[Updated Constantly]

HERE

CCNA Cyber Ops (Version 1.1) – Chapter 10 Exam Answers Full

1. Which HIDS is an open source product?

- Tripwire
- **OSSEC ***
- Cisco AMP
- AlienVault USM

B. The Open Source HIDS SECurity (OSSEC) software is an open source HIDS that uses a central manager server and agents that are installed on the hosts that are to be monitored.

2. In Windows Firewall, when is the Domain profile applied?

- When the host accesses the Internet
- When the host checks emails from an enterprise email server
- **When the host is connected to a trusted network such as an internal business network ***
- When the host is connected to an isolated network from the Internet by another security device

C. The Domain profile in Windows Firewall configuration is for connections to a trusted network, such as a business network, that is assumed to have an adequate security infrastructure.

3. Which function does CVSS provide?

- **Risk assessment ***
- Penetration testing
- Vulnerability assessment
- Central security management service

A. The Common Vulnerability Scoring System (CVSS) is a risk assessment tool to convey the common attributes and severity of vulnerabilities in computer hardware and software systems.

4. In addressing an identified risk, which strategy aims to decrease the risk by taking measures to reduce vulnerability?

- Risk sharing
- Risk retention
- **Risk reduction ***
- Risk avoidance

C. There are four potential strategies for responding to risks that have been identified:
Risk avoidance: Stop performing the activities that create risk.
Risk reduction: Decrease the risk by taking measures to reduce vulnerability.
Risk sharing: Shift some of the risk to other parties.
Risk retention: Accept the risk and its consequences.

5. Which regulatory compliance regulation specifies security standards for U.S.government systems and contractors to the U.S. government?

- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act of 2002 (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- **Federal Information Security Management Act of 2002 (FISMA) ***

D. The major regulatory compliance options include:
Federal Information Security Management Act of 2002 (FISMA):
Specifies security standards for U.S. government systems and contractors to the U.S. government.
Sarbanes-Oxley Act of 2002 (SOX): Sets new or expanded requirements for all U.S. public company boards, management, and public accountingfirms regarding the way in which corporations control and disclose financial information.
Gramm-Leach-Bliley Act (GLBA): Established that financial institutions must ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.
Health Insurance Portability and Accountability Act (HIPAA):
Requires that all patient personally identifiable healthcare information be stored, maintained, and transmitted in ways that ensure patient privacy and confidentiality.

6. Which three devices are possible examples of network endpoints? (Choose three.)

- Router
- **Sensor ***
- Wireless AP
- **IoT controller ***
- VPN appliance
- **Network security camera ***

B, D, F. IoT components, such as sensors, controllers, and network security cameras, are network endpoints when they are connected to a network. Routers, VPN appliances, and wireless access points are examples of intermediate devices.

7. Which antimalware software approach can recognize various characteristics of known malware files to detect a threat?

- Routing-based
- Behavior-based
- **Signature-based ***
- Heuristics-based

C. Antimalware programs may detect viruses using three different approaches:
Signature-based, by recognizing various characteristics of known malware files
Heuristics-based, by recognizing general features shared by various types of malware
Behavior-based, through analysis of suspicious activities

8. As described by the SANS Institute, which attack surface includes the exploitation of vulnerabilities in wired and wireless protocols used by IoT devices?

- Human Attack Surface
- Internet Attack Surface
- **Network Attack Surface ***

- Software Attack Surface

C. The SANS Institute describes three components of the attack surface:
Network Attack Surface: Exploitation of vulnerabilities in networks
Software Attack Surface: Exploitation of vulnerabilities in web, cloud, or host-based software applications
Human Attack Surface: Exploitation of weaknesses in user behavior

9. In profiling a server, what defines what an application is allowed to do or run on a server?

- User accounts
- Listening ports
- **Service accounts ***
- Software environment

C. The service accounts element of a server profile defines the type of service that an application is allowed to run on a given host.

10. Which class of metric in the CVSS Basic metric group defines the features ofthe exploit such as the vector, complexity, and user interaction required by the exploit?

