Question #1 *Topic 1*

Which type of media should the IR team be handling as they seek to understand the root cause of an incident?

A. Restored media from full backup of the infected host

B. Media from the infected host, copied to the dedicated IR host

C. Original media from the infected host

D. Bit-for-bit image from the infected host

Suggested Answer: *A*
By imaging the media with tools such as dd or Ghost and analyzing the copy, you preserve the original media for later analysis so that the results can be recreated by another competent examiner if necessary.

keicaste 1 year, 10 months ago
None came out
upvoted 1 times

Question #2 *Topic 1*

An incident response team is handling a worm infection among their user workstations. They created an IPS signature to detect and block worm activity on the border IPS, then removed the worms artifacts or workstations triggering the rule. Despite this action, worm activity continued for days after. Where did the incident response team fail?

A. The team did not adequately apply lessons learned from the incident

B. The custom rule did not detect all infected workstations

C. They did not receive timely notification of the security event

D. The team did not understand the worm's propagation method

Suggested Answer: *B*
Identifying and scoping an incident during triage is important to successfully handling a security incident. The detection methods used by the team didnt detect all the infected workstations.

doesntmatter991 3 years, 7 months ago
I think D is more appropriate
upvoted 1 times

Question #3 *Topic 1*

A legacy server on the network was breached through an OS vulnerability with no patch available. The server is used only rarely by employees across several business units. The theft of information from the server goes unnoticed until the company is notified by a third party that sensitive information has been posted on the Internet. Which control was the first to fail?

