1) Welche Aussagen sind bezüglich "A6 - Verlust der Vertraulichkeit sensibler Daten" (OWASP Top 10) wahr?

a) "Der Angreifer stiehlt das Sitzungscookie des Nutzers durch einfaches Mitlesen der unverschlüsselten Kommunikation" ist ein Beispielszenario für diese Schwachstelle. (100%)
b) Um Passwörter, die persistiert werden müssen, zu schützen, sollten diese zuerst "gesalzen" und dann zu einem Hashwert transformiert werden, bevor sie in der Datenbank abgelegt werden. (100%)
c) Sensible Daten erfordern einen zusätzlichen Schutz wie Verschlüsselung auf dem Speicher oder in der Kommunikation, sowie besondere Vorsichtsmaßnahmen, wenn sie mit dem Browser ausgetauscht werden. (100%)
d) Vor dem Persistieren von Daten, sollten diese stets mit TLS verschlüsselt werden. (0%)

2) Welche grundsätzlichen persönlichen Voraussetzungen sollte ein Penetration Tester mitbringen?

a) Ein Penetration Tester muss beim BSI (Bundesamt für Sicherheit in der Informationstechnologie) registriert sein (0%)
b) Da Penetration Tests als Projekte verwaltet werden sollten, muss der Penetration Tester Projektmanagement Skills mitbringen (100%)
c) Hin und wieder muss der Penetration Tester "um die Ecke" denken und sollte daher kreativ sein (100%)
d) Ein Penetration Tester sollte Kenntnisse u.a. in Systemadministration, Betriebssysteme, Netzwerkprotokolle und Programmiersprachen besitzen (100%)

3) Welche der folgenden Antworten beschreiben Methoden für die Informationsbeschaffung?

a) Test der Zutrittskontrollen (0%)
b) Verdeckte und offensichtliche Identifikation der Firewallsysteme (100%)
c) Verdeckte und offensichtliche Angriffe auf tatsächliche Schwachstellen (0%)
d) Test der administrativen Zugänge zur Telefonanlage (0%)

4) Welche Aussagen sind bezüglich "A1 - Injection" (OWASP Top 10) wahr?

a) Injection ermöglicht es Angreifern, Skripte im Browser des Opfers auszuführen. Diese Skripte können Benutzer-Sessions kapern, Webseiten verunstalten oder den Benutzer auf bösartige Websites umleiten. (0%)
b) Die bösartigen Daten des Angreifers können den Interpreter zur Ausführung von ungenehmigten Befehlen oder zum unbefugten Zugriff auf Daten bewegen (100%)
c) Injection funktioniert nur bei SQL-Datenbanken, nicht jedoch bei NoSQL-Datenbanken. Daher sollten SQL-Datenbanken vermieden werden. (0%)
d) Injektionsfehler betreffen nur Systeme, die ein Web-Formular haben, über das der Angreifer schädliche Befehle injizieren kann. (0%)

5) Was sind mögliche Beispielszenarien für längere Attacken?

a) Der Social Engineer installiert Spionagewerkzeuge, um das Opfer über einen längeren Zeitraum zu überwachen. (100%)
b) Der Angreifer versucht mit Hilfe einer Umfrage Informationen über das Unternehmen zu gewinnen. (0%)
c) Der Social Engineer verfasst eine Spear-Phishing E-Mail, um einen Mitarbeiter zum Anklicken auf einen Link zu animieren. (0%)
d) Der Angreifer lässt sich bei einem Partnerunternehmen als Mitarbeiter anstellen, um die Glaubwürdigkeit bei einem Angriff zu erhöhen. (100%)

6) Welche Zuordnungen von standardisierten Ports zu Diensten sind richtig? (nach Definition der nternet Assigned Numbers Authority (IANA))

a) Port: 80
Dienst: HTTP (100%)
b) Port: 443
Dienst: HTTPS (100%)
c) Port: 110
Dienst: FTP (0%)
d) Port: 8888
Dienst: TOMCAT (0%)

7) Welche Aussagen sind bezüglich Dumping Cached Passwords wahr?

