

- 1) Welche der folgenden Aussagen sind zum Thema asymmetrische Verschlüsselungen korrekt?
- a) AES (Advanced Encryption Standard) ist ein Beispiel für einen asymmetrischen Verschlüsselungsstandard. (0%)
  - b) „Asymmetrisches Kryptosystem“ ist ein Oberbegriff für Public-Key-Verschlüsselungsverfahren, Public-Key-Authentifizierung und digitale Signaturen. (100%)**
  - c) RSA (Rivest, Shamir und Adleman) ist ein asymmetrisches kryptographisches Verfahren, das sowohl zum Verschlüsseln, als auch zum digitalen Signieren verwendet werden kann. (100%)**
- 2) Welche Aussage ist bezüglich eines Angriffs durch Manipulation der URL-Parameter wahr?
- a) Die Manipulation von URL-Parametern ist nur zusammen mit einer http-Fake-Attacke sinnvoll. (0%)
  - b) Verantwortlich für die Anfälligkeit ist die Applikation bzw. die Verarbeitung der Parameter in derselben und nicht die Konfiguration des Webserver. (100%)**
  - c) Nur ältere Webserver verarbeiten manipulierte URL-Parameter falsch. Neuere Versionen der gängigen Webserver sind durch ihre Default-Konfiguration geschützt. (0%)
- 3) Welche der folgenden Aussagen bezüglich eines Wörterbuch-Angriffs auf Passwort-Hashes sind korrekt?
- a) Wörterbuch-Angriffe werden erleichtert, wenn der „Verteidiger“ vor der Anwendung der Hash-Funktion eine zufällige Zeichenfolge (Salt) hinzufügt. (0%)
  - b) Der Wörterbuch-Angriff ist eine Methode der Kryptographie, ein bekanntes Passwort mit Hilfe eines Wörterbuchs auf seine Sicherheit hin zu überprüfen. (0%)
  - c) Wörterbuch-Angriffe werden erschwert, wenn der "Verteidiger" vor der Anwendung der Hash-Funktion eine zufällige Zeichenfolge (Salt) hinzufügt. (100%)**
- 4) Welche Aussagen bezüglich des Angriffes Directory Traversal sind wahr?
- a) Bei einem Directory Traversal Angriff versucht der Angreifer, auf Verzeichnisse oder Dateien außerhalb der Webserver-Root zuzugreifen. (100%)**
  - b) Unter Directory Traversal versteht man einen Angriff, bei dem einem Webserver ein falsches Betriebssystem vorgetäuscht wird. (0%)
  - c) Ein Penetrationstest ist eine Möglichkeit, um Directory Traversal zu entdecken. (100%)**
- 5) Welche Aussagen bezüglich der Brute-Force-Methode auf Passwort-Hashes sind wahr?
- a) Bei der Brute-Force-Methode ist die Rechenleistung kein entscheidendes Kriterium, wie schnell ein Passwort geknackt werden kann. (0%)
  - b) Sollte ein 12-stelliges Passwort nur aus alphanumerischen Zeichen bestehen, so ist die Brute-Force-Methode durchschnittlich schneller erfolgreich, als bei einem gleichlangen Passwort, das nur aus Klein- und Großbuchstaben besteht. (0%)
  - c) Sollte ein 8-stelliges Passwort nur aus Zahlen bestehen, so ist die Brute-Force-Methode durchschnittlich schneller erfolgreich, als bei einem gleichlangen Passwort, das aus alphanumerischen Zeichen besteht. (100%)**

- 6) Welche der folgenden Ziele hat ein Penetrationstest?
- a) **Bestätigung der Sicherheit durch eine unabhängige Person. (100%)**
  - b) Aufdecken von organisatorischen Mängeln bei der Untersuchung von Sicherheitsvorfällen. (0%)
  - c) **Die Identifikation von Schwachstellen. (100%)**
- 7) Welche der folgenden Aussagen bezüglich Drive-by-Download sind wahr?
- a) Unter Drive-by-Download versteht man ausschließlich das bewusste Herunterladen von Schadsoftware auf einem Rechner. (0%)
  - b) **Beim Drive-by-Download werden auch Sicherheitslücken des Browsers ausgenutzt. (100%)**
  - c) **Unter Drive-by-Download versteht man das unbewusste und unabsichtliche Herunterladen von Schadsoftware auf einem Rechner. (100%)**
- 8) Welche Anforderungen an eine forensische Untersuchung sind wahr?
