Gedächtnisprotokoll

Rechnersicherheit WS 16/17

16 Seiten - eventuell habe ich Fragen vergessen. Der Umfang ist aber schon sehr nah an dem der Klausur. Die Fragen geben nicht den genauen Wortlaut wieder. Entsprechen aber generell dem Sinn der Frage. Die angegebenen Punkte sind teils erinnert, teils geschätzt.
Für die Klausur gab es 120 Minuten Zeit.

8 Fragen MC. Richtige Antworten geben 1 Punkt. Bei Falschen wird 1 Punkt abgezogen. Bei keiner Antwort gibt es 0 Punkte. Insgesamt können nicht weniger 0 Punkte erreicht werden.

Frage	**Wahr**	**Falsch**
Fuzzing ist eine Schutzmaßnahme bei der zufällig Speicheraddressen berechnet werden.		
Die Same-Origin-Policy besagt, dass der Browser nur JavaScript Code vom Server des Browserherstellers laden darf.		
Social Engineering nutzt Schwachstellen in der zwischenmenschlichen Kommunikation aus.		
Bei Passwörtern ohne Salz haben zwei identische Passwörter auch den selben Hash.		
Ein RAID-System kann gegen Vieren und Fehleingaben schützen.		
Das Kerkhoff'sche Prinzip besagt, das bei der Prüfung von kryptographischen Algorithmen davon ausgegangen werden soll, dass der Angreifer den Algorithmus kennt.		
Kann mich nicht erinnern		
Kann mich nicht erinnern		

(5 Punkte)

Social Engineering

Was unterscheidet "Spearphishing" von "Phishing". Welche Konsequenzen ergeben sich daraus für die angegriffene Person und die technischen Schutzmaßnahmen.

Nennen Sie die 3 Bereiche in denen Maßnahmen gegen Social Engineering erfolgen müssen.

(4 Punkte)
Authentisierung
Nennen Sie die 4 grundlegenden Möglichkeiten eine Person zu authentisieren.

(4 Punkte)

Backup

Unterscheiden Sie Differentielles und Inkrementelles Backup und nennen Sie jeweils Vor- und Nachteile der Verfahren.

(4 Punkte)
Zertifikate
Beschreiben Sie die unterschiedlichen Vorgehensweisen bei Sperrlisten und beim OCSP-Protokoll. Benennen sie jeweils Vor- und Nachteile.

(5 Punkte)
Buffer-Overflow
Beschreiben Sie was beim Buffer-Overflow passiert.

Nennen sie zwei Sicherheitsfehler, die dadurch verursacht werden können.

(3 Punkte)
Entwurf sicherer Systeme
Nennen sie 3 der acht Prinzipien zum Entwurf sicherer Systeme.

(4 Punkte)

IT-Grundschutz Schutzbedarfstabelle

Vervollständigen Sie die folgende ~~Kritikalitätsmatrix~~ für den IT-Grundschutz bezüglich der Sicherheitsziele. Kummulations- und Verteilungs-Effekt sollen dabei **nicht** berücksichtigt werden.

ID	**System**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	
A1	Personaldaten	sehr hoch	hoch	normal	
A2	Planungsdaten	normal	normal	hoch	
A3	Kalender	normal	normal	normal	
S1	Applikationsserver				Hier laufen A1 und A2
S2	Webserver				Nur A3
S3	Datenbankserver				Hier greifen alle Applikationen drauf zu.
S4	Switch				Verbindet alle Server
R1	Serverraum A				Hier stehen alle Server außer A3
R2	Serverraum B				Hier stehen alle anderen Netzwerkkomponenten
G1	Hauptgebäude				Hier befinden sich beide Serverräume

(4 Punkte)
HRU-Modell
Gegeben sind die folgenden 3 Kommandos

```
create_file (s,f) {
     createfile (f)
     create(s,"r", f)
     create(s, "w", f)
     create(s, "own", f)
}

owner_confer(s1, s2, f, p) {
     if( (s1, "own", f) e ZR AND p!="own")
     then create(s2, p, f)
}

non_owner_confer(s1, s2, f, p) {
     if( (s1, p, f) e ZR AND p!="own")
     then create(s2, p, f)
}
```

Gegeben ist die folgende Zugriffsmatrix:

	f1	f2	f3	f4
s1	"r", "w"		"r","w","own"	
s2	"r"	"r"	"w"	"r","w","own"
s3		"r"		

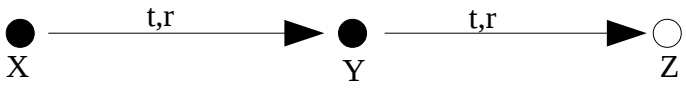
Geben Sie einen sicheren und eine unsicheren Zustand an bzgl. der gegebenen ZR. Begründen Sie, warum der jeweilige Zustand sicher bzw. unsicher ist

sicher (, ,)

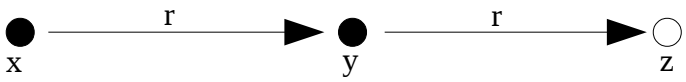
unsicher (, ,)

(4 Punkte)
Take-Grand-Model

Zeigen Sie durch Graphentransformation, wie x de-jure Lesezugriff auf Z erhalten kann. Geben Sie dabei jede notwendige Operation an.



Kann X de-facto Lesezugriff auf Z erhalten? Falls ja, beschreiben Sie wie und wie die entsprechenden Operationen heißen.



(5 Punkte)
RSA
Sie haben einen Privaten Schlüssel (3,33) und eine Öffentlichen (7,33).

a) Geben Sie an welches die maximale Blocklänge k ist. Begründen Sie Ihre Antwort.

b) Signieren Sie die Zahl 3.

(4 Punkte)

Hash-Funktionen

Ist f(x) = x mod 128 eine gute Hashfunktion? Diskutieren sie dabei alle wesentlichen Eigenschaften einer Hashfunktion.

(2 Punkte)
Sicherheitsziele
Geben Sie an welches der drei grundlegenden Sicherheitsziele in den folgenden Szenarien hauptsächlich verletzt wurde.

a) Durch den Ausfall der Klimaanlage in ihrem Serverraum muss das gesamte System heruntergefahren werden.

b) Auf Ihrem System wurde Schadsoftware gefunden. Allerdings lässt sich die genau Herkunft nicht rekonstruieren, da Zeitstempel auf dem System manipuliert wurden und somit der Ablauf der Verbindung zwischen den ihren verschiedenen Rechnern nicht mehr nachvollziehbar ist.

(4 Punkte)
Firewall
Entscheiden Sie, ob eine Paket-filter Firewall in den folgenden Szenarien ausreicht um das Ziel zu erreichen. Begründen Sie Ihre Entscheidung. Gehen Sie dabei auf die entsprechenden Filter der Firewall ein.

a) Verbindungen sollen nur von einer Seite der Firewall initialisiert werden können.

B) Verbindungen per SMTP sollen auf alle Server möglich sein.

(3 Punkte)

IT-Forensik

Sie bekommen Hinweis, dass auf ihrem Webserver ein Command and Control Server für Krypto-Trojaner läuft. Welche Vorgehensweise wählen Sie - Live-Response oder Post-Mortem. Welche Vorteile ergeben sich daraus?