QBank Quiz Domain 4

Test ID: 178834768

Question #1 of 61

Question ID: 1322998

Which process is used to increase data accuracy and integrity and to support data visualization?

A) data warehousing

B) data aggregation

C) data normalization

D) data mapping

Explanation

Data mapping and data mapping software is used to both verify data accuracy and to help visualize data. Many security 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 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.

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

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

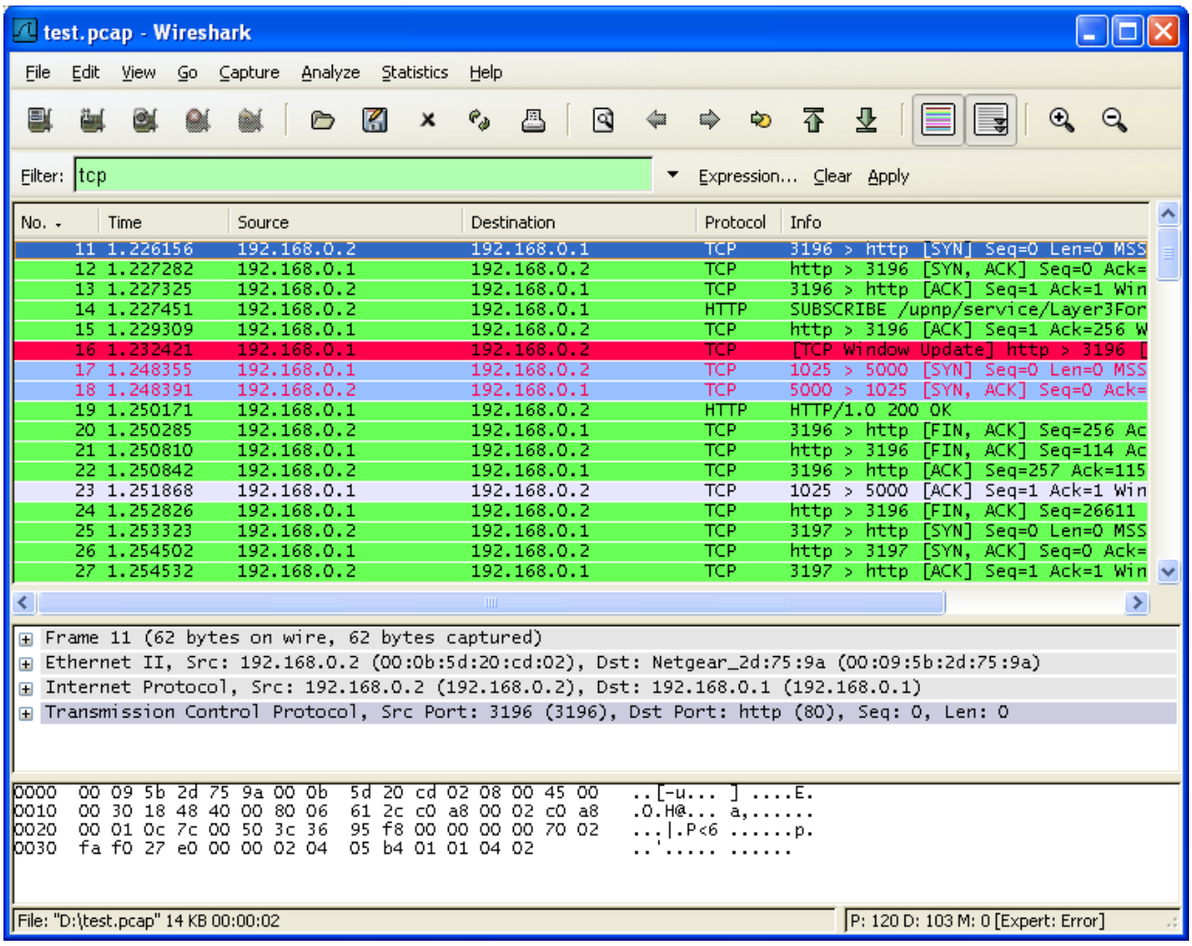
References:

Bridging the Gap > What is Data Mapping?

Question #2 of 61

Question ID: 1323020

Examine the following PCAP file:



What is the source MAC address of the highlighted packet (in red)?

A) 00:09:5b:2d:75:9a

B) 00:0b:5d:20:cd:02

C) 80

D) 192.168.0.2

Explanation

The source and destination MAC addresses are found in the details section of the output (at the bottom). The source is 00:0b:5d:20:cd:02, and the destination is 00:09:5b:2d:75:9a.

Other pieces of information on the same packet are:

- Source IP address - 192.168.0.2 - this is where the packet originated from
- Destination IP address - 192.168.0.1 - this is where the packet is going
- Source port number - 3196 - this number was picked at random by the sending device and will be used as the destination port when the destination device responds to the source.
- Destination port number - 80 - this the destination service being requested, in this case HTTP
- Protocol - TCP - this is the transport protocol in use. In this case, connection oriented TCP

192.168.0.2 is the destination IP address.

80 is the destination port number.

Objective:
Network Intrusion Analysis

Sub-Objective:
Identify key elements in an intrusion from a given PCAP file (Source address; Destination address; Source port; Destination port; Protocols; Payloads)

References:

HYPERLINK "https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/"How-To Geek > How to Use Wireshark to Capture, Filter and Inspect Packets

---

Question #3 of 61

Question ID: 1323002

Examine the following NetFlow entry:

2016-10-17	21:15:28:232	0.00	UDP	127.0.1.1:236744	192.1687.5.5:26353	1	82	1

Which statement is FALSE?

A) This is a single packet.

B) The protocol is UDP.

C) The bytes are 82.

D) The destination port is 236744.

Explanation

The destination port is 236353, not 236744.

The number of bytes is 82.

This entry represents a single packet. The entry with the missing column headings are as follows:

Date	FlowStart	Duration	Protocol	SrcIP address Port	DestIP address Port	Packets	Bytes	Flow
2016-10-17	21:15:28:232	0.00	UDP	127.0.1.1:236744	192.1687.5.5:26353	1	82	1

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

HYPERLINK "https://www.flowmon.com/en/solutions/use-case/netflow-ipfix?msclkid=7aa92f29a1561b55d6e7749d573ad74c&utm_source=bing&utm_medium=cpc&utm_campaign=2017%20BING%20SEA%20Netflow-IPFIX%20%5Bp%2Be%5D&utm_term=netflow&utm_content=Netflow" Flowmon > NetFlow/IPFIX Monitoring

---

Question #4 of 61

Question ID: 1323051

You have been asked to collect all the usernames from an access log. According to policy, usernames must be at least six characters and no more than sixteen characters. Usernames can only include lowercase letters, numbers, underscores, and hyphens, such as the following;

```
tmcmillan062
alang_12
j-hester27909093
```

Which regular expression will locate all valid usernames?

A) `^[a-z1-6]+$`

B) `^[az0_16]*$`

C) `^[az0_16]?$`

D) `^[a-z0-9_-]{6,16}$`

Explanation

The regular expression `^[a-z0-9_-]{6,16}$` will locate all valid usernames. The ^ and $ indicate the beginning and end of the pattern, respectively. The characters inside of the square brackets [] specify what is allowable, being a lowercase letter (a-z), number (0-9), underscore (_), or hyphen (-). The values in the curly braces {} specifies the minimum and maximum number of occurrences, being at least six, but no more than sixteen characters.

The regular expression `^[az0-16]?$` only finds usernames with a single character a, z, 0, 1, _, or 6. Also, the question mark (?) will match these characters zero or one time, returning empty matches.

The regular expression `^[a-z1-6]+$` will locate only usernames that contain one or more lowercase letters or the digits 1 through 6. The plus sign (+) will match one or more occurrence.

The regular expression `^[az0_16]*$` will locate only usernames that contain the characters a, z, 0, _,1 or 6. Also, the asterisk (*) will match zero or more occurrences, returning empty matches.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret basic regular expressions

References:

GNU.org > Software > FindUtils > Manual > Egrep Regular Expressions

---

Question #5 of 61

Question ID: 1323023

Which of the following Wireshark filters excludes an IP address?

A) `ip.addr==192.168.1.0/24`

B) `gateway host <host>`

C) `!ip.addr==192.168.1.2`

D) `eth.addr == 00:60:e0:53:13:d5`

Explanation

The filter `!ip.addr==192.168.1.2` excludes the IP address 192.168/.1.2. The ! character is the key.

The filer `ip.addr==192.168.1.0/24` filters for any IP address in the 192.168.1.0 255.255.255.0 network.

The filter `eth.addr == 00:60:e0:53:13:d5` filters for the MAC address 00:60:e0:53:13:d5.

The primitive `gateway host <host>` filters for packets that used a host as a gateway.

Objective:
Network Intrusion Analysis

Sub-Objective:
Identify key elements in an intrusion from a given PCAP file (Source address; Destination address; Source port; Destination port; Protocols; Payloads)

References:

LinuxHint > How to Filter By IP in Wireshark

Question #6 of 61

Question ID: 1323026

Which of the following Wireshark filters does NOT have valid syntax?

A) `tcp.port==443`

B) `tcp port == 443`

C) `ip.addr==<addr>or ip.host==<host>`

D) `eth.addr == 00:60:e0:53:13:d5`

Explanation

The filter `tcp port == 443` is not valid. To filter for port 443, the filter would be `tcp.port==443`.

The filter `ip.addr==<addr>or ip.host==<host>` filters for a host address or a host name.

The filter `eth.addr == 00:60:e0:53:13:d5` filters for the MAC address 00:60:e0:53:13:d5.

Objective:
Network Intrusion Analysis

Sub-Objective:
Identify key elements in an intrusion from a given PCAP file (Source address; Destination address; Source port; Destination port; Protocols; Payloads)

References:

LinuxHint > How to Filter By IP in Wireshark

Question #7 of 61

Question ID: 1322993

Which of the following checks the health of a system before allowing access to the network?