A. Security awareness

B. Access control

C. Data classification

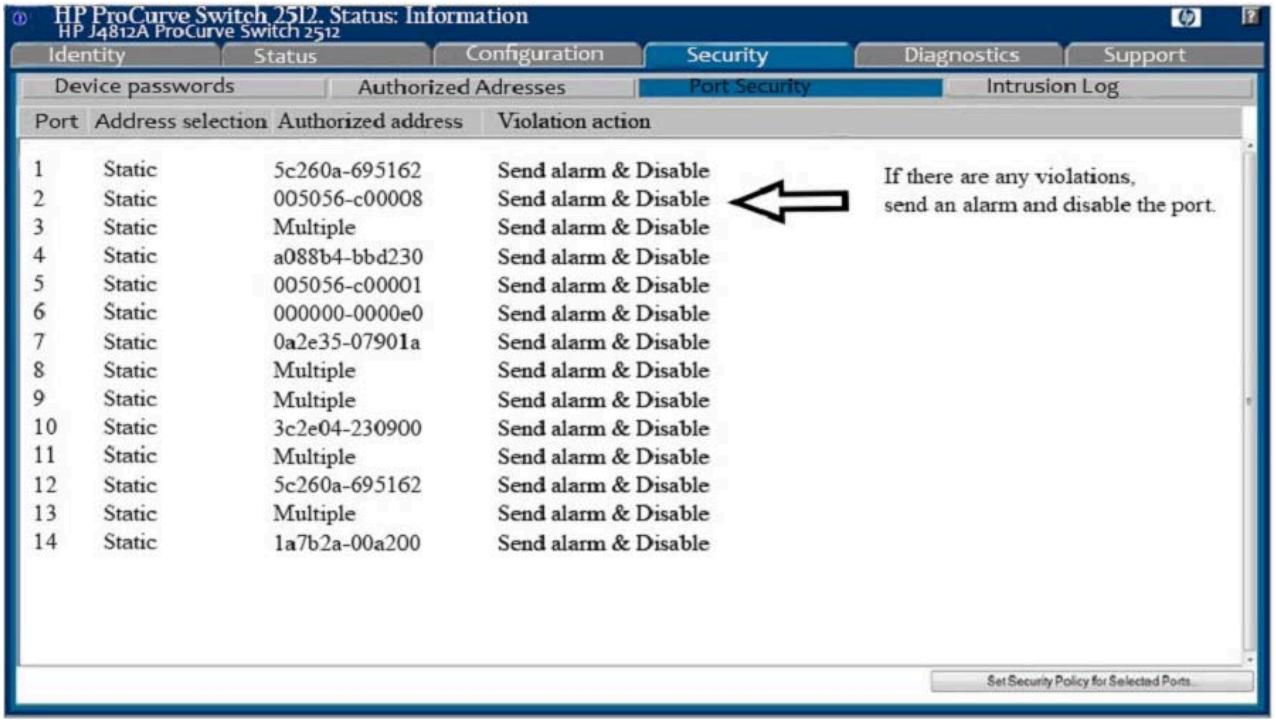
D. Incident response

Suggested Answer: *C*
The legacy system was not properly classified or assigned an owner. It is critical that an organization identifies and classifies information so proper controls and measures should be put in place. The ultimate goal of data classification is to make sure that all information is properly protected at the correct level.
This was not a failure of incident response, access control or security awareness training.

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Analyze the screenshot below. Which of the following attacks can be mitigated by these configuration settings?



A. A Denial-of-Service attack using network broadcasts

B. A Replay attack

C. An IP masquerading attack

D. A MAC Flood attack

Suggested Answer: *D*

Both BPDU Guard and Root Guard are used to prevent a new switch from becoming the Root Bridge. They are very similar but use different mechanisms.

Rootguard allows devices to use STP, but if they send superior BDPUs (i.e. they attempt to become the Root Bridge), Root Guard disables the port until the offending BPDUs cease. Recovery is automatic.

If Portfast is enabled on a port, BPDU Guard will disable the port if a BPDU is received. The port stays disabled until it is manually re-enabled. Devices behind such ports cannot use STP, as the port would be disabled as soon as they send BPDUs (which is the default behavior of switches).

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

Of the following pieces of digital evidence, which would be collected FIRST from a live system involved in an incident?

A. Event logs from a central repository

B. Directory listing of system files

C. Media in the CDrom drive

D. Swap space and page files

Suggested Answer: *D*
Best practices suggest that live response should follow the order of volatility, which means that you want to collect data which is changing the most rapidly. The order of volatility is:

Memory -

Swap or page file -
Network status and current / recent network connections

Running processes -
Open files

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

Which of the following attacks would use ".." notation as part of a web request to access restricted files and directories, and possibly execute code on the web server?

A. URL directory

B. HTTP header attack

C. SQL injection

D. IDS evasion

E. Cross site scripting

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

At the start of an investigation on a Windows system, the lead handler executes the following commands after inserting a USB drive. What is the purpose of this command? C:\ >dir / s / a dhsra d: \ > a: \ IRCD.txt

A. To create a file on the USB drive that contains a listing of the C: drive

B. To show hidden and archived files on the C: drive and copy them to the USB drive

C. To copy a forensic image of the local C: drive onto the USB drive

D. To compare a list of known good hashes on the USB drive to files on the local C: drive

Suggested Answer: *C*
This command will create a text file on the collection media (in this case you would probably be using a USB flash drive) named IRCD.txt that should contain a recursive directory listing of all files on the desk.

EggyEd 5 years, 1 month ago
This command generates a directory listing and not a forensic copy. Anser A should be the correct one
upvoted 3 times

Question #8 *Topic 1*

Why might an administrator not be able to delete a file using the Windows del command without specifying additional command line switches?

A. Because it has the read-only attribute set

B. Because it is encrypted

C. Because it has the nodel attribute set

D. Because it is an executable file

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Why would the pass action be used in a Snort configuration file?

A. The pass action simplifies some filtering by specifying what to ignore.

B. The pass action passes the packet onto further rules for immediate analysis.

C. The pass action serves as a placeholder in the snort configuration file for future rule updates.

D. Using the pass action allows a packet to be passed to an external process.

E. The pass action increases the number of false positives, better testing the rules.

Suggested Answer: *A*
The pass action is defined because it is sometimes easier to specify the class of data to ignore rather than the data you want to see. This can cut down the number of false positives and help keep down the size of log data.
False positives occur because rules failed and indicated a threat that is really not one. They should be minimized whenever possible.
The pass action causes the packet to be ignored, not passed on further. It is an active command, not a placeholder.

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

On which layer of the OSI Reference Model does the FWSnort utility function?

A. Physical Layer

B. Data Link Layer

C. Transport Layer

D. Session Layer

E. Application Layer

Suggested Answer: *C*

The FWSnort utility functions as a transport layer inline IPS.

