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

			1
			Informationssicherheit schützt (1 Punkt)
	IT Sicharbait 2 M	loitoro Erag	Sie haben die folgende Antwort gegeben:
	IT-Sicherheit 2 - W	reitere Frag	gr
	Montag, 11. Februar 2019 18:2		
		4	mationssicherheit schützt die Vertraulichkeit, Integrität und Verfügbar
	Virus Einsprung (1 Punkt)		
	Sie haben die folgende Antwo		aller relevanten Informationen einer Institution 🔀
	Welcher Virus verschleiert sei	nen <i>Einsprung</i> ?	o nur der personenbezogenen Daten einer Institution 🚷
			nur der elektronisch gespeicherten Daten einer Institution 🚷
	© EPO-Virus	Von (inkl)	alle nicht-kritischen Information einer Institution
	(LI O VII us)	448964	
	O Überschreibender Virus	-	€ 2
	Oberschreibender virus	449046	
	0	Bis (inkl)	
	Appending-Virus		
	0		
	Companion-Virus		
			Infektionswege (2 Punkte)
5			Sie haben die folgende Antwort gegeben:
	Viren-Selbstschutz (1 Pun	_	
	Sie haben die folgende Antwo		
	Was ist kein Viren-Selbstschu	ıtz?	Was sind die wesentlichen Infektionswege für Schadsoftware?
			was sind die wesendichen mierklonswege für Schladsoftware?
	Strength		
	Strength		 Ausführung des Schadprogramms durch Benutzer
	O Charallela		☐ Ausnutzen einer Schwachstell des Syste 3
	Stealth		Durchführen eines Man-in-the-Middle Angmis
	0		☐ Spoofing der Benutzer-Identität ✓
	Polymorphie		I and the second
	0		
	Metamorphie		
6	Handy-Wurm ikee (1 Punk	t)	
	Sie haben die folgende Antwo	_	
	_		n Erfolg des Handy-Wurms <i>ikee nicht r</i> elevant?
	Welche Voludssetzung des III	iones war far den	TETTOIG des riding Warms thee ment relevants
	0		
	Das Telefon musste entsperrt	sein	
	0		
		n Jailbreak für nich	cht-offizielle Anwendungen offen sein
	•		
	O Auf dem Telefon musste ein b	estimmter SSH Se	Server installiert sein
	_		
	O Standard-Passwörter musster	n unverändert sein	Virusaufbau (2 Punkte)
	Standard russworter mussici	r directandere Seni	Sie haben die folgende Antwort gegeben:
7			
,	Trojanisches Pferd (1 Puni	kt)	
	Sie haben die folgende Antwo	rt gegeben:	Welche Teile gehören (ggf. optional) zum Aufbau eines Virus?
	Was stimmt für ein <i>trojanisch</i>	es Pferd <u>nicht</u> ?	
	-		☐ Erkennungsteil 🎛
	0		☐ Bedingungsteil 😵
	Infiziert andere Dateien		☐ Versteckungsteil
	0		☐ Kontrollteil ⊘

	Enthält griechische Soldaten
	0
	Hat tatsächliche nützliche Funktionalität
	O 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
	0
	Mit schadhaft verlinkten Werbebannern
	O Mit der Qualität von Partnerprogrammen
	O Mitario facile au Vandauritaura
	Mit einfacher Verbreitung
9	Software-Schwachstelle (1 Punkt)
	Sie haben die folgende Antwort gegeben:
	Was ist normalerweise kein Grund für Software-Schwachstellen?
	0
	Technische Limitationen der Programmiersprache
	C Schlechte Programmierung
	O Komplexität der Systeme
	0
	Zeitdruck in Projekten
10	Teilmenge (1 Punkt)
	Sie haben die folgende Antwort gegeben:
	Was ist eine Teilmenge von was?
	0
	Exploits sind eine Teilmenge von Angriffen, die wiederum eine Teilmenge von Gefährdungen sind
	O Angriffe sind eine Teilmenge von Exploits, die wiederum eine Teilmenge von Gefährdungen sind
	O Gefährdungen sind eine Teilmenge von Exploits, die wiederum eine Teilmenge von Angriffen sind
	O Angriffe sind eine Teilmenge von Gefährdungen, die wiederum eine Teilmenge von Exploits sind
11	Puffor (1 Punkt)
	Puffer (1 Punkt) Sie haben die folgende Antwort gegeben:
	and the state of t

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

	O FF
	O 77
	O 09
.2	Buffer Overflow (1 Punkt) Sie haben die folgende Antwort gegeben: Was versucht ein Angreifer bei einem <i>Buffer Overflow</i> gezielt auf dem Stack zu überschreiben?
	© Rücksprungadresse
	O Übergabeparameter
	O Base Pointer
	O Lokale Variablen
13	Formatstring-Angriff (1 Punkt) Sie haben die folgende Antwort gegeben: Was passt zu Formatzeichen bei einem Formatstring-Angriff?
	O %s
	O &s
	O \$s
	O §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
	O Rootkit
	O Backdoor
	O Botnetz
15	XSS (1 Punkt) Sie haben die folgende Antwort gegeben:

IT Sicherheit 2 Seite 3

	Welche Hauptvariante von XSS gibt es?	
	© Reflected	
	O Permanent	
	O Advanced	
16	O Hooked	
10	BIOS (1 Punkt)	
	Sie haben die folgende Antwort gegeben:	
	Was war ein <i>Universalpasswort</i> für BIOS?	
	C (LKWPETER)	
	O PKWPETER	
	O BUSPETER	
	O KRANPETER	
17	Rootkit (2 Punkte) Sie haben die folgende Antwort gegeben: Wie können Rootkits unter Windows Schadcode in User	r-Prozesse bringen?
	SetWindowsHookEx	
	Debbugging System	Rootkit (2 Punkte) Sie haben die folgende Antwort gegeben:
	☐ ForceWeakTasks	
	☐ EnableApplicationHeap	Wie können Rootkits unter Windows Schadcode in User-Prozesse bringen? ☐ SetWindowsHookEx ★
	Inline Function Hooking (1 Punkt)	☐ Debbugging System ☐ ForceWeakTasks ☐ EnableApplicationHeap ☐
18		
	Sie haben die folgende Antwort gegeben: Was macht Inline Function Hooking?	
	O Modifiziert die ersten Bytes einer DLL zum Einsprung ir	n den Schadcode
	O Modifiziert die Adresstabelle einer DLL zum Einsprung	
	mouniziert die Adresstabelle einer DEL zum Einsprüng	iii deli Schadcode
	O Modifiziert den Funktionsaufruf in einer DLL mit falsche	en Parametern

O 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 eingeschränktere 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
	O Army
23	Round Robin (1 Punkt) Sie haben die folgende Antwort gegeben: Auf welches Botnetz trifft zu, dass Adressen der C&C-Server per <i>Round-Robin</i> vergeben werden und ständig wechseln?
	O Single-Flux
	C Peer-to-Peer
	O Hydra
	C Alureon
24	Britney Spears (1 Punkt) Sie haben die folgende Antwort gegeben: Welcher Account von <i>Britney Spears</i> wurde als Befehlskanal von C&C-Servern missbraucht?
	C Instagram
	O Facebook
	O SnapChat
	C Twitter
25	Flut-Angriffe (1 Punkt) Sie haben die folgende Antwort gegeben: Welche Protokolle werden in der Vorlesung als Beispiele für Flut-Angriffe genannt?
	O UDP und ICMP
	C TCP und IP
	O UDP und TCP
	C ICMP und IP
26	Sniffer (1 Punkt) Sie haben die folgende Antwort gegeben: Was ist ohne Zustimmung ein nicht legitimer Einsatz von Sniffern?

