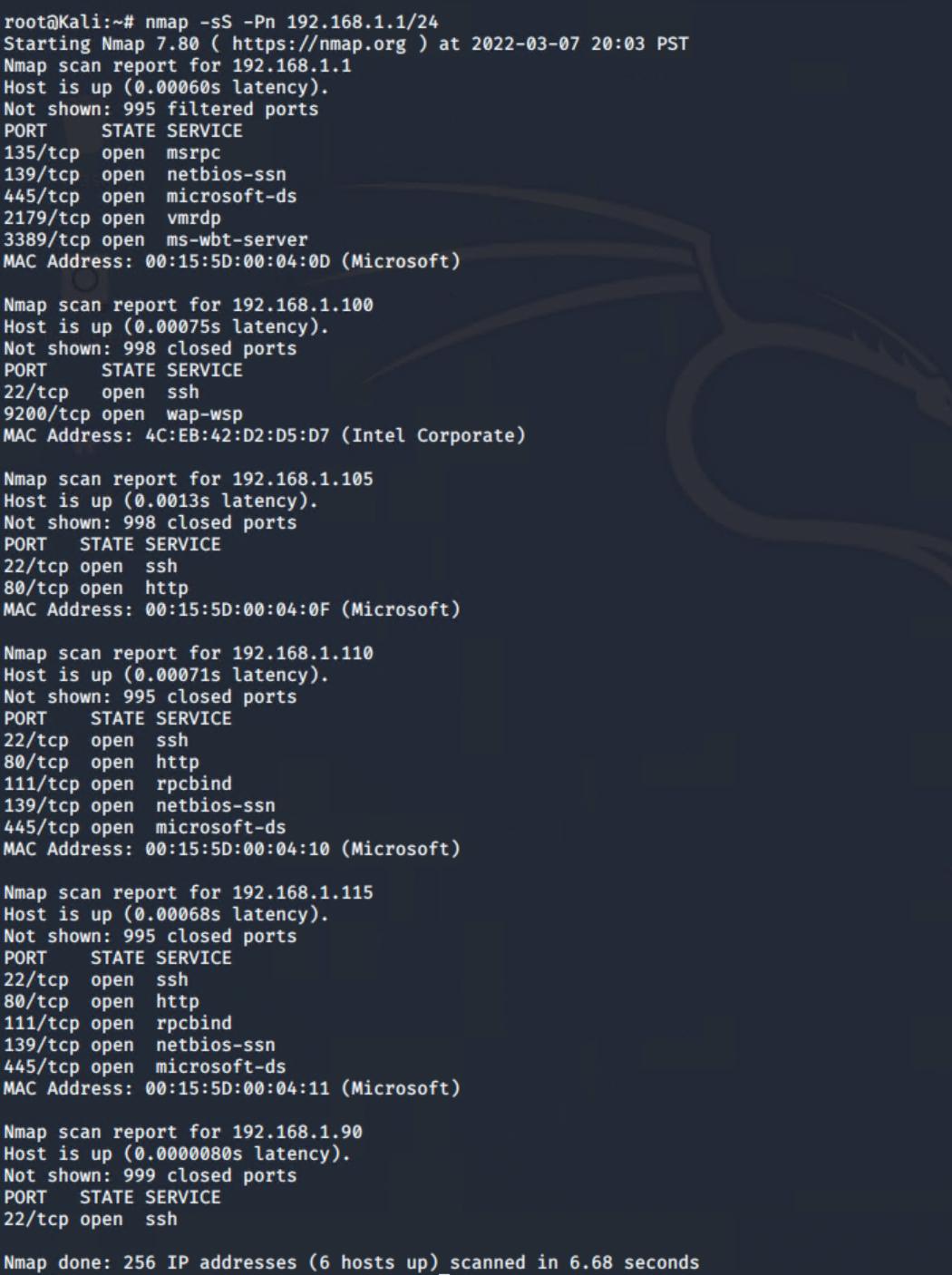
# **Red Team: Summary of Operations**

## **Table of Contents**

* [Exposed Services](#_eqv8yj8wokfw)
* [Critical Vulnerabilities](https://docs.google.com/document/d/14AyOpxkFVeIdks6w3nfCTGGtn3DG1Hf3bHn4gFAZLtU/edit#)
* [Exploitation](#_ncpt9tjrcwau)