Community vote distribution

E (100%)

saucehozz 2 years, 9 months ago

Selected Answer: E

Forgot to vote for: E

upvoted 2 times

saucehozz 2 years, 9 months ago

fwsnort is a perl script that translates Snort rules into equivalent iptables rules. This runs at the application layer.

fwsnort translates SNORT rules into iptables rules on Linux systems and generates a corresponding iptables policy in iptables-save format. This ruleset allows network traffic that matches Snort signatures (i.e. attacks and other suspicious network behavior) to be logged and/or dropped by iptables directly without putting an interface into promiscuous mode or queuing packets from kernel to user space.

upvoted 1 times

doesntmatter991 3 years, 7 months ago

FWSnort is not mentioned in the materials.

upvoted 1 times

Question #11 *Topic 1*

Which command tool can be used to change the read-only or hidden setting of the file in the screenshot?

A. attrib

B. type

C. tasklist

D. dir

Suggested Answer: *A*
attrib r or +r will remove or add the read only attribute from a file.

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

Which Unix administration tool is designed to monitor configuration changes to Cisco, Extreme and Foundry infrastructure devices?

A. SNMP

B. Netflow

C. RANCID

D. RMON

Suggested Answer: *C*

RANCID is a Unix tool which can be used to monitor changes to the following networked devices and more: IOS, CatOS, PIX, Juniper, Foundry, HP
ProCurve, Extreme.

doesntmatter991 3 years, 7 months ago

RANCID is not mentioned within the SANS content

upvoted 1 times

Question #13 *Topic 1*

If a Cisco router is configured with the "service config" configuration statement, which of the following tools could be used by an attacker to apply a new router configuration?

A. TFTPD

B. Hydra

C. Ettercap

D. Yersinia

Suggested Answer: *A*

doesntmatter991 3 years, 7 months ago

TFTPD is not mentioned in SANS content

upvoted 2 times

Question #14 *Topic 1*

Who is ultimately responsible for approving methods and controls that will reduce any potential risk to an organization?

A. Senior Management

B. Data Owner

C. Data Custodian

D. Security Auditor

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

An internal host at IP address 10.10.50.100 is suspected to be communicating with a command and control whenever a user launches browser window. What features and settings of Wireshark should be used to isolate and analyze this network traffic?

A. Filter traffic using ip.src = = 10.10.50.100 and tcp.srcport = = 80, and use Expert Info

B. Filter traffic using ip.src = = 10.10.50.100 and tcp.dstport = = 53, and use Expert Info

C. Filter traffic using ip.src = = 10.10.50.100 and tcp.dstport = = 80, and use Follow TCP stream

D. Filter traffic using ip.src = = 10.10.50.100, and use Follow TCP stream

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

Michael, a software engineer, added a module to a banking customers code. The new module deposits small amounts of money into his personal bank account.
Michael has access to edit the code, but only code reviewers have the ability to commit modules to production. The code reviewers have a backlog of work, and are often willing to trust the software developers testing and confidence in the code.
Which technique is Michael most likely to engage to implement the malicious code?

A. Denial of Service

B. Race Condition

C. Phishing

D. Social Engineering

Suggested Answer: *C*

doesntmatter991 3 years, 7 months ago

Would argue that this is Social Engineering rather than Phishing as it relies on the trust of Michael

upvoted 3 times

Question #17 *Topic 1*

A company wants to allow only company-issued devices to attach to the wired and wireless networks. Additionally, devices that are not up-to-date with OS patches need to be isolated from the rest of the network until they are updated. Which technology standards or protocols would meet these requirements?

A. 802.1x and Network Access Control

B. Kerberos and Network Access Control

C. LDAP and Authentication, Authorization and Accounting (AAA)

D. 802.11i and Authentication, Authorization and Accounting (AAA)

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

When attempting to collect data from a suspected system compromise, which of the following should generally be collected first?

A. The network connections and open ports

B. The contents of physical memory

C. The current routing table

D. A list of the running services

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Before re-assigning a computer to a new employee, what data security technique does the IT department use to make sure no data is left behind by the previous user?

A. Fingerprinting

B. Digital watermarking

C. Baselining

D. Wiping

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

What feature of Wireshark allows the analysis of one HTTP conversation?

