Exam Report: 8.4.12 Practice Questions

Date: 5/4/2020 11:12:51 pm
Time Spent: 2:18

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 38%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

You believe your system has been hacked. Which of the following is the first thing you should check?

- ~~Modified timestamps~~
- Hidden files
- System log files
- Browser history

Explanation

System log files are the first place to check for questionable activity. Typically hackers erase only the parts of the logs that show hacking actions. To the extent possible, a hacker makes the log appear as it did before the attack. This can be done without admin privileges. The following logs in Windows files are commonly deleted by a hacker:

- SECEVENT.EVT logs failed logins and file access without privileges
- SYSEVENT.EVT logs anomalies in system operations and driver failure
- APPEVENT.EVT logs application variants

These files are continuously open, running, and logging activity. A good hacker will remove any unneeded files that were added during the hack and also remove information in the files that were generated by the attack.

There are many additional ways to clear online tracks, including the following:

- Browse in private mode
- Delete history in address field and stored history
- Clear cookies and caches
- Delete downloads, saved sessions, and user JavaScript
- Disable password manager and clear its data
- Create multiple users
- Clear Most Recently Used and toolbar data
- Alter timestamp on files

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_COVER_TRACKS_ERASE_EVIDENCE_01_EH1]

Question 2: Correct

Who would be most likely to erase only parts of the system logs file?

- An everyday user
- The network admin
- A penetration tester

A black hat hacker

Explanation

Hackers are known for erasing only the parts of the logs that show the hacking actions and making the files appear as they did before the attack arrived.

Penetration testers don't usually modify or delete any of the logs.

Network administrators would most likely erase all the log files.

Everyday users should have no reason to enter or erase log files.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_COVER_TRACKS_ERASE_EVIDENCE_02_EH1]

Question 3: Correct

Phil, a hacker, has found his way into a secure system. He is looking for a Windows utility he can use to retrieve, set, back up, and restore logging policies. Which of the following utilities should he consider?

- secedit
- poledit
- auditpol
- gpedit

Explanation

Auditpol is a utility you can use to retrieve, set, back up, and restore logging policies on Windows.

Group Policy Editor (gpedit.msc) allows you to edit a Group Policy object in Active Directory.

System Policy Editor (poledit.exe) allows you to edit the Local System policy.

Windows Security Configuration Editor (secedit.exe) configures and analyzes system security by comparing your current configuration to specified security templates.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_COVER_TRACKS_FACTS_01_EH1]

Question 4: Correct

Which of the following could a hacker use Alternate Data Streams (ADS) for?

- Tracking evidence
- Hiding evidence
- Erasing evidence
- Modifying evidence

Explanation

Alternate Data Streams (ADS) was created to allow compatibility with Macintosh files. One of its features is the ability to have multiple streams of data simultaneously. The alternate stream of data isn't seen in Windows Explorer. Executables can be activated from the command line, but remain unseen. This functionality allows the attacker to actively run programs undetected.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_COVER_TRACKS_HIDE_EVIDENCE_01_EH1]

Question 5: Incorrect

James, a hacker, has hacked into a Unix system and wants to change the timestamps on some files to hide his tracks. Which of the following timestamp tools would he most likely use?

- Touch
- ctime
- Meterpreter
- ~~Timestomp~~

Explanation

The touch command in Linux, Unix, and OSX can be used to alter the timestamp. It can change the time to the current time or to any specific time. Touch is already available on the system and nothing needs to be installed.

Timestomp is a tool for modifying or deleting a time stamp on a file to hide when it was created, accessed, or modified.

ctime is a header file that contains definitions of functions to get and manipulate date and time information and requires programming efforts to use.

Meterpreter is Metasploit's payload. It has many features for covering tracks, including the ability to change the timestamp on accessed files.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_COVER_TRACKS_MODIFY_TIME_01_EH1]

Question 6: Incorrect

Which of the following best describes CCleaner?

