Question 1

5 out of 10 points

Create an ACL which blocks SSH from Kali but allows VNC.

Selected Answer: sudo iptables -A INPUT -p tcp --dport 22 -j DROP
sudo iptables -A INPUT -p tcp --dport 5900 -j ACCEPT

Correct Answer: **sudo iptables -A INPUT -s 10.0.2.15 -p tcp --dport 22 -j DROP**

Question 2

10 out of 10 points

Create 3 rules to allow ports for web services only.

Selected Answer: 1) sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT 2) sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT 3) sudo iptables -A INPUT -j DROP

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
Exact Match	sudo iptables -I INPUT -p tcp --dport 80 -m conntrack --ctstate NEW, ESTABLISHED -j ACCEPT	
Exact Match	sudo iptables-I INPUT -p tcp --dport 443 -m conntrack --ctstate NEW, ESTABLISHED -j ACCEPT	
Exact Match	sudo iptables -A INPUT -j DROP	

Question 3

10 out of 10 points

Create rules that will only allow VNC and FTP from Kali.

Selected Answer: sudo iptables -A INPUT -p tcp --dport 5900 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT
sudo iptables -A INPUT -j DROP

Correct Answer: **sudo iptables -I INPUT -s 10.0.2.15 -p tcp --dport 20 -j ACCEPT**
sudo iptables -I INPUT -s 10.0.2.15 -p tcp --dport 21 -j ACCEPT
sudo iptables -I INPUT -s 10.0.2.15 -p tcp --dport 5900 -j ACCEPT
sudo iptables -A INPUT -j DROP

Question 4

10 out of 10 points

Create an ACL which will block SMTP and allow everything else.

Selected Answer: sudo iptables -A INPUT -p tcp --dport 25 -j DROP
sudo iptables -A INPUT -j ACCEPT

Correct Answer: **sudo iptables -A INPUT -p tcp --dport 25 -j DROP**

Question 5

5 out of 10 points

Create rules to deny SSH and FTP from Kali.

Selected Answer: sudo iptables -A INPUT -p tcp --dport 22 -j DROP
sudo iptables -A INPUT -p tcp --dport 21 -j DROP

Correct Answer: sudo iptables -A INPUT -s 10.0.2.15 -p tcp --dport 20 -j DROP
sudo iptables -A INPUT -s 10.0.2.15 -p tcp --dport 21 -j DROP
sudo iptables -A INPUT -s 10.0.2.15 -p tcp --dport 22 -j DROP

Question 6

10 out of 10 points

Create a ACL to block SSH

Selected Answer: sudo iptables -A INPUT -p tcp --dport 22 -j DROP

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
Exact Match	sudo iptables -A INPUT -p tcp --dport 22 -j DROP	

Question 7

10 out of 10 points

Create 3 additional ACLs of your choosing. List them and explain what they would do.

Selected Answer:

1) sudo iptables -A INPUT -p tcp --dport 23 -j DROP

This first rule filters traffic to telnet.

2) sudo iptables -A INPUT -s 10.0.2.15 -p tcp --dport 512 -j ACCEPT

sudo iptables -A INPUT DROP

This rules says that traffic can only come from a specific source, using the -s command. In this case it's saying that only traffic from port 512 on the Kali machine. Traffic from everywhere else is dropped.

3) sudo iptables -A INPUT -p tcp --dport 2121 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 6000 -j DROP

This rules is allowing traffic to port 2121, but denying traffic to port 6000.

Correct Answer: [None]

Question 8

10 out of 10 points

What are some administrative issues with IPTables?

Selected Answer: There are many open ports and therefore a lot of parameters that a network admin needs to specify to teach a firewall what packets are acceptable and what packets could potentially be hostile. Another issue is that a network admin can only create one rule at a time and this can be time consuming.

Correct Answer: Some administrative issues with this include restrictive access to only the administrator and the root directory. People without authorization to the root user will not be able to access these tables if needed. The tool also only works on linux devices. If your network has machines that run on Windows or OSX, then iptables is not available to them.

Question 9

10 out of 10 points

How can this functionality be useful in a real-world setting?

Selected Answer: IPTable functionality is useful in a real world setting because network admins have the ability to establish access control parameters for their network to keep it secure and decrease the attack surface. Network admins can create rules that teach a firewall to recognize threats trying to access or leave a network.

Correct Answer: This functionality can be used in real world situations on Linux based systems. The flexibility allows administrators to curate the firewall to the system and to specific network traffic conditions. A network administrator can use this ACL to limit and filter the traffic that moves in and out of machines and networks. This can create isolation of machines to their function and not allow any unnecessary points of entry for attackers. It will also not allow machines to send out packets they should not be sending.

Question 10

10 out of 10 points

Why is having functionality like IPTables important?

Selected Answer: IPTables rely on rules, set by a network admin, that specify criteria a packet must meet to enter or leave a netowrk. It's important because the network admins can customize their network and maintain control over traffic. IPTables give network admins the ability to configure a firewall to decrease the attack surface of a network.

Correct Answer: The flexibility of the iptable command-line is important when setting rules for a firewall. Iptables allow for the management of network traffic. Iptables ensure that the firewall has customized requirements for both incoming and outgoing traffic and ensures that the system will not be vulnerable to an attack. Iptables have a set of rules that are compared against all packets that come through the network and will ensure that the network traffic is properly filtered.