### **Exposed Services**

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

**nmap -sS -Pn 192.168.1.1/24 **

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

Target 1

| **SERVICE** | **PORT** |
| --- | --- |
| ssh | 22 |
| http | 80 |
| rpcbind | 111 |
| netbios-ssn | 139 |
| microsoft-ds | 445 |

The following vulnerabilities were identified on each target:

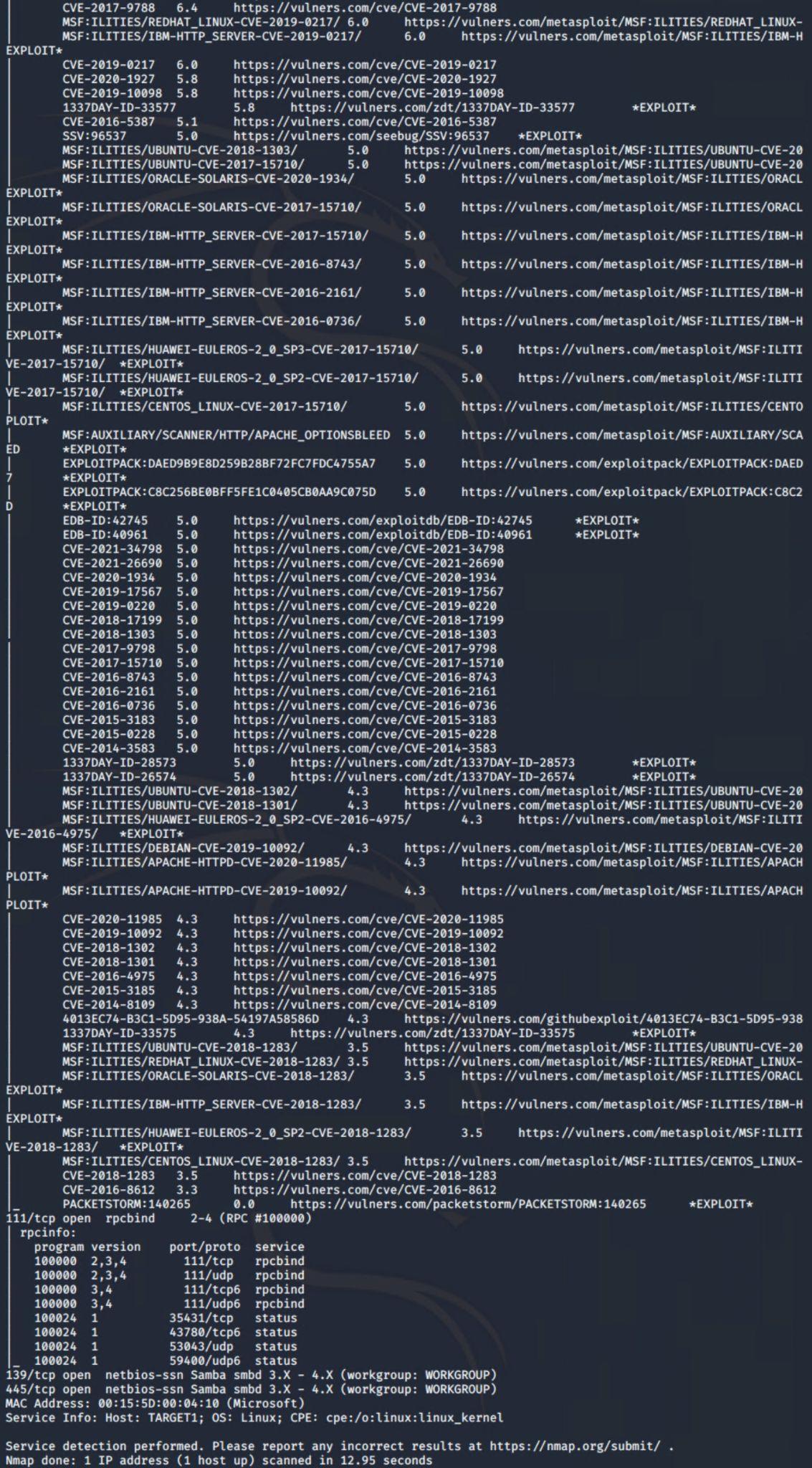
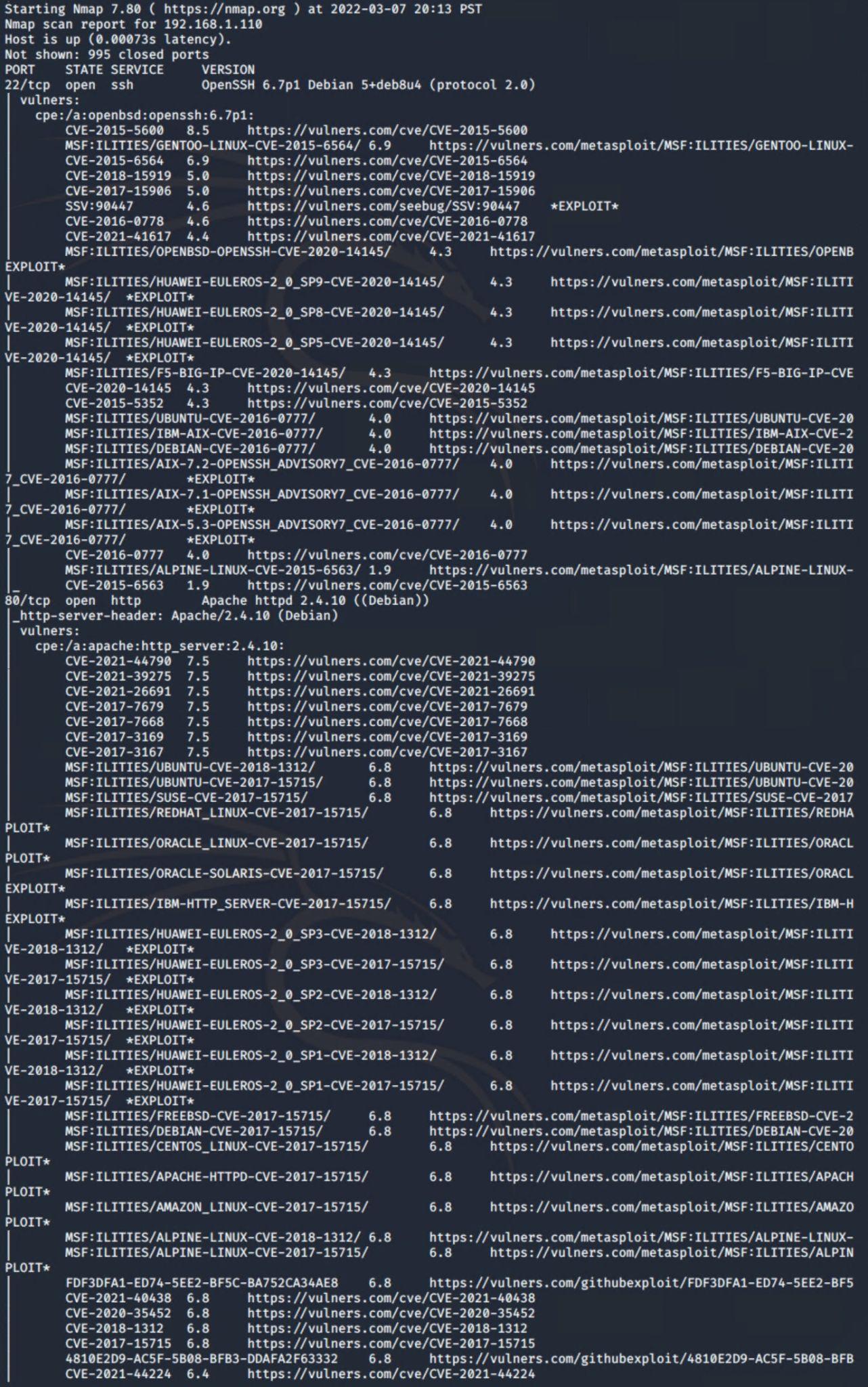
Target 1