a) Dumping Cached Passwords ist ein Synonym für Pass-the-Hash (0%)
b) Das primäre Ziel von Dumping Cached Passwords ist das Installieren von Rootkits und Backdoors. (0%)
c) Kerberos oder NTLM sind anfällig für Dumping Cached Passwords Angriffe (100%)
d) Windows speichert die letzten zehn Domänenanmeldeinformationen für den Fall, dass der Domänencontroller offline geschaltet wird (100%)

8) Welche Antwortmöglichkeiten beschreiben Grundtechniken des Social Engineerings?

a) Social Proof (100%)
b) Vortäuschen von Identitäten (100%)
c) Aufbau einer Vertrauenskette (100%)
d) Tailoring (0%)

9) Welche Aussagen sind bezüglich Privelege Escalation (Rechteausweitung) wahr?

a) Aktuelle Malware Protection und Anti Virus Software verhindert horizontale aber nicht vertikale Privilegienerweiterung (0%)
b) Eine Unterform der Privelege Escalation ist die Horizontal Privelege Escalation (100%)
c) Das primäre Ziel einer Privelege Escalation ist das Umleiten von Geld auf das Konto des Angreifers. (0%)
d) Ein Beispielszenario für Horizontal Privelege Escalation ist: Internet Banking User A greift auf das Internet Bankkonto von User B zu (100%)

10) Welche Aussagen sind bezüglich der Grundtechniken des Social Engineerings wahr?

a) Beim Social Proof wird der Einfluss der Gesellschaft genutzt, denn der Mensch passt sich i.d.R. seiner sozialen Umgebung an. (100%)
b) Autoritätshörigkeit bedeutet, dass die meisten Mitarbeiter stets darauf bedacht sind, Anordnungen von Vorgesetzten pflichtbewusst nachzugehen. (100%)
c) Beim "Aufbau einer Vertrauenskette" soll das Opfer annehmen, dass der Social Engineer von einer anderen Stelle bereits überprüft wurde. (100%)
d) Um die Glaubwürdigkeit zu erhöhen, sollten in einem Gespräch mit dem Opfer möglichst wenige Insider-Informationen eingebunden werden. (0%)

11) Welche Aussagen sind bezüglich NTLM (NT LAN Manager) wahr?

a) NTLM verwendet eine FaceID-Authentifizierung (0%)
b) NTLM ist ein Authentifizierungsverfahren für Rechnernetze (100%)
c) Der Nachfolger des NTLM-Protokolls ist RADIUS. (0%)
d) NTLM verwendet eine Challenge-Response-Authentifizierung (100%)

12) Welche Aussagen sind bezüglich "A3 - Cross-Site Scripting (XSS)" (OWASP Top 10) wahr?

a) XSS bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit Datenbanken, die durch mangelnde Maskierung oder Überprüfung von Metazeichen in Benutzereingaben entsteht. (0%)
b) JavaScript ist eine Programmiersprache, die für XSS ausgenutzt werden kann. (100%)
c) Die einzig sinnvolle Maßnahme gegen XSS ist die clientseitige Validierung der nicht vertrauenswürdigen Daten. (0%)
d) XSS ermöglicht es Angreifern, Skripte im Browser des Opfers auszuführen, die Benutzer-Sessions kapern, Webseiten verunstalten oder den Benutzer auf bösartige Websites umleiten können. (100%)

13) Laut der Passwortrichtlinie müssen für die Wahl des Passworts Klein- und Großbuchstaben aus dem englischen Alphabet (a-z entspricht 26 Zeichen) sowie Ziffern verwendet werden. Alle anderen Zeichen sind nicht erlaubt. Welche Aussagen sind richtig?

a) Die Erhöhung der Passwortlänge um 1 Zeichen erhöht die Komplexität um den Faktor 26. (0%)
b) Die Länge des Passwortes ist wichtiger als die Größe des Zeichensatzes (100%)
c) Der Zeichensatz besteht aus 62 Elementen. (100%)
d) Ein Passwort mit einer Länge von genau 12 Zeichen hat eine Komplexität von 12^62. (0%)

14) Welche Aussagen sind bezüglich "A9 - Verwendung von Komponenten mit Schwachstellen" (OWASP Top 10) wahr?

