QBank Quiz Domain 3

Test ID: 178834730

Question #1 of 52

Question ID: 1322960

How are attributes of ownership and control of an object managed in Linux?

A) processes

B) permissions

C) rights

D) iptables

Explanation

Just as in Windows, Linux manages ownership and control of an object though the use of permissions. Permissions issues that can be encountered include users being assigned allow permissions that they should not have or being denied access when they need it.

Implementing file auditing will allow you to determine who is accessing files regularly. If a user or group is given access to files and you discover that they are not accessing them, you may want to remove their file permissions. Recertification is the process of examining a user's permissions and determining if they still need access to what was previously granted.

iptables is a firewall built into Linux. It requires elevated privileges to operate and must be executed by the root user; otherwise it fails to function. On most Linux systems, iptables is installed as `/usr/sbin/iptables`.

Rights are network actions granted to a person, such as the right to manage a printer.

A program or service in Linux is called a process, although services are also called daemons. A process is a single application as seen from the perspective of the processor. Multiprocessing is the operation of more than one process at a time.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

Linux > Understanding Linux File Permissions

Question #2 of 52

Question ID: 1322976

You are collecting evidence at an investigation. For what reason would you use a hashing tool?

A) to digitally alter the drive

B) to encrypt the drive to protect it from alteration

C) to ensure the integrity of the hard drive

D) to digitally sign the drive

Explanation

When the drive is presented as evidence in court, you must be able to prove it has not been altered. You should create a message digest of the drive and save it. The same process can be done in court and matched to the earlier message digest, which can prove it has not changed.

A bit-level copy of the original disk proves helpful in the forensic investigation. A bit-level copy of a hard disk refers to making a copy at the sector level to cover every part of the area that can store user data, such as slack space and free space. When creating a copy of the original disk, you should also perform a forensic hashing of the disk contents, both before and after the copy is made, and hash the image itself. By doing so, you can compare the hash values that are generated to ensure that image remains intact.

Hashing algorithms do not encrypt anything. They generate message digests. Encryption algorithms, not hashing algorithms, encrypt data.

There is no process for digitally signing a drive.

You do not want to alter the drive, even if you could alter the drive with hashing.

In summary, guidelines for evidence collection are:

Upon seizing digital evidence, actions taken should not change that evidence.

When it is necessary for a person to access original digital evidence, that person must be forensically competent.

All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.

An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.

Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Objective:
Host-Based Analysis

Sub-Objective:
Compare tampered and untampered disk images

References:

DataNarro > Understanding Forensic Copies & Hash Functions

Question #3 of 52

Question ID: 1322981

What is the process of taking data from multiple sources, such as IPS, firewall, and router, and combining it into a single integrated log file?

A) data normalization
B) data mapping
C) data aggregation
D) data warehousing

Explanation

Aggregation is the process of taking data from multiple sources, such as IPS, firewall, and router, and combining it into a single integrated log file. A Security Information and Event (SIEM) system collects data from the different security devices in the system, such as firewalls and IPSs, and then aggregates the log files for analysis.

Data mapping and data mapping software issued is used to both verify data accuracy and to help visualize data. Many trends and patterns can only be recognized when data has been visualized into a graph or chart.

Normalization is the process of eliminating redundancy and protecting integrity of the data. When utilized with IPS systems, it manages multiple incoming streams of data and ensure that all data exists only in one form. This eliminates redundant data.

Data warehousing is the combination of data from multiple data sources or databases into a single repository for analysis and manipulation.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret operating system, application, or command line logs to identify an event

References:

Bridging the Gap > What is Data Mapping?

Question #4 of 52

Question ID: 1322984

Which of the following is not a file type supported by the search capabilities of the IIS parser tool?

A) IIS logs
B) PDF
C) CSV
D) file system

Explanation

PDF files are not supported by the search capabilities of the IIS parser tool.

The IIS parser tool is a powerful versatile tool that can run SQL-like queries against log files. Among the file types supported are:

- CSV
- file system
- IIS logs
- event logs
- the registry
- Active Directory

Objective:
Host-Based Analysis

Sub-Objective:
Interpret operating system, application, or command line logs to identify an event

References:

Microsoft Downloads > Log Parser 2.2

Question #5 of 52

Question ID: 1322985

What security goal is satisfied by hashing algorithms?

A) confidentiality

B) integrity

C) availability

D) non-disclosure

Explanation

Hashing algorithms are used to generate hashes or message digests of the data. This is a string of characters that can be used later to verify the integrity if the data. If a regeneration of a hash value results in a message digest that is different from the first, the data has changed. If they match, it has not.

Hashing does not provide confidentiality. That requires encryption algorithms.

Hashing does not provide non-disclosure. Non-disclosure is the same as confidentiality.

Hashing does not increase availability. Availability requires redundancy.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)

References:

JScrambler > Hashing Algorithms

Question #6 of 52

Question ID: 1322980

Which statement is NOT true of data normalization?

A) It intercepts and stores data in one form only

B) It reduces integrity

C) It supports confidentiality

D) It reduces redundancy

Explanation

Rather than reducing integrity, data normalization increases integrity. Normalization is the process of eliminating redundancy and protecting integrity of the data. When data normalization is utilized with IPS systems, the IPS manages multiple incoming streams of data and ensures that all data exists only in one form. This eliminates redundant data.

The following statements are all true or data normalization:

- It reduces redundancy.
- It supports integrity.
- It intercepts and stores data in one form only.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret operating system, application, or command line logs to identify an event

References:

HYPERLINK "https://www.helpnetsecurity.com/2013/01/07/the-importance-of-data-normalization-in-ips/" Helpnet Security > The importance of data normalization in IPS

Question #7 of 52

Question ID: 1322973

Which evidence is always considered the best evidence?

A) direct
B) corroborative
C) indirect
D) hearsay

Explanation

Direct evidence is always considered the best because it does not require any reasoning or inference to arrive at the conclusion to be drawn from the evidence. An eyewitness account is direct evidence.

Hearsay is never admissible in court. This is when someone testifies they heard someone else say something they witnessed (also called second hand).

Corroborative evidence is that which supports other evidence. For example, if someone testifies that they saw it raining and another person testifies that they heard rain, the second testimony is considered corroborative evidence.

Indirect evidence suggests but does not prove anything. For example, if a man is accused of gambling and has been seen with gamblers, that is indirect evidence.

Objective:
Host-Based Analysis

Sub-Objective:
Identify type of evidence used based on provided logs (Best evidence; Corroborative evidence; Indirect evidence)

References:

The Free Dictionary > Direct Evidence

Question #8 of 52

Question ID: 1322966

What is the purpose of validating the attacking host’s IP address?

A) revealing the threat vector
B) identifying the target
C) identifying the protocol in use
D) revealing the threat actor

Explanation

Validating the attacking host's IP address is part of identifying the attacker. The attacker is the threat actor. It is the start of tracking this individual down.

Validating the attacking host IP address will not help identifying the threat vector. The threat vector is the delivery mechanism of the attack, such as email or malware.

Validating the attacking host's IP address will not help identify the target. The destination IP address will reveal the target.

