

ITS2 - 2019 Klausurfragen - wahrscheinlich	2
ITS2 - 2018 Klausurfragen	25
ITS2 - 2019 ProbeKlausur 100%	53

Sie haben die folgende Antwort gegeben:

## IT-Sicherheit 2 - Weitere Frage

Montag, 11. Februar 2019

18:26

**Virus Einsprung (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welcher Virus verschleiert seinen *Einsprung*?

- ☐ EPO-Virus
- ☐ Überschreibender Virus
- ☐ Appending-Virus
- ☐ Companion-Virus

Von (inkl)  
448964  
-  
449046  
Bis (inkl)

Informationssicherheit schützt die Vertraulichkeit, Integrität und Verfügbarkeit

- ☐ aller relevanten Informationen einer Institution ✗
- ☐ nur der personenbezogenen Daten einer Institution ✗
- ☐ nur der elektronisch gespeicherten Daten einer Institution ✗
- ☐ alle nicht-kritischen Information einer Institution ✗

5

**Viren-Selbstschutz (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was ist **kein** Viren-Selbstschutz?

- ☐ Strength
- ☐ Stealth
- ☐ Polymorphie
- ☐ Metamorphie

**Infektionswege (2 Punkte)**

Sie haben die folgende Antwort gegeben:

Was sind die *wesentlichen* Infektionswege für Schadsoftware?

- ☐ Ausführung des Schadprogramms durch Benutzer ✗
- ☐ Ausnutzen einer Schwachstelle des Systems ✗
- ☐ Durchführen eines Man-in-the-Middle Angriffs ✓
- ☐ Spoofing der Benutzer-Identität ✓

6

**Handy-Wurm ikee (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welche Voraussetzung des iPhones war für den Erfolg des Handy-Wurms *ikee* **nicht** relevant?

- ☐ Das Telefon musste entsperrt sein
- ☐ Das Telefon musste mit einem Jailbreak für nicht-offizielle Anwendungen offen sein
- ☐ Auf dem Telefon musste ein bestimmter SSH Server installiert sein
- ☐ Standard-Passwörter mussten unverändert sein

**Virusaufbau (2 Punkte)**

Sie haben die folgende Antwort gegeben:

Welche Teile gehören (ggf. optional) zum Aufbau eines Virus?

- ☐ Erkennungsteil ✗
- ☐ Bedingungsteil ✗
- ☐ Versteckungsteil ✓
- ☐ Kontrollteil ✓

7

**Trojanisches Pferd (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was stimmt für ein *trojanisches Pferd* **nicht**?

- ☐ Infiziert andere Dateien
- ☐

Enthält griechische Soldaten



Hat tatsächliche nützliche Funktionalität



Besteht aus zwei miteinander verbundenen Programmen

**8 Trojanisches Pferd (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Womit wirbt ein Trojanisches Pferd für sich selbst?



Mit der Nützlichkeit des Wirtsprogramms



Mit schadhaft verlinkten Werbebannern



Mit der Qualität von Partnerprogrammen



Mit einfacher Verbreitung

**9**

**Software-Schwachstelle (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was ist normalerweise **kein** Grund für Software-Schwachstellen?



Technische Limitationen der Programmiersprache



Schlechte Programmierung



Komplexität der Systeme



Zeitdruck in Projekten

**10**

**Teilmenge (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was ist eine Teilmenge von was?



Exploits sind eine Teilmenge von Angriffen, die wiederum eine Teilmenge von Gefährdungen sind



Angriffe sind eine Teilmenge von Exploits, die wiederum eine Teilmenge von Gefährdungen sind



Gefährdungen sind eine Teilmenge von Exploits, die wiederum eine Teilmenge von Angriffen sind



Angriffe sind eine Teilmenge von Gefährdungen, die wiederum eine Teilmenge von Exploits sind

**11**

**Puffer (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Sie schreiben den String „overflow“ in einen 9 Byte langen Puffer. Was steht im neunten Byte (hexadezimal)?

☐ 00

☐ FF

☐ 77

☐ 09

12

**Buffer Overflow (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was versucht ein Angreifer bei einem *Buffer Overflow* gezielt auf dem Stack zu überschreiben?

☒ Rücksprungadresse

☐ Übergabeparameter

☐ Base Pointer

☐ Lokale Variablen

13

**Formatstring-Angriff (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was passt zu Formatzeichen bei einem *Formatstring-Angriff*?

☒ %s

☐ &s

☐ \$s

☐ §s

14

**Drive-by-Infection (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wodurch infiziert man sich meistens bei einer *Drive-by-Infection*?

☒ Exploit-Kit

☐ Rootkit

☐ Backdoor

☐ Botnetz

15

**XSS (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welche *Hauptvariante* von XSS gibt es?



Reflected



Permanent



Advanced



Hooked

16

### BIOS (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was war ein *Universalpasswort* für BIOS?



LKWPETER



PKWPETER



BUSPETER



KRANPETER

17

### Rootkit (2 Punkte)

Sie haben die folgende Antwort gegeben:

Wie können Rootkits unter Windows Schadcode in User-Prozesse bringen?



SetWindowsHookEx

Debugging System



ForceWeakTasks







EnableApplicationHeap

### Rootkit (2 Punkte)

Sie haben die folgende Antwort gegeben:

Wie können Rootkits unter Windows Schadcode in User-Prozesse bringen?

- ☐ SetWindowsHookEx 
- ☐ Debugging System 
- ☐ ForceWeakTasks 
- ☐ EnableApplicationHeap 

18

### Inline Function Hooking (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was macht *Inline Function Hooking*?



Modifiziert die ersten Bytes einer DLL zum Einsprung in den Schadcode



Modifiziert die Adresstabelle einer DLL zum Einsprung in den Schadcode



Modifiziert den Funktionsaufruf in einer DLL mit falschen Parametern



Modifiziert den inneren Code einer DLL zum Einsprung in den Schadcode

19

**Rootkits (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welche Aussage stimmt im Vergleich von *Kernel-Mode Rootkits* mit User-Mode Rootkits?

☐

Kernel-Mode Rootkits haben eingeschränkere Kompatibilität

☐

Kernel-Mode Rootkits nutzen die gleichen Hooking-Mechanismen

☐

Kernel-Mode Rootkits weisen eine geringere Komplexität auf

☐

Kernel-Mode Rootkits haben weniger Privilegien

20

**Scareware (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Scareware...

☐

verunsichert Benutzer

☐

zeigt zusätzliche Werbung

☐

verhindert die Nutzung von Daten oder Computer

☐

sammelt heimlich Informationen

21

**DoS (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was bedeutet *Ressourcensättigung* im Zusammenhang mit **DoS**?

☐

Rechner werden überlastet

☐

Netzwerke werden überlastet

☐

Mitarbeiter werden überlastet

☐

Spannung wird überlastet

22

**Botnetz (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wer kontrolliert ein *Botnetz*?

☐

C&C Server

☐

Master-Zombie

☐

Slave-Zombie



Army

23

**Round Robin (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Auf welches Botnetz trifft zu, dass Adressen der C&C-Server per *Round-Robin* vergeben werden und ständig wechseln?



Single-Flux



Peer-to-Peer



Hydra



Alureon

24

**Britney Spears (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welcher Account von *Britney Spears* wurde als Befehlskanal von C&C-Servern missbraucht?



Instagram



Facebook



SnapChat



Twitter

25

**Flut-Angriffe (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welche Protokolle werden in der Vorlesung als Beispiele für *Flut-Angriffe* genannt?



UDP und ICMP



TCP und IP



UDP und TCP



ICMP und IP

26

**Sniffer (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was ist **ohne** Zustimmung ein nicht legitimer Einsatz von Sniffen?



Leistungsüberwachung von Mitarbeitern

☐ Erkennen von Angriffen

☐ Filtern von verbotenen Inhalten

☐ Troubleshooting

27

**IP Spoofing (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was ist ein Problem bei *IP Spoofing*?

☒ Sender erhält keine Antworten

☐ Ist für Angreifer nur über die Programmierung von raw sockets anwendbar

☐ Kein DoS-Angriff möglich

☐ Wird von NMAP nicht unterstützt

28

**ARP-Spoofing (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welche Eigenschaften von ARP werden für *ARP-Spoofing* genutzt?

☒ ARP ist zustandslos und erlaubt gratuitous ARP

☐ ARP ist zustandsbehaftet und erlaubt gratuitous ARP

☐ ARP ist zustandslos und verbietet gratuitous ARP

☐ ARP ist zustandsbehaftet und verbietet gratuitous ARP

29

**DNS Cache Poisoning (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was ist für einen erfolgreichen *DNS Cache Poisoning* Angriff notwendig?

