2024

Week 5

MICHELLE PANTELOURIS

Task 1

Port 21

```
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 2325 guesses in 180 seconds, average tps: 12.1

Nmap scan report for 10.150.150.12
Host is up (0.20s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 214 guesses in 180 seconds, average tps: 1.1
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root) groups=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      https://www.securityfocus.com/bid/48539
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.66.66.230
```

```
root@kali: /home/kali/Desktop
File  Actions  Edit  View  Help
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root) groups=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/ex
ploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-
backdoored.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
```

IPA: 10.150.150.12

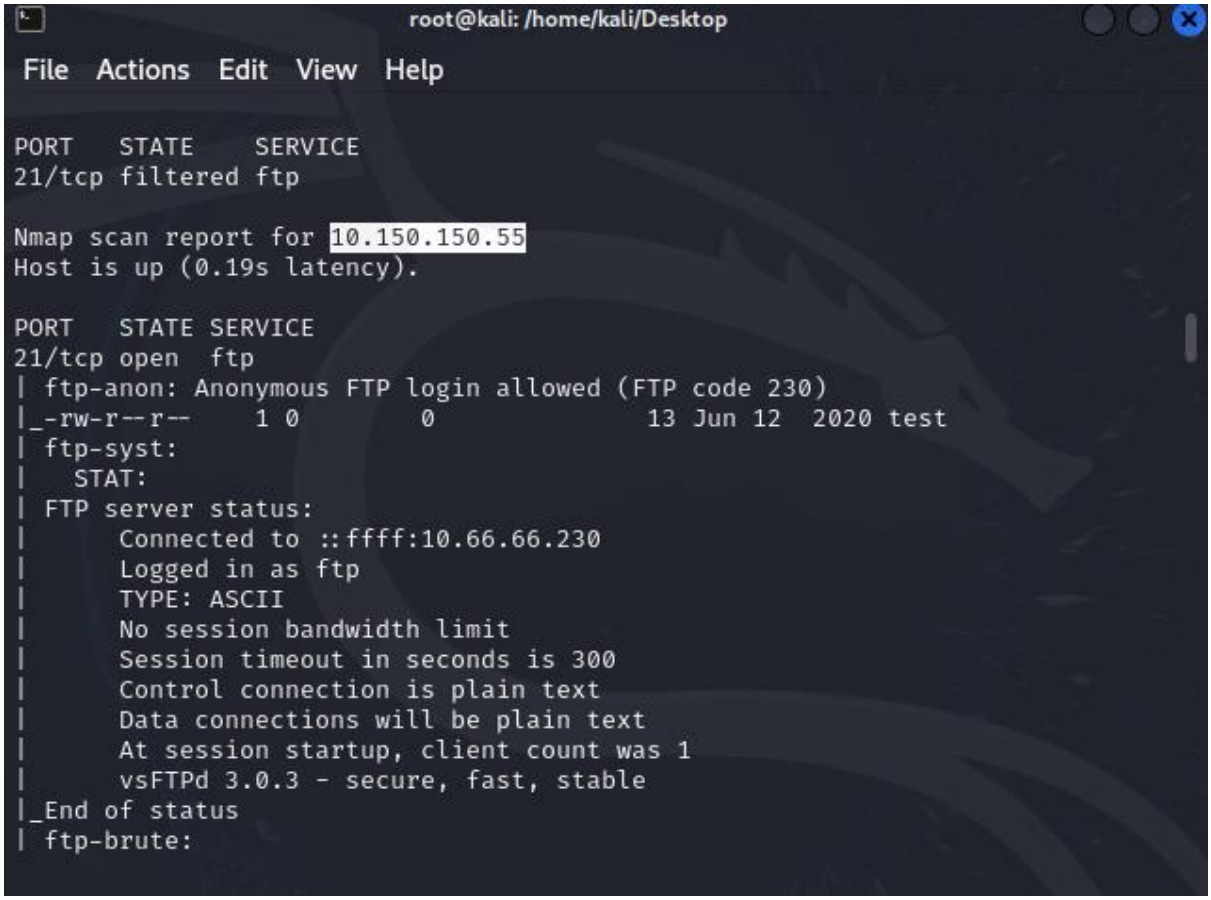
Open Ports - 21

Services - ftp

Services Version – vsFTPd 2.3.4

Detected Vulnerabilities – Anonymous FTP logins allowed, A backdoor which opens a shell on port 6200/tcp.