Validating the attacking host's IP address will not help in identifying the protocol in use. The protocol in use can be seen in the Protocol column of a packet capture.

The client and server port identities identify the source and destination ports in use. If this source is NOT a well-known port (above 1024), the source is probably a client. If the source port is well known, it is likely the server.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the role of attribution in an investigation (Assets; Threat actor; Indicators of compromise; Indicators of attack)

References:

A10 > How to Identify and Block an Application Attacker

Question #9 of 52

Question ID: 1325275

Which statement is false of heuristics-based scanning?

A) it slows performance
B) it creates many false negatives
C) it may require fine tuning
D) it is time consuming

Explanation

Heuristic based malware scanning does not create false negatives. A false negative occurs when malware is present and not detected. Heuristic based malware scanning does create many false positives, where malware is reported to be present but is not.

By fine tuning the heuristics algorithm, the number of false positives can be reduced to a manageable level.

Heuristics scanning is time consuming and will degrade performance.

Heuristics is any approach to problem solving, learning, or discovery that employs a practical method, not guaranteed to be optimal, perfect, logical, or rational, but instead sufficient for reaching an immediate goal. Heuristic detection can be thought of as a type of software profiling. Security experts analyze known examples of malicious code and benign software to develop lists of characteristics of both.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the functionality of these endpoint technologies in regard to security monitoring (Host-based intrusion

detection; Antimalware and antivirus; Host-based firewall; Application-level whitelisting/blacklisting; Systems-based sandboxing)

References:

Kaspersky > What is Heuristic Analysis?

Question #10 of 52

Question ID: 1325277

You are reviewing malware detection reports that were run for four of your sites. Which detection ratio indicates the most secure site?

A) 20/65

B) 65/65

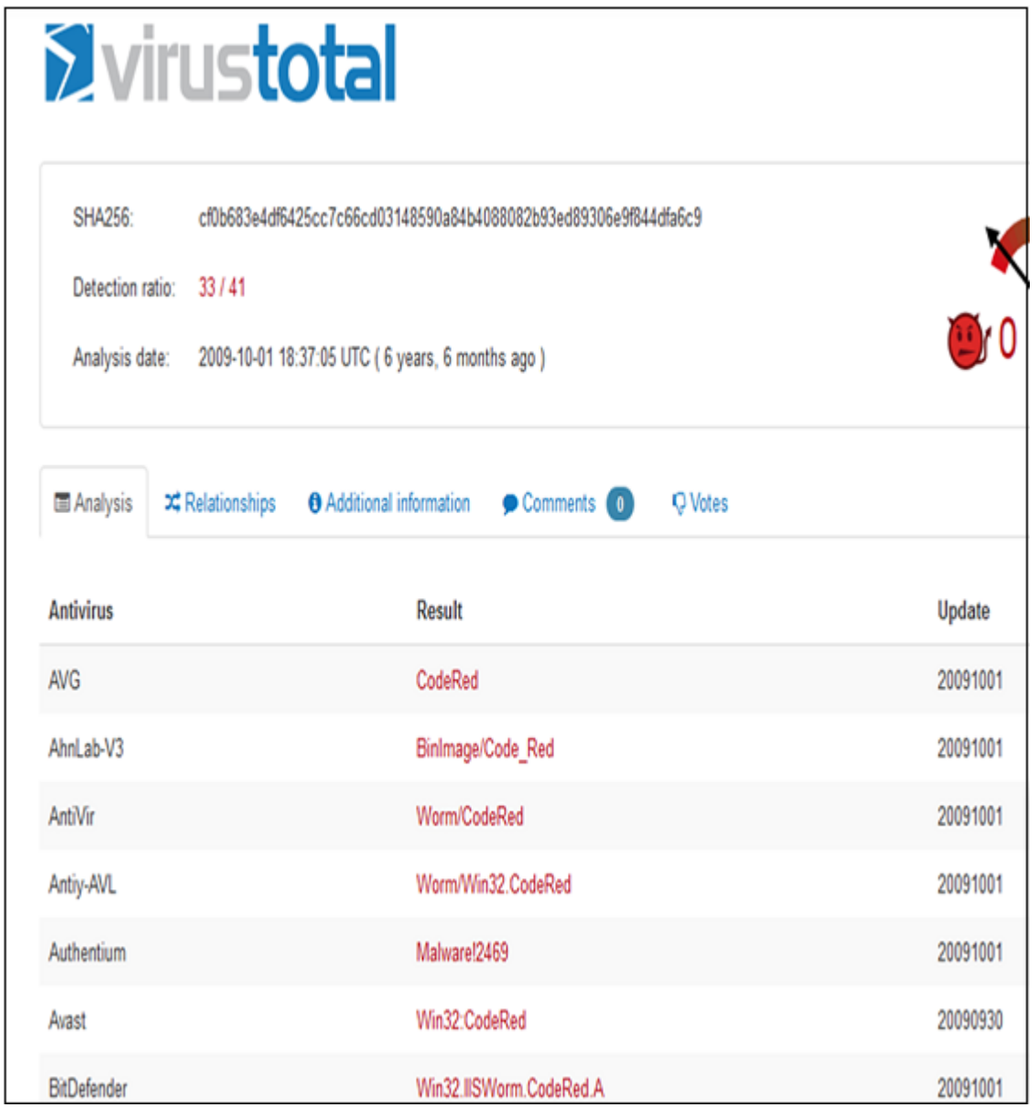
C) 30/65

D) 0/65

Explanation

The left-hand number represents the number of checks that indicated issues, while the right-hand number represents total number of issues checked. The ratio 0/65 indicates that all 65 checks were marked benign, and therefore indicates the most secure site.

An example of this metric is shown in the malware analysis tool by Virus total. As shown in the screenshot, the detection ratio for this scan is 31 out of 41:



Ratios of 20/65, 30/65 and 65/65 indicate that a certain percentage of the checks did NOT come back benign, meaning there are infections present.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)

References:

Cisco > Products & Services > Security > Advanced Malware Protection (AMP)

Question #11 of 52

Question ID: 1322950

Which of the following can be used to control access to a Linux device?

A) file rights
B) iptables
C) file permissions
D) forking

Explanation

Iptables is a Linux firewall that can be used to control access to the device.

File permissions are used in Linux to control access to files, not the device itself.

File rights is not a term used when discussing access to files in Linux.

Forking occurs when a process spawns another process. This produces two nearly identical versions of the same process. They are not identical, however, because they can tell the difference between the original and the spawned version.

File rights are used in Linux to control access to files, not the device.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

Ubuntu > IptablesHowTo

Question #12 of 52

Question ID: 1322963

Which statement is true with regard to evidence collection?

A) Always call police.
B) Always protect the integrity of the evidence.
C) Allow full access to the crime scene.

D) Always shut the computer down first.

Explanation

You should always protect the confidentiality and the integrity of all evidence collected and ensure that a proper chain of custody is maintained.

You should never shut the computer down until all volatile (memory) evidence is collected.

You should tightly control access to the crime scene.

You should always consider calling the police carefully as they will take control of the investigation.

