**FRAGE 1 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 01**

1. What is the goal of distributed Denial-of-Service attacks?
2. What do they have in common with regular Denial-of-Service attacks?
3. Describe the major difference between distributed Denial-of-Service attacks and distributed Denial-of-Service attacks.
4. The goal of distributed Denial-of-Service attacks is to disrupt a service / render it unavailable (1P).
5. They have this goal in common with regular Denial-of-Service attacks. (1P)
6. Regular Denial-of-Service attacks carry out attacks from single systems (2P), whereas distributed Denial-of-Service attacks use as many attacking systems as possible (2P).

**FRAGE 2 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 01**

Name the individual steps that are missing from the general network forensics process depicted.

2 Collection, 3 Preservation, 4 Examination, 5a Analysis and 5b Investigation, 6 Presentation (1P each)

**FRAGE 3 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 01**

Define "network forensics".

Network forensics is the capture, recording, (2P for this aspect) and analysis (2P) of network events (2P) in order to discover the source of security attacks (1P) or other security incidents (1P).

**FRAGE 4 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 01**

During performance monitoring, it is noticed that a web server is under an unusual amount of system load.

1. Name an attack that can be the cause of this.
2. Name and describe a mitigation technique that can keep the web service operational for regular users.
3. What is a precondition for the mitigation technique?
4. (Distributed) Denial-of-Service attack (2P).
5. Mitigation can be carried out by scrubbing (2P), meaning that illegitimate requests are identified and ignored/dropped before reaching the server(2P).
6. Precondition is the correct identification of malicious requests (2P).

Alternative answer b) outscaling the attack (2P) by allocating sufficient resources (2P) to handle the requests.

Alternative answer c) Precondition for this is the scalability (2P) of the server system based on the design of the underlying infrastructure.

**FRAGE 5 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 01**

1. Name a scenario with a concrete target in which a security incident can lead to a reasonable countermeasure.
2. Name an appropriate counteraction and indicate how the countermeasure is effective against the type of scenario.
3. The investigation of a spear phishing (3P) incident against an employee (1P) (Other answers acceptable).
4. This can lead to the establishment of personnel training programs (3P) that leads to an in increased awareness in endangered personnel (3P). (Other answers acceptable. 3P scenario, 1P target, 3P counteraction, 3P how the counteraction is effective.)

**FRAGE 6 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 01**

Describe the difference between an alert generated by an IDS, a security event, and a security incident and illustrate the differences by means of an example.

A security alert is raw output from a sensor (IDS) (2P).

It is only an actual security event if it is not a false positive (2P).

It only becomes a security incident if an actual policy is violated. (2P).

An example for this is the (technically legitimate) access to a system by a user whose credentials should have expired (2P example), which is a security incident, since it violates a standing policy. (2P correct classification) (other answers are acceptable.)

**FRAGE 7 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 02**

A network-based application wants to transmit data to another application.

1. In what units of information is this data encapsulated when using the TCP/IP stack before it is sent as bits on a physical connection?
2. Which information is added at each step?
3. The data are wrapped into segments (1P). These segments are then wrapped into packets (1P). These packets are then wrapped into frames (1P).
4. Segments contain process information (1P) in the form of port numbers, while packets contain the (recipient and sender) system's address (1P). Frames contain error detection and correction data (1P).

**FRAGE 8 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 02**

Distinguish connection-oriented protocols from connectionless protocols.

1. How is the data exchanged?
2. Who communicates with whom?
3. Connection-oriented protocols provide a stream-oriented communication channel (2P), while connectionless protocols transport individual messages / datagrams (2P).
4. Connection-oriented protocols exchange data between two peers (1P), while connectionless protocols transmit the messages from one peer to one or more recipients (1P).

**FRAGE 9 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 02**

Distinguish the internet layer from the link layer.

1. What is their chief concern?
2. Which elements are exchanged on each layer?
3. The chief objective of the internet layer is to interconnect systems that are not necessarily directly connected / adjacent to each other (2P). The link layer provides a reliable (2P) connection between adjacent (2P) systems.
4. The internet layer transports packets (1P), while the link layer transports frames(1P).

**FRAGE 10 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 02**

The IEEE 802 series of standards operates on a wide variety of hardware, from radio communication to copper cables. Which two goals of the layered network architecture were achieved, so that this makes no difference for network applications? Explain your answer.

Transparency (1P), because higher level protocols like IP can use the services of these protocols without any change (3P), and Independence from physical conditions (1P), because the higher level protocol works over both physical transmission techniques (3P).

**FRAGE 11 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 02**

Modern networks are designed to implement a layered architecture.

1. Name and describe a goal of this approach.
2. Name a concrete network protocol and describe how it fulfills this goal.
3. Separation of concerns (2P - name) as a goal implies that independent teams can work on individual aspects of a new protocol (3P - description).
4. The IPv6 Protocol (2P example name) has been developed as a means to address specific problems of IPv4 while protocols that run on top of (for example TCP) or below (for example Ethernet) IPv4 are essentially unaffected (3P justification).

**FRAGE 12 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 02**

RFC 1772 obsoletes RFC 1655 and is a draft standard, while RFC 1655 is a proposed standard.

1. Which RFC is newer? Justify your answer.
2. Which RFC is more likely to be in used in practice? Justify your answer.
3. Which RFC should be used for new implementations? Justify your answer.
4. RFC 1772 is the newer RFC (1P), because the number is higher (2P).
5. RFC 1655 is more likely to be encountered in practice (1P), since its status as a "proposed standard" indicates that it is already widely adapted in practice (3P).
6. New implementations should be based on RFC 1722 because it probably resolves some shortcomings of RFC 1655 (3P -- correctly justified decision).

OR: new implementations should use RFC 1655 because the proposed standard is more likely to be encountered in practice at the moment (3P -- correctly justified decision).

**FRAGE 13 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 03**

Name the three steps involved in a typical conversation using the TCP protocol.

A connection is established (2P), the two peers exchange data (2P), and finally the connection is closed by either of the peers (2P).

**FRAGE 14 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 03**

1. What is the purpose of SOCKS proxying?
2. Describe how this purpose is achieved.
3. SOCKS proxying is a way to circumvent firewalls / cross network segment boundaries (3P for either aspect).
4. The SOCKS protocol makes the server system transmit data on behalf of the client, relaying replies back to the client (3P).

