zdt/1337DAY-ID-32502 \*EXPLOIT\*  | CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312  | CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715  | CVE-2019-10082 6.4 https://vulners.com/cve/CVE-2019-10082  | CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788  | CVE-2019-10097 6.0 https://vulners.com/cve/CVE-2019-10097  | CVE-2019-0217 6.0 https://vulners.com/cve/CVE-2019-0217  | EDB-ID:47689 5.8 https://vulners.com/exploitdb/EDB-ID:47689 \*EXPLOIT\*  | CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927  | CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098  | 1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 \*EXPLOIT\*  | CVE-2016-5387 5.1 https://vulners.com/cve/CVE-2016-5387  | SSV:96537 5.0 https://vulners.com/seebug/SSV:96537 \*EXPLOIT\*  | MSF:AUXILIARY/SCANNER/HTTP/APACHE\_OPTIONSBLEED 5.0 https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/HTTP/APACHE\_OPTIONSBLEED \*EXPLOIT\*  | EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 5.0 https://vulners.com/exploitpack/EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 \*EXPLOIT\*  | EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D 5.0 https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D \*EXPLOIT\*  | CVE-2020-9490 5.0 https://vulners.com/cve/CVE-2020-9490  | CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934  | CVE-2019-10081 5.0 https://vulners.com/cve/CVE-2019-10081  | CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220  | CVE-2019-0196 5.0 https://vulners.com/cve/CVE-2019-0196  | CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199  | CVE-2018-17189 5.0 https://vulners.com/cve/CVE-2018-17189  | CVE-2018-1333 5.0 https://vulners.com/cve/CVE-2018-1333  | CVE-2018-1303 5.0 https://vulners.com/cve/CVE-2018-1303  | CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798  | CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710  | CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743  | CVE-2016-2161 5.0 https://vulners.com/cve/CVE-2016-2161  | CVE-2016-0736 5.0 https://vulners.com/cve/CVE-2016-0736  | CVE-2015-3183 5.0 https://vulners.com/cve/CVE-2015-3183  | CVE-2015-0228 5.0 https://vulners.com/cve/CVE-2015-0228  | CVE-2014-3583 5.0 https://vulners.com/cve/CVE-2014-3583  | 1337DAY-ID-28573 5.0 https://vulners.com/zdt/1337DAY-ID-28573 \*EXPLOIT\*  | 1337DAY-ID-26574 5.0 https://vulners.com/zdt/1337DAY-ID-26574 \*EXPLOIT\*  | CVE-2019-0197 4.9 https://vulners.com/cve/CVE-2019-0197  | EDB-ID:47688 4.3 https://vulners.com/exploitdb/EDB-ID:47688 \*EXPLOIT\*  | CVE-2020-11993 4.3 https://vulners.com/cve/CVE-2020-11993  | CVE-2020-11985 4.3 https://vulners.com/cve/CVE-2020-11985  | CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092  | CVE-2018-1302 4.3 https://vulners.com/cve/CVE-2018-1302  | CVE-2018-1301 4.3 https://vulners.com/cve/CVE-2018-1301  | CVE-2018-11763 4.3 https://vulners.com/cve/CVE-2018-11763  | CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975  | CVE-2015-3185 4.3 https://vulners.com/cve/CVE-2015-3185  | CVE-2014-8109 4.3 https://vulners.com/cve/CVE-2014-8109  | 1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 \*EXPLOIT\*  | CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283  | CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612  | PACKETSTORM:152441 0.0 https://vulners.com/packetstorm/PACKETSTORM:152441 \*EXPLOIT\*  | PACKETSTORM:140265 0.0 https://vulners.com/packetstorm/PACKETSTORM:140265 \*EXPLOIT\*  | EDB-ID:46676 0.0 https://vulners.com/exploitdb/EDB-ID:46676 \*EXPLOIT\*  | EDB-ID:42745 0.0 https://vulners.com/exploitdb/EDB-ID:42745 \*EXPLOIT\*  | EDB-ID:40961 0.0 https://vulners.com/exploitdb/EDB-ID:40961 \*EXPLOIT\*  | 1337DAY-ID-663 0.0 https://vulners.com/zdt/1337DAY-ID-663 \*EXPLOIT\*  | 1337DAY-ID-601 0.0 https://vulners.com/zdt/1337DAY-ID-601 \*EXPLOIT\*  | 1337DAY-ID-4533 0.0 https://vulners.com/zdt/1337DAY-ID-4533 \*EXPLOIT\*  | 1337DAY-ID-3109 0.0 https://vulners.com/zdt/1337DAY-ID-3109 \*EXPLOIT\*  | 1337DAY-ID-2237 0.0 https://vulners.com/zdt/1337DAY-ID-2237 \*EXPLOIT\*  | 1337DAY-ID-1415 0.0 https://vulners.com/zdt/1337DAY-ID-1415 \*EXPLOIT\*  |\_ 1337DAY-ID-1161 0.0 https://vulners.com/zdt/1337DAY-ID-1161 \*EXPLOIT\*  MAC Address: 00:15:5D:00:04:10 (Microsoft)  Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  Nmap done: 1 IP address (1 host up) scanned in 38.34 seconds |