In summary, guidelines for evidence collection are:

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the role of attribution in an investigation (Assets; Threat actor; Indicators of compromise; Indicators of attack)

References:

Elsevier > Digital Investigation

Question #13 of 52

Question ID: 1322956

Which of the following is the Windows equivalent of a daemon in Linux?

A) forks

B) services

C) processes

D) handles

Explanation

Services are part of the Windows OS that operate in the background. They are called daemons in Linux. Common services are identified by port numbers.

Handles are logical associations with a shared resource like a file. When a thread opens a file, it establishes a "handle" to the file.

A process is a single application as seen from the perspective of the processor. Multiprocessing is the operation of more than one process at a time.

A fork is an operation whereby a process creates a copy of itself. The fork operation creates a separate address space for the child. The child process has an exact copy of all the memory segments of the parent process.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

Digitial Citizen > What are Windows services, what do they do and how do you manage them?

Question #14 of 52

Question ID: 1322959

When a Linux process creates a child process, it is called what?

A) thread
B) instance
C) subprocess
D) fork

Explanation

A fork in Linux is a new process created by a running process. A fork is an operation whereby a process creates a copy of itself. The fork operation creates a separate address space for the child. The child process has an exact copy of all the memory segments of the parent process.

An instance is one copy of a running process. A second copy is called another instance.

Subprocess is not a term used to describe Linux processes and forks.

A thread represents a single set of sequential machine-code instructions that the processor executes. A thread also may be thought of as a subset of a process, as a process may have multiple threads.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

Linux/UNIX system programming training > Linux Programmer's Manual

---

Question #15 of 52

Question ID: 1325276

Which statement is false with respect to personal firewalls?

A) they can deny port numbers
B) they can deny services
C) they can take an action to prevent an attack
D) they can deny probing requests

Explanation

Personal firewalls cannot take an action to prevent an attack. They can only block specified traffic types. Only intrusion prevention systems can take actions top prevent an in attack that is in progress.

Personal firewalls can block both services and port numbers. One of the key protections it can provide is the prevention of probing requests from malicious individual seeking information.

Intrusion prevention systems (IPS) and intrusion detection systems (IDS) work together to complement each other. IPS systems can block activities on certain Web sites. Users may be allowed to access the sites but may be prevented from accessing certain features within the site. In other cases, the entire site may be blocked, depending on the security requirements for the organization.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the functionality of these endpoint technologies in regard to security monitoring (Host-based intrusion detection; Antimalware and antivirus; Host-based firewall; Application-level whitelisting/blacklisting; Systems-based sandboxing)

References:

Comodo > What is a Personal Firewall?

Question #16 of 52

Question ID: 1322961

What term us used to describe programs running in the background in Linux?

A) daemons
B) threads
C) services
D) processes

Explanation

Programs that are called services in Windows are called daemons in Linux. For example, the HTTP daemon in the destination server machine receives an HTTP request and, after any necessary processing, it returns the requested file.

Daemons are referred to as services in Windows.

A process is a single application as seen from the perspective of the processor. Multiprocessing is the operation of more than one process at a time.

A thread represents a single set of sequential machine-code instructions that the processor executes. A thread also may be thought of as a subset of a process as a process may have multiple threads.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

LINFO > Daemon Definition

Question #17 of 52

Question ID: 1322958

Which of the following is a file that contains a reference to another file or directory in the form of an absolute or relative path?

A) symlink

B) fork

C) handle

D) thread

Explanation

A symbolic link in Linux (also symlink or soft link) is a term for any file that contains a reference to another file or directory in the form of an absolute or relative path.

A thread represents a single set of sequential machine-code instructions that the processor executes. A thread also may be thought of as a subset of a process as a process may have multiple threads.

Handles are logical associations with a shared resource like a file. When a thread opens a file, it establishes a "handle" to the file.

A fork is an operation whereby a process creates a copy of itself. The fork operation creates a separate address space for the child. The child process has an exact copy of all the memory segments of the parent process.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

Indiana University > Create a symbolic link in Unix

Question #18 of 52

Question ID: 1322988

You discover several client machines are infected with malware that begins to make outbound calls (connection attempts) to a remote server after infection. You run a malware analysis tool. What information could you derive from any domain names and host IP addresses in the malware analysis report?

A) the next machine that will be infected

B) the first machine infected

C) destination of the callouts

D) signature of the malware

Explanation

The domain names and host IP addresses could be used to potentially determine the destination of the callouts, which are probably being made to a command and control server under the control of the hacker.

Although the malware signature might be indicated in the analysis report, it is not derived from domain names and host IP addresses.

Anti-virus or anti-malware products have a database of known forms of malware, which is a collection of code snippets, signatures, or data patterns from discovered-in-the-wild malicious code. Anti-virus software is usually very reliable at detecting known exploits. Unfortunately, anti-malware is not very effective at detecting new malware. Malware signatures are used by malware detection engines to identify malicious malware. This approach is not the only one. Some tools use heuristics, in which the tool looks for system behavior that is consistent with a malware infection. These types can sometimes identify zero-day malware attacks.

The domain names and host IP addresses cannot be used to determine either the last machine in your network infected or the next machine. The analysis report only refers to the local infected machine.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)

References:

Network World > Cisco ASA Innovation Tracks Botnet/Malicious Activity

---

Question #19 of 52

Question ID: 1322972

Which of the following is an example of corroborative evidence?

A) a spike in DNS traffic
B) a threat intelligence feed showing the command-and-control server hosts malware
C) a log that shows communication with a command-and-control server from malware
D) a firewall log verifying communication with a command-and-control server

Explanation

The spike in DNS traffic corroborated the other issues is corroborative evidence, as it usually accompanies these issues.

A log that shows communication with a command-and-control server from malware is direct evidence.

A firewall log verifying communication with a command-and-control server is also direct evidence.

A threat intelligence feed showing the command-and control server hosts malware is indirect evidence.

Guidelines for evidence collection are:

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Objective:
Host-Based Analysis

Sub-Objective:
Identify type of evidence used based on provided logs (Best evidence; Corroborative evidence; Indirect evidence)

References:

Criminal Law > Circumstantial versus Direct Evidence

Question #20 of 52

Question ID: 1322964

What is the process of identifying the malicious individual called?

A) threat actor attribution

B) process isolation

C) asset attribution

D) sandboxing

Explanation

Threat actor attribution is the identification of as many characteristics as possible regarding the threat actor. IP host names, IP addresses, and domain names are all important.

Asset attribution is the identification of all affected assets in an attack.

Sandboxing is a technique to confine the execution of an application to an environment (typically virtual) where it cannot interact with any other systems. Cuckoo Sandbox is an open source software for automating analysis of suspicious files. To do so, it makes use of custom components that monitor the behavior of the malicious processes while running in an isolated environment.

Process isolation is a technique used by operating systems to separate and confine the operation of one process from another.

The attack vector is the method used by the threat actor. Attack vectors include:

- viruses
- e-mail attachments
- Web pages
- pop-up windows
- instant messages
- chat rooms

Objective:
Host-Based Analysis

Sub-Objective:
Describe the role of attribution in an investigation (Assets; Threat actor; Indicators of compromise; Indicators of attack)

References:

SecureWorks > Does Threat Attribution Matter?