**FRAGE 15 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 03**

Name two applications of the UDP protocol and justify why UDP is a good choice for each of them.

1P for each application name, 3P for each justification.

Example: The Network Time Protocol is used to synchronize computer clocks (1P). It can be used over UDP in order to minimize the latency which might distort the desired time value (3P).

Messages that need to reach multiple recipients at the same time or where the recipients are not known before sending the message (1P) can use UDP because UDP supports sending broadcasts (3P).

**FRAGE 16 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 03**

The TCP protocol uses send and receive buffers on both peers.

1. What is their main purpose?
2. Name the technique that fulfills this purpose.
3. What additional information can be derived from their states?

a) Their main purpose is to ensure the sequence of data (3P) exchanged between peers by using a b) sliding window technique (2P).

1. The state of send and receive buffers can hint at problems in the underlying network layers (3P).

**FRAGE 17 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 03**

The TCP Syn flood attack is an effective means to carry out Denial-of-Service attacks. Describe how TCP Syn flood attacks work.

1. What mechanism of the TCP protocol is exploited?
2. How does this mechanism drain server resources?
3. Is it possible to defend against a TCP Syn flood attack on the application layer? Explain your answer.
4. TCP SYN flood attacks exploit the three-way-handshake (2P) of the TCP connection establishment.
5. When a server receives a SYN segment (2P), buffers are allocated (2P) for the expected connection and server resources are drained.
6. It is not possible to defend against a SYN flood attack on the application layer (2P), since it is carried out on fundamental properties of the TCP transport layer (2P).

**FRAGE 18 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 03**

Some remote desktop tools let users control remote machines as if the users were directly operating the machine. Which transport layer protocol makes the most sense for this application scenario? Explain your answer.

TCP (2P), because TCP enables a stream-based (3P), bidirectional (2P) communications channel that ensures the sequence of events, which is important in remote control scenarios (3P).

**FRAGE 19 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 04**

What is the main difference between IPv4 and IPv6 addresses?

IPv4 addresses are 32 bits long (3P), whereas IPv6 addresses are 128 bits long (3P).

**FRAGE 20 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 04**

Name three aspects that are managed by the Internet Assigned Numbers Authority.

(2P each) Reserved / Special IP ranges, Protocol numbers, port numbers, whois information via regional registries, autonomous system numbers

**FRAGE 21 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 04**

A network administrator wants to make sure that their routers are configured correctly and that IP packets are routed along the correct path.

1. Which tool can they use to find this out?
2. How does the tool named in a) work?
3. They can use "traceroute" (2P).
4. It works by sending ICMP messages to a relevant destination address (2P). These packets have a varying time-to-live value (2P), so that routers along the way will report that the packet has expired (2P).

**FRAGE 22 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 04**

1. What is the purpose of the Dynamic Host Configuration Protocol (DHCP)?
2. How does the Dynamic Host Configuration Protocol (DHCP) work?
3. DHCP's purpose is to deliver network configuration data (2P), such as an available IP address (1P) to new network clients.
4. A client machine requests this information by sending a broadcast (3P) message, which is then answered by a DHCP server (2P).

**FRAGE 23 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 04**

1. What is the purpose of Network Address Translation?
2. Which circumstances make it necessary?
3. How does it work? Describe an example including self-chosen addresses and ports.
4. The purpose of NAT is to share a (single) regular IP address with a number of systems (2P).
5. It became necessary when the number of systems connected to the internet exceeded the IPv4 address space (2P).
6. Packets from an internal network using a private IP address block, like 192.168.177.\* (2P for choosing a private IP block) are retransmitted by the NAT router with their source address and port changed (2P). Replies that arrive with these changed address as destination are transformed back into the original values of the outgoing packets (2P).

**FRAGE 24 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 04**

A guest tries to use IPv4 autoconfiguration in order to connect to a hotel's network.

1. Will they be able to directly access the internet? If so, why? If **not**, why **not**?
2. Name three measures the hotel's IT staff can take in order to enable a working connection.
3. No (2P), because packets from the IP block used for autoconfiguration may not be routed (2P).
4. A proxy server (2P) or a NAT-enabled router (2P) used by the hotel. The hotel could also run a DHCP server (2P).

**FRAGE 25 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 05**

1. What is the purpose of the Address Resolution Protocol?
2. How does the Address Resolution Protocol work?
3. The purpose of the ARP is the association of IP addresses with MAC addresses (2P).
4. If a MAC address for an IP address is wanted, a broadcast message (2P) is sent. The corresponding system replies with its MAC and IP address (2P).

**FRAGE 26 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F1/Lektion 05**

1. What is the main purpose of the Border Gateway Protocol?
2. How are routes configured?
3. On what basis are routes configured?
4. The main purpose of the Border Gateway Protocol is the interconnection of Autonomous Systems (2P).
5. Routes are configured manually (2P),
6. based on specific policies (2P) defined within the organization responsible for the autonomous system or between the interconnected autonomous systems.

**FRAGE 27 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 05**

Explain how routers that implement the Routing Information Protocol detect that a connection to a neighboring router is unavailable.

Neighboring routers regularly exchange information (2P). They use timers (1P) associated with individual routes (2P). If a timer runs out without a message about a specific route being received, this route is marked as unavailable (3P).

**FRAGE 28 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F1/Lektion 05**

1. Name an attack scenario against routing.
2. Describe the outcome of the attack.
3. How is it carried out?

(2P name, 3P outcome, 3P how it is carried out). Example: a) ARP Poisoning (2P):

1. An attacker impersonates another system on the link-local level (link layer) (3P)
2. by sending a counterfeit ARP reply (3P) to local systems.

**FRAGE 29 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 05**

Consider the information depicted in the figure.

1. What is the purpose of the Routing Information Protocol?
2. Given the example network structure depicted, describe how the breakdown of the link between R6 and R3 is handled by the Routing Information Protocol running on R6.
3. The main purpose of the Routing Information Protocol is the optimization of the routes (2P) taken to reach distant networks.
4. Because a timer runs out, R6 notices that the connection to R3 is unavailable and alters its routing table accordingly (2P). R6 then notifies its neighboring routers R1 and R5 of the change (3P), which in turn change their routing tables accordingly. This change then propagates to R4, R3, and R2 (3P).

**FRAGE 30 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F1/Lektion 05**

Consider the example network structure depicted in the figure.