- Impact
- **Exploitability ***
- Modified Base
- Exploit Code Maturity

B. The Base metric group of CVSS represents the characteristics of a vulnerability that are constant over time and across contexts. It contains two classes of metrics:
Exploitability metrics: Features of the exploit such as the vector,complexity, and user interaction required by the exploit
Impact metrics: The impacts of the exploit rooted in the CIA triad of confidentiality, integrity, and availability

11. Which step in the Vulnerability Management Life Cycle performs inventory of all assets across the network and identifies host details, including operating system and open services?

- Assess
- **Discover ***
- Remediate
- Prioritize assets

B. The steps in the Vulnerability Management Life Cycle include these:
Discover: Inventory all assets across the network and identify host details, including operating systems and open services to identify vulnerabilities.
Prioritize assets: Categorize assets into groups or business units, and assign a business value to asset groups based on their criticality to business operations.
Assess: Determine a baseline risk profile to eliminate risks based on asset criticality, vulnerability threats, and asset classification.
Report: Measure the level of business risk associated with your assets according to your security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.
Remediate: Prioritize according to business risk and fix vulnerabilities in order of risk.
Verify: Verify that threats have been eliminated through follow-up audits.

12. In network security assessments, which type of test is used to evaluate the risk posed by vulnerabilities to a specific organization, including assessment of the likelihood of attacks and the impact of successful exploits on the organization?

- **Risk analysis ***
- Port scanning
- Penetration testing
- Vulnerability assessment

A. A risk analysis includes assessment of the likelihood of attacks, identifies types of likely threat actors, and evaluates the impact of successful exploits on the organization.

13. In most host-based security suites, which function provides robust logging of security-related events and sends logs to a central location?

- intrusion detection and prevention
- anti-phishing
- **telemetry**
- safe browsing

The telemetry functionality in most host-based security suites provides robust logging functionality and submits logs to a central location for analysis.

14. On a Windows host, which tool can be used to create and maintain blacklists and whitelists?

- **Group Policy Editor**
- Local Users and Groups
- Computer Management
- Task Manager

In Windows, blacklisting and whitelisting settings can be managed through the Group Policy Editor.

15. Which statement describes agentless antivirus protection?

- Host-based antivirus systems provide agentless antivirus protection.
- The antivirus protection is provided by the router that is connected to a cloud service.
- The antivirus protection is provided by the ISP.
- **Antivirus scans are performed on hosts from a centralized system.**

Host-based antivirus protection is also known as agent-based. Agent-based antivirus runs on every protected machine. Agentless antivirus protection performs scans on hosts from a centralized system.

16. In network security assessments, which type of test employs software to scan internal networks and Internet facing servers for various types of vulnerabilities?

- risk analysis
- penetration testing
- **vulnerability assessment**
- strength of network security testing

In vulnerability assessment, security analysts use software to scan internal networks and Internet facing servers for various types of vulnerabilities. Tools for vulnerability assessment include the open source OpenVAS platform, Microsoft Baseline Security Analyzer, Nessus, Qualys, and Fireeye Mandiant services.

17. The IT security personnel of an organization notice that the web server deployed in the DMZ is frequently targeted by threat actors. The decision is made to implement a patch management system to manage the server. Which risk management strategy method is being used to respond to the identified risk?

- risk avoidance
- risk retention
- **risk reduction**
- risk sharing

There are four potential strategies for responding to risks that have been identified:

- Risk avoidance – Stop performing the activities that create risk.
- Risk reduction – Decrease the risk by taking measures to reduce vulnerability.
- Risk sharing – Shift some of the risk to other parties.
- Risk retention – Accept the risk and its consequences.

18. In addressing a risk that has low potential impact and relatively high cost of mitigation or reduction, which strategy will accept the risk and its consequences?