A. Follow UDP Stream

B. Follow TCP Stream

C. Conversation list > IPV4

D. Setting a display filter to 'tcp'

Suggested Answer: *B*

Follow TCP Stream is a feature of Wireshark that allows the analysis of a single TCP conversation between two hosts over multiple packets. Filtering packets using tcp in the filter box will return all TCP packets, not grouping by a single TCP conversation. HTTP is TCP not UDP, so you cannot follow a HTTP stream over UDP.

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

From a security perspective, how should the Root Bridge be determined in a Spanning Tree Protocol (STP) environment?

A. Manually selected and defined by the network architect or engineer.

B. Defined by selecting the highest Bridge ID to be the root bridge.

C. Automatically selected by the Spanning Tree Protocol (STP).

D. All switch interfaces become root bridges in an STP environment.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which tasks would a First Responder perform during the Identification phase of Incident Response?

A. Verify the root cause of the incident and apply any missing security patches.

B. Install or reenable host-based firewalls and anti-virus software on suspected systems.

C. Search for sources of data and information that may be valuable in confirming and containing an incident.

D. Disconnect network communications and search for malicious executables or processes.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

What should happen before acquiring a bit-for-bit copy of suspect media during incident response?

A. Encrypt the original media to protect the data

B. Create a one-way hash of the original media

C. Decompress files on the original media

D. Decrypt the original media

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

How does the Cisco IOS IP Source Guard feature help prevent spoofing attacks?

A. Filters traffic based on IP address once a DHCP address has been assigned

B. Prevents unauthorized MAC addresses from receiving an IP address on the network

C. Blocks unsolicited ARP packets after a client has received an IP address

D. Rate limits client traffic to prevent CAM table flooding

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Which control would BEST help detect a potential insider threat?

A. Mandatory approval process for executive and administrative access requests.

B. Providing the same access to all employees and monitoring sensitive file access.

C. Multiple scheduled log reviews of all employee access levels throughout the year

D. Requiring more than one employee to be trained on each task or job duty.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

How would an attacker use the following configuration settings?

A. A client based HIDS evasion attack

B. A firewall based DDoS attack

C. A router based MITM attack

D. A switch based VLAN hopping attack

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

What is the most common read-only SNMP community string usually called?

A. private

B. mib

C. open

D. public

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

What would a penetration tester expect to access after the following metasploit payload is delivered successfully?
Set PAYLOAD windows / shell / reverse _ tcp

A. VNC server session on the target

B. A netcat listener on the target

C. A meterpreter prompt on the target

D. A command prompt on the target

Suggested Answer: *D*
set PAYLOAD windows/shell/reverse_tcp should get you to a command prompt on the host system. A different payload is used to get a meterpreter session. This payload does not start a VNC server or netcat listener on the target system.

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

Requiring background checks for employees who access protected data is an example of which type of data loss control?

A. Mitigation

B. Prevention

C. Monitoring

D. Identification

Suggested Answer: *B*

Once sensitive data is identified and classified, preventive measures can be taken. Among these are software-based controls, such as auditing and access control, as well as human controls such as background checks, psychological examinations, and such.

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Which of the following is an operational security control that is used as a prevention mechanism?

A. Labeling of assets

B. Heat detectors

C. Vibration alarms

D. Voltage regulators

Suggested Answer: *A*
The following are considered operational security prevention controls: Security gates, guards, and dogs; Heating, ventilation, and air conditioning
(HVAC); Fire suppressant; Labeling of assets (classification and responsible agents); Off-site storage (recovery); Safes and locks. The other distractors are considered operational security detection controls.

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

Why would a Cisco network device with the latest updates and patches have the service config setting enabled, making the device vulnerable to the TFTP Server
Attack?

A. Disabling telnet enables the setting on the network device.

B. This setting is enabled by default in the current Cisco IOS.

C. Allowing remote administration using SSH under the Cisco IOS also enables the setting.

D. An attack by Cisco Global Exploiter will automatically enable the setting.

E. This older default IOS setting was inherited from an older configuration despite the upgrade.

Suggested Answer: *B*
Enabling the service config setting causes a Cisco router to be vulnerable to the TFTP Server Attack since it will actively try to retrieve a new configuration file from the nearest TFTP server. An attacker can insert a malicious update file in this process to compromise the Cisco router. The service config setting was disabled by default in the Cisco IOS in version 12.0, but had been enabled by default in the 11.x series of the IOS trains. This feature is often enabled in later versions since organizations dont always realize the risk of this setting and will leave it enabled as the migrate through multiple
IOS upgrades.
The other items listed dont enable the service config setting.

