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 192.168.1.0/24

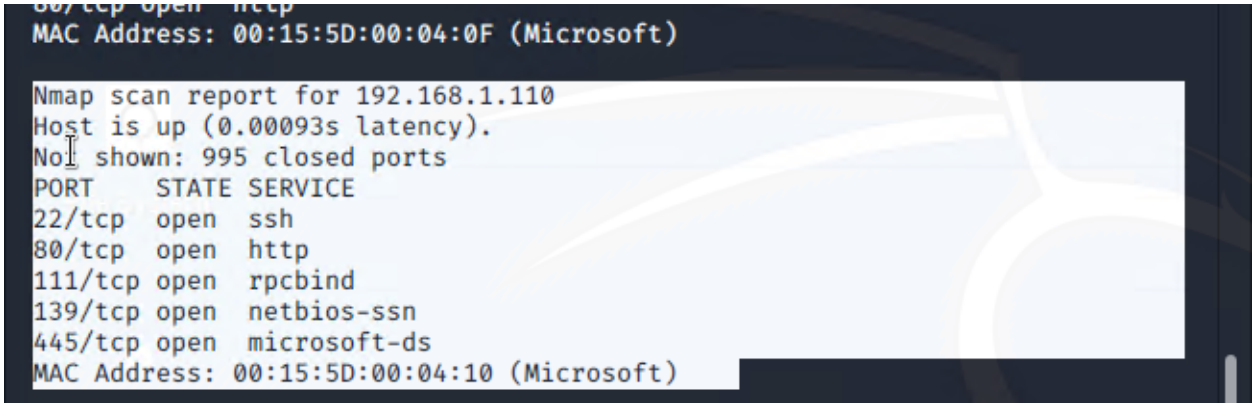
```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-06 14:07 PST
Nmap scan report for 192.168.1.1
Host is up (0.00065s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00044s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.0029s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.110
Host is up (0.0010s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
```

This scan identifies the services below as potential points of entry:
- Target 1 List of Exposed Services



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

The following vulnerabilities were identified on each target:
- Target 1 List of Critical Vulnerabilities

1. Port 22/tcp Open ssh services (cpe: /a:openbsd:openssh: 6.7pl)
   This vulnerability makes it easier for attackers to remotely attack and conduct brute-force attacks, or cause a denial of service.

   - CVE-2015-5600
   - CVSS Score 8.5
   - Confidentiality Impact Partial (There is considerable informational disclosure.)
   - Integrity Impact None (There is no impact to the integrity of the system)
   - Availability Impact Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
   - Access Complexity Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
   - Authentication Not required (Authentication is not required to exploit the vulnerability.)
   - Vulnerability Type(s) Denial Of Service/ Brute force attacks.

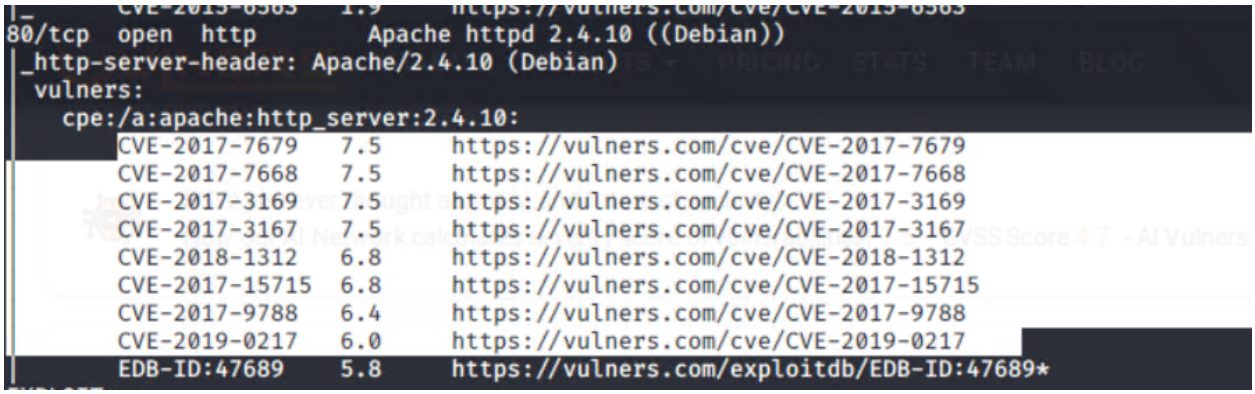
2. Port 80/tcp open http (Http-server-header : Apache /2.4.10 (Debian)