- a) Es sind ausschließlich Methoden erlaubt, die von der Fachwelt beschrieben und allgemein akzeptiert sind. (0%)
  - b) **Mit demselben Ausgangsmaterial müssen Dritte bei gleicher Methodik und den gleichen Hilfsmitteln zu identischen Ergebnissen kommen. (100%)**
  - c) **Bei der Anfertigung einer forensischen Duplikation müssen Lesefehler eindeutig erkannt und protokolliert und durch ein vorher festgelegtes Füllmuster ersetzt werden. (100%)**
- 9) Welche Aussagen sind bezüglich Cross-Site-Scripting wahr?
- a) **Bei einem Cross-Site-Scripting Angriff kann der Angreifer, dem Benutzer eine andere als die aufgerufene Webseite unterschieben. (100%)**
  - b) Unter Cross-Site-Scripting versteht man das Ausnutzen einer Sicherheitslücke im Zusammenhang mit einer Datenbank, die durch den Mangel der Maskierung oder Überprüfung von Metazeichen, bei einer Benutzereingabe entstehen. (0%)
  - c) Nur Applikationen, die in Java Script geschrieben sind, sind von Cross-Site-Scripting betroffen. (0%)
- 10) Welche Aussagen bezüglich ARP (Address Resolution Protocol) sind richtig?
- a) ARP wird in Ethernet-Netzen (IPV6) zur Ermittlung von MAC-Adressen bei gegebenen IP-Adressen verwendet. (0%)
  - b) **Die MAC-Adressen jeder Schnittstelle sind theoretisch weltweit eindeutig. (100%)**
  - c) Sollte ein ARP Request lokal nicht erfolgreich sein, so wird die Anfrage an benachbarte Netzwerksegmente weitergeleitet. ARP Relay. (0%)
- 11) Welche der folgenden Antworten bezüglich DNS-Spoofing bzw. Cache Poisoning sind wahr?
- a) **DNS-Spoofing ist ein Angriff auf das Domain Name System. (100%)**
  - b) **Das Ziel von DNS-Spoofing bzw. Cache Poisoning ist es, den Datenverkehr unbemerkt zu einem anderen Computer zu lenken. (100%)**
  - c) Unter DNS-Spoofing bzw. Cache Poisoning versteht man das Blockieren aller DNS-Server einer Infrastruktur, so dass nicht mehr im Internet gesurft werden kann. (0%)

- 12) Welche Aussagen bezüglich IT-Forensik sind wahr?
- a) Die IT-Forensik ist eine Datenanalyse, bei der es nicht auf ein methodisches Vorgehen ankommt, da nur die Ergebnisse in einem Bericht dokumentiert werden. (0%)
  - b) Bei einer forensischen Analyse ist es prinzipiell wichtig, nach Spuren zu suchen, die die These, wie ein Angriff stattgefunden haben könnte, untermauern oder widerlegen. (100%)**
  - c) Die IT-Forensik dient der Aufklärung von Sicherheitsvorfällen. (100%)**
- 13) Welche der folgenden Aussagen zum Man-in-the-Middle-Angriff (MITM) sind wahr?
- a) Bei einem Man-in-the-Middle-Angriff versucht der Angreifer, sich physisch oder logisch zwischen zwei Kommunikationspartner zu schieben. (100%)**
  - b) Bei einem Man-in-the-Middle Angriff können Daten mitgelesen werden, jedoch ist keine Datenmanipulation möglich. (0%)
  - c) Ein Man-in-the-Middle-Angriff ist immer damit verbunden, dass ein falscher DHCP-Server vorgespielt werden muss. Dieser falsche DHCP-Server gibt an einen falschen DNS-Server bzw. Gateway aus, der vom Angreifer kontrolliert wird. (0%)
- 14) Welche der folgenden Kriterien sind im Klassifikationsschema für Penetrationstests nach BSI vorhanden?