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

In order to determine if network traffic adheres to expected usage and complies with technical standards, an organization would use a device that provides which functionality?

A. Stateful packet filtering

B. Signature matching

C. Protocol anomaly detection

D. CRC checking

E. Forward error correction

Suggested Answer: *C*

In addition to standards compliance, Protocol Anomaly Detection determines whether data within the protocol adheres to expected usage. Even if a communication stream complies with a protocol standard, the way in which the protocol is being used may be inconsistent with what is expected. Perimeter devices that perform protocol anomaly detection contain in-depth knowledge of protocol standards and expected usage and are able to detect traffic that does not comply with those guidelines.

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

Which of the following tools is the most capable for removing the unwanted add-on in the screenshot below?

A. ProcessExplorer

B. Taskkill

C. Paros

D. Hijack This

Suggested Answer: *B*

EggyEd 5 years, 1 month ago

tasskkill will kill the process running the internet browser program. A proxy (like paros) is needed to analysis the http traffic that builds the content of the webpage. --> Paros should be the correct answer

upvoted 1 times

dirk_gentley 5 years, 4 months ago

HijackThis is a no-frills tool to detect and remove suspicious elements from your web browsers.

upvoted 2 times

Question #34 *Topic 1*

An analyst will capture traffic from an air-gapped network that does not use DNS. The analyst is looking for unencrypted Syslog data being transmitted. Which of the following is most efficient for this purpose?

A. tcpdump –s0 –i eth0 port 514

B. tcpdump –nnvvX –i eth0 port 6514

C. tcpdump –nX –i eth0 port 514

D. tcpdump –vv –i eth0 port 6514

Suggested Answer: *B*

When using tcpdump, a n switch will tell the tool to not resolve hostnames; as this network makes no use of DNS this is efficient. The vv switch increases the tools output verbosity. The –s0 increases the snaplength to "all" rather than the default of 96 bytes. The –nnvvX would make sense here except that the port in the filter is 6514 which is the default port for encrypted Syslog transmissions.

EggyEd 5 years, 1 month ago

So the right answer is C

upvoted 1 times

Question #35 *Topic 1*

Throughout the week following a new IPS deployment, nearly every user on the protected subnet submits helpdesk tickets regarding network performance and not being able to access several critical resources. What is the most likely reason for the performance issues?

A. The incoming traffic is overflowing the device's TAP buffer

B. The in-line TAP experienced a hardware failure

C. The IPS sensor was changed from test mode to production mode

D. The IPS sensor was powered off or moved out of band

Suggested Answer: *A*

When deploying an IPS, you should carefully monitor and tune your systems and be aware of the risks involved. You should also have an in-depth understanding of your network, its traffic, and both its normal and abnormal characteristics. It is always recommended to run IPS and active response technologies in test mode for a while to thoroughly understand their behavior.

If the IPS had been previously powered off the performance issues would have impacted all network traffic, not just critical resources, and the issue would have begun on day 1 of deployment.

A hardware failure of the TAP would bring connectivity to a stop, not just impact users access to critical resources.

If the IPS and/or TAP cannot keep up with traffic, the users issues would have been more sporadic, rather than focused on a sudden loss to critical resources.

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

Which of the following is best defined as "anything that has the potential to target known or existing vulnerabilities in a system?"

A. Vector

B. Gateway

C. Threat

D. Exploit

Suggested Answer: *A*

EggyEd 5 years, 1 month ago

My first choice would be an exploit. as a known vulnerability is mentioned. A exploit is a small program that has the ability to abuse this vulnerability

upvoted 1 times

Question #37 *Topic 1*

An outside vulnerability assessment reveals that users have been routinely accessing Gmail from work for over a year, a clear violation of this organizations security policy. The users report "it just started working one day". Later, a network administrator admits he meant to unblock Gmail for just his own IP address, but he made a mistake in the firewall rule.
Which security control failed?

