25/tcp open smtp Postfix smtpd

|\_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|\_Not valid after: 2010-04-16T14:07:45

|\_ssl-date: 2022-06-24T07:04:21+00:00; -43s from scanner time.

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2\_RC4\_128\_WITH\_MD5

| SSL2\_DES\_64\_CBC\_WITH\_MD5

| SSL2\_RC2\_128\_CBC\_WITH\_MD5

| SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5

| SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5

|\_ SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5

apt install smtp-user-enum

┌──(root💀kali)-[~]

└─# smtp-user-enum -M VRFY -t 192.168.1.36 -U /usr/share/wordlists/metasploit/unix\_users.txt 1 ⨯

Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

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

| Scan Information |

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

Mode ..................... VRFY

Worker Processes ......... 5

Usernames file ........... /usr/share/wordlists/metasploit/unix\_users.txt

Target count ............. 1

Username count ........... 168

Target TCP port .......... 25

Query timeout ............ 5 secs

Target domain ............

######## Scan started at Sat Jun 25 10:11:41 2022 #########

192.168.1.36: backup exists

192.168.1.36: bin exists

192.168.1.36: daemon exists

192.168.1.36: distccd exists

192.168.1.36: ftp exists

192.168.1.36: games exists

192.168.1.36: gnats exists

192.168.1.36: irc exists

192.168.1.36: list exists

192.168.1.36: libuuid exists

192.168.1.36: lp exists

192.168.1.36: mail exists

192.168.1.36: man exists

192.168.1.36: mysql exists

192.168.1.36: news exists

192.168.1.36: nobody exists

192.168.1.36: postfix exists

192.168.1.36: postgres exists

192.168.1.36: postmaster exists

192.168.1.36: proxy exists

192.168.1.36: root exists

192.168.1.36: ROOT exists

192.168.1.36: service exists

192.168.1.36: sshd exists

192.168.1.36: sys exists

192.168.1.36: sync exists

192.168.1.36: syslog exists

192.168.1.36: user exists

192.168.1.36: uucp exists

192.168.1.36: www-data exists

######## Scan completed at Sat Jun 25 10:11:46 2022 #########

30 results.

168 queries in 5 seconds (33.6 queries / sec)

msf6 > use auxiliary/scanner/smtp/smtp\_enum

msf6 auxiliary(scanner/smtp/smtp\_enum) > options

Module options (auxiliary/scanner/smtp/smtp\_enum):

Name Current Setting Required Description

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

RHOSTS yes The target host(s), see https://github.com/rapid7

/metasploit-framework/wiki/Using-Metasploit

RPORT 25 yes The target port (TCP)

THREADS 1 yes The number of concurrent threads (max one per hos

t)

UNIXONLY true yes Skip Microsoft bannered servers when testing unix

users

USER\_FILE /usr/share/metasploit-framew yes The file that contains a list of probable users a

ork/data/wordlists/unix\_user ccounts.

s.txt

msf6 auxiliary(scanner/smtp/smtp\_enum) > set rhosts 192.168.1.36

rhosts => 192.168.1.36

msf6 auxiliary(scanner/smtp/smtp\_enum) > run

[\*] 192.168.1.36:25 - 192.168.1.36:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

[+] 192.168.1.36:25 - 192.168.1.36:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data

[\*] 192.168.1.36:25 - Scanned 1 of 1 hosts (100% complete)

[\*] Auxiliary module execution completed

┌──(root💀kali)-[~]

└─# nc 192.168.1.36 25

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

VRFY root

252 2.0.0 root

VRFY SYS

252 2.0.0 SYS

VRFY admin

550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table

VRFY VRFY unix