A) NAC
B) NAT
C) DAC
D) SIEM

Explanation

Network Access Control (NAC) is a component that checks for the presence of all security patches, operating system updates, and antivirus definitions before allowing access to the network. It ensures that the computer on the network meet an organization's security policies. NAC user policies can be enforced based on the location of the network user, group membership, or some other criteria.

Media access control (MAC) filtering is a form of NAC. NAC provides host health checks for any devices connecting to the network. Hosts may be allowed or denied access or placed into a quarantined state based on this health check.

Network Address Translation (NAT) is a service that converts private IP addresses to public IP addresses and vice versa. It does not control network access based on the health of a host. 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.

A Security Information and Event Management (SIEM) system aggregates the security logs of the devices, analyzes the log in real time, and alerts for security issues and attacks. It does not control network access based on the health of a host. Aggregation is a SIEM feature that allows the collection of various events that are flagged by network hardware and software applications.

Correlation is a SIEM feature that looks for similarities in events that are collected from different devices. Correlation allows the analyst to examine seemingly unique events and determine the patterns between them.

Automated alerting and triggers are a SIEM feature that allow the system to react based on predetermined criteria. Alerts include one or more systems that notify an administrator when a predetermined event occurs. Triggers take it a step further, and respond to the event with a series of programmed actions. As an example, an NIPS can shut down port 80 when an unusually high amount of web traffic floods the network.

Discretionary Access Control (DAC) is an access system in which the owner of a resource controls access to the resource. It does not control network access based on the health of a host. The DAC model uses ACL to identify the users who have permissions to a resource. An access control list (ACL) is a security mechanism used to designate those users who can gain various types of access, such as read, write, and execute access, to resources on a network. An ACL provides security as granular as the file level.

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

Techopedia > Cisco Network Admission Control (Cisco NAC)

Question #8 of 61

Question ID: 1323048

What is the term for program or service in Linux?

A) thread
B) processes

C) handles

D) forks

Explanation

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.

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:
Network Intrusion Analysis

Sub-Objective:
Interpret common artifact elements from an event to identify an alert (IP address (source / destination); Client and server port identity; Process (file or registry); System (API calls) Hashes; URI / URL)

References:

Shichao's Notes > Daemon Processes

Question #9 of 61

Question ID: 1323003

Refer to the following output.

```
sIP|dIP|sPort|dPort|pro|packets|bytes|flags|s Time|duration|eTime

192.168.5.5|203.36.54.3|443|36954|6|52|3120|A|2018/10/03T00:09:41.326|1774.520|2018/10/09T00:39:17.231
```

What statement is true of this record?

A) The protocol is UDP.

B) The destination port number is 443.

C) The number of packets is 6.

D) The source IP address is 192.168.5.5.

Explanation

The source IP address is 192.168.5.5. The first row are column headings separated by the |. If you match them with the next line, you will see that the source IP (sIP) is 192.168.5.5. This generic output could have come from a NetFlow device or from a protocol analyzer that is command line based. On its own, this output does not indicate an attack is underway.

The destination port number is 36954, not 443. That is the source port number.

Other common port numbers are:

- FTP – 20, 21
- SSH, SFTP – 22
- TELNET – 23
- SMTP – 25
- DNS – 53
- DHCP – 67, 68
- TFTP – 69
- HTTP – 80
- POP3 – 110
- NTP – 123
- NetBIOS – 137–139
- IMAP – 143
- SNMP – 161
- LDAP – 389

- SSL and HTTPS – 443
- LDAPS – 636
- MS SQL Server – 1433

The protocol is number 6, which is the number for TCP, not UDP.

The number of packets is 52, not 6. 6 is the protocol number.

The components in the entry mean the following:

- dIP - Destination IP address (203.36.54.3)
- sPort - Source port number (443)
- dPort - Destination port number (36954)
- pro - Protocol -TCP (protocol number 6)
- Packets - Number of packets (52)
- bytes - Number of bytes (3120)
- Flags - TCP flag ACK (A)
- sTime- system time
- Duration - time the exchange took
- eTime - sum of user and system time

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

CERT > Network Analysis with SiLK (PDF)

Question #10 of 61

Question ID: 1323047

What is the database where low-level operating system settings are stored in Windows?

A) config,sys
B) Settings folder
C) Registry
D) MIB

Explanation

The database where here low-level operating system settings are stored in Windows is called the Windows Registry.

A management information base (MIB) is where Simple Network Management Protocol (SNMP) settings are stored, not low-level operating system settings. Network management systems based upon SNMP contain two primary elements: a manager and agents. The manager is the console through which a network administrator performs network management functions. Agents are the entities that interface to the actual devices being managed. SNMP can monitor almost any type of network device, such as hubs, servers, interface cards, repeaters, and bridges. Threshold alarms can be set for all the parameters that the agent can monitor.

The config.sys file is used in the DOS OS and not Windows.

The Settings folder is not where low-level operating system settings are stored in Windows. The Settings folder stores user-defined settings.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret common artifact elements from an event to identify an alert (IP address (source / destination); Client and server port identity; Process (file or registry); System (API calls) Hashes; URI / URL)

References:

Microsoft Docs > Windows > Apps > Windows System Information > Registry

---

Question #11 of 61

Question ID: 1323040

Which of the following Wireshark filter filters for ports?

A) `tcp.port==443`

B) `ip.addr==<addr>or ip.host==<host>`

C) `tcp port equals 443`

D) `eth.addr == 00:60:e0:53:13:d5`

Explanation

The filter `tcp.port==443` filters for all packets referring to port 443.

The filter `ip.addr==<addr>or ip.host==<host>` filters for a host address or a host name.

The filter `eth.addr == 00:60:e0:53:13:d5` filters for the MAC address 00:60:e0:53:13:d5.

The filter `tcp port equals 443` is not valid syntax.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret common artifact elements from an event to identify an alert (IP address (source / destination); Client and server port identity; Process (file or registry); System (API calls) Hashes; URI / URL)

References:

LinuxHint > How to Filter By IP in Wireshark

Question #12 of 61

Question ID: 1323043

After performing some retrospective analysis following an attack, your boss asks you to explore system API calls. What type of communication is this?

A) operating system to browser

B) application to browser

C) browser to application

D) user program to file system

Explanation

System Application Process Interface or API calls are sent from the user program to the file system. They indicate attempts to interact with the underlying file system.

While there are APIs for communication between components such as browsers and applications as well, system APIs refer to communication with the file system.

System API calls are one of the common artifact elements or sources of security events that should be monitored.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret common artifact elements from an event to identify an alert (IP address (source / destination); Client and server port identity; Process (file or registry); System (API calls) Hashes; URI / URL)

References:

How Stuff Works > How to Leverage an API for Conferencing

Question #13 of 61

Question ID: 1323017

Which of the following techniques has as its focus transactional data?

A) Packet capture

B) network TAP

C) NetFlow

D) SNMP

Explanation

Netflow focuses not on the payload but on the connection details about each end of a conversation. Netflow records traffic flows that are distinguished by the following characteristics shared by each end of a connection:

- Ingress interface (SNMP ifIndex)
- Source IP address
- Destination IP address
- IP protocol
- Source port for UDP or TCP, 0 for other protocols
- Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
- IP Type of Service

Simple network protocol (SNMP) is polling method used to collect information about devices such as temperature. Analysis does not focus on transactional data.

Packet capture utilities like Wireshark include transactional data but that is not the main focus of the tool. Analysis focuses more on the payloads being sent.

A network TAP collects all data on the configured port (although that can be filtered) and analysis focuses mainly on payload rather than transactional data

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare inline traffic interrogation and taps or traffic monitoring

References:

]Products & Services > Cisco IOS and NX-OS Software > Cisco IOS Technologies > Management Instrumentation > Cisco IOS NetFlow

---

Question #14 of 61

Question ID: 1322997

You adopt an algorithm that distinguishes the most significant alert from a given set of events from multiple data sources in Firepower. What are you creating?

A) causation rule

B) access list

C) correlation rule

D) access rule

Explanation

A correlation rule is an algorithm you create in the Firepower console that attempts to rank alerts generated by various devices that populate the Firepower console. It a matter of assigning weights to various attack or incident types.

An access rule is a synonym for access control list in that it also controls access to something.

Access list is short for access control list, which is a set of rules defining who has access and what type of access that is.

There is no such things as a causation rule in the Firepower console, but the terms are related. Correlation means two things occur together while causation goes a step further and indicate one causes the other.

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

Cisco > Support > Product Support > Security > Cisco Firepower Management Center > Configuration Guides > Firepower Management Center Configuration Guide, Version 6.0 > Chapter: Correlation Policies

---

Question #15 of 61

Question ID: 1323035

Which service resolves host names to IP addresses?

A) ARP
B) TCP
C) ICMP
D) DNS

Explanation

Domain Name System (DNS) is a client-server application that can resolve host names to IP addresses and vice versa. A DNS server provides a centralized database of domain name-to-IP address resolutions on a server or servers that other computers on a network can use for name resolution.

Internet Control Message Protocol (ICMP) is a diagnostic and error message generating protocol that is part of the TCP/IP suite. ICMP operates at the Internet layer of the OSI model.

Transmission Control Protocol (TCP) is a protocol in the TCP/IP suite responsible for guaranteed delivery. It uses a three-way handshake to establish a connection before any data transfer takes place.

Protocols can use either User Datagram (UDP) or TCP to communicate. UDP is connectionless, while TCP is connection-oriented.

Address Resolution Protocol (ARP) resolves IP addresses to MAC addresses. It uses a broadcast mechanism to learn the MAC address of a host known only by its IP address. The media access control (MAC) address uniquely identifies a node on a network segment. ARP tables show the relationship of IP addresses to MAC addresses and are located on most devices.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

Network Solutions > Managing Domain Name Servers

Question #16 of 61

Question ID: 1323050

Which hashing algorithm is the most secure?

