Multiple Choice Semestertest SEP / Informatik Sicherheit 2020 Ar

Aus Kurs-DVD Modulen 1-4 und Herdt Buch Netzwerke Sicherheit
Zeit: 45 Minuten

Name: _____
Datum: ***14.08.2020***_____
Klasse: ***TIST5-AR-20S-19051' Informatik-Sicherheit***__

1	Suche für den Begriff in der Spalte A den dazu passenden Begriff in der Spalte B aus.				1
	Spalte A	Antwort	Auswahl	Spalte B	
1.	Hacker		A	Sichere Verbindung auf IP Ebene	
2.	Cracker		B	Asymmetrischer Verschlüsselungs Algorithmus	
3.	RSA		C	Programme welche den Computer zerstören wollen	
4.	AES		D	Symmetrischer Verschlüsselungs Algorithmus	
5.	Wurm		E	Suchen Lücken und melden diese	
6.	Virus		F	Verschlüsselte authentifizierte Verbindung zwischen Client und Server	
7.	SSL		G	Suchen Lücken und nutzen diese	
8.	IPSec		H	Programme welche den Computer als Wirt ausnutzen	

2	Entschlüssle das untenstehende Wort, welches mit der Cäsar-Chiffre symmetrisch verschlüsselt wurde. Schlüssel ist 3.	1

Verschlüsseltes Wort : lqirupdwlnvlfkhukhlw

Entschlüsseltes Wort : ……..

Hilfe: a b c d e f g h i j k l m n o p q r s t u v w x y z

……

3	Welche Begriffe können Sie dem IT Grundschutz nach BSI zuordnen.	1-n
	Versicherungs-Schutz	☐
	Malware-Schutz	☐
	Verbindungs-Schutz	☐
	Datenabfluss-Schutz	☐
	Informations-Schutz	☐
	Kündigungs-Schutz	☐
	Zugriffs-Schutz	☐
	Rechts-Schutz	☐

4	Was verstehen man unter dem Begriff „Wipen“.	1
	Daten nach einem Backup verifizieren	☐
	Daten mehrfach überschreiben und löschen	☐
	Daten nach einem versehentlichen Löschen wieder rekonstruieren	☐

5	Welche 5 Regeln gegen Malware sind empfohen.	5
	Computer immer ausschalten	☐
	Unbekannten Programme misstrauen	☐
	Antispy-Tool installieren	☐
	Computer vernetzen	☐
	Updates einspielen	☐
	Firewall installieren	☐
	Antiviren SW installieren	☐
	Keine Office Programme einsetzen	☐

6	Was versteht man unter MTBF (Mean Time Between Failure).	1
	Wie lange geht es bis ein Fehler auftritt	☐
	Wie lange es dauert bis Fehler behoben ist	☐
	Wie viele Arten von Fehlern aufgetreten sind	☐
	Wie lange ein Ausfall ein System lahmlegt	☐

7	Welche Verschlüsselung-Methode ist ca. 1000 mal schneller.	1
	symmetrisch	☐
	asymmetrisch	☐

8	Beim asymmetrischen Verfahren wird.	2
	Eine Nachricht mit dem Public-Key des Empfängers verschlüsselt	☐
	Eine Nachricht mit dem Public-Key des Empfängers entschlüsselt	☐
	Eine Nachricht mit dem Private-Key des Empfängers verschlüsselt	☐
	Eine Nachricht mit dem Private-Key des Empfängers entschlüsselt	☐

9	Wie können die vier Grundregeln der Informatiksicherheit gewährleistet werden, suche für den Begriff in der Spalte A den dazu passenden Begriff in der Spalte B aus.				1
	Spalte A	Antwort	Auswahl	Spalte B	
1.	Verfügbarkeit		A	Verschlüsselung	
2.	Verfügbarkeit		B	Backup	
3.	Vertraulichkeit		C	Hashing	
4.	Vertraulichkeit		D	Protokollierung	
5.	Integrität		E	RAID	
6.	Integrität		F	Ohne Internet und Netzwerk	
7.	Verbindlichkeit		G	Digitale Signatur	
8.	Verbindlichkeit		H	SSL	

