Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
PD Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2011/2012
Übungsblatt 11

Abgabetermin: 01.02.2012 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikumsinfrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungswebseite zum Übungsbetrieb an.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per **E-Mail** an die Adresse **uebung-itsec_AT_lrz.de** oder schriftlich vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 24: (H) IPSec

Das IP-Protokoll weist einige Schwachstellen im Hinblick auf die Vertraulichkeit und Integrität der übertragenen Daten, sowie im Hinblick auf die Authentisierung auf. Abhilfe sollte die Erweiterung IP Security (IPSec) schaffen.

a. Gegeben sei ein IT-System mit der IP-Adresse 10.250.17.120. Das zugehörige Security-Gateway habe die IP 10.250.17.254. Das Zielsystem habe die IP 10.10.1.1 mit Security-Gateway 10.10.1.254. Für die Kommunikation soll

   - AH im Transport-Mode zwischen den Endsystemen
   - ESP im Tunnel-Mode zwischen den Security-Gateways

   verwendet werden. Geben Sie für alle beteiligten Systeme exemplarische Inhalte aller relevanten Security Associations an; gehen Sie dabei davon aus, dass die Vertraulichkeit über AES-Verschlüsselung und die Integritätssicherung über MD5-Prüfsummen sicher gestellt werden soll.

b. Geben Sie, analog zu den Folien im Vorlesungsskript (z.B. Kap. 11, Folie 19) , den Inhalt des übertragenen Pakets an. Gehen Sie dabei von einem zu übertragenden IPv4-Datagramm aus. Geben Sie für alle an dieser Stelle relevanten Header-Felder korrekte Werte an.

c. Welche Möglichkeit(en) gibt es außer IKEv2 für den Schlüsselaustausch im Rahmen von IPSec? Nennen Sie mindestens einen Nachteil dieser Möglichkeit(en)?

d. In der IKE_INIT-Phase (IKEv2) wird das Diffie-Hellman-Verfahren eingesetzt. Wie lautet der ausgetauschte Schlüssel, wenn Alice den Schlüsselaustausch initiiert und als Wert für die Primzahl 23 sowie 5 als Wert für die Primitive Wurzel vorgibt. Gehen Sie davon aus, dass die gewählte Zufallszahl von Alice 6 und die von Bob 15 ist.

Aufgabe 25: (H) SSL

Die Kommunikation beim Online-Banking sollte aus Sicherheitsgründen verschlüsselt erfolgen und wird daher nicht mit HTTP sondern durch die SSL-gesicherte Variante HTTPS realisiert.

a. Beschreiben Sie den grundsätzlichen Ablauf des SSL Record-Protokolls.

b. Welche Nachricht wird versendet, wenn der Server dem Client eine CertificateRequest-Nachricht sendet, dieser aber keines besitzt?

c. Im Rahmen des SSL-Handshake-Protokolls werden Zufallszahlen (Nonces) verwendet. Wann werden diese ausgetauscht, wo werden Sie im späteren Verlauf des Protokolls verwendet und welchen Zweck haben diese?

d. Haben Client und Server bereits miteinander kommuniziert, so gibt es die Möglichkeit diese Session wieder aufzunehmen. Beschreiben Sie den Ablauf dieser Wiederaufnahme. Welche Nachrichten werden hierzu ausgetauscht. Welche Auswirkungen hat die Wiederaufnahme für das berechnete Master Secret?

Aufgabe 26: (K) Firewalls und Intrusion Detection

a. Welche Firewall-Techniken lassen sich im Allgemeinen unterscheiden? Beschreiben Sie die jeweilige Technik und zeigen Sie mindestens einen sinnvollen Einsatzzweck auf.

b. Erstellen Sie exemplarisch Firewall-Regeln, um die folgenden Anforderungen zu erfüllen. Achten Sie dabei auch auf Vollständigkeit Ihres Regelwerks unter Berücksichtigung maximaler Sicherheit:

   - Der Zugriff auf den Firmen-eigenen Webserver soll von extern per HTTPS möglich sein
   - Die Administration des Webservers erfolgt von dedizierten Managementstationen (IPs: 10.10.18.5 und 10.10.18.200) per ssh
   - Verbieten Sie explizit den Telnet-Zugang auf den Webserver aus dem internen LAN
   - Die Security-Policy verbietet den Mitarbeitern des Kunden unter anderem den Aufruf von Jobsearch-Seiten

   Ihre Firewall besitzt die externe IP-Adresse 212.34.128.12. Ihr Webserver besitzt die IP-Adresse 10.10.19.6 und befindet sich in einer DMZ. Das interne LAN die Adressen 10.10.18.0/24. Welche zusätzliche Konfiguration an Ihrer Firewall müssen Sie für den Zugriff auf den internen Webserver durchführen?

c. Welche grundsätzlichen Erkennungstechniken findet man bei einem Netz-basierten Intrusion Detection System? Nennen Sie Vor- und Nachteile.

d. Intrusion Detection Systeme lassen sich umgehen. Beschreiben Sie mindestens eine mögliche Evasiontechnik.