A) DES
B) MD5
C) SHA 3
D) SHA 2

Explanation

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

MD5 is the least secure of the listed hashing algorithms. 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.

SHA-256, also referred to as SHA-2, is a newer version of SHA and uses 256-bit checksums.

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

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret common artifact elements from an event to identify an alert (IP address (source / destination); Client and server port identity; Process (file or registry); System (API calls) Hashes; URI / URL)

References:

Nist > NIST Releases SHA-3 Cryptographic Hash Standard

Question #17 of 61

Question ID: 1323022

In Wireshark, what field indicates the device that is the recipient of a packet?

A) protocol
B) destination
C) Info
D) source

Explanation

The Destination field indicates the receiver of the packet. This is the target of the intrusion.

The Source field indicates the device that sends the initial packet of a session.

The Protocol field indicates the Transport layer protocol in use (TCP or UDP). A UDP header is comprised of only four values: source port, destination port, length, and checksum.

The Info field contains details about the TCP flags that are set in a TCP packet.

Objective:
Network Intrusion Analysis

Sub-Objective:
Identify key elements in an intrusion from a given PCAP file (Source address; Destination address; Source port; Destination port; Protocols; Payloads)

References:

How-To Geek >How to Use Wireshark to Capture, Filter and Inspect Packets

---

Question #18 of 61

Question ID: 1323006

An employee visits a malicious website, but the IDS does not detect the visit or alert you. What is this called?

A) False negative
B) True negative
C) False positive
D) True positive

Explanation

A false negative means the system made a mistake (False) and missed (negative) an issue.

A true positive means the IDS correctly (True) detected an issue (positive).

A true negative means the IDS correctly (True) did not detect an issue (negative).

A false positive means the IDS mistakenly (False) identified an attack (positive).

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare impact and no impact for these items (False positive; False negative; True positive; True negative; Benign)

References:

Live Science > What Are False Positives and False Negatives?

Question #19 of 61

Question ID: 1323005

What type of data is displayed in the following output?

```
Date  flow start  Duration Proto Src IP Addr:Port Dst IP Addr:Port  Packets  Bytes Flows
2010-09-01 00:00:00.459  0.000 UDP  127.0.0.1:24920- >  192.168.0.1:22126  1  46  1
2010-09-01 00:00:00.363  0.000 UDP  192.168.0.1:22126 >  127.0.0.1:24920  1  80  1
```

A) mirrored traffic

B) NetFlow traffic

C) traffic from a tap

D) firewall log

Explanation

The traffic displayed is from a NetFlow capture. NetFlow can collect IP traffic statistics on all interfaces where NetFlow is enabled, and later export those statistics as NetFlow records toward at least one NetFlow collector. Each flow is a unidirectional set of communication processes that share the following.

- Ingress interface
- Source IP address
- Destination IP address
- IP protocol
- Source port for UDP or TCP, 0 for other protocols
- Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
- IP Type of Service

Traffic from a TAP or traffic mirrored to a SPAN port would not be organized in this way. Its output in a capture tool like Wireshark would provide the ability to open the packet and look at its parts.

A network test access points (TAP) is an external monitoring device that mirrors the traffic that passes between two network nodes. A tap (test access point) is a hardware device inserted at a specific point in the network to monitor data.

The SPAN feature, which is sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer.

A firewall log output would indicate whether traffic was allowed or denied according to the firewall rules, which is not indicated in the output provided.

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

Cisco > Products & Services > Cisco IOS and NX-OS Software > Cisco IOS Technologies > Management Instrumentation > Cisco IOS NetFlow > White Papers > Introduction to Cisco IOS NetFlow - A Technical Overview > Document ID: 1518925696681207

Question #20 of 61

Question ID: 1323052

You need to locate the date within the timestamp of event logs from across multiple countries. You must locate dates that use the MM/DD/YYYY, MM/DD/YYYY, DD/MM/YYYY, MM-DD-YYYY, and DD-MM-YYYY.

Which regular expression will match these date formats?

A) `[0-9]{2}.[0-9]{2}.[0-9]{4}`

B) `[0-9]{2}*[0-9]{2}*[0-9]{4}`

C) `[0-9]{2}/[0-9]{2}/[0-9]{4}`

D) `[0-9]{2}-[0-9]{2}-[0-9]{4}`

Explanation

The regular expression `[0-9]{2}.[0-9]{2}.[0-9]{4}` will match the date formats listed in the scenario. The period (.) is a single character wildcard, allowing for slashes or hyphens.

The regular expressions `[0-9]{2}/[0-9]{2}/[0-9]{4}` and `[0-9]{2}-[0-9]{2}-[0-9]{4}` will only match examples when a slash or hyphen is specified, respectively.

The regular expression `[0-9]{2}*[0-9]{2}*[0-9]{4}` will cause an error because the asterisk (*) indicates zero or more occurrences and does not represent a character. For example, if you wanted to match one or more hyphens, you would enter `-*`, and this would match MM-DD-YYYY or MM----DD---YYYY for any number of hyphens.

The other quantifier characters are ? for zero or one occurrence, and + for one or more occurrence. For example, `[0-1]?[0-9]` would match 01, 12, 0, and 8, because the first digit of 0 or 1 is optional in the two-digit number.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret basic regular expressions

References:

GNU.org > Software > FindUtils > Manual > Egrep Regular Expressions

---

Question #21 of 61

Question ID: 1323019

Examine the following packet capture. (Not all packets are shown.)

1589	**6.536985**	**125.65.33.5**	**10.2.3.6**	**TCP**	**62**	**80- 40216 [ACK] Seq=14593 ACK=4447 Win=655535 Len=0**
1953	**6.698745**	**125.65.33.5**	**10.2.3.6**	**TCP**	**62**	**80- 40216 [ACK] Seq=14593 ACK=5907 Win=655535 Len=0**
1954	**7.232688**	**125.65.33.5**	**10.2.3.6**	**TCP**	**62**	**80- 40216 [ACK] Seq=14593 ACK=6871 Win=655535 Len=0**
1955	**7.635124**	**125.65.33.5**	**10.2.3.6**	**HTTP**	**442**	**HTTP/1.1 200 OK (GIF65b)**

Which statement is FALSE with regards to this capture?

A) Packet 1953's source is 10.2.3.6.

B) Packet 1589's transport protocol is TCP.

C) Packet 1954's destination is 10.2.3.6.

D) Packet 1955 contains a file that is extractable with Wireshark.

Explanation

The source of packet 1953 is 125.65.33.5, not 10.2.3.6. The missing column headings are as follows:

No.	Time	Source	Destination	Protocol	Length	Info

The other statements are true.

The packet 1955 contains a file that is extractable with Wireshark called GIF65b.

Packet 1589's transport protocol is TCP.

Packet 1954's destination is 10.2.3.6.

Objective:
Network Intrusion Analysis

Sub-Objective:
Extract files from a TCP stream when given a PCAP file and Wireshark

References:

How-To Geek > How to Use Wireshark to Capture, Filter and Inspect Packets

---

Question #22 of 61

Question ID: 1323031

What information can be discovered from the user agent field in an HTTP packet?

A) browser version
B) domain name of attacker
C) destination site
D) IP address of attacker

Explanation

The user agent transmits information about the browser and the operating system of the device. An example is shown below:

```
Mozilla/5.001 (windows; U; NT4.0; en-us) Gecko/25250101
```

It does not include the IP address of the attacker, the domain name of the attacker, or the destination site. That information is contained in other fields in the HTTP header (domain name) and the IP packet (IP address).

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

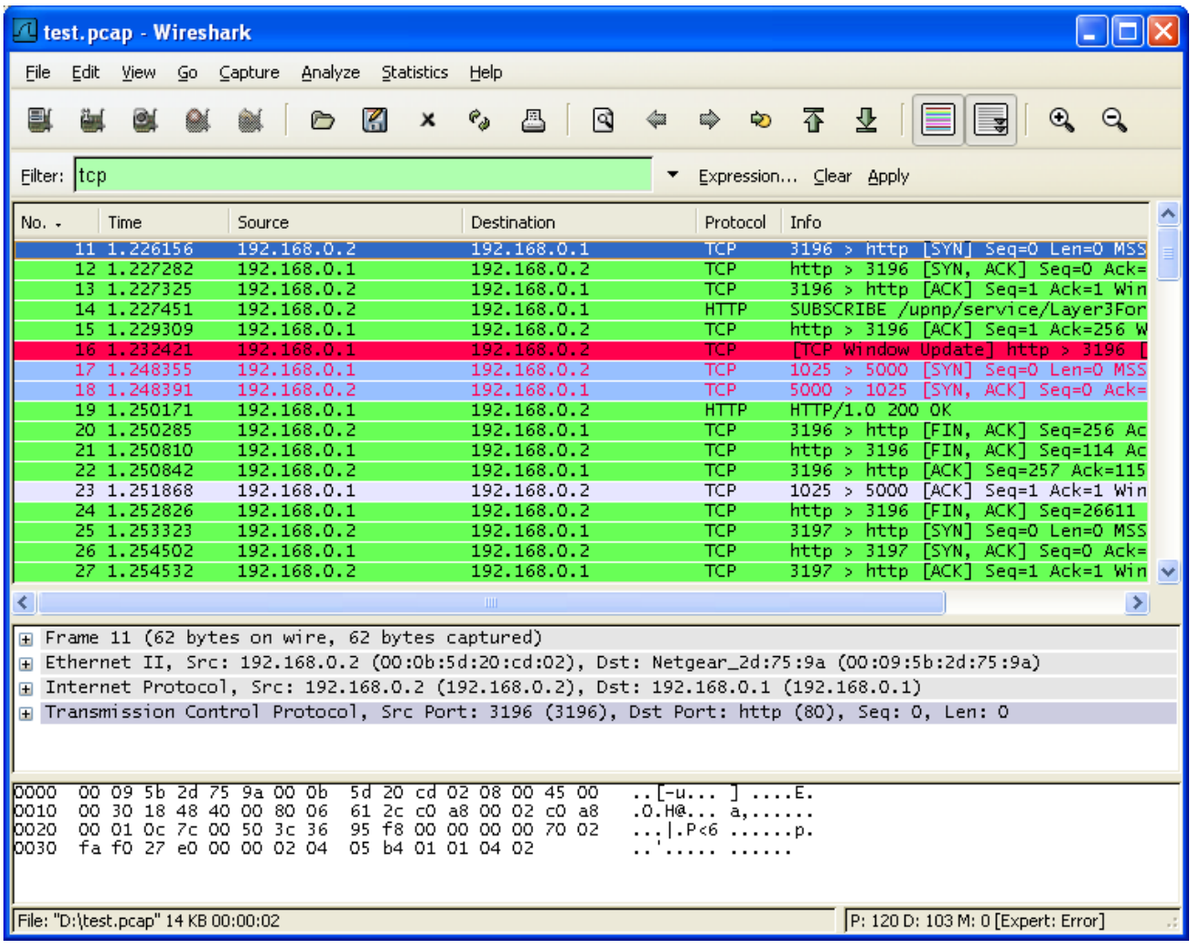
References:

WhatIsMyIPAddress > What is a User Agent?

