[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Wintersemester 2015/16, Montag, 01.02.2016, 14:00 Uhr

Name:_____ Punkte:_____/100 (40 zum Bestehen) Note:____

Disclaimer:
- Zugelassene Hilfsmittel: keine ausser Stifte und Lineal
- Der Lösungsweg muss bei allen Aufgaben ersichtlich sein
- Ähnlichkeiten mit realen Institutionen sind rein zufällig und nicht beabsichtigt

Aufgabe 1: Begriffswelt

__/10 __/10 Punkte

Für den nächsten Star Wors™ Film, den Sie produzieren wollen, benötigen Sie für die Spezialeffekte mannigfaltige IT Infrastruktur. Dann können Sie bestimmt auch die folgenden Begriffe leicht kurz erklären:

ARP, DNS, Asymmetrische Redundanz, Insel, Stealth Scanner, ARP-Spoofing, Proxy, Zuverlässigkeit, Buffer Overflow, Vertraulichkeit

Aufgabe 2: Safety

A)__/6 B)__/9 C)__/9 D)__/2+4+2+3+2 __/37 Punkte

A) Der Produzent Ihres Filmes verwechselt Safety und Security sehr häufig, helfen Sie ihm, indem Sie in der folgenden Tabelle ankreuzen welche Themen eher mit Safety und welche eher mit Security zu tun haben:

Thema	Safety	Security
Höhere Gewalt		
Sniffing		
Malware		
Hardware-Defekt		
DDoS		

B) Kreuzen Sie ihm bitte nun noch jeweils an, welche Methoden beim Erreichen welcher Schutzziele sinnvoll sind:

	Redundanz	„Firewall“++	Kryptographie	Policies
Verfügbarkeit				
Integrität				
Vertraulichkeit				
Zurechenbarkeit				
Rechtsverbindlichkeit				

C) Für die Netzwerkanbindung Ihrer Renderingfarm stehen drei getrennte Uplinks zur Verfügung, jeder davon hat eine Verfügbarkeit von 80%. Damit die Uplinks funktionieren, müssen die Endgeräte mit Strom versorgt werden: die Stromversorgung hat eine Verfügbarkeit von 50%. Wie hoch ist die Verfügbarkeit der Netzwerkanbindung?

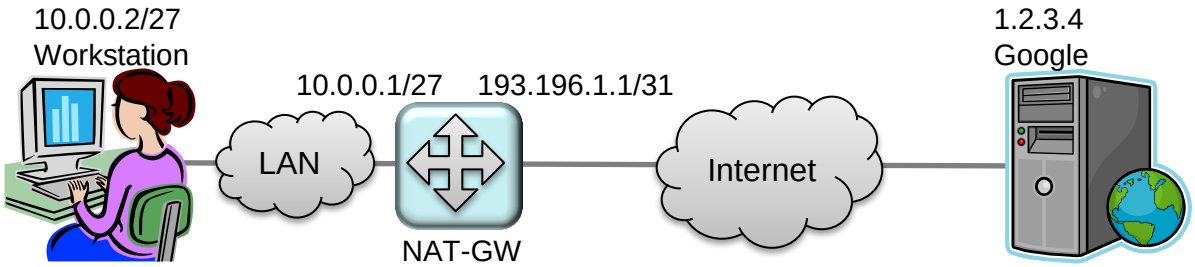
D) Auch bei den Systemen auf denen letztlich die Tricks in Ihrem neuen Film gerendert werden spielt Redundanz eine Rolle, jedoch erlaubt die Lizenz der Rendering-Software immer nur einen aktiven Haupt-Server. Daher haben Sie sich für eine einfache 1:1 Redundanz mit einem aktiven und einem passiven System entschlossen.

1. Auf welchen Ebenen könnten Sie ein Takeover zwischen dem aktiven und dem passiven System durchführen?
2. In welchen Eigenschaften unterscheiden sich diese Ebenen zur Service-Übernahme? Stellen Sie strukturiert Vor- und Nachteile gegenüber!
3. Welche Rolle hat dabei der Heartbeat?
4. Welche Methoden, so einen Heartbeat zu implementieren fallen Ihnen ein?
5. Was versteht man unter einer „Split Brain“ Situation?

Aufgabe 3: Security

A)__/6 B)__/6 C)__/7 D)__/10 E)__/10 F)__/8 G)__/6 __/53 Punkte

A) Bei der Anbindung Ihrer Rendering-Farm verwenden Sie unter anderem NAT mit folgendem Setup:



Die Workstation soll zu Google zwei HTTP-Verbindungen aufmachen. Füllen Sie die folgende Masquerading-Tabelle mit den dann vorzufindenen Inhalten:

SRC IP	SRC PORT	NAT IP	NAT PORT	DST IP	DST PORT

B) Als Film-Produzent von Star Wors™ haben Sie natürlich auch stets ein Auge auf Piraten, die Ihre wertvollen Inhalte stehlen möchten. Da kann es schon mal vorkommen, dass Sie zurückschlagen müssen und Informationen über einen Angreifer herausfinden müssen. Schreiben Sie hierzu in Pseudocode zunächst einen einfachen Port-Scanner!

C) Nun müssen Sie aber auch überwachen, wann, von woher und wie Sie angegriffen werden – dazu dient Ihnen erweiterte Loganalyse als Intrusion Detection. Beschreiben Sie Ihren Setup, am besten anhand eines kleinen Übersichtsbildes!

D) Manche Angreifer sitzen auch auf der Leitung, dann kommt es zu ARP-Spoofing. Welche Schritte sind hier nacheinander erforderlich, um erfolgreich per ARP-Spoofing als Angreifer Verkehr mitschneiden zu können?

E) Sehr viele genervte Angreifer möchten auch einfach nur ihren Betrieb stören, da ihnen der drittletzte Film (darin machten Sie sich ausführlich über Nerds lustig) nicht gefallen hat. In diesem Fall kann es zu DDoS Angriffen kommen. Sie haben sich ausführlich mit dem Thema befasst: welche Phasen und Vorgänge gibt es im Allgemeinen, wenn eine Infrastruktur für DDoS durch Angreifer geschaffen und dann erstmalig genutzt werden soll?

F) Die Ursache vieler Sicherheitsprobleme auch in Ihrer Produktionsfirma sind Buffer Overflows. Welche Abhilfen (oder Ansätze von Abhilfen) gibt es gegen Buffer Overflows?

G) Bei der Ausnutzung solcher Buffer Overflows werden oft NOP-Rutschen verwendet. Zu welchem Zweck? Wie lange sollte so eine NOP-Rutsche sein?