### Port 22

| **CVE** | **SEVERITY** |
| --- | --- |
| [CVE-2015-5600](https://vulners.com/cve/CVE-2015-5600) | 8.5 / High |
| [CVE-2015-6564](https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2015-6564/) | 6.9 / Medium |
| [CVE-2018-15919](https://vulners.com/cve/CVE-2018-15919) | 5.0 / Medium |
| [CVE-2017-15906](https://vulners.com/cve/CVE-2017-15906) | 5.0 / Medium |
| [SSV:90447](https://vulners.com/seebug/SSV:90447)  ([CVE-2016-0777](https://vulners.com/cve/CVE-2016-0777)) | 4.6 / Medium |
| [CVE-2016-0778](https://vulners.com/cve/CVE-2016-0778) | 4.6 / Medium |
| [CVE-2021-41617](https://vulners.com/cve/CVE-2021-41617) | 4.4 / Medium |
| [CVE-2020-14145](https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/)  (OpenSSH Vulnerability) | 4.3 / Medium |
| [CVE-2020-14145](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/) (Huawei EulerOS/SP9) | 4.3 / Medium |
| [CVE-2020-14145](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/)  (Huawei EulerOS/SP8) | 4.3 / Medium |
| [CVE-2020-14145](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/)  (Huawei EulerOS/SP5) | 4.3 / Medium |
| [CVE-2020-14145](https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/) (F5 Networks/F5 Big IP) | 4.3 / Medium |
| [CVE-2020-14145](https://vulners.com/cve/CVE-2020-14145) | 4.3 / Medium |
| [CVE-2015-5352](https://vulners.com/cve/CVE-2015-5352) | 4.3 / Medium |
| [CVE-2016-0777](https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2016-0777/)  (Ubuntu/USN-2869-1) | 4.0 / Medium |
| [CVE-2016-0777](https://vulners.com/metasploit/MSF:ILITIES/IBM-AIX-CVE-2016-0777/)  (IBM AIX) | 4.0 / Medium |
| [CVE-2016-0777](https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-CVE-2016-0777/)  (Debian) | 4.0 / Medium |
| [CVE-2016-0777](https://vulners.com/metasploit/MSF:ILITIES/AIX-7.2-OPENSSH_ADVISORY7_CVE-2016-0777/)  (AIX 7.2) | 4.0 / Medium |
| [CVE-2016-0777](https://vulners.com/metasploit/MSF:ILITIES/AIX-7.1-OPENSSH_ADVISORY7_CVE-2016-0777/)  (AIX 7.1) | 4.0 / Medium |
| [CVE-2016-0777](https://vulners.com/metasploit/MSF:ILITIES/AIX-5.3-OPENSSH_ADVISORY7_CVE-2016-0777/)  (AIX 5.3) | 4.0 / Medium |
| [CVE-2016-0777](https://vulners.com/cve/CVE-2016-0777) | 4.0 / Medium |
| [CVE-2015-6563](https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-CVE-2015-6563/) (Alpine Linux) | 1.9 / Low |
| [CVE-2015-6563](https://vulners.com/cve/CVE-2015-6563) | 1.9 / Low |