CVE/CWE – 2001-2523



IPA: 10.150.150.55

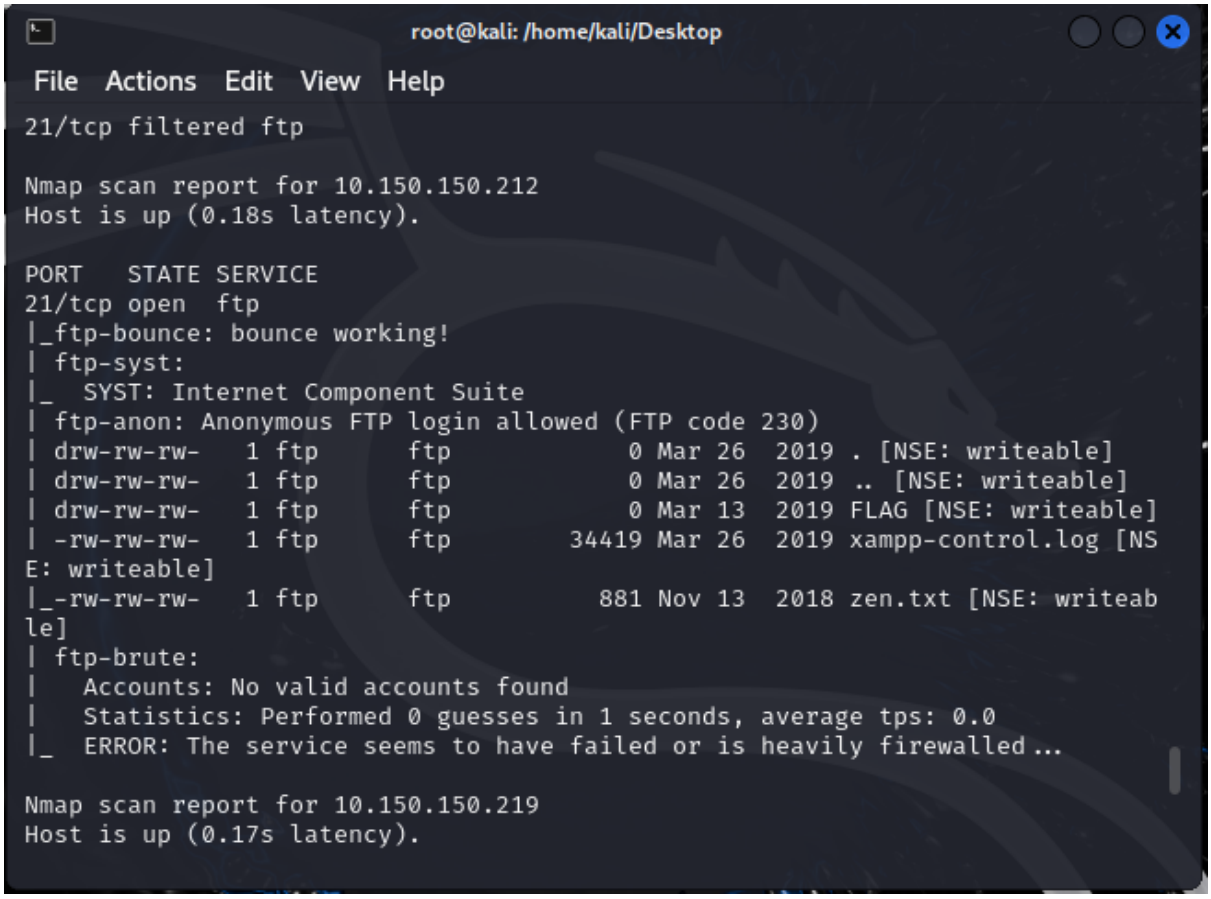
Open Ports - 21

Services - ftp

Services Version – vsFTPd 3.0.3

Detected Vulnerabilities – Anonymous FTP logins allowed

CVE/CWE – N/A



IPA: 10.150.150.212

Open Ports - 21

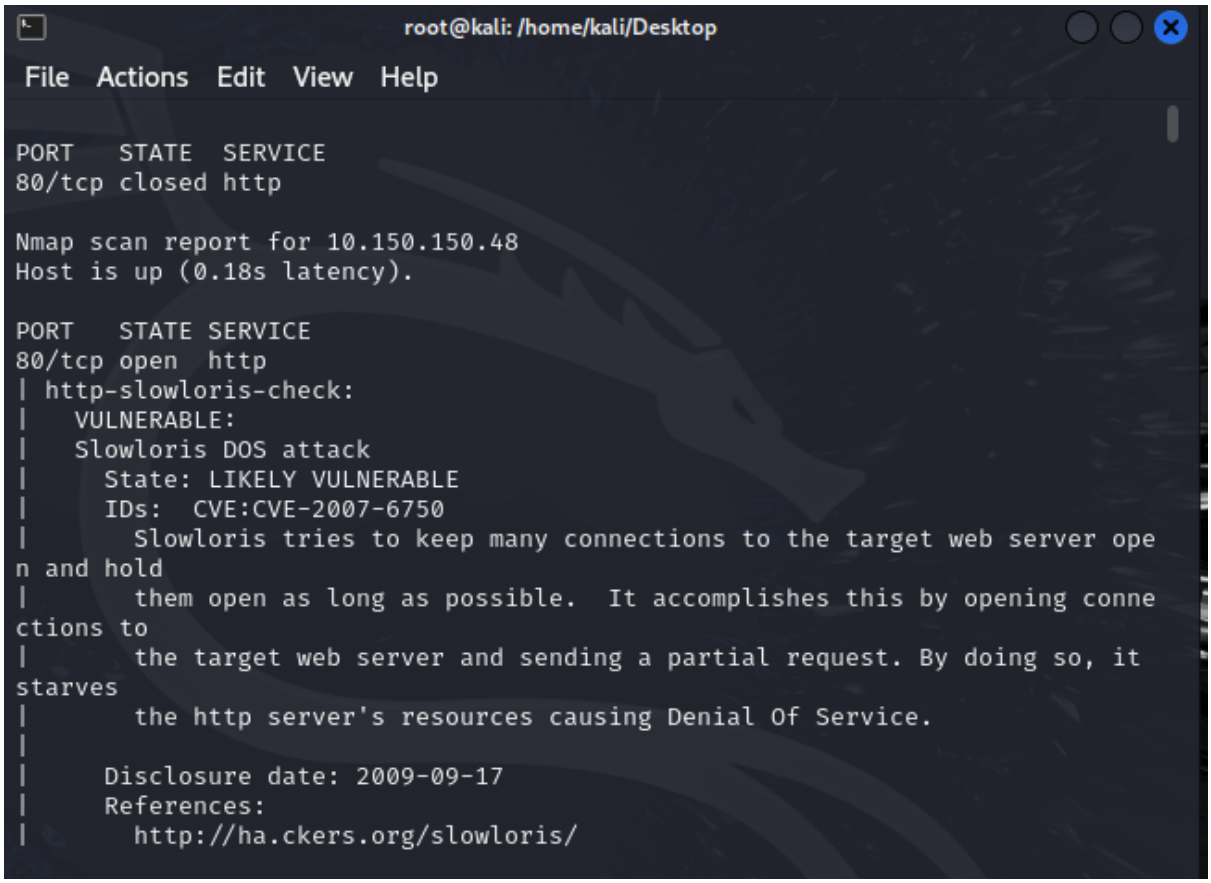
Services - ftp

Services Version – N/A

Detected Vulnerabilities – Anonymous FTP logins allowed

CVE/CWE – N/A

Port 80



IPA: 10.150.150.48, 10.150.150.57, 10.150.150.80, 10.150.150.123, 10.150.150.138, 10.150.150.212

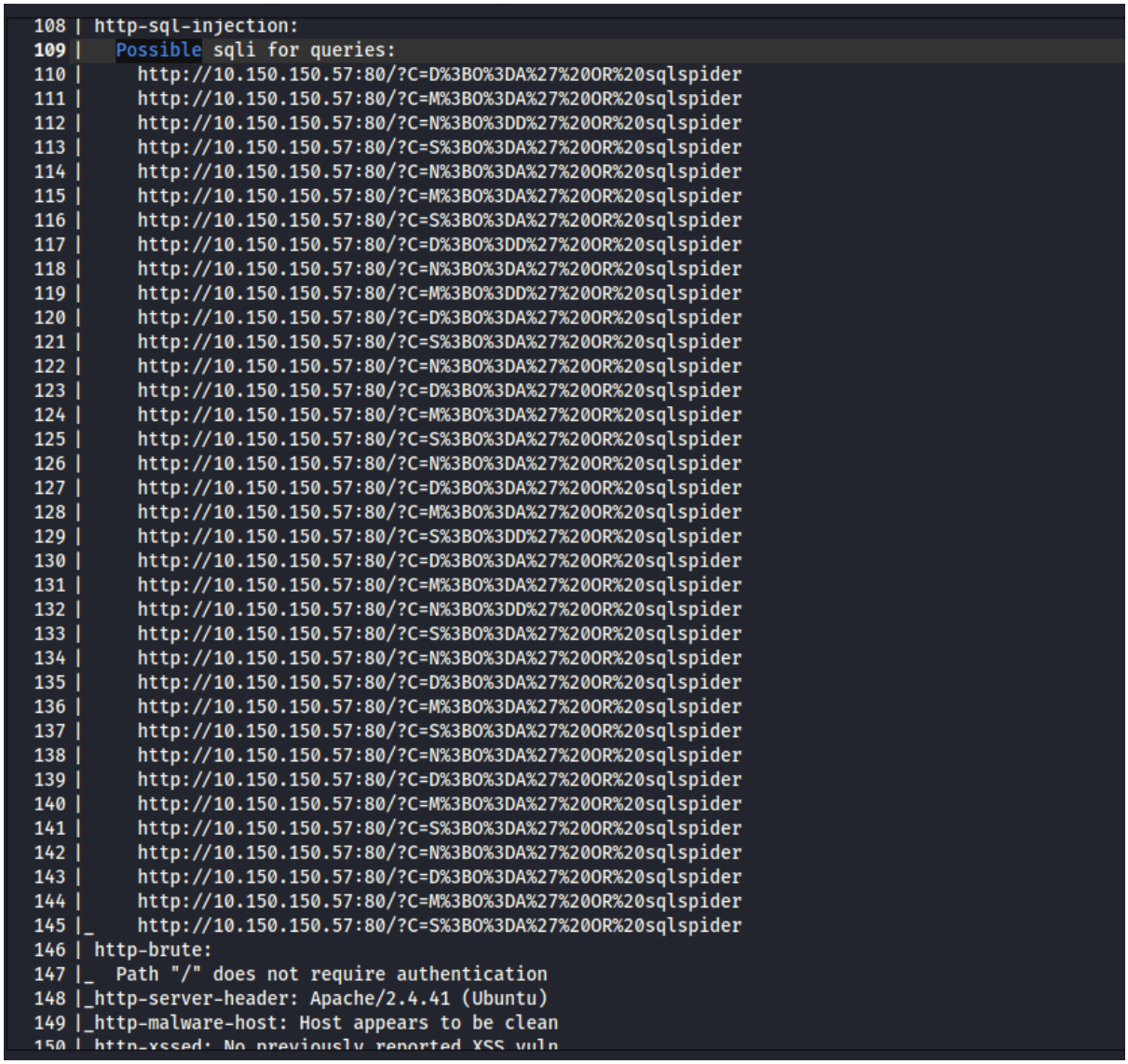
Open Ports - 80

Services - http

Services Version – Apache/2.4.41 (Unix) OpenSSL/1.1.0l

Detected Vulnerabilities – Slowloris DOS attack

CVE/CWE –2007-6750



```
| http-sql-injection:
|   Possible sqli for queries:
|     http://10.150.150.57:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=D%3BO%3DD%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=M%3BO%3DD%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=S%3BO%3DD%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|_    http://10.150.150.57:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http-brute:
|_  Path "/" does not require authentication
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-malware-host: Host appears to be clean
| http-xssed: No previously reported XSS vuln
```

