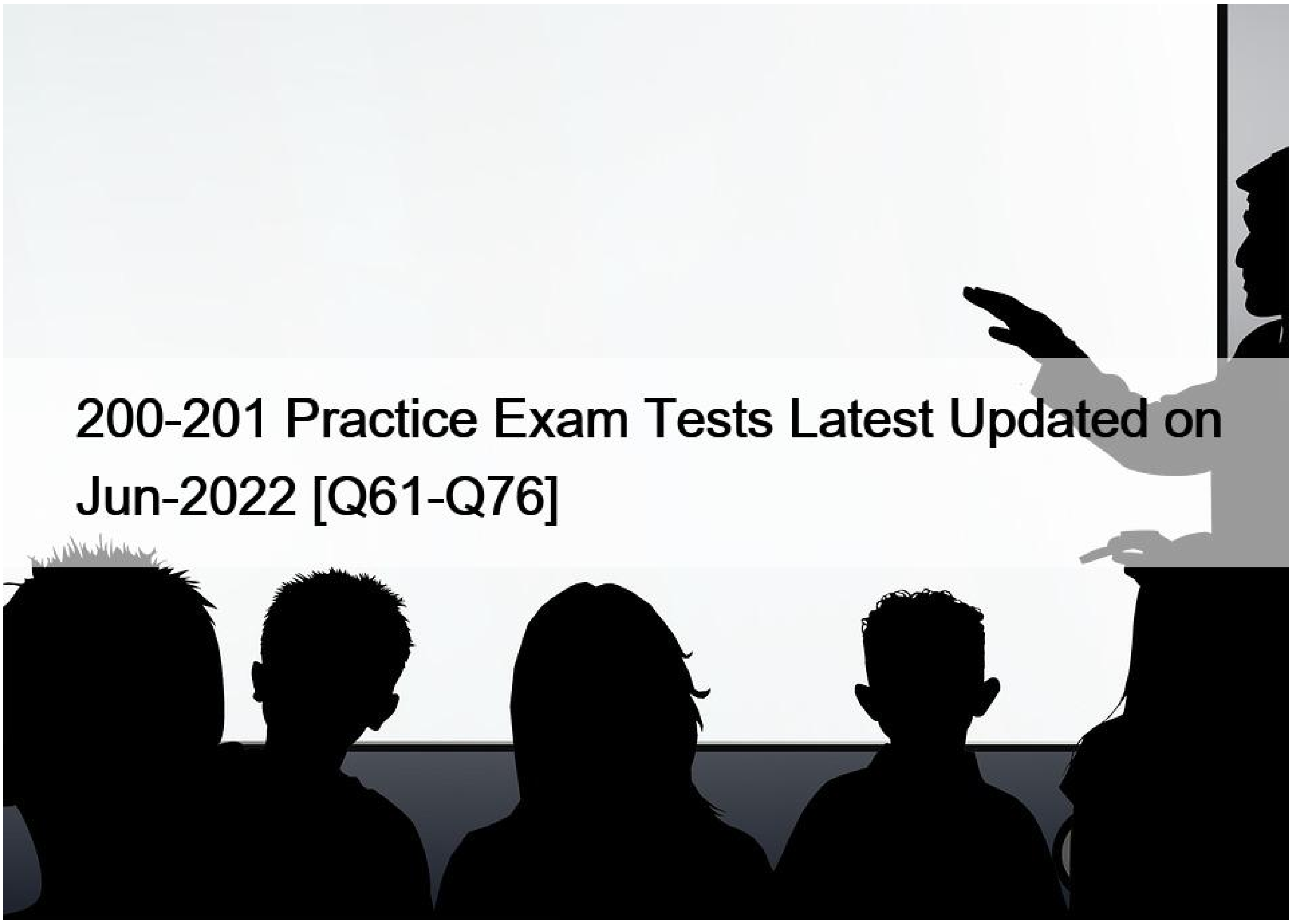
200-201 Practice Exam Tests Latest Updated on Jun-2022 [Q61-Q76



200-201 Practice Exam Tests Latest Updated on Jun-2022
Pass 200-201 Exam in First Attempt Guaranteed Dumps!

NO.61 Which security technology allows only a set of pre-approved applications to run on a system?
* application-level blacklisting
* host-based IPS
* application-level whitelisting
* antivirus

NO.62 Which two elements are used for profiling a network? (Choose two.)
* session duration
* total throughput
* running processes
* listening ports
* OS fingerprint

Explanation

A network profile should include some important elements, such as the following:

Total throughput &#8211; the amount of data passing from a given source to a given destination in a given period of time Session duration &#8211; the time between the establishment of a data flow and its termination Ports used &#8211; a list of TCP or UDP processes that are available to accept data Critical asset address space &#8211; the IP addresses or the logical location of essential systems or data Profiling data are data that system has gathered, these data helps for incident response and to detect incident Network profiling = throughput, sessions duration, port used, Critical Asset Address Space Host profiling = Listening ports, logged in accounts, running processes, running tasks,applications

NO.63 Which type of data consists of connection level, application-specific records generated from network traffic?
* transaction data
* location data
* statistical data
* alert data
Section: Security Monitoring

