Vulnix

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -p- -A
192.168.103.149
130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-07 06:57 EST
Nmap scan report for 192.168.103.149
Host is up (0.0023s latency).
Not shown: 65518 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 10:cd:9e:a0:e4:e0:30:24:3e:bd:67:5f:75:4a:33:bf (DSA)
|   2048 bc:f9:24:07:2f:cb:76:80:0d:27:a6:48:52:0a:24:3a (RSA)
|_  256 4d:bb:4a:c1:18:e8:da:d1:82:6f:58:52:9c:ee:34:5f (ECDSA)
25/tcp   open  smtp       Postfix smtpd
|_smtp-commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2021-03-07T12:00:29+00:00; 0s from scanner time.
79/tcp   open  finger     Linux fingerd
|_finger: No one logged on.\x0D
110/tcp  open  pop3?
|_ssl-date: 2021-03-07T12:00:30+00:00; +1s from scanner time.
111/tcp  open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4      111/tcp   rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100000  3,4        111/tcp6  rpcbind
|   100000  3,4        111/udp6  rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/tcp6  nfs
|   100003  2,3,4     2049/udp   nfs
|   100003  2,3,4     2049/udp6  nfs
|   100005  1,2,3    44459/tcp6  mountd
|   100005  1,2,3    51870/udp6  mountd
|   100005  1,2,3    57332/udp   mountd
|   100005  1,2,3    59665/tcp   mountd
|   100021  1,3,4    34109/udp   nlockmgr
|   100021  1,3,4    41913/tcp   nlockmgr
|   100021  1,3,4    43612/udp6  nlockmgr
|   100021  1,3,4    50159/tcp6  nlockmgr
|   100024  1        49652/udp   status
|   100024  1        50961/udp6  status
|   100024  1        51299/tcp   status
|   100024  1        58054/tcp6  status
|   100227  2,3       2049/tcp   nfs_acl
|   100227  2,3       2049/tcp6  nfs_acl
|   100227  2,3       2049/udp   nfs_acl
|_  100227  2,3       2049/udp6  nfs_acl
143/tcp  open  imap       Dovecot imapd
|_ssl-date: 2021-03-07T12:00:29+00:00; +1s from scanner time.
512/tcp  open  exec       netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
```

993/tcp open ssl/imaps?
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail server
| Not valid before: 2012-09-02T17:40:22
|_Not valid after: 2022-09-02T17:40:22
|_ssl-date: 2021-03-07T12:00:29+00:00; +1s from scanner time.
995/tcp open ssl/pop3s?
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail server
| Not valid before: 2012-09-02T17:40:22
|_Not valid after: 2022-09-02T17:40:22
|_ssl-date: 2021-03-07T12:00:29+00:00; +1s from scanner time.
2049/tcp open nfs_acl   2-3 (RPC #100227)
39142/tcp open mountd   1-3 (RPC #100005)
41913/tcp open nlockmgr 1-4 (RPC #100021)
46414/tcp open mountd   1-3 (RPC #100005)
51299/tcp open status   1 (RPC #100024)
59665/tcp open mountd   1-3 (RPC #100005)
Service Info: Host: vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 182.05 seconds

22/tcp

22/tcp   open ssh   OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 10:cd:9e:a0:e4:e0:30:24:3e:bd:67:5f:75:4a:33:bf (DSA)
| 2048 bc:f9:24:07:2f:cb:76:80:0d:27:a6:48:52:0a:24:3a (RSA)
|_ 256 4d:bb:4a:c1:18:e8:da:d1:82:6f:58:52:9c:ee:34:5f (ECDSA)

BruteForce

┌──(kali㉿kali)-[~/Desktop/exe]
└─$ hydra -L users.txt -P /usr/share/wordlists/rockyou.txt 192.168.103.149 ssh -t 4
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 10:14:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 372954374 login tries (l:26/p:14344399), ~93238594 tries per task
[DATA] attacking ssh://192.168.103.149:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 372954330 to do in 141270:35h, 4 active
[STATUS] 33.33 tries/min, 100 tries in 00:03h, 372954274 to do in 186477:09h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 372954170 to do in 213290:48h, 4 active

25/tcp

25/tcp   open smtp   Postfix smtpd
|_smtp-commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

|_ssl-date: 2021-03-07T12:00:29+00:00; 0s from scanner time.

nmap

