

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/exploits/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

```
root@kali: /home/kali/Desktop
File Actions Edit View Help

PORT    STATE    SERVICE
21/tcp  filtered ftp

Nmap scan report for 10.150.150.55
Host is up (0.19s latency).

PORT    STATE    SERVICE
21/tcp  open     ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0      0      13 Jun 12  2020 test
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.66.66.230
|   Logged in as ftp
|   TYPE: ASCII
|   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 3.0.3 - secure, fast, stable
|_End of status
| ftp-brute:
```

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

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
21/tcp filtered ftp

Nmap scan report for 10.150.150.212
Host is up (0.18s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-bounce: bounce working!
|_ftp-syst:
|_SYST: Internet Component Suite
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drw-rw-rw- 1 ftp      ftp      0 Mar 26 2019 . [NSE: writeable]
|_drw-rw-rw- 1 ftp      ftp      0 Mar 26 2019 .. [NSE: writeable]
|_drw-rw-rw- 1 ftp      ftp      0 Mar 13 2019 FLAG [NSE: writeable]
|_rw-rw-rw- 1 ftp      ftp      34419 Mar 26 2019 xampp-control.log [NSE: writeable]
|_rw-rw-rw- 1 ftp      ftp      881 Nov 13 2018 zen.txt [NSE: writeable]
|_ftp-brute:
|_Accounts: No valid accounts found
|_Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
|_ERROR: The service seems to have failed or is heavily firewalled...

Nmap scan report for 10.150.150.219
Host is up (0.17s latency).
```

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

```
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).

PORT  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 open and hold
|   them open as long as possible. It accomplishes this by opening connections 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

```

108 | http-sql-injection:
109 |   Possible sql for queries:
110 |     http://10.150.150.57:80/?C=D%3B0%3DA%27%200R%20sqlspider
111 |     http://10.150.150.57:80/?C=M%3B0%3DA%27%200R%20sqlspider
112 |     http://10.150.150.57:80/?C=N%3B0%3DD%27%200R%20sqlspider
113 |     http://10.150.150.57:80/?C=S%3B0%3DA%27%200R%20sqlspider
114 |     http://10.150.150.57:80/?C=N%3B0%3DA%27%200R%20sqlspider
115 |     http://10.150.150.57:80/?C=M%3B0%3DA%27%200R%20sqlspider
116 |     http://10.150.150.57:80/?C=S%3B0%3DA%27%200R%20sqlspider
117 |     http://10.150.150.57:80/?C=D%3B0%3DD%27%200R%20sqlspider
118 |     http://10.150.150.57:80/?C=N%3B0%3DA%27%200R%20sqlspider
119 |     http://10.150.150.57:80/?C=M%3B0%3DD%27%200R%20sqlspider
120 |     http://10.150.150.57:80/?C=D%3B0%3DA%27%200R%20sqlspider
121 |     http://10.150.150.57:80/?C=S%3B0%3DA%27%200R%20sqlspider
122 |     http://10.150.150.57:80/?C=N%3B0%3DA%27%200R%20sqlspider
123 |     http://10.150.150.57:80/?C=D%3B0%3DA%27%200R%20sqlspider
124 |     http://10.150.150.57:80/?C=M%3B0%3DA%27%200R%20sqlspider
125 |     http://10.150.150.57:80/?C=S%3B0%3DA%27%200R%20sqlspider
126 |     http://10.150.150.57:80/?C=N%3B0%3DA%27%200R%20sqlspider
127 |     http://10.150.150.57:80/?C=D%3B0%3DA%27%200R%20sqlspider
128 |     http://10.150.150.57:80/?C=M%3B0%3DA%27%200R%20sqlspider
129 |     http://10.150.150.57:80/?C=S%3B0%3DD%27%200R%20sqlspider
130 |     http://10.150.150.57:80/?C=D%3B0%3DA%27%200R%20sqlspider
131 |     http://10.150.150.57:80/?C=M%3B0%3DA%27%200R%20sqlspider
132 |     http://10.150.150.57:80/?C=N%3B0%3DD%27%200R%20sqlspider
133 |     http://10.150.150.57:80/?C=S%3B0%3DA%27%200R%20sqlspider
134 |     http://10.150.150.57:80/?C=N%3B0%3DA%27%200R%20sqlspider
135 |     http://10.150.150.57:80/?C=D%3B0%3DA%27%200R%20sqlspider
136 |     http://10.150.150.57:80/?C=M%3B0%3DA%27%200R%20sqlspider
137 |     http://10.150.150.57:80/?C=S%3B0%3DA%27%200R%20sqlspider
138 |     http://10.150.150.57:80/?C=N%3B0%3DA%27%200R%20sqlspider
139 |     http://10.150.150.57:80/?C=D%3B0%3DA%27%200R%20sqlspider
140 |     http://10.150.150.57:80/?C=M%3B0%3DA%27%200R%20sqlspider
141 |     http://10.150.150.57:80/?C=S%3B0%3DA%27%200R%20sqlspider
142 |     http://10.150.150.57:80/?C=N%3B0%3DA%27%200R%20sqlspider
143 |     http://10.150.150.57:80/?C=D%3B0%3DA%27%200R%20sqlspider
144 |     http://10.150.150.57:80/?C=M%3B0%3DA%27%200R%20sqlspider
145 |     http://10.150.150.57:80/?C=S%3B0%3DA%27%200R%20sqlspider
146 | http-brute:
147 |   Path "/" does not require authentication
148 |_http-server-header: Apache/2.4.41 (Ubuntu)
149 |_http-malware-host: Host appears to be clean
150 | 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