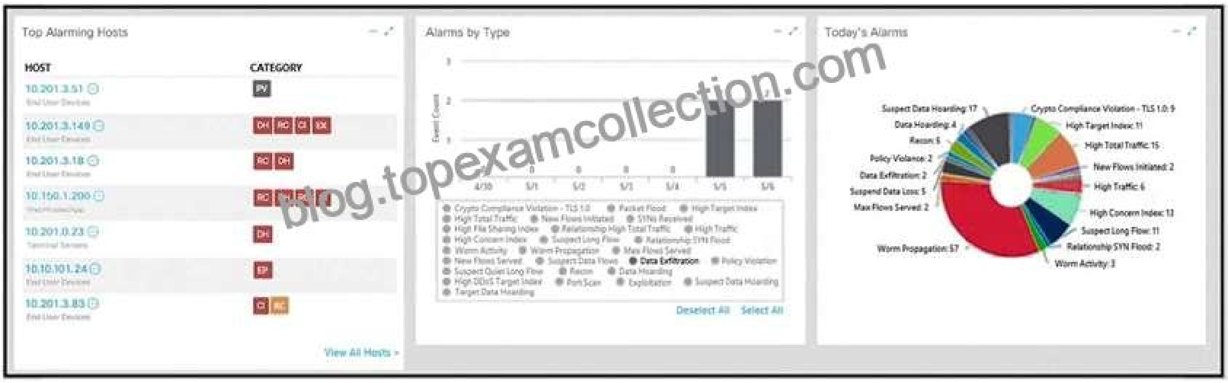
Explanation/Reference:

NO.64 You have identified a malicious file in a sandbox analysis tool. Which piece of file information from the analysis is needed to search for additional downloads of this file by other hosts?
* file name
* file hash value
* file type
* file size

NO.65 What makes HTTPS traffic difficult to monitor?
* SSL interception
* packet header size
* signature detection time
* encryption

NO.66 What is personally identifiable information that must be safeguarded from unauthorized access?
* date of birth
* driver&#8217;s license number
* gender
* zip code

NO.67



Top Alarming Hosts

HOST	CATEGORY
10.201.3.51 End User Devices	PV
10.201.3.149 End User Devices	DH RC CI EX
10.201.3.18 End User Devices	RC DH
10.150.1.200 [illegible]	RC [illegible]
10.201.0.23 Terminal Servers	DH
10.10.101.24 End User Devices	EP
10.201.3.83 End User Devices	CI RC

View All Hosts »

Refer to the exhibit. What is the potential threat identified in this Stealthwatch dashboard?
* A policy violation is active for host 10.10.101.24.
* A host on the network is sending a DDoS attack to another inside host.
* There are two active data exfiltration alerts.
* A policy violation is active for host 10.201.3.149.
Section: Host-Based Analysis

NO.68 How does an attack surface differ from an attack vector?
* An attack vector recognizes the potential outcomes of an attack, and the attack surface is choosing a method of an attack.
* An attack surface identifies vulnerable parts for an attack, and an attack vector specifies which attacks are feasible to those parts.
* An attack surface mitigates external vulnerabilities, and an attack vector identifies mitigation techniques and possible workarounds.
* An attack vector matches components that can be exploited, and an attack surface classifies the potential path for exploitation

NO.69 A security incident occurred with the potential of impacting business services. Who performs the attack?
* malware author
* threat actor
* bug bounty hunter
* direct competitor

NO.70 An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group.

What is the initial event called in the NIST SP800-61?
* online assault
* precursor
* trigger
* instigator
Explanation

A precursor is a sign that a cyber-attack is about to occur on a system or network. An indicator is the actual alerts that are generated as an attack is happening. Therefore, as a security professional, it&#8217;s important to know where you can find both precursor and indicator sources of information.

The following are common sources of precursor and indicator information:

* Security Information and Event Management (SIEM)

* Anti-virus and anti-spam software

* File integrity checking applications/software

* Logs from various sources (operating systems, devices, and applications)

* People who report a security incident

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NO.71 One of the objectives of information security is to protect the CIA of information and systems.

What does CIA mean in this context?
* confidentiality, identity, and authorization
* confidentiality, integrity, and authorization
* confidentiality, identity, and availability
* confidentiality, integrity, and availability
Section: Security Concepts

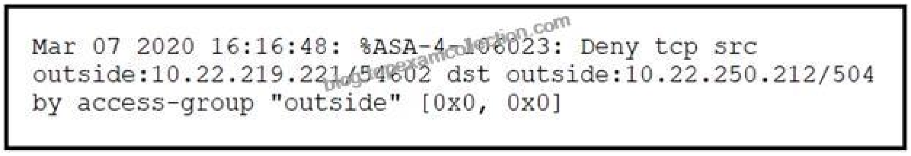
NO.72 A malicious file has been identified in a sandbox analysis tool.

Which piece of information is needed to search for additional downloads of this file by other hosts?
* file type
* file size
* file name
* file hash value

NO.73 What is the practice of giving an employee access to only the resources needed to accomplish their job?
* principle of least privilege
* organizational separation
* separation of duties
* need to know principle
Section: Security Concepts

NO.74 What is a difference between SIEM and SOAR?
* SOAR predicts and prevents security alerts, while SIEM checks attack patterns and applies the mitigation.
* SlEM&#8217;s primary function is to collect and detect anomalies, while SOAR is more focused on security operations automation and response.
* SIEM predicts and prevents security alerts, while SOAR checks attack patterns and applies the mitigation.
* SOAR&#8217;s primary function is to collect and detect anomalies, while SIEM is more focused on security operations automation and response.

NO.75 Refer to the exhibit.



```
Mar 07 2020 16:16:48: %ASA-4-106023: Deny tcp src
outside:10.22.219.221/54602 dst outside:10.22.250.212/504
by access-group "outside" [0x0, 0x0]
```

Which technology generates this log?
* NetFlow
* IDS
* web proxy
* firewall

NO.76 An analyst is exploring the functionality of different operating systems.

What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?
* queries Linux devices that have Microsoft Services for Linux installed

* deploys Windows Operating Systems in an automated fashion
* is an efficient tool for working with Active Directory
* has a Common Information Model, which describes installed hardware and software