1. Describe how the routing table of router R2 looks for network D. What are the distance vector values?
2. How does the routing table of R2 change if the connection between R1 and R6 breaks down?
3. The destination is always D as per question. Two possible gateways are R1 and R3, with a distance metric for D of 4 via R1 (3P) and 3 via R3 (3P).
4. If the connection between R1 and R6 breaks down, the distance metric via R1 changes to 5 (3P), while the distance metric for gateway R3 remains unchanged (1P).

**FRAGE 31 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 06**

Name three types of entries in a DNS database.

2P each; examples: A, AAAA, CNAME, NS, MX, SOA, TXT, SRV

**FRAGE 32 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 06**

1. Describe a "reverse DNS" lookup.
2. What is the difference between a "reverse DNS" and a regular DNS query?
3. A reverse DNS lookup asks a DNS server to provide a fully qualified domain name for a given IP address (3P),
4. whereas regular DNS lookups request an IP address associated with a given symbolic name (3P).

**FRAGE 33 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 06**

1. Pick a suitable Fully Qualified Domain Name with at least four components.
2. Identify its components in order to exemplify the DNS host name hierarchy.
3. server21.mail.google.com (2P) (Other answers acceptable)
4. The FQDN consists of the components: Top-level domain: com (2P), domain: google (2P), subdomain: mail (1P), hostname: server21 (1P) (Answers have to match picked example, points are distributed 50/50 between the name of the component and the concrete value in the picked example)

**FRAGE 34 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 06**

The "Sender Policy Framework" (SPF) and the "Domain-based Message Authentication, Reporting and Conformance" (DMARC) are two countermeasure approaches that deal with a similar problem.

1. Describe the problem that these two approaches address.
2. What role does the Domain Name System play in each approach?
3. What differentiates the two approaches?
4. Both approaches deal with the fight against spam mails (2P).
5. Both approaches use the DNS as a place to store public information (2P).
6. While SPF tries to establish the authenticity of mail senders (2P), DMARC provides a way to define what should happen with suspicious mail (2P).

**FRAGE 35 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 06**

How can a client obtain an authoritative reply for the DNS name "[www.amazon.de](http://www.amazon.de/)"? Describe the individual steps and pay attention to the communication partners of the client.

Since an authoritative reply is requested, the client asks a root server (2P) for the address of the DNS server responsible for the top-level domain "de" (3P). This server is then asked for the nameserver responsible for the domain "amazon" (3P). This server is then contacted and the request for the ""www" hostname is issued (2P). This reply is authoritative.

**FRAGE 36 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 06**

1. Name a technique by which the authenticity of DNS entries can be ensured.
2. Describe the verification process of an entry using an appropriate example.

a) The technique that provides this authenticity is called DNSSEC / DNS Security Extensions (2P for name). b) DNSSEC stores signatures (2P) with corresponding entries in the zone (1P). The signature can be validated using the public key (2P) that is also contained in the zone. This public key can be verified using an entry from the higher-level DNS server (3P).

**FRAGE 37 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 07**

Name two approaches HTTP/2 uses in order to improve on the shortcomings of HTTP/1.1.

Request/response interactions are handled concurrently. Headers are encoded more efficiently.

Requests can be prioritized to retrieve important data first. (Two of the three answers are sufficient, 3P each)

**FRAGE 38 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 07**

Name two extensions to the SMTP protocol and briefly describe the purpose of each.

3P each (1P per name, 2P per description):

8BITMIME (allows the transmission of non-text data), AUTH (enables authentication), STARTTLS (enables the encryption of the conversation)

**FRAGE 39 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 07**

1. Describe a typical application scenario for the HTTP protocol.
2. What information is contained in the requests and responses?
3. A user uses a web browser to interact with a web server (1P) in order to obtain information (1P).
4. The web browser requests the given URI (1P) using a method of choice (1P) (GET/POST/PUSH/DELETE/HEAD) to which the server replies with a corresponding status code (2P) and the requested content (2P).

(The web browser then proceeds to request additional content referenced in the original document.)

**FRAGE 40 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 07**

Describe a typical application scenario for the SMTP protocol.

A Mail Client software uses SMTP to send an E-Mail (1P). In order to do this, it connects to the SMTP server and introduces itself (2P). It then proceeds to declare sender and recipient values (2P) and transmits the mail content (2P). Finally, the server acknowledges the receipt of the mail (1P).

**FRAGE 41 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 07**

1. Why is HTTP a stateless protocol?
2. What does this mean for the interdependence of requests?
3. What technology has been introduced to counteract this fundamental protocol property? Explain why.
4. HTTP is based on a simple request/response paradigm (3P).
5. This means that every request can be immediately answered by the server, independent from previous requests (3P).
6. In order to introduce a state into HTTP-based conversations, cookies (3P) are used to store information associated with conversations and enable things like "shopping carts" (1P).

**FRAGE 42 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 07**

Why is it relatively easy to retrace a user's interaction with a HTTP server if they use unencrypted HTTP/1.1? (**Hint:** Focus on how the requests and responses are transmitted, and consider the role of the underlying protocol.)

HTTP/1.1 is a text-based (2P) protocol that reuses (2P) one TCP connection for subsequent requests to the same server. This means that subsequent requests are associated with the initial TCP connection. These requests are handled in a sequential manner (3P), so that an observer can retrace the individual steps of the user's interaction with a web server using the TCP sequence numbers (3P).

**FRAGE 43 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 08**

Name three goals of the "Security Architecture for IP" (IPSec).

2P each: access control, integrity, origin authentication, replay detection / protection, confidentiality

**FRAGE 44 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 08**

Name the three goals of Transport Layer Security.

Authentication (2P), Confidentiality (2P), Integrity (2P)

**FRAGE 45 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 08**

The "Security Architecture for IP" (IPSec) can be operated in two different modes.

1. Name the two modes.
2. Name the main difference between the two modes.
3. Transport mode (2P) and Tunnel mode (2P)
4. In Transport mode, only the IP payload is encrypted (2P). In Tunnel mode, entire packets are encrypted and wrapped in new packets (2P).

**FRAGE 46 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 08**

A network administrator wants to access an application server system from home using a remote desktop tool. This kind of access is only allowed from within the organization.