a) Anwendungen, die Komponenten mit bekannten Schwachstellen nutzen, können die Verteidigungsmechanismen der Anwendung aushebeln und so eine Reihe von Angriffen ermöglichen. (100%)
b) Bei der Verwendung von Komponenten sollte vorab gecheckt werden, ob diese bekannte Sicherheitslücken enthalten. (100%)
c) Selbstentwickelte Komponenten haben selten Sicherheitslücken. (0%)
d) Komponenten wie Bibliotheken, Frameworks und andere Software-Module laufen oft unter den gleichen Rechten wie die Anwendung selbst. (100%)

15) Welche Felder hat ein UDP Header?

a) UDP Flag (0%)
b) FIN Flag (0%)
c) Zieladresse (100%)
d) ACK Flag (0%)

16) Welche Aussagen sind bezüglich Speicher Rootkits wahr?

a) Die beste Methode zur Entfernung ist die vollständige Neuinstallation des Betriebssystems (100%)
b) Speicher-Rootkits existieren nur im Arbeitsspeicher des laufenden Systems (100%)
c) Nach dem Neustart („reboot“) des Systems sind diese Rootkits nicht mehr aktiv. (100%)
d) Speicher-Rootkits verstecken sich im BIOS des Rechners und werden vor dem Betriebssystem in den Speicher geladen (0%)

17) Welche Aussagen sind bezüglich Kerberos wahr?

a) Der Kerberos-Server selbst authentifiziert sich nicht gegenüber dem Client sondern nur gegenüber dem Server. (0%)
b) Mit Kerberos können Man-in-the-Middle-Angriffe abgewehrt werden (100%)
c) Das Kerberos Protokoll bietet keinen Schutz gegenüber Replay-Angriffen, bei denen zuvor aufgezeichnete Daten erneut versendet werden. (0%)
d) Nur auf dem Server muss ein Kerberos-Client installiert und konfiguriert sein, mit dem Client kommuniziert der Kerberos Server nicht. (0%)

18) Welche Aussagen sind bezüglich Pass-the-Hash (PtH) wahr?

a) Die einzige Möglichkeit, an zusätzliche Hashes zu kommen (Hash harvesting), ist das Auslesen der Hashes aus dem Arbeitsspeicher (bei Windows konkret der LSASS.EXE) des beherrschten Rechners. (0%)
b) Diese Technik kann gegen jeden Server oder Dienst ausgeführt werden, der die LM- oder NTLM-Authentifizierung akzeptiert, unabhängig davon ob auf einer Maschine Windows, Unix oder ein anderes Betriebssystem läuft. (100%)
c) Ein Pass-the-Hash Angriff ist eine modifizierte Man-in-The-Middle-Attack, bei der Angreifer den Hash durch seine Position in der Kommunikationstruktur abfangen können. (0%)
d) Pass-the-Hash läuft wie folgt ab:
1. User schickt eine Zugangsanfrage
2. Server schickt eine Challenge Message
3. User schickt Username und gestohlenes Hash
4. Server validiert Hash und gewährt Zugang (100%)

19) Welche Felder hat ein TCP Header?

a) Acknowledgement Nummer (100%)
b) Session ID (0%)
c) OS Version (0%)
d) Sequenznummern (100%)

20) Welche Aussagen sind bezüglich "A8 - Cross-Site Request Forgery (CSRF)" (OWASP Top 10) wahr?

a) Das Opfer muss auf der anfälligen Web-Anwendung eingeloggt sein, damit der Angreifer seinen Angriff ausführen kann. (100%)
b) Der Angreifer manipuliert beim CSRF Angriff die Session ID des Nutzers. (0%)
c) CSRF funktioniert nur, wenn der Nutzer die Ausführung von Skripten erlaubt. (0%)
d) Die Ursache für CSRF ist eine Sicherheitslücke im Browser des Nutzers. (0%)

21) Welche öffentliche Quellen sind geeignet, um an Informationen über das Opfer zu gelangen?