☒ Angreifer muss schnell eine passende DNS-Antwort liefern

☐ Angreifer muss schnell eine passende DNS-Anfrage senden

☐ Angreifer muss eine korrekt verschlüsselte DNS-Antwort liefern

☐ Angreifer muss eine korrekt verschlüsselte DNS-Anfrage senden

30

**Pharming (1 Punkt)**

Sie haben die folgende Antwort gegeben:



Was ist *Pharming*?



Password Phishing auf Server-Farm



Angriff auf die kritische Infrastruktur im Gesundheitswesen



Sammlung einer großen Anzahl von Phishing-Mails



Manipulation einer Webseite zum Anlocken vieler Benutzer

31

**Man-in-the-Middle (1 Punkt)**

Sie haben die folgende Antwort gegeben:

**Angreifer E** führt einen Man-in-the-Middle-Angriff auf **A** und **B** durch.

Was sagt er wem?



Zu A: ich bin B. Zu B: ich bin A.



Zu E: ich bin A. Zu E: ich bin B.



Zu A: ich bin A. Zu B: ich bin B.



Zu A: ich bin E. Zu B: ich bin E.

32

**Phishing und Web-Spoofing (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was passiert bei einem *Man-in-the-Middle-Angriff* in der Variante **Phishing** und **Web-Spoofing**?



Phishing-Mails leiten Benutzer auf falsche Webseite



Phishing-Mails mit Weblinks werden abgefangen und umgeleitet



Webseiten leiten Benutzer auf Phishing-Mail-Server



Webseiten versenden Phishing Mails.

33

**Passwörter herausfinden (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wie können Angreifer Passwörter nicht herausfinden?



Key Breaking



Social Engineering



Shoulder Surfing



34

**Passwörter raten (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was wird beim Raten von Passwörtern von Angreifern häufig **nicht** getestet ...

☐

Rainbow Tables

☐

Tastaturzeichenfolgen

☐

Fußballvereine

☐

Telefonnummern

35

**Hashkette (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Gegeben sei die folgende Hashkette: „ $A \rightarrow H \rightarrow H(A) \rightarrow R \rightarrow B \rightarrow H \rightarrow H(B) \rightarrow R \rightarrow C \rightarrow H \rightarrow H(C) \rightarrow R \rightarrow D$ “ mit **H** Hash-Funktion und **R** Reduktionsfunktion. Die Benutzung der Kette für den Hashwert  $H(B)$  liefert zunächst das Passwort **D**.

Wie geht die korrekte Ermittlung des Passworts weiter?

☐

Sie starten von A aus vorwärts und das gesuchte Passwort ist B.

☐

Sie starten von A aus vorwärts und das gesuchte Passwort ist C.

☐

Sie starten von D aus rückwärts und das gesuchte Passwort ist B.

☐

Sie starten von D aus rückwärts und das gesuchte Passwort ist C.

36

**Szenario-Vorbereitung (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wie nennt man die *Szenario-Vorbereitung* beim Social Engineering?

☐

Pre-Texting

☐

Plain-Texting

☐

Post-Texting

☐

Task-Texting

37

**Angriffserkennung (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welche Art von Maßnahme sorgt im Fall eines echten Angriffs für eine schnelle Erkennung?

☐

detect

- ☐ predict
- ☐ prevent
- ☐ respond

38

**Krypto-Gebiet (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welches Gebiet gibt es **nicht**?

- ☒ Kryptomorphie
- ☐ Kryptologie
- ☐ Kryptografie
- ☐ Kryptanalyse

39

**asymmetrische Schlüssel (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was stimmt für asymmetrische Schlüssel?

- ☒ Ver- und Entschlüsselung erfolgen mit zwei unterschiedlichen Schlüsseln
- ☐ Privater und öffentlicher Schlüssel sind unabhängig
- ☐ Der öffentliche Schlüssel kann für eine sichere Signatur verwendet werden
- ☐ Schlüsselpaar kann über eine große Primzahl berechnet werden

40

**Hashfunktion (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Eine Hashfunktion heißt auch...

- ☒ Streuwertfunktion
- ☐ Zuordnungsfunktion
- ☐ Kürzungsfunktion
- ☐ Sicherungsfunktion

41

**offline Bruce Force Angriff (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was trifft für einen *offline Bruce Force Angriff* auf einen verschlüsselten Text zu?



Findet den Schlüssel in endlicher Zeit



Findet den Schlüssel in unendlicher Zeit (theoretischer Angriff)



Findet den Schlüssel nicht, wenn dieser mindestens 256 Bit lang ist



Findet den Schlüssel nicht, unabhängig von der Schlüssellänge

42

### One-Time Pad (1 Punkt)

Sie haben die folgende Antwort gegeben:

Warum kann ein *Unbreakable Code* in Form eines **One-Time Pads** nicht angegriffen werden?



Angriff ergibt alle möglichen Klartexte



Angriff ergibt verwürfelten Klartext



Angriff ergibt nur Nullen als Klartext



Angriff ergibt gar keinen Klartext

43

### Zugriffskontrolle (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welches ist kein Schritt der *Zugriffskontrolle*?



Identifikation



Authentisierung



Authentifizierung



Identifizierung

44

### Authentisierung (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welche Authentisierung benutzt keinen zweiten Faktor?



Geldschein



Bankkarte



Sim-Karte



Personalausweis

45

**Biometrische Verfahren (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welches biometrische Verfahren wurde in der Vorlesung nicht angesprochen?

☐

Mundgeometrie

☐

Unterschrift

☐

Stimme

☐

Venen der Handoberfläche

46

**Salts (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was trifft für *Salts* nicht zu?

☐

Salt ist zum Schutz vor Diebstahl verschlüsselt

☐

Saltedhash (password) = hash(password + salt)

☐

Salt ist langer Zufallswert

☐

Salt wird zusammen mit Hash auf dem Server gespeichert

47

**Authentisierung durch Besitz (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was ist keine Authentisierung durch *Besitz*?

☐

Passwort

☐

Bankkarte

☐

Handy

☐

Mitarbeiterausweis

48

**Zugriffskontrollmodell (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welches Zugriffskontrollmodell gibt es nicht?

☐

TAC

☐

DAC

☐

MAC



RBAC

49

**Mandatory Access Control (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was wird beim Zugriffskontrollmodell **Mandatory Access Control** miteinander verglichen?



Freigabe (Clearance) mit Sicherheitskennung (Security Label)



Sicherheitskennung (Security Label) mit Zugriffsliste (Access Control List)



Zugriffsliste (Access Control List) mit Rolle (Role)



Rolle (Role) mit Freigabe (Clearance)

50

**Vertraulichkeitsstufen (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welche Regeln gibt es für *Vertraulichkeitsstufen*?



Read-Down und No-Write-Down



No-Read-Down und No-Write-Down



No-Read-Down und Write-Down



Read-Down und Write-Down

51

**Nachweis (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was lässt sich nur *extrem schwierig* nachweisen?



Rechner ist frei von Schadsoftware



Eine gerade erst bekannt gewordene Schadsoftware ist auf dem Rechner



Eine Standard-Datei auf dem Rechner wurde manipuliert



Ein Programm verhält sich falsch

52

**Erkennungsmethoden von Antivirensoftware (2 Punkte)**

Sie haben die folgende Antwort gegeben:

Was sind *Erkennungsmethoden von Antivirensoftware*?



Signaturen



Heuristik



Quarantäne



Meldung

Erkennungsmethoden von Antivirensoftware (2 Punkte)

Sie haben die folgende Antwort gegeben:

Was sind *Erkennungsmethoden* von Antivirensoftware?

- ☐ Signaturen 
- ☐ Heuristik 
- ☐ Quarantäne 
- ☐ Meldung 

53

#### SSL Schutzziel (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welches Schutzziel wird von SSL **nicht** abgedeckt?



Verfügbarkeit



Vertraulichkeit



Integrität



Authentizität

54

#### PKI Zertifikate (1 Punkt)

Sie haben die folgende Antwort gegeben:

Wie werden bei PKI Zertifikate organisiert?



In einer Baumstruktur



In einer doppelt verketteten Liste



In einem Feld



In einer Certificate Revocation List

55

#### Zustand einer SSL-Verbindung (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welcher Parameter wird für den Zustand einer SSL-Verbindung **nicht** benötigt?

☐ Server Read Seed

☐ Client Random

☐ Client Write MAC Secret

☐ Server Write Key

56

### SSL Record Protokoll (1 Punkt)

Sie haben die folgende Antwort gegeben:

In welcher Reihenfolge arbeitet das *SSL Record Protokoll*?

