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

PORT STATE SERVICE
21/tcp open ftp
| ftp-brute:
| Accounts: No valid accounts found
|_ Statistics: Performed 214 guesses in 180 seconds, average tps: 1.1
| 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-wstpd-backdoor:
| VULNERABLE:
| VSFTPd version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: CVE:CVE-2011-2523 BID:8859
| 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/rapid//metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb https://jstmy.securityfocus.com/bld/48539
| ftp-ssyte:
| STAT: | FTP server status: | Connected to 10.66.66.6320
```

```
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

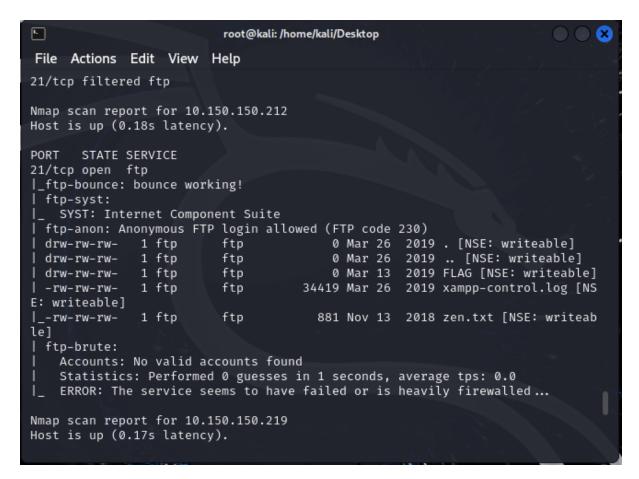


Open Ports - 21

Services - ftp

Services Version - vsFTPd 3.0.3

Detected Vulnerabilities – Anonymous FTP logins allowed



Open Ports - 21

Services - ftp

Services Version - N/A

Detected Vulnerabilities – Anonymous FTP logins allowed

Port 80

```
E
                          root@kali: /home/kali/Desktop
File Actions Edit View Help
PORT
      STATE SERVICE
80/tcp closed http
Nmap scan report for 10.150.150.48
Host is up (0.18s latency).
      STATE SERVICE
80/tcp open http
 http-slowloris-check:
    VULNERABLE:
    Slowloris DOS attack
      State: LIKELY VULNERABLE
      IDs: CVE:CVE-2007-6750
        Slowloris tries to keep many connections to the target web server ope
n and hold
        them open as long as possible. It accomplishes this by opening conne
ctions to
        the target web server and sending a partial request. By doing so, it
starves
        the http server's resources causing Denial Of Service.
      Disclosure date: 2009-09-17
      References:
        http://ha.ckers.org/slowloris/
```

