[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Wintersemester 2017/18, Mittwoch, 14.02.2018

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

Disclaimer:
- Zugelassene Hilfsmittel: keine ausser Stifte und Lineal
- Der Lösungsweg muss bei allen Aufgaben ersichtlich sein

Aufgabe 1: Begriffswelt

__/10 __/10 Punkte

Ihr Unternehmen Parná ist aktiver Cloud Provider. Wie viele andere kämpft es zur Zeit gegen die berühmte „Schmelzwasser“ Sicherheitslücke. Vor diesem Hintergrund ist Ihr Know-How gefragt.

Erklären Sie kurz folgende 10 Begriffe aus der IT Security Vorlesung:
DDoS, Zuverlässigkeit, Spoofing, Bastion, IT Grundschutz, Tunnel, XSS, Honeypot, statische Redundanz, NOP Rutsche

Aufgabe 2: Safety

A)__/ 10 B)__/10 C)__/10 D)__/10 __/40 Punkte

A) Um immun gegen die „Schmelzwasser“ Attacke zu sein benötigen Sie ein BIOS Update (hilft nur in 80% der Fälle) oder ein Betriebssystem-Update (hilft nur in 60% der Fälle), aber diese beiden Updates sind generell nur bei Systemen die neuer sind als 2015 (50% Ihrer Systeme) möglich. Welche „Schmelzwasser“-Anfälligkeitswahrscheinlichkeit hat Ihr Unternehmen?

B) An welchem Rahmenparameter aus A) (BIOS, OS, Systemalter) wäre es am lohnenswertesten, 10% besser zu sein, um insgesamt die geringste Anfälligkeit zu erreichen? Begründen Sie Ihre Antwort!

C) Die IT-Security ist auf dem Prüfstand. Welche Schutzziele kennen Sie? Welche (mindestens 3) sind davon für Sie als Cloud Provider relevant? Begründen Sie Ihre Wahl! Mit welchen Maßnahmen erreichen Sie die von Ihnen als relevant erkannten Ziele. Beantworten Sie die Frage strukturiert!

D) Ihr Chef bekommt bei der Bewertung der Schmelzwasser Lücke einige Themen durcheinander. Erklären Sie ihm den Unterschied zwischen Zuverlässigkeit und Verfügbarkeit.
Ist für Sie als Cloud-Anbieter eher Verfügbarkeit oder Zuverlässigkeit wichtig?
Mit welcher Art von Redundanz erreichen Sie dies?
Hätte dies auch gegen die „Schmelzwasser“ Attacke geholfen?

Aufgabe 3: Security

A)__/8 B)__/8 C)__/10 D)__/8 E)__/10 F)__/6 __/50 Punkte

A) Sie sollen den Kunden Ihres Cloud Providers helfen ihre gekauften IoT Devices sicherer zu betreiben.
Schreiben Sie für die Kunden eine FAQ mit mindestens 4 Punkten und kurzer Erläuterung.

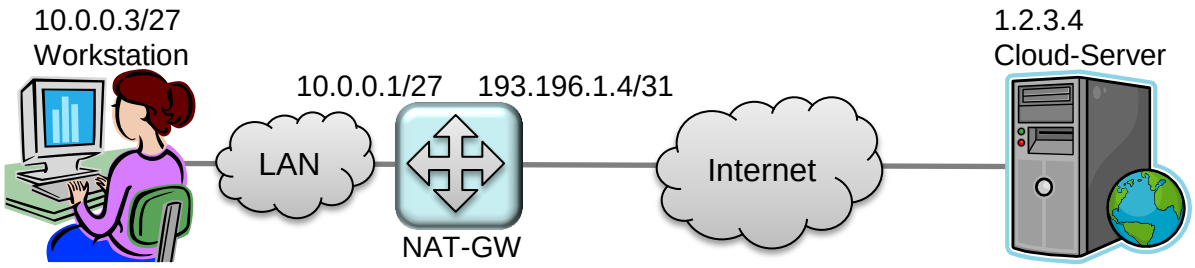
B) Neben „Schmelzwasser“ sind Sie auch noch Ziel einer DDoS Attacke geworden. Wie können Sie sich davor schützen?

C) Die Sicherheits-Awareness ist aktuell besonders groß - erklären Sie Ihrem Chef anhand einer Stack-Skizze wie ein Buffer Overflow funktioniert. Mit welchen Maßnahmen lassen sich Buffer Overflows vermeiden?

D) Damit Ihre Mitarbeiter über das Internet an der Lösung der „Schmelzwasser“ Problematik mitarbeiten können, sollen deren Laptops mit Ihrer Zentrale verbunden werden.
1) Skizzieren Sie den Aufbau des Netzes am Internet-Anschluss Ihres Cloud-Providers mit den Bausteinen aus der Vorlesung
2) Welche Richtlinien definieren Sie für die Laptops und deren Benutzung?

E) Sie wollen die Sicherheit Ihrer Cloud-Server überprüfen. Schreiben Sie in Pseudocode einen Port Scanner, welcher die gefundenen Informationen mit einer Vulnerability DB abgleicht und im Falle einer Sicherheitslücke einen Alarm triggert.

F) Bei der Anbindung der Arbeitsplätze in Ihrer Entwicklungsabteilung an die Cloud-Server verwenden Sie unter anderem NAT mit folgendem Setup:



Die Workstation soll zum Cloud-server zwei HTTPS-Verbindungen aufmachen. Füllen Sie die folgende NAT-Tabelle des NAT-GW mit den dann vorzufindenden Inhalten:

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