

Exam Report: 9.2.9 Practice Questions

Date: 5/5/2020 10:57:44 am
Time Spent: 0:32

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 40%



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1:

Incorrect

Daphne has determined that she has malware on her Linux machine. She prefers to only use open-source software. Which anti-malware software should she use?

- ☐ Bitdefender
- ➡ ☐ ClamAV
- ☐ Avira
- ☐ Kaspersky

Explanation

ClamAV is an open-source anti-malware program that works with most versions of Linux.

Kaspersky, Avira, and Bitdefender are popular anti-malware programs, but are not open-source.

References

TestOut Ethical Hacker Pro - 9.2 Combat Malware

[e_combat_malware_eh1.exam.xml Q_ANTI_MALWARE_ANTI_MAL_SOFTWARE_01_EH1]

▼ Question 2:

Correct

Anti-malware software utilizes different methods to detect malware. One of these methods is scanning. Which of the following best describes scanning?

- ☐ Scanning is when the anti-malware software opens a virtual environment to mimic CPU and RAM activity. Malware code is executed in this environment instead of the physical processor.
- ➡ ☒ Scanning uses live system monitoring to detect malware immediately. This technique utilizes a database that needs to be updated regularly. Scanning is the quickest way to catch malware programs.
- ☐ Scanning aids in detecting new or unknown malware that is based on another known malware. Every malware has a fingerprint, or signature. If a piece of code contains similar code, the scan should mark it as malware and alert the user.
- ☐ Scanning establishes a baseline and keeps an eye on any system changes that shouldn't happen. The program will alert the user that there is possible malware on the system.

Explanation

Scanning uses live system monitoring to detect malware immediately. This technique utilizes a database that needs to be updated regularly. Scanning is the quickest way to catch malware programs. If the database is not updated, the scanner won't be able to detect new malware threats.

Integrity checkers establish a baseline and keeps an eye on any system changes that shouldn't happen. The program will alert the user that there is possible malware on the system.

Code emulation is when the anti-malware software opens a virtual environment to mimic CPU and RAM activity. Malware code is executed in this environment instead of the physical processor.

Heuristic analysis aids in detecting new or unknown malware that is based on another known malware. Every malware has a fingerprint, or signature. If a piece of code contains similar code, the scan should mark it as malware and alert the user.


References

TestOut Ethical Hacker Pro - 9.2 Combat Malware

[e_combat_malware_eh1.exam.xml] Q_ANTI_MALWARE_MAL_DET_METHOD_01_EH1]

▼ Question 3: Incorrect

Which of the following is the first step you should take if malware is found on a system?

- ☐ Check for suspicious or unknown registry entries.
-  ☐ Isolate the system from the network immediately.
- ☐ Sanitize the system using updated anti-malware software.
- ☒ ~~Look through the event log for suspicious events.~~

Explanation

If malware is found on a system, you should:

1. Isolate the system from the network immediately.
2. Verify that the anti-malware software is updated and running. If its not, update it and scan the system.
3. Sanitize the system using updated anti-malware software and appropriate techniques.

Part of a penetration test is checking for malware vulnerabilities. When performing a penetration test, the penetration tester follows a set of steps:

1. Scan for open ports.
2. Scan for running processes.
3. Check for suspicious or unknown registry entries.
4. Verify all running Windows services.
5. Check startup programs.
6. Look through event log for suspicious events.
7. Verify all installed programs.
8. Scan files and folders for manipulation.
9. Verify device drivers are legitimate.
10. Check all network and DNS settings and activity.
11. Scan for suspicious API
12. Run anti-malware scans.


References

TestOut Ethical Hacker Pro - 9.2 Combat Malware

[e_combat_malware_eh1.exam.xml] Q_ANTI_MALWARE_MAL_DET_METHOD_02_EH1]

▼ Question 4: Incorrect

Daphne suspects a Trojan horse is installed on her system. She wants to check all active network connections to see which programs are making connections and the FQDN of where those programs are connecting to. Which command will allow her to do this?

- ☒ ~~netstat -a -b~~
- ☐ netstat -f -a
- ☐ netstat -f -a -b
-  ☐ netstat -f -b

Explanation

netstat -f -b shows the fully qualified domain name (FQDN) and the name of programs that are making connections.

netstat -a -b shows the open ports on the local system and the names of programs that are making connections.

netstat -f -a shows the fully qualified domain name and the open ports on the local system.

netstat -f -a -b shows the fully qualified domain name, the open ports on the local system, and the names of programs that are making connections.


References

TestOut Ethical Hacker Pro - 9.2 Combat Malware

[e_combat_malware_eh1.exam.xml Q_ANTI_MALWARE_OPEN_PORT_NETSTAT_01_EH1]

▼ Question 5: Correct

Part of a penetration test is checking for malware vulnerabilities. During this process, the penetration tester will need to manually check many different areas of the system. After these checks have been completed, which of the following is the next step?

- ☐ Document all findings
-  ☒ Run anti-malware scans
- ☐ Isolate system from network
- ☐ Sanitize the system

Explanation

After the penetration tester has run system scans and checked different areas of the system, anti-malware scans should be run. Before running these scans, make sure the software is updated.

After the anti-malware scans have been performed, the pentester needs to document all findings. The documentation will help you determine the next steps to take if malware is detected.

If malware is detected on the system, the first step is to isolate the system from the network.

If malware is detected on the system, the system will need to be sanitized after it has been isolated from the network.

References

TestOut Ethical Hacker Pro - 9.2 Combat Malware

[e_combat_malware_eh1.exam.xml Q_ANTI_MALWARE_PEN_TEST_MAL_01_EH1]