1. How can this be achieved without going through the approval process for new firewall rules if the administrator already has external access to a Secure Shell server?
2. How likely is this to cause a security alert by an Intrusion Detection System?
3. The administrator can use "Local Port Forwarding" (2P) to use the existing SSH server as a proxy server (2P) and access the application server.
4. How likely a detection is depends on the configuration of the IDS, since it is not really an attack pattern (2P), but the monitored traffic might be higher than is typical for this SSH service (2P).

**FRAGE 47 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 08**

A company wants to use a valid certificate for their web server. Describe the signing process in detail.

(**Hint:** Remember to specify who the subject of the certificate is, and who sends what pieces of information to whom.)

The web server is the subject of the certificate (1P). The organization needs to create a public/private key pair (1P). The organization creates a certificate signing request that contains the information on the web server (1P) and the public key (1P). This information is sent to a certificate authority (1P) which verifies the information in the request (1P) and creates the certificate by signing the certificate (1P) using their private key (2P). The certificate is now sent back to the organization and can be deployed on the web server (1P).

**FRAGE 48 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 08**

Consider a Man-in-the-Middle attack that is being carried out during a key exchange that follows the principles of the Diffie-Hellman key exchange.

1. What is a precondition?
2. What happens in each step of the attack?
3. What is the final outcome of the attack?
4. Higher-level Man-in-the-Middle attacks rely on a successful lower layer Man-in-the-Middle attack so that the IP address of a system can be impersonated (2P).
5. The attacker impersonates the server (2P) and accepts a connection from a client (1P). It then establishes a second connection to the server (1P), using its own public key (2P).
6. In essence, the attacker creates two independent secure communications channels that are under the attacker's control, one towards the client, one towards the server (2P).

**FRAGE 49 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 09**

Name two properties of signature-based Intrusion detection systems.

3P each: signature-based systems are efficient / signature-based systems cannot detect unknown attacks / signature-based systems rarely emit false positives

**FRAGE 50 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 09**

Name two objectives of Security Information and Event Management systems.

3P each: integrate and consolidate security data / provide an overview of security-related data / consolidate log data from multiple systems / provide a data source for evidence collection and storage

**FRAGE 51 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 09**

A business-critical application system needs to be closely monitored. Name the type of Intrusion Detection System that should be used for this task. Explain your answer.

A host-based system should be used (2P), because it provides a close inside-view of the going-on on the system (3P). It can also detect physical inside attackers (3P).

**FRAGE 52 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 09**

Name and briefly describe two suspicious events that can be detected by netflow analysis. Give an example of what each event might indicate.

(2P for event name/ description and 2P for example):

Sudden abnormal bursts of traffic (e.g. data exfiltration).

Amount of traffic per protocol (e.g. hiding communication within another protocol). Invalid sequence numbers in TCP (e.g. TCP RST attack or Session Hijacking).

Communication of protocols over non-standard ports (e.g. hidden communication channels).

**FRAGE 53 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 09**

1. What are false positives in the context of cyber security events?
2. How can false positives help to improve cyber security?
3. Use an appropriate example that illustrates the scenario, including how the false positive came to be and what consequences can be drawn.
4. False positives are security alerts that are evaluated as if they were security events, which they are not (2P).
5. They offer an opportunity to improve rules / policies / sensors / … (2P for appropriate aspect).
6. Example: 3P for appropriate example (e.g. a new use case for an existing system triggered the IDS because a new kind of access to that system was detected), 3P for appropriate consequences (e.g. the rules of the IDS are adapted to the new use case and the new security implications are evaluated)

**FRAGE 54 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 09**

1. What are false negatives in the context of cyber security events?
2. How can they come to be?
3. Use an appropriate example that illustrates the scenario, how the false negative came to be and what consequences can be drawn.
4. False negatives are events that should have triggered a security event but did not. (2P).
5. False negatives can only be found by actively taking actions that should trigger security events but don't do so (3P).
6. During a security exercise, a breach of a firewall might not be detected by an IDS. (2P for appropriate example) This can lead to a refinement of the IDS rules / update or exchange of the vulnerable firewall. (3P for appropriate consequences)

**FRAGE 55 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 10**

Name three data dimensions that are relevant for cyber security data.

(2P each of): Severity of the events / Network segments / Business criticality / Compliance relevancy / Geolocation / Operating system types and versions / (Software and service) exposure level / Device type / Traffic type / Time data

**FRAGE 56 VON 120**

**DLBCSEINF01\_E\_Offen\_leicht\_F2/Lektion 10**

Name three data classification techniques that can be applied to cyber security data.

(2P for each of) Naïve Bayes / Bayesian Networks / Markov chains / Decision Tree algorithms / Support Vector Machines / Artificial Neural Networks

**FRAGE 57 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 10**

A behavior-based Intrusion Detection System sends out a security alert about suspicious network activity. Upon closer inspection, it is discovered that a work station is attempting to establish connections to an IP address that is listed in a DNS Blackhole List.

1. What are DNS Blackhole Lists?
2. What does this mean for the listed address?
3. Which two concrete measures should be taken next?
4. DNS Blackhole Lists contain addresses that have been involved in sending spam e-mails in the past (2P).
5. Consequently, addresses listed are not trustworthy (2P).
6. Further communication attempts should be blocked (2P) and the workstation inspected for malware (2P).

**FRAGE 58 VON 120**

**DLBCSEINF01\_E\_Offen\_mittel\_F2/Lektion 10**

DNS data changes all the time.

1. Why is that?
2. What does this mean for network forensics investigations?
3. Which two data sources can mitigate this problem for network forensics?
4. The Domain Name System is essentially a distributed database (2P). Entries in different zones are added, removed and modified as normal part of the operation all the time (2P).
5. This means that DNS data collected as evidence for a network forensics investigation may have changed since the investigation (2P).
6. In order to provide DNS data that is current at the time of the incident, techniques like passive DNS and DNS repositories need to be used (2P).

**FRAGE 59 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 10**

A network-based Intrusion Detection System detects malicious network traffic coming from outside the organization. This kind of traffic is generally generated by botnets of compromised systems. The organization's firewall has already been configured to block the traffic.

1. Which further measures should be taken to put an end to the attack?
2. Which other stakeholders are involved in this incident?
3. How can they be identified in order to contact them?
4. It should be attempted to stop the attack at its source (2P).
5. The organization(s) that the attack is coming from (3P) has/have an interest in knowing about the incident.
6. They can be identified using the Autonomous System Numbers (3P) that provide a link between the compromised IP addresses and the responsible organizations (2P).