Question #23 of 61

Question ID: 1323041

What application protocol is in use in this capture?



A) HTTP

B) DHCP

C) SSL

D) DNS

Explanation

The application protocol is indicated in the details section as the destination port of 80, which is HTTP.

The application protocol is not DHCP. Were that the case, the destination port numbers in the details section would be 67 and 68.

DNS is not the protocol in use. Were it in use, the destination port number in the details section would be 53.

If SSL were the application protocol, the destination would have been port 443.

You should be familiar with the following common protocols and their default ports:

- FTP – 20, 21
- SSH, SFTP – 22
- TELNET – 23
- SMTP – 25
- DNS – 53
- DHCP – 67, 68
- TFTP – 69
- HTTP – 80
- POP3 – 110
- NTP – 123
- NetBIOS – 137–139
- IMAP – 143
- SNMP – 161
- LDAP – 389
- SSL and HTTPS – 443
- LDAPS – 636
- MS SQL Server – 1433

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret common artifact elements from an event to identify an alert (IP address (source / destination); Client and server port identity; Process (file or registry); System (API calls) Hashes; URI / URL)

References:

How-To Geek > How to Use Wireshark to Capture, Filter and Inspect Packets

---

Question #24 of 61

Question ID: 1323004

Which of the following devices can request connection blocking in response to an attack?

A) firewall

B) IPS

C) IDS

D) router

Explanation

A promiscuous IPS can take several actions in response to an attacker, including:

- request connection blocking
- reset TCP connections
- request host blocking

An intrusion prevention system (IPS) detects network intrusion attempts and controls access to the network for the intruders. An IPS is an improvement over an intrusion detection system (IDS) because an IPS actually prevents intrusion.

An IDS cannot take any actions; it can only alert you. A signature-based IDS relies upon a database that contains the identities of possible attacks. This database is known as the signature database. A signature-based IDS watches for intrusions that match a known identity or signature. The signature database must be updated for a signature-based IDS to remain effective.

A network-based IDS is attached to the network in a place where it can monitor all network traffic. It implements passive and active responses. Passive responses include logging, notification, and shunning. Active responses include terminating processes or sessions, network configuration changes, and deception.

An anomaly-based IDS detects activities that are unusual. With this type of IDS, there is an initial learning period before anomalies can be detected. Once the baselines are established, an anomaly-based IDS can detect anomalies. Sometimes the baseline is established through a manual process.

A behavior-based IDS looks for behavior that is not allowed and acts accordingly.

A router and a firewall cannot take actions in response to attacks.

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

Cisco > Support > Product Support > Security > Cisco IPS 4200 Series Sensors > Configuration Guides > Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 7.0 > Chapter: Configuring Interfaces

---

Question #25 of 61

Question ID: 1323030

In the HTTP header, which of the following header fields indicates the domain name of the server (for virtual hosting) and the TCP port number on which the server is listening?

A) date

B) host

C) authorization

D) urgent pointer

E) referrer

Explanation

The host field indicates the domain name of the server (for virtual hosting) and the TCP port number on which the server is listening.

Other examples of HHTP header fields are:

- Accept - Media type(s) that is(/are) acceptable for the response
- Content-Length - The length of the request body in octets (8-bit bytes)
- From - The email address of the user making the request
- Referrer - The address of the previous web page from which a link to the currently requested page was followed
- Host - The domain name of the server (for virtual hosting), and the TCP port number on which the server is listening
- Date - The date and time that the message was originated
- Authorization - Authentication credentials for HTTP authentication

There is no urgent pointer field in an HTTP header. This field is found in TCP headers. The following lists the fields found in a TCP header:

- Urgent Pointer: Refers to the first urgent data byte in the packet.
- Sequence Number: Refers to the first byte of data in the current message. This field helps TCP to reassemble the packets in the correct order. For example, when data is transferred between an FTP server and FTP client, the receiver uses this field to reassemble the packets into the original file.
- Data Offset: Refers to the number of 32-bit words in the TCP header.
- Window: Refers to the size of the available space for the incoming data.
- Source Port and Destination Port: Refer to the point where upper-layer source and destination processes receive TCP services. Both TCP and UDP packets contain these fields.
- Acknowledgment Number: Refers to the sequence number of the next byte of data that the sender will receive.
- Reserved: Reserved for future use.
- Flags: Contains control information, such as the SYN and ACK bits which are used to establish and acknowledge communication, and the FIN bit which is used to terminate the connection.
- Checksum: An indicator of any damage to the header while being in transit. Both TCP and UDP packets contain this field.
- Options: Used to specify TCP options. Only TCP packets contain this field.
- Data: Has upper-layer information.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

Wiki > List of HTTP header fields

Question #26 of 61

Question ID: 1323039

A host is sending a ping packet to another host in the same subnet. For which IP address does the sending host perform an ARP broadcast to resolve?

A) the IP address of the destination host

B) the IP address of the DNS server

C) the IP address of the router

D) its own IP address

Explanation

All communication within a subnet is based on MAC addresses. When the destination is in the same subnet, the source device performs an ARP broadcast to learn the MAC address of the destination host.

The Address Resolution Protocol (ARP) is used in TCP/IP to resolve media access control (MAC) addresses to IP addresses. MAC addresses are configured on each NIC on an Ethernet network so that the nodes can be identified on the network. ARP enables the MAC addressing that Ethernet requires to interoperate with the IP addressing that TCP/IP requires. You can use the arp utility to view and manage the ARP cache on a computer. The ARP cache contains the IP address-to-MAC address resolutions on a computer. To use the arp utility, you

can issue the arp command with various switches at a command prompt. The source device will perform an ARP broadcast to learn the MAC address of the router in cases were the destination is in another subnet. Then the router will take over from there.

The source device will never perform an ARP broadcast to learn its own MAC address.

The only time a source device will perform an ARP broadcast to learn the MAC address of the DNS server is when communication is being done by name and not IP address.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

Dummies > Network Basics: Local Host ARP Requests

Question #27 of 61

Question ID: 1323014

Which statement is true with regard to SPAN and network taps?

A) The switch treats SPAN data with a higher priority than to-port data
B) The SPAN port should be used only for relatively high-throughput situations
C) Network TAPs have no IP address
D) TAPs alter the time relationships of frames

Explanation

Network test access points (TAPs) have no IP address and no MAC address. Therefore, they cannot be hacked.

TAPs are passive hardware devices that send a copy of the frame to the analyzer. A network TAP is an external monitoring device that mirrors the traffic that passes between two network nodes. A TAPs are inserted at a specific point in the network to monitor data.

The switch treats port mirroring (SPAN) data with a lower priority than to-port data, which is why is a high throughput scenario the switch might drop some packets before they get sent to the port where the analyzer resides. The SPAN feature, which is sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer.

TAPs do not alter the time relationships of frames. Spacing and response times are especially important with VoIP.

Because of the low priority the switch places on SPAN traffic, you should use the SPAN port only for relatively low-throughput situations.

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare inline traffic interrogation and taps or traffic monitoring

References:

Network Test Access Point (TAP) and Port Mirroring (SPAN)

Question #28 of 61

Question ID: 1322994

You are using the Cisco FMC to locate the first time a file event occurred involving the device at 192.168.5.3. What tool can be used?

A) retrospective analysis
B) trajectory map
C) dynamic ARP inspection
D) DHCP snooping

Explanation

On the trajectory map, you can locate the first time a file event occurred involving an IP address. This highlights a path to that data point, as well as any intervening file events and IP addresses related to the first file event.

Retrospective analysis is looking at data captured in the past and is typically used to determine when an attack or malware event started. Cisco Advanced Malware Protection (AMP) is capable of such analysis.

Dynamic ARP inspection (DAI) is an approach to preventing ARP attacks by implementing DHCP snooping. This allows the switch to record all DHCP records from the server and then disallows any ARP traffic from a spoofed MAC address.

DHCP snooping is used to prevent rogue DHCP servers and is also used as a part of the DAI solution.

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

Cisco > Support > Product Support > Security > Cisco Firepower Management Center > Configuration Guides > Firepower Management Center Configuration Guide, Version 6.0 > Chapter: File/Malware Events and Network File Trajectory

---

Question #29 of 61

Question ID: 1323032

At what layer of the OSI model does Internet Protocol (IP) operate?

A) Layer 4

B) Layer 3

C) Layer 1

D) Layer 2

Explanation

Both IPv4 and IPv6 operate at the Network Layer or Layer 3 of the Open System Interconnection (OSI) model.

