CYBR371

LAB 4

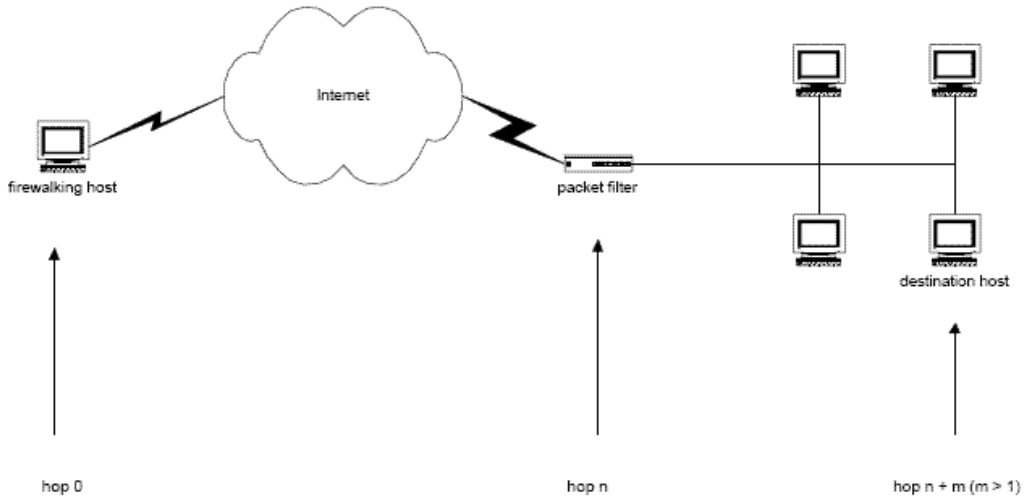
Olivia Fletcher
300534281
fletcholiv

Part A - Netlab

Question 1 [1 mark]

What is Firewalking (the technique and/or the tool) and how can it be used in an attack process against a potential target? [Max 250 words].

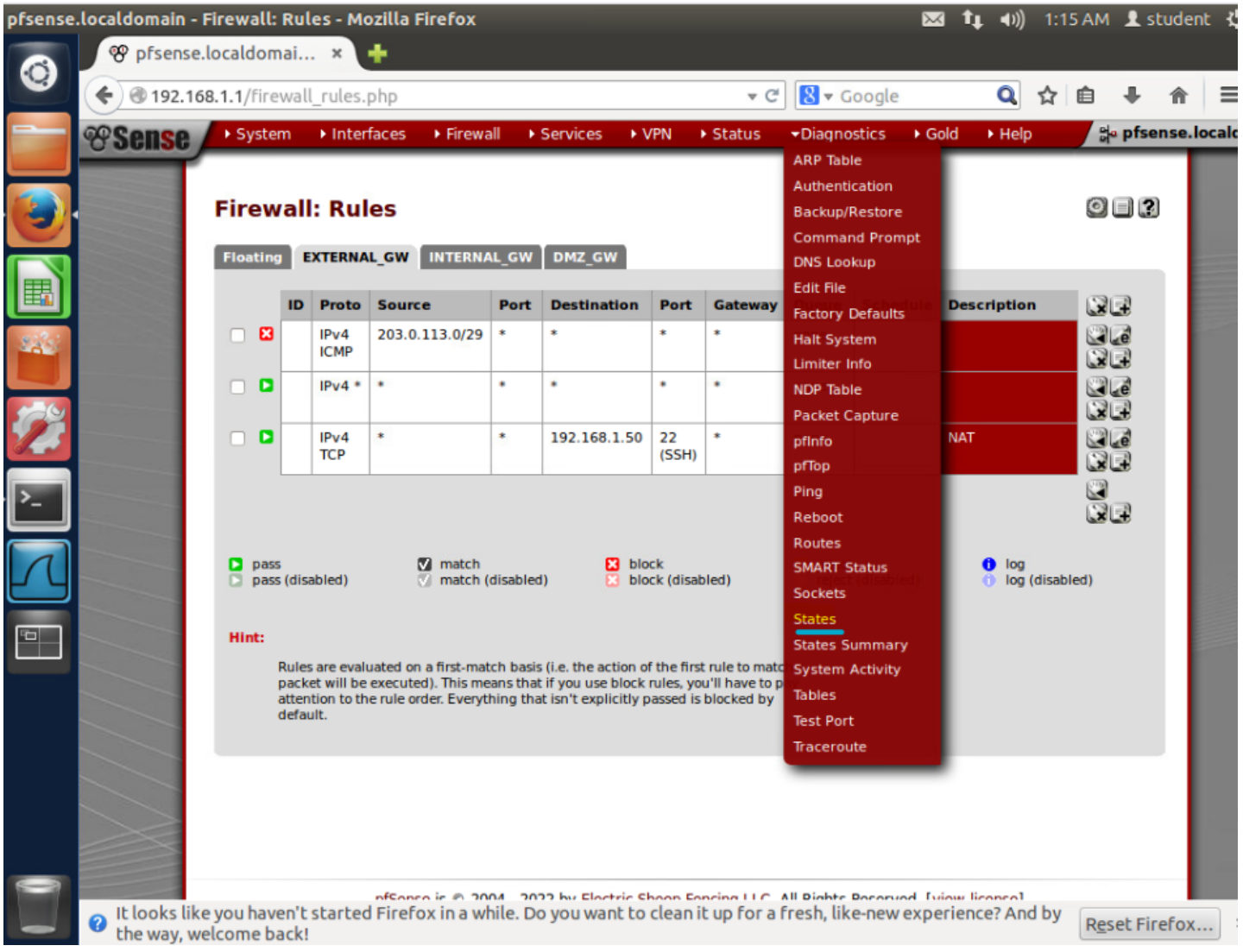
- The use of Firewalking is for an active network security analysis of trace route IP packets to determine which layer 4 protocols a specific firewall will allow. This determines which ports are open and whether packets are able to pass through the packet filtering firewall.
- An attacker uses this tool as it shows the attacker which packet types are able to pass through the destination/victims firewall to pass security measures.
- The victims firewall will work by scanning each and every packet and will determine whether it will be blocked by ACL/firewall and then dropped/rejected
- The attacker has used the firewalk tool and has sent different packets with control information to different ports to test which ones are able to pass through this scan and if successful instead of being rejected by the firewall it will then expire and elicit an ICMP exceeded message to the attacker.
- The attacker now knows which ports are open on the victims device using the firewalk scan information.