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:
109
110
         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
111 |
112 |
         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
113
         http://10.150.150.57:80/?C=N%3BO%3DA%27%20OR%20sqlspider
114
115 |
         http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
116 |
         http://10.150.150.57:80/?C=S%3B0%3DA%27%200R%20sqlspider
117
         http://10.150.150.57:80/?C=D%3BO%3DD%27%20OR%20sqlspider
118
         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
119
120
         http://10.150.150.57:80/?C=D%3B0%3DA%27%200R%20sqlspider
121
         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
122
         http://10.150.150.57:80/?C=D%3BO%3DA%27%20OR%20sqlspider
123
         http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
124
125
         http://10.150.150.57:80/?C=S%3B0%3DA%27%20OR%20sqlspider
         http://10.150.150.57:80/?C=N%3BO%3DA%27%20OR%20sqlspider
126
127
         http://10.150.150.57:80/?C=D%3BO%3DA%27%20OR%20sqlspider
128
         http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
129
         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
130
131
         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
132
133
         http://10.150.150.57:80/?C=S%3BO%3DA%27%20OR%20sqlspider
134
         http://10.150.150.57:80/?C=N%3BO%3DA%27%20OR%20sqlspider
135
         http://10.150.150.57:80/?C=D%3BO%3DA%27%20OR%20sqlspider
136
         http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
137
         http://10.150.150.57:80/?C=S%3B0%3DA%27%200R%20sqlspider
138
         http://10.150.150.57:80/?C=N%3BO%3DA%27%20OR%20sqlspider
139
         http://10.150.150.57:80/?C=D%3B0%3DA%27%20OR%20sqlspider
         http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
140
141
         http://10.150.150.57:80/?C=S%3B0%3DA%27%20OR%20sqlspider
142
         http://10.150.150.57:80/?C=N%3BO%3DA%27%20OR%20sqlspider
143
         http://10.150.150.57:80/?C=D%3B0%3DA%27%20OR%20sqlspider
144
         http://10.150.150.57:80/?C=M%3BO%3DA%27%20OR%20sqlspider
145
         http://10.150.150.57:80/?C=S%3BO%3DA%27%20OR%20sqlspider
146 | http-brute:
       Path "/" does not require authentication
147 |
148 | http-server-header: Apache/2.4.41 (Ubuntu)
149 | http-malware-host: Host appears to be clean
150 | http_vssed. No previously reported XSS vuln
```

Open Ports - 80

Services - http

Services Version - Apache/2.4.41

Detected Vulnerabilities - SQLi

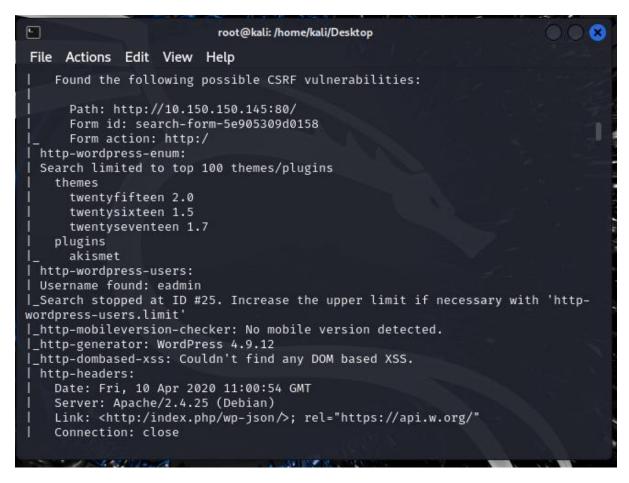
```
F
                            root@kali: /home/kali/Desktop
File Actions Edit View Help
    ETag: "5c94ba76-264"
    Accept-Ranges: bytes
   (Request type: HEAD)
 http-comments-displayer: Couldn't find any comments.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
 http-vuln-cve2011-3192:
    VULNERABLE:
    Apache byterange filter DoS
      State: VULNERABLE
      IDs: BID:49303 CVE:CVE-2011-3192
        The Apache web server is vulnerable to a denial of service attack whe
n numerous
        overlapping byte ranges are requested.
      Disclosure date: 2011-08-19
      References:
        https://www.tenable.com/plugins/nessus/55976
        https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
https://seclists.org/fulldisclosure/2011/Aug/175
        https://www.securityfocus.com/bid/49303
 http-server-header: nginx/1.10.3
 http-feed: Couldn't find any feeds.
 http-brute:
    Path "/" does not require authentication
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

Open Ports - 80

Services - http

Services Version – Apache/2.4.41 (Unix) OpenSSL/1.1.01

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



Open Ports - 80

Services - http

Services Version – Apache/2.4.25

Detected Vulnerabilities - CRSF

Open Ports - 80

Services - http

Services Version - Apache/2.4.25

Detected Vulnerabilities - SQLi

```
\leftarrow! — Account links \rightarrow
http-csrf:
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.150.150.222
Found the following possible CSRF vulnerabilities:
    Path: http://10.150.150.222:80/
    Form id: search_mini_form
Form action: http://10.150.150.222/catalogsearch/result/
    Path: http://10.150.150.222:80/
    Form id:
Form action:
    Path: http://10.150.150.222:80/
    Form action: http://10.150.150.222/checkout/cart/add/uenc/aHR0cDovLzEwLjE1MC4xNTAuMjIyL2luZGV4LnBocA%2C%2C/product/2057/
    Path: http://10.150.150.222:80/
    Form action: http://10.150.150.222/checkout/cart/add/uenc/aHR0cDovLzEwLjE1MC4xNTAuMjIyL2luZGV4LnBocA%2C%2C/product/2056/
    Path: http://10.150.150.222:80/
    Form action: http://10.150.150.222/checkout/cart/add/uenc/aHR0cDovLzEwLjE1MC4xNTAuMjIyL2luZGV4LnBocA%2C%2C/product/2055/
    Path: http://10.150.150.222:80/
    Form id: Form action: http://10.150.150.222/checkout/cart/add/uenc/aHR0cDovLzEwLjE1MC4xNTAuMjJyL2luZGV4LnBocA%2C%2C/product/2054/
    Path: http://10.150.150.222:80/
    Form id: Form action: http://10.150.150.222/checkout/cart/add/uenc/aHR0cDovLzEwLjE1MC4xNTAuMjIyL2luZGV4LnBocA%2C%2C/product/2053/
    Path: http://10.150.150.222:80/
    Form action: http://10.150.222/checkout/cart/add/uenc/aHR0cDovLzEwLjE1MC4xNTAuMjJyL2luZGV4LnBocA%2C%2C/product/2052/
    Path: http://10.150.150.222:80/
    Form id:
```