PORT 80

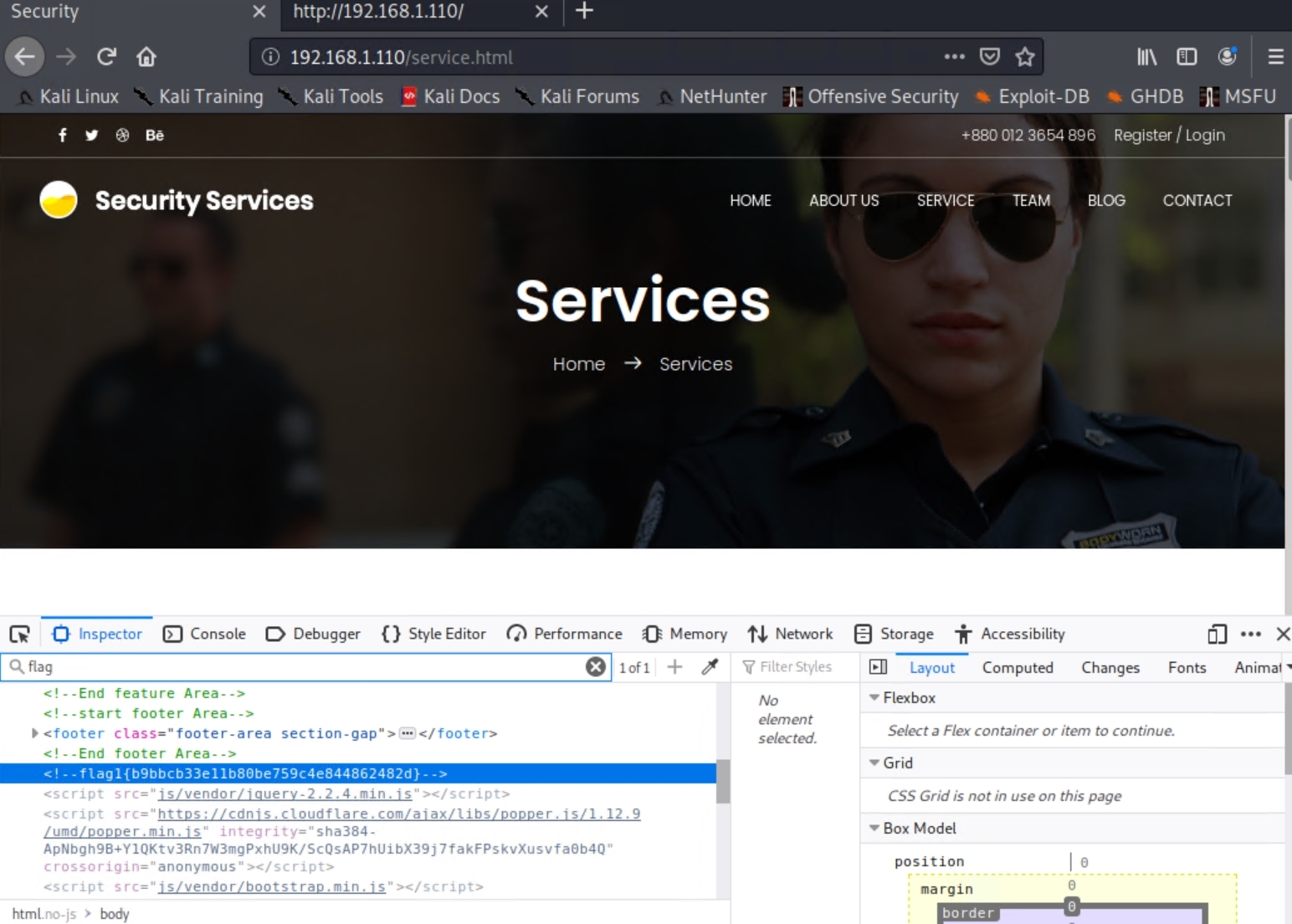
| **CVE** | **SEVERITY** |
| --- | --- |
| [CVE-2021-44790](https://vulners.com/cve/CVE-2021-44790) | 7.5 / High |
| [CVE-2021-39275](https://vulners.com/cve/CVE-2021-39275) | 7.5 / High |
| [CVE-2021-26691](https://vulners.com/cve/CVE-2021-26691) | 7.5 / High |
| [CVE-2017-7679](https://vulners.com/cve/CVE-2017-7679) | 7.5 / High |
| [CVE-2017-7668](https://vulners.com/cve/CVE-2017-7668) | 7.5 / High |
| [CVE-2017-3169](https://vulners.com/cve/CVE-2017-3169) | 7.5 / High |
| [CVE-2017-3167](https://vulners.com/cve/CVE-2017-3167) | 7.5 / High |
| [CVE-2018-1312](https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1312/) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2017-15715/) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2017-15715/) (SUSE) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2017-15715/)  (Red Hat) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/ORACLE_LINUX-CVE-2017-15715/)  (Oracle Linux) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2017-15715/)  (Oracle Solaris 11) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2017-15715/)  (IBM HTTP Server) | 6.8 / Medium |
| [CVE-2018-1312](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2018-1312/) (Huawei EulerOS/SP3) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2017-15715/) (Huawei EulerOS/SP3) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2017-15715/)  (Huawei EulerOS/SP2) | 6.8 / Medium |
| [CVE-2018-1312](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2018-1312/)  (Huawei EulerOS/SP2) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP1-CVE-2017-15715/)  (Huawei EulerOS/SP1) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP1-CVE-2017-15715/) (Huawei EulerOS/SP1) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/FREEBSD-CVE-2017-15715/)  (FreeBSD) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-CVE-2017-15715/)  (Debian) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-CVE-2017-15715/)  (Centos Linux) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-CVE-2017-15715/)  (Apache HTTPD) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/AMAZON_LINUX-CVE-2017-15715/)  (Amazon Linux AMI) | 6.8 / Medium |
| [CVE-2018-1312](https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-CVE-2018-1312/)  (Alpine Linux) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-CVE-2017-15715/)  (Alpine Linux) | 6.8 / Medium |
| [CVE-2021-40438](https://vulners.com/cve/CVE-2021-40438) | 6.8 / Medium |
| [CVE-2020-35452](https://vulners.com/cve/CVE-2020-35452) | 6.8 / Medium |
| [CVE-2018-1312](https://vulners.com/cve/CVE-2018-1312) | 6.8 / Medium |
| [CVE-2017-15715](https://vulners.com/cve/CVE-2017-15715) | 6.8 / Medium |
| [Server-Side Request Forgery Exploit](https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332) (CVE-2021-40438) | 6.8 / Medium |
| [CVE-2021-44224](https://vulners.com/cve/CVE-2021-44224) | 6.4 / Medium |
| [CVE-2017-9788](https://vulners.com/cve/CVE-2017-9788) | 6.4 / Medium |