☐ Fragmentieren, optional komprimieren, MAC berechnen, verschlüsseln

☐ Optional komprimieren, fragmentieren, MAC berechnen, verschlüsseln

☐ Fragmentieren, optional komprimieren, verschlüsseln, MAC berechnen

☐ Optional komprimieren, fragmentieren, verschlüsseln, MAC berechnen

57

### SSL Handshake (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welcher Nachrichtentyp taucht im SSL Handshake nie auf?

☐ ClientHelloDone

☐ ServerHelloDone

☐ ServerHello

☐ ClientHello

58

### SSL (2 Punkte)

Sie haben die folgende Antwort gegeben:

Wofür benötigt SSL die Funktion „ $MD5(Pre-Master-Secret \parallel SHA('A' \parallel Pre-Master-Secret \parallel R_C \parallel R_S)) \dots$ “?

☐ Berechnung des Master-Secrets

☐ Berechnung des Key-Blocks

☐ Berechnung des Message Authentication Codes

☐ Berechnung des Fortezza-Schlüssels

SSL (2 Punkte)

Sie haben die folgende Antwort gegeben:

Wofür benötigt SSL die Funktion „ $MD5(Pre-Master-Secret \parallel SHA('A' \parallel Pre-Master-Secret \parallel R_C \parallel R_S)) \dots$ “?

- ☐ Berechnung des Master-Secrets
- ☐ Berechnung des Key-Blocks
- ☐ Berechnung des Message Authentication Codes
- ☐ Berechnung des Fortezza-Schlüssels



59

### VPN (2 Punkte)

Sie haben die folgende Antwort gegeben:

Auf welchen Ebenen werden **VPNs** realisiert?



Sicherungsschicht



Netzwerkschicht



Sitzungsschicht





Transportschicht


### VPN (2 Punkte)

Sie haben die folgende Antwort gegeben:

Auf welchen Ebenen werden **VPNs** realisiert?

☐ Sicherungsschicht 

☐ Netzwerkschicht 

☐ Sitzungsschicht 

☐ Transportschicht 

60

### Firewalls (2 Punkte)

Sie haben die folgende Antwort gegeben:

Was können **Firewalls**?



Illegalen Zugriff auf internen Systeme verhindern



Denial-of-Service- Angriffe abwehren



Vor bösartigen Insidern schützen







Vor Angriffen schützen, die über autorisierte Zugriffe stattfinden

## Firewalls (2 Punkte)

Sie haben die folgende Antwort gegeben:

Was können **Firewalls**?

- ☐ Illegalen Zugriff auf internen Systeme verhindern 
- ☐ Denial-of-Service- Angriffe abwehren 
- ☐ Vor bösartigen Insidern schützen 
- ☐ Vor Angriffen schützen, die über autorisierte Zugriffe stattfinden 

61

### Zustandsloser Paketfilter (1 Punkt)

Sie haben die folgende Antwort gegeben:

Nach welchen Kriterien filtert ein *zustandsloser* Paketfilter typischerweise?

- ☒ IP-Adressen und Ports
- ☐ Ports und Anwendungsheader
- ☐ Anwendungsheader und MAC-Adressen
- ☐ MAC-Adressen und IP-Adressen

Eingehende TCP-SYN (ACK=0) nur zum Webserver (Port 80) oder Mailserver (Port 25) erlauben

62

### Firewallregel (1 Punkt)

Sie haben die folgende Antwort gegeben:

Sie möchten mit Ihrem zustandslosen Paketfilter „verhindern, dass Ihre Rechner von *außen* ‚gepingt‘ werden.“ Welche Regel passt?

- ☒ Alle eingehenden ICMP-Echo-Request-Pakete verwerfen
- ☐ Alle eingehenden ICMP-Echo-Reply-Pakete verwerfen
- ☐ Alle ausgehenden ICMP-Echo-Request-Pakete verwerfen
- ☐ Alle ausgehenden ICMP-Echo-Reply-Pakete verwerfen

Alle eingehenden ICMP-Echo-Request-Pakete verwerfen.  
aus Tabelle (transparenter text)

63

### Default Deny (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was bedeutet „**default deny**“ und wie wird es bei ACLs verwendet?

- ☒ Die Regel bedeutet „Alles, was nicht explizit erlaubt ist, ist verboten“ und wird als letzte Regel der ACL automatisch angewendet
- ☐ Die Regel bedeutet „Alles, was nicht explizit verboten ist, ist erlaubt“ und wird als letzte Regel der ACL automatisch angewendet



Die Regel bedeutet „Alles, was nicht explizit erlaubt ist, ist verboten“ und wird als erste Regel der ACL automatisch angewendet



Die Regel bedeutet „Alles, was nicht explizit verboten ist, ist erlaubt“ und wird als erste Regel der ACL automatisch angewendet

64

#### Screened Host Architecture (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist das Merkmal einer *Screened Host Architecture*?



Benutzt eine DMZ



Dienste werden als Proxies auf internem Bastion-Host angeboten



Benötigt immer zwei Netzwerkkarten



Verhindert die unerlaubte Umgehung des Proxies

65

#### WPA/WPA2 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist Teil der WPA- und WPA2-Instanzen-Authentisierung?



4-Way-Handshake



1-Way-Handshake



2-Way-Handshake



3-Way-Handshake

66

#### Versäumnisse (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was gehört **nicht** zu den häufigsten Versäumnissen bei der Informationssicherheit?



Beachtung von Sicherheitsrichtlinien



Unzureichende IT-Sicherheitsstrategie



Schlechte Konfiguration von IT-Systemen



Sorgloser Umgang mit Passwörtern

67

#### Beachtung (1 Punkt)

Sie haben die folgende Antwort gegeben:

Warum werden Sicherheitsrichtlinien oft nicht beachtet?

☐

Bequemlichkeit

☐

Kosten

☐

Zeitmangel

☐

Fehlende Sicherheitsorganisation

Sie haben 0 von 1 möglichen Punkten erreicht.

68

**Unsichere Vernetzung (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wie kann man unsicherer Vernetzung / Internet-Anbindung entgegenwirken?

☐

Vorsicht bei Web-Browsern und Emails walten lassen

☐

Ordnung am Arbeitsplatz halten

☐

Bildschirm bei Abwesenheit sperren

☐

Zutrittsschutz einrichten

69

**Wie kann man Gefahren durch Einbrecher und Katastrophen entgegenwirken?**

☐

Mobile Geräte nicht unbeaufsichtigt lassen

☐

Angemessene Berücksichtigung von IT-Sicherheit

☐

Virenschutzprogramme einsetzen

☐

Sicherheits-Patches einspielen

70

**Wodurch werden der Informationssicherheit häufig Grenzen gesetzt?**

☐

Zugriff und Kosten

☐

Kosten und Zutritt

☐

Zutritt und Kommunikation

☐

Kommunikation und Zugriff

71

**Kosten (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Der Nutzen einer Sicherheitsmaßnahme beträgt **50.000 Euro**, der erwartete Verlust mit Maßnahme **100.000 Euro**, der ohne Maßnahme **200.000 Euro** (*alle Werte pro Jahr*).

Wie groß sind die Kosten der Maßnahme pro Jahr?

☐

50.000 Euro

☐

100.000 Euro

☐

150.000 Euro

☐

200.000 Euro

72

### Fehlende Werte (1 Punkt)

Sie haben die folgende Antwort gegeben:

Zur Berechnung des Nutzens einer Sicherheitsmaßnahme steht Ihnen der Wert für den erwarteten Verlust ohne Maßnahme ( $E(\text{Verlust ohne Maßnahme})$ ) zur Verfügung.

Welche Werte fehlen Ihnen? (*Alle Werte beziehen sich auf ein Jahr*)

☐

$E(\text{Verlust mit Maßnahme})$  und (Kosten der Maßnahme)

☐

(Kosten der Maßnahme) und (Kosten ohne Maßnahme)

☐

(Kosten ohne Maßnahme) und  $E(\text{Verlust der Maßnahme})$

☐

$E(\text{Verlust der Maßnahme})$  und  $E(\text{Verlust mit Maßnahme})$

73

### Schwachstelle (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist eine *Schwachstelle*?

☐

Sicherheitsrelevanter Fehler eines IT-Systems

☐

Ereignis, das Vertraulichkeit von Informationen beeinträchtigen kann

☐

Vorfall, der sich negativ auf die Verfügbarkeit eines Systems auswirkt

☐

Schadcode, der einen Computer infizieren kann

74

### Risiko (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was hat **keinen** Einfluss auf ein Risiko?

☐

Maßnahmenkosten

☐

Gefährdung



Eintrittswahrscheinlichkeit



Schadenspotential

75

**Risiko-Behandlungsstrategie (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welche Art von *Risiko-Behandlungsstrategie* verfolgt eine Versicherung?



