[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Sommersemester 2020, Mittwoch, 22.07.2020, 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

Aufgabe 1: Begriffswelt

__/10 __/10 Punkte

Sie haben erkannt, dass es in unserer Zeit wichtig ist, auch per digitaler Videokonferenz kommunizieren zu können und planen, den neuen Dienst „Boom“ an den Start zu bringen, um die Menschen einander näher zu bringen.

Dazu ist natürlich einiges an Security-Wissen erforderlich, schreiben Sie zunächst ein Glossar mit kurzen Erklärungen für die folgenden Begriffe aus dem Themenbereich:

Insel, NOP-Rutsche, USV, Rechtsverbindlichkeit, Stateful Inspection, Threat Model, Wurm, XSRF, ISO 27001, Shell Code

Aufgabe 2: Safety

A)__/8 B)__/8 C)__/6 D)__/8 __/30 Punkte

A) Der Chefentwickler der Videoconferencing-Lösung stellt Ungereimtheiten im Lastenheft fest. Safety und Security werden darin synonym verwendet. Erklären Sie weshalb das nicht korrekt ist. Nennen Sie jeweils 2 Beispiele für Security- sowie Safetymaßnahmen. Müsste es bei den Anforderungen zu Ihrem „Boom“ Dienst eher um Safety oder Security gehen? Begründen Sie Ihre Wahl!

B) Um auch wirklich sicher zu gehen, dass die Audio- und Videoströme beim Nutzer ankommen, bauen Sie redundante Cloud-Infrastrukturen in Europa, Asien und den USA auf. Mindestens eine davon muss funktionieren, damit die Menschen kommunizieren können. Jede Cloud-Infrastruktur hat eine Ausfallwahrscheinlichkeit von 50%. Außerdem darf kein Hacker-Angriff passieren, falls ein Hacker-Angriff passiert, zerstört er alle drei – die Wahrscheinlichkeit dass ein Hacker Erfolg hat ist 80%.
Wie groß ist die Verfügbarkeit Ihres weltumspannenden Videokonferenzsystems?

C) Welche Verfügbarkeit hätte Ihre Systemlandschaft wenn eine weitere redundante „Boom“ Infrastruktur in Australien aufgebaut würde?

D) Welches bzw. welche Schutzziel(e) werden mit der Umsetzung der untenstehenden Maßnahmen jeweils verfolgt (Hinweis: lässt sich gut in einer Tabelle darstellen)?
Verschlüsselung, 4-Augen Prinzip, RAID, Australisches RZ, Paketfilter, Archivsystem, Zugangskontrolle zum RZ, Digitale Signatur

Aufgabe 3: Security

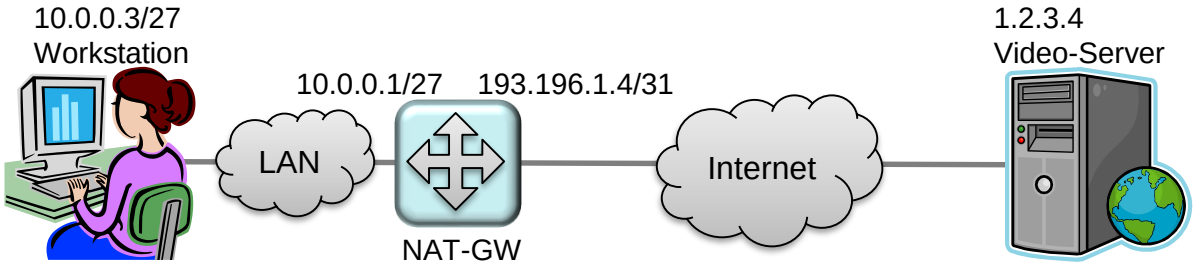
A)__/5 B)__/5 C)__/5 D)__/5 E)__/5 F)__/7 G)__/6 H)__/9 I)__/8 J)__/5 __/60 Punkte

A) Software, die für das Videokonferenzsystem notwendig ist, entsteht in einem Entwicklungsprozess den man in verschiede Phasen unterteilen kann. Ordnen sie die SSDLC Aktivitäten der richtigen Phase zu:

Anforderungsphase	Fuzzing Tests
Entwurfsphase	Bedrohungsmodellierung
Entwicklungsphase	Reaktionsplan
Überprüfungsphase	Risikobewertung
Deploymentphase	Statische Code Analyse

B) Neben technischen Maßnahmen sind auch Regeln ein wichtiger Mechanismus, um Security zu stärken. Entwerfen Sie eine Policy (min. 5 Regeln) für Admins, die zu Wartungsarbeiten in Ihr RZ müssen.

C) Bei der Anbindung Ihrer Entwicklungsclients verwenden Sie unter anderem NAT mit folgendem Setup:



Die Workstation soll zum Video-Server zwei HTTPS-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

D) Weshalb gilt NAT (neben dem Einsparen von „echten“ IP Adressen) auch als Sicherheitsmaßnahme? Welche Problematik haben Ihre „Boom“ Clients zu lösen falls sie hinter einem NAT Gateway installiert werden?

E) Welche Gefahr besteht in folgendem Code-Fragment, und warum?

```
SavePasswords(char *pNewPwd)
{
    unsigned int counter;
    char p4PSN[11];
    int cboom, cbam, cbim = 32;
    strcpy(p4PSN, pNewPwd);
    /* TODO: pwd mit salt versehen */
}
```

F) Beschreiben Sie das Stack-Layout direkt nach dem Aufruf von `SavePasswords`!

G) Beim Ausnutzen von Buffer Overflows kommt Shellcode zur Anwendung. Welche typischen Eigenschaften und Grenzen hat Shellcode?

H) Es ist essentiell, bei den öffentlichen Schnittstellen zur Übertragung der Chat-Inhalte Ihres Videokonferenzsystems Maßnahmen gegen Exploits in Form von Buffer Overflows zu ergreifen.
Warum sind eigentlich Interpreter und auf Bytecode-Interpretation basierende Sprachen keine allgemeingültige Abhilfe gegen Sicherheitslücken in Form von Buffer Overflows?
Was können die Hersteller von Interpretern und Bytecode-Interpretern tun um Buffer Overflows zu vermeiden?

I) Zwei große Unternehmen möchten Ihr neues Produkt stören, indem sie DDoS Attacken auf die Videokonferenz-Server abfeuern. Nennen und erklären Sie kurz möglichst viele Gegenmaßnahmen die ergriffen werden könnten.

J) Ein Sicherheitforscher weist Sie darauf hin, dass Ihr „Boom“ Client anfällig für UNC Path Injection (z.B. \\?\C:\Windows\SYSTEM32\calc.exe) in der Chat Funktion ist. Welches Sicherheitsprinzip hat Ihr Entwickler nicht beachtet?