- risk reduction
- risk avoidance
- **risk retention**
- risk sharing

There are four potential strategies for responding to risks that have been identified:

- Risk avoidance – Stop performing the activities that create risk.
- Risk reduction – Decrease the risk by taking measures to reduce vulnerability.
- Risk sharing – Shift some of the risk to other parties.
- Risk retention – Accept the risk and its consequences.

19. What is a host-based intrusion detection system (HIDS)?

- It identifies potential attacks and sends alerts but does not stop the traffic.
- It detects and stops potential direct attacks but does not scan for malware.
- It is an agentless system that scans files on a host for potential malware.
- **It combines the functionalities of antimalware applications with firewall protection.**

A current HIDS is a comprehensive security application that combines the functionalities of antimalware applications with firewall protection. An HIDS not only detects malware but also prevents it from executing. Because the HIDS runs directly on the host, it is considered an agent-based system.

20. What type of antimalware program is able to detect viruses by recognizing various characteristics of a known malware file?

- behavior-based
- agent-based
- **signature-based**
- heuristic-based

Using a signature-based approach, host security software can detect viruses and malware by recognizing various characteristics of known malware files.

21. Which device in a LAN infrastructure is susceptible to MAC address-table overflow and spoofing attacks?

- firewall

- workstation
- server
- **switch**

Switches are LAN infrastructure devices interconnecting endpoints. They are susceptible to LAN-related attacks including MAC address-table overflow attacks, spoofing attacks, LAN storm attacks, STP manipulation attacks, and VLAN attacks.

22. Which criterion in the Base Metric Group Exploitability metrics reflects the proximity of the threat actor to the vulnerable component?

- user interaction
- **attack vector**
- attack complexity
- privileges required

The Base Metric Group Exploitability metrics include the criteria:

- Attack vector – a metric that reflects the proximity of the threat actor to the vulnerable component
- Attack complexity – a metric that expresses the number of components, software, hardware, or networks, that are beyond control of the attacker and that must be present in order for a vulnerability to be successfully exploited
- Privileges required – a metric that captures the level of access that is required for a successful exploit of the vulnerability
- User interaction – second component of the attack complexity metric that expresses the presence or absence of the requirement for user interaction in order for an exploit to be successful
- Scope – a metric that expresses whether multiple authorities must be involved in an exploit

23. In addressing an identified risk, which strategy aims to stop performing the activities that create risk?

- risk reduction
- **risk avoidance**
- risk retention
- risk sharing

There are four potential strategies for responding to risks that have been identified:

- Risk avoidance – Stop performing the activities that create risk.
- Risk reduction – Decrease the risk by taking measures to reduce vulnerability.
- Risk sharing – Shift some of the risk to other parties.
- Risk retention – Accept the risk and its consequences.

24. Which statement describes the term iptables?

- It is a file used by a DHCP server to store current active IP addresses.
- It is a DHCP application in Windows.
- It is a DNS daemon in Linux.
- **It is a rule-based firewall application in Linux.**

Iptables is an application that allows Linux system administrators to configure network access rules.

25. For network systems, which management system addresses the inventory and control of hardware and software configurations?

- asset management
- vulnerability management
- risk management
- **configuration management**

Configuration management addresses the inventory and control of hardware and software configurations of network systems.

26. Which statement describes the anomaly-based intrusion detection approach?

- It compares the signatures of incoming traffic to a known intrusion database.
- It compares the antivirus definition file to a cloud based repository for latest updates.
- It compares the operations of a host against a well-defined security policy.
- **It compares the behavior of a host to an established baseline to identify potential intrusions.**

With an anomaly-based intrusion detection approach, a baseline of host behaviors is established first. The host behavior is checked against the baseline to detect significant deviations, which might indicate potential intrusions.

27. What is the first step taken in risk assessment?

- **Identify threats and vulnerabilities and the matching of threats with vulnerabilities.**
- Establish a baseline to indicate risk before security controls are implemented.
- Compare to any ongoing risk assessment as a means of evaluating risk management effectiveness.
- Perform audits to verify threats are eliminated.