Übertragung



Reduktion



Akzeptanz



Vermeidung

76

**Aktiver Angriff (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welcher der folgenden Angriffe ist **aktiv**?



ARP Spoofing



Sniffing im WLAN



Shoulder Surfing



Passwort-Cracking offline

77

**Pre-Attack (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was gehört zur Phase *Pre-Attack* im typischen Angriffsverlauf?



Enumeration



Penetration



Exploitation



Spuren verwischen

78

**Schwachstellen testen und Ausnutzen (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was ist ein Framework zum *Testen* und *Ausnutzen* von Schwachstellen?

- ☐ metasploit
- ☐ nmap
- ☐ cryptolocker
- ☐ slammer

79

### Commodity Threat (1 Punkt)

Sie haben die folgende Antwort gegeben:  
Was trifft auf einen Commodity Threat zu?

- ☐ km breit und cm tief
- ☐ km breit und km tief
- ☐ cm breit und cm tief
- ☐ cm breit und km tief

80

Pivoting (1 Punkt)  
Sie haben die folgende Antwort gegeben:

Was beschreibt den Begriff **Pivoting**?

- ☐ Nach Erst-Infektion von infiziertem System aus weitere Systeme im Zielnetz angreifen ✗
- ☐ Die Rechte des angreifenden Benutzers auf Admin-Rechte ausweiten ✗
- ☐ Die eigentliche Payload ausführen und die Mission ausführen ✗
- ☐ Sich auf dem Zielsystem festsetzen, z.B. durch die Verwendung von Rootkits ✗

Sie haben 0 von 1 möglichen Punkten erreicht.

### 81 Idle-Scan (1 Punkt)

Sie haben die folgende Antwort gegeben:  
Was trifft für einen funktionierenden *Idle-Scan*

- ☐ Betriebssystem vergibt Identifier für aufeinanderfolgende IP-Pakete mit festem Inkrement
- ☐ Opfer befindet sich im Leerlauf
- ☐ IP des Angreifers wird mit der IP des Opfers gespoof
- ☐ Die zweite Nachricht des Angreifers geht an den Zombie

82

### Virenarten (1 Punkt)

Sie haben die folgende Antwort gegeben:  
Welche Art von Viren gibt es **nicht**?

- ☐ Bot-Viren
- ☐ Speicherresidente Viren
- ☐ Programm-Viren
- ☐ Skript-Viren

**Schadcode (1 Punkt)**

Sie haben die folgende Antwort gegeben:

**Nutzt Wirtsdatei, reproduziert sich nicht und wird passiv verteilt.**

Um welche Art von Schadcode handelt es sich?



Trojanisches Pferd



Virus



Wurm



Exploit



# IT-Sicherheit 2 Klausurfragen

Montag, 11. Februar 2019 17:33

## ITS2 Klausur 2-1 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welches ist keines der drei klassischen Schutzziele der Informationssicherheit?

☐

Authenticity

☐

Integrität

☐

Confidentiality

☐

Verfügbarkeit

## ITS2 Klausur 2-2 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was gehört nicht zu den häufigsten Versäumnissen bei der Informationssicherheit?

☐

Schlechte Konfiguration von IT-Systemen

☐

Nichtbeachtung von Sicherheitsrichtlinien

☐

Einbrecher und Elementarschäden

☐

Sichere Vernetzung / Internetanbindung

## ITS2 Klausur 2-3 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist kein sorgloser Umgang mit Passwörtern?

☐

Passwort-Safe benutzen

☐

Passwort aufschreiben

☐

Passwort weitergeben

☐

Standard-Passwörter nutzen

## ITS2 Klausur 2-4 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Wie kann man einer unzureichenden Sicherheitsstrategie entgegenwirken?



Leitungsebene muss IT-Sicherheit unterstützen



Standardeinstellungen anpassen



Restriktion von nach außen angebotenen Daten



Wartungs-und Reparaturarbeiten regeln

### ITS2 Klausur 2-5 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Wie kann man schlechter Wartung entgegenwirken?



Sicherheits-Patches regelmäßig einspielen



Passwörter häufig wechseln



Notfallpläne aufstellen



Sicherheit in allen Projekten frühzeitig berücksichtigen

### ITS2 Klausur 2-6 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Sie sind ein kleines Unternehmen mit fünf Mitarbeitern und fünf Rechnern.

Wieviel kostet 100% Sicherheit?



Unendlich viel (es gibt keine 100% Sicherheit)



Gar kein Geld, nur Personaleinsatz



Ca. 500 Euro



Ca. 10.000 Euro

### ITS2 Klausur 2-7 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Wie berechnet sich der Nutzen einer Sicherheitsmaßnahme (E = Erwartungswert, alle Werte beziehen sich auf 1 Jahr)?



$E(\text{Verlust ohne Maßnahme}) - E(\text{Verlust mit Maßnahme}) - \text{Kosten der Maßnahme}$

☐  $E(\text{Verlust mit Maßnahme}) + \text{Kosten der Maßnahme} - E(\text{Verlust ohne Maßnahme})$

☐  $\text{Kosten der Maßnahme} - E(\text{Verlust ohne Maßnahme}) - E(\text{Verlust mit Maßnahme})$


☐  $E(\text{Verlust ohne Maßnahme}) - E(\text{Verlust mit Maßnahme}) + \text{Kosten der Maßnahme}$

### ITS2 Klausur 2-8 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Der Nutzen einer Sicherheitsmaßnahme beträgt 100.000 Euro, die Kosten der Maßnahme 100.000 Euro, der erwartete Verlust ohne Maßnahme 200.000 Euro (alle Werte pro Jahr).

Wie groß ist der erwartete Verlust mit Maßnahme pro Jahr?

☐ 0 Euro 

☐ 100.000 Euro

☐ 200.000 Euro

☐ 300.000 Euro

### ITS2 Klausur 2-9 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist eine Bedrohung?

☐ Ereignis, das Vertraulichkeit von Informationen beeinträchtigen kann



☐ Sicherheitsrelevanter Fehler eines IT-Systems

☐ Fehlende Patches in einem System

☐ Unzureichend Schulung der Mitarbeiter

### ITS2 Klausur 2-10 (1 Punkt)

Sie haben die folgende Antwort gegeben:



Welche drei Eingangsgrößen bestimmen ein Risiko in Bezug auf Informationssicherheit?

☐ Eintrittswahrscheinlichkeit, Schadenspotential, Gefährdung

☐ Gefährdung, Eintrittswahrscheinlichkeit, Bedrohung

☐



Schadenspotential, Bedrohung, Schwachstelle



Gefährdung, Schwachstelle, Schadenspotential

### ITS2 Klausur 2-11 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Ein Unternehmen verbietet die Nutzung von USB-Sticks. Um was für eine Behandlungsstrategie handelt es sich?



Vermeidung



Übertragung



Reduktion



Akzeptanz

### ITS2 Klausur 2-12 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welcher der folgenden Angriffe ist passiv?



Sniffing im WLAN



Password-Cracking online



DNS Cache Poisoning



Distributed DoS

### ITS2 Klausur 2-13 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Zu welcher Angriffsphase gehört Reconnaissance?



Pre-Attack



Attack



Post-Attack



Improve-Attack

### ITS2 Klausur 2-14 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welches Programm ist ein *Port Scanner*?

☐

nmap

☐

netcat

☐

ping

☐

john the ripper

### ITS2 Klausur 2-15 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was trifft auf einen Advanced Persistent Threat zu?

☐

cm breit und km tief

☐

km breit und cm tief

☐

km breit und km tief

☐

cm breit und cm tief

### ITS2 Klausur 2-16 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was beschreibt den Begriff „*Privilege Escalation*“?

☐

Die Rechte des angreifenden Benutzers auf Admin-Rechte ausweiten

☐

Nach Erst-Infektion von infiziertem System aus weitere Systeme im Zielnetz angreifen

☐

Die eigentliche Payload ausführen und die Mission ausführen

☐

Sich auf dem Zielsystem festsetzen, z.B. durch die Verwendung von Rootkits

### ITS2 Klausur 2-17 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Sie führen einen TCP SYN Scan durch.

Welches Paar von Nachrichten signalisiert einen geschlossenen Port?