C Leistungsüberwachung von Mitarbeitern

	C Erkennen von Angriffen
	O Filtern von verbotenen Inhalten
	O Troubleshooting
27	IP Spoofing (1 Punkt)
	Sie haben die folgende Antwort gegeben: Was ist ein Problem bei <i>IP Spoofing</i> ?
	Sender erhält keine Antworten
	O Ist für Angreifer nur über die Programmierung von raw sockets anwendbar
	O Kein DoS-Angriff möglich
	O 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?
	O ARP ist zustandslos und erlaubt gratuitious ARP
	O ARP ist zustandsbehaftet und erlaubt gratuitious ARP
	O ARP ist zustandslos und verbietet gratuitious ARP
	O ARP ist zustandsbehaftet und verbietet gratuitious 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
	O Angreifer muss schnell eine passende DNS-Anfrage senden
	O Angreifer muss eine korrekt verschlüsselte DNS-Antwort liefern
	O Angreifer muss eine korrekt verschlüsselte DNS-Anfrage senden
30	Pharming (1 Punkt)

29

30

Sie haben die folgende Antwort gegeben:

IT Sicherheit 2 Seite 7

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 ...

0

Rainbow Tables

0

Tastaturzeichenfolgen

0

Fußballvereine

0

Telefonnummern

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?

0

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

0

Sie starten von A aus vorwärts und das gesuchte Passwort ist ${\sf C}.$

0

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

0

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?

0

Pre-Texting

0

Plain-Texting

0

Post-Texting

0

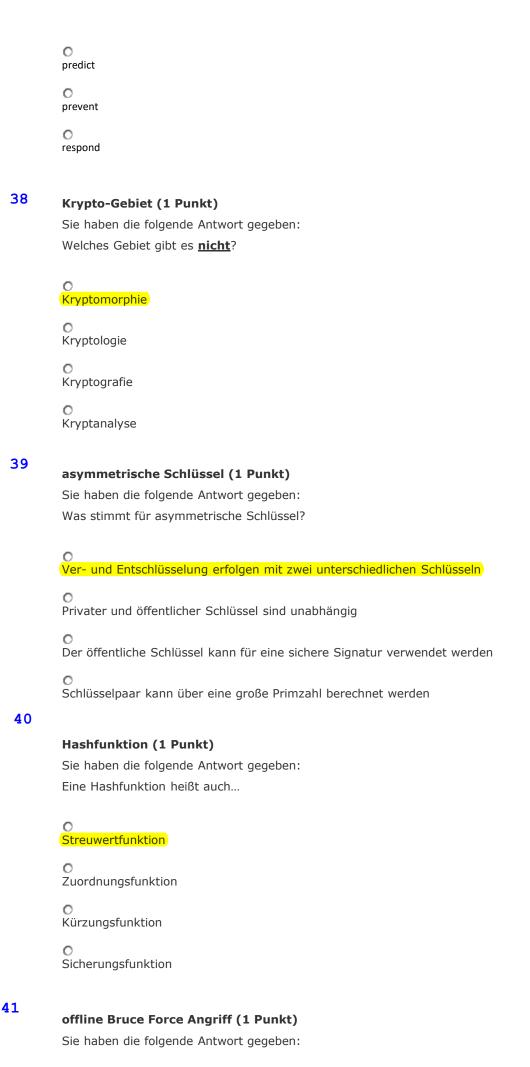
Task-Texting

37 Angriffserkennung (1 Punkt)

Sie haben die folgende Antwort gegeben:

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

O detect



0
Findet den Schlüssel in endlicher Zeit
Findet den Schlüssel in unendlicher Zeit (theoretischer Angriff)
O Findet den Schlüssel nicht, wenn dieser mindestens 256 Bit lang ist
O Findet den Schlüssel nicht, unabhängig von der Schlüssellänge
One-Time Pad (1 Punkt) Sie haben die folgende Antwort gegeben: Warum kann ein <i>Unbreakable Code</i> in Form eines One-Time Pads nicht angegriffen werden?
O Angriff ergibt alle möglichen Klartexte
O Angriff ergibt verwürfelten Klartext
O Angriff ergibt nur Nullen als Klartext
O Angriff ergibt gar keinen Klartext
Zugriffskontrolle (1 Punkt) Sie haben die folgende Antwort gegeben: Welches ist kein Schritt der Zugriffskontrolle?
C Identifikation
O Authentisierung
O Authentifizierung
O Identifizierung
Authentisierung (1 Punkt) Sie haben die folgende Antwort gegeben: Welche Authentisierung benutzt <u>keinen</u> zweiten Faktor?
© Geldschein
O Bankkarte
O Sim-Karte
O Personalausweis

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

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?

O 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?

DAC

MAC

O RBAC

49

Mandatory Access Control (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was wird beim Zugriffskontrollmodell Mandatory Access Control miteinander verglichen?

0

Freigabe (Clearance) mit Sicherheitskennung (Security Label)

0

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

0

Zugriffsliste (Access Control List) mit Rolle (Role)

0

Rolle (Role) mit Freigabe (Clearance)

50

Vertraulichkeitsstufen (1 Punkt)

Sie haben die folgende Antwort gegeben:

Welche Regeln gibt es für Vertraulichkeitsstufen?

0

Read-Down und No-Write-Down

0

No-Read-Down und No-Write-Down

C

No-Read-Down und Write-Down

0

Read-Down und Write-Down

51

Nachweis (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was lässt sich nur extrem schwierig nachweisen?

0

Rechner ist frei von Schadsoftware

0

Eine gerade erst bekannt gewordene Schadsoftware ist auf dem Rechner

Ö

Eine Standard-Datei auf dem Rechner wurde manipuliert

0

Ein Programm verhält sich falsch

52

Erkennungsmethoden von Antivirensoftware (2 Punkte)

Sie haben die folgende Antwort gegeben:

Was sind Erkennungsmethoden von Antivirensoftware?