**FRAGE 60 VON 120**

**DLBCSEINF01\_E\_Offen\_schwer\_F2/Lektion 10**

Modern malware is customized to a specific attack scenario. This makes the malware very difficult to detect by signature-based systems.

1. Which kind of techniques can enable detection despite this problem?
2. Name one concrete technique and describe it by answering the following questions.
3. What is the purpose of the technique?
4. Name a prerequisite, which is required in order for this technique to work.
5. Why is this prerequisite required by the technique?
6. Machine Learning techniques (2P) can enable the detection of previously unknown malware.
7. A concrete technique is decision tree algorithms (2P for fitting example), which are used for
8. classification (2P for matching purpose) tasks.
9. This technique requires appropriate training data (2P).
10. because it is a supervised learning method (2P)



The data collected by means of network forensics has to …

**Wählen Sie eine Antwort:**

Wireshark is …

**Wählen Sie eine Antwort:**

**FRAGE 61 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 01**

|  |
| --- |
| be anonymized. |
| recommend concrete actions. |
| *stand up in court.* |
| positively identify attackers. |

**FRAGE 62 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 01**

|  |
| --- |
| an intrusion detection system. |
| an archival network forensics data system. |
| *a network traffic analysis tool.* |
| a Security Information and Event Management system. |



Attackers attempt to obfuscate their traces on compromised systems. Security-related

systems can also be compromised. Which of the steps of the generic network forensics process aims to make such tampering with evidence impossible?

**Wählen Sie eine Antwort:**

In order to select the network forensics data that is relevant for a specific case, a specific step

is included in the generic network forensics process. Which step is this?

**Wählen Sie eine Antwort:**

**FRAGE 63 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 01**

|  |
| --- |
| The examination step |
| *The preservation step* |
| The detection step |
| The collection step |

**FRAGE 64 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 01**

|  |
| --- |
| The collection step |
| The preservation step |
| The detection step |
| *The examination step* |



An intrusion detection system has detected irregular access to an internal research database.

Upon further investigation, it is revealed that the irregularity was detected because an external guest was given credentials by a researcher to appreciate his work.

What is the correct assessment of this scenario?

**Wählen Sie eine Antwort:**

An intrusion detection system has detected irregular access to an internal research database.

Upon further investigation, it is revealed that the irregularity was detected because a researcher had to use a different machine.

What is the correct assessment of this scenario?

**Wählen Sie eine Antwort:**

**FRAGE 65 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 01**

|  |
| --- |
| This is a security alert. |
| This is a false positive. |
| This is a security event. |
| *This is a security incident.* |

**FRAGE 66 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 01**

|  |
| --- |
| This is a security alert. |
| This is a security event. |
| *This is a false positive.* |
| This is a security incident. |



What is the chief concern of the transport layer?

**Wählen Sie eine Antwort:**

Connection-oriented protocols …

**Wählen Sie eine Antwort:**

**FRAGE 67 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 02**

|  |
| --- |
| To represent transmitted data with integrity |
| *To denote which processes communicate with each other* |
| To denote which machines communicate with each other |
| To represent the information that is interchanged |

**FRAGE 68 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 02**

|  |
| --- |
| provide an asynchronous communication channel. |
| incur a lower overhead than connectionless protocols. |
| leave the task of reestablishing a sequence of events to the application layer. |
| *provide a synchronous communication channel.* |



An application layer protocol intends to distribute small messages as quickly as possible to a

large number of recipients. Individual messages are expendable, as long as the time constraint is met. Which type of underlying protocol should the protocol use?

**Wählen Sie eine Antwort:**

Internet standards are published by the IETF in RFC documents. What happens when a

standard needs to be fundamentally changed?

**Wählen Sie eine Antwort:**

**FRAGE 69 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 02**

|  |
| --- |
| A network layer protocol |
| A link layer protocol |
| *A connectionless protocol* |
| A connection-oriented protocol |

**FRAGE 70 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 02**

|  |
| --- |
| The existing RFC document is changed to reflect the new standard techniques and all interestedparties are notified of the change. |
| A new update document for the RFC document is released and all teams that implement thestandard have to implement the change. |
| *A new RFC document is drawn up as a draft standard and published as a new RFC document.* |
| A new RFC document is drawn up and the previous version is removed from the RFC archive. |



RFC 1149 describes the transmission of IP packets by means of avian carriers, such as

pigeons. In 2001, ICMP ping messages were exchanged over an implementation in practice without changing the IP protocol. Which layer of the layered network architecture was thereby implemented?

**Wählen Sie eine Antwort:**

The "Echo" protocol is an application layer protocol that simply sends back any data it

receives. Which layer of the TCP/IP model stores the address to which the reply should be sent?

**Wählen Sie eine Antwort:**

**FRAGE 71 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 02**

|  |
| --- |
| The transport layer |
| The application layer |
| The internet layer |
| *The link layer* |

**FRAGE 72 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 02**

|  |
| --- |
| *The internet layer* |
| The link layer |
| The application layer |
| The transport layer |



The UDP header contains data on …

**Wählen Sie eine Antwort:**

A SOCKS proxy …

**Wählen Sie eine Antwort:**

**FRAGE 73 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 03**

|  |
| --- |
| *source and destination port.* |
| sequence number. |
| the header length. |
| acknowledgement number. |

**FRAGE 74 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 03**

|  |
| --- |
| emits broadcast messages in order to detect other SOCKS proxies. |
| mitigates denial-of-service type attacks. |
| separates network segments on the network layer based on access rules. |
| *transmits data on behalf of other systems.* |



How do UDP reflection attacks work?

**Wählen Sie eine Antwort:**

How does TCP detect missing packets?