Question #21 of 52

Question ID: 1322979

What is the term for an operation that purges redundant data while maintaining data integrity?

A) normalization

B) aggregation

C) modularization

D) warehousing

Explanation

Normalization is the process of eliminating redundancy and protecting integrity of the data. When data normalization is utilized with IPS systems, the IPS manages multiple incoming streams of data and ensures that all data exists only in one form. This eliminates redundant data. Normalization is the part of the security analysis process that reduces the sheer amount of data and makes the process cleaner and more efficient.

Modularization is the breaking of a process into modules. A great example is the OSI model, which breaks the communication process down into seven modules or layers.

Aggregation is the process of taking data from multiple sources, such as IPS, firewall and router, and combining it into a single integrated log file. A Security Information and Event (SIEM) system collects data from the different security devices in the system, such as firewalls and IPSs, and then aggregates the log files for analysis.

Data warehousing is the combination of data from multiple data sources or databases into a single repository for analysis and manipulation.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret operating system, application, or command line logs to identify an event

References:

HYPERLINK "https://www.helpnetsecurity.com/2013/01/07/the-importance-of-data-normalization-in-ips/" Helpnet Security > The importance of data normalization in IPS

Microsoft Docs > Office > Access > Description of the database normalization basics

---

Question #22 of 52

Question ID: 1325273

Which of the following is deployed on an endpoint as an agent or standalone application?

A) HIDS

B) NIDS

C) NIPS

D) NGFW

Explanation

A host-based intrusion detection system (HIDS) monitors individual workstations on a network.

A network intrusion detection system (NIDS) is a system that operated on the network and detects attacks on that network. It monitors real-time traffic over the network, captures the packets, and analyzes them either through a signature database or against the normal traffic pattern behavior to ensure that there are no intrusion attempts or malicious threats. The primary disadvantage of an NIDS is its inability to analyze encrypted information. For example,

the packets that traverse through a Virtual Private Network (VPN) tunnel cannot be analyzed by the NIDS. An NIDS would most likely be used to detect, but not react to, behavior on the network.

A network intrusion prevention system (NIPS) is a system that operated on the network and detects attacks on that network while also taking actions to stop the attack. Intrusion prevention systems (IPS) and intrusion detection systems (IDS) work together to complement each other. IPS systems can block activities on certain Web sites. Users may be allowed to access the sites but may be prevented from accessing certain features within the site. In other cases, the entire site may be blocked, depending on the security requirements for the organization.

A next generation firewall (NGFW) is one that monitors all layers if the OSI model. It is not deployed on a host.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the functionality of these endpoint technologies in regard to security monitoring (Host-based intrusion detection; Antimalware and antivirus; Host-based firewall; Application-level whitelisting/blacklisting; Systems-based sandboxing)

References:

RedScan > HIDS - Host-based intrusion

Question #23 of 52

Question ID: 1325274

Which statements are false with respect to a HIDS?

A) protect the network where deployed

B) can read encrypted files

C) deployed on a host

D) can only create alerts

Explanation

A host intrusion detection system (HIDS) is deployed on a host. It protects ONLY that host.

The following characteristics are true of a HIDS:

- deployed on a host
- can read encrypted files
- can only create alerts
- can have more restrictive polices than a NIDS
- can generate alerts based on desktop behavior

Intrusion prevention systems (IPS) and intrusion detection systems (IDS) work together to complement each other. IPS systems can block activities on certain Web sites. Users may be allowed to access the sites but may be prevented from accessing certain features within the site. In other cases, the entire site may be blocked, depending on the security requirements for the organization.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the functionality of these endpoint technologies in regard to security monitoring (Host-based intrusion

detection; Antimalware and antivirus; Host-based firewall; Application-level whitelisting/blacklisting; Systems-based sandboxing)

References:

RedScan > HIDS - Host-based intrusion

Question #24 of 52

Question ID: 1322975

You are about to begin a forensic investigation. Which of the following is NOT part of the investigation?

A) Perform network traffic and log analysis.

B) Capture video.

C) Capture a system image.

D) Follow the incident response plan.

Explanation

Following an incident response plan is NOT part of an investigation. An incident response plan describes how to respond to various types of security incidents, but it is not part of the forensic investigation. All of the other options are part of an investigation.

You should capture a system image to take a "snapshot" of the system at the time you begin the investigation. This will preserve the state of the system at the time. The system image can be examined later. Network traffic and logs should be analyzed. Variations in baselines can indicate repeated attacks, and password hack attempts would show up in the logs. You should also capture video of the scene. Video records a series of individual frames, which can be tagged to help identify points of interest. The video should also indicate the location, date, time and the person who recorded the video. This step is referred to as active logging.

An investigation also involves recording the time offset, taking hashes and screenshots, and completing witness interviews. You should record time offset of the videos and all devices. It is not uncommon for a time to be off by a few seconds or even minutes. It is critical that you are able to trace events across multiple workstations and devices. You can add an entry into the log of a machine with the incorrect time to show the difference between the recorded time and the actual time. The time offset for every device and video that is captured must be recorded so that all evidence can be synched. You should take hashes of any digital evidence collected. This hash can then be compared to a hash that is calculated at a later date to ensure that the digital evidence has not been modified in any way. If the hash values are the same, the integrity of the digital evidence is verified. Screenshots allow you to record the information displayed on a computer screen or a smartphone. If the computer is powered down, whatever is on the screen would be lost without a screenshot. Witness interviews are an element of forensic investigation. It is important to talk to witness as early as possible after an incident. As time passes, recollections may change, and details may be forgotten. If at all possible, you should use some type of electronic recording system to document the interview. This is referred to as intelligence gathering.

In summary, the rules for forensic investigation are:

- Follow order of volatility rules.
- Capture a system image.
- Get copies of both a network traffic capture and logs.
- Ensure that the correct record time offset is obtained to ensure that any recordings can be calibrated together.
- Takes hashes of all files and images.
- Record the appropriate screenshots.
- Record any witnesses, including contact information.
- Keep track of man hours and expense involved in the forensic process.
- Obtain and preserve any video capture that exists, including computer video and CCTV.

- Perform big data analysis.

Objective:
Host-Based Analysis

Sub-Objective:
Compare tampered and untampered disk images

References:

CompTIA Security+ Deluxe Study Guide: SY0-501. Chapter 12: Disaster Recovery and Incident Response

---

Question #25 of 52

Question ID: 1322941

You are assessing application or service availability with a port scan. All services use default ports. This is an example of what type of exploit analysis?

A) probabilistic
B) intuitive
C) deterministic
D) predictive

Explanation

In deterministic analysis, all data used for analysis is known beforehand. An example of this type of analysis is port scanning because we clearly understand the rules of the TCP three way handshake beforehand and we know the default port numbers

In probabilistic analysis we don't have all data beforehand and works on probabilities.

Predictive analysis is not a term that is used when describing exploit analysis.