☐

Auf ein SYN folgt ein RST

☐

Auf ein SYN/ACK folgt ein RST

☐

Auf ein RST folgt ein SYN/ACK

☐

Auf ein RST folgt ein SYN

#### ITS2 Klausur 2-18 (1 Punkt)

Sie haben die folgende Antwort gegeben:

*Nutzt keine Wirtsdatei, und verteilt sich selbst aktiv durch Reproduktion und über Kommunikationsschnittstellen.*

Um welche Art von Schadcode handelt es sich?

☐

Wurm

☐

Virus

☐

Trojanisches Pferd

☐

Exploit

#### ITS2 Klausur 2-19 (2 Punkte)

Sie haben die folgende Antwort gegeben:

Welche zeitliche Reihenfolge von links nach rechts ist für Schwachstellen korrekt? **(Wählen Sie zwei Antworten)**

☐

Schwachstelle wird eingeführt, Schwachstelle wird veröffentlicht, Virenschutz wird ergänzt

☐

Exploit released in the wild, Schwachstelle wird veröffentlicht, Patch wird veröffentlicht

☐

Patch wird veröffentlicht, Patch wird installiert, Exploit released in the wild





☐

Schwachstelle vom Hersteller erkannt, Schwachstelle wird eingeführt, Patch wird installiert

### ITS2 Klausur 2-19 (2 Punkte)

Sie haben die folgende Antwort gegeben:

Welche zeitliche Reihenfolge von links nach rechts ist für Schwachstellen korrekt? **(Wählen Sie zwei Antworten)**

- ☐ Schwachstelle wird eingeführt, Schwachstelle wird veröffentlicht, Virenschutz wird ergänzt 
- ☐ Exploit released in the wild, Schwachstelle wird veröffentlicht, Patch wird veröffentlicht 
- ☐ Patch wird veröffentlicht, Patch wird installiert, Exploit released in the wild 
- ☐ Schwachstelle vom Hersteller erkannt, Schwachstelle wird eingeführt, Patch wird installiert 

### ITS2 Klausur 2-20 (2 Punkte)

Sie haben die folgende Antwort gegeben:

Welche Teile gehören (ggf. optional) zum Aufbau eines Virus? **(Wählen Sie zwei Antworten)**

☐ Vermehrungsteil

☐ Tarnungsteil





☐ Steuerungsteil

☐ Verschlüsselungsteil

### ITS2 Klausur 2-20 (2 Punkte)

Sie haben die folgende Antwort gegeben:

Welche Teile gehören (ggf. optional) zum Aufbau eines Virus? **(Wählen Sie zwei Antworten)**

- ☐ Vermehrungsteil 
- ☐ Tarnungsteil 
- ☐ Steuerungsteil 
- ☐ Verschlüsselungsteil 

### ITS2 Klausur 2-21 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welcher Virus muss aufgrund eines *Sprungbefehls* Originaldaten ans Ende schieben?

☐ Appending-Virus



Überschreibender Virus



Prepending-Virus



Companion-Virus

### ITS2 Klausur 2-22 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist ein *Viren-Selbstschutz*?



Metamorphie



Hypermorphie



Paramorphie



Antimorphie

### ITS2 Klausur 2-23 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist keine Strategie von Email-Würmern um Benutzer zum Öffnen des Anhangs zu bewegen?



Zufriedenheit



Schockwirkung



Neugier



Harmlosigkeit

### ITS2 Klausur 2-24 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welches Transportprotokoll und wie viele Scans/s nutzte der **SQL-Slammer**?



UDP und 26.000 Scans/s



TCP und 26.000 Scans/s



UDP und 376 Scans/s



TCP und 376 Scans/s



**ITS2 Klausur 2-25 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wie entstehen **Trojanische Pferde**?



Einsatz eines Linkers



Setzen von Rechten



Bottom-Up Ansatz



Top-Down Ansatz

**ITS2 Klausur 2-26 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wie wird ein Trojanisches Pferd aktiv?



Start des Wirtsprogramms



Autorun



Fernsteuerung



Ausnutzen einer Schwachstelle

**ITS2 Klausur 2-27 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wo suchen Angreifer Schwachstellen am liebsten?



In weitverbreiteten Systemen



In herausfordernden Systemen



In php geschriebenen Systemen



In präventiven Systemen

**ITS2 Klausur 2-28 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was trifft für Exploit Kits nicht zu?

- ☐ Nutzen Schwachstellen des Betriebssystems aus
- ☐ Sind eine Sammlung von Exploits
- ☐ Werden als kommerzielle Software oder Dienstleistung verkauft
- ☐ Bestehen aus einer Reihe von Webseiten



### ITS2 Klausur 2-29 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Wie wird *Speicherplatz* vergeben?

- ☐ Heap wächst nach oben, Stack nach unten
- ☐ Stack wächst nach oben, Heap nach unten
- ☐ Beide wachsen nach oben
- ☐ Beide wachsen nach unten

### ITS2 Klausur 2-30 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was passt zu einem *nicht-persistentem* XSS Angriff?

- ☐ Link in Email
- ☐ Anhang in Email
- ☐ USB-Stick
- ☐ SQL-Injection

### ITS2 Klausur 2-31 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welche Webseiten kommen bei *stored* XSS eher nicht in Frage?

- ☐ Infowebseiten



Gästebücher



Bewerbungen



Verkaufsanzeigen

### ITS2 Klausur 2-32 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist ein *Drive-by-Download*?



Automatischer Download bei Besuch einer Webseite



Automatischer Download bei Einstecken eines USB-Drives



Automatischer Download bei der Registrierung im fremden Netz



Automatischer Download bei einem mobilen Gerät

### ITS2 Klausur 2-33 (2 Punkte)

Sie haben die folgende Antwort gegeben:

Welche Eigenschaften hat eine Watering Hole Attack? **(Wählen Sie zwei Antworten)**



Infektion von Webseiten



Webseite von Zielgruppe benutzt



Basiert immer auf vorheriger SQL-Injection







Webserver hat sogenannte Watering-Schwachstelle

ITS2 Klausur 2-33 (2 Punkte)

Sie haben die folgende Antwort gegeben:

Welche Eigenschaften hat eine Watering Hole Attack? **(Wählen Sie zwei Antworten)**

- ☐ Infektion von Webseiten 
- ☐ Webseite von Zielgruppe benutzt 
- ☐ Basiert immer auf vorheriger SQL-Injection 
- ☐ Webserver hat sogenannte Watering-Schwachstelle 

**ITS2 Klausur 2-34 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welche zusätzliche Funktion bieten Rootkits gegenüber Backdoors?

- ☒ Mechanismen zum Verbergen der Existenz
- ☐ Umgehung der Authentifizierung
- ☐ Alternativer Zugang
- ☐ Privilege Escalation

**ITS2 Klausur 2-35 (2 Punkte)**

Sie haben die folgende Antwort gegeben:





Wie können Rootkits unter Windows Schadcode in User-Prozesse bringen? **(Wählen Sie zwei Antworten)**

- ☒ Application Extensions
- ☒ Schwachstellen in Anwendungen
- ☐ Kernel API Functions
- ☐ User Control Settings

ITS2 Klausur 2-35 (2 Punkte)

Sie haben die folgende Antwort gegeben:

Wie können Rootkits unter Windows Schadcode in User-Prozesse bringen? **(Wählen Sie zwei Antworten)**

- ☐ Application Extensions 
- ☐ Schwachstellen in Anwendungen 
- ☐ Kernel API Functions 
- ☐ User Control Settings 

ITS2 Klausur 2-36 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was macht IAT Hooking? 

☐

Modifikation der Auflösung von Adressen bei API-Aufrufen

☐

Modifikation der Anwendung bei API-Aufrufen

☐

Modifikation des Interfaces bei API-Aufrufen

☐

Modifikation der angefragten Information bei API-Aufrufen

ITS2 Klausur 2-37 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Spyware...

☐

sammelt heimlich Informationen

☐

zeigt zusätzliche Werbung

☐

verhindert die Nutzung von Daten oder Computer

☐

verunsichert Benutzer

ITS2 Klausur 2-38 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Cryptolocker verschlüsselt die Benutzerdaten mit...

- ☐ dem öffentlichen Schlüssel des Angreifers
- ☒ dem privaten Schlüssel des Angreifers
- ☐ mit dem geheimen symmetrischen Schlüssel des Angreifers
- ☐ mit einer kryptographischen Hashfunktion

**ITS2 Klausur 2-39 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wer bildet die *Army* eines Botnetzes?

- ☒ Master-Zombies und Slave-Zombies
- ☐ Command & Control Server und Master Zombies
- ☐ Slave-Zombies und Opfer-Rechner
- ☐ Opfer-Rechner und Command & Control Server

**ITS2 Klausur 2-40 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welche Maßnahme kann die *Größe* von P2P-Botnetzen reduzieren?