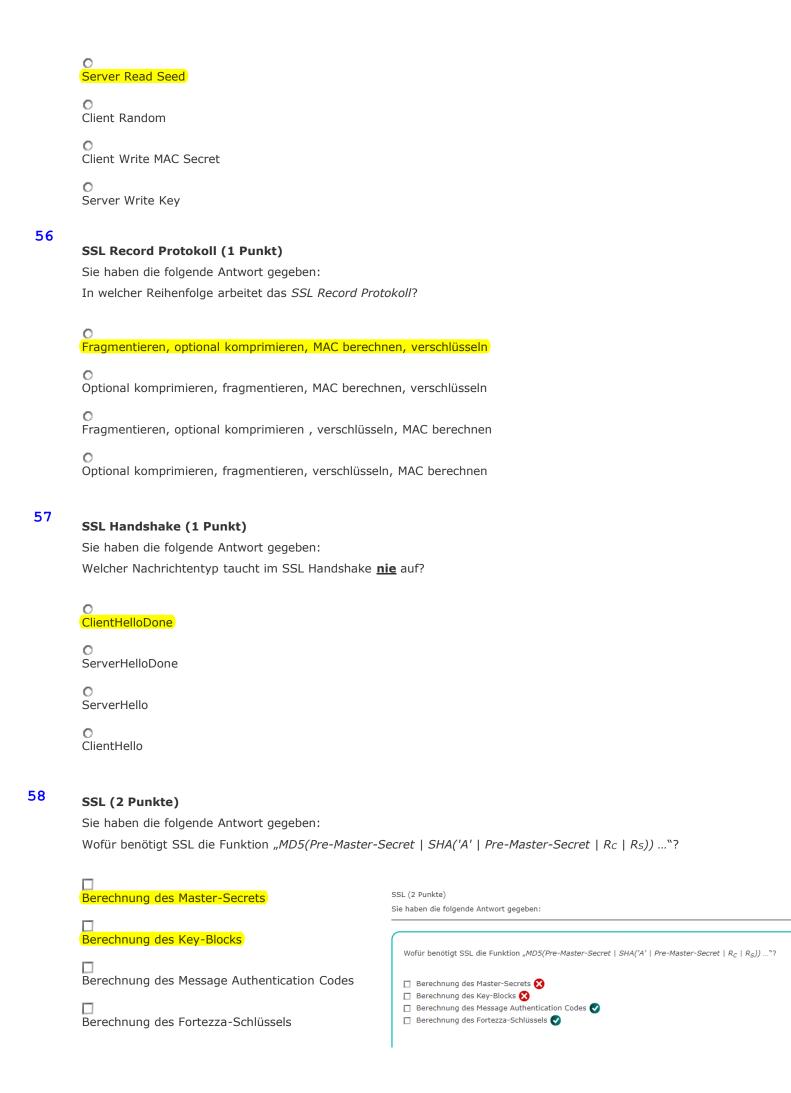


Heuristik)
☐ Quarantäne
□ Meldung
Erkennungsmethoden von Antivirensoftware (2 Punkte)
Sie haben die folgende Antwort gegeben:
Was sind Erkennungsmethoden von Antivirensoftware?
☐ Signaturen ※ ☐ Heuristik ※
☐ Quarantäne ✔
☐ Meldung ②
SSL Schutzziel (1 Punkt) Sie haben die folgende Antwort gegeben: Welches Schutzziel wird von SSL <u>nicht</u> abgedeckt?
O Verfügbarkeit
O Vertraulichkeit
O Integrität
O Authentizität
PKI Zertifikate (1 Punkt) Sie haben die folgende Antwort gegeben:
Wie werden bei PKI Zertifikate organisiert?
O In einer Baumstruktur
O In einer doppelt verketteten Liste
O In einem Feld
O In einer Certificate Revocation List
Zustand einer SSL-Verbindung (1 Punkt)
Sie haben die folgende Antwort gegeben:

54

55

Welcher Parameter wird für den Zustand einer SSL-Verbindung $\underline{\textbf{nicht}}$ benötigt?



Firewalls (2 Punkte)		
Sie haben die folgende Antwort gegeben:		
Was können Firewalls ?		
☐ Illegalen Zugriff auf internen Systeme verhind	dern 😵	
 □ Denial-of-Service- Angriffe abwehren □ Vor bösartigen Insidern schützen 		
☐ Vor Angriffen schützen, die über autorisierte 2	Zugriffe stattfind	den 🗸
Zustandsloser Paketfilter (1 Punkt)		
Sie haben die folgende Antwort gegeben:		
Nach welchen Kriterien filtert ein <i>zustandsloser</i> Pake	tfilter typischerv	veise?
0		
IP-Adressen und Ports		
O Ports und Anwendungsheader		
O Anwendungsheader und MAC-Adressen		le TCP-SYN (ACK=0) nur
MAC-Adressen und IP-Adressen		erver (Port 80) oder (Port 25) erlauben
Firewallregel (1 Punkt)		
Sie haben die folgende Antwort gegeben:		
Sie möchten mit Ihrem zustandslosen Paketfilter "ver Welche Regel passt?	rhindern, dass I	hre Rechner von <i>außen 'gepingt</i> ' werd
O Alle eingehenden ICMP-Echo-Request-Pakete verwer	<mark>fen</mark>)	Alle eingehenden ICMP-Echo-
0		Request-Pakete verwerfen.
Alle eingehenden ICMP-Echo-Reply-Pakete verwerfer	า	aus Tabele (transparenter text)
O Alle ausgehenden ICMP-Echo-Request-Pakete verwei	rfen	
O Alle ausgehenden ICMP-Echo-Reply-Pakete verwerfe	n	
Default Deny (1 Punkt)		

61

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

O 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 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 WPA/WPA2 (1 Punkt) Sie haben die folgende Antwort gegeben: Was ist Teil der WPA- und WPA2-Instanzen-Authentisierung? 4-Way-Handshake O 1-Way-Handshake O 2-Way-Handshake O 3-Way-Handshake 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 O Sorgloser Umgang mit Passwörtern

67 Beachtung (1 Punkt)

64

65

	Warum werden Sicherheitsrichtlinien oft nicht beachtet?
	© Bequemlichkeit
	O Kosten
	O Zeitmangel
	C 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?
	C Vorsicht bei Web-Browsern und Emails walten lassen
	O
	Ordnung am Arbeitsplatz halten
	O Bildschirm bei Abwesenheit sperren
	<u>O</u>
	Zutrittsschutz einrichten
69	Wie kann man Gefahren durch Einbrecher und Katastrophen entgegenwirken?
	O Mobile Geräte nicht unbeaufsichtigt lassen
	O Angemessene Berücksichtigung von IT-Sicherheit
	O Virenschutzprogramme einsetzen
	O Sicherheits-Patches einspielen
70	
, 0	Wodurch werden der Informationssicherheit häufig Grenzen gesetzt?
	C Zugriff und Kosten
	C Kosten und Zutritt
	C Zutritt und Kommunikation
	C Kommunikation und Zugriff
71	

Sie haben die folgende Antwort gegeben:

69

70

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*).

Wir groß sind die Kosten der Maßnahme pro Jahr?

50.000 Euro

0

100.000 Euro

0

150.000 Euro

0

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 ($E(Verlust\ ohne\ Maßnahme)$) zur Verfügung.

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

E(Verlust mit Maßnahme) und (Kosten der Maßnahme)

(Kosten der Maßnahme) und (Kosten ohne Maßnahme)

© (Kosten ohne Maßnahme) und E(Verlust der Maßnahme)

(Kosten ohne Maßnahme) und E(Verlust der Maßnahme)

E(Verlust der Maßnahme) und E(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

O Vorfall, der sich negativ auf die Verfügbarkeit eines Systems auswirkt

O Schadcode, der einen Computer infizieren kann

74

Risiko (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was hat keinen Einfluss auf ein Risiko?

