Penetration Testing Report: SMTP Service Enumeration on Port 25

Target: 10.137.0.149

Test Conducted By: MD SAMSUL KABIR

Date:21/09/2024

Test Scope: Authorized penetration testing on the SMTP service.

Summary:

An assessment of the SMTP service running on port 25 was conducted using Nmap and Metasploit Framework tools to identify potential vulnerabilities and enumerate valid users.

Findings:

Service Detection:

Port: 25/tcp

Service: SMTP

Version: Cisco PIX sanitized smtpd

State: Open

Summary

An assessment of the SMTP service running on port 25 was conducted using Nmap and Metasploit Framework tools to identify potential vulnerabilities and enumerate valid users. The analysis revealed critical information regarding the exposed SMTP service and associated risks.

Nmap detected the SMTP service indicating that it is exposed to the network, which may allow for potential enumeration or exploitation.

User Enumeration: Using the Metasploit module auxiliary/scanner/smtp/smtp_enum, valid usernames were successfully enumerated. The following usernames were identified: _apt, backup, bin, daemon, dnsmasq, games, gnats, irc, landscape, list, lp, lxd, mail, man, messagebus, mysql, news, nobody, pollinate, postfix, postmaster, proxy, sshd, sync, sys, syslog, systemd-coredump, systemd-network, systemd-resolve, systemd-timesync, tcpdump, tss, usbmux, uucp, uuidd, www-data

Potential Risks:

Following the successful enumeration of valid usernames from the SMTP service, there is a significant risk of brute-force attacks targeting these accounts. Attackers can utilize automated tools to attempt a large number of password combinations against the identified users, potentially leading to unauthorized access. Once access is obtained, attackers could leverage compromised accounts for further infiltration into the network, data exfiltration, or privilege escalation. The exposure of valid usernames greatly increases the attack surface, making it essential to implement mitigations against such attacks.

The enumeration of valid usernames can lead to further attacks, such as password guessing or phishing attempts.

An exposed SMTP service may be vulnerable to attacks, including spam relay or exploitation of service misconfigurations.

Remote Code Execution-Some older versions of SMTP or improperly configured services might be vulnerable to remote code execution exploits.

Recommendations:

To mitigate brute-force attack it is recommended to enforce strong password policies, implement account lockout mechanisms after repeated failed login attempts, and enable multi-factor authentication (MFA) wherever possible.

Implement strong authentication mechanisms and consider using SMTP authentication to limit unauthorized access.

Restrict access to the SMTP service from untrusted networks or implement firewall rules to control inbound traffic.

Regularly review and update user accounts and remove any unnecessary or inactive users.

Consider disabling the enumeration feature if it is not required for legitimate use.

Conclusion:

The enumeration of usernames on the SMTP service indicates a potential security risk that should be addressed promptly. The organization is advised to implement the recommended security measures to mitigate the identified vulnerabilities.

Proof & Findings

First we did “Nmap 10.137.0.149” to check the open ports.

```
hackme@hackme: ~
File  Actions  Edit  View  Help

┌──(hackme㉿hackme)-[~]
└─$ nmap 10.137.0.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-20 23:50 AEST
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.021s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
5000/tcp  open  upnp
5001/tcp  open  commplex-link
5003/tcp  open  filemaker
8000/tcp  open  http-alt
8080/tcp  open  http-proxy
8888/tcp  open  sun-answerbook
9000/tcp  open  cslistener
9001/tcp  open  tor-orport
9200/tcp  open  wap-wsp
50000/tcp open  ibm-db2

Nmap done: 1 IP address (1 host up) scanned in 14.67 seconds

┌──(hackme㉿hackme)-[~]
└─$ msfconsole
```

Open Ports

To further analyze the services running on port 25 (SMTP) of the target system (IP: 10.137.0.149), I executed the command nmap -sV -p 25 10.137.0.149. This command is specifically designed to perform a service version detection on a targeted port, which in this case is port 25, commonly associated with SMTP. The -sV flag instructs Nmap to probe the open port and determine the version of the service running on it, providing valuable information for vulnerability assessment. The scan revealed that the SMTP service is running on a Cisco PIX firewall with a sanitized SMTP daemon, indicating the presence of a firewall security mechanism. Understanding the exact service and version is crucial for identifying potential vulnerabilities and assessing the security posture of the system.

```
hackme@hackme: ~
File  Actions  Edit  View  Help

┌──(hackme㉿hackme)-[~]
└─$ nmap -sV -p 25 10.137.0.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-21 18:42 AEST
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.075s latency).

PORT   STATE SERVICE VERSION
25/tcp open  smtp    Cisco PIX sanitized smtpd
Service Info: Device: firewall; CPE: cpe:/o:cisco:pix_firewall_software

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.98 seconds

┌──(hackme㉿hackme)-[~]
└─$
```