The three steps of risk assessment in order are as follows:

1. Identify threats and vulnerabilities and the matching of threats with vulnerabilities.
2. Establish a baseline to indicate risk before security controls are implemented.
3. Compare to an ongoing risk assessment as a means of evaluating risk management effectiveness.

28. Which statement describes the threat-vulnerability (T-V) pairing?

- **It is the identification of threats and vulnerabilities and the matching of threats with vulnerabilities.**
- It is the comparison between known malware and system risks.
- It is the detection of malware against a central vulnerability research center.
- It is the advisory notice from a vulnerability research center.

A mandatory activity in risk assessment is the identification of threats and vulnerabilities and the matching of threats with vulnerabilities, also called threat-vulnerability (T-V) pairing.

29. Which security procedure would be used on a Windows workstation to prevent access to a specific set of websites?

- whitelisting
- HIDS
- **blacklisting**
- baselining

Blacklists can be used to identify and prevent specific applications, websites, or services from being downloaded or executed within an enterprise network.

30. Which statement describes the use of a Network Admission Control (NAC) solution?

- **It provides network access to only authorized and compliant systems.**
- A Network Admission Control solution provides filtering of potentially malicious emails before they reach the endpoint.
- It provides endpoint protection from viruses and malware.
- It provides filtering and blacklisting of websites being accessed by end users.

Network Admission Control (NAC) allows only authorized and compliant systems to connect to a network.

31. Which statement describes the Cisco Threat Grid Glovebox?

- It is a network-based IDS/IPS.
- It is a firewall appliance.
- It is a host-based intrusion detection system (HIDS) solution to fight against malware
- **It is a sandbox product for analyzing malware behaviors.**

Cisco ThreatGrid Glovebox is a sandbox product for analyzing malware behaviors.

32. Which type of antimalware software detects and mitigates malware by analyzing suspicious activities?

- heuristics-based
- packet-based
- **behavior-based**
- signature-based

Antimalware programs may detect viruses using three different approaches:

- signature-based – by recognizing various characteristics of known malware files
- heuristics-based – by recognizing general features shared by various types of malware
- behavior-based – through analysis of suspicious activities

33. Which regulatory compliance regulation sets requirements for all U.S. public company boards, management and public accounting firms regarding the way in which corporations control and disclose financial information?

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act of 2002 (FISMA)
- **Sarbanes-Oxley Act of 2002 (SOX)**

There are five major regulatory compliance regulations including:

- Federal Information Security Management Act of 2002 (FISMA) – specifies security standards for U.S. government systems and contractors to the U.S. government.
- Sarbanes-Oxley Act of 2002 (SOX) – sets new or expanded requirements for all U.S. public company boards, management and public accounting firms regarding the way in which corporations control and disclose financial information.
- Gramm-Leach-Bliley Act (GLBA) – established that financial institutions must ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.
- Health Insurance Portability and Accountability Act (HIPAA) – requires that all patient personally identifiable healthcare information be stored, maintained, and transmitted in ways that ensure patient privacy and confidentiality.

34. Which statement describes the term attack surface?

- **It is the total sum of vulnerabilities in a system that is accessible to an attacker.**
- It is the group of hosts that experiences the same attack.
- It is the network interface where attacks originate.
- It is the total number of attacks toward an organization within a day.

An attack surface is the total sum of the vulnerabilities in a system that is accessible to an attacker. The attack surface can consist of open ports on servers or hosts, software that runs on Internet-facing servers, wireless network protocols, and even users.

35. Which step in the Vulnerability Management Life Cycle determines a baseline risk profile to eliminate risks based on asset criticality, vulnerability threat, and asset classification?

- **assess**
- discover
- verify
- prioritize assets

The steps in the Vulnerability Management Life Cycle include these:Discover – inventory all assets across the network and identify host details, including operating systems and open services, to identify vulnerabilities
Prioritize assets – categorize assets into groups or business units, and assign a business value to asset groups based on their criticality to business operations
Assess – determine a baseline risk profile to eliminate risks based on asset criticality, vulnerability threats, and asset classification
Report – measure the level of business risk associated with assets according to security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.
Remediate – prioritize according to business risk and fix vulnerabilities in order of risk
Verify – verify that threats have been eliminated through follow-up audits

36. When a network baseline is being established for an organization, which network profile element indicates the time between the establishment of a data flow and its termination?

