**VAPT report on Stapler**

**#Commands I use in linux**

**#arp-scan -l**

**#ifconfig**

**So continuing with ip 192.168.56.101 for stapler**

**# nmap -sS -sV 192.168.56.101**

nmap -A 192.168.56.101

Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-02 00:23 EST

Nmap scan report for red (192.168.56.101)

Host is up (0.00063s 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 192.168.43.187

| 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 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

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: 7

| Capabilities flags: 63487

| Some Capabilities: ConnectWithDatabase, Support41Auth, IgnoreSigpipes, Speaks41ProtocolOld, DontAllowDatabaseTableColumn, InteractiveClient, Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, SupportsLoadDataLocal, ODBCClient, FoundRows, SupportsCompression, IgnoreSpaceBeforeParenthesis, LongPassword, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatments

| Status: Autocommit

| Salt: C\*)Fzu|D\_\x14Z^@qI\x1Af :C

|\_ Auth Plugin Name: mysql\_native\_password

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=7.80%I=7%D=11/2%Time=5F9F97D7%P=x86\_64-pc-linux-gnu%r(NUL

SF:L,2D58,"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\xf5\x01\0\0\x04\x14\0\0\0\xadz\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\xa2O\x0e\xdd\x994\x9c\xe7\xfe\x871\xb0N\xea\x1c\x80\xd63w\xf1\xa

SF:f\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\

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\xb9O\xf5\xe3\xcc\

SF:x9a\xed\xbf`a\xd0\xa2\xc5KV\x86\xad\n\x7fou\xc4\xfa\xf7\xa37\xc4\|\xb0\

SF:xf1\xc3\x84O\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\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\x

SF:cc\[qt\x8a\xef\xbao/\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\.L\xf2\\g@\x08D\xbb\xbfp\xb5\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\x13O\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\xb

SF:cL}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\

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");

MAC Address: 08:00:27:6A:2A:09 (Oracle VirtualBox virtual NIC)

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 - 4.9

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

To check on serer ie port 80

**#nikto –h 192.168.56.101**

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 192.168.56.101

+ Target Hostname: 192.168.56.101

+ Target Port: 80

+ Start Time: 2020-11-05 15:15:40 (GMT-5)

---------------------------------------------------------------------------

+ Server: No banner retrieved

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ OSVDB-3093: /.bashrc: User home dir was found with a shell rc file. This may reveal file and path information.

+ OSVDB-3093: /.profile: User home dir with a shell profile was found. May reveal directory information and system configuration.

+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response

+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host

+ End Time: 2020-11-05 15:16:07 (GMT-5) (27 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested

Then for more info

# enum4linux 192.168.56.101

Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Nov 3 00:18:52 2020

==========================

| Target Information |

==========================

Target ........... 192.168.56.101

RID Range ........ 500-550,1000-1050

Username ......... ''

Password ......... ''

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

======================================================

| Enumerating Workgroup/Domain on 192.168.56.101 |

======================================================

[+] Got domain/workgroup name: WORKGROUP

==============================================

| Nbtstat Information for 192.168.56.101 |

==============================================

Looking up status of 192.168.56.101

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 192.168.56.101 |

=======================================

[+] Server 192.168.56.101 allows sessions using username '', password ''

=============================================

| Getting domain SID for 192.168.56.101 |

=============================================

Domain Name: WORKGROUP

Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

========================================

| OS information on 192.168.56.101 |

========================================

Use of uninitialized value $os\_info in concatenation (.) or string at ./enum4linux.pl line 464.

[+] Got OS info for 192.168.56.101 from smbclient:

[+] Got OS info for 192.168.56.101 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 192.168.56.101 |

===============================

Use of uninitialized value $users in print at ./enum4linux.pl line 874.

Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 877.

Use of uninitialized value $users in print at ./enum4linux.pl line 888.

Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 890.

===========================================

| Share Enumeration on 192.168.56.101 |

===========================================

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 192.168.56.101

//192.168.56.101/print$ Mapping: DENIED, Listing: N/A

//192.168.56.101/kathy Mapping: OK, Listing: OK

//192.168.56.101/tmp Mapping: OK, Listing: OK

//192.168.56.101/IPC$ [E] Can't understand response:

NT\_STATUS\_OBJECT\_NAME\_NOT\_FOUND listing \\*

======================================================

| Password Policy Information for 192.168.56.101 |

======================================================

[+] Attaching to 192.168.56.101 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 192.168.56.101 |

================================

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

=========================================================================

| Users on 192.168.56.101 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-1-5-32 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-1-5-21-864226560-67800430-3082388513 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-1-22-1 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 192.168.56.101 |

===============================================

No printers returned.

enum4linux complete on Tue Nov 3 00:20:01 2020

From enum4linux I got users.