Vulnerability scan results Target 2

|  |
| --- |
| root@Kali:~# nmap --script vuln -sV -p80 192.168.1.115  Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-11 02:04 PST  Nmap scan report for 192.168.1.115  Host is up (0.00073s latency).  PORT STATE SERVICE VERSION  80/tcp open http Apache httpd 2.4.10 ((Debian))  | http-csrf:  | Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.115  | Found the following possible CSRF vulnerabilities:  |  | Path: http://192.168.1.115:80/  | Form id:  | Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01  |  | Path: http://192.168.1.115:80/wordpress/  | Form id: search-form-5fd344347ed95  | Form action: http://raven.local/wordpress/  |  | Path: http://192.168.1.115:80/index.html  | Form id:  | Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01  |  | Path: http://192.168.1.115:80/service.html  | Form id:  | Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01  |  | Path: http://192.168.1.115:80/contact.php  | Form id: myform  | Form action:  |  | Path: http://192.168.1.115:80/contact.php  | Form id:  | Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01  |  | Path: http://192.168.1.115:80/team.html  | Form id:  |\_ Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01  |\_http-dombased-xss: Couldn't find any DOM based XSS.  | http-enum:  | /wordpress/: Blog  | /wordpress/wp-login.php: Wordpress login page.  | /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'  | /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'  | /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'  | /manual/: Potentially interesting folder  |\_ /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'  |\_http-server-header: Apache/2.4.10 (Debian)  |\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  | vulners:  | cpe:/a:apache:http\_server:2.4.10:  | CVE-2020-11984 7.5 https://vulners.com/cve/CVE-2020-11984  | CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679  | CVE-2017-7668 7.5 https://vulners.com/cve/CVE-2017-7668  | CVE-2017-3169 7.5 https://vulners.com/cve/CVE-2017-3169  | CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167  | EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB 7.2 https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB \*EXPLOIT\*  | CVE-2019-0211 7.2 https://vulners.com/cve/CVE-2019-0211  | 1337DAY-ID-32502 7.2 https://vulners.com/zdt/1337DAY-ID-32502 \*EXPLOIT\*  | CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312  | CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715  | CVE-2019-10082 6.4 https://vulners.com/cve/CVE-2019-10082  | CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788  | CVE-2019-10097 6.0 https://vulners.com/cve/CVE-2019-10097  | CVE-2019-0217 6.0 https://vulners.com/cve/CVE-2019-0217  | EDB-ID:47689 5.8 https://vulners.com/exploitdb/EDB-ID:47689 \*EXPLOIT\*  | CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927  | CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098  | 1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 \*EXPLOIT\*  | CVE-2016-5387 5.1 https://vulners.com/cve/CVE-2016-5387  | SSV:96537 5.0 https://vulners.com/seebug/SSV:96537 \*EXPLOIT\*  | MSF:AUXILIARY/SCANNER/HTTP/APACHE\_OPTIONSBLEED 5.0 https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/HTTP/APACHE\_OPTIONSBLEED \*EXPLOIT\*  | EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 5.0 