   In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

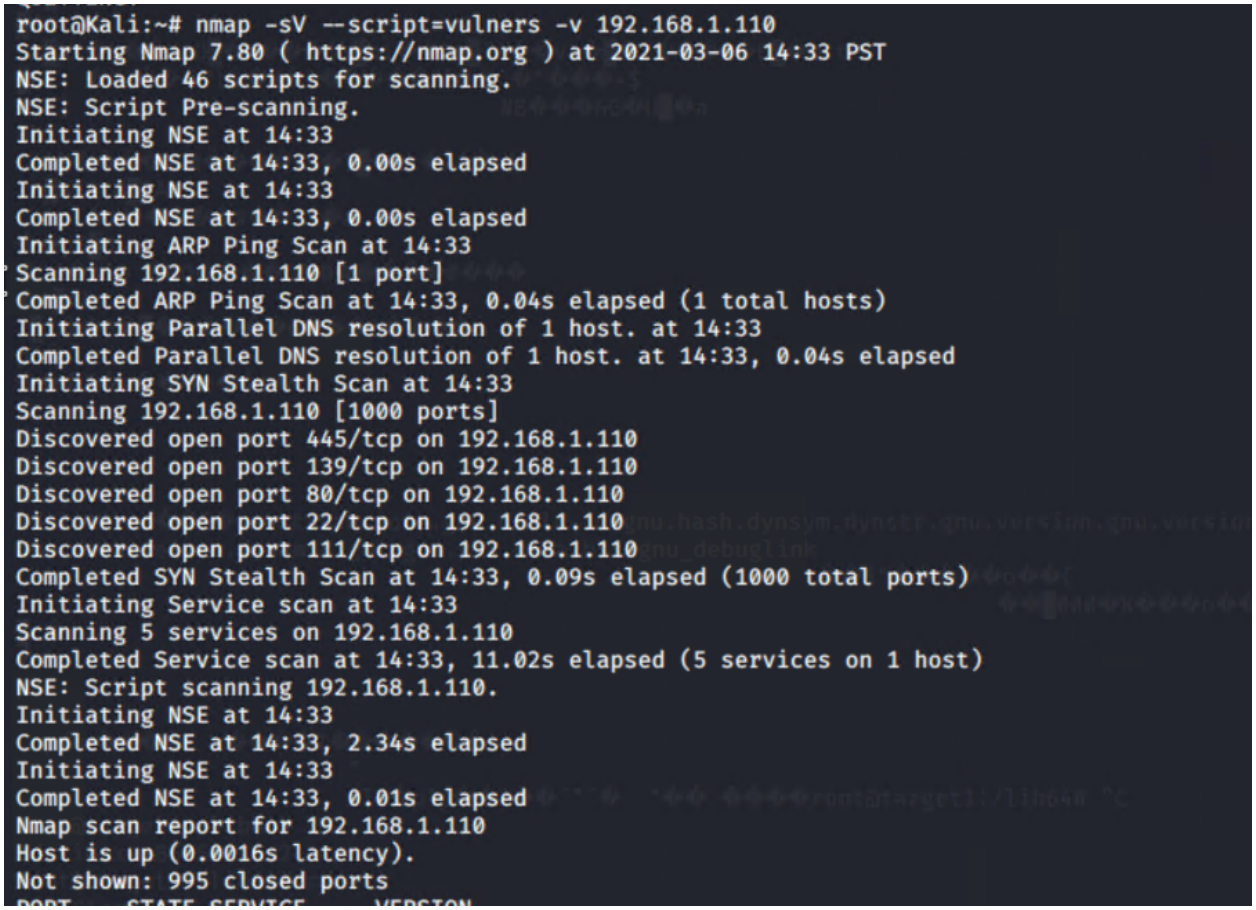
   - Vulnerability Details: CVE-2017-7679
   - CVSS Score 7.5
   - Confidentiality Impact : Partial (There is considerable informational disclosure.)
   - Integrity Impact: Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)