- a) Umfang (100%)**
  - b) Verbreitungskoeffizienz (0%)
  - c) Zuverlässigkeit (0%)
- 15) Welche der folgenden Aussagen sind bezüglich SQL-Injection wahr?
- a) SQL-Injection ist meist dann möglich, wenn durch mangelnde Maskierung bzw. Überprüfung von Benutzer-Eingaben SQL-Befehle ausgeführt werden. (100%)**
  - b) Das Ziel von SQL-Injection ist das Ausspionieren von Informationen oder das Zerstören von Daten. (100%)**
  - c) SQL-Injections sind dann möglich, wenn Daten wie beispielsweise Benutzereingaben ungeprüft in den SQL-Interpreter gelangen. (100%)**
- 16) Die Verschlüsselung mit Rot13 (rotate by 13 places) ist ein bekanntes Verschlüsselungsverfahren. Welche Aussagen sind wahr?
- a) Die Technik gilt als sicher, wenn der Schlüssel größer als 512 bit ( $2^{512} = 1,3407807929942597099574024998206e+154$ ) ist. (0%)
  - b) Die Technik dient zum Verschleiern von Text z.B. bei Information, da der Leser aktiv etwas tun muss und nicht "zufällig" den Text lesen kann. (100%)**
  - c) Es ist ein symmetrisches Verschlüsselungsverfahren, das auf der monographischen und monoalphabetischen Substitution basiert. (100%)**
- 17) Welche der folgenden Aussagen zum Begriff "Google Hacking" sind wahr?
- a) Mit Hilfe des Parameters "intitle" kann man in URLs nach einer bestimmten Zeichenfolge suchen. (0%)
  - b) Google Hacking ist eine Software von Google für Penetrationstests. (0%)
  - c) site: ist ein Befehl, der verwendet werden kann, wenn man gezielt eine Information auf einer speziellen Seite sucht. (100%)**

- 18) Welche der folgenden Tätigkeiten gelten als aktives Footprinting?
- a) **OS-Fingerprinting (100%)**
  - b) **WHOIS-Abfrage (100%)**
  - c) Besuch auf der Webseite (0%)
- 19) Welche der folgenden Antworten in Bezug auf ARP-Spoofing und dem Adress-Resolution-Protocol (ARP) sind wahr?
- a) Das Ziel von ARP-Spoofing ist es, durch Manipulation der TCP-Adresse, Datenkommunikation abzuhören. (0%)
  - b) **Das ARP-Protocol dient der Zuordnung von IP-Adressen auf MAC-Adressen. (100%)**
  - c) **ARP-Spoofing kann erkannt werden, wenn auf höheren Protokollebenen, z.B. bei SSH Verbindungen, der Kommunikationspartner erneut überprüft wird. (100%)**
- 20) Welche Antworten sind bezüglich Sniffer wahr?
- a) **Es ist von der Netzwerkstruktur abhängig, welche Daten ein Sniffer sehen kann. (100%)**
  - b) **Ein Sniffer ist ein Tool der Netzwerkanalyse. (100%)**
  - c) **Ein Sniffer ermöglicht das Mitlesen des Datenverkehrs. (100%)**
- 21) Welche der folgenden Antworten zum Thema Session Hijacking sind wahr?
- a) Bei Session Hijacking ist das Ziel des Angreifers, sich bei Verbindungsaufbau zwischen den beiden Kommunikationspartnern zu platzieren. (0%)
  - b) **Session Hijacking kann auch durchgeführt werden, wenn man sich nicht im selben Netzwerksegment wie einer der beiden Kommunikationspartner befindet. (100%)**
  - c) Session Hijacking findet nur auf der zweiten Ebene - die Sicherungsschicht Data Link Layer - des OSI-Schichtenmodells statt. (0%)
- 22) Welche der folgenden Aussagen bezüglich Hash-Funktionen sind wahr?
- a) Bei einer Hash-Funktion sollte man immer vom Hash-Wert auf die ursprüngliche Zeichenfolge schließen können. (0%)
  - b) Eine Hash-Funktion ist eine zwischen zwei Parteien vereinbarte Zeichenfolge, die zur Authentifizierung benutzt wird (0%)
  - c) **Die kryptologische Hashfunktion ist eine spezielle Form der Hashfunktion, welche kollisionsresistent oder eine Einwegfunktion (oder beides) ist. (100%)**
- 23) Welche Aussagen sind bezüglich der Tätigkeit "Aufbereitung und Präsentation" bei einer forensischen Untersuchung wahr?
