Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/12/2022 9:05:08 pm • Time spent: 04:00

Score: 70%

Passing Score: 80%

Question 1: ✓ Correct

A security administrator logs onto a Windows server on her organization's network. Then she runs a vulnerability scan on that server.

Which type of scan was conducted in this scenario?

○ Intrusive scan

➡ ● Credentialed scan

○ Non-intrusive scan

○ Non-credentialed scan

EXPLANATION

In a credentialed scan, the security administrator authenticates to the system prior to starting the scan. A credentialed scan usually provides detailed information about potential vulnerabilities. For example, a credentialed scan of a Windows workstation allows you to probe the registry for security vulnerabilities.

With a non-credentialed scan, the security administrator does not authenticate to the system prior to running the scan.

An intrusive scan finds a potential vulnerability and then actively attempts to exploit it.

A non-intrusive scan is the more common type of scan performed.

REFERENCES

11.4.2 Vulnerability Assessment Facts

q_vuln_assess_cred_secp7.question.fex

Question 2: ✓ Correct

In your role as a security analyst, you ran a vulnerability scan, and several vulnerabilities were reported. Upon further inspection, none of the vulnerabilities actually existed.

Which type of result is this?

○ True positive

○ False negative

➡ ● False positive

○ True negative

EXPLANATION

False positives occur when a scan says there is a vulnerability, but there is none. They happen as a matter of course and should be discovered during the follow-up to the scan.

False negatives occur when the scanner misses a vulnerability.

True negatives occur when the scanner says there are no vulnerabilities and there are none.

True positives occur when the scanner shows a vulnerability that does exist.

REFERENCES

11.4.2 Vulnerability Assessment Facts

q_vuln_assess_false_secp7.question.fex

▼ **Question 3:** ✓ Correct

A security administrator needs to run a vulnerability scan that analyzes a system from the perspective of a hacker attacking the organization from the outside.

Which type of scan should he or she use?

○ Credentialed scan

○ Port scan

➡ ● Non-credentialed scan

○ Network-mapping scan

EXPLANATION

In a non-credentialed scan, the security administrator does not authenticate to the system prior to running the scan. A non-credentialed scan can be valuable because it allows the scanner to see the system from the same perspective that an attacker would see it. However, a non-credentialed scan does not typically produce the same level of detail as a credentialed scan.

In a credentialed scan, the security administrator authenticates to the system prior to starting the scan.

A port scan probes systems for open ports, but it does not run a full vulnerability assessment.

A network-mapping scan is a type of port scan that discovers devices on the network and then organizes those devices in a graphical display.

REFERENCES

11.4.2 Vulnerability Assessment Facts

q_vuln_assess_non_cred_secp7.question.fex

Question 4: ✓ Correct

In your role as a security analyst, you need to stay up to date on the latest threats. You are currently reviewing the latest real-time updates on cyberthreats from across the world.

Which of the following resources are you MOST likely using?

➡ ● Threat feeds

○ Intelligence fusion

○ Advisories and bulletins

○ Threat hunting

EXPLANATION

Threat feeds provide real-time updates on cyberthreats across the world. They can provide information such as suspicious domains, known malware, known malicious IP addresses, and more. The **tracert** command shows the path a packet takes to reach its destination. This is not the best tool to check for connectivity between two network devices.

Advisories and bulletins are usually updated weekly and provide much more detailed information on the newest threats.

Intelligence fusion is the sharing of information between multiple government agencies and private security firms.

Threat hunting is the human-based, proactive and methodical monitoring of a network, systems, and software. This is done in order to detect any suspicious activity that may have evaded the automated tools.

REFERENCES

11.4.2 Vulnerability Assessment Facts

q_vuln_assess_threat_secp7.question.fex

Question 5: ✕ Incorrect

You want to be able to identify the services running on a set of servers on your network. Which tool would BEST give you the information you need?

- ➡ ○ Vulnerability scanner
- ○ Network mapper
- ○ Protocol analyzer
- ● ~~Port scanner~~

EXPLANATION

Use a vulnerability scanner to gather information about systems such as the applications or services running on a system. A vulnerability scanner often combines functions found in other tools and can perform additional functions, such as identifying open firewall ports, missing patches, and default or blank passwords.

A port scanner is a tool that probes systems for open ports. A port scanner tells you which ports are opened in the firewall, but it cannot identify services running on a server if the firewall port has been closed. A network mapper is a tool that can discover devices on a network and shows those devices in a graphical representation. Network mappers typically use a ping scan to discover devices and a port scanner to identify open ports on those devices.

Use a protocol analyzer to identify traffic that is sent on the network medium and traffic sources. Services could still be running on a server that do not generate network traffic that a protocol analyzer would catch.

REFERENCES

11.4.2 Vulnerability Assessment Facts

q_vuln_assess_vuln_01_secp7.question.fex

▼ **Question 6:** ✓ Correct

You have run a vulnerability scanning tool and identified several patches that need to be applied to a system. What should you do next after applying the patches?