Intuitive is also not a term used when describing exploit analysis

Objective:
Host-Based Analysis

Sub-Objective:
Describe the functionality of these endpoint technologies in regard to security monitoring (Host-based intrusion detection; Antimalware and antivirus; Host-based firewall; Application-level whitelisting/blacklisting; Systems-based sandboxing)

References:

HYPERLINK "https://www.quora.com/What-is-the-difference-between-probabilistic-and-deterministic-models" Quora > What is the difference between probabilistic and deterministic models?

Question #26 of 52

Question ID: 1322969

Which of the following represents the chronological history of the possession of digital evidence?

A) chain of custody
B) evidence management

C) discovery

D) schedule of possession

Explanation

Chain of custody is a term that represents the chronological history of the possession of digital evidence. If it does not account for the security of the evidence at all times the evidence may be successfully challenged as corrupted.

Evidence management is a broader term that includes chain of custody, but also refers to the collection of the evidence.

Discovery is the exchange of evidence by both sides before a trial.

Schedule of possession is not a term that is used when discussing digital forensics.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the role of attribution in an investigation (Assets; Threat actor; Indicators of compromise; Indicators of attack)

References:

Study.com > What is the Chain of Custody? - Definition, Procedures & Importance

---

Question #27 of 52

Question ID: 1322955

Which of the following are logical associations with a shared resource like a file?

A) processes

B) handles

C) forks

D) threads

Explanation

Handles are logical associations with a shared resource like a file. When a thread opens a file, it establishes a "handle" to the file.

A thread represents a single set of sequential machine-code instructions that the processor executes. A thread also may be thought of as a subset of a process as a process may have multiple threads. Multithreading is when the processor can operate on more than one thread at a time.

A process is a single application as seen from the perspective of the processor. Multiprocessing is the operation of more than one process at a time.

A fork is an operation whereby a process creates a copy of itself. The fork operation creates a separate address space for the child. The child process has an exact copy of all the memory segments of the parent process.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

ServerFault > What is a Process Handle?

Question #28 of 52

Question ID: 1322942

Which of the following is the technique used by Java that prevents certain functions when the applet is sent as part of a Web page?

A) sandboxing

B) reference monitor

C) process isolation

D) segmentation

Explanation

Sandboxing is a technique used by Java as well as other applications to prevent the operation of the program from interfering with any other programs running.

Sandboxing also refers to developing an application outside of the production environment. Sandboxing can also be useful to test a legacy operating system that may not have security patches. Virtual machines are often used to create the sandbox. Memory allocation issues may be discovered during sandbox testing, but are not directly a part of the sandbox functionality.

Process isolation is a technique used by operating systems to isolate one running process from any other. It is not done in memory but in the processor queue.

Reference monitor is an abstract concept implemented by the security kernel of the operating system. It manages access from untrusted component to those that are part of the trusted computer base.

Segmentation is not a term used to discuss Java activities and operation.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the functionality of these endpoint technologies in regard to security monitoring (Host-based intrusion detection; Antimalware and antivirus; Host-based firewall; Application-level whitelisting/blacklisting; Systems-based sandboxing)

References:

Webopedia > sandbox

Question #29 of 52

Question ID: 1322962

What type of information is contained in the `/var/log` file in Linux?

A) kernel ring buffer information

B) global system messages, including the messages that are logged during system startup

C) all of the above

D) syslog and Apache access logs

Explanation

The information in the `/var/log` file in Linux includes Apache and syslog access logs.

Global system messages, including the messages that are logged during system startup are in the `/var/log/messages` file.

Kernel ring buffer information is stored in the `/var/log/dmesg` file.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

The Geek Stuff > 20 Linux Log Files that are Located under /var/log Directory

---

Question #30 of 52

Question ID: 1322967

What statement is FALSE about probabilistic analysis?

A) It indicates how likely the event is.

B) The answer is not definitive.

C) It is used in decision- making scenarios.

D) All data is known beforehand.

Explanation

In probabilistic analysis, data is not known beforehand. That is a characteristic of deterministic analysis.

The following statements are true of probabilistic analysis:

- The answer is not definitive.
- It is used in decision-making scenarios.
- It indicates how likely the event is.
- It uses powerful predicative tools.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the role of attribution in an investigation (Assets; Threat actor; Indicators of compromise; Indicators of attack)

References:

HYPERLINK "https://www.quora.com/What-is-the-difference-between-probabilistic-and-deterministic-models" Quora > What is the difference between probabilistic and deterministic models?

Question #31 of 52

Question ID: 1322949

When discontinuous free space is created by the adding and removing of data on a hard drive, what has occurred?

A) alternative data streams

B) fragmentation

C) steganography

D) forking

Explanation

Fragmentation is the occurrence of discontinuous free space that is created by the adding and removing of data on a hard drive. Fragmentation slows access to files that are scattered across the disk.

Forking occurs when a process spawns another process. This produces two nearly identical versions of the same process. They are not identical, however, because they can tell the difference between the original and the spawned version.

Alternative data streams are a feature of Windows New Technology File System (NTFS) that contains metadata for locating a specific file by author or title. The security issue with this process is that the information contained does not alter the size or title of the file. This means it is “hidden.”

Steganography is the science of hiding data within data, usually a graphic image. Steganography tools are used to imbed the file in the image and then the same tool is used at the destination to extract the file from the image.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

Remo > What is fragmentation in hard drive?

Question #32 of 52

Question ID: 1322991

Which encryption algorithm is weakest?

A) DES

B) Triple DES

C) MD5

D) AES

Explanation

Digital encryption standard (DES) is the first version of DES and the weakest of the listed encryption algorithms. DES is a private key encryption standard that is used in IPSec to ensure that data packets are confidentially transmitted. It uses a 64-bit key, but 8 bits are used for a parity check. Therefore, the effective key size of DES is 56 bits.

The DES algorithm uses 16 rounds of computation. The order and the type of computations performed depend upon the value supplied to the algorithm through the cipher blocks.

DES has many security issues. Triple DES (3DES.) is a later version of DES that performs three rounds of encryption and 48 rounds of computation. It offers high resistance to differential cryptanalysis because it uses so many rounds. The encryption and decryption process performed by 3DES takes longer due to the higher processing power required.

Advanced encryption algorithm (AES) is the strongest of the listed encryption algorithms. The Advanced Encryption Standard (AES) uses 128-bit, 192-bit, and 256-bit encryption keys.

MD5 is a one-way hashing algorithm, not an encryption algorithm.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)

References:

Techopedia > Triple DES

Question #33 of 52

Question ID: 1322951

Which of the following is the latest Linux file system?

A) ext5
B) ext2
C) ext3
D) ext4

Explanation

Ext4 is the latest Linux file system. One of the improvements over ext3 is support for unlimited subdirectories. Ext4 modifies important data structures of the filesystem, such as the ones destined to store the file data. The result is a filesystem with an improved design, better performance, reliability, and features. Other improvements are:

- Supports volumes with sizes up to 1 exabyte (EB) and files with sizes up to 16 terabytes (TB)
- Supports extents
- Is backwards compatible with ext3 and ext2
- Uses extents to replace the traditional block mapping scheme used by ext2 and ext3

Ext2 was the first commercial-grade file system for Linux. It is no longer in use. The ext2 filesystem does not support journaling, which would help in recovery after a crash.