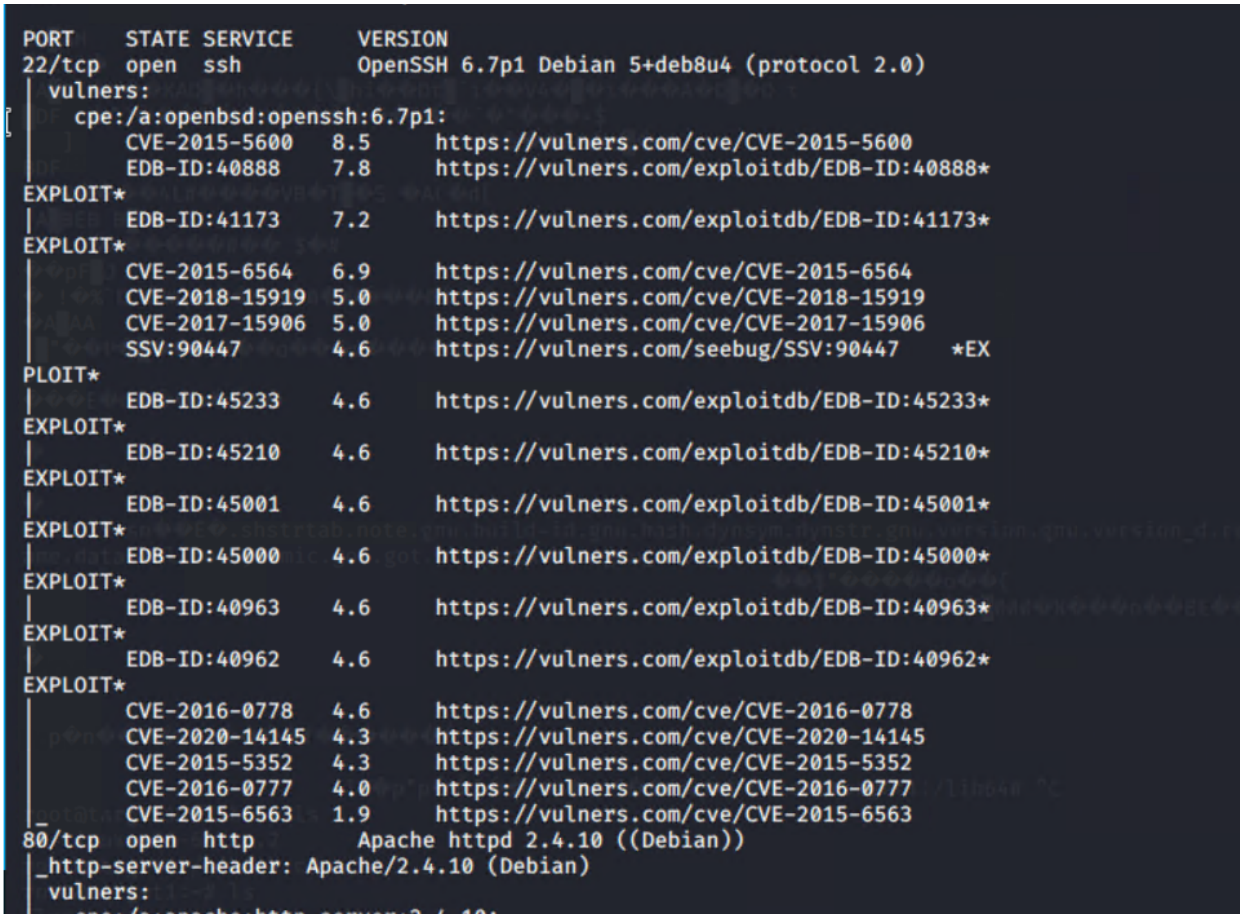
- Availability Impact: Partial (There is reduced performance or interruptions in resource availability.)
- Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
- Authentication : Not required (Authentication is not required to exploit the vulnerability.)
- Vulnerability Type(s) Overflow

Other vulnerabilities are ;