A. Access control

B. Authentication

C. Auditing

D. Rights management

Suggested Answer: *C*
Audits are used to identify irregular activity in logged (after-the-fact) records. If this activity went unnoticed or uncorrected for over a year, the internal audits failed because they were either incomplete or inaccurate.
Authentication, access control and managing user rights would not apply as a network admin could be expected to have the ability to configure firewall rules.

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

Which action would be the responsibility of the First Responder once arriving at the scene of a suspected incident as part of a Computer Security Incident
Response Plan (CSIRP)?

A. Making the decision of whether or not to notify law enforcement on behalf of the organization.

B. Performing timeline creation on the system files in order to identify and remove discovered malware.

C. Copying critical data from suspected systems to known good systems so productivity is not affected by the investigation.

D. Conducting initial interviews and identifying the systems involved in the suspected incident.

Suggested Answer: *D*
The First Responder plays a critical role in the Incident Response process on the CSIRT (Computer Security Incident Response Team).
Here is a list of some typical responder tasks:
Make sure that the correct system is identified and photograph the scene, if necessary.
Conduct an initial interview (not an interrogation) of any witnesses.
The decision to notify law enforcement requires explicit approval and direction form management and/or counsel. While a First Responder may collect initial data while minimally intruding on the system, no major changes, or indepth media analysis should be performed by the First Responder when initially responding to a suspected incident.

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

A company classifies data using document footers, labeling each file with security labels "Public", "Pattern", or "Company Proprietary". A new policy forbids sending "Company Proprietary" files via email. Which control could help security analysis identify breaches of this policy?

A. Monitoring failed authentications on a central logging device

B. Enforcing TLS encryption for outbound email with attachments

C. Blocking email attachments that match the hashes of the company's classification templates

D. Running custom keyword scans on outbound SMTP traffic from the mail server

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Although the packet listed below contained malware, it freely passed through a layer 3 switch. Why didn't the switch detect the malware in this packet?

A. The packet was part of a fragmentation attack

B. The data portion of the packet was encrypted

C. The entire packet was corrupted by the malware

D. It didn't look deeply enough into the packet

Suggested Answer: *D*

Routers, layer 3 switches, some firewalls, and other gateways are packet filtering devices that use access control lists (ACLs) and perform packet inspection. This type of device uses a small subset of the packet to make filtering decisions, such as source and destination IP address and protocol. These devices will then allow or deny protocols based on their associated ports. This type of packet inspection and access control is still highly susceptible to malicious attacks, because payloads and other areas of the packet are not being inspected. For example, application level attacks that are tunneled over open ports such as
HTTP (port 80) and HTTPS (port 443).

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

In an 802.1x deployment, which of the following would typically be considered a Supplicant?

A. A network switch

B. A perimeter firewall

C. A RADIUS server

D. A client laptop

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

You have been tasked with searching for Alternate Data Streams on the following collection of Windows partitions; 2GB FAT16, 6GB FAT32, and 4GB NTFS. How many total Gigabytes and partitions will you need to search?

A. 4GBs of data, the NTFS partition only.

B. 12GBs of data, the FAT16, FAT32, and NTFS partitions.

C. 6GBs of data, the FAT32 partition only.

D. 10GBs of data, both the FAT32 and NTFS partitions.

Suggested Answer: *C*

dirk_gentley 5 years, 4 months ago

Alternate Data Streams (ADS) are a file attribute only found on the NTFS file system.

upvoted 3 times

Question #43 *Topic 1*

What piece of information would be recorded by the first responder as part of the initial System Description?

A. Copies of log files

B. System serial number

C. List of system directories

D. Hash of each hard drive

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

Which type of attack could be used to obtain IOS router configuration files without a valid user password?

A. ARP cache poisoning

B. CDP sniffing

C. SNMP man in the middle

D. TFTP brute force

Suggested Answer: *D*

TFTP is a protocol to transfer files and commonly used with routers for configuration files, IOS images, and more. It requires no authentication. To download a file you need only know (or guess) its name. CDP, SNMP and ARP are not used for accessing or transferring IOS configuration files.

Currently there are no comments in this discussion, be the first to comment!