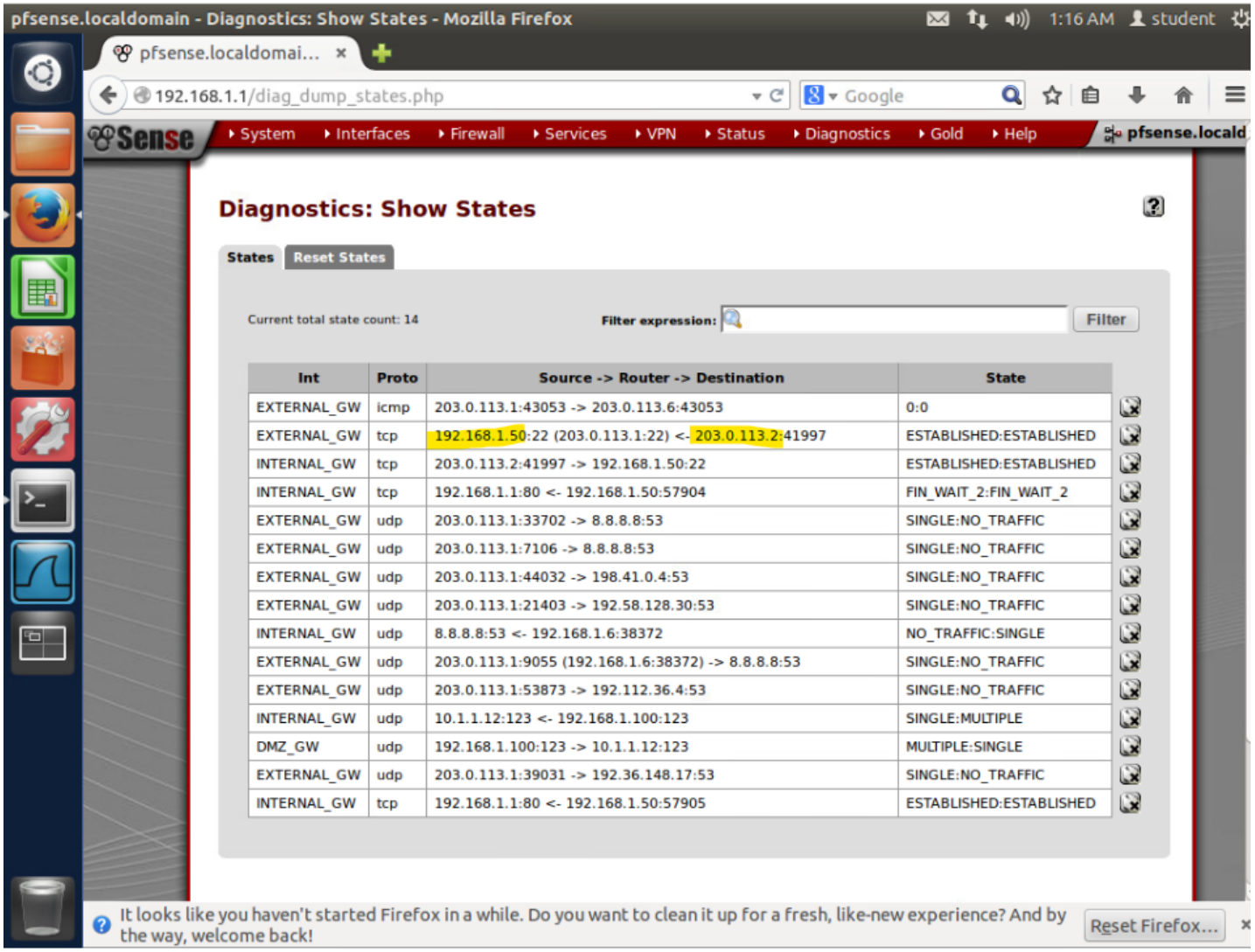


Question 2 [1 mark]

Is pfsense a stateful or a stateless firewall? Demonstrate the statefulness or the statelessness of pfsense firewall using the lab “Configuring a Network-Based Firewall ". You may include a screenshot.

- pfsense is a stateful firewall, it remembers all information/data about incoming connections through the firewall which means the traffic can reply automatically
- The data in saved in the State table as shown here; (This would not be the case if pfsense was not stateless based)
- Second screenshot showing the saved connection between the Kali and the Ubuntu machine through pfsense





Part B - Packet Filtering Firewalls

Question 1 [0.5 marks]

We have the following rule in our iptables on the server (i.e. 192.168.1.1). The client (192.168.1.78) however fails to initiate an SSH connection. Explain why this is the case.

'#sudo iptables -A INPUT -p tcp -s 192.168.1.78 -d 192.168.1.1 –dport 22 -i enp0s2 –j ACCEPT'

'#sudo iptables -A OUTPUT -p tcp -s 192.168.1.78 –sport 22 -d 192.168.1.1 –dport 22 ACCEPT'

'#sudo iptables -P INPUT DENY'

'#sudo iptables -P OUTPUT DENY'

- Although iptables prioritize by using the first input stream rule, in this case the first 2 lines are ignored as the third and fourth line are setting the default policy, overriding what was previously read in stream. " -P INPUT DENY" is the reason the client cannot ssh in.