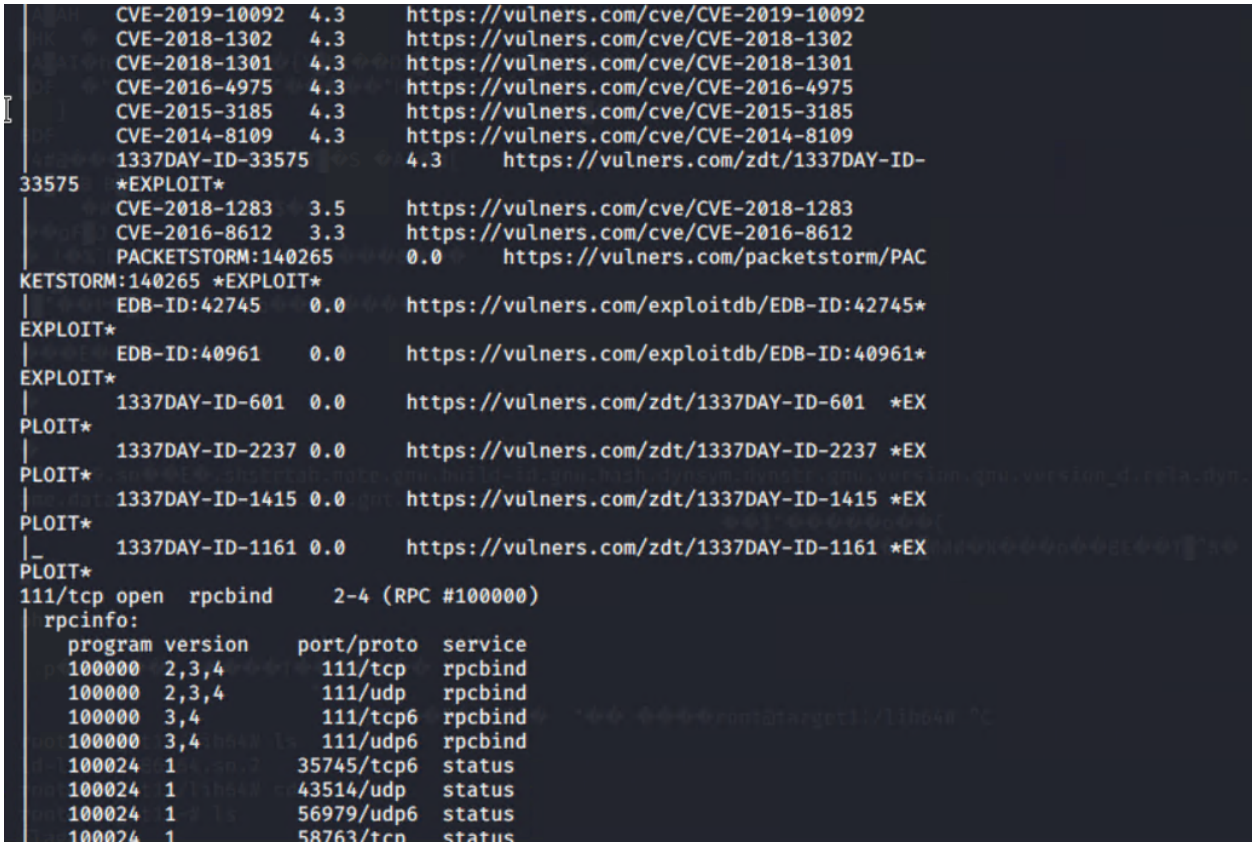
Vulnerability scan results to prove the identified vulnerabilities.


root@Kali:~# nmap -sV --script=vulners -v 192.168.1.110
Starting Nmap 7.80 (https://nmap.org) at 2021-03-06 14:33 PST
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:33
Completed NSE at 14:33, 0.00s elapsed
Initiating NSE at 14:33
Completed NSE at 14:33, 0.00s elapsed
Initiating ARP Ping Scan at 14:33
Scanning 192.168.1.110 [1 port]
Completed ARP Ping Scan at 14:33, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:33
Completed Parallel DNS resolution of 1 host. at 14:33, 0.04s elapsed
Initiating SYN Stealth Scan at 14:33
Scanning 192.168.1.110 [1000 ports]
Discovered open port 445/tcp on 192.168.1.110
Discovered open port 139/tcp on 192.168.1.110
Discovered open port 80/tcp on 192.168.1.110
Discovered open port 22/tcp on 192.168.1.110
Discovered open port 111/tcp on 192.168.1.110
Completed SYN Stealth Scan at 14:33, 0.09s elapsed (1000 total ports)
Initiating Service scan at 14:33
Scanning 5 services on 192.168.1.110
Completed Service scan at 14:33, 11.02s elapsed (5 services on 1 host)
NSE: Script scanning 192.168.1.110.
Initiating NSE at 14:33
Completed NSE at 14:33, 2.34s elapsed
Initiating NSE at 14:33
Completed NSE at 14:33, 0.01s elapsed
Nmap scan report for 192.168.1.110
Host is up (0.0016s latency).
Not shown: 995 closed ports