- ☒ Malware-Beseitigung auf den Opfern
- ☐ Beseitigung der C&C-Server
- ☐ Abschalten aller Master-Zombies
- ☐ Abschalten aller Slave-Zombies

**ITS2 Klausur 2-41 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was ist ein typischer Befehlskanal für C&C-Server?

- ☒ IRC
- ☐ ORB
- ☐ RSA
- ☐

**ITS2 Klausur 2-42 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Auf welche Art wird DNS für DoS-Angriffe missbraucht?

☐

DNS Verstärkung

☐

DNS Cache Poisoning

☐

DNS Changer

☐

DNS Fluten

**ITS2 Klausur 2-43 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was bewirkt ein *TCP SYN Angriff*?

☐

Zu viele halboffene Verbindungen und dadurch Blockade

☐

Absturz des Empfängers durch falsche Flags

☐

Übernahme der Session durch Raten der Sequenznummer

☐

Verlust des Verbindungsaufbaupakets und dadurch Stop der Verbindung

**ITS2 Klausur 2-44 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

In welchem Modus sammelt ein Sniffer alle Daten der NIC?

☐

promiscuous

☐

non-promiscuous

☐

persistant

☐

non-persistent

**ITS2 Klausur 2-45 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Warum ist die Sicherheit eines MAC-Address-Filters trügerisch?



Sender-MAC-Adresse kann per Software geändert werden



MAC-Address-Filter funktionieren nicht bei WLANs



Empfänger-MAC-Adressen sind non-promiscuous



Trotz MAC-Address-Filters können die verkapselten IP-Pakete durchkommen

### ITS2 Klausur 2-46 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was passiert bei *DNS Cache Poisoning*?



Angreifer schleust gefälschte Informationen in den Cache eines DNS-Servers ein



Angreifer schleust eine falsche DNS-Cache Adresse in den Client ein



Über einen DNS-Eintrag wird der ARP-Cache geändert



Es findet ein DoS-Angriff auf den DNS-Cache statt

### ITS2 Klausur 2-47 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist für einen erfolgreichen DNS Cache Poisoning Angriff **nicht** relevant?



Hostname des angefragten DNS-Servers muss stimmen



IP-Adresse und Port des angefragten DNS-Servers müssen stimmen



IP-Adresse und Port des anfragenden Hosts müssen stimmen



Die Referenznummer der Anfrage muss stimmen

### ITS2 Klausur 2-48 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was verschleiert *Spoofing*?



Die eigene Identität





Den Empfänger



Die Ziel-IP



Das verwendete Protokoll

### ITS2 Klausur 2-49 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Im Folgenden sind die Adressen gekürzt!

Angreifer E (IP: 3.3, MAC: EE) führt einen Man-in-the-Middle-Angriff auf A (IP: 1.1, MAC: AA) und B (IP: 2.2, MAC: BB) durch.

Welche ARP-Reply schickt er an B?



Meine IP ist 1.1 und meine MAC ist EE.



Meine IP ist 3.3 und meine MAC ist EE.



Meine IP ist 3.3 und meine MAC ist AA.



Meine IP ist 1.1 und meine MAC ist AA.

### ITS2 Klausur 2-50 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was kann ein Man-in-the-Browser-Angriff nicht?



Salted Hashes knacken



Daten außerhalb des verschlüsselten Tunnels modifizieren



Webseiten Manipuliere



Eingabefelder auslesen

### ITS2 Klausur 2-51 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist kein Ansatz zum Password Cracking?



Hooking



Brute Force



Raten



Rainbow Tables

### ITS2 Klausur 2-52 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Rainbow-Tables basieren auf welchem Kompromiss?



Time-Memory Tradeoff



Memory-Cost Tradeoff



Cost-Benefit Tradeoff



Benefit-Time Tradeoff

### ITS2 Klausur 2-53 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Für Passwörter seien aus dem ASCII-Zeichensatz nur Großbuchstaben und Ziffern zugelassen. Wie viele unterschiedliche Passwörter mit 10 Zeichen gibt es?



36 hoch 10



10 hoch 36



26 hoch 20



20 hoch 26

### ITS2 Klausur 2-54 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist keine Social-Engineering Technik?



Cash Poisoning



Spear Phishing



Baiting



CEO Fraud

### 2-55 (1 Punkt)

Welche Art von Maßnahme schützt Systeme gegen Bedrohungen?



prevent



detect



predict



respond

### ITS2 Klausur 2-56 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was stimmt für symmetrische kryptografische Algorithmen?



Ver- und Entschlüsselung erfolgen mit dem gleichen Schlüssel



Ver- und Entschlüsselung erfolgen mit zwei unterschiedlichen Schlüsseln



Schützt nicht die Integrität von Nachrichten



Schützt die Verfügbarkeit von Nachrichten

### ITS2 Klausur 2-57 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Schwache Kollisionsresistenz bedeutet ...



Schwierig zu Urbild  $x$  ein davon verschiedenes Urbild  $x'$  zu finden mit  $h(x)=h(x')$



Schwierig zwei verschiedene Urbilder  $x$  und  $x'$  zu finden mit  $h(x)=h(x')$



Schwierig zwei verschiedene Hashwerte  $h(x)$  und  $h(x')$  zu finden mit  $x=x'$



Schwierig zu Hashwert  $h(x)$  einen davon verschiedenen Hashwert  $h(x')$  zu finden mit  $x=x'$

### ITS2 Klausur 2-58 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Ein Message Authentication Code ist...



ein Prüfwert einer Nachricht, der unter Einbezug eines (geheimen) symmetrischen Schlüssels erzeugt wird



ein Prüfwert einer Nachricht, der unter Einbezug eines privaten (asymmetrischen) Schlüssels erzeugt wird



ein Prüfwert einer Nachricht, der unter Einbezug eines öffentlichen (asymmetrischen)

Schlüssels erzeugt wird



ein Prüfwert einer Nachricht, der ohne Schlüssel erzeugt wird

### ITS2 Klausur 2-59 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Wie nennt man die Aussage „Die Sicherheit eines Verschlüsselungsverfahrens beruht auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus“?



Kerckhoffs Prinzip



Locardsches Prinzip



Moore's Law



Murphy's Law

### ITS2 Klausur 2-60 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Subjekt A möchte gegenüber einer Kontrollinstanz B seine Identität nachweisen.  
Was gilt?



A authentisiert sich gegenüber B



A identifiziert sich gegenüber B



A authentifiziert sich gegenüber B



A autorisiert sich gegenüber B

### ITS2 Klausur 2-61 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Wie nennt man bei biometrischen Verfahren die Rate, mit der unberechtigte zugelassen werden?



False Acceptance Rate



Correct Acceptance Rate



False Rejection Rate



Correct Rejection Rate

**ITS2 Klausur 2-62 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was ist keine sinnvolle Passwortregel?



Lange Lebensdauer



Keine Wiederverwendung



Mindestlänge



Kein Weitergeben

**ITS2 Klausur 2-63 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was ist keine Methode für Einmal-Passwörter?



One-Time-Pads



Gedruckte Liste



Zusenden per SMS



Generierung in Token

**ITS2 Klausur 2-64 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wie nennt man den Mechanismus bei Smart Cards, der zur Karten-Authentifizierung eingesetzt wird?



Challenge/Response



PIN-Kontrolle



Kartenlesen



RFID

**ITS2 Klausur 2-65 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wofür steht in Deutschland die Vertraulichkeitsstufe VS-NfD?



**Verschlusssache – Nur für den Dienstgebrauch**



Vertraulich/Secret – Nutzungsstufe für Deutschland



Verschlusssache – Nutzungsstufe für Deutschland



Vertraulich/Secret – Nur für den Dienstgebrauch

**ITS2 Klausur 2-66 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Was gilt für ein rollenbasiertes Zugriffskontrollmodell nicht?



**Rollen erben die Rechte der Benutzer**



Rollen orientieren sich an Organigramm der Institution



Benutzer werden Rollen zugeordnet



Zugriffsrechte werden Rollen zugeordnet

**ITS2 Klausur 2-67 (2 Punkte)**

Sie haben die folgende Antwort gegeben:

Was sind Erkennungsmethoden von Antivirensoftware? **(Wählen Sie zwei Antworten)**



**Sandbox**



**Verhaltensanalyse**



Isolation




Alarm


**ITS2 Klausur 2-67 (2 Punkte)**

Sie haben die folgende Antwort gegeben:

Was sind Erkennungsmethoden von Antivirensoftware? **(Wählen Sie zwei Antworten)**

☐ Sandbox 

☐ Verhaltensanalyse 

☐ Isolation 

☐ Alarm 

### ITS2 Klausur 2-68 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welche Methode eignet sich nicht zum Entfernen von Malware?