a) Soziale Netzwerke sind gute Quellen, um an private Informationen über das Opfer zu gelangen. (100%)
b) Der Eintrag im Domain Name Service kann Informationen zum Vorstand bzw. Geschäftsführer, zu täglichem Traffic und zu Domainnamen enthalten. (0%)
c) E-Mail Adressen auf der Homepage des Unternehmen können den Namen von Mitarbeitern enthalten. (100%)
d) Die Homepage des Unternehmens ist eine gute Quelle, um Informationen über das Unternehmen zu bekommen. (100%)

22) Welche Aussagen sind bezüglich Kernel Rootkits wahr?

a) Unter Windows werden Kernel-Rootkits häufig durch die Einbindung neuer .sys-Treiber realisiert (100%)
b) Kernel-Rootkits ersetzen Teile des Compilers durch eigenen Code, um sich selbst zu tarnen („stealth“) (0%)
c) Die Funktionalitäten des Kernel Rootkits werden am häufigsten durch Nachladen von Task-Modulen (LTE: linked task extensions) erweitert (0%)
d) Da eine hundertprozentige Entfernung von Rootkits durch einen Rootkit-Cleaner möglich ist, kann meist auf eine vollständige Neuinstallation des Betriebssystems verzichtet werden. (0%)

23) Welche Angriffe auf der Netzwerkebene gibt es tatsächlich?

a) Smurf-Angriff (100%)
b) TCP Sequence Prediction (100%)
c) SSL-Spoofing (0%)
d) ARP-Spoofing (100%)

24) Warum wird der Mensch bei einem Hacking Angriff als "schwächstes Glied in der Kette" gesehen?

a) ISO/IEC 27001 bietet ein einen Standard für ein Managementsystem, das die Infomationssicherheit erhöht. Nicht nach ISO/IEC 27001 zertifizierte Unternehmen haben deshalb schwache Mitarbeiter. (0%)
b) Die meisten Mitarbeiter haben Angst vor Disziplinarmaßnamen, weswegen sie die Sicherheitsmaßnahmen heimlich, aber bewusst, umgehen. Sie achten stets darauf, dass der Vorgesetzte es nie erfährt. (0%)
c) Eine fehlende Klassifizierung von Informationen kann leicht dazu führen, dass diese aus Versehen offengelegt werden. (100%)
d) Eine Erhöhung der Sicherheit kann auch dazu führen dass die Usability sinkt. Deshalb suchen manche Mitarbeiter Wege, um die Sicherheitsmaßnahmen zu umgehen. (100%)

25) Welche Aussagen sind bezüglich dem TLS Protokoll (Transport Layer Security) wahr?

a) Wenn der Client sich mit einem eigenen Zertifikat auch gegenüber dem Server authentifiziert, gilt TLS als sicher. (0%)
b) TLS-Implementierungen sind in wiederkehrender Regelmäßigkeit von sicherheitsrelevanten Implementierungsfehlern betroffen. (100%)
c) Im OSI-Modell ist TLS in der Sicherungsschicht (Data Link Layer) angeordnet. (0%)
d) Mit Hilfe des BEAST Angriffes kann ein Hacker mit einem Chosen-Plaintext-Angriff auf verschlüsselte Infomationen durchführen (100%)

26) Welche Aussagen sind bezüglich "OS-Fingerprinting" und "Banner Grabbing" wahr?

a) UDPrint ist ein Tool, um OS Fingerprinting via UDP durchzuführen (0%)
b) OS-Fingerprinting kann sowohl eine aktive als auch eine passive Informationsbeschaffungsmethode darstellen (100%)
c) Nmap ist ein Tool, um OS Fingerprinting durchzuführen (100%)
d) Die 67-Bit-Signatur kann Aufschluss darüber geben, welches Betriebssystem auf einem Host läuft (100%)

27) Welche Gegenmaßnahmen können helfen, Rootkits zu entfernen bzw. sich gegen diese zu schützen?

a) BIOS hardwareseitig mit einem Schreibschutz versehen (100%)
b) Austausch der Hardware (100%)
c) Neuinstallation des Betriebssystems (100%)
d) Einsatz von Betriebssystemvirtualisierung in Containern um Rootkits zu isolieren. (0%)

28) Welche Fragen sollte sich ein Social Engineer stellen, um sich auf einen Angriff über das Telefon vorzubereiten, bei dem eine Identität vorgetäuscht wird?