Ext3 is the second version of the file system. The journaling feature in filesystems helps in recovery after a crash. The ext3 filesystem provides journaling capability.

There is no Ext5.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

HYPERLINK "https://wiki.archlinux.org/index.php/Ext4" ArchLinux > Ext4

IBM > Learn Linux > Create partitions and filesystems

Question #34 of 52

Question ID: 1322965

Which of the following represents an attack source?

A) host file

B) attack vector

C) threat actor

D) action on objectives

Explanation

A threat actor is anyone posing a threat through malicious activity. Some well-known threat actors globally are:

- APT10 - a Chinese group that has been around since early 2009. Their primary mission seems to be targeting defense contractors around the world.
- Turla - a popular Russian group most known for targeting government agencies around the world.
- Gosya - A popular Russian hacker who has been spotted selling the infamous Nuke Bot.
- Darkhotel - obtained their name from compromising hotel Wi-Fi systems,
- Mr. Po Panda - This actor's primary focus has been to deface company websites.
- ||JackSparrow|| - tries to pose as researchers, but has been known to conduct website defacements unexpectedly.

A host file is a file on a Windows machine that can contain manual IP address to name mappings.

The attack vector is not the individual. It is the method used by the threat actor. Attack vectors include:

- viruses
- e-mail attachments
- Web pages
- pop-up windows
- instant messages
- chat rooms

Action on objectives refers to the goal of the hacker. For example, it might be to deliver a ransomware letter.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the role of attribution in an investigation (Assets; Threat actor; Indicators of compromise; Indicators of attack)

References:

Proactive Defense > Understanding the 4 Main Threat Actor Types

---

Question #35 of 52

Question ID: 1322948

In what increments is FAT32 allocated?

A) 16 bits

B) 12 bits

C) 64 bits

D) 32 bits

Explanation

FAT32 is the version of File Allocation Table (FAT) introduced with Windows 95 OEM Service Release 2 (OSR2) and Windows 98. FAT32 supports a 32-bit allocation table. It is used for medium sized to very large hard disk volumes. Each entry is 28 bits, the maximum number of clusters is about 268,435,456, and the cluster size is 4 KB to 32 KB.

FAT12 is an early FAT file system that allocated by 12 bits. FAT12 was used for floppy disks and very small hard disk volumes. Each entry is 12 bits the maximum number of clusters is 4086. The cluster size is .5 to 4 KB.

FAT or FAT16 uses a 16-bit allocation table. It was used for small to moderate size hard disk volumes. Each entry is 16 bits, the maximum number of clusters is 65526, and the cluster size is 2 KB to 32 KB.

NTFS and exFAT are examples of file systems that allocate with 64 bits. NTFS is the default file system now in Windows. It allocates with 64 bits. exFat is used for flash drives.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

Microsoft TechNet > Wiki > Windows File Systems

Question #36 of 52

Question ID: 1322952

Which of the following represents a single set of sequential machine-code instructions that the processor executes?

A) processes
B) threads
C) handles
D) forks

Explanation

A thread represents a single set of sequential machine-code instructions that the processor executes. A thread also may be thought of as a subset of a process, as a process may have multiple threads. Multithreading is when the processor can operate on more than one thread at a time.

A process is a single application as seen from the perspective of the processor. Multiprocessing is the operation of more than one process at a time.

Handles are logical associations with a shared resource like a file. When a thread opens a file, it establishes a "handle" to the file.

A fork is an operation whereby a process creates a copy of itself. The fork operation creates a separate address space for the child. The child process has an exact copy of all the memory segments of the parent process.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

Techopedia > Threaded Code

Question #37 of 52

Question ID: 1322978

What is the main purpose of data normalization?

A) aggregate data

B) eliminate redundancy

C) duplicate data streams

D) synchronize of time stamps

Explanation

Normalization is the process of eliminating redundancy and protecting the integrity of the security event data. When data normalization is utilized with IPS systems, the IPS manages multiple incoming streams of data and ensures that all data exists only in one form. This eliminates redundant data.

Aggregation is the process of taking data from multiple sources, such as IPS, firewall and router, and combining it into a single integrated log file. A Security Information and Event (SIEM) system collects data from the different security devices in the system, such as firewalls and IPSs, and then aggregates the log files for analysis.

While the synchronization of time on all systems is key for data aggregation, that is not the purpose of normalization.

Duplication of data streams is not the goal of normalization. Normalization is the process of eliminating redundancy and protecting integrity.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret operating system, application, or command line logs to identify an event

References:

HYPERLINK "https://www.helpnetsecurity.com/2013/01/07/the-importance-of-data-normalization-in-ips/" HelpNet Security > The importance of data normalization in IPS

Question #38 of 52

Question ID: 1322970

Which of the following is an example of circumstantial evidence?

A) eyewitness report

B) a smoking gun

C) fingerprints

D) a video of someone entering the crime scene

Explanation

A video is considered circumstantial evidence as it proves they were there, but not necessarily that they did it. This type of evidence requires some inference or reasoning for conclusions to be drawn for the evidence. Direct evidence does not require any inference or reasoning and is somewhat self-evident.

A smoking gun taken from the perpetrator is direct evidence.

Fingerprints at the crime scene are direct evidence.

An eyewitness report is also direct evidence.

Objective:
Host-Based Analysis

Sub-Objective:
Identify type of evidence used based on provided logs (Best evidence; Corroborative evidence; Indirect evidence)

References:

Criminal Law > Circumstantial versus Direct Evidence

Question #39 of 52

Question ID: 1322977

What service is required to construct an accurate timeline of events from collected device logs?

A) NTP
B) DHCP
C) DNS
D) NAT

Explanation

The Network Time Protocol (NTP) should be used to keep all the device clocks in synch. Without it, a proper timeline cannot be created. NTP uses port number 123. NTP synchronization is the means by which clocks on various systems are brought into alignment. It is essential that all internal systems are synchronized. Being synchronized with a world time source helps to ensure that all logs and audit trails are in harmony in order to make investigations and historical research into the chronological order of events easier.

Dynamic Host Configuration Protocol (DHCP) is used to automate IP configuration delivery. It uses ports 67 and 68 and not only reduces administrative workload, but also eliminates human error in statically configuring IP configurations.

Domain Name System (DNS) resolves host and domain names to IP addresses and vice versa. It uses port 53 and eliminates the need to know the IP address of a host or domain name when connecting to the host or domain.

Network Address Translation (NAT) converts private IP addresses to public IP addresses and vice versa. It is a technology that allows resources that are using private IP addresses to communicate with the Internet through the NAT device and using a single public IP address.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret operating system, application, or command line logs to identify an event

References:

NTP > The Network Time Protocol

Question #40 of 52

Question ID: 1322947

What occurs when you allow specific executable files while denying all others?