10	Ordnen Sie die Begriffe für die Erstellung eines Sicherheitskonzeptes gemäss Ihrer Ausführungsreihenfolge.		1
	Antwort	Auswahl	
1.		A: Sicherheitsplan	
2.		B: Umsetzungskonzept	
3.		C: Risikoanalyse	
4.		D: Grad der benötigten Sicherheit und des Schutzes definieren	

11	Was sind polymorphe Viren.	1
	Sie nisten sich im Bootsektor ein	☐
	Sie verändern ihr Aussehen nach jeder Infektion	☐
	Sie belegen den Slack Bereich der Cluster	☐

12	Wie muss ein komplexes Passwort (max. Sicherheit) aufgebaut werden. Markiere die **notwendigen** Anforderungen (Ankreuzen).	1-n

	Antwort	Auswahl
1.		8-stellig
2.		4-stellig
3.		20-stellig
4.		Sonderzeichen
5.		Zahlen
6.		Grossbuchstaben
7.		Kleinbuchstaben

13	Was sind Botnetze.	1
	Zusammenschluss von logische gestohlenen Computern	☐
	Vortäuschen von glaubwürdigen Mail Absendern zum Zwecke von Passwortdiebstahl	☐
	Sammlung von Softwaretools, die nach dem Einbruch in einen PC auf dem betroffenen System installiert werden	☐

14	Was ist ein Brute-Force Angriff.	1
	Klartext selber bestimmen, verschlüsseln und versuchen den Schlüssel heauszufinden	☐
	Teile bekannt – Versucht Schlüssel zu erraten	☐
	Systematik, mit „Probieren“ herausfinden	☐

15	Was ist eine digitale Signatur.	1
	Nachricht mit dem RSA Private Key verschlüsseln	☐
	Nachricht mit dem RSA Public Key verschlüsseln	☐
	Nachricht mit dem AES symmetrische verschlüsseln	☐

16	Was ist ein Hash Wert.	1
	Verbindung zwischen symmetrischem und asymmetrischen Verfahren	☐
	Mathematisches Verfahren, das quasi eine Prüfsumme erzeugt	☐
	Bezeichnung für Public Key	☐

17	Zähle 6 ungeplante Bedrohungen → Höhere Gewalt auf.	6
		☐
		☐
		☐
		☐
		☐
		☐

18	Wie bereiten Hacker meistens einen Netzwerk Angriff vor.	1
	Telefonieren dem Opfer und ausspionieren	☐
	Einsatz von Portscanner um die offnen Ports zu erspähen	☐
	Falsches Mail senden um Daten zu sammeln	☐

19	Bei einer „Cipher-text only attack” wird was zu Hilfe genommen.	1
	Häufigkeitsanalyse	☐
	Infos aus Cookies	☐
	Programm zum Durchprobieren von Möglichkeiten	☐

20	Aus welchen 3 Tätigkeiten besteht das „Microsoft Solutions Framework“.	3
	Evaluieren	☐
	Planen	☐
	Verwehren	☐
	Verwalten	☐
	Erstellen	☐

VPF::LockBox 3 RSA - Форум программистов - Vingrad.ru

21	Gegeben ist ein Cryptosytem mit , Gesucht ist der private Key d:	1
	Prime1:= 11; Prime2:= 13;	
	RSA_exponent:= 7;	
	$e \cdot d = 1 \bmod \phi(n)$	
	101	☐
	103	☐
	105	☐
	108	☐

Probiere (Iteriere) nun die Möglichkeit von d 100 – 110 durch [100..110] mit

if (getEPublic * it mod getPHI_N = 1)

Chffriere nun ein Zeichen m

$F(m,d) = m\hat{}d \bmod n$

22	Berechne das ungefähre Risiko von	5
	Harddisk Crash	☐
	Datendefekt	☐
	Ransomware	☐
	Password Fishing	☐
	Smart Card defeklt	☐