The TCP/IP suite of protocols includes Address Resolution Protocol (ARP), Internet Protocol (IP), Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP).

The TCP/IP suite operates at Layer 2, Layer 3, and Layer 4 of the OSI model as follows:

- Layer 2, Data Link: ARP
- Layer 3, Network: IP, ICMP, IGMP, ARP
- Layer 4, Transport: TCP, UDP

The TCP/IP suite operates at Layer 1, Layer 2, and Layer 3 of the TCP/IP model as follows:

- Layer 1, Link: ARP
- Layer 2, Internet: IP, ICMP, IGMP, ARP
- Layer 3, Transport: TCP, UDP

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

Cisco Press > Articles > Cisco Certification > CCNA Routing and Switching > Fundamentals of IP for the CCNA INTRO Exam #640-821 > Typical Features of OSI Layer 3

Cisco Press > Articles > Cisco Certification > CCNA Routing and Switching > The TCP/IP and OSI Networking Models

---

Question #30 of 61

Question ID: 1323033

Which of the following protocols uses both TCP and UDP?

A) Telnet

B) TFTP

C) DNS

D) HTTP

Explanation

Domain Name System (DNS) protocol uses UDP when resolution queries are sent to a server by a client, but its uses TCP for zone transfers between DNS servers. According to RFC 1035, UDP is the recommended method for queries. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are both Transport layer protocols.

A DNS server provides a centralized database of domain name-to-IP address resolutions on a server or servers that other computers on a network can use for name resolution.

HTTP only uses TCP as its transport protocol. It uses port 80 and is used to transmit web traffic. Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files, such as text, graphic images, sound, video, and other multimedia files, on the World Wide Web. HTTP is an application protocol that works at the Application layer of the OSI model. The HTTP files can contain references to other files that will elicit additional transfer requests when they are selected.

TFTP only uses UDP as its transport mechanism. Its uses UDP port 69. Trivial File Transfer Protocol (TFTP) is a connectionless version of the File Transfer Protocol (FTP). TFTP transfers files between a client and a server. TFTP works at the Application layer of the OSI model.

Telnet only uses TCP as its transport protocol. It uses TCP port 23, and is used to manage a device remotely from the command line. It transits in clear text and should not be used. SSH is a better alternative. Secure Shell (SSH) is used to create an encrypted remote terminal connection

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

Quora > Why does DNS use UDP?

Question #31 of 61

Question ID: 1323038

What is the function of ARP?

A) resolves MAC addresses to IP addresses

B) resolves host names to IP addresses

C) resolves port numbers to IP addresses

D) resolves IP addresses to MAC addresses

Explanation

Address Resolution Protocol (ARP) resolves IP addresses to MAC addresses. It uses a broadcast mechanism to learn the MAC address of a host known only by its IP address. The media access control (MAC) address uniquely identifies a node on a network segment. ARP tables show the relationship of IP addresses to MAC addresses and are located on most devices.

There is no mechanism for translating port numbers to IP addresses. The IP address and port number combination of a source or destination is called a socket.

Domain Name System (DNS) is the service that translates host names to IP addresses. DNS uses UDP when resolution queries are sent to a server by a client, but its uses TCP for zone transfers between DNS servers. According to RFC 1035, UDP is the recommended method for queries. A DNS server provides a centralized database of domain name-to-IP address resolutions on a server or servers that other computers on a network can use for name resolution.

There is currently no service that resolves MAC addresses to IP addresses.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

Lifewire > ARP (Address Resolution Protocol) and Your Computer Network

---

Question #32 of 61

Question ID: 1323009

You need to obtain a version of FireSIGHT that allows you to generate an alert based on an intrusion event with a specific impact flag. What FireSIGHT license do you need?

A) Any
B) Malware
C) FireSIGHT +Protection.
D) FireSIGHT

Explanation

For this ability you need the FireSIGHT +Protection license. Alert generation possibilities are based in the license held. The following table indicates the license needed for various alert generations.

For an alert based on …….	License required
an intrusion event with a specific impact flag	FireSIGHT + Protection
a specific type of discovery event	FireSIGHT
a network-based malware event	Malware
a correlation policy violation	the license required to trigger the policy violation
a connection event	the license required to log the connection
health module status changes	Any

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare deep packet inspection with packet filtering and stateful firewall operation

References:

Cisco > Support > Product Support > Security > Cisco Firepower Management Center > Configuration Guides > FireSIGHT System User Guide Version 5.4.1 > Chapter: Configuring External Alerting

---

Question #33 of 61

Question ID: 1323015

Your main concern with respect to traffic monitoring is to retain total visibility of the traffic at the risk of oversubscription of the ports configured for monitoring. What type of monitoring should you choose?

A) RSPAN
B) SPAN
C) TAP
D) ERSPAN

Explanation

If your concern is no loss of data you should choose a network tap and specifically one operating in normal mode. In normal or breakout mode, the tap (which is a hardware device) ensure no packet loss at the risk of oversubscription of the ports configured for monitoring.

All of the other options are forms of inline monitoring which is done from an existing networks device. All forms of SPAN run the risk of packets being dropped due to congestion on the collecting ports.

Port Mirroring also known as SPAN (Switched Port Analyzer), sends a copy of all network packets seen on one port (or an entire VLAN) to another port, where the packets can be analyzed. In this technique, the collecting and receiving ports are on the same switch.

Remote SPAN (Switched Port Analyzer), sends a copy of all network packets seen on one port (or an entire VLAN) to another port, where the packets can be analyzed. In this technique, the collecting and receiving ports are on different switches.

Encapsulated Remote Switched Port Analyzer (ERSPAN) is a feature used to send traffic for sniffing over layer 3 networks and it works by encapsulating the traffic using a GRE tunnel.

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare inline traffic interrogation and taps or traffic monitoring

References:

What is a Network TAP, Anyway?

Question #34 of 61

Question ID: 1323024

Examine the tcpdump file below:

```
00:0 0:04.569542 IP mcmillan.cisco.com.25463>55.61.125.55.ftp:Flags {S}, seq 3652489461, winn 29200, options {mss 1460, sackOK, TS val 1193145695 ecr0, nop, wscale 7}, length 0
00:0 0:04.569542 IP mcmillan.cisco.com.25463>55.61.125.55.ftp:Flags {S}, seq 3652489461, winn 29200, options {mss 1460, sackOK, TS val 1193146532 ecr0, nop, wscale 7}, length 0
00:0 0:04.569542 IP mcmillan.cisco.com.25463>55.61.125.55.ftp:Flags {S}, seq 3652489461, winn 29200, options {mss 1460, sackOK, TS val 1193146742 ecr0, nop, wscale 7}, length 0
00:0 0:04.569542 IP mcmillan.cisco.com.25463>55.61.125.55.ftp:Flags {S}, seq 3652489461, winn 29200, options {mss 1460, sackOK, TS val 1193146995 ecr0, nop, wscale 7}, length 0
```

What statement is true?

A) The host at 55.61.12.55 is the source.
B) The server is responding with four packets.
C) This is a Telnet transaction.
D) The host `mcmillan.cisco.com` is the source.

Explanation

The sender is the host `mcmillan.cisco.com`. This image shows a capture of the host attempting a connection to an FTP server that is not responding. This is why the sequence numbers of the packets are not incrementing.

The host at 55.61.12.55 is the destination and represents the FTP server, as indicated by the element `55.6.125.55.ftp`.

This is not a Telnet transaction. It would say `55.61.125.55.telnet` if that were the case. The capture shows an FTP transaction.

The server is not responding with four packets, as indicated by the non-incrementing sequence number and the fact that all packets are from `mcmillan.cisco.com` to `55.6.125.55` and never vice versa.

Objective:
Network Intrusion Analysis

Sub-Objective:
Identify key elements in an intrusion from a given PCAP file (Source address; Destination address; Source port; Destination port; Protocols; Payloads)

References:

HYPERLINK "https://www.tecmint.com/12-tcpdump-commands-a-network-sniffer-tool/" TecMint > 12 Tcpdump Commands – A Network Sniffer Tool

---

Question #35 of 61

Question ID: 1323034

When you send a ping packet, what protocol are you using?

A) TCP

B) IP

C) ICMP

D) ARP

Explanation

Internet Control Message Protocol (ICMP) is a diagnostic and error message generating protocol that is part of the TCP/IP suite. Ping is one of the utilities that depends on this protocol.

ICMP operates at the Internet layer of the OSI model. The ping command checks the connection to the router end-to-end at the Network layer. It uses the ICMP protocol to send Echo requests and replies to check connectivity to another network host. To ping the address 110.11.32.3, you should enter the following command:

```
ping 110.11.32.3
```

Internet Protocol (IP) is the protocol in the TCP/IP suite that is responsible for routing and IP addressing. It is connectionless and depends on other parts of the TCP/IP suite for delivery.

Transmission Control Protocol (TCP) is a protocol in the TCP/IP suite responsible for guaranteed delivery. It uses a three-way handshake to establish a connection before any data transfer takes place. Protocols can use either User Datagram (UDP) or TCP to communicate. UDP is connectionless, while TCP is connection-oriented.

Address Resolution Protocol (ARP) is responsible for mapping the hardware address of the hosts on broadcast networks with the TCP/IP address of each host. It uses an ARP broadcast to learn the media access control (MAC) address that goes with the IP address in the packet. The ARP utility allows you to view the ARP cache, which maps each IP address to a physical address. ARP works at the Network layer of the OSI model.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

CloudFlare > What is the ICMP?

Question #36 of 61

Question ID: 1325278

Examine the following ASA system message:

```
%ASA-TM-302015:Built inbound connection TCP 12695364 for outside : 192.168.5.5/36214 to inside 192.198.5.20/80
```

Which statement is FALSE?

A) The source IP is 192.168.5.5.

B) The destination port is 302015.

C) The source port is 36214.

D) The destination IP is 192.168.5.20.