A) redlisting

B) blacklisting

C) greylisting

D) whitelisting

Explanation

When you are whitelisting, you are creating a list of allowed applications while denying all others. Those approved applications are designated as whitelisted. These lists can also be used for domain name allowance with DNS. Several products are available that check for applications that are not on the whitelist, including attempts to install those applications. For example, the logs generated by the whitelisting product would tell you if someone had attempted to install a keylogger.

When blacklisting, you create a list of denied applications while allowing all others. These lists can also be used for domain name blocking with DNS. Blacklisting is an allow by default concept, where all software is allowed to execute unless it is on the Deny List.

There is no form of filtering called redlisting or greylisting.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the functionality of these endpoint technologies in regard to security monitoring (Host-based intrusion detection; Antimalware and antivirus; Host-based firewall; Application-level whitelisting/blacklisting; Systems-based sandboxing)

References:

Schneier on Security > Whitelisting vs. Blacklisting

Question #41 of 52

Question ID: 1322989

Which of the following is defined by the NIST in the FIPS 180-4 standard?

A) SHA-1

B) SHA-256

C) SHA-512

D) MD5

Explanation

The SHA-256 hashing algorithm is defined in the FIPS 180-4 standard by the NIST. It is part of the SHA-2 family. The purpose of Secure Hash Algorithm (SHA) is to protect message integrity.

SHA-256, also referred to as SHA-2, is a newer version of SHA and uses 256-bit checksums. SHA-256 should be used with a disk image to protect the image's integrity so that image can be retained for forensic purposes.

MD5 is hashing algorithm but it is not defined in the FIPS 180-4 standard by the NIST. MD5 is the least secure of the listed hashing algorithms. MD5 is a one-way hashing algorithm. One-way hashing refers to inserting a string of variable length into a hashing algorithm and producing a hash value of fixed length. This hash value is appended to the end of the message being sent. This hash value is recomputed at the receivers end in the same fashion in which it was created by using the same computational logic. If the recomputed hash value is the same as the generated hash value, the message was not altered during the course of transmission.

Secure hash algorithm (SHA)-1 is the first version of SHA, and is the least secure version of SHA hashing algorithm. SHA-1 is a hashing algorithm that creates a message digest, which can be used to determine whether a file has been changed since the message digest was created. An unchanged message should create the same message digest on multiple passes through a hashing algorithm. It is not defined in the FIPS 180-4 standard by the NIST.

SHA-512 is a more secure version of SHA-256 and differs only in the number of rounds of computation. it is not defined in the FIPS 180-4 standard by the NIST.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)

References:

MTL > Scripts > SHA-256 Cryptographic Hash Algorithm

Question #42 of 52

Question ID: 1322986

Which of the following is used to support data integrity?

A) SHA2
B) DES
C) multiple network cards
D) DSA

Explanation

SHA2 is a family of hashing algorithms. Hashing is used to prove integrity or prove that the data has not changed since the hash values were generated.

Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data. It supports confidentiality.

Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It is used to support non-repudiation.

Multiple network cards are an example of redundancy. Redundancy supports evaluability.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)

References:

WiseGeek > What is a Hashing Algorithm?

Question #43 of 52

Question ID: 1322971

Which of the following does NOT support evidence preservation during an incident?

A) bagging each item separately

B) tagging each piece of evidence

C) rebooting all involved systems prior to collection

D) maintaining chain of custody

Explanation

You should never reboot systems until all volatile evidence is collected. Evidence found in volatile locations, such as memory, will be lost if you do this.

Guidelines for collection include:

- Tag each piece of evidence.
- Bag each item separately.
- Maintain chain of custody.
- Never store evidence on a drive that itself is evidence.
- Control access to the scene.
- Report to authorities as required.

Objective:
Host-Based Analysis

Sub-Objective:
Identify type of evidence used based on provided logs (Best evidence; Corroborative evidence; Indirect evidence)

References:

Surety > Ensure Your Digital Evidence Will Stand Up in Court

Question #44 of 52

Question ID: 1322968

Which type of analysis attempts to gauge how likely an exploit is?

A) probabilistic

B) intuitive

C) predictive

D) deterministic

Explanation

Probabilistic analysis is done assuming the likelihood that an exploit will happen but you don’t know when or how.

The following are true of probabilistic analysis:

- The answer is not definitive.
- It is used in decision-making scenarios.
- It indicates how likely the event is.
- It uses powerful predicative tools.

Predictive analysis is not a term that is used when describing exploit analysis.

Intuitive is also not a term used when describing exploit analysis

In deterministic analysis all data used for analysis is known beforehand. An example of this type of analysis is port scanning because we clearly understand the rules of the TCP three-way handshake beforehand.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the role of attribution in an investigation (Assets; Threat actor; Indicators of compromise; Indicators of attack)

References:

HYPERLINK "https://www.quora.com/What-is-the-difference-between-probabilistic-and-deterministic-models"Quora > What is the difference between probabilistic and deterministic models?

Question #45 of 52

Question ID: 1322953

What is the recommended range of settings for virtual memory allocation in Windows?

A) half of the installed RAM

B) 4 times the installed RAM

C) the same as the installed RAM

D) 1 to 3 times installed RAM

Explanation

While Windows can handle virtual memory allocation automatically and usually does a good job, increasing the allocation can improve performance. The virtual memory allocation should be set between 1 and 3 times the size of the RAM.

Virtual memory is space on the hard drive used as memory when memory is maxed out. When memory contention arises, the virtual memory manager moves items out of memory to the hard drive to free up more memory. When that bit of information is found to missing in memory, the VMM goes back to the page file on the hard drive and moves it back into memory. This process of moving items back and forth from real memory to virtual memory is called paging.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

Technastic > How to Change Virtual Memory Allocation Size in Windows 10

Question #46 of 52

Question ID: 1322982

What type of analysis is required when an application uses ephemeral ports in its operation?

A) probabilistic

B) predictive

C) deterministic

D) intuitive

Explanation

Probabilistic analysis is done assuming the likelihood that an exploit will happen, but you do not know when or how.

The following are true of probabilistic analysis:

- The answer is not definitive.
- It is used in decision making scenarios.
- It indicates how likely the event is.
- It uses powerful predicative tools.

For example, since you can't know for sure what ephemeral port will be used by an application you must use probabilistic analysis.

Predictive analysis is not a term that is used when describing exploit analysis.

Intuitive is also not a term used when describing exploit analysis

In deterministic analysis all data used for analysis is known beforehand. An example of this type of analysis is port scanning because we clearly understand the rules of the TCP three way handshake beforehand and we know the default port numbers

Objective:
Host-Based Analysis

Sub-Objective:
Interpret operating system, application, or command line logs to identify an event

References:

HYPERLINK "https://www.quora.com/What-is-the-difference-between-probabilistic-and-deterministic-models" Quora > What is the difference between probabilistic and deterministic models?

Question #47 of 52

Question ID: 1322983

Which of the following is NOT an event category in the Windows Security Log?

A) Directory service access
B) Account management
C) Object access
D) Logoff events

Explanation

While there is a category called Logon events (which will also contain logoff events), there is no Logoff events category. This category records all local logons and logoffs both successful and unsuccessful.

Object access records all attempts to access resources such as files and folders.