a) Welchen Akzent hat die gespielte Person? (100%)
b) Wie beschäftigt ist die gespielte Person? (100%)
c) Wie sprachgewandt ist die gespielte Person? (100%)
d) Welche Skills hat die gespielte Person? (100%)

29) Welche Aussagen sind bezüglich eines TCP Handshakes wahr?

a) Nach dem Drei-Wege-Handschlag ist die Verbindung für beide Kommunikationspartner gleichberechtigt, man kann einer bestehenden Verbindung auf TCP-Ebene nicht ansehen, wer der Server und wer der Client ist. (100%)
b) Sequenznummern werden bei TCP verwendet, um eine vollständige Übertragung in der richtigen Reihenfolge und ohne Duplikate (also einen Datenstrom) zu realisieren. (100%)
c) Der Destination Port muss beim Drei-Wege-Handschlag immer kleiner 1024 sein (0%)
d) Er läuft wie folgt ab:
1. SYN seq= x ack = 0 (Client)
2. SYN ACK seq= y ack = x +1 (Server)
3. ACK seq= x +1 ack = y +1 (Client) (100%)

30) Welche Aussagen sind bezüglich unterstützenden Technologien beim Social Engineering wahr?

a) Ein Rogue Access Point kann den Datenverkehr, der über ihn läuft, mitschneiden. (100%)
b) Ein Rogue Access Point ist der Access Point des Zielunternehmens. (0%)
c) Audio Recording Tools eignen sich, um Tonaufnahmen von Gesprächen zu machen. (100%)
d) WIFI Pineapple ist ein Gerät, das jede SSID imitieren kann. (100%)

31) Welche Aussagen sind bezüglich "A4 - Unsichere direkte Objektreferenzen" (OWASP Top 10) wahr?

a) Ohne eine Zugriffsprüfung oder anderen Schutz, können Angreifer u.U. direkte Verweise manipulieren, um unberechtigt auf Daten zuzugreifen. (100%)
b) Diese Sicherheitlücke lässt sich mit einem "Stored Procedure" beheben. (0%)
c) Unsichere direkte Objektreferenzen können auch auf Systemdateien auf der Festplatte des Benutzers verweisen. (0%)
d) Die Secure Coding Richtlinie sollte jeden Programmierer darauf aufmerksam machen, dass direkte Objektreferenzen einen effektiven Schutz vor unberechtigtem Zugriff benötigen. (100%)

32) Welche der folgenden Aussagen sind bezüglich Brute-Force wahr?

a) Die Anzahl der möglichen Kombinationen ist abhängig von der Passwortlänge (100%)
b) Die Entzifferungsdauer ist abhängig von den möglichen Kombinationen und der Leistung des verwendeten Rechners (100%)
c) Die Brute-Force-Methode ist eine Lösungsmethode für Probleme aus den Bereichen Informatik, Kryptologie und Spieltheorie, die auf dem Ausprobieren aller möglichen Fälle beruht (100%)
d) Die Anzahl der möglichen Kombinationen ist abhängig von dem verwendeten Zeichensatz (100%)

33) Welche der folgenden Antworten beschreiben Methoden für den aktiven Angriff?

a) Brute Force Attacke (100%)
b) Test von Vertrauensbeziehungen zwischen Systemen (100%)
c) Test der Zutrittskontrollen (100%)
d) Computerbasiertes Social-Engineering (100%)

34) Welche Aussagen sind bezüglich Ping of Death und ICMP wahr?

a) Ein manipuliertes ICMP-Datenpaket erzeugt aufgrund eines Fehlers in der Implementierung des Internet Protocols einen Buffer Overflow (100%)
b) Das Ziel ist es, das angegriffene System so zu manipulieren, dass es ICMP Pakete an andere Rechner im Netzwerk sendet (0%)
c) Der Ping of Death ist eine Denial-of-Service-Attacke (DoS-Attacke) (100%)
d) Das Blockieren von ICMP an einer Firewall ist das einzige Mittel den PoD Angriff erfolgreich zu verhindern. (0%)

35) Welche Aussagen sind bezüglich "Session Hijacking" wahr?