- **session duration**
- critical asset address space
- ports used
- total throughput

Important elements of a network profile include:

- Total throughput – the amount of data passing from a given source to a given destination in a given period of time
- Session duration – the time between the establishment of a data flow and its termination
- Ports used – a list of TCP or UDP processes that are available to accept data
- Critical asset address space – the IP addresses or the logical location of essential systems or data

37. Which two classes of metrics are included in the CVSS Base Metric Group? (Choose two.)

- Modified Base
- Confidentiality Requirement
- Exploit Code Maturity
- **Exploitability**

- **Impact metrics**

The Base Metric Group of CVSS represents the characteristics of a vulnerability that are constant over time and across contexts. It contains two classes of metrics, Exploitability and Impact.

38. Which two criteria in the Base Metric Group Exploitability metrics are associated with the complexity of attacks? (Choose two)

- scope
- **attack complexity**
- **user interaction**
- attack vector
- privileges required

The Base Metric Group Exploitability metrics include these criteria:

- Attack vector – a metric that reflects the proximity of the threat actor to the vulnerable component
- Attack complexity – a metric that expresses the number of components, software, hardware, or networks, that are beyond control of the attacker and that must be present in order for a vulnerability to be successfully exploited
- Privileges required – a metric that captures the level of access that is required for a successful exploit of the vulnerability
- User interaction – second component of the attack complexity metric that expresses the presence or absence of the requirement for user interaction in order for an exploit to be successful
- Scope – a metric that expresses whether multiple authorities must be involved in an exploit

39. Use the following scenario to answer the questions. An entrepreneur is starting a small business and is considering the server services needed for the startup company. The company handling the IT service is presenting options to the company.
a) If the entrepreneur decides to go with Linux server, how are services handled differently from how Windows server services would be handled?

- **The services are managed using configuration files. ***
- Services can only be managed from the Administrator account.
- Services use only TCP port numbers because they are more secure.
- The PowerShell environment can be used to make configuration changes.

Explanation:
Linux server services are managed using configuration files that contain specific information about the service including port number, location of the hosted resources, and client authorization details.

b) The company will be using both Linux- and Windows-based hosts. Which two solutions would be used in a distributed firewall network design? (Choose two.)

- **iptables ***
- SIEM
- Snort
- **Windows Firewall ***
- Wireshark

Explanation:
A network design that uses distributed firewalls centrally manages security rules and pushes those rules to the Linux and Windows host machines. Windows-based hosts use the Windows Firewall, whereas the Linux-based hosts use a firewall application such as iptables or nftables. Snort is an open source network intrusion prevention software. Wireshark is a packet capture tool and Security information and event management (SIEM) provides real-time analysis of alerts and log entries generated by network appliances such as IDSs and firewalls.

c)Which protocol should be recommended to the company to monitor and manage network performance?

- NTP
- PAT
- **SNMP ***
- SSH

Explanation:
The Simple Network Management Protocol (SNMP) is an application layer protocol used to monitor and manage the network. Network devices have SNMP agents that communicate with the SNMP manager where the SNMP management software runs.

d)The IT company is recommending the use of PKI applications. In which two instances might the entrepreneur make use of PKIs? (Choose two.)

