**Unit 1**

**1.1**

1. Please mark the correct statement(s).

* Network forensics proactively prevents attacks.
* Network forensics can only be applied once the damage is done.
* *Network forensics can help to identify current security threats.*

1. Please list two purposes of network forensics.

*Network forensics enables an improvement in security.*

*Network forensics provides evidence for law enforcement.*

*Network forensics enables security experts and organizations to detect attacks and security incidents.*

*Network forensics enables security experts and organizations to assess damage caused by security incidents.*

*Network forensics enables security experts and organizations to identify systems affected by security incidents.*

1. Please complete the following sentence:

In order to be used in court, collected data must be stored in a *tamperproof* manner.

**1.2**

1. Please mark the correct statement(s).

* Unprocessed data can be used for investigation purposes.
* *The incident response can include immediate countermeasures.*
* The systems deployed for network monitoring do not require maintenance.

1. Please complete the following sentence:

For a successful investigation, it is imperative that the collected data are chronologically *synchronized/ordered.*

**1.3**

1. Please mark the correct statement(s).

* *IDSs need to be deployed so that they complement each other.*
* IDSs can identify attackers.
* IDSs block undesired network traffic.

1. Please describe and differentiate between two types of IDSs.

*Host-based IDSs monitor individual systems, and network-based IDSs monitor network segments.*

*Behavior-based IDSs report deviations from normal operation, and signature-based IDSs evaluate predetermined rules.*

1. Please complete the following sentence:

To be categorized as a security incident, a security event must be *confirmed* and its *impact assessed*.

**1.4**

1. Please complete the following sentence:

Denial-of-service (DoS) attacks aim to *disable or disrupt* *services* by initiating a massive number of *requests.*

1. Please mark the correct statement(s).

* Identifying the attacker in a (D)DoS attack is trivial.
* *(D)DoS attacks can serve as a diversion for other malicious actions*.
* *(D)DoS attacks are easy to detect but difficult to mitigate*.

**1.5**

1. Please mark the correct statement(s).

* *Splunk focuses on extensive data consolidation and analysis.*
* Wireshark is a network-based IDS.
* Network traffic analysis can only be performed using expensive commercial products.

1. Please name two network intrusion detection systems.

*Zeek*

*Snort*

*Suricata*

**Unit 2**

**2.1**

1. Please complete the following sentence:

Upper layers of the TCP/IP model are not concerned with the *physical* conditions*.*

1. Please mark the correct statement(s).

* The TCP/IP model can only work on current network infrastructure.
* *The presentation and session management described in the ISO/OSI model is handled on the application layer of the TCP/IP model*.
* The link layer is responsible for exchanging bits between two peers.

1. Please describe one goal of the transport layer.

*associating exchanged information with processes*

*isolating the application layer from the details of the lower layers*

**2.2**

1. Please mark the correct statement(s).

* Connectionless protocols ensure that every peer has received the data.
* *Connection-oriented protocols compensate for transmission errors and glitches.*
* *Connectionless protocols enable the simultaneous transmission of data to multiple peers.*

1. Please complete the following sentence:

Connection-oriented protocols see the data exchange as analogous to a *dialogue* or *phone call.*

**2.3**

1. Please mark the correct statement(s).

* The IETF is a single group of people that publishes internet standards.
* *Internet standards must go through a long process to be designated as such.*
* Proposed standards must provide multiple interoperable implementations*.*

1. Please complete the following sentence:

The *IANA/ICANN* is the ultimate authority on protocol numbers*.*

**Unit 3**

**3.1**

1. Please complete the following sentence:

UDP enables *fast/efficient/low-latency* communication at the cost of *reliability/the preservation of order of sequence/guaranteed delivery.*

1. Please mark the correct statement(s).

* UDP is independent from the Internet Protocol.
* The integrity of data exchanged via UDP can never be guaranteed.
* *The integrity of data exchanged via UDP must be ensured by the application-layer protocol that uses them*.

**3.2**

1. Please complete the following sentence:

TCP ensures *reliability/the preservation of order of sequence/error detection/flow control* incommunication at the cost of *speed/efficiency/latency.*

1. Please mark the correct statement(s).

* TCP is independent from the Internet Protocol.
* *TCP can transmit data streams of indeterminate lengths.*
* The integrity of data exchanged via TCP must be ensured by the application-layer protocol that uses them.

**3.3**

1. Please mark the correct statement(s).

* *The sender detects that a TCP segment has been lost.*
* The receiver detects that a TCP segment has been lost.
* The receiver asks the sender to retransmit a missing TCP segment.

**3.4**

1. Please mark the correct statement(s).

* *SOCKS proxying can be used to circumnavigate firewall rules.*
* *SOCKS proxying is an intermediate layer between the application and transport layers.*
* SOCKS proxying is an intermediate layer between the transport layer and the network layer.