a) Ziel des Angreifers ist es, durch die „Entführung“ dieser Sitzung die Vertrauensstellung auszunutzen, um dieselben Privilegien wie der rechtmäßig authentifizierte Benutzer zu erlangen (100%)
b) UDP Sitzungen können nicht entführt werden (100%)
c) TCP Sitzungen können entführt werden (100%)
d) Session Hijacking ist ein Angriff auf eine verbindungsbehaftete Datenkommunikation zwischen zwei Computern (100%)

36) Welche Angriffsmöglichkeiten gibt es, um das Betriebssystem anzugreifen?

a) OS-Force-Breaking (0%)
b) Buffer Overflow (100%)
c) Jailbreaking (100%)
d) Dumping Cached Passwords (100%)

37) Welche Aussagen sind bezüglich "A5 - Sicherheitsrelevante Fehlkonfiguration" (OWASP Top 10) wahr?

a) Die Konfiguration von Servern sollte stets vom Informationssicherheitsbeauftragten (ISB) abgenommen werden. (0%)
b) Software, die Defaultpasswörter verwendet, darf unter keinen Umständen eingesetzt werden, selbst wenn diese änderbar wären. (0%)
c) Sichere Einstellungen sollten definiert, umgesetzt und gepflegt werden, da Defaultwerte oft unsicher sind. (100%)
d) ISO/IEC 27001 zertifizierte Software bietet einen besonderen Schutz gegen diese Art von Schwachstellen. (0%)

38) Was gehört zu einer vollständigen Dokumentation eines Penetrationstestes?

a) Dokumentation aller Sicherheitsvorfälle vor dem Penetration Test (0%)
b) Dokumentation der durchgeführten aktiven Angriffe (inkl. Logfiles der eingesetzten Tools) (100%)
c) Dokumentation der abgearbeiteten Prüfungsschritte zur Informationsbeschaffung (100%)
d) Abschlussbericht (100%)

39) Welche Aussagen sind bezüglich Credential Harvesting wahr?

a) Das "Nmap Tool" ist ein Programm, das Credential Harvesting unterstützt. (0%)
b) Credential Harvesting ist eine Social Engineering Methode. (100%)
c) Beim Credential Harvesting werden über eine "Fake" Loginseite Zugangsdaten gesammelt. (100%)
d) Um an die Zugangsdaten des Opfers zu gelangen, kann einem Credential Harvesting Angriff ein SMiShing Angriff vorausgehen. (100%)

40) Welche Aussagen sind bezüglich "Buffer Overflow" wahr?

a) Buffer Overflow kann beim Kopieren von Daten von einem Puffer zum anderen erfolgen. (100%)
b) Um sich gegen Buffer Overflow zu schützen, sollte stets ein verschlüsselter Arbeitsspeicher eingesetzt werden. (0%)
c) Auf Grunde der Architektur des Prozessors sind Buffer Overflow Fehler nur bei Software, die auf einem PC installiert ist möglich. (0%)
d) Buffer Overflow ist eine alte Sicherheitslücke und kann auf modernen System nicht mehr auftreten. (0%)

41) Welche grundsätzlichen Phasen hat ein Penetration Test?

a) Abschlussanalyse (100%)
b) Informationsbeschaffung (100%)
c) Pflege von Kontakten zu Behörden (0%)
d) Definition von Messzahlen (KPI) zu Information Security Incidents (0%)

42) Welche der folgenden Systeme beschreiben symmetrische Kryptosysteme?

a) Caesar-Verschlüsselung (100%)
b) AES - Advanced Encryption Standard (100%)
c) One-Time-Pad (100%)
d) Diffie Hellman (0%)

43) Was sind mögliche Angriffsvektoren beim reinen Social Engineering?

a) Der Social Engineer manipuliert den Drucker, um an die Druckdaten zu gelangen. (0%)
b) Der Social Engineer ruft das Opfer per Telefon an, um es zu einer bestimmten Handlung zu bewegen. (100%)
c) Der Social Engineer beschafft sich Informationen über das Opfer aus öffentlichen Quellen, um sich auf weitere Angriffe vorzubereiten. (100%)
d) Der Social Engineer knackt die Türen zu den Büroräumen, um Zutritt zu erhalten. (100%)