- **802.1x authentication ***
- FTP transfers
- **HTTPS web service ***
- local NTP server
- file and directory access permission

Explanation: The Public Key Infrastructure (PKI) is a third party-system referred to as a certificate authority or CA. The PKI is the framework used to securely exchange information between parties. Common PKI applications are as follows:

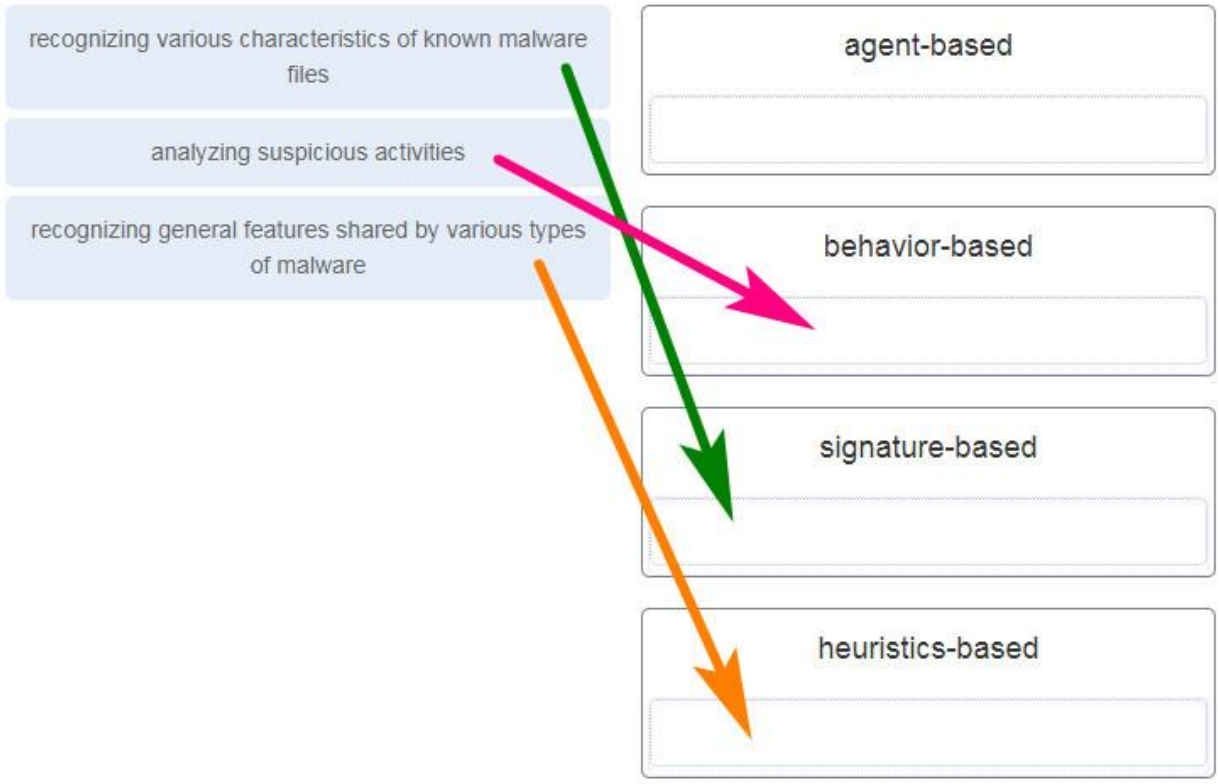
- SSL/TLS certificate-based peer authentication
- IPsec VPNs
- HTTPS web traffic
- network access control using 802.1x authentication
- secure email using S/MIME
- secure instant messaging
- approve and authorize applications with Code signing
- protect data with EFS
- use two-factor authentication
- secure USB storage devices

e)The entrepreneur is concerned about company employees having uninterrupted access to important resources and data. Which of the CIA triad components would address the concern?

