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. (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
- 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).
- You will also need to modify iptables so that a RST packet is not sent.
- Take a screenshot that shows your RAM utilization of the vm going up.
- Capture a single SMBLoris packet and submit to [here](#) (Instructions on how to do that are on that page).
- You should be able to see your username at [here](#), provide a screenshot of your username on that page.

Land Attack

Read what this type of attack is [here](#). This attack could still be relevant due to IoT. Simulate the attack by sending a single packet to your windows machine. Capture 1 packet with tcpdump as indicated on [this](#) page. Take a screenshot that you have entered the winners page.

To Submit

- Screenshots indicated above