Explanation

The destination port is the number to the right of the / next to the destination IP address of 192.168.5.20. The destination port is 80.

The source IP is the first address, or 192.168.5.5.

The destination IP is the second number, or 192.168.5.20

The source port is the number to the right of the / next to the source IP address of 192.168.5.5. It is 36214.

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

Cisco > Support > Product Support > Security > Cisco ASA 5500-X Series Firewalls > Error and System Messages > Cisco ASA Series Syslog Messages

---

Question #37 of 61

Question ID: 1323046

Which IP address would be found on a host that is unable to connect to the DHCP server?

A) 192.168.5.5

B) 172.16.3.3

C) 200.1.1.5

D) 169.254.1.3

Explanation

When a machine cannot find the DHCP server, it will assign itself an IP address in the 169.254.0.0 range by default. This is a process called Automatic Private IP Addressing (APIPA). It is a good item to note when troubleshooting connectivity issues with a device, because it clearly indicates that:

- The device is set to obtain an address automatically (which could be an error)
- The device is not finding the DHCP server (either its down, unavailable or out of IP addresses)

The 169.254.1.3 address is a valid Automatic Private IP Addressing (APIPA) address. By default, Windows 10 client computers are configured to use an APIPA address if the DHCP server goes down. The addresses in the APIPA range are 169.254.0.0 through 169.254.255.255. These addresses are not routable, and are therefore only usable on the local subnet.

To prevent the use of APIPA addresses, you should change the default settings on the Alternate Configuration tab of the Internet Protocol Version 4 Properties dialog box. On this tab, you can specifically configure a static IP address that the computer can use.

The 200.1.1.5 address is a Class C address in the public range.

The 192.168.5.5 address is a Class C address in the public range.

The 172.16.3.3 address is a Class C address in the public range.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret common artifact elements from an event to identify an alert (IP address (source / destination); Client and server port identity; Process (file or registry); System (API calls) Hashes; URI / URL)

References:

Webopedia > APIPA - Automatic Private IP Addressing

Question #38 of 61

Question ID: 1322996

Examine the following IDS log:

Date	Priority	Description	Source	Destination	Protocol	Event
2013-09-06 18:28:26	2	DNS named version attempt (Attempted Inf...	192.168.56.1:46190	192.168.56.205:53	UDP	Alert
2013-09-06 18:28:25	2	SCAN nmap XMAS (Attempted Information Le...	192.168.56.1:47320	192.168.56.205:20	TCP	Alert
2013-09-06 18:28:25	1	SHELLCODE x86 inc ebx NOOP (Executable c...	192.168.56.1:47361	192.168.56.205:44609	UDP	Alert
2013-09-06 18:28:25	3	ICMP PING (Misc activity)	192.168.56.1:8	192.168.56.205:0	ICMP	Alert
2013-09-06 18:28:25	3	ICMP PING undefined code (Misc activity)	192.168.56.1:8	192.168.56.205:9	ICMP	Alert

Which line number indicates the attacker is sending TCP packets with three flags set?

A) 3

B) 4

C) 1

D) 2

Explanation

The second line indicates a port scan by nmap. The tool output specifies an XMAS attack. An XMAS attack is one in which the attacker sends a TCP packet with three flags set (FIN, PSH and URG) If the attacker receives no response the port is open. If he receives a RST, the port is closed.

A XMAS scan is called that because we say that the malicious packet is “lit up like a XMAS tree”. This packet is used to determine if the port is open or closed. While the same can be determined with a TCP SYN scan, the XMAS scan often returns results faster.

The first line is an attempt to determine the version of DNS in use.

The third line is an attempt at a NOP slide, one way to force a buffer overflow attack.

The fourth line is a suspicious PING.

An XMAS attack is a type of DoS which uses several invalid TCP header flag sets. The TCP header flag byte is comprised of eight flag positions, in the following order [CEUAPRSF]:

- CWR (congestion window reduced) - used in relation to congestion management
- ECN-E (explicit congestion notification - echo) - used in relation to congestion management
- URG (urgent) - causes devices to transmit the flagged packet in priority to other packets
- ACK (acknowledgement) - a confirmation of receipt or of an event
- PSH (push) - triggers any buffered data to be transmitted immediately
- RST (reset) - used to disconnect a current or pending session
- SYN (synchronization) - used to initiate and set up a session
- FIN (finish) - used to gracefully shut down a session

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

IETF > TCP SYN Flooding Attacks and Common Mitigations

Question #39 of 61

Question ID: 1322992

In the following IDS log, what is the destination service?

Severity	Date	Time	Seq ID	Source IP	Source port	Dest IP	Dest Port	Description
6	Oct 10 2018	051552	33536	192.168.5.3	22541	203.6.1.3	53	

A) SMTP

B) DHCP

C) DNS

D) HTTP

Explanation

The destination port number column of the IDS log shows the port number is 53, which is the port number for DNS.

The destination service is not HTTP. That port number would be 80.

The destination service is not SMTP. That port number would be 25.

The destination service is not DHCP. That port number would be 67 or 68.

You should be familiar with the following common protocols and their default ports:

- FTP – 20, 21
- SSH, SFTP – 22
- TELNET – 23
- SMTP – 25
- DNS – 53
- DHCP – 67, 68
- TFTP – 69
- HTTP – 80
- POP3 – 110
- NTP – 123
- NetBIOS – 137–139
- IMAP – 143
- SNMP – 161
- LDAP – 389
- SSL and HTTPS – 443
- LDAPS – 636
- MS SQL Server – 1433
- HTTPS- 443

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

Cisco Press > Articles > Cisco Network Technology > General Networking > Intrusion Detection: Cisco IDS Overview

---

Question #40 of 61

Question ID: 1323042

You are investigating suspicious communication between two devices in your environment. The source socket is 205.16.3.74:5696 and the destination socket is 192.168.5.3:53. What service should you suspect is under attack?

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

Explanation

You should suspect a DNS attack, most likely an attempt at an unauthorized zone transfer. The destination port is port 53. Unless there is a non-default service running on that port, that port is used for DNS.

You should not suspect DHCP. By default, DHCP uses ports 67 and 68., not 53.

You should not suspect HTTP. By default, HTTP uses port 80.

You should not suspect NTP. By default, NTP uses port 123.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret common artifact elements from an event to identify an alert (IP address (source / destination); Client and server port identity; Process (file or registry); System (API calls) Hashes; URI / URL)

References:

Cisco Security > DNS Best Practices, Network Protections, and Attack Identification

---

Question #41 of 61

Question ID: 1323036

Which protocol does NOT transmit information (such as usernames and credentials) in clear text?

A) FTP

B) SNMP

C) TFTP

D) HTTPS

Explanation

Hypertext Transfer Protocol Secure (HTTPS) uses Secure Sockets Layer (SSL) to encrypt HTTP traffic. HTTPS only supports the encryption of HTTP traffic. Secure Sockets Layer (SSL) supports an encryption key length of 40 bits or 128 bits. SSL 3.0 is the current version of SSL. Transport Layer Security (TLS) encrypts the messages transmitted between two authenticated computers, preventing third parties from reading the messages. TLS is the protocol being used when Secure Sockets Layer (SSL) is implemented.

Hypertext Transfer Protocol (HTTP) transmits information in clear text. HTTP uses port 80, and HTTPS uses port 443.

File Transfer Protocol (FTP) is a standard Internet protocol used to exchange files between computers on the Internet. Like HTTP, which transfers Web pages that can be displayed and related files, FTP transmits data in clear text. However, Secure FTP (SFTP) is a secure alternative to FTP that uses TLS/SSL to encrypt transmissions.

Trivial File Transfer Protocol (TFTP) is a simple protocol used to move files between machines on different networks implementing UDP. It is a connectionless version of the File Transfer Protocol (FTP) that lacks many of the features of FTP.

Simple Mail Transfer Protocol (SMTP) is used to transfer e-mail messages from e-mail clients to e-mail servers. SMTP is also used to transfer e-mail messages between e-mail servers.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

WolfSSL > Differences between SSL and TLS Protocol Versions

Question #42 of 61

Question ID: 1323013

Which of the following occurs at Layer 7 of the OSI model?

A) deep packet inspection

B) stateful firewall operation

C) packet filtering

D) VLANs

Explanation

Deep packet inspection is performed by application firewalls, which operate at Layer 7 (the Application layer) of the OSI model. This is the examination of the actual data portion of the IP packet. An application firewall is typically integrated into another type of firewall to filter traffic that is traveling at the Application layer of the Open Systems Interconnection (OSI) model. An embedded firewall is typically implemented as a component of a hardware device, such as a switch or a router.

Stateful firewall operation occurs at Layer 3. This type of inspection monitors the TCP three-way handshake which occurs at Layer 3. Stateful firewalls, monitor the state of each TCP connection as well. When traffic is encountered, a stateful firewall first examines a packet to see if it is the result of a previous connection. Information about previous connections is maintained in the state table.

With a stateful firewall, a packet is allowed if it is a response to a previous connection. If the state table holds no information about the packet, the packet is compared to the access control list (ACL). Depending on the ACL, the packet will be forwarded to the appropriate host or dropped completely.

Packer filtering can be done based on IP addresses and port numbers. That means this type of filtering occurs at Layers 3 and 4.

VLANs filter traffic by MAC addresses, and as such operate at Layer 2 of the OSI model.

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare deep packet inspection with packet filtering and stateful firewall operation

References:

BloggersPath > What Is Deep Packet Inspection And Its Advantages and Disadvantages?

Question #43 of 61

Question ID: 1323011

Which of the following is NOT an element examined by a stateful or traditional firewall?

A) protocol information
B) source and destination port number
C) data
D) source and destination IP address

Explanation

Stateful or traditional firewalls do not perform data inspection. Data inspection requires an Application layer firewall.