**Wählen Sie eine Antwort:**

**FRAGE 75 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 03**

|  |
| --- |
| An attacker intercepts UDP traffic to a legitimate server. This traffic is sent to a system under the attacker's control. The traffic is analyzed for valuable information on the victim's networkinfrastructure. |
| Spoofed packets sent by an attacker arrive at the victim's address. The victim sends its replyarbitrarily to other systems. The high amount of error messages from the other systems causes stress on the victim's network infrastructure. |
| Spoofed packets sent by an attacker arrive at a legitimate server. This server sends its repliesback to the attacker. The replies are scanned for vulnerable software versions used in the victim's network infrastructure. |
| *Spoofed packets sent by an attacker arrive at a legitimate server. This server sends its reply to the**victim's address. The additional data in the replies causes stress on the victim's network infrastructure.* |

**FRAGE 76 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 03**

|  |
| --- |
| *The sender keeps a timer for segments in the send buffer. If no acknowledgement is received**before the timer runs out, the sender transmits again.* |
| The receiver keeps a timer for segments in the receive buffer. If no consecutive segment isreceived before it runs out, the receiver requests a retransmission. |
| The sender keeps a timer for segments in the receive buffer. If no acknowledgment is receivedbefore the timer runs out, the sender transmits again. |
| The receiver keeps a timer for segments in the send buffer. If no consecutive segment is receivedbefore the timer runs out, it requests retransmission. |



An administrator uses a remote desktop tool that does not use encryption to transmit

commands to remote control a server system. Which attack can immediately trigger remote code execution by an attacker?

**Wählen Sie eine Antwort:**

Internet of Things applications interconnect many different sensors and actuators driven by

embedded hardware. Why is there a demand to use UDP for this kind of usage scenario?

**Wählen Sie eine Antwort:**

**FRAGE 77 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 03**

|  |
| --- |
| *A TCP Session Hijacking attack* |
| A TCP RST attack |
| A UDP reflection attack |
| A TCP SYN flood attack |

**FRAGE 78 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 03**

|  |
| --- |
| *Using UDP broadcast messages enables many systems to communicate with each other without**the need for extensive configuration.* |
| UDP ensures the integrity of the transmitted messages, so that the sensor information arrivesintact at the destination. |
| The high overhead of TCP makes it impossible for embedded systems to handle the transfer ratesnecessary for Internet-of-Things applications. |
| The low overhead of UDP ensures that messages arrive in their sequence of events, so thatsensor data can be quickly reacted to. |



How do routers know if an IP address is in the local network segment?

**Wählen Sie eine Antwort:**

The SOCKS protocol …

**Wählen Sie eine Antwort:**

**FRAGE 79 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 04**

|  |
| --- |
| The IP address consists of a network and a host part. The ARP table configured in the routerdetermines if the network part of the IP address matches the router's. |
| The router contains a routing table that has an entry for the IP address range of the local networksegment. |
| The router contains a statically configured list of all IP addresses within the local network segment. |
| *The IP address consists of a network and a host part. The subnet mask configured in the router**determines if the network part of the IP address matches the router's.* |

**FRAGE 80 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 04**

|  |
| --- |
| can be used to provide transport layer encryption. |
| is a helper protocol for status messages. |
| is a high-performance successor to the HTTP protocol. |
| *can be used as an attack vector.* |



What is the purpose of ICMP?

**Wählen Sie eine Antwort:**

In order to save valuable IPv4 addresses, some internet providers offer "Dual-Stack Lite".

Using this technique, end users are only assigned public IPv6 addresses while they are still able to access IPv4 services.

This is a special case application of which technique?

**Wählen Sie eine Antwort:**

**FRAGE 81 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 04**

|  |
| --- |
| *ICMP is a helper protocol for the transmission of status messages on the network layer.* |
| ICMP is a signature protocol that provides authenticity for IP packets. |
| ICMP is an integrity protocol that carries checksums for UDP datagrams. |
| ICMP is a handshake protocol for the establishment of TCP connections. |

**FRAGE 82 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 04**

|  |
| --- |
| Routing |
| Proxying |
| *Network Address Translation* |
| Firewalling |



A system has the IPv4 address 172.16.20.1. What can be said about this system?

**Wählen Sie eine Antwort:**

Which of the following constitutes a firewall rule that is possible?

**Wählen Sie eine Antwort:**

**FRAGE 83 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 04**

|  |
| --- |
| *The default subnet mask of this system's network is 255.255.0.0.* |
| This system has obtained its address through IPv4 autoconfiguration. |
| The system can directly send packets to the internet. |
| At most 253 other systems are connected to the same network segment. |

**FRAGE 84 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 04**

|  |
| --- |
| ALLOW all outgoing UDP connections from IP address Y. |
| *DROP all incoming TCP connections on port 80 from network segment X.* |
| DROP all outgoing TCP connections that contain the text "password". |
| ALLOW all incoming HTTP connections from network segment X that are authenticated. |



What is the consequence of a TCP RST attack on a BGP router?

**Wählen Sie eine Antwort:**

Which of the following statements about autonomous system numbers is correct?

**Wählen Sie eine Antwort:**

**FRAGE 85 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 05**

|  |
| --- |
| The router and its peer consider the link permanently broken. |
| The router and its peer consider the link available, even though the attacker can eavesdrop on thetraffic. |
| *The router and its peer consider the link broken until it is reestablished.* |
| The router and its peer consider the link available, even though it is broken. |

**FRAGE 86 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 05**

|  |
| --- |
| An autonomous system number is assigned to exactly one BGP router. |
| An autonomous system number is assigned to exactly one person. |
| An autonomous system number is assigned to exactly one IP address block. |
| *An autonomous system number is assigned to exactly one organization.* |



The ARP table …

**Wählen Sie eine Antwort:**

Two organizations want to use each other's infrastructure in order to connect to the internet.

What is required in order to use the Border Gateway Protocol for this purpose?

**Wählen Sie eine Antwort:**

**FRAGE 87 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 05**

|  |
| --- |
| is used to store the known IP address blocks of statically configured routing tables. |
| *is used to store the known MAC addresses associated with local IP addresses.* |
| is used to store BGP policies and rules. |
| is used to store distance vectors in router systems. |

**FRAGE 88 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 05**

|  |
| --- |
| Both organizations need a Domain Name. |
| Both organizations need an ARP table. |
| Both organizations need a routing table. |
| *Both organizations need an autonomous system number.* |



Given the network structure depicted, to which neighboring router would router R1 pass an IP

packet in order to reach network D?

**Wählen Sie eine Antwort:**

**FRAGE 89 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 05**

|  |
| --- |
| Router 3 |
| Router 5 |
| *Router 6* |
| Router 2 |



Given the network structure depicted, to which neighboring router would router R3 pass an IP

packet in order to reach network A?

**Wählen Sie eine Antwort:**

**FRAGE 90 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 05**

|  |
| --- |
| Router 4 |
| *Router 2* |
| Router 1 |
| Router 6 |



What is a DNS Zone?