nmap -sV -p 25 10.137.0.149

We can enumeration the user those who is using SMPT. “search smpt” gives us the options and we can use the options to grab the users.

```
hackme@hackme: ~
File  Actions  Edit  View  Help
[-] Unknown command: searchh. Did you mean search? Run the help command for more details.
msf6 > search smtp

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

   #   Name                                                      Disclosure Date  Ran
k       Check  Description
   -   ----                                                      ---------------  ---
-       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                      2015-10-01       nor
mal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
   1     \_ target: Bash Completion                              .                .
         .      .
   2     \_ target: Cron                                         .                .
         .      .
   3   auxiliary/server/capture/smtp                             .                nor
mal     No     Authentication Capture: SMTP
   4   auxiliary/scanner/http/gavazzi_em_login_loot              .                nor
mal     No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Databa
se
   5   exploit/unix/smtp/clamav_milter_blackhole                 2007-08-24       exc
ellent  No     ClamAV Milter Blackhole-Mode Remote Code Execution
   6   exploit/windows/browser/communicrypt_mail_activex         2010-05-19       gre
at      No     CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
   7   exploit/linux/smtp/exim_gethostbyname_bof                 2015-01-27       gre
at      Yes    Exim GHOST (glibc gethostbyname) Buffer Overflow
   8   exploit/linux/smtp/exim4_dovecot_exec                     2013-05-03       exc
ellent  No     Exim and Dovecot Insecure Configuration Command Injection
   9   exploit/unix/smtp/exim4_string_format                     2010-12-07       exc
ellent  No     Exim4 string_format Function Heap Buffer Overflow
   10  auxiliary/client/smtp/emailer                             .                nor
mal     No     Generic Emailer (SMTP)
   11  exploit/linux/smtp/haraka                                 2017-01-26       exc
```

```
   13    \_ target: linux x86                                    .                .
         .      .
   14  exploit/windows/http/mdaemon_worldclient_form2raw         2003-12-29       gre
at      Yes    MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
   15    \_ target: Universal MDaemon.exe                        .                .
         .      .
   16    \_ target: Debugging test                               .                .
         .      .
   17  exploit/windows/smtp/ms03_046_exchange2000_xexch50        2003-10-15       goo
d       Yes    MS03-046 Exchange 2000 XEXCH50 Heap Overflow
   18  exploit/windows/ssl/ms04_011_pct                          2004-04-13       ave
rage    No     MS04-011 Microsoft Private Communications Transport Overflow
   19    \_ target: Windows 2000 SP4                             .                .
         .      .
   20    \_ target: Windows 2000 SP3                             .                .
         .      .
   21    \_ target: Windows 2000 SP2                             .                .
         .      .
   22    \_ target: Windows 2000 SP1                             .                .
         .      .
   23    \_ target: Windows 2000 SP0                             .                .
         .      .
   24    \_ target: Windows XP SP0                               .                .
         .      .
   25    \_ target: Windows XP SP1                               .                .
         .      .
   26  auxiliary/dos/windows/smtp/ms06_019_exchange              2004-11-12       nor
mal     No     MS06-019 Exchange MODPROP Heap Overflow
   27  exploit/windows/smtp/mercury_cram_md5                     2007-08-18       gre
at      No     Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
   28  exploit/unix/smtp/morris_sendmail_debug                   1988-11-02       ave
rage    Yes    Morris Worm sendmail Debug Mode Shell Escape
   29  exploit/windows/smtp/njstar_smtp_bof                      2011-10-31       nor
```

Search smtp

A search for SMTP-related modules in Metasploit to identify potential vulnerabilities on the target's SMTP service. The search returned various exploits and auxiliary tools that can be used to attack or gather information about SMTP servers. Some of the exploits target vulnerabilities like remote code execution or buffer overflows, such as in Apache James Server or OpenSMTPD. The auxiliary modules provide functionalities for capturing SMTP authentication details, enumerating users, and checking for open relays. I'll proceed by selecting and configuring the appropriate module to exploit or gather intel on the target's SMTP service.