- A tool that can remove files and clear internet browsing history. It also frees up hard disk space. It clears the temporary files, history, and cookies from each of the six major search engines.
- A command line tool in Windows 2000 that will dump a remote or local event log into a tab-separated text file. It can also be used to filter specific types of events.
- ~~A software that can clear cookies, stored data like passwords, browser history, and temporary cached files. It can clear the recycling bin, clipboard data, and recent documents lists as well.~~
- A program that searches for carrier files through statistical analysis techniques, scans for data hiding tools, and can crack password-protected data to extract the payload.

Explanation

CCleaner is a cleaning tool that can remove files and clear internet browsing history. It also frees up hard disk space. It clears the temporary files, history, and cookies from each of the six major search engines.

Clear My History is software that can clear cookies, stored data like passwords, browser history, and temporary cached files. It can clear the recycling bin, clipboard data, and recent documents lists as well.

Dump Event Log is a command line tool in Windows 2000 that will dump an event log remotely or on a local system into a tab-separated text file. It can also be used to filter specific types of events.

StegoHunt searches for carrier files through statistical analysis techniques, scans for data hiding tools, and can crack password-protected data to extract the payload.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_COVER_TRACKS_TOOLS_01_EH1]

Question 7: Incorrect

Mark is moving files from a device that is formatted using NTFS to a device that is formatted using FAT. Which of the following is he trying to get rid of?

- Malicious alternate data streams.

- Antivirus and anti-spyware programs.
- Software programs that hackers use.
- ~~Encrypted steganographic information.~~

Explanation

To get rid of malicious alternate data streams, move suspect files to a partition or device that is formatted using FAT. Since FAT doesn't support alternate data streams, the alternate file streams will be removed when the file is moved. Remember to keep your antivirus software updated. Tools that detect and remove infected ADS include LADS, Stream Detector, LNS, and Forensic Toolkit.

Steganography is the method of embedding data into legitimate files like graphics, banner ads, or plain text messages to hide it, and then extracting the data once it reaches its destination.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_HIDE_PROGRAMS_NTFS_DATA_01_EH1]

Question 8: Incorrect

Which of the following best describes a rootkit?

- Can modify the operating system and the utilities of the target system.
- Allows each file an unlimited number of data streams with unlimited size.
- ~~Scans the system and compares the current scan to the clean database.~~
- Allows the user to create a password to make the hidden file more secure.

Explanation

Rootkits can modify the operating system and the utilities of the target system. Rootkits contain packet sniffers, utilities that remove logs, DDoS programs, IRC bots, and backdoor programs.

OmniHide Pro can hide files in photos, movies, documents, and music. It allows the user to create a password to make the hidden file more secure.

Integrity-based detection works by running a tool to scan a clean system to create a database. The integrity-based detection scans the system and compares the current scan to the clean database. Any dissimilarities between the clean baseline database and the current scan are flagged, and a notification is sent.

NTFS allows each file an unlimited number of data streams with unlimited size.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_HIDE_PROGRAMS_ROOT_KIT_01_EH1]

Question 9: Correct

Which of the following is also known as ZeroAccess and has virus, Trojan horse, and rootkit components?

- Sirefef
- DeepSound
- GrayFish
- Touch

Explanation

Sirefef, also as ZeroAccess, has virus, Trojan horse, and rootkit components. As a rootkit, it is unseen by antivirus and anti-spyware programs. Sirifef conceals itself by changing the internal process of the target operating system. This program is difficult to remove and can create problems with Windows Firewall and Defender Service, remote hosts, and browser settings. It creates a folder to store additional malware.

GrayFish is a rootkit tool that runs within the Windows operating system.

DeepSound is a tool for hiding data in audio files and for extracting files from audio tracks. It also has the option to encrypt the files.

The touch command in Linux, Unix, and OSX can be used to alter the timestamp. It can change the time to the current time or to any specific time.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_HIDE_PROGRAMS_ROOT_KIT_02_EH1]

Question 10: Incorrect

Jerry runs a tool to scan a clean system to create a database. The tool then scans the system again and compares the second scan to the clean database. Which of the following detection methods is Jerry using?