O Maßnahr

Maßnahmenkosten

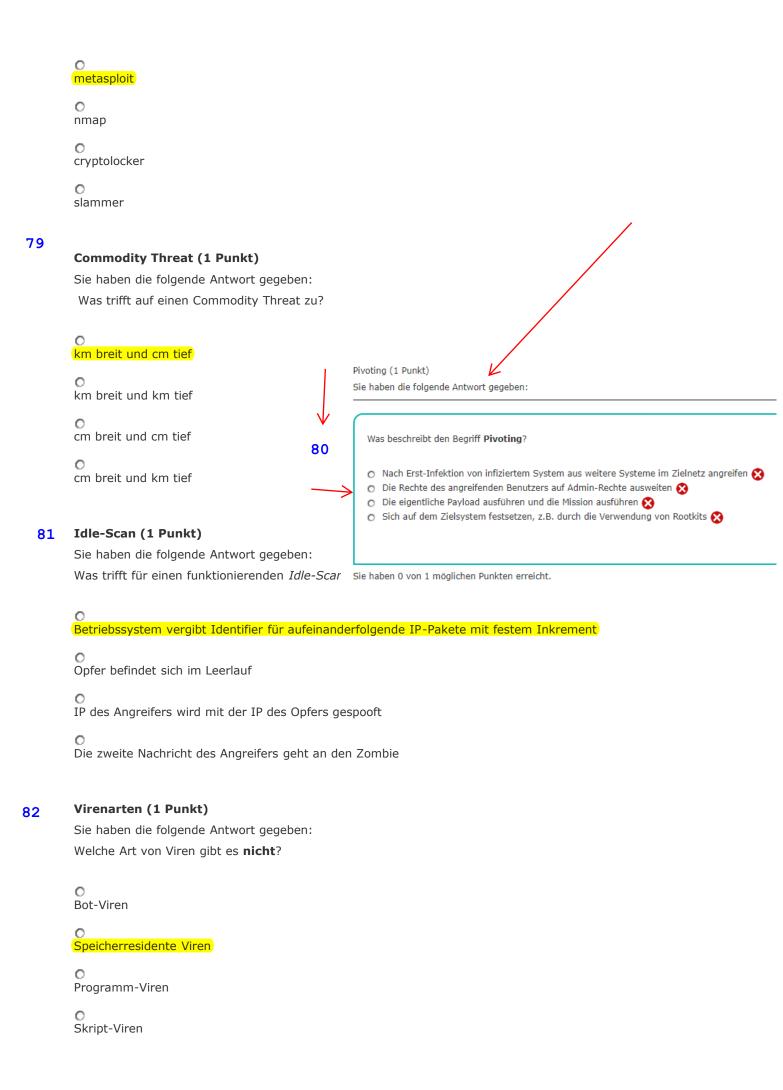
	Gefährdung
	© Eintrittswahrscheinlichkeit
	O Schadenspotential
75	
	Risiko-Behandlungsstrategie (1 Punkt) Sie haben die folgende Antwort gegeben: Welche Art von Risiko-Behandlungsstrategie verfolgt eine Versicherung?
	© Übertragung
	© Reduktion
	O Akzeptanz
	O Vermeidung
76	Aktiver Angriff (1 Punkt) Sie haben die folgende Antwort gegeben: Welcher der folgenden Angriffe ist aktiv?
	ARP Spoofing
	O Sniffing im WLAN
	O Shoulder Surfing
	Passwort-Cracking offline
77	
	Pre-Attack (1 Punkt)
	Sie haben die folgende Antwort gegeben: Was gehört zur Phase <i>Pre-Attack</i> im typischen Angriffsverlauf?
	© Enumeration
	© Penetration
	© Exploitation
	O Spuren verwischen
78	

75

Schwachstellen testen und Ausnutzen (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was ist ein Framework zum Testen und Ausnutzen von Schwachstellen?



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?

C Trojanisches Pferd

O Virus

0

Wurm

0

Exploit

IT-Sicherheit 2 Klausurfragen

Montag, 11. Februar 2019 17:33

ITS2 Klausur 2-1 (1 Punkt)

Sie haben die folgende Antwort gegeben:

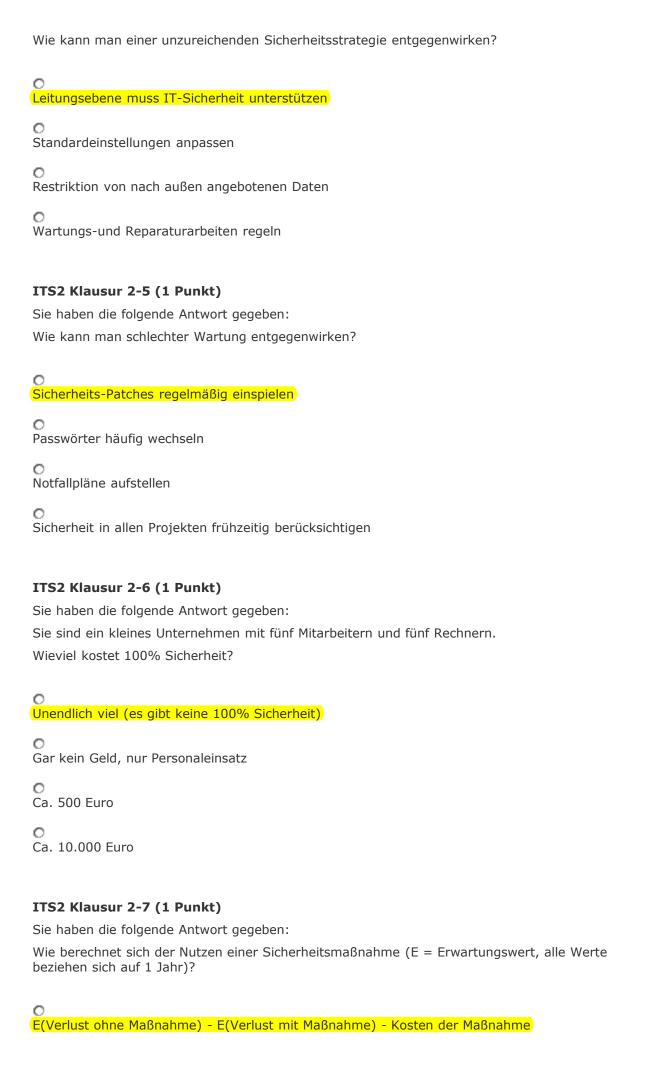
Welches ist keines der drei klassischen Schutzziele der Informationssicherheit?

