[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Sommersemester 2016, Montag, 04.07.2016, 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

Sie bereiten ein Referendum (Volksabstimmung) im Internet unter den Einwohnern von Molwanien bzgl. des Ausstiegs aus der KATO (Kommunik Antlantisk Tritisk Organisationisk) vor. IT-Sicherheit spielt dabei eine sehr große Rolle, und damit alle Mitarbeiter die selbe Sprache sprechen erklären Sie ihnen bitte kurz folgende Begriffe aus der IT-Security:

Shellcode, NOP-Rutsche, Asymmetrische Redundanz, VPN, ARP-Spoofing, XSRF, Verfügbarkeit, USV, Vertraulichkeit, Policy

Aufgabe 2: Safety

A)__/6 B)__/8 C)__/8 D)__/7 __/29 Punkte

A) Für Ihr Online-Referendum ist die Rechtssicherheit eine wichtige Voraussetzung. Wie können Sie die Konformität Ihrer Umsetzung gegenüber gesetzlichen Anforderungen belegen?

B) Auch die Risikobetrachtung ist zentral für Molwanien und die KATO. Kreuzen Sie ihm bitte an, welche Maßnahmen beim Erreichen welcher Schutzziele sinnvoll sind:

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

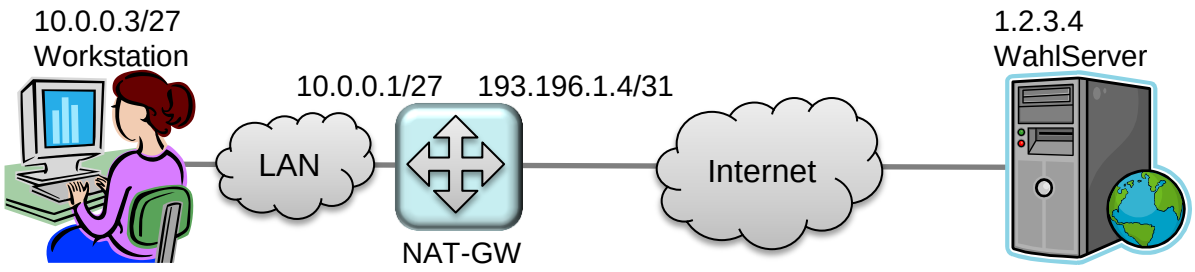
C) Die Abstimmungsberechtigten im Molwanien können auch per Briefwahl (90% verfügbar, in manchen Fällen geht‘s auch schief), per persönlicher Präsenz in Wahllokalen (70% verfügbar) und nun eben per Internet (30% verfügbar) teilnehmen. Wie groß ist somit die Gesamt-Verfügbarkeit von Abstimmungsverfahren für das Referendum?

D) Das Risiko, dass ein Abstimmungsbüro gekapert wird beträgt 5%. Zur Absicherung gegen solchen Missbrauch setzen Sie 10000 Molwanische Pfund(₰) ein. Sollte ein Abstimmungsbüro hintergangen werden, entsteht ein Schaden von 400000 ₰. Lohnt sich die Absicherung, oder geben Sie zu viele ₰ dafür aus?

Aufgabe 3: Security

A)__/7 B)__/7 C)__/12 D)__/5 E)__/8 F)__/8 G)__/6 H)__/8 __/61 Punkte

A) Bei der Anbindung Ihrer Clients in Abstimmungsbüros verwenden Sie unter anderem NAT mit folgendem Setup:



Die Workstation soll zum Wahlserver 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

B) Ergänzend zu NAT im Abstimmungsbüro benötigen Sie auch Firewallregeln vor dem Wahlserver. Verbessern Sie den folgenden Regelsatz für eingehende Verbindungen (Nehmen Sie sich bitte gestalterische Freiheiten):

```
DROP TCP 25
DROP UDP 53
ALLOW TCP 80
```

C) Ein kritisches Element zur Absicherung gegen Spoofing sind die Identitätsabbildungsebenen mit Protokollen wie ARP oder DNS, sowie Session Management auf den höheren OSI-Layern.
Welche Gefahren für ein politisches Online-Instrument wie das des Molwanien-Referendums entstehen durch Spoofing?
Welche Schutzmechanismen helfen gegen Spoofing auf den höheren OSI-Layern?
Um die Gefahr von klassischem Spoofing zu illustrieren, formulieren Sie bitte in Pseudo-Code den Ablauf einer ARP-Spoofing-Attacke aus Angreifer-Sicht!

D) 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 */
}
```

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

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

G) Es ist essentiell, bei den öffentlichen Schnittstellen der Abstimmungsdatenübertragung 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?

H) Eine radikale Gruppierung möchte das Referendum erschweren indem sie DDoS Attacken auf die Wahlserver fährt. Nennen und erklären Sie kurz möglichst viele Gegenmaßnahmen die ergriffen werden könnten.