Question 2 [0.5 marks]

Our server is running a Telnet service listening on port 23. We would like to stop any new Telnet connections from a client with the IP address of 10.0.2.5. Is the following a good rule to block the Client? Explain.

'#sudo iptables -A INPUT -s 10.0.2.5 -p tcp –sport 23 -j DROP'

- Yes and no, instead of using "--sport 23" we change that to "--dport23" so;
- sudo iptables -A INPUT -s 10.0.2.5 -p tcp –dport 23 -j DROP

- -A INPUT, chain for representing a packet coming into the system
- -s 10.0.2.5, stating the (source) IP address to block
- -p tcp, packet
- –dport 23, setting destination port to block as 23
- -j DROP, drop all connections coming from 10.0.2.5 IP using port 23

Question 3 [0.5 marks]

Write a rule to drop all the new incoming SSH service requests received on your primary interface which has a MAC address of 30:65:EC:22:14:D1.

- sudo iptables -A INPUT -s 30:65:EC:22:14:D1 -j DROP

- -A INPUT, specifying the chain
- -s 30:65:EC:22:14:D1, is specifying the MAC (source) address to block
- -j DROP, drop all connections (including ssh requests) using the 30:65:EC:22:14:D1 MAC

Question 4 [0.5 marks]

Write a rule to drop any incoming packets with "INVALID" state.

- sudo iptables -A INPUT -m state –state INVALID -j DROP

- -A INPUT, specifying the chain type
- -m state –state INVALID, setting the state of which would not be accepted
- -j DROP, drop all connections with an INVALID state