Alle Prozesse der Schadsoftware aus dem Arbeitsspeicher entfernen



Spezialsoftware zur Entfernung nutzen



Rechner manuell nach Anleitung von Spezialisten säubern



Re-Installation des Systems mit sauberem Betriebssystem und Anwendungen

### ITS2 Klausur 2-69 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was wird bei SSL in einem Zertifikat insbesondere zertifiziert?



Öffentlicher Schlüssel einer Instanz



Privater Schlüssel einer Instanz



Geheimer symmetrischer Schlüssel einer Instanz



Master-Key einer Instanz

### ITS2 Klausur 2-70 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Woran erkennt man bei SSL einen Man-in-the-Middle-Angriff auf die Verbindung?



Browser meldet ein ungültiges Zertifikat



Browser meldet eine Dateimodifikation



Browser meldet „604 – connection unsecure“



Angriff kann nicht erkannt werden

### ITS2 Klausur 2-71 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was macht ein Trusted List in Bezug auf PKI?



Speicherung von mehreren Wurzel-Zertifikaten im Browser



Cross-Zertifizierung durch CA auf gleicher Ebene



Cross-Zertifizierung durch zusätzliche Zertifikate



Zertifizierung durch CA auf neuer Ebene

### ITS2 Klausur 2-72 (2 Punkte)

Sie haben die folgende Antwort gegeben:

Welche beiden Aufgaben hat das SSL Handshake Protocol? **(Wählen Sie zwei Antworten)**



Authentifizierung der Kommunikationspartner



Aushandlung kryptografischer Parameter



Signalisierung von Fehlern



Wechsel von Verschlüsselungs-Algorithmen

ITS2 Klausur 2-72 (2 Punkte)

Sie haben die folgende Antwort gegeben:

Welche beiden Aufgaben hat das SSL Handshake Protocol? **(Wählen Sie zwei Antworten)**

☐ Authentifizierung der Kommunikationspartner ❌

☐ Aushandlung kryptografischer Parameter ❌

☐ Signalisierung von Fehlern ✔️

☐ Wechsel von Verschlüsselungs-Algorithmen ✔️

### ITS2 Klausur 2-73 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Warum benötigt man Perfect Forward Secrecy?



Schutz vor Kompromittierung von Langzeitschlüsseln



Verlängerung der Sicherheit eines Verschlüsselungsverfahrens



Geheimhaltung beim Weiterleiten von Daten



Verschlüsselungsverfahren für die Post-Quantum-Zeit

### ITS2 Klausur 2-74 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welche TLS-Variante befindet sich derzeit im Entwurf?



TLS 1.3



TLS 1.7



TLS 1.1



TLS 1.5



**ITS2 Klausur 2-75 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Auf welches Sicherheitsprotokoll baut kein VPN auf?

☐

S-MIME

☐

IPSec

☐

SSL

☐

SSH

**ITS2 Klausur 2-76 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wie nennt man das Verschicken von Daten über eine VPN-Verbindung?

☐

Tunneling

☐

Bridging

☐

Authenticating

☐

Encrypting

**ITS2 Klausur 2-77 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Wie nennt man eine Firewall auf einem einzelnen Rechner?

☐

Personal Firewall

☐

Client Firewall

☐

NIC Firewall

☐

PC Firewall

**ITS2 Klausur 2-78 (1 Punkt)**

Sie haben die folgende Antwort gegeben:

Welche Firewall-Technologie gibt es nicht?

☐

## Transport-Gateways



Anwendungs-Gateways



Zustandslose Paketfilter



Zustandsbasierte Paketfilter

### ITS2 Klausur 2-79 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Sie möchten mit Ihrem zustandslosen Paketfilter „*eingehende TCP-Verbindungen nur zum Webserver und zum Mailserver erlauben*“.

Welche Regel passt?



Eingehende TCP-SYN (ACK=0) nur zum Webserver (Port 80) oder Mailserver (Port 25) erlauben.



Eingehende TCP-SYN (SYN=0) nur zum Webserver (Port 80) oder Mailserver (Port 25) erlauben.



Ausgehende TCP-SYN (ACK=0) nur zum Webserver (Port 80) oder Mailserver (Port 25) erlauben.



Ausgehende TCP-SYN (SYN=0) nur zum Webserver (Port 80) oder Mailserver (Port 25) erlauben.

### ITS2 Klausur 2-80 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was bedeutet „*default permit*“ und wie wird es bei ACLs verwendet?



Die Regel bedeutet „Alles, was nicht explizit erlaubt ist, ist verboten“ und wird bei Interfaces ohne ACL automatisch benutzt



Die Regel bedeutet „Alles, was nicht explizit verboten ist, ist erlaubt“ und wird bei Interfaces ohne ACL automatisch benutzt



Die Regel bedeutet „Alles, was nicht explizit erlaubt ist, ist verboten“ und wird bei Interfaces mit ACL automatisch benutzt



Die Regel bedeutet „Alles, was nicht explizit verboten ist, ist erlaubt“ und wird bei Interfaces mit ACL automatisch benutzt

### ITS2 Klausur 2-81 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was unterscheidet den zustandsbasierten Paketfilter vom zustandslosen?



Merkt sich den Verbindungsstatus über TCP Flags



Merkt sich den Verbindungsstatus über ICMP Flags



Merkt sich den Verbindungsstatus über IP Flags



Merkt sich den Verbindungsstatus über UDP Flags

### ITS2 Klausur 2-82 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist das Merkmal einer *Screened Host Architecture*?



Dienste werden als Proxies auf internem Bastion-Host angeboten



Benutzt eine DMZ



Benötigt immer zwei Netzwerkkarten



Setzt ein Perimeter-Netz ein

### ITS2 Klausur 2-83 (2 Punkte)

Sie haben die folgende Antwort gegeben:

Welche Kommunikations-Modi gibt es bei WLAN? **(Wählen Sie zwei Antworten)**



Infrastruktur-Modus



Ad-Hoc-Modus



WPS-Modus







Autoconnect-Modus

Sie haben die folgende Antwort gegeben:

---

Welche Kommunikations-Modi gibt es bei WLAN? **(Wählen Sie zwei Antworten)**

- ☐ Infrastruktur-Modus 
- ☐ Ad-Hoc-Modus 
- ☐ WPS-Modus 
- ☐ Autoconnect-Modus 

# Probeklausur

Dienstag, 12. Februar 2019 01:09

## 1. ITS PK9 [ID: 448755]

Nutzt Wirtsdatei, reproduziert sich lokal und wird passiv verteilt. Um welche Art von Schadcode handelt es sich?



Virus



Wurm



Trojanisches Pferd



Exploit

## 2. ITS PK12 [ID: 448758]

Was stimmt für einen erfolgreichen SQL-Injection-Angriff mit dem String „1' OR 1=2;#“ im Passwort-Feld einer Login-Seite?



Die SQL-Anfrage hinter dem String ist auskommentiert



Der Bedingungsteil der SQL-Abfrage ist immer wahr



Der Parameter des Benutzernamens wird für den Angriff benutzt



Der Parameter des Passworts ist leer

## 3. ITS PK18 [ID: 448764]

Welcher Begriff ist in Bezug auf die „Speicherung“ von Passwörtern auf Servern richtig?



Passwort-Hashing



Passwort-Verschlüsselung



Passwort-Verschleierung



Passwort-Keying

## 4. ITS PK8 [ID: 448754]

Welche Art von Viren gibt es nicht?



Speicherresistente Viren



Makro-Viren



Programm-Viren



Daten-Viren

## 5. ITS PK16 [ID: 448762]

Was ist der Effekt, wenn der DNS-Eintrag in der Netzwerkkonfiguration eines Clients manipuliert wird?

- ☒ Einem Hostnamen wird eine falsche IP-Adresse zugeordnet
- ☐ Rahmen gehen an den falschen Rechner im gleichen Subnetz
- ☐ Die IP-Adresse eines Pakets wird im Netz geändert
- ☐ Das Standardgateway bekommt eine falsche Adresse

## 6. ITS PK29 [ID: 448775]

Sie möchten mit Ihrem zustandslosen Paketfilter „Rechner vor DNS-Anfragen an andere als den definierten DNS-Server schützen.“

Welche Regel passt?