44) Welche Aussagen sind bezüglich Userland Rootkits wahr?

a) Userland-Rootkits sind vor allem unter MacOS populär, da sie unter Windows nicht funktionieren (0%)
b) Userland-Rootkits können nur in Assemblercode programmiert werden (0%)
c) Userland-Rootkits benötigen keinen Zugriff auf der Kernel-Ebene (100%)
d) Userland-Rootkits stellen jeweils eine DLL (Dynamic Link Library) bereit, die sich anhand verschiedener API-Methoden direkt in alle Prozesse einklinkt (100%)

45) Welche Aussagen sind bezüglich IP Adressen wahr?

a) Eine IPv4-Adresse besteht aus einem Netzanteil und einem Hostanteil (100%)
b) IPv4 benutzt 64-Bit-Adressen (0%)
c) IPv6 benutzt 265-Bit-Adressen (0%)
d) Mehrere Rechner befinden sich im selben Teilnetz (= lokal), wenn der Netzanteil ihrer Adresse (IPv4) gleich ist (100%)

46) Welche Aussagen sind bezüglich Thread Modeling wahr?

a) Neben einem Threat Model wird beim Threat Modeling typischerweise auch eine priorisierte Liste von potenziellen künftigen Sicherheitsvorfällen erzeugt. (0%)
b) Threat Modeling ermöglicht eine fundierte Entscheidungsfindung über das Sicherheitsrisiko. (100%)
c) Threat Modeling ist ein Prozess zur Erfassung, Organisation und Analyse aller Informationen, die sich auf die Sicherheit eines Systems auswirken. (100%)
d) Threat Modeling ist ein Prozess zur Erfassung, Organisation und Analyse aller eingesetzten Tools im Unternehmen. (0%)

47) Was sind mögliche Beispielszenarien für schnelle Attacken?

a) Der Angreifer kontaktiert den Help Desk, um ein neues Passwort zu bekommen. (100%)
b) Der Angreifer versucht mit Hilfe einer Umfrage Informationen über das Unternehmen zu gewinnen. (100%)
c) Der Angreifer lässt sich beim Zielunternehmen als Praktikant anstellen, um näher am Opfer zu sein. (0%)
d) Der Social Engineer verfasst eine Spear-Phishing E-Mail, um einen Mitarbeiter zum Anklicken auf einen Link zu animieren. (100%)

48) Welche Aussagen sind bezüglich "A2 - Fehler im Authentifizierungs- und Session Management" (OWASP Top 10) wahr?

a) Nutzersitzungen sollten erst beendet werden, wenn sich der Nutzer abmeldet. Dies unterstützt die Verfügbarkeit und Performance des Systems. (0%)
b) Durch ein fehlerhaftes Session-Management könnten Sitzungen entführt (Session Hijacking) werden. (100%)
c) Session IDs sollten nie im Klartext persistiert werden, da sie ansonsten entführt werden können. (0%)
d) Die Session IDs, die vom Browser generiert werden, sollten immer eindeutig sein, da ein Angreifer ansonsten die Webapplikation hacken kann. (0%)

49) Was sind mögliche Angriffszenarien, um die Autoritätshörigkeit von Mitarbeitern auszunutzen?

a) Der Social Engineer gibt sich als Teil des Managements aus. (100%)
b) Der Social Engineer verkleidet sich als Polizeibeamter. (100%)
c) Der Social Engineer manipuliert das Smartphone des Chefs, um an seine Kontaktliste zu gelangen. (0%)
d) Der Social Engineer gibt sich als Bürgermeister aus. (100%)

50) Welche Aktivitäten müssen laut der allgemeinen Methodik beim Threat Modeling durchgeführt werden?

a) Identifizierung von Messzahlen zu Information Security Incidents (0%)
b) Entwicklung eines Security Threat Response Plans (100%)
c) Dokumentation der durchgeführten aktiven Angriffe (inkl. Logfiles der eingesetzten Tools) (0%)
d) Aufklärendes Gespräch mit dem CEO des Unternehmens (0%)