**Wählen Sie eine Antwort:**

Which of the following DNS record types is used for the DNS Security Extensions?

**Wählen Sie eine Antwort:**

**FRAGE 91 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 06**

|  |
| --- |
| The data registered with a regional internet registry |
| A table on one DNS server |
| *A boundary of responsibility* |
| An IP address that is associated with a Fully Qualified Domain Name |

**FRAGE 92 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 06**

|  |
| --- |
| CNAME |
| SOA |
| *RRSIG* |
| SRV |



A software program tries to obtain an authoritative reply for the fully qualified domain name

"login.research.mycompany.de". Which system should this authoritative answer come from if all of the following DNS servers exist?

**Wählen Sie eine Antwort:**

The DNS root servers …

**Wählen Sie eine Antwort:**

**FRAGE 93 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 06**

|  |
| --- |
| *The DNS server that manages the zone "research.mycompany.de"* |
| The DNS server that manages the root zone "." |
| The DNS server that manages the top-level zone "de" |
| The DNS server that manages the zone "mycompany.de" |

**FRAGE 94 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 06**

|  |
| --- |
| *contain authoritative information on the nameservers that manage all top-level domains.* |
| are directly under the control of the Internet Assigned Numbers Authority. |
| can be contacted using a single static IP address, ensuring they are always easy to find. |
| contain authoritative information on all domains that are managed by regional internet registrars. |



The IP address for the fully qualified domain name "web.mycompany.com" is secured using

the DNS Security Extensions. How can this entry be verified?

**Wählen Sie eine Antwort:**

DNS servers under attacker control can be used to control botnets. What makes this control

technique hard to detect?

**Wählen Sie eine Antwort:**

**FRAGE 95 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 06**

|  |
| --- |
| The "com" zone contains a public key for this entry. This public key can be verified using thesignature that is stored in the "mycompany.com" zone. |
| The "com" zone contains a signature for this entry. This signature can be verified using the publickey that is also stored in the zone. |
| *The "mycompany.com" zone contains a signature for this entry. This signature can be verified**using the public key that is also stored in the zone.* |
| The "mycompany.com" zone contains a public key for this entry. This public key can be verifiedusing the private key that is also stored in the zone. |

**FRAGE 96 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 06**

|  |
| --- |
| The security extensions for DNS generally encrypt DNS traffic, so that not even deep packetinspection can reveal transferred commands. |
| Authoritative DNS replies are the exception. This makes it easy to counterfeit DNS replies. |
| DNS over UDP makes it impossible to identify the communication partners. |
| *DNS caching mechanisms can transport the control information without a direct connection**between the compromised DNS server and the victim.* |



Which of the following represents an improvement to HTTP/2 compared to HTTP/1.1?

**Wählen Sie eine Antwort:**

Which of the following statements about the Simple Mail Transfer Protocol is correct?

**Wählen Sie eine Antwort:**

**FRAGE 97 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 07**

|  |
| --- |
| HTTP/2 uses UDP as an underlying transport layer protocol, which greatly reduces the latency ofresponses. |
| *HTTP/2 allows multiple requests to be handled at the same time.* |
| HTTP/2 is a stateful protocol that eliminates the need for the transmission of redundantinformation. |
| HTTP/2 can be cached more efficiently by browsers. |

**FRAGE 98 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 07**

|  |
| --- |
| SMTP requires authentication. |
| *SMTP requires a stateful interaction.* |
| SMTP requires encryption. |
| SMTP requires error handling on the server side. |



Is HTTP/2 compatible enough with HTTP/1.1 so that a pure HTTP/2 server handle HTTP/1.1

requests?

**Wählen Sie eine Antwort:**

**FRAGE 99 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 07**

|  |
| --- |
| Yes, HTTP/2 servers contain a method to downgrade the connection. |
| Yes, HTTP/2 enables the same interactions as HTTP/1.1. |
| *No, HTTP/2 uses a different message header format from HTTP/1.1.* |
| No, HTTP/2 requires clients to formulate all their requests in advance so that the server cangenerate the responses in parallel. |



Given the depiction of the message exchange between two peers, which of these application

layer protocols is probably the basis of the dialogue?

**Wählen Sie eine Antwort:**

**FRAGE 100 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 07**

|  |
| --- |
| *HTTP/2* |
| HTTP/1.1 |
| HTTP/1.0 |
| SMTP |



Why is HTTP/1.1 more suitable for modern web content than HTTP/1.0?

**Wählen Sie eine Antwort:**

Load balancers are special web servers that distribute requests to a number of other web

servers behind the load balancer that handle these requests.

When many requests arrive, the incurred load is shared between these backend web servers. Which fundamental property of web protocols enables this technique?

**Wählen Sie eine Antwort:**

**FRAGE 101 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 07**

|  |
| --- |
| *Modern web content contains a lot of additional content that would cause HTTP/1.0 to create a lot**of new connections at the cost of high overheads.* |
| Modern web content contains a lot of sensitive data that needs to be protected using encryptionfeatures contained in HTTP/1.1. |
| Modern web content contains more scripts that dynamically add content. This could not have beenhandled by HTTP/1.0. |
| Modern web content contains images with higher resolution. This increased traffic could not havebeen handled by HTTP/1.0 without high overheads. |

**FRAGE 102 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 07**

|  |
| --- |
| *HTTP is a stateless protocol, so every single request is independent from previous ones.* |
| The headers used by HTTP ensure that a client only ever talks to the same web server behind theload balancer. |
| HTTP/2 is specifically designed to handle simultaneous request/response dialogues. |
| HTTP/1.1 allows the reuse of a single connection for a multitude of subsequent requests. |



Which protocol does HTTP use to add security to the HTTP protocol?

**Wählen Sie eine Antwort:**

Which layer of the TCP/IP reference model is the Secure Shell protocol stack situated on?

**Wählen Sie eine Antwort:**

**FRAGE 103 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 08**

|  |
| --- |
| IPSec |
| *TLS* |
| DNSSec |
| SSH |

**FRAGE 104 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 08**

|  |
| --- |
| The transport layer, because it directly uses the services of the internet layer. |
| The link layer, because it directly uses the services of the physical layer. |
| *The application layer, because it directly uses the services of the transport layer.* |
| The internet layer, because it directly uses the services of the link layer. |



Root certificates are the end of a verification chain. How are they signed?