IPA: 10.150.150.57

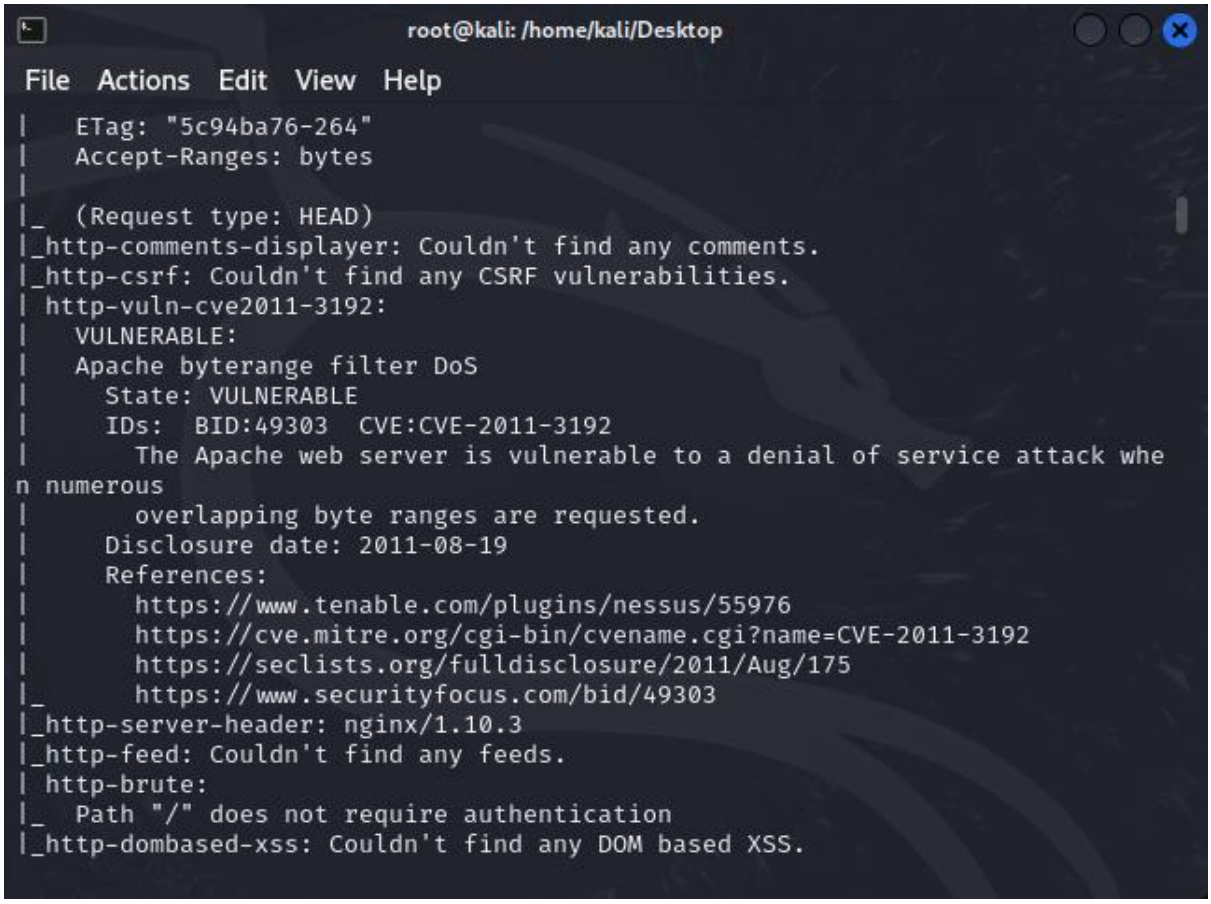
Open Ports - 80

Services - http

Services Version – Apache/2.4.41

Detected Vulnerabilities – SQLi

CVE/CWE –2011-3192



IPA: 10.150.150.145