- a) **In diesem Schritt werden als erster Teilschritt die Erkenntnisse einer Untersuchung in Form eines Berichtes dokumentiert. (100%)**
  - b) In dieser Phase wird die vorgefundene Situation anhand der gesicherten Informationen durch interne und externe Experten untersucht. (0%)
  - c) In diesem Schritt wird als zweite Teilaktivität das Vorgehen in Form einer Präsentation vorgestellt. (0%)

- 24) Welche der folgenden Aussagen zum Thema "Cracker" sind richtig?
- a) Ein Cracker ist eine Person, die es mit dem Gesetz nicht so genau nimmt und bei ihrem Angriff bewusst oder absichtlich die Beschädigung von Informationen hinnimmt. (100%)
  - b) Der Begriff "Cracker" ist nicht eindeutig. Vor allem in der Presse werden Hacker und Cracker als Synonyme verwendet. (100%)
  - c) Ein Cracker überprüft die Sicherheit von Programmen, Systemen und/oder Services im Bereich der IT. (100%)
- 25) Welche der folgenden Aussagen zum Thema OS-Fingerprinting sind wahr?
- a) Um sich gegen OS-Fingerprinting zu schützen, kann man z.B. die sog. Banner der Service, wie z.B. FTP verfälschen. (100%)
  - b) Unter OS-Fingerprinting versteht man das Ermitteln des Betriebssystems über ein Netz unter Beobachtung von diversen Reaktionsarten. (100%)
  - c) Man unterscheidet implizites und explizites OS-Fingerprinting. (0%)
- 26) Bringen Sie diese Tätigkeiten einer forensischen Untersuchung in die richtige Reihenfolge.
- a) Identifizierung - Datensicherung - Analyse - Aufbereitung und Präsentation (100%)
  - b) Datensicherung - Analyse - Identifizierung - Aufbereitung und Präsentation (0%)
  - c) Datensicherung - Identifizierung - Analyse - Aufbereitung und Präsentation (0%)
- 27) Welche Aussagen bezüglich IP-Spoofing bzw. dem Internet-Protocol sind wahr?
- a) Bei IP-Spoofing wird dafür gesorgt, dass der DHCP-Server falsche IP-Adressen ausgibt. (0%)
  - b) Das Internet-Protocol ist in der ersten Schicht (Netzzugang) der Internetprotokollfamilie zugeordnet. (0%)
  - c) IPv4 benutzt 32-Bit-Adressen. (100%)
- 28) Welche Maßnahmen können getroffen werden, um das Risiko des versehentlichen Herunterladens (Drive-by-Download) von Schadsoftware zu verringern?
- a) Einführen von Domain Name System Security Extensions (DNSSEC), um die Integrität der heruntergeladenen Daten zu erhöhen. (0%)
  - b) Eine täglich aktualisierte Anti-Virus-Software minimiert das Risiko. (100%)
  - c) Bei der Verwendung von HTTPS-Verbindungen sinkt das Risiko einer Infektion deutlich. (0%)
- 29) Welche Aussagen sind bezüglich der Tätigkeit "Identifizierung" bei einer forensischen Untersuchung wahr?
- a) Der Tätigkeitsschwerpunkt liegt in der möglichst genauen Dokumentation der vorgefundenen Situation. (100%)
  - b) Die Aktivität "Identifizierung" ist der erste Schritt einer forensischen Untersuchung. (100%)
  - c) Neben der Bestandsaufnahme des eigentlichen Sicherheitsvorfalles werden auch bei dieser Phase erste Vermutungen angestellt. (100%)

- 30) Was sind grundlegende Voraussetzungen für die Sicherheit des Einmalschlüssel-Verfahrens (One-Time-Pad)?
- a) **Der Einmalschlüssel muss so lang sein wie die Nachricht. (100%)**
  - b) **Der Einmalschlüssel muss für alle Zeiten geheim bleiben. (100%)**
  - c) Auch eine sichere Aufbewahrung des Schlüssels ist nicht essentiell. (0%)