Musterlösungen zur
Hauptklausur
Kurs 01867 „Sicherheit im Internet II“

vom 23.09.2006

Aufgabe 1 (12P)

2P
Welche zwei Datenbanken/ Tabellen verwaltet ein DNS-Server?

- Forward Zone.
- Reverse Zone.

2P
Welche Funktion erfüllen diese Datenbanken?

- Forward Zone: Abbildung von Namen auf IP-Adressen.
- Reverse Zone: Abbildung von IP-Adressen auf Namen.

2P
Was versteht man unter Spoofing und was ist DNS-Spoofing?

- Spoofing: ist ein Maskierungsangriff, das Vortäuschen einer falschen Identität.
- DNS-Spoofing: Manipulation der Forward oder Reverse Zone.

2P
Was passiert bei einem IP—spoofing, wenn IP-Adressen mit DHCP vergeben werden?

ARP-Pakete gehen an alle angeschlossenen Geräte.
Auf eine ARP-Anfrage wird vom Angreifer eine gefälschte ARP-Antwort oder eine gefälschte ARP-Nachricht geschickt.

2P
Beschreiben Sie kurz die lineare Kryptoanalyse!

Man versucht lineare Ausdrücke aus den Bits R(i) des Klartextes und Y(i) des Geheimtextes der Form $R(i,1)\oplus\ldots\oplus R(i,n)\oplus Y(j,1)\oplus\ldots\oplus Y(j,m)=0$ zu konstruieren. Wenn die Wahrscheinlichkeit für diesen Ausdruck wahr zu werden von ½ deutlich abweicht, lässt dies Rückschlüsse auf den Schlüssel zu.

1P
Lineare Kryptoanalyse ist ein known-plaintext-Angriff, um welche Art des Angriffs handelt es sich bei differenzieller Kryptoanalyse?

Chosen plaintext.

1P
Welche Zustände kann das Q-Bit bei Quantencomputern annehmen?

0, 1 und einen Überlagerungszustand.

Aufgabe 2 (18P)

2P
Welche Güterarten werden bei e-commerce unterschieden? Nennen Sie Beispiele!

- Materielle Güter: Bücher, Fernseher, Herd, Waschmaschine,…
- Immaterielle Güter: Musik, Filme, Nachrichten, Software in digitaler Form…

Daneben gibt es noch eine Unterscheindung von Gütern hinsichtlich ihres Wertes.

2P
Bei Bezahlung mit Kreditkarte durch einen Angreifer entsteht bei Widerspruch des rechtmäßigen Inhabers der Kreditkarte ein Schaden. Wie versuchen Kreditkartenfirmen diesen Schaden zu minimieren?

- Ein Händler der Kreditkartenzahlungen ohne Vorlegen der Karte akzeptieren will, muss einen MOTO (Mail Order/ Telephone Order)-Vertrag mit der Kreditkartenfirma schließen.
- Weitere Kartenprüfnummern. Auf der Rückseite der Karte befindet sich eine zusätzliche Prüfziffer aus 3-4 Stellen

1P
Was ist double spending?

Die Erstellung beliebig vieler Kopien digitalen Geldes.

4P
Um eine digitale Münze zu verändern, so dass man nach einer digitalen Signatur die Veränderung wieder rückgängig machen kann, ohne die Signatur zu zerstören, wählt der Kunde eine Zufallszahl z und sendet der Bank die unsignierte Münze UM (M Datensatz der Münze, K_p public $UM=M \cdot z^{K_p} \bmod n$ **. key, K_g private key, n der zu den Schlüsseln gehörende Modulus).**

Die Bank erstellt die digitale Signatur $SM=UM^{K_g} \bmod n$ **.**
Wie kann der Kunde nun die Münze M der Bank signieren?

Der Kunde berechnet SM/z mod n.

1P
Was macht ein Rewebber/ wie arbeitet dieser?

Der Rewebber anonymisiert die Zugriffe des Clients beim Surfen durch entfernen aller Informationen aus dem http-request.

5P
Wie ist es möglich, die vom Client angewählten Webseiten trotz eingesetztem Rewebber ohne direkten Zugriff auf den Anonymisierungs-Host und den Client nachzuvollziehen?

Alle http-Anfragen des Clients gelangen personalisiert bis zum Rewebber-Host. Alle bis zum Rewebber-Host besuchten Hosts erhalten ebenfalls diese Anfragen (was man leicht mit tracteroute/ tracert nachvollziehen kann). Mit einem Werkzeug wie „Etherreal“ kann der Netzwerkverkehr über diese Hosts abgehört werden, woraus man den http-request rekonstruieren kann.

3P

Worauf muss beim Aufsetzen eines Rewebber-Host geachtet werden?

Da alle Pakete über den Rewebber laufen (auch Downloads!), muss dieser mit einer sehr guten Netzwerkanbindung versehen sein. Dies gilt ebenfalls für die auf dem Weg zum Rewebber passierten Hosts. Bei JAP sieht man, dass jeder der angegebenen Rewebber-Hosts den Durchsatz deutlich senkt.
Der Rewebber muss sehr gut gegen Angriffe geschützt sein (ähnlich DNS-Server). Erfolgreiche Angriffe auf den Rewebber machen das gesamte System unbrauchbar, da alle Pakete wieder personalisiert werden können.

Aufgabe 3 (20P)

1P

Was macht ein VPN?