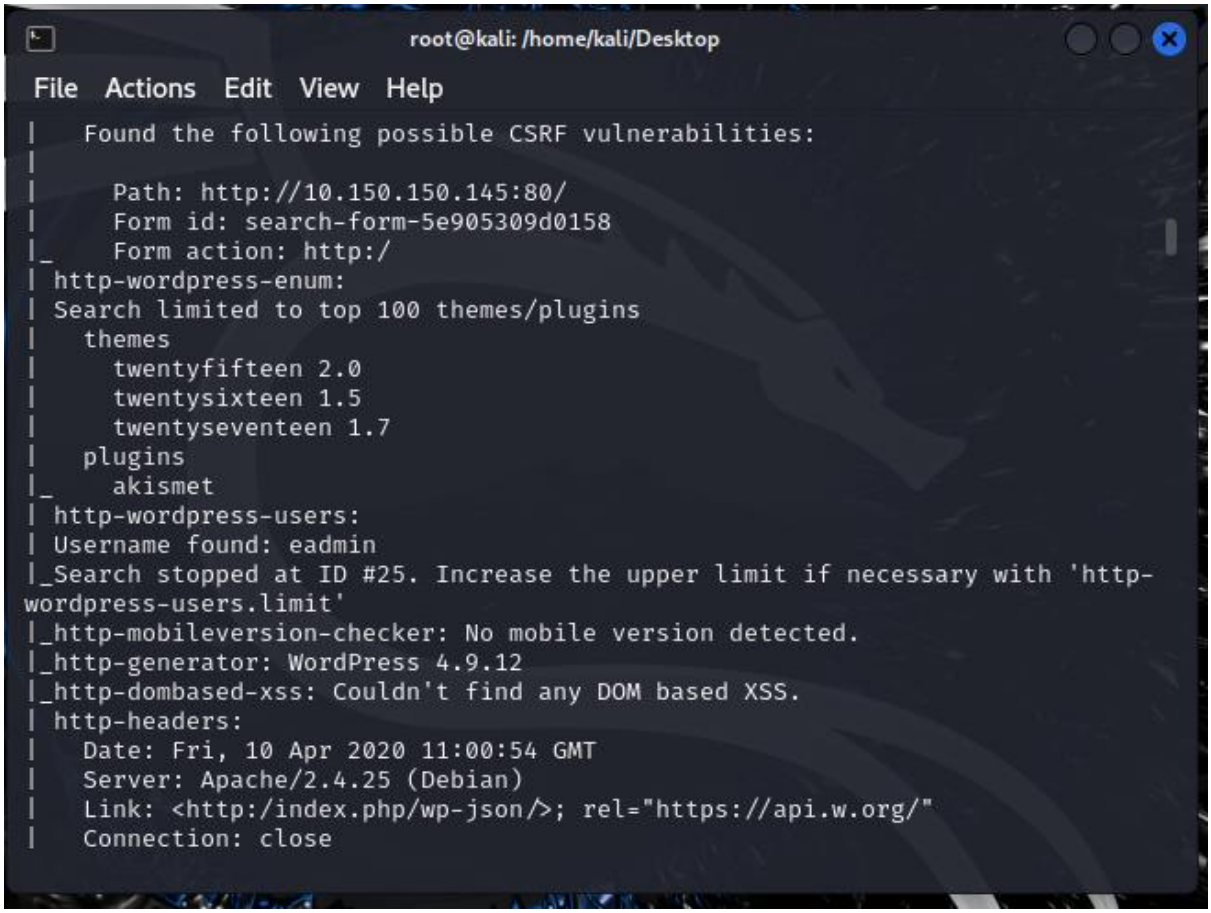
Open Ports - 80

Services - http

Services Version – Apache/2.4.41 (Unix) OpenSSL/1.1.0l

Detected Vulnerabilities – Apache web server is vulnerable to a dos attack.