- authentication
- **availability ***
- confidentiality

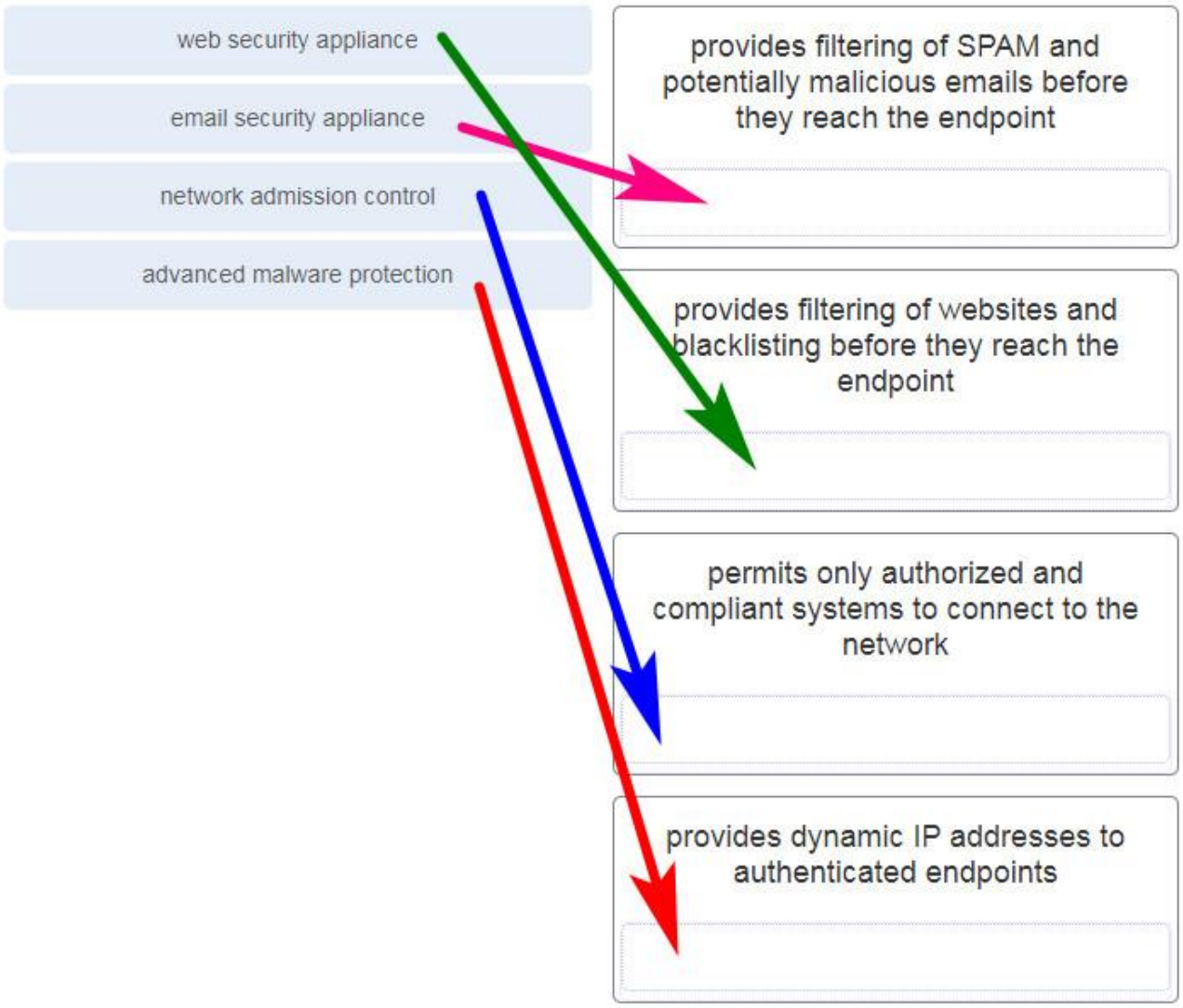
- integrity

38. Match the description to the antimalware approach. (Not all options are used.)



Antimalware programs may detect viruses using three different approaches:
signature-based – by recognizing various characteristics of known malware files
heuristics-based – by recognizing general features shared by various types of malware
behavior-based – through analysis of suspicious activities

39. Match the network-based antimalware solution to the function. (Not all options are used.)



Match the network-based antimalware solution to the function

web security appliance –> provides filtering of websites and blacklisting before they reach the endpoint
email security appliance –> provides filtering of SPAM and potentially malicious emails before they reach the endpoint
network admission control –> permits only authorized and compliant systems to connect to the network
advanced malware protection –> provides dynamic IP addresses to authenticated endpoints