Muhammad Izham Bin Norhamadi
B032020039

No: Date:

Question 1

Benefits of local AAA authetication
1) Fast establish connection with router
2) Authenticate user using username and password stored in local database

Benefits of server-based authentication
1) Secure establish connection with router
2) Authaticates Cisco Secure ACS

Question 2

1) RADIUS server authenticates user credentials and provide user's access privileges according to Active Directory server
2) Provide a central server that manages users and their privileges

Question 3

Standard	Extended
1) Filters packets based on layer 3 source information	1) Filters based on layer 3 and layer 4 source destination information
2) Permit or deny entire TCP/IP protocol suite	2) Specifies a specific IP protocol and port number

Muhammad Izham Bin Norhamadi
B022020039

No:

Date:

Question 4

i. A spoofing attack is when a malicious party impersonates another device or user on a network

ii. 1) All zeros addresses
2) Broadcast addresses
3) Local host address (127.0.0.0/8)
4) Reserved private addresses (RFC 1918)
5) IP multicast address range (224.0.0.0/4)

iii. 1) Local host address - 127.0.0.1
2) All zeros addresses - 0.0.0.0

iv. ACL can be used to drop packets from invalid addresses which come from address spoofing. For example an interface that receives a private address coming from public network will be dropped.

Muhammad Izham Bin Norhamadi
B032020039

No: Date:

Question 5

i. Extended ACL

ii. 1) Allow messages to travel to and from server 10.10.10.1
2) Log messages that travels from the internet to router

iii. On interface Serial 0/0/0 to filter traffic coming from internet to internal network containing server and workstation

Question 6

i.
```
access-list 101 permit tcp 10.0.1.0 0.0.0.255
 host 10.0.2.1 eq www
access-list 101 permit tcp 10.0.1.0 0.0.0.255
 host 10.0.3.1 eq www
access-list 101 deny icmp 10.0.1.0 0.0.0.255
 host 10.0.2.1
access-list 101 deny icmp 10.0.1.0 0.0.0.255
 host 10.0.3.1
```

ii. Apply ACL on interface Fa0/0 on R1

Muhammad Izham Bin Norhamadi

B032020039

No: Date:

Question 7

i. IDS advantages

1) No impact on network (latency, jitter)

2) No network impact if there is a sensor failure

IDS disadvantages

1) Response action cannot stop trigger packets

2) More vulnerable to network security evasion techniques

ii. IPS advantages

1) Stops trigger packets

2) Can use stream normalization techniques

IPS disadvantages

1) Sensor issue might affect network traffic

2) Sensor overloading impacts the network

iii. IPS

Justification:

- IPS provide active network security to protect network from malicious activities
- IPS can be used to monitor and give you deep understanding of how traffic moves across your network

Muhammad Izham Bin Norhamadi

B032020039

No: Date:

Question 8

- Despite implementing security tools in network, some actions must be taken to reduce vulnerabilities that can't be covered by security tools
- Steps must be taken to increase securities in the network that are not reachable by security tools

Question 9

i. ARP attack

ii. The attacker have access to the network and have scanned the IP addresses of two devices in the network such as a PC and a router

iii. The attacker uses spoofing tool to send out forged ARP responses that advertise the attacker's MAC address as the owner of both IP addresses. The two devices update their ARP cache entries to connect to attacker's machine instead of each other.

iv. 1) Use static ARP - define static ARP entry for an IP address to prevent devices from listening to ARP response
2) Use packet filtering - packet filtering solution can identify poisoned ARP by seeing conflicting source information and stop them before they reach devices.

STANDARD

Muhammad Ikhom Bin Norhamadi
B032020039

No: Date:

Question 10

i. Benefits of VPN

1) Secure connection - VPN provide security by using advanced encryption and authentication protocols to protect data from unauthoriced access

2) Cost savings - Organizations can use VPNs to reduce connectivity costs while increasing remote connection bandwidth

3) Remote access to internal network - VPN can give employees access to internal application or data in organization from their home network

ii. Risks of VPN

1) Security risk - If an attacker gain access to remote employee's VPN credentials, they can accees all data in internal network

2) VPN appliances are a single point of failure - If a VPN rendered inoperable by an attack, there will be risk of business interruption for organizations that support sizeable remote workforce

3) VPN provide little to no audit records - Any actions by third-party vendor VPN can't be monitored or recorded in case of a breach.

Muhammad Ichom Bin Norhamadi
B032020039

No:

Date:

Question 11

i. Remote access VPN

	Site-to-site VPN	Remote access VPN
Use case	Combines seperate office networks into a shared LAN ecosystem	Connects individual users to private internal networks
Setup	Must be set up on all premises. Each end devices automatically gains access to internal network with no additional configuration	Each client's device needs to have specific software or configuration to connect with HQ server. The HQ server must also accept incoming VPN traffic
Data flow	Data moves through the office's gateway and leaves fully encrypted	Each user creates their own VPN tunnel when connecting. Data leaving the device is encrypted
Users	Office employees connecting to other branch offices or headquarters	Employees working from home or other locations than the office or regular users