CVE/CWE –2011-3192



IPA: 10.150.150.145

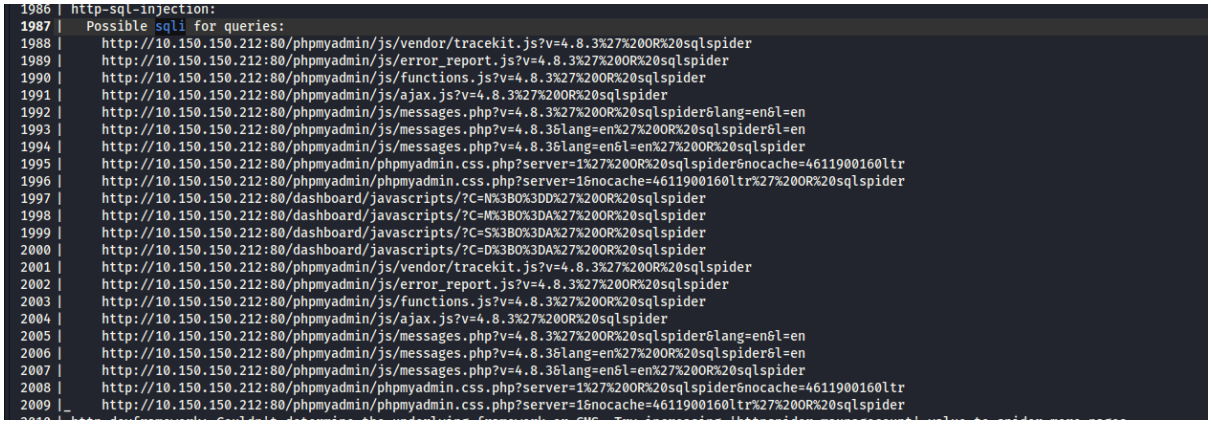
Open Ports - 80

Services - http

Services Version – Apache/2.4.25

Detected Vulnerabilities – CRSF

CVE/CWE –N/A



IPA: 10.150.150.212

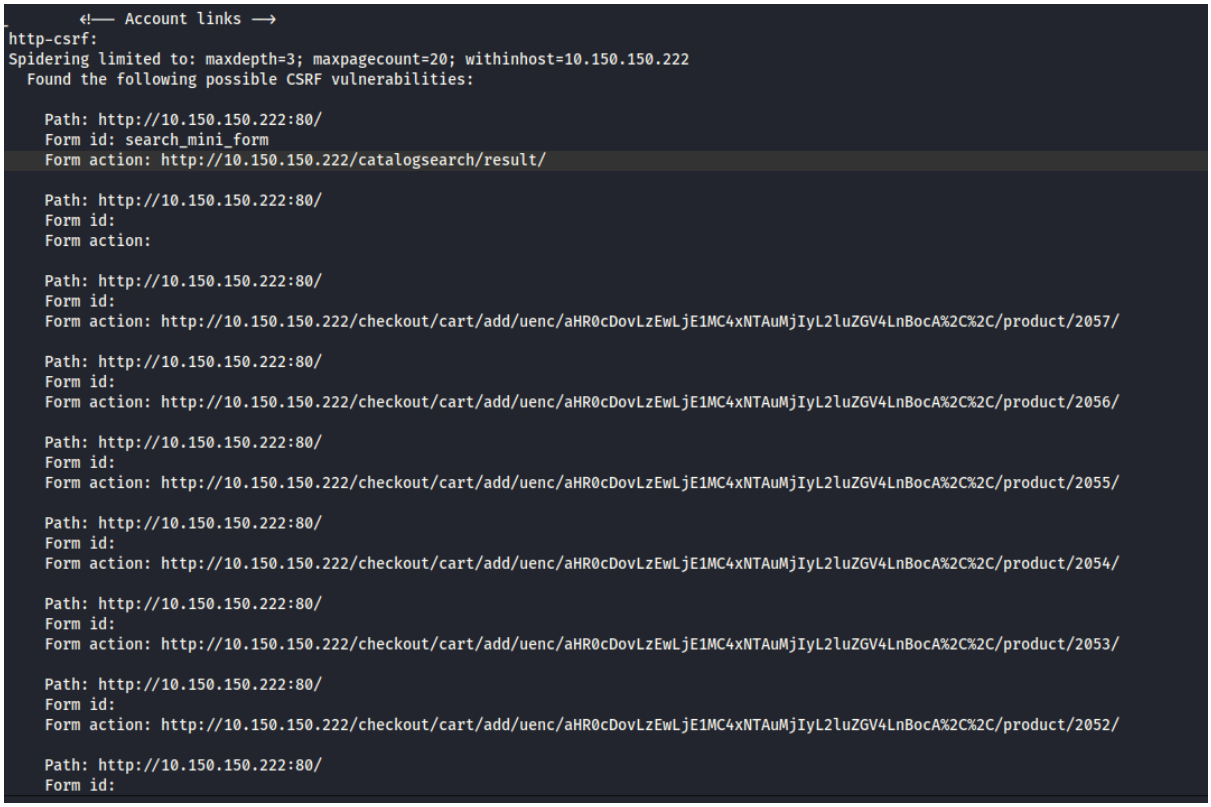
Open Ports - 80

Services - http

Services Version – Apache/2.4.25

Detected Vulnerabilities – SQLi

CVE/CWE –2011-3192