https://vulners.com/exploitpack/EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 \*EXPLOIT\*  | EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D 5.0 https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D \*EXPLOIT\*  | CVE-2020-9490 5.0 https://vulners.com/cve/CVE-2020-9490  | CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934  | CVE-2019-10081 5.0 https://vulners.com/cve/CVE-2019-10081  | CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220  | CVE-2019-0196 5.0 https://vulners.com/cve/CVE-2019-0196  | CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199  | CVE-2018-17189 5.0 https://vulners.com/cve/CVE-2018-17189  | CVE-2018-1333 5.0 https://vulners.com/cve/CVE-2018-1333  | CVE-2018-1303 5.0 https://vulners.com/cve/CVE-2018-1303  | CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798  | CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710  | CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743  | CVE-2016-2161 5.0 https://vulners.com/cve/CVE-2016-2161  | CVE-2016-0736 5.0 https://vulners.com/cve/CVE-2016-0736  | CVE-2015-3183 5.0 https://vulners.com/cve/CVE-2015-3183  | CVE-2015-0228 5.0 https://vulners.com/cve/CVE-2015-0228  | CVE-2014-3583 5.0 https://vulners.com/cve/CVE-2014-3583  | 1337DAY-ID-28573 5.0 https://vulners.com/zdt/1337DAY-ID-28573 \*EXPLOIT\*  | 1337DAY-ID-26574 5.0 https://vulners.com/zdt/1337DAY-ID-26574 \*EXPLOIT\*  | CVE-2019-0197 4.9 https://vulners.com/cve/CVE-2019-0197  | EDB-ID:47688 4.3 https://vulners.com/exploitdb/EDB-ID:47688 \*EXPLOIT\*  | CVE-2020-11993 4.3 https://vulners.com/cve/CVE-2020-11993  | CVE-2020-11985 4.3 https://vulners.com/cve/CVE-2020-11985  | CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092  | CVE-2018-1302 4.3 https://vulners.com/cve/CVE-2018-1302  | CVE-2018-1301 4.3 https://vulners.com/cve/CVE-2018-1301  | CVE-2018-11763 4.3 https://vulners.com/cve/CVE-2018-11763  | CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975  | CVE-2015-3185 4.3 https://vulners.com/cve/CVE-2015-3185  | CVE-2014-8109 4.3 https://vulners.com/cve/CVE-2014-8109  | 1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 \*EXPLOIT\*  | CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283  | CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612  | PACKETSTORM:152441 0.0 https://vulners.com/packetstorm/PACKETSTORM:152441 \*EXPLOIT\*  | PACKETSTORM:140265 0.0 https://vulners.com/packetstorm/PACKETSTORM:140265 \*EXPLOIT\*  | EDB-ID:46676 0.0 https://vulners.com/exploitdb/EDB-ID:46676 \*EXPLOIT\*  | EDB-ID:42745 0.0 https://vulners.com/exploitdb/EDB-ID:42745 \*EXPLOIT\*  | EDB-ID:40961 0.0 https://vulners.com/exploitdb/EDB-ID:40961 \*EXPLOIT\*  | 1337DAY-ID-663 0.0 https://vulners.com/zdt/1337DAY-ID-663 \*EXPLOIT\*  | 1337DAY-ID-601 0.0 https://vulners.com/zdt/1337DAY-ID-601 \*EXPLOIT\*  | 1337DAY-ID-4533 0.0 https://vulners.com/zdt/1337DAY-ID-4533 \*EXPLOIT\*  | 1337DAY-ID-3109 0.0 https://vulners.com/zdt/1337DAY-ID-3109 \*EXPLOIT\*  | 1337DAY-ID-2237 0.0 https://vulners.com/zdt/1337DAY-ID-2237 \*EXPLOIT\*  | 1337DAY-ID-1415 0.0 https://vulners.com/zdt/1337DAY-ID-1415 \*EXPLOIT\*  |\_ 1337DAY-ID-1161 0.0 https://vulners.com/zdt/1337DAY-ID-1161 \*EXPLOIT\*  MAC Address: 00:15:5D:00:04:11 (Microsoft)  Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  Nmap done: 1 IP address (1 host up) scanned in 38.02 seconds |