Authenticity
O Integrität
Confidentiality
O Verfügbarkeit
ITS2 Klausur 2-2 (1 Punkt)
Sie haben die folgende Antwort gegeben:
Was gehört <u>nicht</u> zu den häufigsten Versäumnissen bei der Informationssicherheit?
Schlechte Konfiguration von IT-Systemen
Nichtbeachtung von Sicherheitsrichtlinien
C 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
O Passwort weitergeben

ITS2 Klausur 2-4 (1 Punkt)

Standard-Passwörter nutzen

Sie haben die folgende Antwort gegeben:



© E(Verlust mit Maßnahme) + Kosten der Maßnahme - E(Verlust ohne Maßnahme)
© Kosten der Maßnahme - E(Verlust ohne Maßnahme) - E(Verlust mit Maßnahme)
© E(Verlust ohne Maßnahme) - E(Verlust mit Maßnahme) + 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?
O Euro
O 100.000 Euro
O 200.000 Euro
O 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
O Sicherheitsrelevanter Fehler eines IT-Systems
© Fehlende Patches in einem System
O 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
0

Schadenspotential, Bedrohung, Schwachstelle
O 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?
O Vermeidung
O Übertragung
Reduktion
O Akzeptanz
ITS2 Klausur 2-12 (1 Punkt) Sie haben die folgende Antwort gegeben: Welcher der folgenden Angriffe ist passiv?
Sniffing im WLAN
O Password-Cracking online
O DNS Cache Poisoning
O Distributed DoS
ITS2 Klausur 2-13 (1 Punkt) Sie haben die folgende Antwort gegeben: Zu welcher Angriffsphase gehört Reconnaissance?
Pre-Attack
O Attack
O Post-Attack
O Improve-Attack

Sie haben die folgende Antwort gegeben: Welches Programm ist ein Port Scanner? 0 nmap netcat 0 ping john the ripper ITS2 Klausur 2-15 (1 Punkt) Sie haben die folgende Antwort gegeben: Was trifft auf einen Advanced Persistent Threat zu? 0 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:

ITS2 Klausur 2-14 (1 Punkt)

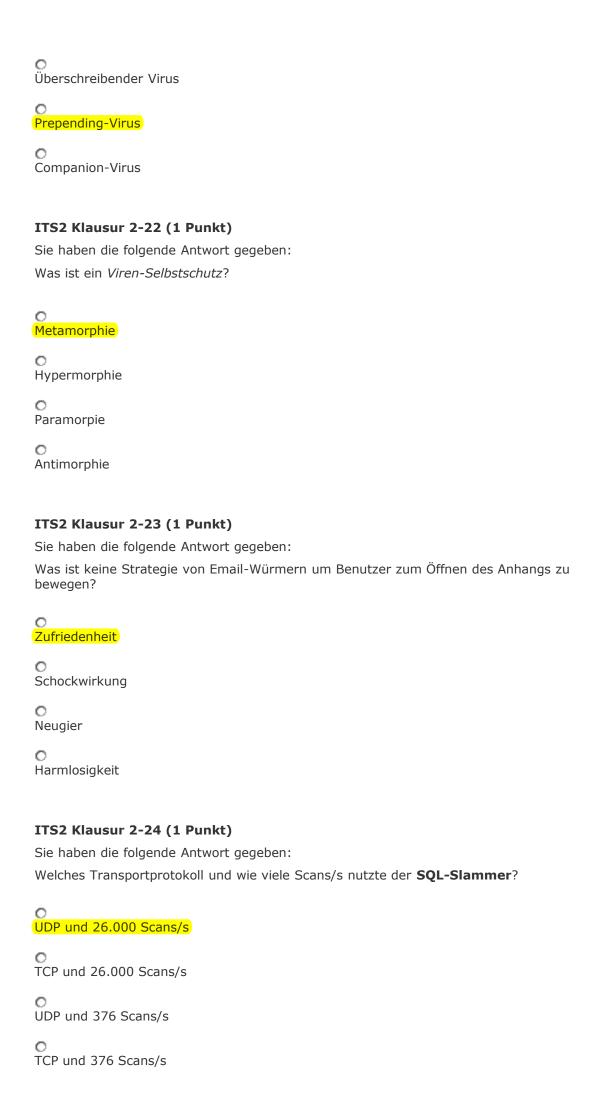
Sie führen einen TCP SYN Scan durch.

Welches Paar von Nachrichten signalisiert einen geschlossenen Port	:?
0	

Auf ein SYN folgt ein RST
_
Auf ein SYN/ACK folgt ein RST
0
Auf ein RST folgt ein SYN/ACK
O 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
O Virus
C 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
Exploit released in the wild, Schwachstelle wild veronentiicht, Fatch wild veronentiicht
Patch wird veröffentlicht, Patch wird installiert, Exploit released in the wild
Schwachstelle vom Hersteller erkannt, Schwachstelle wird eingeführt, Patch wird installiert

O Appending-Virus

Welche zeitliche Reihenfolge von links nach rechts ist für Schwachstellen korrekt? (Wählen Sie zwei Antworten) Schwachstelle wird eingeführt, Schwachstelle wird veröffentlicht, Virenschutz wird erganzt	
Exploit released in the wild, Schwachstelle wird veröffentlicht, Patch wird veröffentlicht	Welche zeitliche Reihenfolge von links nach rechts ist für Schwachstellen korrekt? (Wählen Sie zwei Antworten
Sie haben die folgende Antwort gegeben: Welche Teile gehören (ggf. optional) zum Aufbau eines Virus? (Wählen Sie zwei Antworten) Vermehrungsteil Tarnungsteil Steuerungsteil 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) Wermehrungsteil Tarnungsteil Steuerungsteil Steuerungsteil Verschlüsselungsteil Tarnungsteil Steuerungsteil Steuerungsteil Steuerungsteil Welche Teile gehören (ggf. optional) zum Aufbau eines Virus? (Wählen Sie zwei Antworten)	 □ Exploit released in the wild, Schwachstelle wird veröffentlicht, Patch wird veröffentlicht □ Patch wird veröffentlicht, Patch wird installiert, Exploit released in the wild
Welche Teile gehören (ggf. optional) zum Aufbau eines Virus? (Wählen Sie zwei Antworten) Vermehrungsteil Tamungsteil Steuerungsteil 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 Tamungsteil Steuerungsteil Verschlüsselungsteil Verschlüsselungsteil Tamungsteil Steuerungsteil Steuerungsteil Verschlüsselungsteil Verschlüs	ITS2 Klausur 2-20 (2 Punkte)
Antworten) Vermehrungsteil	Sie haben die folgende Antwort gegeben:
Tarnungsteil Steuerungsteil 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 Verschlüsselungsteil ITS2 Klausur 2-21 (1 Punkt) Sie haben die folgende Antwort gegeben:	
Tarnungsteil Steuerungsteil 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 Verschlüsselungsteil ITS2 Klausur 2-21 (1 Punkt) Sie haben die folgende Antwort gegeben:	Voume have a stail
Steuerungsteil Uerschlüsselungsteil 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) Uermehrungsteil Tarnungsteil Steuerungsteil Verschlüsselungsteil Verschlüsselungsteil Steuerungsteil Steuerungsteil Steuerungsteil Steuerungsteil Steuerungsteil Steuerungsteil Steuerungsteil Steuerungsteil	vermenrungsteil
Steuerungsteil 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:	Tarnungsteil)
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:	
Sie haben die folgende Antwort gegeben: Welche Teile gehören (ggf. optional) zum Aufbau eines Virus? (Wählen Sie zwei Antworten) □ Vermehrungsteil (Tarnungsteil (Verschlüsselungsteil (Verschlüsselungs	
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:	ITS2 Klausur 2-20 (2 Punkte)
<pre></pre>	Sie haben die folgende Antwort gegeben:
<pre></pre>	
☐ Tarnungsteil Steuerungsteil Verschlüsselungsteil Verschlüsselungsteil Verschlüsselungsteil Verschlüsselungsteil Sie haben die folgende Antwort gegeben:	Welche Teile gehören (ggf. optional) zum Aufbau eines Virus? (Wählen Sie zwei Antworten)
☐ Steuerungsteil ✔ ☐ Verschlüsselungsteil ✔ ITS2 Klausur 2-21 (1 Punkt) Sie haben die folgende Antwort gegeben:	
ITS2 Klausur 2-21 (1 Punkt) Sie haben die folgende Antwort gegeben:	☐ Steuerungsteil
Sie haben die folgende Antwort gegeben:	☐ Verschlüsselungsteil
	ITS2 Klausur 2-21 (1 Punkt)
Welcher Virus muss aufgrund eines Sprungbefehls Originaldaten ans Ende schieben?	Sie haben die folgende Antwort gegeben:
	Welcher Virus muss aufgrund eines Sprungbefehls Originaldaten ans Ende schieben?