Traditional firewalls examine all of the following:

- protocol information
- source and destination port number
- source and destination IP address

Stateful firewalls monitor the state of each TCP connection as well. When traffic is encountered, a stateful firewall first examines a packet to see if it is the result of a previous connection. Information about previous connections is maintained in the state table.

With a stateful firewall, a packet is allowed if it is a response to a previous connection. If the state table holds no information about the packet, the packet is compared to the access control list (ACL). Depending on the ACL, the packet will be forwarded to the appropriate host or dropped completely.

Stateful firewalls can be used to track connectionless protocols, such as the User Datagram Protocol (UDP), because they examine more than the packet header.

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare deep packet inspection with packet filtering and stateful firewall operation

References:

CertificationKits > CCNA Security: Stateful Firewall Overview

---

Question #44 of 61

Question ID: 1323016

Which data type is captured by a sniffer but not by a Net flow export?

A) source and destination IP addresses
B) source and destination ports used
C) source and destination MAC address
D) payload

Explanation

Netflow records traffic flows that are distinguished by the following characteristics shared by each end of a connection:

- Ingress interface (SNMP ifIndex)
- Source IP address

- Destination IP address
- IP protocol
- Source port for UDP or TCP, 0 for other protocols
- Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
- IP Type of Service

Netflow analysis focuses on the conversation and the endpoints rather than the payload. It collects less information than full packet capture but is faster and is the tool of choice when performing network intelligence activates.

Full packet capture provides the details needed when focusing on the payload such as when a malware attack is underway but packet capture probes have to be deployed in targeted locations which can be cumbersome and costly. The maintenance demands of probes also limit the deployments on a large scale. As a result, it is usually impossible to gain enterprise wide visibility using packet analyzers by themselves.

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare inline traffic interrogation and taps or traffic monitoring

References:

Products & Services>Cisco IOS and NX-OS Software>Cisco IOS Technologies>Management Instrumentation>Cisco IOS NetFlow

---

Question #45 of 61

Question ID: 1323007

An employee visits a malicious website, and the IDS alerted you. What is this called?

A) False positive
B) False negative
C) True positive
D) True negative

Explanation

A true positive means the IDS correctly (True) detected an issue (positive).

A false negative means the system made a mistake (False) and missed (negative) an issue.

A true negative means the IDS correctly (True) did not detect an issue (negative).

A false positive means the IDS mistakenly (False) identified an attack (positive).

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare impact and no impact for these items (False positive; False negative; True positive; True negative; Benign)

References:

Live Science > What Are False Positives and False Negatives?

Question #46 of 61

Question ID: 1323044

Which of the following can be used to verify the integrity of a document?

A) S boxes
B) IVs
C) encryption keys
D) message digests

Explanation

Message digests are generated by hashing algorithms. These values can be regenerated later, and if the values match, it proves that the data has not changed.

Encryption keys are used to encrypt, and decrypt data not produce message digests or perform integrity verification.

S boxes are parts of encryption algorithms and are not used to verify integrity.

Initialization vectors (IVs) are used to introduce randomness to the encryption process and are not used to verify integrity.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret common artifact elements from an event to identify an alert (IP address (source / destination); Client and server port identity; Process (file or registry); System (API calls) Hashes; URI / URL)

References:

Techopedia > Message Digest

Question #47 of 61

Question ID: 1323027

Using the OSI model as a reference, where would you find the source and destination IP address in a captured packet?

A) Layer 3 header

B) Layer 4 header

C) Layer 1 header

D) Layer 2 header

Explanation

The source and destination address are found in the Layer 3 header. This includes both IPv4 and IPv6 addresses.

The Layer 4 header contains source and destination port numbers. These include both TCP and UDP ports.

The Layer 2 header contains source and destination MAC addresses. This section of the packet is also called the Ethernet frame, and the addresses are sometimes called Ethernet addresses.

The Layer 1 or PHY header is where physical information is contained.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

Cisco Press > Articles > Cisco Network Technology > General Networking > Internet Addressing and Routing First Step > IP Header Format

---

Question #48 of 61

Question ID: 1323021

Which of the following Wireshark filters filters by IP subnet?

A) `ip.addr==192.168.1.0/24`

B) `http.user_agent contains Firefox`

C) `!ip.addr==192.168.1.2`

D) `eth.addr == 00:60:e0:53:13:d5`

Explanation

The filter `ip.addr==192.168.1.0/24` filters for any IP address in the 192.168.1.0 255.255.255.0 network.

The filter `!ip.addr==192.168.1.2` excludes the IP address 192.168/.1.2. The `!` character is the key.

The filter `eth.addr == 00:60:e0:53:13:d5` filters for the MAC address 00:60:e0:53:13:d5.

The filter `http.user_agent` filters for user agents containing Firefox.

Objective:
Network Intrusion Analysis

Sub-Objective:
Identify key elements in an intrusion from a given PCAP file (Source address; Destination address; Source port; Destination port; Protocols; Payloads)

References:

LinuxHint > How to Filter By IP in Wireshark

Question #49 of 61

Question ID: 1323008

The IDS alerted you there was an attack when there was none. What is this called?

A) False negative
B) False positive
C) True positive
D) True negative

Explanation

A false positive means the IDS mistakenly (False) identified an attack (positive).

A true positive means the IDS correctly (True) detected an issue (positive).

A false negative means the system made a mistake (False) and missed (negative) an issue.

A true negative means the IDS correctly (True) did not detect an issue (negative).

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare impact and no impact for these items (False positive; False negative; True positive; True negative; Benign)

References:

Live Science > What Are False Positives and False Negatives?

Question #50 of 61

Question ID: 1323012

You need to examine information at Layer 7 in packets. What type of firewall do you need?

A) stateful
B) application
C) stateless packer filtering
D) packer filtering

Explanation

Stateful or traditional firewalls do not perform data inspection. This requires an application firewall. Data inspection causes this firewall to have the most impact on performance. An application firewall is an example of a component added to a hardware firewall. An application firewall is designed to filter traffic at the Application layer of the Open Systems Interconnection (OSI) model.

Traditional firewalls examine the following:

- protocol information
- source and destination port number

- source and destination IP address

An embedded firewall is integrated into a router.

A software firewall is installed on a server operating system, such as Windows Server 2016 or Linux.

A hardware firewall is a black box device, which is designed to be deployed on a network with a minimum of configuration and installation effort.

Stateful firewalls monitor the state of each TCP connection as well. When traffic is encountered, a stateful firewall first examines a packet to see if it is the result of a previous connection. Information about previous connections is maintained in the state table.

Stateful firewalls can be used to track connectionless protocols, such as the User Datagram Protocol (UDP), because they examine more than the packet header.

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare deep packet inspection with packet filtering and stateful firewall operation

References:

f5.com > What is an Application Firewall?

Question #51 of 61

Question ID: 1323049

Which hashing algorithm is the strongest?

A) MD5
B) SHA-256
C) SHA-1
D) SHA-512

Explanation

SHA-512 is a more secure version of SHA-256 and differs only in the number of rounds of computation.

MD5 is the least secure of the listed hashing algorithms. 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.

SHA-1 is the first version of SHA and is the least secure version of SHA hashing algorithm. The MD5 algorithm produces 128-bit checksums, and SHA produces 160-bit checksums.

The SHA-256 hashing algorithm is part of the SHA-2 family. SHA-256, also referred to as SHA-2, is a newer version of SHA and uses 256-bit checksums.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret common artifact elements from an event to identify an alert (IP address (source / destination); Client and server port identity; Process (file or registry); System (API calls) Hashes; URI / URL)

References:

MTL > Scripts > SHA-256 Cryptographic Hash Algorithm

Question #52 of 61

Question ID: 1323025

Which of the following Wireshark filter filters for the MAC address?

A) `gateway host <host>`

B) `!ip.addr==192.168.1.2`

C) `eth.addr == 00:60:e0:53:13:d5`

D) `ip.addr==<addr>or ip.host==<host>`

Explanation

The filter `eth.addr == 00:60:e0:53:13:d5` filters for the MAC address 00:60:e0:53:13:d5.

The filter `ip.addr==<addr>or ip.host==<host>` filters for a host address or a host name.

The filter `!ip.addr==192.168.1.2` excludes the IP address 192.168/.1.2. The ! character is the key.

The primitive `gateway host <host>` filters for packets that used a host as a gateway.

Objective:
Network Intrusion Analysis

Sub-Objective:
Identify key elements in an intrusion from a given PCAP file (Source address; Destination address; Source port; Destination port; Protocols; Payloads)

References:

HYPERLINK "https://linuxhint.com/filter_by_ip_wireshark/" LinuxHint > How to Filter By IP in Wireshark

---

Question #53 of 61

Question ID: 1323037

Which of the following would one NOT expect to find in a packet capture of an HTTP packet?

A) referrer header

B) SYN flag

C) user agent

D) host

Explanation

SYN flags are seen in TCP packets that are part of the three-way TCP handshake. Once the connection setup is complete, the HTTP packets will not have this element.

Among the elements in an HTTP packets are the following:

- user agent - software (a software agent) that is acting on behalf of a user
- referrer header - URL data from an HTTP header field identifying the Web link used to direct users to a Web page.
- host - sending device

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

Techopedia > Referrer

Question #54 of 61

Question ID: 1323028

Which of the following is a public IPv6 address?

A) FE80::2

B) 2001:420:1101:1::a

C) FD::4

D) FF02::88

Explanation

The address 2001:420:1101:1::a is a global unicast (reached on the Internet) address. IPv6 globally routable unicast addresses start with the first four characters in the range of 2000 to 3999. This address type is equivalent to IPv4's public address.

An IPv6 address is shortened according to the following rules:

- Remove leading zeros.
- Remove the consecutive fields of zeros with double colons (::).
- Use the double colon (::) only once.

Because you can eliminate any leading zeros within a hextet, :0055: can simply be :55:.

Because you can eliminate consecutive hextets of all 0s only once with an address, 2001:0420:1101:0001:0000:0000:0000:a can be written 2001:420:1101:1::a.