- Integrity-based
- ~~Cross view-based~~
- Signature-based
- Behavior-based

Explanation

Integrity-based detection works by running a tool to scan a clean system to create a database. The integrity-based detection scans the system and compares the current scan to the clean database. Any dissimilarities between the clean baseline database and the current scan are flagged, and a notification is sent.

Signature-based detection scans a system's processes and executable files, looking for byte sequences of known malicious rootkit programs.

Behavior-based detection searches for deviations in normal behaviors and patterns of an operating system.

Cross view-based detection uses an algorithm as it goes through the system files, processes, and registry keys to create a baseline that is compared to the data returned by the operating system's APIs.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_HIDE_PROGRAMS_ROOT_KIT_03_EH1]

Question 11: Correct

Which of the following best describes the heuristic or behavior-based detection method?

- Scans a system's processes and executable files, looking for byte sequences of known malicious rootkit programs.
- Uses an algorithm as it goes through the system files, processes, and registry keys to create a baseline that is compared to the data returned by the operating system's APIs.
- Searches for execution path hooking, which allows a function value in an accessible environment to be changed.
- Runs a tool to scan a clean system and create a database, then scans the system and compares the current scan to the clean database.

Explanation

Heuristic or behavior-based detection searches for deviations in an operating system's normal behaviors and patterns. One of the patterns it searches for is execution path hooking, which allows a function value in an accessible environment to be changed. This is a behavior used by rootkits.

Integrity-based detection works by running a tool to scan a clean system to create a database. The integrity-based detection scans the system and compares the current scan to the clean database. Any

dissimilarities between the clean baseline database and the current scan are flagged, and a notification is sent.

Cross view-based detection uses an algorithm as it goes through the system files, processes, and registry keys to create a baseline that is compared to the data returned by the operating system's APIs.

Signature-based detection scans a system's processes and executable files, looking for byte sequences of known malicious rootkit programs.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_HIDE_PROGRAMS_ROOT_KIT_04_EH1]

Question 12: Incorrect

The method of embedding data into legitimate files like graphics to hide it and then extracting the data once it reaches its destination is called:

- ~~Execution path profiling~~
- Rootkits
- NTFS data streaming
- Steganography

Explanation

Steganography is the method of embedding data into legitimate files like graphics, banner ads, or plain text messages to hide it, and then extracting the data once it reaches its destination.

Hackers also hide programs through NTFS alternate data streams (ADS). When a file is created or copied to NTFS, one data stream stores the attributes, and a second stores the data. NTFS allows each file an unlimited number of data streams with unlimited size. Because they are hidden, a hacker can inject malicious code into these alternate data streams and execute the code without being detected by the user or system administrator.

A rootkit is a software program that hackers use to establish root- or admin-level privileges to a system. Rootkits are a set of programs designed to covertly access a system and allow the hacker to control its functions. Using a rootkit, a hacker can hide added applications and processes, obtain sensitive data, and set up the system to act as a server for bot updates.

Runtime execution path profiling checks for variations in the runtime execution path of all executable files and system processes.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_HIDE_PROGRAMS_STEGANOGRAPHY_01_EH1]

Question 13: Incorrect

Cameron wants to send secret messages to his friend Brandon, who works at a competitor's company. To secure these messages, he uses a technique to hide a secret message within a video. Which of the following techniques is he using?

- Steganography
- Public-key cryptograph
- ~~Encryption~~
- RSA algorithm

Explanation

Steganography is the method of embedding data into legitimate files like graphics, banner ads, or plain text messages to hide it, and then extracting the data once it reaches its destination.

Encryption is the translation of data into a secret code.

RSA (Rivest, Shamir, Adleman) is an algorithm used to encrypt and decrypt messages.

Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related but nonidentical keys, a public key and a private key.

References

TestOut Ethical Hacker Pro - 8.4 Cover Your Tracks
[e_cover_tracks_eh1.exam.xml Q_HIDE_PROGRAMS_STEGANOGRAPHY_02_EH1]