**3.5**

1. Please complete the following sentence:

Attacks on the transport layer, such as TCP and UDP implementations, do not rely on vulnerable *application-layer* software*.*

1. Please mark the correct statement(s).

* Denial-of-service attacks are always launched directly.
* *SYN flood attacks exhaust a system’s resources*.
* Attackers cannot eavesdrop on TCP connections.

1. Please describe a UDP reflection attack.

*An attacker counterfeits requests to an intermediate UDP-based service. The UDP-based service then sends its replies to the ultimate victim of the attack. If the volume of the replies exceeds the victim’s network capacity, the attack is successful.*

**Unit 4**

**4.1**

1. Please complete the following sentence:

The Internet Protocol is an implementation of the *network* layer*.*

1. Please mark the correct statement(s).

* Routing separates network segments.
* Routing is always manually defined by a network architect.
* *Routing is based on routing tables in intermediate devices, such as routers.*

1. Please describe an application of ICMP.

*notification of unavailable network resources/systems*

*measuring round-trip times*

*making network routes/paths between systems visible*

**4.2**

1. Please mark the correct statement(s).

* IP autoconfiguration enables internet access without configuration.
* *DHCP is a protocol that delivers network configuration information on request.*
* Only one DHCP server can exist in a network at one time*.*

1. Please complete the following sentence:

DHCP works because UDP datagrams do not require a *source* address and can be sent to the local *broadcast* address*.*

**4.3**

1. Please mark the correct statement(s).

* The IANA always knows all relevant information for an IP address.
* Application-layer services can only communicate via the ports specified by the IANA.
* *The IANA is responsible for assigning IP address ranges to regional registrars.*

**4.4**

1. Please complete the following sentence:

NAT can allow *private* networks to talk to the internet*.*

1. Please mark the correct statement(s).

* *Firewalls operate on the network layer.*
* *Firewalls operate on the transport layer.*
* Firewalls operate on the link layer.

**4.5**

1. Please mark the correct statement(s).

* SOCKS is a network-layer protocol.
* Once connected, a SOCKS client uses the connection to transmit data to a third system.
* *SOCKS proxies are intended to circumvent firewalls.*

**Unit 5**

**5.1**

1. Please mark the correct statements.

* ARP response messages contain authenticity information.
* *ARP response messages cause changes in the ARP tables of receiving systems.*
* ARP response messages are sent periodically.

**5.2**

1. Please mark the correct statement(s).

* RIP messages are exchanged via TCP.
* RIP messages are encrypted.
* *RIP messages are exchanged by routers.*

1. Please list three reasons for a router to send a RIP message.

*it has received a request to do so*

*a timer has run out*

*a local change in the network topology has been detected*

1. Please complete the following sentence:

RIP tries to optimize network routing using a *distance-vector* algorithm.

**5.3**

1. Please mark the correct statements.

* The Border Gateway Protocol uses UDP to exchange routing information.
* *The Border Gateway Protocol is used to implement policies on a network level.*
* The Border Gateway Protocol is used to find the most efficient route between autonomous systems.

**5.4**

1. Please mark the correct statements.

* *AS numbers are required for inter-domain routing using BGP.*
* AS numbers are required for intra-domain routing using BGP.
* AS numbers are required for inter-domain routing using RIP.

**5.5**

1. Please mark the correct statement(s).

* RIP was specifically designed with protection from attacks in mind.
* BGP is impervious to attacks due to its reliance on TCP as a transport-layer protocol.
* *ARP poisoning is a method with which an attacker can impersonate a victim system.*

**Unit 6**

**6.1**

1. Please mark the correct statement(s).

* Subdomains are assigned by the IANA.
* *Fully qualified domain names globally identify systems connected to the internet.*
* There is exactly one DNS root server.

**6.2**

1. Please mark the correct statements.

* *The Domain Name System* *can be described as a distributed database.*
* The Domain Name System only contains IP addresses and their symbolic names.
* The Domain Name System always gives correct answers to queries.

1. Please list two entry types in DNS other than IP address records.

*SRV*

*MX*

*CNAME*

*SOA*

*TXT*

*NS*

1. Please complete the following sentence:

An *authoritative* DNS lookup retrieves its information directly from the responsible DNS server.

**6.3**

1. Please mark the correct statement(s).

* DNSSEC is used to encrypt DNS network traffic.
* *DNSSEC provides authenticity for data obtained by DNS queries.*
* The Domain Name System was designed with data integrity in mind.

**6.4**

1. Please mark the correct statement(s).

* SPF prevents identity theft.
* DMARC prevents identity theft.
* *DMARC provides a way to define how receivers of illegitimate mails should interact with supposed originator domains.*

**Unit 7**

**7.1**

1. Please complete the following sentence:

HTTP communication follows the *request-response* paradigm.

1. Please mark the correct statement(s).

* HTTP can only exchange hypertext documents.
* HTTP is a stateful communication protocol.
* *HTTP contains error-reporting capabilities.*

**7.2**

1. Please mark the correct statement(s).

* HTTP/2 is an incremental improvement over HTTP/1.1.
* *HTTP/2 is intended to provide a faster user experience.*
* HTTP/2 uses the exact same message format as HTTP/1.1.