Es sorgt für die sichere Kommunikation zweier oder mehr räumlich getrennter lokaler Netze.

4P

Wie funktioniert CHAP?

1) der Benutzer gibt seine Kennung ein.
2) Vom Server wird die Kennung geprüft, indem er eine Zufallszahl (Challenge) generiert und an den Client sendet.
3) Der Client fügt nun Kennung, Passwort und Challenge aneinander, berechnet den Hashwert dieses Strings und schickt diesen an den Server.
4) Der Server berechnet, da er Kennung, Passwort und Challenge kennt ebenfalls den Hashwert und vergleicht diesen mit dem des Clients.

1P

Was stellt CHAP sicher?

Die Identität des Clients.

3P

Ordnen Sie die folgenden Protokolle Layer 2/ Layer 3 zu!

Protokoll	Layer
PPP	
CHAP	
IPSec	
PAP	
PPTP	
L2TP	

Protokoll	Layer
PPP	2
CHAP	2
IPSec	3
PAP	2
PPTP	2
L2TP	2

2P

Welche Übertragungsmodi bei IPSec gibt es?

Transport- und Tunnelmodus. Diese können auch kombiniert werden.

4P

Wie funktioniert die Verschlüsselung bei IPSec, wenn Authentification Header und anschließend Encapsulation Security Payload (ESP) eingesetzt werden? Schildern Sie die Veränderungen im IP-Header und in der IP-Nutzlast und ob symmetisch oder asymmetrisch verschlüsselt wird.

1) der IP-Header bleibt im Wesentlichen unverändert.
2) Aus dem TCP-Header wird ein MAC berechnet und als Authentification Header (AH) in das IP-Paket eingefügt.
3) Das entstandene IP-Paket wird nun symmetrisch verschlüsselt.
4) Ein ESP-Header/ Trailer an den Anfang/Ende des verschlüsselten Teils des IP-Pakets gepackt.

1P

Was leistet ein Intrusion Detection System (IDS)?

Es unterstützt den Systemadministrator bei der Erkennung von Angriffen durch Meldung von Anomalien.

3P

Ein findiger Hacker hat sich Administrationsrechte auf einem Rechner innerhalb eines Subnetzes verschafft und hört z.B. mit Etherreal den Netzwerkverkehr ab. Leider sieht er nur den Datenverkehr den gehackten Rechner betreffend und Broadcasts. In welcher Art von Netzwerk befindet sich der Rechner?

Der Rechner befindet sich in einem Switched Network.

1P

Warum würde man ein IDS vor der Firewall eines Netzwerkes platzieren wollen?

Um gelungene Angriffe besser protokollieren/ analysieren zu können.

Aufgabe 4 (24P)

6P

Nennen Sie die für Internet Service Provider gültigen Vorschriften aus dem Kurstext.

- Telekommunikationsgesetz.
- Telekommunikationsgesetzdatenschutzverordnung.
- Telekommunikationsgesetzüberwachungsverordnung.
- Gesetz gegen unlauteren Wettbewerb.
- Handelsgesetzbuch.
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich.

2P

Was trägt man in die probability impact Matrix ein, welche Funktionen erfüllt sie?

- Eintrittswahrscheinlichkeit und Schadensumfang.
- In der Risikoanalyse werden die größten Risiken genauer betrachtet.

2P

Was ist beim Entwurf sicherer Systeme mit Interposition gemeint?

Schalten eines Zwischenstücks zwischen zwei Systemen, z.B. ein Proxy.

1P

Handelt es sich bei der Java-Sandbox um einen Wrapper, Interposition, Compartmentalization oder Identifikation und Authentisierung?

Compartmentalization.

1P

Wozu benötigt man das Lightweight Directory Access Protocol?

Zur konsistenten und einheitlichen Verwaltung von Benutzerdaten.

2P

Wie kann es sein, dass ein IDS auf einem Rechner vor der Firewall einen Angriff um 17:38 Uhr feststellt und ein andres IDS hinter der Firewall denselben Angriff um 17:20 protokolliert, was ist zu tun, damit der Fehler beseitigt wird?

Die Uhren der beiden Rechner können nicht korrekt synchronisiert sein. Um die Uhren zu synchronisieren, sollte das Network Time Protocol eingesetzt werden.

12P

Nennen Sie die ersten zwei erforderlichen Schritte zur Konstruktion eines sicheren Systems. Untergliedern und diskutieren Sie dabei die typischen ersten zwei Teilphasen eines Projekts im Hinblick auf das Thema Sicherheit.

Analyse:

Funktionale Anforderungsanalyse.
Beschreibung der Daten und der Beziehungen untereinander mit denen das System später arbeiten soll.

Bedrohungsanalyse: Untersuchung, welche Bereiche gefährdet sind.

Gefährdungsbereiche (externe Angriffe, interne Angriffe, DoS, Abstreiten, Rechtemißbrauch)
Analyse der Ursachen für Gefährdungen (benutzerbedingt, technisch, organisatorisch).
Bekannte Bedrohungen vergleichbarer Systeme sammeln und vergleichen.

Risikoanalyse:

Bedrohungen anhand Eintrittswahrscheinlichkeit und Schadensumfang bewertet
(**probability impact Matrix**).

Entwurf:

Identifikation und Authentisierung
Rechtevergabe,
Protokollierung.