Scapy 3

SMBLoris

Read this to learn about what this attack is. Your challenge is to recreate the attack using Scapy. Essentially, if you send "\x00\x01\xff\xff" to an smb port (445) you can consume the target's memory (send as raw data). (You have to send a lot of them (a loop) to be able to see this). So here is your task,

- using a windows machine under your control (vm)
- make sure it is listening on port 445. An easy way to do this: create a folder on the desktop, go to properties, enable sharing. Probably do an nmap on the target to make sure it is listening on the port
- I changed my RAM to only 1g, so that the results were more obvious.
- Modify your earlier tcp socket code to repeatedly start new sockets to port 445 (remember that in a loop you will need to alternate the port number so that it doesn't discard the packet).
  - **HINT:** maybe create your IP datagram outside your loop. Inside your loop, create the tcp segment and do the handhshake and send the raw data. Make sure to change/increment your port number each time
  - **HINT2:** My loop structure looks like this: `for port in range(33000, 35100):`
- You will also need to modify iptables so that a RST packet is not sent. (Something like `iptables -F; iptables -A OUTPUT -p tcp --tcp-flags RST RST -j DROP`)
- Take a screenshot that shows your RAM utilization of the vm going up.

To Submit

- Screenshots indicated above