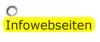
Sie haben die folgende Antwort gegeben: Wie entstehen Trojanische Pferde? Einsatz eines Linkers Setzen von Rechten Bottom-Up Ansatz Top-Down Ansatz ITS2 Klausur 2-26 (1 Punkt) Sie haben die folgende Antwort gegeben: Wie wird ein Trojanisches Pferd aktiv? Start des Wirtsprogramms Autorun Fernsteuerung 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 2-25 (1 Punkt)

ITS2 Klausur 2-28 (1 Punkt)

Sie haben die folgende Antwort gegeben:

_	
○ Sind ein	e Sammlung von Exploits
_	
O Werden	als kommerzielle Software oder Dienstleistung verkauft
0	
<mark>Bestehe</mark>	n aus einer Reihe von Webseiten
ITS2	Klausur 2-29 (1 Punkt)
Sie ha	ben die folgende Antwort gegeben:
Wie wi	rd <i>Speicherplatz</i> vergeben?
_	
Heap v	vächst nach oben, Stack nach unten
0	
Stack	wächst nach oben, Heap nach unten
O Baida	wachsen nach oben
_	wachsen hach oben
O Beide	wachsen nach unten
ITS2	Klausur 2-30 (1 Punkt)
	ben die folgende Antwort gegeben:
Was p	asst zu einem <i>nicht-persistentem</i> XSS Angriff?
0	
O <mark>Link in</mark>	Email)
0	
O Anhan	<mark>Email</mark>) g in Email
O Anhan	g in Email
O Anhan O USB-S	g in Email tick
O Anhan O USB-S	g in Email
O Anhan O USB-S	g in Email tick
O Anhan O USB-S O SQL-Ir	g in Email tick



C Gästebücher
O Bewerbungen
O Verkaufsanzeigen
ITS2 Klausur 2-32 (1 Punkt) Sie haben die folgende Antwort gegeben: Was ist ein <i>Drive-by-Download</i> ?
0
Automatischer Download bei Besuch einer Webseite
O Automatischer Download bei Einstecken eines USB-Drives
O Automatischer Download bei der Registrierung im fremden Netz
O 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

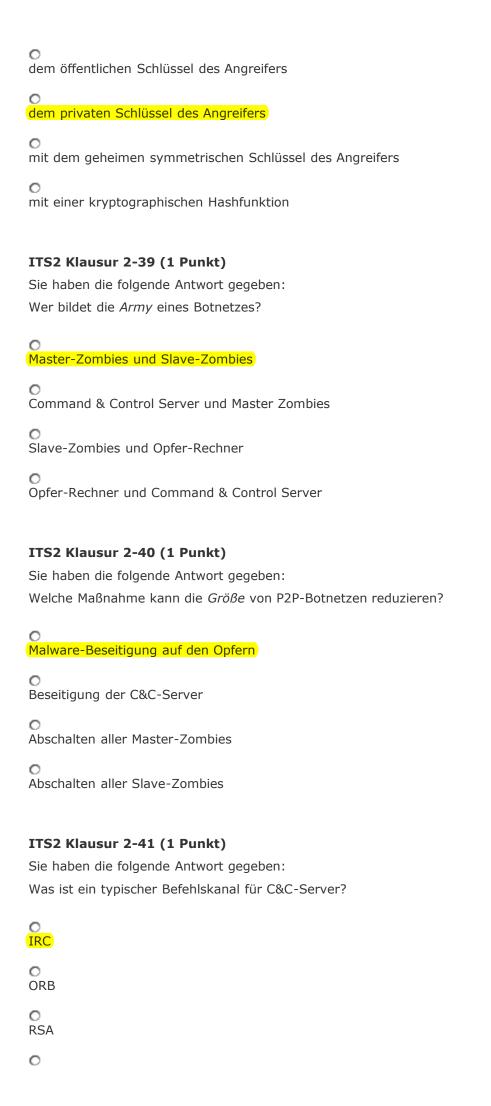
Sie haben die folgende Antwort gegeben:

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?
O Mechanismen zum Verbergen der Existenz
O Umgehung der Authentifizierung
O Alternativer Zugang
O 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

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
O Modifikation der Anwendung bei API-Aufrufen
O Modifikation des Interfaces bei API-Aufrufen
O Modifikation der angefragten Information bei API-Aufrufen
ITS2 Klausur 2-37 (1 Punkt) Sie haben die folgende Antwort gegeben: Spyware
Sammelt heimlich Informationen
o zeigt zusätzliche Werbung
overhindert 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...



ITS2 Klausur 2-42 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Auf welche Art wird DNS für DoS-Angriffe missbraucht?
O DNS Verstärkung
O DNS Cache Poisoning
O DNS Changer
O 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
La vicio naisonone versinaangen ana adaaran siookaac
Absturz des Empfängers durch falsche Flags
Ö Übernahme der Session durch Raten der Sequenznummer
O 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
O non-promiscuous
© persistant
O non-persistant

ITS2 Klausur 2-45 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Sender-MAC-Adresse kann per Software geändert werden
O MAC-Address-Filter funktionieren nicht bei WLANs
© Empfänger-MAC-Adressen sind non-promiscuous
O Trotz MAC-Address-Filters können die verkapselten IP-Pakete durchkommen
ITS2 Klausur 2-46 (1 Punkt)
Sie haben die folgende Antwort gegeben: Was passiort bei DNS Casha Poisoning?
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
Ö 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?
3 3 <u></u>
0
Hostname des angefragten DNS-Servers muss stimmen
O IP-Adresse und Port des angefragten DNS-Servers müssen stimmen
O IP-Adresse und Port des anfragenden Hosts müssen stimmen
O Die Referenznummer der Anfrage muss stimmen
ITS2 Klausur 2-48 (1 Punkt)
Sie haben die folgende Antwort gegeben:
Was verschleiert <i>Spoofing</i> ?
Die eigene Identität

O Den Empfänger
O Die Ziel-IP
O 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?
Sie haben die folgende Antwort gegeben:
Sie haben die folgende Antwort gegeben: Was kann ein Man-in-the-Browser-Angriff nicht?
Sie haben die folgende Antwort gegeben: Was kann ein Man-in-the-Browser-Angriff nicht? C Salted Hashes knacken
Sie haben die folgende Antwort gegeben: Was kann ein Man-in-the-Browser-Angriff nicht? C Salted Hashes knacken Daten außerhalb des verschlüsselten Tunnels modifizieren
Sie haben die folgende Antwort gegeben: Was kann ein Man-in-the-Browser-Angriff nicht? Consider Manipuliere
Sie haben die folgende Antwort gegeben: Was kann ein Man-in-the-Browser-Angriff nicht? Calted Hashes knacken Daten außerhalb des verschlüsselten Tunnels modifizieren Webseiten Manipuliere Eingabefelder auslesen ITS2 Klausur 2-51 (1 Punkt) Sie haben die folgende Antwort gegeben:
Sie haben die folgende Antwort gegeben: Was kann ein Man-in-the-Browser-Angriff nicht? Calted 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?