| [CVE-2019-0217](https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2019-0217/)  (Red Hat) | 6.0 / Medium |
| [CVE-2019-0217](https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0217/) (IBM HTTP Server) | 6.0 / Medium |
| [CVE-2019-0217](https://vulners.com/cve/CVE-2019-0217) | 6.0 / Medium |
| [CVE-2020-1927](https://vulners.com/cve/CVE-2020-1927) | 5.8 / Medium |
| [CVE-2019-10098](https://vulners.com/cve/CVE-2019-10098) | 5.8 / Medium |
| [1337DAY-ID-33577](https://vulners.com/zdt/1337DAY-ID-33577) | 5.8 / Medium |
| [CVE-2016-5387](https://vulners.com/cve/CVE-2016-5387) | 5.1 / Medium |
| [SSV:96537](https://vulners.com/seebug/SSV:96537)  ([CVE-2017-9798](https://nvd.nist.gov/vuln/detail/CVE-2017-9798)) | 5.0 / Medium |
| [CVE-2018-1303](https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1303/) | 5.0 / Medium |
| [CVE-2017-15710](https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2017-15710/) | 5.0 / Medium |
| [CVE-2020-1934](https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2020-1934/) | 5.0 / Medium |
| [CVE-2017-15710](https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2017-15710/) (Oracle Solaris) | 5.0 / Medium |
| [CVE-2017-15710](https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2017-15710/)  (IBM HTTP Server) | 5.0 / Medium |
| [CVE-2016-8743](https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2016-8743/) | 5.0 / Medium |
| [CVE-2016-2161](https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2016-2161/) | 5.0 / Medium |
| [CVE-2016-0736](https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2016-0736/) | 5.0 / Medium |
| [CVE-2017-15710](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2017-15710/)  (Huawei EulerOS/SP3) | 5.0 / Medium |
| [CVE-2017-15710](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2017-15710/)  (Huawei EulerOS/SP2) | 5.0 / Medium |
| [CVE-2017-15710](https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-CVE-2017-15710/)  (Centos Linux) | 5.0 / Medium |
| [Apache Optionsbleed Scanner](https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/HTTP/APACHE_OPTIONSBLEED) | 5.0 / Medium |
| [Apache mod\_session\_crypto](https://vulners.com/exploitpack/EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7) | 5.0 / Medium |
| [Apache 2.2.34 2.4.27](https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D) | 5.0 / Medium |
| [EDB-ID:42745](https://vulners.com/exploitdb/EDB-ID:42745) | 5.0 / Medium |
| [EDB-ID:40961](https://vulners.com/exploitdb/EDB-ID:40961) | 5.0 / Medium |
| [CVE-2021-34798](https://vulners.com/cve/CVE-2021-34798) | 5.0 / Medium |
| [CVE-2021-26690](https://vulners.com/cve/CVE-2021-26690) | 5.0 / Medium |
| [CVE-2020-1934](https://vulners.com/cve/CVE-2020-1934) | 5.0 / Medium |
| [CVE-2019-17567](https://vulners.com/cve/CVE-2019-17567) | 5.0 / Medium |
| [CVE-2019-0220](https://vulners.com/cve/CVE-2019-0220) | 5.0 / Medium |
| [CVE-2018-17199](https://vulners.com/cve/CVE-2018-17199) | 5.0 / Medium |
| [CVE-2018-1303](https://vulners.com/cve/CVE-2018-1303) | 5.0 / Medium |