- ☒ Verwerfen von allen ausgehenden DNS Anfragen normaler Hosts, die nicht den definierten Server nutzen
- ☐ Zulassen von allen ausgehenden DNS Anfragen normaler Hosts, die an den definierten Server gehen
- ☐ Zulassen von allen ausgehenden DNS Anfragen normaler Hosts, die nicht den definierten Server nutzen
- ☐ Verwerfen von allen ausgehenden DNS Anfragen normaler Hosts, die an den definierten Server gehen

## 7. ITS PK6 [ID: 448752]

Welcher der folgenden Angriffe ist aktiv?

- ☒ Sniffing am Switch
- ☐ Sniffing im WLAN
- ☐ Shoulder Surfing
- ☐ Einem Gespräch lauschen

## 8. ITS PK3 [ID: 448749]

Wie kann man der schlechten Konfiguration von IT-Systemen entgegenwirken?

- ☒ Lesen der Handbücher
- ☐ Verwendung von Firewalls
- ☐ Sanktionen
- ☐ Bildschirm in Abwesenheit sperren

## 9. ITS PK15 [ID: 448761]

Welches Spoofing wurde in der Veranstaltung nicht vorgestellt?

- ☒ UDP-Spoofing
- ☐

- ☐ IP-Spoofing
- ☐ ARP-Spoofing
- ☐ MAC-Spoofing

## 10. ITS PK23 [ID: 448769]

Welches Zugriffskontrollmodell gibt es nicht?

- ☒ diskretgesteuert
- ☐ benutzerbestimmbar
- ☐ systembestimmt
- ☐ rollenbasiert

## 11. ITS PK19 [ID: 448765]

Was trifft nicht für einen LM Hash mit 14 ASCII-Zeichen zu?

- ☒ LM Hash kombiniert Passwort mit Salt
- ☐ LM Hash wandelt alle Buchstaben in Großbuchstaben um
- ☐ LM Hash teilt Passwort in zwei Gruppen von je 7 Zeichen
- ☐ LM Hash hasht jede Gruppe separat

## 12. ITS PK2 [ID: 448748]

Was gehört nicht zu den häufigsten Versäumnissen bei der Informationssicherheit?

- ☒ Ausreichende IT-Sicherheitsstrategie
- ☐ Unsichere Vernetzung / Internet-Anbindung
- ☐ Nichtbeachtung von Sicherheitsrichtlinien
- ☐ Schlechte Wartung von IT-Systemen

## 13. ITS PK13 [ID: 448759]

Was läuft nicht als *Kernel-Level Code* auf Ring 0 der i386-Architektur?

- ☒ Internet Explorer
- ☐ Dateisystem
- ☐ Monitoring Tools
- ☐ Antivirus-Tools

## 14. ITS PK5 [ID: 448751]

Wann liegt eine Gefährdung vor?



Bedrohung trifft auf Schwachstelle



Schwachstelle hat eine positive Eintrittswahrscheinlichkeit



Positive Eintrittswahrscheinlichkeit und hohes Schadenspotential fallen zusammen



Hohes Schadenspotential für eine Form der Bedrohung

## 15. ITS PK26 [ID: 448772]

Welches Protocol gibt es in der SSL Protokoll-Architektur?



SSL Change Cipherspec



SSL Alarm



SSL Compression



SSL Negotiation

## 16. ITS PK4 [ID: 448750]

Die Kosten einer Sicherheitsmaßnahme betragen 50.000 Euro, der erwartete Verlust mit Maßnahme 100.000 Euro, der ohne Maßnahme 300.000 Euro (alle Werte pro Jahr).

Wie groß ist der Nutzen pro Jahr?



150.000 Euro



-350.000 Euro



250.000 Euro



450.000 Euro

## 17. ITS PK17 [ID: 448763]

Angriffe E führt einen Man-in-the-Middle-Angriff auf A durch, bei dem er den Internet-Verkehr von A abhören möchte. Welche Information gibt er an A?



Meine IP ist: IP(Standard Gateway) und meine MAC ist: MAC(E).



Meine IP ist: IP(Standard Gateway) und meine MAC ist: MAC(Standard Gateway).



Meine IP ist: IP(lokalen DNS Server) und meine MAC ist: MAC(E).



Meine IP ist: IP(lokalen DNS Server) und meine MAC ist: MAC(lokalen DNS Server).

## 18. ITS PK25 [ID: 448771]

Was macht ein *Bridge Trust Center* in Bezug auf PKI?



Cross-Zertifizierung durch CA auf gleicher Ebene



Cross-Zertifizierung durch zusätzliche Zertifikate





Zertifizierung durch CA auf neuer Ebene



Speicherung von mehreren Wurzel-Zertifikaten im Browser

## 19. ITS PK30 [ID: 448776]

Was ist kein bei WLAN verwendetes Protokoll / Verfahren?



NIC



TKIP



CCMP



802.1X

## 20. ITS PK22 [ID: 448768]

Welches ist kein Faktor zur Authentisierung?



Bezeichnung



Wissen



Besitz



Merkmal

## 21. ITS PK27 [ID: 448773]

Welche Art von VPN-Tunnel wird in Unternehmen kaum verwendet?



Home Office zu Mobile Office



Mobile Office zu Unternehmensstandort



Unternehmensstandort zu Unternehmensstandort



Unternehmensstandort zu Home Office

## 22. ITS PK32 [ID: 448778]

Wie wird das Zugriffskontrollmodell *Discretionary Access Control* oft implementiert?



als ACL



als MAC



als IDS



als DES

## 23. ITS PK10 [ID: 448756]

Welche Verbreitungsart passt nicht zu *P2P-Würmern*?



**Ausführung über Autorun**

- ☐ Kopieren in freigegebene Ordner
- ☐ Imitierung von P2P-Protokoll-Antworten
- ☐ Ausnutzung von Schwachstellen des P2P-Netzes

**24. ITS PK11 [ID: 448757]**

Was ist ein Exploit?

**Eine Software**

- ☐ Eine Middleware
- ☐ Eine Hardware
- ☐ Eine Bloatware

**25. ITS PK24 [ID: 448770]**

Was ist in Bezug auf Softwareschwachstellen entscheidend?

**Patch Management**

- ☐ Firewall-Regeln
- ☐ Zugriffskontrolle
- ☐ Verschlüsselung

**26. ITS PK1 [ID: 448747]**

Informationssicherheit schützt die Vertraulichkeit, Integrität und Verfügbarkeit...

**aller relevanten Informationen einer Institution**

- ☐ nur der personenbezogenen Daten einer Institution
- ☐ nur der elektronisch gespeicherten Daten einer Institution
- ☐ aller nicht-kritischen Information einer Institution

**27. ITS PK14 [ID: 448760]**

Welche Flux-Botnetze gibt es nicht?

**P2P-Flux**

- ☐ Fast-Flux
- ☐ Single-Flux
- ☐ Double-Flux

**28. ITS PK28 [ID: 448774]**

Welche Gestaltungsmöglichkeit ergibt sich durch den Einsatz von Firewalls nicht?

- ☒ Verteilte Authentifizierung der Kommunikationspartner
- ☐ Bündelung von Sicherheitsmaßnahmen an einem Punkt
- ☐ Sicherheitsrichtlinien lassen sich einfacher durchsetzen
- ☐ Ideal um Missbrauch zu protokollieren

## 29. ITS PK21 [ID: 448767]

Was ist kein kryptographisches Verfahren?

- ☒ Hashfunktion
- ☐ Symmetrische Verschlüsselung
- ☐ Asymmetrische Verschlüsselung
- ☐ Message Authentication Code

## 30. ITS PK7 [ID: 448753]

Was gehört zur Phase Attack im typischen Angriffsverlauf?

- ☒ Penetration
- ☐ Footprinting
- ☐ Port Scanning
- ☐ Enumeration

## 31. ITS PK31 [ID: 448777]

Was stimmt für Funknetze im Vergleich zu kabelgebundenen Netzen in Bezug von Sicherheit **nicht**?

- ☒ Autorisierung ist schwieriger
- ☐ Abhören ist einfacher
- ☐ Erfordert Re-Authentisierung
- ☐ Aufenthaltsort des Geräts ist besonders zu schützen

## 32. ITS PK20 [ID: 448766]

Was ist keine Technik des *Social Engineerings*?

- ☒ IP-Address Spoofing
- ☐ Ausspionieren des persönlichen Umfeld des Opfers
- ☐ Vortäuschen falscher Identitäten
- ☐

Ausnutzen von Verhaltensweisen wie Autoritätshörigkeit