```
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.
```

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


```
root@kali: /home/kali/Desktop
File Actions Edit View Help
| Found the following possible CSRF vulnerabilities:
|
| Path: http://10.150.150.145:80/
| Form id: search-form-5e905309d0158
| Form action: http:/
|_ http-wordpress-enum:
| Search limited to top 100 themes/plugins
| themes
| twentyfifteen 2.0
| twentysixteen 1.5
| twentyseventeen 1.7
| plugins
| akismet
|_ http-wordpress-users:
| Username found: eadmin
|_ Search stopped at ID #25. Increase the upper limit if necessary with 'http-
wordpress-users.limit'
|_ http-mobileversion-checker: No mobile version detected.
|_ http-generator: WordPress 4.9.12
|_ http-dombased-xss: Couldn't find any DOM based XSS.
| http-headers:
| Date: Fri, 10 Apr 2020 11:00:54 GMT
| Server: Apache/2.4.25 (Debian)
| Link: <http://index.php/wp-json/>; rel="https://api.w.org/"
| Connection: close
```

IPA: 10.150.150.145

Open Ports - 80

Services - http

Services Version – Apache/2.4.25

Detected Vulnerabilities – CSRF

CVE/CWE –N/A


```

1986 | http-sql-injection:
1987 | Possible sql for queries:
1988 | http://10.150.150.212:80/phpmyadmin/js/vendor/tracekit.js?v=4.8.3%27%200R%20sqlspider
1989 | http://10.150.150.212:80/phpmyadmin/js/error_report.js?v=4.8.3%27%200R%20sqlspider
1990 | http://10.150.150.212:80/phpmyadmin/js/functions.js?v=4.8.3%27%200R%20sqlspider
1991 | http://10.150.150.212:80/phpmyadmin/js/ajax.js?v=4.8.3%27%200R%20sqlspider
1992 | http://10.150.150.212:80/phpmyadmin/js/messages.php?v=4.8.3%27%200R%20sqlspider&lang=en&l=en
1993 | http://10.150.150.212:80/phpmyadmin/js/messages.php?v=4.8.3%27%200R%20sqlspider&l=en
1994 | http://10.150.150.212:80/phpmyadmin/js/messages.php?v=4.8.3%27%200R%20sqlspider
1995 | http://10.150.150.212:80/phpmyadmin/phpmyadmin.css.php?server=1%27%200R%20sqlspider&nocache=4611900160ltr
1996 | http://10.150.150.212:80/phpmyadmin/phpmyadmin.css.php?server=1%27%200R%20sqlspider
1997 | http://10.150.150.212:80/dashboard/javascripts/?C=N%3B0%3DD%27%200R%20sqlspider
1998 | http://10.150.150.212:80/dashboard/javascripts/?C=M%3B0%3DA%27%200R%20sqlspider
1999 | http://10.150.150.212:80/dashboard/javascripts/?C=S%3B0%3DA%27%200R%20sqlspider
2000 | http://10.150.150.212:80/dashboard/javascripts/?C=D%3B0%3DA%27%200R%20sqlspider
2001 | http://10.150.150.212:80/phpmyadmin/js/vendor/tracekit.js?v=4.8.3%27%200R%20sqlspider
2002 | http://10.150.150.212:80/phpmyadmin/js/error_report.js?v=4.8.3%27%200R%20sqlspider
2003 | http://10.150.150.212:80/phpmyadmin/js/functions.js?v=4.8.3%27%200R%20sqlspider
2004 | http://10.150.150.212:80/phpmyadmin/js/ajax.js?v=4.8.3%27%200R%20sqlspider
2005 | http://10.150.150.212:80/phpmyadmin/js/messages.php?v=4.8.3%27%200R%20sqlspider&lang=en&l=en
2006 | http://10.150.150.212:80/phpmyadmin/js/messages.php?v=4.8.3%27%200R%20sqlspider&l=en
2007 | http://10.150.150.212:80/phpmyadmin/js/messages.php?v=4.8.3%27%200R%20sqlspider
2008 | http://10.150.150.212:80/phpmyadmin/phpmyadmin.css.php?server=1%27%200R%20sqlspider&nocache=4611900160ltr
2009 | http://10.150.150.212:80/phpmyadmin/phpmyadmin.css.php?server=1%27%200R%20sqlspider

```

IPA: 10.150.150.212

Open Ports - 80

Services - http

Services Version – Apache/2.4.25

Detected Vulnerabilities – SQLi

CVE/CWE –2011-3192