IPA: 10.150.150.222

Open Ports - 80

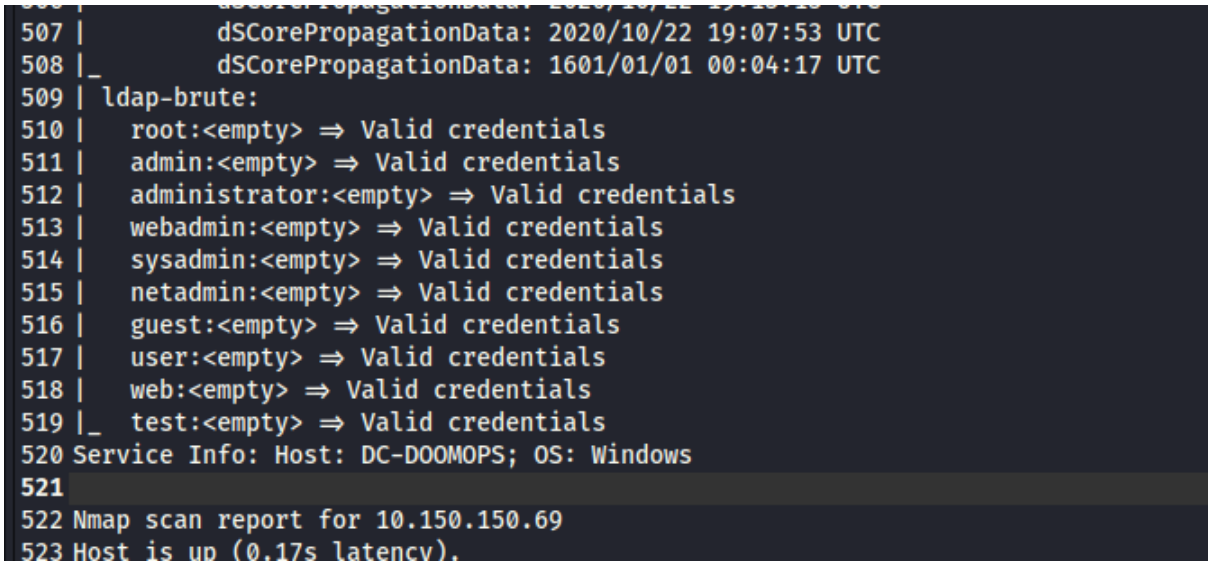
Services - http

Services Version – Apache/2.4.25

Detected Vulnerabilities – SQLi

CVE/CWE –2011-3192

Port 389



IPA: 10.150.150.66

Open Ports - 389

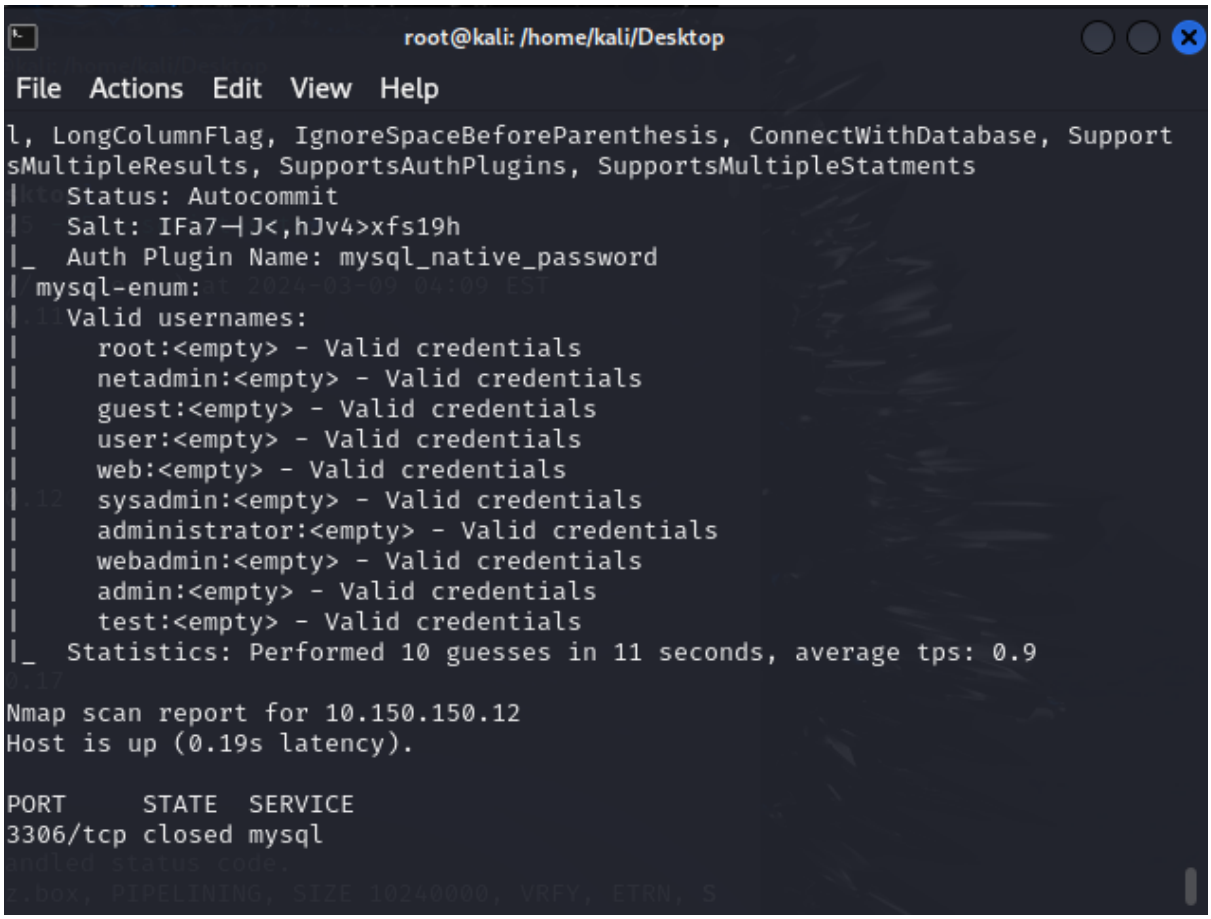
Services - ldap

Services Version – DC-DOOMOPS; OS: Windows

Detected Vulnerabilities – Shows valid credentials

CVE/CWE –N/A