**Wählen Sie eine Antwort:**

What is a cypher suite?

**Wählen Sie eine Antwort:**

**FRAGE 105 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 08**

|  |
| --- |
| Root certificates are signed by the certificate authority of the operating system they come with. |
| *Root certificates are self-signed certificates.* |
| Root certificates are signed by other root certificates. |
| Root certificates are not signed. |

**FRAGE 106 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 08**

|  |
| --- |
| A cypher suite is a software library that contains cryptographic algorithms for different purposesthat is used to implement confidentiality. |
| *A cypher suite is a set of cryptographic algorithms and parameters for different purposes that are**used throughout a typical conversation.* |
| A cypher suite is a specification document that contains cryptographic algorithms and parametersthat are allowed to operate within a specific application layer protocol. |
| A cypher suite is a certified software product that is allowed to operate within a specific applicationlayer protocol in order to provide confidentiality. |



Only one mode of operation for IPSec can be used with Network Address Translation (NAT).

Which one and why?

**Wählen Sie eine Antwort:**

An organization uses a specialized system that was developed in-house to manage customer

data. Because remote work will be enabled with this system, confidentiality of the exchanged data now needs to be provided. How can this be achieved?

**Wählen Sie eine Antwort:**

**FRAGE 107 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 08**

|  |
| --- |
| IPSec Transport mode protects only the IP payload, so that NAT techniques can still work with theoriginal packet headers. |
| IPSec Translation mode protects only the IP payload, so that NAT techniques can still work withthe original packet headers. |
| *IPSec Tunnel mode wraps the protected IP packets in new packets. The integrity of the wrapped**packets is untouched by NAT.* |
| IPSec Routing mode wraps the protected IP packets in new packets. The integrity of the wrappedpackets is untouched by NAT. |

**FRAGE 108 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 08**

|  |
| --- |
| The specialized system can be made accessible from outside by adapting firewall rules. |
| The specialized system can be adapted to enforce the use of certificates for authentication. |
| The specialized system can be adapted to enforce IPSec as the underlying communication layer. |
| *The specialized system can be adapted to enforce the Transport Layer Security as the underlying**communication layer.* |



The rules for behavior-based intrusion detection systems are created …

**Wählen Sie eine Antwort:**

Which of the following suspicious actions can be detected by netflow monitoring?

**Wählen Sie eine Antwort:**

**FRAGE 109 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 09**

|  |
| --- |
| manually by cyber security specialists with experience. |
| automatically by the system from observed attack patterns. |
| manually by the system's manufacturer from a knowledge base. |
| *automatically by the system from an observed normal state*. |

**FRAGE 110 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 09**

|  |
| --- |
| Large numbers of failed authentication attempts |
| The use of factory default usernames and passwords |
| The alteration of log files on critical systems |
| *The use of communication protocols over non-standard ports* |



Intrusion Prevention Systems can support which step in the information security incident

management process?

**Wählen Sie eine Antwort:**

A signature-based Intrusion Prevention System reacts on a detected Denial-of-Service attack.

How would this event be categorized?

**Wählen Sie eine Antwort:**

**FRAGE 111 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 09**

|  |
| --- |
| Assess |
| *Respond* |
| Plan |
| Detect |

**FRAGE 112 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 09**

|  |
| --- |
| *BLOCKED* |
| ALLOW |
| SUSPICIOUS |
| MALICIOUS |



An application system that is currently being tested in order to evaluate its worth for an

organization is still in its factory state. Among other things, this means that default credentials are set on the system. Which type of system can identify this potential attack vector?

**Wählen Sie eine Antwort:**

In an organization, the user identity management process is not always executed properly. As

a result, terminated user accounts are still valid for some systems. Which type of system can detect such discrepancies?

**Wählen Sie eine Antwort:**

**FRAGE 113 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 09**

|  |
| --- |
| An Intrusion Detection System |
| An Intrusion Detection and Prevention System |
| An Intrusion Prevention System |
| *A Security Information and Event Management System* |

**FRAGE 114 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 09**

|  |
| --- |
| An Intrusion Detection and Prevention System |
| *A Security Information and Event Management System* |
| An Intrusion Detection System |
| An Intrusion Prevention System |



Which security data dimension is especially important for network forensics investigations and

why?

**Wählen Sie eine Antwort:**

Which of the following statements about whois data is correct?

**Wählen Sie eine Antwort:**

**FRAGE 115 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 10**

|  |
| --- |
| Geolocation, because the geographic origin of an attack reveals the attacker's intentions |
| Operating system types, because some operating systems are more vulnerable to attacks thanothers |
| *Time data, because attack patterns are evidenced by a sequence of events* |
| Software and service exposure level, because test systems cannot be used as attack vectors |

**FRAGE 116 VON 120**

**DLBCSEINF01\_E\_MC\_leicht/Lektion 10**

|  |
| --- |
| Whois data is always current. |
| Whois data contains geographical information. |
| Whois data is publicly available without restrictions. |
| *Whois data can help to identify suspicious peers.* |



Counterfeit digital certificates are an attractive means to perform man-in-the-middle attacks on

systems that use a public key infrastructure for authentication. Which of the following methods provides an additional means to verify certificates?

**Wählen Sie eine Antwort:**

Which property of Certificate Transparency makes it a relatively reliable tool to detect

counterfeit certificates?

**Wählen Sie eine Antwort:**

**FRAGE 117 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 10**

|  |
| --- |
| Certificate Revocation |
| Certificate Expiry |
| *Certificate Transparency* |
| Certificate Signing |

**FRAGE 118 VON 120**

**DLBCSEINF01\_E\_MC\_mittel/Lektion 10**

|  |
| --- |
| Publicity |
| Redundancy |
| Traceability |
| *Immutability* |



Given the dataset depicted, what is the confidence of the association rule "Source Code

Repository → Software Development"?

**Wählen Sie eine Antwort:**

**FRAGE 119 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 10**

|  |
| --- |
| 4/7 |
| 5/7 |
| 6/7 |
| *5/6* |



Given the dataset depicted, what is the support of the association rule "Financial Accounting

System → Accounting"?

**Wählen Sie eine Antwort:**

**FRAGE 120 VON 120**

**DLBCSEINF01\_E\_MC\_schwer/Lektion 10**

|  |
| --- |
| 6 |
| *2* |
| 4 |
| 7 |