Then further I try to login on ftp ie on port 21

# ftp 192.168.56.101

Connected to 192.168.56.101.

220-

220-|-----------------------------------------------------------------------------------------|

220-| Harry, make sure to update the banner when you get a chance to show who has access here |

220-|-----------------------------------------------------------------------------------------|

220-

So found one users here Harry

Further bruteforcing and logged in with username and password both anonymous

Name (192.168.56.101:root): anonymous

331 Please specify the password.

Password:

230 Login successful.

ftp> ls -al

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

drwxr-xr-x 2 0 0 4096 Jun 04 2016 .

drwxr-xr-x 2 0 0 4096 Jun 04 2016 ..

-rw-r--r-- 1 0 0 107 Jun 03 2016 note

226 Directory send OK.

Find a file and download that file ie note

ftp> mget note

here press y------

mget note? y

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 (69.4300 kB/s)

Opening that file

#cat note

Elly, make sure you update the payload information. Leave it in your FTP account once your are done! john.

from this we can conclude there are 3 users whose names are Elly,Harry,John.

Then we bruteforce using hydra and got password for user elly

# hydra -l elly -e nsr ftp://192.168.56.101

Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-11-03 00:37:49

[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:1/p:3), ~1 try per task

[DATA] attacking ftp://192.168.56.101:21/

[21][ftp] host: 192.168.56.101 login: elly password: ylle

1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-03 00:37:53

we got id and password for elly ie password ylle.

we again tried to connect through that id and password for elly.

# ftp 192.168.56.101

Connected to 192.168.56.101.

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 (192.168.56.101:root): elly

331 Please specify the password.

Password:

230 Login successful.

And wow loged successfully

Using hydra again for user bruteforcing ie users found from enum4linux

**# hydra -L user\_list.txt -P user\_list.txt 192.168.**56.101 **ftp**

Hydra v8.2 (c) 2016 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 2017-05-15 15:57:45  
[DATA] max 16 tasks per 1 server, overall 64 tasks, 729 login tries (l:27/p:27), ~0 tries per task  
[DATA] attacking service ftp on port 21  
**[21][ftp] host: 192.168.1.30 login: SHayslett password: SHayslett**  
[STATUS] 281.00 tries/min, 281 tries in 00:01h, 448 to do in 00:02h, 16 active  
[STATUS] 281.50 tries/min, 563 tries in 00:02h, 166 to do in 00:01h, 16 active  
1 of 1 target successfully completed, 1 valid password found  
Hydra (<http://www.thc.org/thc-hydra>) finished at 2017-05-15 16:00:22

**# ftp 192.168.**56.101

Connected to 192.168.56.101  
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 (192.168.1.30:root): **SHayslett**  
331 Please specify the password.  
Password:**SHayslett**

ie **SHayslett** Password:**SHayslett**

Trying to access SSH we come across a username Barry. Apart from we could not find anything that was interesting.

Then moving towards the ssh port

# ssh root@192.168.56.101  
The authenticity of host '192.168.1.30 (192.168.1.30)' can't be established.  
ECDSA key fingerprint is SHA256:WuY26BwbaoIOawwEIZRaZGve4JZFaRo7iSvLNoCwyfA.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.1.30' (ECDSA) to the list of known hosts.  
-----------------------------------------------------------------  
~ Barry, don't forget to put a message here ~  
-----------------------------------------------------------------  
root@192.168.1.30's password:

Then moving towards nc and what we got in last list of more user

Hence **enumerating using nc**

**# nc 192.168.** 56.101  **666**  
Pd��Hp���,2  
 message2.jpgUT +�QWJ�QWux  
<snip>

**# nc 192.168.**56.101 **666 > pic.jpeg**

**# file pic.jpeg**  
pic.jpeg: Zip archive data, at least v2.0 to extract

**# unzip pic.jpeg**  
Archive: pic.jpeg  
 inflating: message2.jpg

Found these user on pic

**[+] Identified the following 10 user/s:  
 +----+---------+-----------------+  
 | Id | Login | Name |  
 +----+---------+-----------------+  
 | 1 | john | John Smith |  
 | 2 | elly | Elly Jones |  
 | 3 | peter | Peter Parker |  
 | 4 | barry | Barry Atkins |  
 | 5 | heather | Heather Neville |  
 | 6 | garry | garry |  
 | 7 | harry | harry |  
 | 8 | scott | scott |  
 | 9 | kathy | kathy |  
 | 10 | tim | tim |  
 +----+---------+-----------------+**

So there is more left but my pc is not working good