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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2010/2011
Übungsblatt 10

Abgabetermin: 02.02.2011 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikums Infrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungs Webseite zum Übungsberieb an.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email, in der Vorlesung oder 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)** IKEv2 & SSL-Protokoll-Architektur

In der Vorlesung wurde der Ablauf des IKEv2-Protokolls erläutert.

a. Beschreiben Sie in Stichpunkten den Ablauf des IKEv2-Protokolls.

b. Welche Nachrichten werden in der IKE_AUTH-Phase zwischen den Kommunikationspartnern ausgetauscht. Was ist der Zweck dieser Phase.

c. Was ist die Aufgabe des Traffic Selectors? Können der Traffic-Selector des Initiators und der Traffic-Selector des Responders unterschiedliche Werte enthalten?

d. Beschreiben Sie die SSL/TLS Protokoll-Architektur und stichpunktartig die Aufgaben des jeweiligen Protokolls.

Aufgabe 25: **(H)** 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.

   – Der Zugriff auf den Firmen-eigenen Webserver soll von extern per HTTP und HTTPS möglich sein
   – Der Zugriff auf den firmeninternen Webserver soll aus dem internen LAN zusätzlich per ssh möglich sein

- Verbieten Sie explizit den Telnet-Zugang auf den internen 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 eine mögliche Vorgehensweise.