Port 3306



IPA: 10.150.150.11

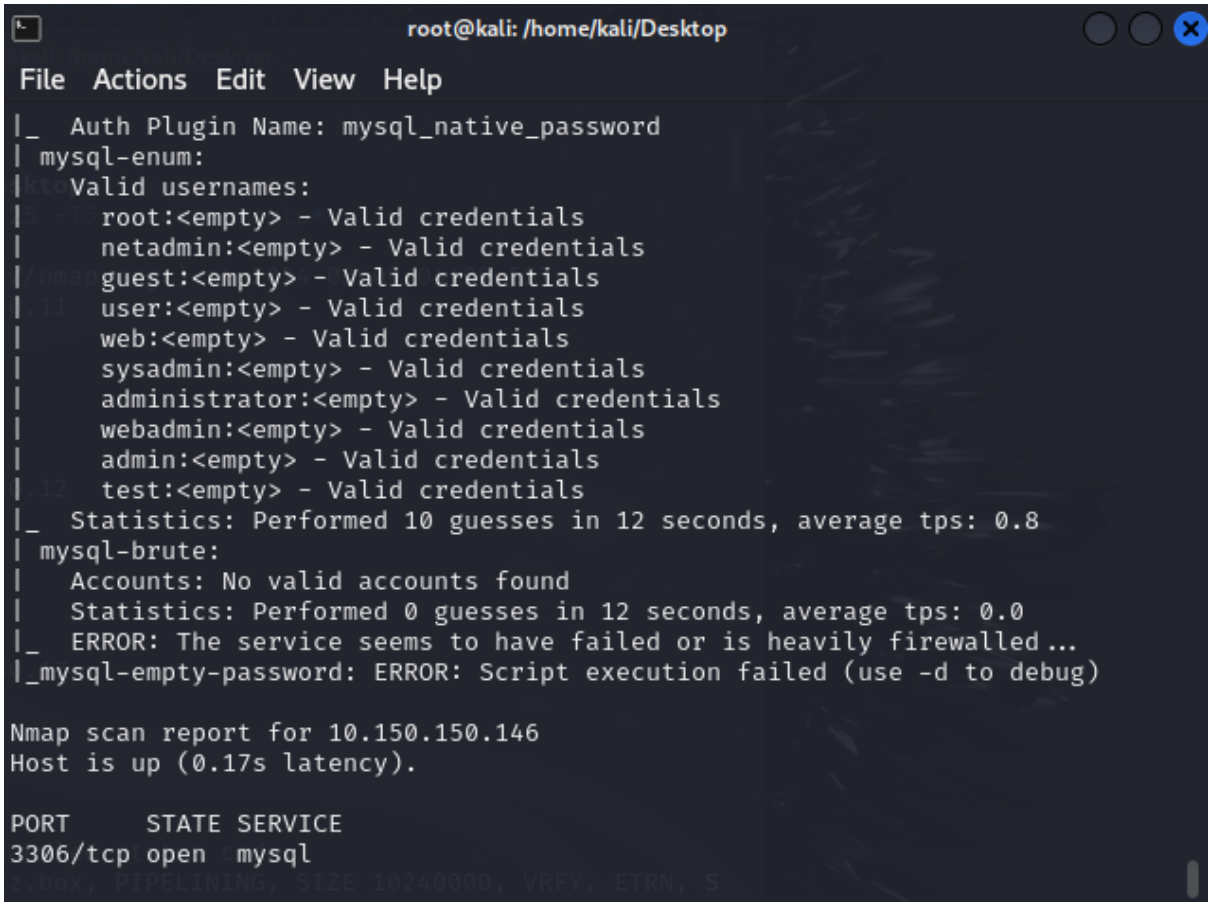
Open Ports - 3306

Services - MySQL

Services Version – 5.5.5-10.4.14-MariaDB

Detected Vulnerabilities – Shows valid credentials

CVE/CWE –N/A



IPA: 10.150.150.145

Open Ports - 3306

Services - MySQL

Services Version – 5.5.5-10.1.26-MariaDB-0+deb9u1

Detected Vulnerabilities – Shows valid credentials

CVE/CWE –N/A