Account management records all attempts to make changes to user accounts.

Directory service access records all attempts to make changes to Active Directory.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret operating system, application, or command line logs to identify an event

References:

Microsoft Docs > Windows > Security > Manage auditing and security log

---

Question #48 of 52

Question ID: 1325272

Which of the following Cisco tools makes retrospective analysis possible?

A) Cisco ASA

B) Cisco AMP

C) Cisco Talos

D) Cisco Ironport

Explanation

Cisco Advanced Malware Protection (AMP) comes in a Network version and an Endpoint version. It can use threat intelligence to perform retrospective (looking back in time) analysis. This would allow an administrator to do something like determine when malware entered your network, as in many cases it enters long before you discover it.

Cisco Advanced Security Appliance (ASA) is the standard Cisco firewall product and does not do retrospective analysis.

Cisco Ironport comes in a web version and email version, and is designed to protect those types of systems. It does not perform retrospective analysis.

Although Cisco Talos feeds are sometimes used in the process of performing retrospective analysis, it is not the component that does it. Cisco Talos is the threat intelligence sharing system that Cisco uses for all customers of the feature. The Talos team protects data, and infrastructure. Its researchers, data scientists, and engineers collect information about existing and developing threats. They then deliver protection against attacks and malware. Talos underpins the entire Cisco security ecosystem.

Objective:
Host-Based Analysis

Sub-Objective:
Describe the functionality of these endpoint technologies in regard to security monitoring (Host-based intrusion detection; Antimalware and antivirus; Host-based firewall; Application-level whitelisting/blacklisting; Systems-based sandboxing)

References:

Cisco > Products > Security > Advanced Malware Protection (AMP)

Question #49 of 52

Question ID: 1322990

Which of the following is not a hashing algorithm?

A) DES

B) SHA-3

C) SHA-1

D) MD5

Explanation

Digital encryption standard (DES) is an encryption algorithm, not a hashing algorithm. DES is a private key encryption standard that is used in IPSec to ensure that data packets are confidentially transmitted.

MD5 is a one-way hashing algorithm. One-way hashing inserts a string of variable length into a hashing algorithm and produces a hash value of fixed length. This hash value is appended to the end of the message being sent. The receiver recomputes the hash by using the same computational logic. If the recomputed hash value is the same as the generated hash value, the message was not altered during the course of transmission.

Secure Hashing Algorithm 1 (SHA 1) is the first and least secure version of SHA.

Secure Hashing Algorithm 3 (SHA 3) is the latest and most secure version of SHA.

Objective:
Host-Based Analysis

Sub-Objective:
Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)

References:

Nist > NIST Releases SHA-3 Cryptographic Hash Standard

Question #50 of 52

Question ID: 1322957

Which part of the Windows OS creates process isolation?

A) virtual cache
B) virtual address space
C) virtual memory
D) virtual swap

Explanation

Each process in Windows is assigned its own virtual address space in memory. By segregating memory in this way, process isolation is achieved.

Virtual cache is not a term used when discussing address spaces that a Windows process is allowed to access.

Virtual memory is space on the hard drive used as memory when memory is maxed out. When memory contention arises, the virtual memory manager moves items out of memory to the hard drive to free up more memory. When that bit of information is found to missing in memory the VMM goes back to the page file on the hard drive and moves it back into memory. This process of moving items back and forth from real memory to virtual memory is called paging.

Virtual swap is not a term used when discussing address spaces that a Windows process is allowed to access. A swap file is another name for a page file.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

Question #51 of 52

Question ID: 1322954

Which of the following provides the ability to allow scripting languages to manage Windows computers both locally and remotely?

A) EMI

B) RMI

C) WMI

D) STP

Explanation

Windows Management Instrumentation (WMI) consists of a set of extensions that allow access to settings and information through the command line, making the scripting of operations possible. The command-line interface to WMI called Windows Management Instrumentation Command-line (WMI).

Electromagnetic interference (EMI) is the inference with data traversing cables by strong electromagnetic energy generated by sources such as machinery. The transformers in fluorescent lighting systems are a common cause of network communications problems. If a network cable that is highly susceptible to EMI, such as unshielded-twisted pair (UTP) cable, is placed near lighting transformers, then the magnetic field produced by the transformers can cause network communications problems. You can replace UTP cable that runs near sources of EMI with shielded cable, such as shielded twisted-pair (STP) cable or coaxial cable. Fiber-optic cable is immune to EMI.

Radio frequency interference (RFI) occurs near sources of high power radio transmissions. TV stations, radio stations, cellular telephones, and CB radios can be sources of RFI. RFI can cause network communications problems, and intermittent computer problems such as spontaneously rebooting computers and data errors.

Spanning tree protocol (STP) is a loop avoidance protocol used with switches. Switching loops occur when multiple Layer 2 paths to a network cause a switch to flood broadcasts endlessly. This endless broadcast flood is called a "broadcast storm," and it causes severe network congestion. STP can be used to prevent these problems on a switched or bridged network.

Objective:
Host-Based Analysis

Sub-Objective:
Identify components of an operating system (such as Windows and Linux) in a given scenario

References:

Microsoft Docs > Windows > Apps > Windows Management Instrumentation > About WMI

Question #52 of 52

Question ID: 1322974

During a forensic investigation, you are asked to make a copy of the contents of a hard drive. You need to ensure that this evidence can be used in court if needed. Which statement is true of disk imaging in this investigation?

A) A byte-level copy of the disk assists in the forensic investigation.

B) The original copy of the disk should be used.

C) The content of the memory should not be dumped.

D) A bit-level copy of the disk assists in the forensic investigation.

Explanation

A bit-level copy of the original disk proves helpful in the forensic investigation. A bit-level copy of a hard disk refers to making a copy at the sector level to cover every part of the area that can store user data, such as slack space and free space. When creating a copy of the original disk, you should also perform a forensic hashing of the disk contents, both before and after the copy is made. In addition, a forensic hashing of the image itself should be performed. By doing so, you can ensure that image remains intact by comparing the hash values that are generated.

A byte-level copy of the hard disk is not preferred for forensic analysis after an incident has occurred. A byte-level copy initiates the forensic imaging of the attacked workstation.

To ensure the integrity of the evidence, the forensic investigation is not performed on the actual system. The system is taken offline by disconnecting it from the network, dumping the contents of the memory, and powering down the system. A backup copy of the system is taken, and this backup copy is used for investigation purposes. The output from the forensic imaging software should be directed towards a small computer system interface (SCSI) drive or some other media that is external to the system being investigated. This is done to initiate the forensic imaging of the attacked workstation. Changes made to the system, such as changing the file timestamps and modifying the files, can destroy the evidence. Therefore, skilled personnel should perform the forensic investigation to ensure that the evidence is unharmed and uncorrupted.

Objective:
Host-Based Analysis

Sub-Objective:
Compare tampered and untampered disk images

References:

Guidelines for Evidence Collection and Archiving, faqs.org > RFC 3227 - Guidelines for Evidence Collection and Archiving

CompTIA Security+ Deluxe Study Guide: SY0-501, Chapter 12: Disaster Recovery and Incident Response