```
┌──(kali㉿kali)-[~]
└─$ nmap --script=smtp-* 192.168.103.149
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-07 07:32 EST
Nmap scan report for 192.168.103.149
Host is up (0.0011s latency).
Not shown: 988 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
|_smtp-commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| smtp-enum-users:
|_  Method RCPT returned a unhandled status code.
|_smtp-open-relay: Server doesn't seem to be an open relay, all tests failed
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
79/tcp  open  finger
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
993/tcp  open  imaps
995/tcp  open  pop3s
2049/tcp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

metasploit

```
Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                     Required  Description
   ----       ---------------                                     --------  -----------
   RHOSTS     192.168.103.149                                       yes       The target host(s), range CIDR
identifier, or hosts file with syntax 'file:<path>'
   RPORT      25                                                  yes       The target port (TCP)
   THREADS    1                                                   yes       The number of concurrent threads (max one
per host)
   UNIXONLY   true                                                yes       Skip Microsoft bannered servers when
testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that
contains a list of probable users accounts.

msf6 auxiliary(scanner/smtp/smtp_enum) > run
```

[*] 192.168.103.149:25 - 192.168.103.149:25 Banner: 220 vulnix ESMTP Postfix (Ubuntu)
[+] 192.168.103.149:25 - 192.168.103.149:25 Users found: , backup, bin, daemon, games, gnats, irc, landscape, libuuid, list, lp, mail, man, messagebus, news, nobody, postfix, postmaster, proxy, sshd, sync, sys, syslog, user, uucp, whoopsie, www-data
[*] 192.168.103.149:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

79/tcp

79/tcp open finger Linux fingerd
|_finger: No one logged on.\x0D

110/tcp

110/tcp open pop3?
|_ssl-date: 2021-03-07T12:00:30+00:00; +1s from scanner time.

111/tcp

111/tcp open rpcbind 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
| 100000 3,4 111/udp6 rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/tcp6 nfs
| 100003 2,3,4 2049/udp nfs
| 100003 2,3,4 2049/udp6 nfs
| 100005 1,2,3 44459/tcp6 mountd
| 100005 1,2,3 51870/udp6 mountd
| 100005 1,2,3 57332/udp mountd
| 100005 1,2,3 59665/tcp mountd
| 100021 1,3,4 34109/udp nlockmgr
| 100021 1,3,4 41913/tcp nlockmgr
| 100021 1,3,4 43612/udp6 nlockmgr
| 100021 1,3,4 50159/tcp6 nlockmgr
| 100024 1 49652/udp status
| 100024 1 50961/udp6 status
| 100024 1 51299/tcp status
| 100024 1 58054/tcp6 status
| 100227 2,3 2049/tcp nfs_acl
| 100227 2,3 2049/tcp6 nfs_acl
| 100227 2,3 2049/udp nfs_acl
|_ 100227 2,3 2049/udp6 nfs_acl

Enum

```
┌──(kali㉿kali)-[~]
└─$ rpcinfo -p
192.168.103.149
1 ×
   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  49652  status
    100024    1   tcp  51299  status
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100227    2   tcp   2049
    100227    3   tcp   2049
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100227    2   udp   2049
    100227    3   udp   2049
    100021    1   udp  34109  nlockmgr
    100021    3   udp  34109  nlockmgr
    100021    4   udp  34109  nlockmgr
    100021    1   tcp  41913  nlockmgr
    100021    3   tcp  41913  nlockmgr
    100021    4   tcp  41913  nlockmgr
    100005    1   udp  52983  mountd
    100005    1   tcp  39142  mountd
    100005    2   udp  49081  mountd
    100005    2   tcp  46414  mountd
    100005    3   udp  57332  mountd
    100005    3   tcp  59665  mountd
```

143/tcp

```
143/tcp   open  imap      Dovecot imapd
|_ssl-date: 2021-03-07T12:00:29+00:00; +1s from scanner time.
```

512/tcp

```
512/tcp   open  exec      netkit-rsh rexecd
```

513/tcp

```
513/tcp   open  login
```

514/tcp

514/tcp open tcpwrapped

netcat

└─$ nc -vn 192.168.103.149 514
(UNKNOWN) [192.168.103.149] 514 (shell) open

993/tcp

993/tcp open ssl/imaps?
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail server
| Not valid before: 2012-09-02T17:40:22
|_Not valid after: 2022-09-02T17:40:22
|_ssl-date: 2021-03-07T12:00:29+00:00; +1s from scanner time.

995/tcp

995/tcp open ssl/pop3s?
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail server
| Not valid before: 2012-09-02T17:40:22
|_Not valid after: 2022-09-02T17:40:22
|_ssl-date: 2021-03-07T12:00:29+00:00; +1s from scanner time.

2049/tcp

2049/tcp open nfs_acl   2-3 (RPC #100227)
39142/tcp open mountd   1-3 (RPC #100005)
41913/tcp open nlockmgr 1-4 (RPC #100021)
46414/tcp open mountd   1-3 (RPC #100005)
51299/tcp open status   1 (RPC #100024)
59665/tcp open mountd   1-3 (RPC #100005)

showmount

┌──(kali㉿kali)-[~]
└─$ showmount --exports 192.168.103.149
Export list for 192.168.103.149:
/home/vulnix *