Open Ports - 80

Services - http

Services Version – Apache/2.4.25

Detected Vulnerabilities - SQLi

Port 389

```
507 I
              dSCorePropagationData: 2020/10/22 19:07:53 UTC
508 |_
              dSCorePropagationData: 1601/01/01 00:04:17 UTC
509 | ldap-brute:
        root:<empty> ⇒ Valid credentials
        admin:<empty> ⇒ Valid credentials
511 |
512 |
        administrator:<empty> ⇒ Valid credentials
        webadmin:<empty> ⇒ Valid credentials
513 |
514 |
        sysadmin:<empty> ⇒ Valid credentials
        netadmin:<empty> ⇒ Valid credentials
515 l
516 l
        guest:<empty> ⇒ Valid credentials
        user:<empty> ⇒ Valid credentials
517
518 l
        web:<empty> ⇒ Valid credentials
519 | test:<empty> ⇒ Valid credentials
520 Service Info: Host: DC-DOOMOPS; OS: Windows
521
522 Nmap scan report for 10.150.150.69
523 Host is up (0.17s latency).
```

IPA: 10.150.150.66

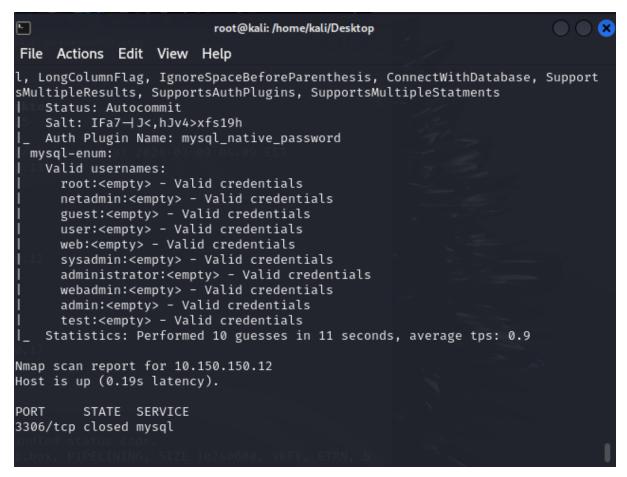
Open Ports - 389

Services - Idap

Services Version - DC-DOOMOPS; OS: Windows

Detected Vulnerabilities – Shows valid credentials

Port 3306



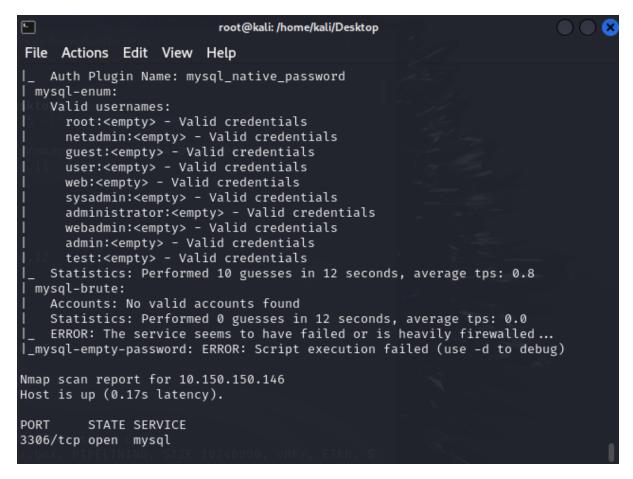
IPA: 10.150.150.11

Open Ports - 3306

Services - MySQL

Services Version – 5.5.5-10.4.14-MariaDB

Detected Vulnerabilities – Shows valid credentials



Open Ports - 3306

Services - MySQL

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

Detected Vulnerabilities – Shows valid credentials