SMTP VRFY Scanner

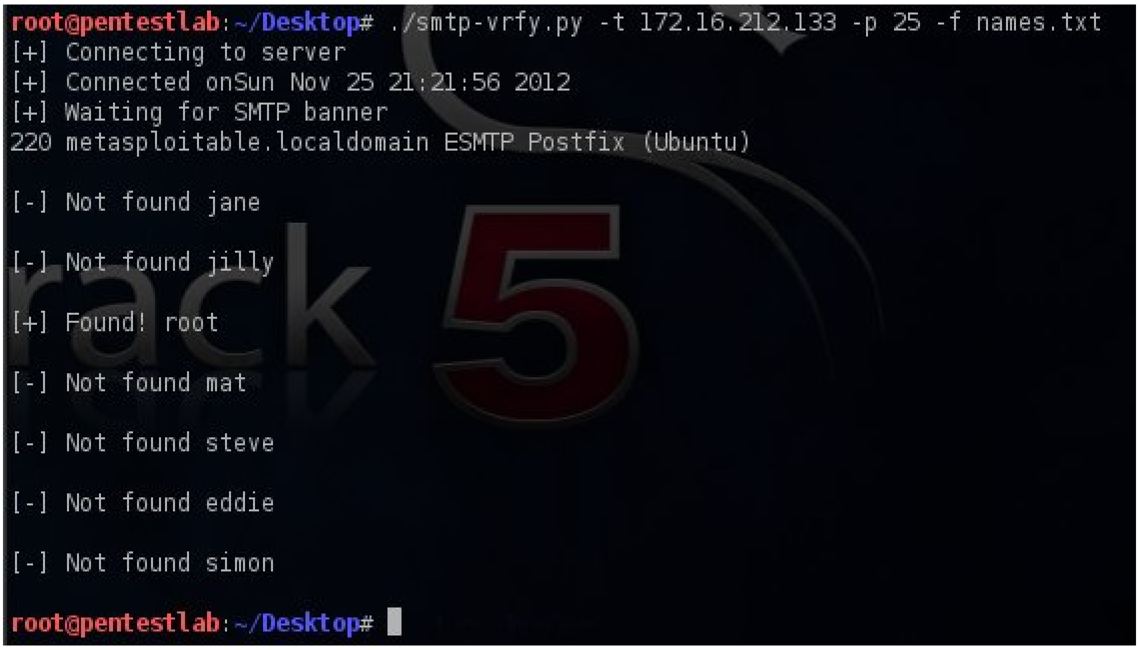
pentestlab.blog/category/coding/page/6

November 26, 2012

This is a python script that tries to connect on port 25 and performs automatic username enumeration through the vrfy command by supplying a .txt file with usernames.

```
#!/usr/bin/python
# This was written for educational and learning purposes only.
# The author will be not responsible for any damage!
# SMTP VRFY Scanner

import socket, sys, fileinput, re, time
from optparse import OptionParser

usage =  "./%prog -t <target> -p <port> -i <inputfile>\nExample: ./%prog -t
74.52.252.187 -p 25 -f names.txt"
parser = OptionParser(usage=usage)
parser.add_option("-t", type="string",
action="store", dest="target",
help="Target Host")
parser.add_option("-p", type="int",
action="store", dest="port",
help="Target Port")
parser.add_option("-f", action="store",
dest="filename",help="Inputfile")
(options, args) = parser.parse_args()

host = options.target
port = options.port
inputfile = options.filename

if len(sys.argv) != 7:
print "\n|---------------------------------------------------------------|"
print "|             SMTP vrfy enumeration scanner v0.5                |"
print "|                      by MrMe 07/2009                          |"
print "|                    Special Greetz: krma                       |"
print "|---------------------------------------------------------------|\n"
parser.print_help()
sys.exit()
try:
names = open(sys.argv[6], "r")
except(IOError):
print "Error: Check your wordlist path\n"
sys.exit(1)

line = names.readline()
counter = 0
```

```
print "[+] Connecting to server"
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)

def connect():
try:
connect=s.connect((host,port))
except socket.timeout:
print "\n[-] Server timed out"
sys.exit(1)
except socket.error:
print "\n[-] There was an error with the server"
sys.exit(1)
print "[+] Connected on" +timer()
print "[+] Waiting for SMTP banner"
banner=s.recv(1024)
print banner

def timer():
now = time.localtime(time.time())
return time.asctime(now)

connect()

for line in names:
s.send('VRFY '+line)
result=s.recv(1024)
bad = re.match("502",result)
bad1 = re.search("send some mail",result)
found = re.search("252",result)
notfound = re.match("550",result)
if bad or bad1:
print "[-] This server is not vulnerable!"
sys.exit(1)
elif notfound:
print "[-] Not found "+line
elif found:
print "[+] Found! "+line
if counter == 20:
s.close()
print "[+] Resetting connection"
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
connect()
counter = 0
counter +=1

s.close()
```



```
root@pentestlab:~/Desktop# ./smtp-vrfy.py -t 172.16.212.133 -p 25 -f names.txt
[+] Connecting to server
[+] Connected onSun Nov 25 21:21:56 2012
[+] Waiting for SMTP banner
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

[-] Not found jane

[-] Not found jilly

[+] Found! root

[-] Not found mat

[-] Not found steve

[-] Not found eddie

[-] Not found simon

root@pentestlab:~/Desktop#
```

SMTP VRFY Scanner – Demo

Author:MrMe