Search smpt_enum:

This module is a utility used for **SMTP user enumeration**. It helps identify valid usernames on an SMTP server by trying common usernames or usernames from a list.

```
hackme@hackme: ~
File  Actions  Edit  View  Help

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search smtp_enum

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

   #  Name                                  Disclosure Date  Rank    Check  Descr
iption
   -  ----                                  ---------------  ----    -----  -----
------
   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 aux
iliary/scanner/smtp/smtp_enum

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > ahow options
[-] Unknown command: ahow. Run the help command for more details.
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

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

   Name       Current Setting      Required  Description
```

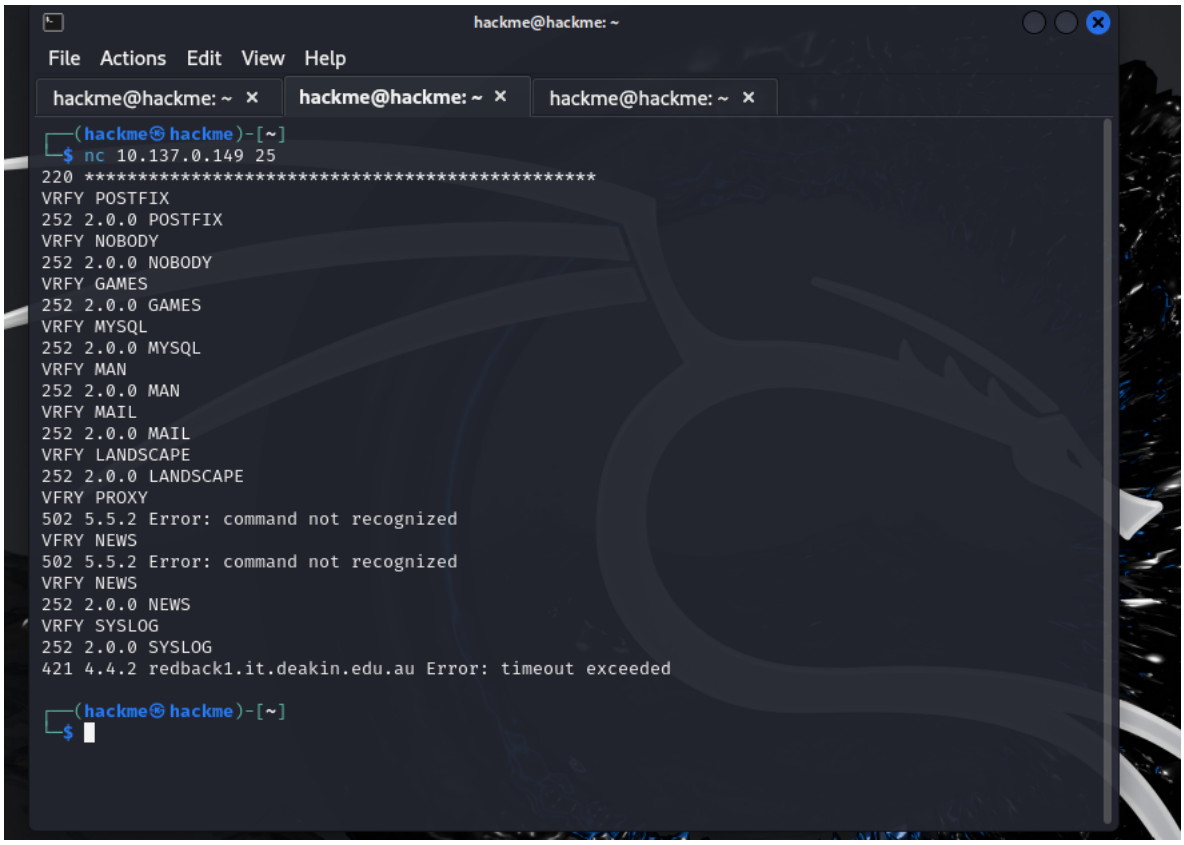
```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOST 10.137.0.149
RHOST => 10.137.0.149
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 10.137.0.149:25       - 10.137.0.149:25 Banner: 220 ********************
***************************
[+] 10.137.0.149:25       - 10.137.0.149:25 Users found: , _apt, backup, bin,
 daemon, dnsmasq, games, gnats, irc, landscape, list, lp, lxd, mail, man, mes
sagebus, mysql, news, nobody, pollinate, postfix, postmaster, proxy, sshd, sy
nc, sys, syslog, systemd-coredump, systemd-network, systemd-resolve, systemd-
timesync, tcpdump, tss, usbmux, uucp, uuidd, www-data
[*] 10.137.0.149:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Users found

"auxiliary/scanner/smtp/smtp_enum" module to enumerate users on the target mail server with IP 10.137.0.149. After loading the module and setting the target's IP (RHOST) and port 25 (RPORT), I executed the enumeration process. The module successfully connected to the SMTP service and retrieved a list of valid users on the system, including accounts such as _apt, bin, daemon, mysql,

postfix, and www-data. This user information can be valuable for further attacks, such as credential-based attacks or privilege escalation attempts. The scan was completed successfully, with detailed SMTP banner information also retrieved from the target.

Now with netcad server we can verify the users.



Users verified