| [CVE-2017-9798](https://vulners.com/cve/CVE-2017-9798) | 5.0 / Medium |
| [CVE-2017-15710](https://vulners.com/cve/CVE-2017-15710) | 5.0 / Medium |
| [CVE-2016-8743](https://vulners.com/cve/CVE-2016-8743) | 5.0 / Medium |
| [CVE-2016-2161](https://vulners.com/cve/CVE-2016-2161) | 5.0 / Medium |
| [CVE-2016-0736](https://vulners.com/cve/CVE-2016-0736) | 5.0 / Medium |
| [CVE-2015-3183](https://vulners.com/cve/CVE-2015-3183) | 5.0 / Medium |
| [CVE-2015-0228](https://vulners.com/cve/CVE-2015-0228) | 5.0 / Medium |
| [CVE-2014-3583](https://vulners.com/cve/CVE-2014-3583) | 5.0 / Medium |
| [1337DAY-ID-28573](https://vulners.com/zdt/1337DAY-ID-28573) | 5.0 / Medium |
| [1337DAY-ID-26574](https://vulners.com/zdt/1337DAY-ID-26574) | 5.0 / Medium |
| [CVE-2018-1302](https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1302/) | 4.3 / Medium |
| [CVE-2018-1301](https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1301/) | 4.3 / Medium |
| [CVE-2016-4975](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2016-4975/) | 4.3 / Medium |
| [CVE-2019-10092](https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-CVE-2019-10092/) | 4.3 / Medium |
| [CVE-2020-11985](https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-CVE-2020-11985/) | 4.3 / Medium |
| [CVE-2019-10092](https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-CVE-2019-10092/) | 4.3 / Medium |
| [CVE-2020-11985](https://vulners.com/cve/CVE-2020-11985) | 4.3 / Medium |
| [CVE-2019-10092](https://vulners.com/cve/CVE-2019-10092) | 4.3 / Medium |
| [CVE-2018-1302](https://vulners.com/cve/CVE-2018-1302) | 4.3 / Medium |
| [CVE-2018-1301](https://vulners.com/cve/CVE-2018-1301) | 4.3 / Medium |
| [CVE-2016-4975](https://vulners.com/cve/CVE-2016-4975) | 4.3 / Medium |
| [CVE-2015-3185](https://vulners.com/cve/CVE-2015-3185) | 4.3 / Medium |
| [CVE-2014-8109](https://vulners.com/cve/CVE-2014-8109) | 4.3 / Medium |
| [Exploit for Cross-site Scripting](https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D) | 4.3 / Medium |
| [1337DAY-ID-33575](https://vulners.com/zdt/1337DAY-ID-33575) | 4.3 / Medium |
| [CVE-2018-1283](https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1283/) (Ubuntu) | 3.5 / Low |
| [CVE-2018-1283](https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2018-1283/)  (Redhat Linux) | 3.5 / Low |
| [CVE-2018-1283](https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2018-1283/)  (Oracle Solaris) | 3.5 / Low |
| [CVE-2018-1283](http://cve-2018-1283)  (IBM HTTP Server) | 3.5 / Low |
| [CVE-2018-1283](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2018-1283/)  (Huawei EulerOS/SP2) | 3.5 / Low |
| [CVE-2018-1283](https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-CVE-2018-1283/)  (Centos Linux) | 3.5 / Low |
| [CVE-2018-1283](https://vulners.com/cve/CVE-2018-1283) | 3.5 / Low |
| [CVE-2016-8612](https://vulners.com/cve/CVE-2016-8612) | 3.3 / Low |
| [Apache mod\_session\_crypt 2.5](https://vulners.com/packetstorm/PACKETSTORM:140265) | 0.0 / None |