Exploitation

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

**Target 1**

**Flag1** hash value: `b9bbcd33e11b80be759c4e844862482d`

Exploit Used

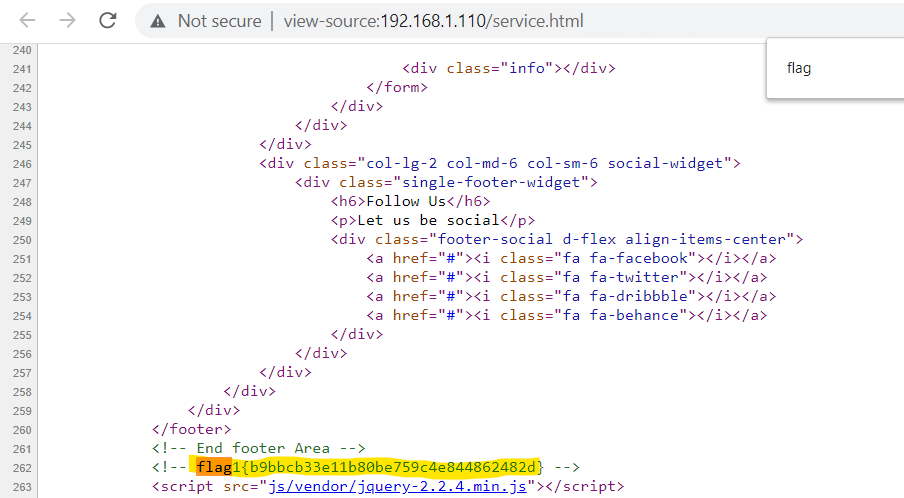
* CWE-540: Inclusion of Sensitive Information in Source Code

<https://cwe.mitre.org/data/definitions/540.html>

* CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

<https://cwe.mitre.org/data/definitions/200.html>

* Click SERVICE link > 192.168.1.110/service.html, Right Click, View Source



**Flag2** hash value: `fc3fd58dcdad9ab23faca6e9a36e581c`

Exploit Used

* CWE-521: Weak Password Requirements

<https://cwe.mitre.org/data/definitions/312.html>

* CWE-522: Insufficiently Protected Credentials

<https://cwe.mitre.org/data/definitions/522.html>

* an easily guessed password for user michael (ssh login), search file system to locate flag file in /var/www



**Flag3** hash value: `afc01ab5650591e7dccf93122770cd2`

Exploit Used

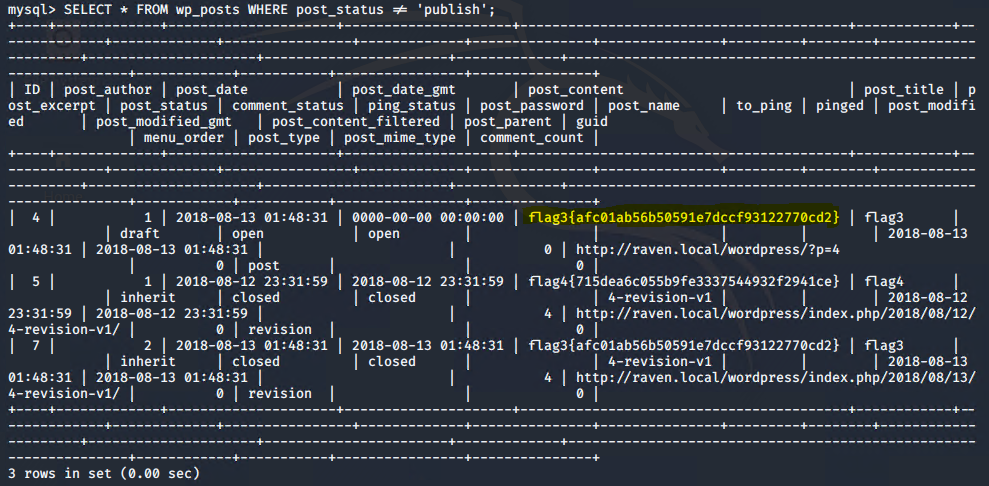
* CWE-260: Password in configuration file

<https://cwe.mitre.org/data/definitions/260.html>

* CWE-312: Cleartext Storage of Sensitive Information

<https://cwe.mitre.org/data/definitions/312.html>

* 'select \* FROM wp\_posts WHERE post\_status != 'publish''