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
O 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? O 36 hoch 10
0 10 hoch 36
26 hoch 20
O 20 hoch 26
ITS2 Klausur 2-54 (1 Punkt) Sie haben die folgende Antwort gegeben: Was ist <u>keine</u> Social-Engineering Technik?
Cash Poisoning
O Spear Phishing
O Baiting
© CEO Fraud

2-55 (1 Punkt)

Welche Art von Maßnahme schützt Systeme gegen Bedrohungen?

prevent prevent
O detect
O predict
O 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 and Entschassering entrigen mit dem gleichen Schlasser
O Ver- und Entschlüsselung erfolgen mit zwei unterschiedlichen Schlüsseln
C Schützt nicht die Integrität von Nachrichten
Schutzt hicht die Integritat von Nachhenten
Schützt die Verfügbarkeit von Nachrichten
ITS2 Klausur 2-57 (1 Punkt) Sie haben die folgende Antwort gegeben: Schwache Kollisionsresistenz bedeutet
0
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 $x=x'$
${f C}$ 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
o ein Prüfwert einer Nachricht, der unter Einbezug eines privaten (asymmetrischen) Schlüssels erzeugt wird
O 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
C Locardsches Prinzip
Moore's Law
O 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?
C A authentisiert sich gegenüber B
O A identifiziert sich gegenüber B
C A authentifiziert sich gegenüber B
O 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
C False Rejection Rate
Correct Rejection Rate

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 0 **RFID** ITS2 Klausur 2-65 (1 Punkt) Sie haben die folgende Antwort gegeben:

ITS2 Klausur 2-62 (1 Punkt)

Wofür steht in Deutschland die Vertraulichkeitsstufe VS-NfD?

0

Verschlusssache – Nur für den Dienstgebrauch
O Vertraulich/Secret – Nutzungsstufe für Deutschland
O 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
O Rollen orientieren sich an Organigramm der Institution
O Benutzer werden Rollen zugeordnet
O 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 Sandbox
\textstyle
Isolation
Alarm
ITS2 Klausur 2-67 (2 Punkte)
Cia bahan dia falaanda Antonosta aarahan.
Sie haben die folgende Antwort gegeben:
Was sind Erkennungsmethoden von Antivirensoftware? (Wählen Sie zwei Antworten)
☐ Sandbox & ☐ Verhaltensanalyse &
☐ Isolation ✓ ☐ Alarm ✓

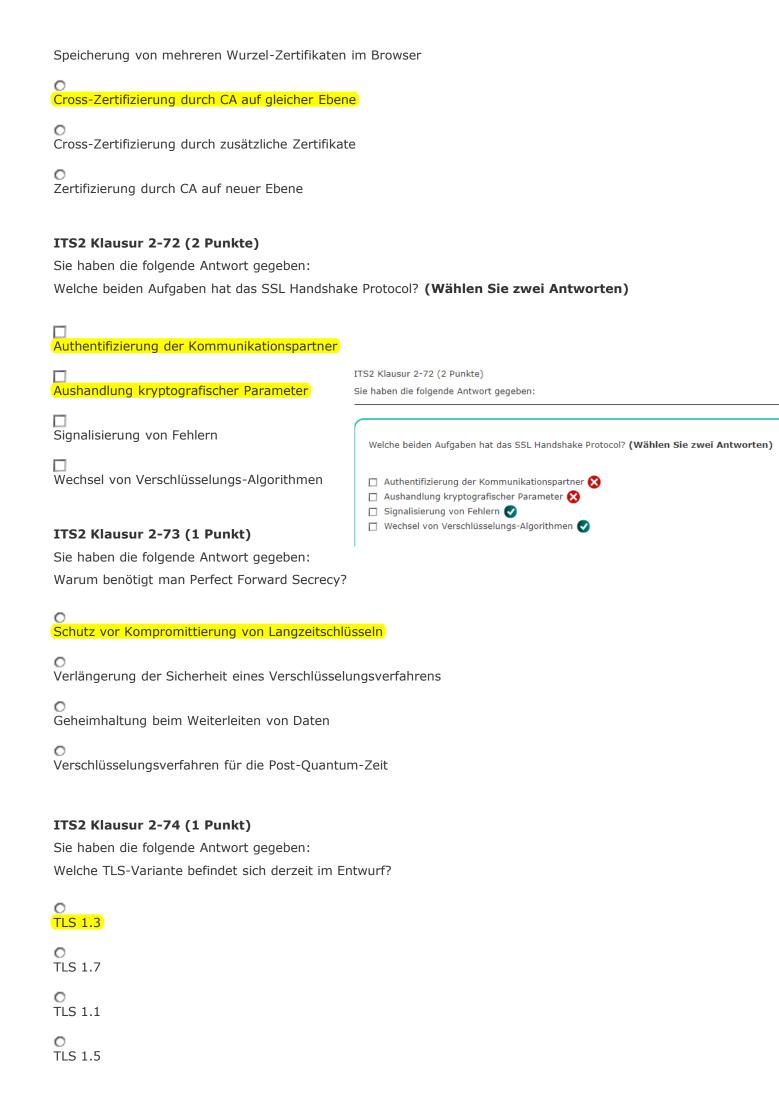
Welche Methode eignet sich nicht zum Entfernen von Malware? Alle Prozesse der Schadsoftware aus dem Arbeitsspeicher entfernen Spezialsoftware zur Entfernung nutzen Rechner manuell nach Anleitung von Spezialisten säubern Re-Installation des Systems mit sauberem Betriebssystem und Anwendungen ITS2 Klausur 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:

ITS2 Klausur 2-68 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was macht ein Trusted List in Bezug auf PKI?