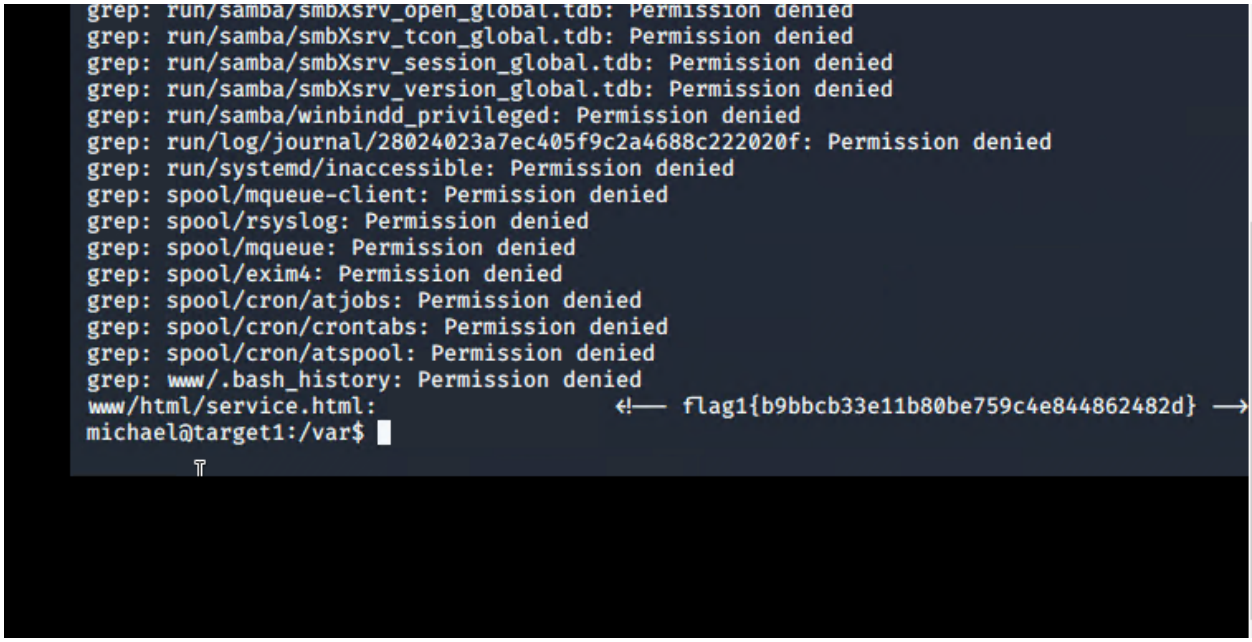
```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888*
EXPLOIT*
|       EDB-ID:41173    7.2     https://vulners.com/exploitdb/EDB-ID:41173*
EXPLOIT*
|       CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
|       CVE-2018-15919  5.0     https://vulners.com/cve/CVE-2018-15919
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       SSV:90447       4.6     https://vulners.com/seebug/SSV:90447    *EX
PLOIT*
|       EDB-ID:45233    4.6     https://vulners.com/exploitdb/EDB-ID:45233*
EXPLOIT*
|       EDB-ID:45210    4.6     https://vulners.com/exploitdb/EDB-ID:45210*
EXPLOIT*
|       EDB-ID:45001    4.6     https://vulners.com/exploitdb/EDB-ID:45001*
EXPLOIT*
|       EDB-ID:45000    4.6     https://vulners.com/exploitdb/EDB-ID:45000*
EXPLOIT*
|       EDB-ID:40963    4.6     https://vulners.com/exploitdb/EDB-ID:40963*
EXPLOIT*
|       EDB-ID:40962    4.6     https://vulners.com/exploitdb/EDB-ID:40962*
EXPLOIT*
|       CVE-2016-0778   4.6     https://vulners.com/cve/CVE-2016-0778
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2015-5352   4.3     https://vulners.com/cve/CVE-2015-5352
|       CVE-2016-0777   4.0     https://vulners.com/cve/CVE-2016-0777
|_      CVE-2015-6563   1.9     https://vulners.com/cve/CVE-2015-6563
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
| vulners:
```

```
|       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-2017-9788   6.4     https://vulners.com/cve/CVE-2017-9788
|       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    *EX
PLOIT*
|       MSF:AUXILIARY/SCANNER/HTTP/APACHE_OPTIONSBLEED  5.0     https://vul
ners.com/metasploit/MSF:AUXILIARY/SCANNER/HTTP/APACHE_OPTIONSBLEED      *EX
PLOIT*
|       EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7    5.0     https://vul
ners.com/exploitpack/EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7       *EX
PLOIT*
|       EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D    5.0     https://vul
ners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D       *EX
PLOIT*
|       CVE-2020-1934   5.0     https://vulners.com/cve/CVE-2020-1934
|       CVE-2019-0220   5.0     https://vulners.com/cve/CVE-2019-0220
|       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-2018-1303   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
```