○ Document your actions.

○ Update the vulnerability scanner definition files.

○ Use a port scanner to check for open ports.

➡ ● Run the vulnerability assessment again.

EXPLANATION

After fixing an identified vulnerability, you should re-run the vulnerability scan to verify that everything has been fixed and that additional issues are not present.

You should update definition files before you run the first scan. Using a port scanner is unnecessary because most vulnerability scanners include a check of open ports. Documenting your actions should occur after you have finished all necessary actions.

REFERENCES

11.4.2 Vulnerability Assessment Facts

q_vuln_assess_vuln_02_secp7.question.fex

Question 7: ✓ Correct

Which SIEM component is responsible for gathering all event logs from configured devices and securely sending them to the SIEM system?

○ Security automation

➡ ● Collectors

○ SIEM alerts

○ Data handling

EXPLANATION

Collectors are responsible for gathering all event logs from configured devices and securely sending them to the Security Information and Event Management (SIEM) system. Collectors are basically the middleman between devices and the SIEM system.

The data handling component receives the data from the collectors and then reads, analyzes, and separates the data into different categories.

SIEM alerts are responsible for triggering alerts if any data exceeds the established thresholds.

Security automation is a feature of a SOAR system.

REFERENCES

11.4.4 SIEM and SOAR Facts

q_siem_soar_collector_secp7.question.fex

Question 8: ✕ Incorrect

Which of the following Security Orchestration, Automation, and Response (SOAR) system automation components is often used to document the processes and procedures that are to be used by a human during a manual intervention?

- ● ~~Runbook~~
- ➡ ○ Playbook
- ○ Response
- ○ Orchestration

EXPLANATION

Playbooks are linear checklists of required steps and actions that are to be taken to respond to an alert. While playbooks do support automated actions, they are often used to document the processes and procedures that are to be used by a human during a manual intervention.

Runbooks consist of a series of conditional steps to perform actions, such as sending notifications or threat containment. They are not used to document the processes and procedures that are to be used by a human during a manual intervention.

The Orchestration component of the Security Orchestration, Automation, and Response (SOAR) system is responsible for gathering data and information from across the network. This is not used to document the processes and procedures that are to be used by a human during a manual intervention.

The Response component of a SOAR system allows the system to automatically take actions against threats. It is not used to document the processes and procedures used by a human during a manual intervention.

REFERENCES

11.4.4 SIEM and SOAR Facts

q_siem_soar_playbook_secp7.question.fex

▼ Question 9: ✕ Incorrect

You want to make sure that a set of servers only accepts traffic for specific network services. You have verified that the servers are only running the necessary services, but you also want to make sure that the servers do not accept packets sent to those services.

Which tool should you use?

➡ ○ Port scanner

● ~~IPS~~

○ IDS

○ Packet sniffer

○ System logs

EXPLANATION

Use a port scanner to check for open ports on a system or firewall. Compare the list of open ports with the list of ports allowed by your network design and security policy. Typically, a port is open when a service starts or is configured on a device. Open ports for unused services expose the server to attacks directed at that port.

Use a packet sniffer to examine packets on a network. With a packet sniffer, you can identify packets directed toward specific ports, but you won't be able to tell if those ports are open. Examine system logs to look for events that have happened on a system. These events might include a service starting up, but this would not likely reflect open ports.

An intrusion detection system (IDS) is a special network device that can detect attacks and suspicious activity. A passive IDS monitors, logs, and detects security breaches, but it takes no action to stop or prevent an attack. An active IDS (also called an intrusion protection system, or IPS) performs the functions of an IDS but can also react when security breaches occur.

REFERENCES

11.4.4 SIEM and SOAR Facts

q_siem_soar_port_secp7.question.fex

Question 10: ✓ Correct

Which of the following systems is able to respond to low-level security events without human assistance?

○ SIEM

○ IDS

○ Firewall

➡ ● SOAR

EXPLANATION

Security Orchestration, Automation, and Response (SOAR) systems gather and analyze data like SIEM systems, but they take the analysis to the next level. SOAR is a solution stack of compatible software programs that allow an organization to collect data about security threats from multiple sources and respond to low-level security events without human assistance.

Security Information and Event Management (SIEM) tools work by gathering different types of network information and data. This information is moved to one central place. SIEM systems are great tools that help network administrators filter data and improve security monitoring. Still, all alerts require manual intervention.

Intrusion detection systems (IDSs) can trigger alerts, but these systems do not respond to security threats on their own.

A firewall blocks traffic based on the configuration setup. However, firewalls do not respond to security threats on their own.

REFERENCES

11.4.3 SIEM and SOAR

11.4.4 SIEM and SOAR Facts

q_siem_soar_soar_secp7.question.fex