```
⌂← Account links →
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 id:
Form action: http://10.150.150.222/checkout/cart/add/uenc/aHR0cDovLzEwLjE1MC4xNTAuMjIyL2luZGV4LnBocA%2C%2C/product/2057/

Path: http://10.150.150.222:80/
Form id:
Form action: http://10.150.150.222/checkout/cart/add/uenc/aHR0cDovLzEwLjE1MC4xNTAuMjIyL2luZGV4LnBocA%2C%2C/product/2056/

Path: http://10.150.150.222:80/
Form id:
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/aHR0cDovLzEwLjE1MC4xNTAuMjIyL2luZGV4LnBocA%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 id:
Form action: http://10.150.150.222/checkout/cart/add/uenc/aHR0cDovLzEwLjE1MC4xNTAuMjIyL2luZGV4LnBocA%2C%2C/product/2052/

Path: http://10.150.150.222:80/
Form id:
```

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

```
507 |         dSCorePropagationData: 2020/10/22 19:07:53 UTC
508 |         dSCorePropagationData: 1601/01/01 00:04:17 UTC
509 | ldap-brute:
510 |   root:<empty> ⇒ Valid credentials
511 |   admin:<empty> ⇒ Valid credentials
512 |   administrator:<empty> ⇒ Valid credentials
513 |   webadmin:<empty> ⇒ Valid credentials
514 |   sysadmin:<empty> ⇒ Valid credentials
515 |   netadmin:<empty> ⇒ Valid credentials
516 |   guest:<empty> ⇒ Valid credentials
517 |   user:<empty> ⇒ Valid credentials
518 |   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 - ldap

Services Version – DC-DOOMOPS; OS: Windows

Detected Vulnerabilities – Shows valid credentials

CVE/CWE –N/A

Port 3306

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
l, LongColumnFlag, IgnoreSpaceBeforeParenthesis, ConnectWithDatabase, Support
sMultipleResults, SupportsAuthPlugins, SupportsMultipleStatments
|_ Status: Autocommit
|_ Salt: IFa7-J<,hJv4>xfs19h
|_ Auth Plugin Name: mysql_native_password
mysql-enum: 01 2024-03-09 04:09 EST
|_ Valid usernames:
|   root:<empty> - Valid credentials
|   netadmin:<empty> - Valid credentials
|   guest:<empty> - Valid credentials
|   user:<empty> - Valid credentials
|   web:<empty> - Valid credentials
|_ sysadmin:<empty> - Valid credentials
|   administrator:<empty> - Valid credentials
|   webadmin:<empty> - Valid credentials
|   admin:<empty> - Valid credentials
|   test:<empty> - Valid credentials
|_ Statistics: Performed 10 guesses in 11 seconds, average tps: 0.9
|_
Nmap scan report for 10.150.150.12
Host is up (0.19s latency).

PORT      STATE SERVICE
3306/tcp  closed mysql

...box, PIPELINING, SIZE 102400000, VRFY, ETRN, S
```

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

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
|_ Auth Plugin Name: mysql_native_password
| mysql-enum:
| Valid usernames:
| 1 root:<empty> - Valid credentials
| 2 netadmin:<empty> - Valid credentials
| 3 guest:<empty> - Valid credentials
| 4 user:<empty> - Valid credentials
| 5 web:<empty> - Valid credentials
| 6 sysadmin:<empty> - Valid credentials
| 7 administrator:<empty> - Valid credentials
| 8 webadmin:<empty> - Valid credentials
| 9 admin:<empty> - Valid credentials
| 10 test:<empty> - Valid credentials
|_ Statistics: Performed 10 guesses in 12 seconds, average tps: 0.8
| mysql-brute:
| Accounts: No valid accounts found
| Statistics: Performed 0 guesses in 12 seconds, average tps: 0.0
|_ ERROR: The service seems to have failed or is heavily firewalled...
|_mysql-empty-password: ERROR: Script execution failed (use -d to debug)

Nmap scan report for 10.150.150.146
Host is up (0.17s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
tcp_3306  PIPELINING, SIZE 10240000, VREF, ETRN, S
```

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