**Flag4** hash value: `715dea6c055b9fe3337544932f2941ce`

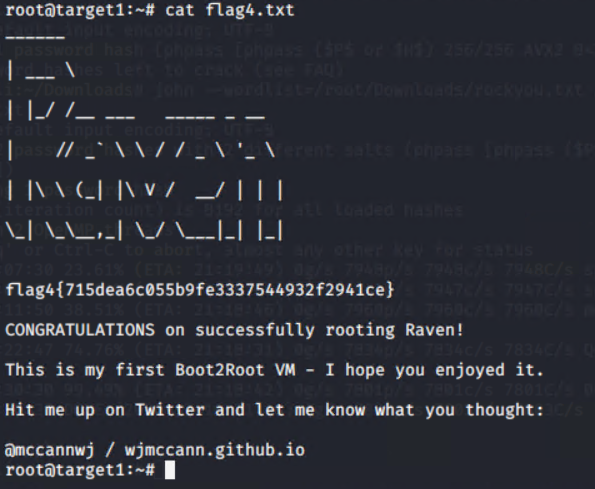
Exploit Used

* CWE-250: Execution with Unnecessary Privileges
* <https://cwe.mitre.org/data/definitions/250.html>

* CWE-269: Improper Privilege Management
* <https://cwe.mitre.org/data/definitions/269.html>
* CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

<https://cwe.mitre.org/data/definitions/22.html>

* used python script to gain a shell as root: 'python -c 'import pty;pty.spawn("/bin/bash")''

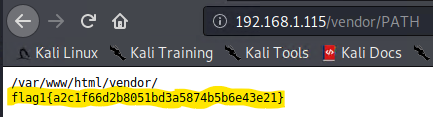


**Target 2**

**Flag1** hash value: `a2c1f66d2b8051db3a5874b5874b5b6e43e21`

Exploit Used

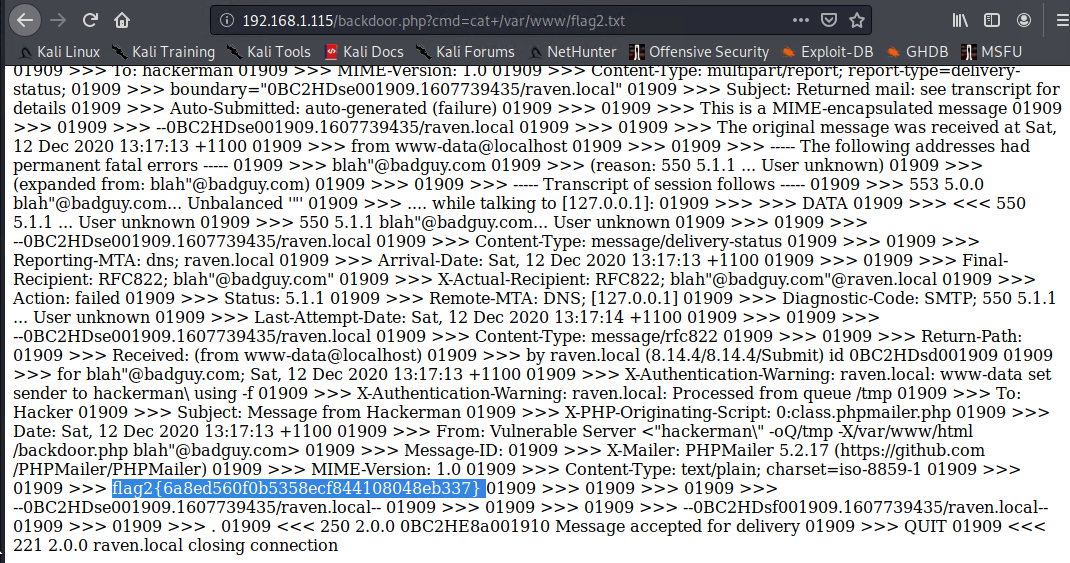
* CWE-548: Information leakage through directory listing
* CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
* http:// 192.168.1.115/vendor/PATH



**Flag2** hash value: `6a8ed560f0b5358ecf844108048eb337`

Exploit Used

* CWE-78: Improper Sanitization of Special Elements used in an OS Command
* CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
* CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
* '192.168.1.115/backdoor.php?cmd=find+/var/www+-type+f+iname+'flag\*''
* '192.168.1.115/backdoor.php?cmd=cat+/var/www/flag2.txt'



**Flag3** hash value: `a0f568aa9de277887f37730d71520d9b`

Exploit Used

* CWE-522: Local file inclusion / directory traversal
* CWE-548: Information leakage through directory listing
* CWE-250: Execution with Unnecessary Privileges
* '192.168.1.115/wordpress/wp-content/uploads/2018/11/flag3.png'