**7.3**

1. Please complete the following sentence:

The SMTP protocol is used to exchange *electronic mail*.

1. Please mark the correct statement(s).

* SMTP is used to retrieve email from a remote mailbox.
* *SMTP is a stateful communication protocol.*
* SMTP is executed over UDP.

**Unit 8**

**8.1**

1. Please list three services the SSH protocol stack can provide.

*remote terminal sessions / interactive command line interfaces*

*file transfer*

*port forwarding*

*x11 forwarding*

*remote command execution*

1. Please mark the correct statement(s).

* In Diffie-Hellman Key exchanges private keys are transmitted over the network.
* *In Diffie-Hellman Key exchanges the public key of a remote peer and the local private key are used to calculate a shared key.*
* In Diffie-Hellman Key exchanges each peer uses a different key for the secure communication channel.

1. Please complete the following sentence:

In asymmetric encryption schemes, data are encrypted using *public* keys and decrypted using *private* keys in to ensure confidentiality.

**8.2**

1. Please list two subprotocols of the IPSec protocol stack.

*Internet Key Exchange / IKEv2*

*Encapsulating Security Payload*

*Authentication Header*

1. Please mark the correct statement(s).

* IPSec always encrypts the traffic source and destination.
* IPSec communicates over UDP.
* *IPSec is used to securely interconnect network segments.*

1. Please complete the following sentence:

Peers of security gateways can be *other security gateways* or *individual hosts*.

**8.3**

1. Please list two security objectives of the TLS protocol stack.

*confidentiality*

*authentication*

*integrity*

1. Please mark the correct statement(s).

* *TLS is never used on its own.*
* TLS always authenticates all peers.
* TLS can be used to secure application-layer protocols without changing their source code.

1. Please complete the following sentence:

TLS operates on the *transport layer* of the TCP/IP reference model.

**8.4**

1. Please mark the correct statement(s).

* *MitM attacks* *require an underlying attack.*
* MitM attacks can be completely negated using encryption techniques.
* MitM attacks are irrelevant when using public key infrastructures for authentication.

1. Please complete the following sentence:

In order to prevent MitM attacks, SSH performs server *key fingerprinting*.

**8.5**

1. Please list three mandatory certificate fields.

*subject name*

*subject public key*

*issuer name*

*validity period*

*signature algorithm*

*signature value*

1. Please mark the correct statement(s).

* Certificates never expire.
* Certificates contain private keys.
* *Certificates authenticate subjects.*

1. Please complete the following sentence:

Root certificates are *self-signed* certificates that are used as *trust anchors*.

**Unit 9**

**9.1**

1. Please mark the correct statement(s).

* Signature-based systems are inefficient.
* *Behavior-based systems are susceptible to false positives.*
* Network-based intrusion detection systems prevent network-based attacks.

**9.2**

1. Please mark the correct statement(s).

* Netflow monitoring works on the basis of historical data.
* *Netflow monitoring uses protocol information to determine suspicious activity.*
* Netflow monitoring cannot indicate the use of unknown protocols.

**9.3**

1. Please mark the correct statement(s).

* *Behavior-based systems are susceptible to false positives.*
* Signature-based systems are susceptible to false positives.
* False negatives can be easily detected.

**9.4**

1. Please list two data sources that can be integrated by SIEMs.

*system logs*

*patch-level data*

*performance data*

**9.5**

1. Please mark the correct statement(s).

* IDSs can help in the preparation phase of incident-management processes.
* *SIEMs can help in the preparation phase of incident-management processes.*
* IPSs can help in the assessment phase of incident-management processes.

**Unit 10**

**10.1**

1. Please mark the correct statement(s).

* Geographic aggregation is important in retracing sequential attack patterns.
* The compliance-relevancy of data is important for retracing sequential attack patterns.
* *Accurate time stamps are important for retracing sequential attack patterns.*

**10.2**

1. Please list two DNS-based data sources.

*DNS blacklists*

*passive DNS*

*DNS repositories*

1. Please mark the correct statement(s).

* Passive DNS data contain whole data sets from domains.
* The criteria for DNS blacklists are fixed.
* *DNS entries can change quickly over time.*

**10.3**

1. Please mark the correct statement(s).

* GeoIP data can be requested from Regional Internet Registries.
* *Data on autonomous systems can be requested from Regional Internet Registries.*
* Regional Internet Registries and the IANA take precedence over regional privacy protection legislation.

**10.4**

1. Please mark the correct statement(s).

* Certificates cannot be revoked.
* Certificate transparency log entries can be altered.
* *Certificate transparency can provide a second channel for verifying certificates.*

**10.5**

1. Please list three classification algorithms.

*Naïve Bayes*

*Bayesian networks*

*Markov chains*

*decision tree algorithms*

*support vector machines*

*artificial neural networks*

1. Please mark the correct statement(s).

* *Cluster analysis is an unsupervised learning method.*
* Classification is an unsupervised learning method.
* *Association rules contain a measure of reliability.*