IPv6 addresses that start with FE80 are called link-local addresses, and are the equivalent of APIPA addresses (169.x addresses) Link-local addresses are used for communication among IPv6 hosts on a link (broadcast segment) only. These addresses are not routable. An IPv6 link-local address is also used on each IPv6 interface.

IPv6 addresses that start with FD are unique-local addresses. They are the equivalent of IPv4 private addresses.

IPv6 addresses that start with FF are IPv6 multicast addresses. Multicast addresses are used to send to groups of computers as defined by a multicast address.

IPv6 addresses are 16 bytes, or 128 bits in length. The following are examples of valid IPv6 addresses:

::10.2.4.1 is an example of an IPv4-compatible IPv6 address, where the first 12 bytes (96 bits) of the address are set to 0.

:: is the IPv6 "unspecified address." It is a unicast address not assigned to any interface, and is used by DHCP-dependent host prior to allocating a real IPv6 address.

2001:0:42:3:ff::1 is a valid IP address, with the :: representing two segments (4 bytes) of compressed zeros.

2001:42:4:0:0:1:34:0 is a valid IP address, with only the leading zeros of each segment truncated.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

Tutorials Point > IPv6 - Address Types & Formats

Question #55 of 61

Question ID: 1323029

Which of the following represents the software that is acting on behalf of a user?

A) user agent
B) representative agent field
C) host field
D) type field
E) cookie

Explanation

The user agent is an HTTP header inside the software that is acting on behalf of a user. For example, it might indicate the browser type and capability. The User-Agent (UA) string is intended to identify devices requesting online content, which helps with intrusion analysis.

The host field indicates the domain name of the server (for virtual hosting), and the TCP port number on which the server is listening.

Other examples of HHTP header fields are:

- Accept - Media type(s) that is(/are) acceptable for the response
- Content-Length - The length of the request body in octets (8-bit bytes)

- From - The email address of the user making the request
- Referrer - The address of the previous web page from which a link to the currently requested page was followed
- Host - The domain name of the server (for virtual hosting), and the TCP port number on which the server is listening
- Date - The date and time that the message was originated
- Authorization - Authentication credentials for HTTP authentication

Cookies are text files with information with stored information about the user. They are not HTTP header fields.

There is no representative agent field in the HTTP header.

There is no type field in the HTTP header. The Type field is the first field in an Internet Control Message Protocol (ICMP) header, and is used to indicate the function or purpose of the communication. The Type field references items known as control messages. A control message is the function or purpose of the ICMP communication. Common examples of Types are:

- 8 for Echo Request
- 0 for Echo Reply
- 11 for Timeout Exceeded
- 3 for Destination Unreachable

There are about sixteen formally defined Types for ICMP. The remaining fields in the ICMP header are Code, Checksum, and Rest of Header. The Code field is used to define or reference a sub-type (i.e., a more specific sub-meaning of the indicated control message). The Checksum field is used to verify that the ICMP communication was not corrupted in transit. The Rest of Header field may hold values when needed based on the Type, or is set to all zeros when unused. For example, a Type 5 Redirect will place an IP address in the Rest of Header field.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret the fields in protocol headers as related to intrusion analysis (Ethernet frame; IPv4; IPv6; TCP; UDP; ICMP; DNS; SMTP/POP3/IMAP; HTTP/HTTPS/HTTP2; ARP)

References:

Wiki > List of HTTP header fields

Question #56 of 61

Question ID: 1323010

Which of the following activities would be a part of retrospective analysis?

A) using historical data to identify an infected host

B) scanning for vulnerabilities with NESSUS

C) attempting to exploit a vulnerability you found

D) using nmap to determine open ports

Explanation

Whenever you use historical data from logs to help identify a breach of any sort, you are engaged in retrospective analysis. A retrospective analysis is performed when the outcome of an event is already known, such as attempting to discover when identified malware first entered your system. GigaStor Security Forensics is another example of a tool that performs retrospective analysis.

Using nmap to determine open ports is a part of network discovery stage of a penetration test. By identifying the open ports, potential attacks may be identified before they occur.

Scanning for vulnerabilities with NESSUS is a part of a vulnerability test.

Attempting to exploit a vulnerability is a later stage in the penetration test.

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare deep packet inspection with packet filtering and stateful firewall operation

References:

HYPERLINK "http://nextgigsystems.com/network_tools/retrospective_net_analysis.html" NextGig > Retrospective Network Analysis

Question #57 of 61

Question ID: 1323001

You suspect there is a threat against your DNS server that makes use of the query process. What type of traffic should you monitor?

A) TCP

B) UDP

C) ARP

D) HTTP

Explanation

You should monitor UDP traffic. DNS servers communicate queries using UDP. In one example of a DNS attack type that makes use of UDP (but not the only one), a malicious individual queries your DNS server for a record unknown to the DNS server. The server then does what it is designed to do, which is forward that query to the domain name listed in the record. In this attack, the listed domain is a malicious domain, and the malicious DNS server responds with a record, but within the record is hidden malware that infects the DNS server.

Using DNS server logs, you can identify this type of communication by performing retrospective analysis to determine when the malware file entered the network.

Many security products maintain a list of known problematic DNS domains. They scan the DNS records (which can be huge in size) for matches and alert you to any communication with a known problem domain.

TCP is not used by DNS for queries. Query traffic will fit into a UDP packet. Because UDP is much faster than TCP, it was chosen as the transport protocol for queries. Reliability is provided by DNS at the application layer.

ARP is used to resolve IP addresses to MAC addresses. It is not a protocol used in DNS query communication.

HTTP is a protocol used by web servers and would be of no use in mapping to find a threat actor that involves DNS servers. However, HTTP headers can be used to map HTTP attacks to their source.

HTTP logs and DNS logs can be correlated to one another. The DNS log will show the domain name and IP address and by matching those to the HTTP log we can identify the contents of the HTTP header to identity the attack type.

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

HYPERLINK "https://securelist.com/use-of-dns-tunneling-for-cc-communications/78203/" Kapersky > Use of DNS Tunneling for C&C Communications

Question #58 of 61

Question ID: 1322999

Which section of the IP header defines the entire packet size in bytes, including header and data?

A) Total length

B) Version

C) Identification

D) IP address

Explanation

The total length field in the IP header indicates the entire packet size in bytes, including header and data. While this is not the most useful field in intrusion analysis, it is good to know what it describes.

The first header field in an IP packet is the four-bit version field. For IPv4, this is always equal to 4.

The source and destination IP address fields contain the source and destination IP addresses.

The identification field is primarily used for uniquely identifying the group of fragments of a single IP datagram.

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

Cisco Press > Articles > Cisco Network Technology > General Networking > Internet Addressing and Routing First Step > IP Header Format

---

Question #59 of 61

Question ID: 1323018

Which statement is true with regard to SPAN and network taps?

A) Network TAPs have no IP address
B) The switch treats SPAN data with a higher priority than to-port data
C) The SPAN port should be used only for relatively high-throughput situations
D) TAPs alter the time relationships of frames

Explanation

Network test access points (TAPs) have no IP address and no MAC address. Therefore, they cannot be hacked.

TAPs are passive hardware devices that send a copy of the frame to the analyzer. A network TAP is an external monitoring device that mirrors the traffic that passes between two network nodes. A TAPs are inserted at a specific point in the network to monitor data.

The switch treats port mirroring (SPAN) data with a lower priority than to-port data, which is why is a high throughput scenario the switch might drop some packets before they get sent to the port where the analyzer resides. The SPAN feature, which is sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer.

TAPs do not alter the time relationships of frames. Spacing and response times are especially important with VoIP.

Because of the low priority the switch places on SPAN traffic, you should use the SPAN port only for relatively low-throughput situations.

Objective:
Network Intrusion Analysis

Sub-Objective:
Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic

References:

Garland Technology > Network Test Access Point (TAP) and Port Mirroring (SPAN)

Question #60 of 61

Question ID: 1323000

You are examining the log on a device that indicates the host device received a packet and then constructed and sent an identical packet, with the exception of the source IP address. What type of log are you viewing?

A) NAC device
B) antivirus appliance log
C) proxy log
D) firewall log

Explanation

Since a proxy server makes web connections on behalf of the host, it is common to find this type of activity in its log.

This activity would not be found in an antivirus appliance log. What would be found are events revolving around detection and elimination of malware in the network (in the case of an appliance) and of the host (in the case of a host-based antivirus).

This activity would not be found in a Network access control (NAC) device. What would be found are events required to assess the security of a device prior to allowing the device access to the network.

This activity would not be found in a firewall log. What would be found are events indicating the blocking or allowing of traffic based on configured firewall policies.

Objective:
Network Intrusion Analysis

Sub-Objective:
Map the provided events to source technologies (IDS/IPS; Firewall; Network application control; Proxy logs; Antivirus; Transaction data (NetFlow))

References:

Vanimpe > Proxy server logs for incident response

Question #61 of 61

Question ID: 1323045

What event artifact cannot be obtained from a URI?

A) host info

B) HTTP GET request for a file

C) user info

D) file hash

Explanation

The hash of the file is not available in the URI.

The Uniform Resource Identifier (URI) can contain the following:

- An optional userinfo subcomponent that may consist of a user name and an optional password, preceded by a colon
- A host subcomponent, consisting of either a registered name (including but not limited to a hostname) or an IP address
- A query component preceded by a question mark (possibly an HTTP request for a file)

The Uniform Resource Locator (URL) is the string used to locate the site. For example, www.google.com is a URL. It can be scanned for known malicious sites based on reputation.

Objective:
Network Intrusion Analysis

Sub-Objective:
Interpret common artifact elements from an event to identify an alert (IP address (source / destination); Client and server port identity; Process (file or registry); System (API calls) Hashes; URI / URL)

References:

Ionos > URI: The Uniform Resource Identifier Explained