Exploitation

The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:
- Target 1
`flag1.txt` hash value_
B9bbcb33e11b80be759c4e844862482d



- **Exploit Used**
  - _TODO: Identify the exploit used_

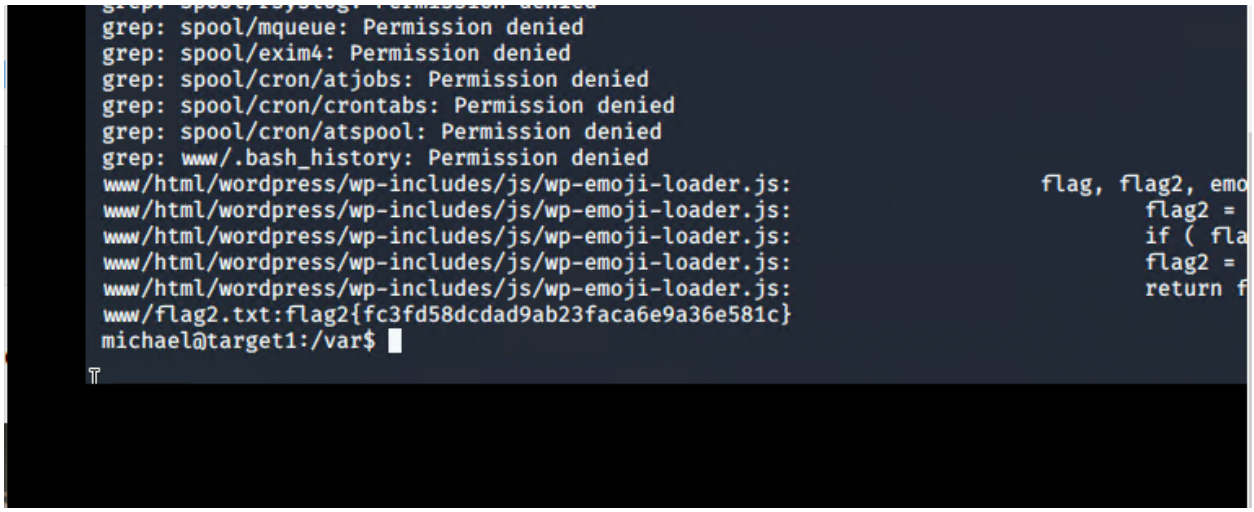
Gain SSH Access to Servers by Brute-Forcing Credentials

Ssh michael@192.168.1.110
Password Guess was “michael”
Cd into Var and grep for flag1.txt

Command run: /var$ grep -rw flag1 *

- `flag2.txt`: _ `flag2.txt` hash value_

Fc3fd58dcdad9ab23faca6e9a36e581c



- **Exploit Used**
  - _Identify the exploit used_

Gain SSH Access to Servers by Brute-Forcing Credentials
Cd into Var directory and Grep for flag2.txt
Grep for flag2.txt

- _The command to run_

/var$ grep -rw flag2 *