Exam Report: 5.9.4 Practice Questions

Date: 1/21/2020 10:58:28 am
Time Spent: 0:47

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 0%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

You have a company network with a single switch. All devices connect to the network through the switch.

You want to control which devices are able to connect to your network. For devices that do not have the latest operating system patches, you want to prevent access to all network devices except for a special server that holds the patches that the computers need to download.

Which of the following components will be part of your solution? (Select two.)

- [x] Remediation servers
- [ ] Extranet
- [x] 802.1x authentication
- [ ] Honeypot
- [ ] DMZ

Explanation

Network Access Control (NAC) controls access to the network by preventing computers from accessing network resources unless they meet certain predefined security requirements. NAC can be used with 802.1x port authentication on a switch to allow or deny access to the network through the switch port. A client that is determined by the NAC agent to be healthy is given access to the network. An unhealthy client that does not meet all the checklist requirements is either denied access or given restricted access to a remediation network, where remediation servers can be contacted to help the client to become compliant. For example, remediation servers might include anti-virus software and definition files that can be installed. If and when the unhealthy client's status changes to healthy, the client is given access to the network.

A *demilitarized zone* (DMZ) is a buffer network (or subnet) that sits between the private network and an untrusted network, such as the internet. DMZs are created with routers and firewall rules to allow or block traffic. DMZs use information in the packet to allow or deny packets.

An *extranet* is a privately-controlled network that distinct from the internet and a private LAN, but located between them. An extranet is often used to grant resource access to business partners, suppliers, and even customers outside of the organization. A *honeypot* is a device or virtual machine that entices intruders by displaying a vulnerable trait or flaw or by appearing to contain valuable data.

References

LabSim for Security Pro, Section 5.9.
[All Questions SecPro2017_v6.exm NETWORK_ACC_CTRL_01]

Question 2: Incorrect

Which step is required to configure a NAP on a Remote Desktop (RD) gateway server?

- ( ) Configure the enforcement point as a RADIUS client to the NAP server

- Edit the properties for the server and select **Request clients to send a statement of health**
- ~~Configure the server to issue a valid statement of health certificate~~
- On the 802.1x switch, define the Remote Desktop (RD) gateway server as a compliant network VLAN

Explanation

When implementing a NAP solution using Remote Desktop (RD) gateway server, you edit the properties to request that clients send a statement of health.

Configuring the enforcement point as a RADIUS client is required in an 802.1x implementation. 802.1x switches are also used in an 802.1x implementation. Certificates are used in an IPsec implementation of NAP. Statements of health are generated and submitted by the client.

References

LabSim for Security Pro, Section 5.9.
[All Questions SecPro2017_v6.exm NETWORK_ACC_CTRL_02]

Question 3: Incorrect

In a NAP system, what is the function of the System Health Validator?

- ~~Prevent users from disabling NAP on the client computer~~
- Generate a statement of health (SoH) that reports the client configuration for health requirements
- Compare the statement of health submitted by the client to the health requirements
- Provide the resources necessary to help non-compliant clients become compliant

Explanation

The System Health Validator (SHV) runs on the NAP server and identifies the client health requirements. The SHV compares the statement of health submitted by the client to the health requirements.

The client software generates the SoH. The Network Access Protection agent and the enforcement client prevent users from disabling NAP. Remediation servers provide the resources to help non-compliant clients become compliant.

References

LabSim for Security Pro, Section 5.9.
[All Questions SecPro2017_v6.exm NETWORK_ACC_CTRL_03]

Question 4: Incorrect

How does IPsec NAP enforcement differ from other NAP enforcement methods?

- DHCP options are used to deliver IP configuration values to non-compliant computers.
- ~~IP filters are defined in network access policies to limit resource access for non-compliant computers.~~
- Clients must be issued a valid certificate before a connection to the private network is allowed.
- A connection request policy is created on the NAP server that uses PEAP and enables quarantine checks.

Explanation

IPsec enforcement is the only NAP implementation method that requires certificates. Clients must be issued a valid certificate before a connection to the private network is allowed.

VPN enforcement uses IP filters defined in network access policies to limit resource access for non-compliant computers. With VPN enforcement, you can also create a connection request policy on the NAP server that uses PEAP and enables quarantine checks. DHCP enforcement uses DHCP options to deliver IP configuration values to non-compliant computers.

References

LabSim for Security Pro, Section 5.9.
[All Questions SecPro2017_v6.exm NETWORK_ACC_CTRL_04]

Question 5: Incorrect

Your organization's security policy requires you to restrict network access to allow only clients that have their firewall enabled.

Which of the following is a collection of components that would allow you to meet this requirement?

- IPsec enforcement
- 802.1x authentication
- Network access protection
- ~~System health validator~~

Explanation

Network Access Protection (NAP) is a collection of components that allow administrators to regulate network access or communication based on a computer's compliance with health requirement policies. For example, you can allow network access only to clients that have anti-virus software, that have the firewall enabled, or that have the latest patches installed. NAP can also ensure ongoing compliance by requiring that a computer maintain adherence to health requirements.

The system health validator, 802.1x authentication, and IPsec enforcement are just a few of the components in the collection that make up NAP.

References

LabSim for Security Pro, Section 5.9.
[All Questions SecPro2017_v6.exm NETWORK_ACC_CTRL_05]