0

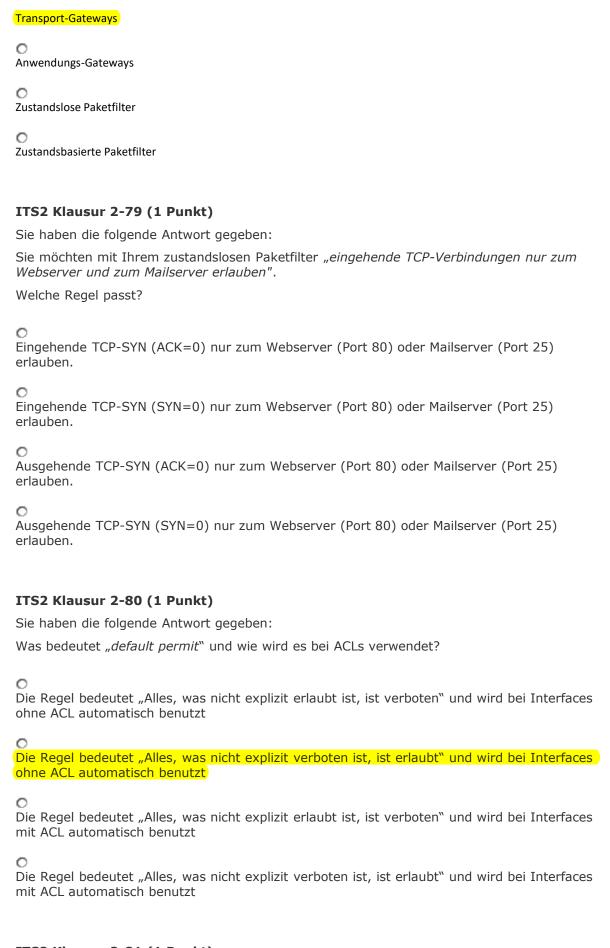


Sie haben die folgende Antwort gegeben: Auf welches Sicherheitsprotokoll baut kein VPN auf? S-MIME O IPSec SSL 0 SSH ITS2 Klausur 2-76 (1 Punkt) Sie haben die folgende Antwort gegeben: Wie nennt man das Verschicken von Daten über eine VPN-Verbindung? C Tunneling Bridging Authenticating Encrypting ITS2 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)

ITS2 Klausur 2-75 (1 Punkt)

Sie haben die folgende Antwort gegeben: Welche Firewall-Technologie gibt es <u>nicht</u>?

0



ITS2 Klausur 2-81 (1 Punkt)

Sie haben die folgende Antwort gegeben:

Was unterscheidet den zustandsbasierten Paketfilter vom zustandslosen?

O Merkt sich den Verbindungsstatus über TCP Flags
O Merkt sich den Verbindungsstatus über ICMP Flags
O Merkt sich den Verbindungsstatus über IP Flags
O Merkt sich den Verbindungsstatus über UDP Flags
ITS2 Klausur 2-82 (1 Punkt)
Sie haben die folgende Antwort gegeben: Was ist das Merkmal einer <i>Screened Host Architecture</i> ?
O Dienste werden als Proxies auf internem Bastion-Host angeboten
O Benutzt eine DMZ
O Benötigt immer zwei Netzwerkkarten
O 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 Antworte
□ Infrastruktur-Modus
□ Ad-Hoc-Modus
WPS-Modus

Autoconnect-Modus

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?



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?



4. ITS PK8 [ID: 448754]

Welche Art von Viren gibt es nicht?



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?

O Lesen der Handbücher

Verwendung von Firewalls

Conletionon

Sanktionen

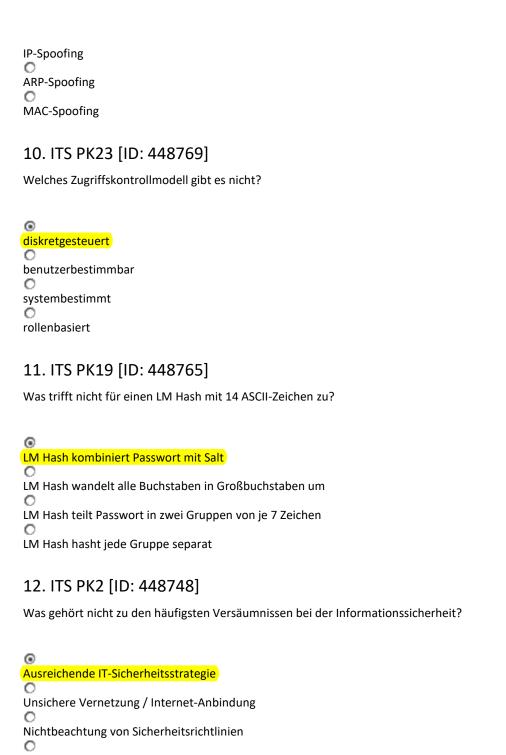
0

Bildschirm in Abwesenheit sperren

9. ITS PK15 [ID: 448761]

Welches Spoofing wurde in der Veranstaltung nicht vorgestellt?

UDP-Spoofing



Schlechte Wartung von IT-Systemen

13. ITS PK13 [ID: 448759]

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



14. ITS PK5 [ID: 448751]

Wann liegt eine Gefährdung vor?

Bedrohung trifft auf Schwachstelle
C
Schwachstelle hat eine positive Eintrittswahrscheinlichkeit
C
Positive Eintrittswahrscheinlichkeit und hohes Schadenspotential fallen zusammen
C
Hohes Schadenspotential für eine Form der Bedrohung

15. ITS PK26 [ID: 448772]

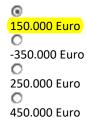
Welches Protocol gibt es in der SSL Protokoll-Architektur?

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).

Wir groß ist der Nutzen pro Jahr?



17. ITS PK17 [ID: 448763]

Angreifer 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(lokaler DNS Server) und meine MAC ist: MAC(E).

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

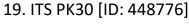
18. ITS PK25 [ID: 448771]

Was macht ein Bridge Trust Center in Bezug auf PKI?

© Cross-Zertifizierung durch CA auf gleicher Ebene C Cross-Zertifizierung durch zusätzliche Zertifikate

Zertifizierung durch CA auf neuer Ebene

Speicherung von mehreren Wurzel-Zertifikaten im Browser

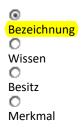


Was ist kein bei WLAN verwendetes Protokoll / Verfahren?



20. ITS PK22 [ID: 448768]

Welches ist kein Faktor zur Authentisierung?



21. ITS PK27 [ID: 448773]

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



22. ITS PK32 [ID: 448778]

Wie wird das Zugriffskontrollmodell Discretionary Access Control oft implementiert?



23. ITS PK10 [ID: 448756]

Welche Verbreitungsart passt nicht zu P2P-Würmern?



Ausführung über Autorun Kopieren in freigegebene Ordner Imitierung von P2P-Protokoll-Antworten 0 Ausnutzung von Schwachstellen des P2P-Netzes 24. ITS PK11 [ID: 448757] Was ist ein Exploit? 0 **Eine Software** Eine Middleware Eine Hardware **Eine Bloatware** 25. ITS PK24 [ID: 448770] Was ist in Bezug auf Softwareschwachstellen entscheidend? 0 Patch Management 0 Firewall-Regeln 0 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?

Fast-Flux Single-Flux

⊚ P2P-Flux

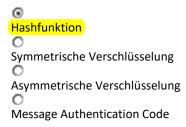
Double-Flux

28. ITS PK28 [ID: 448774]

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

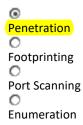
29. ITS PK21 [ID: 448767]

Was ist kein kryptographisches Verfahren?



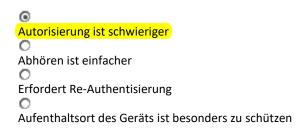
30. ITS PK7 [ID: 448753]

Was gehört zur Phase Attack im typischen Angriffsverlauf?



31. ITS PK31 [ID: 448777]

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



32. ITS PK20 [ID: 448766]

Was ist keine Technik des Social Engineerings?