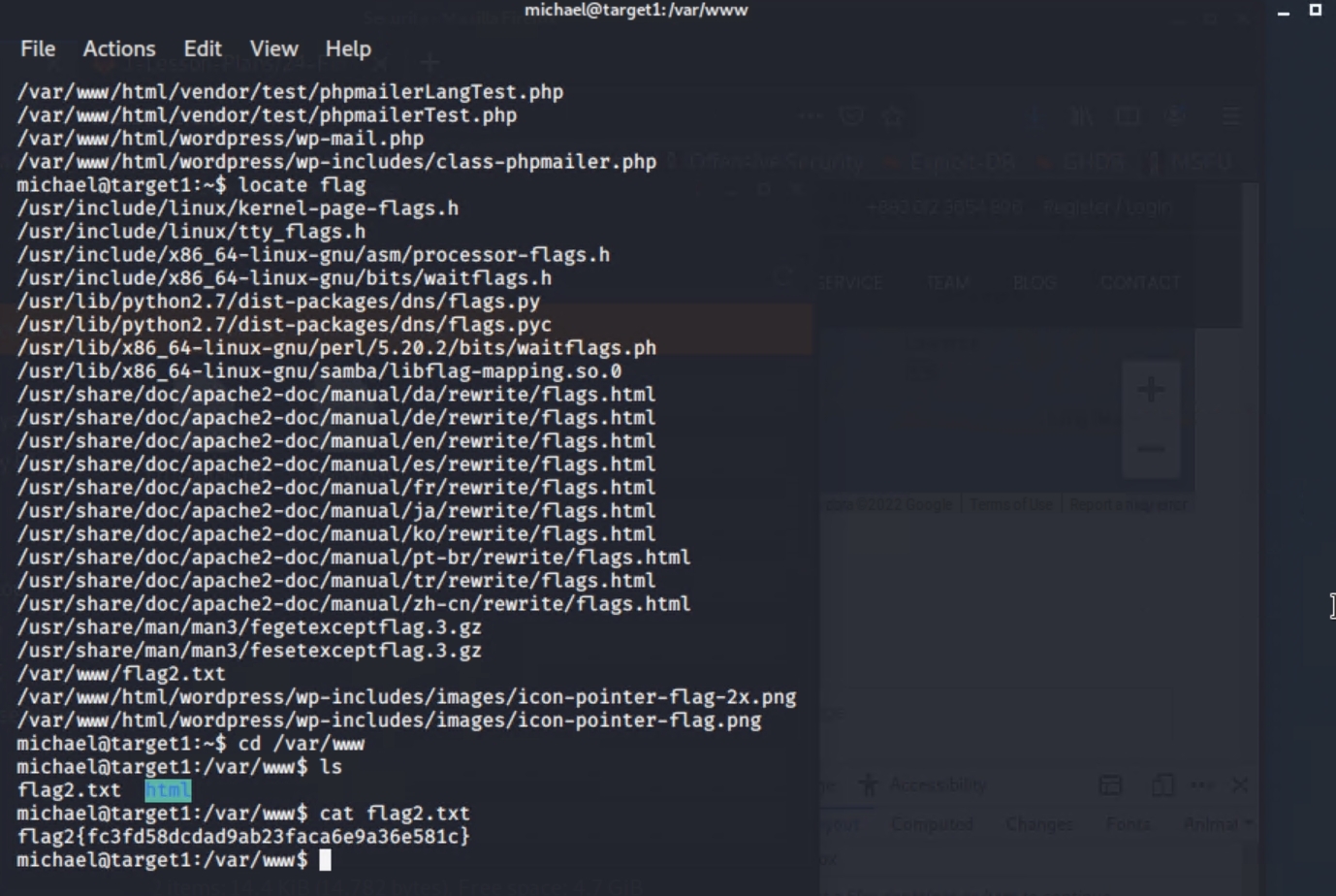
### **Exploitation**

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

* Target 1
  + **flag1.txt: *b9bbcb33e11b80be759c4e844862482d***
    - **Exploit Used**
      * Enumerated the vulnerable WordPress website using the built in developer tools of ‘Inspect Element’ or viewing the ‘Page Source’
      * Right-Clicked to ‘Inspect’ or ‘View Page source’ specifically off the service.html and searched for the flag using ‘flag’.

**

* + **flag2.txt: *fc3fd58dcdad9ab23faca6e9a36e581c***
    - **Exploit Used**
      * Weak SSH passwords and Weak credentials were exploited in order to access the user Michael.
      * ***ssh michael@192.168.1.110 -p 22*** *-* to connect to the host
      * ***locate flag***- locating in the hosts files the keyword ‘flag’
      * ***cd /var/www*** *-* redirecting current directory to the path */var/www*
      * ***cat flag2.txt*** - after listing with *ls* the location of the file, we use cat to read it out and are retracting the information needed



* + **flag3.txt: *afc01ab56b50591e7dccf93122770***
  + **flag4.txt: *715dea6c055b9fe3337544933f294***
    - **Exploit Used**
      * Plain text Database Password Access was exploited to access the database information through MySQL from the user that was infiltrated.
      * Upon deeper inspection through the fields in their designated table from the database ‘wordpress’ we are able to find flag 3 and flag 4 in the ‘wp\_posts’ table.

