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 6

Abgabetermin: 07.12.2011 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 13: (H) Common Vulnerability Scoring System(CVSS)

Das Common Vulnerability Scoring System ist ein IT-Framework zur Charakterisierung und Beschreibung der Auswirkungen von Schwachstellen in IT-Systemen und Applikationen in punkto IT-Sicherheit. Gegeben sei folgende Schwachstellenbeschreibung:

Der TCP/IP-Stack in Microsoft Windows 7 weist bei der Verarbeitung von manipulierten IPv6-Paketen eine Schwachstelle auf. Dadurch ist es einem entfernt agierenden Angreifer möglich, beliebigen Code einzuschleusen und mit Systemrechten auszuführen.

Berechnen Sie den CVSSv2-Score mithilfe des von der NIST bereitgestellten CVSSv2-Calculators (http://nvd.nist.gov/cvss.cfm?calculator&version=2) und geben den zugehörigen Base-Metric-, Temporal- und Environmental-Wert an, so dass Ihre Score-Berechnung nachvollziehbar ist.

a. Berechnen Sie für die beschriebene Schwachstelle den CVSSv2 Base-, Temporal- und Environmental-Score

b. Wie verändert sich der Base-Score, wenn die Schwachstelle nur dann ausgenutzt werden kann, wenn eine Race Condition in einem sehr engen Zeitbereich auftritt?

c. Die beschriebene Schwachstelle wurde auf der Security-Mailingliste *Full-Disclosure* publiziert und deren Ausnutzbarkeit anhand eines Proof-of-Concept (POC) bewiesen. Microsoft (Hersteller!) hat die Schwachstelle offiziell bestätigt, aber bislang nur einen Workaround veröffentlicht. Wie verändert sich dadurch der CVSSv2-Score?

d. In einem bekannten Forum wird jetzt ein Exploit für diese Schwachstelle publiziert, der keine besonderen Voraussetzungen aufweist und somit in jeder Situation funktional ist. Wie verändert sich dadurch der Score aus Aufgabe c)?

e. Glücklicherweise sind in ihrem Unternehmen erst 53% der Windows-Arbeitsplätze auf Windows 7 umgestellt. Wie beeinflusst dieser Umstand das CVSSv2-Scoring?

Aufgabe 14: (H) Steganographie & Advanced Encryption Standard

Mithilfe des Programms *steghide* lassen sich Nachrichten in Bildern per Steganographie einbetten.

a. Laden Sie sich das Programm *steghide* aus dem Internet herunter. Auf der Vorlesungswebsite finden Sie ein Bild (bunt.jpg) in das eine 16-Byte lange Nachricht eingebettet ist. Versuchen Sie diese Nachricht aus dem Bild zu extrahieren. Das Passwort finden Sie auf Folie 18 im Vorlesungsskript Kapitel 5 (Hinweis: Welche Forscher haben einen Known-Plaintext-Angriff auf DES durchgeführt? Format des Passworts: Nachname1undNachname2, also ohne Leerzeichen!) Achten Sie darauf, dass Ihr Lösungsweg nachvollziehbar ist.

b. Gegeben sei folgende Permutations-Matrix: $\begin{pmatrix} 4 & 8 & 15 & 3 \\ 2 & 7 & 11 & 5 \\ 9 & 1 & 6 & 16 \\ 13 & 10 & 14 & 12 \end{pmatrix}$

Das 4. Byte der Nachricht aus Aufgabe a) wird demnach an Stelle s_{11} platziert, usw.! Falls Sie Teilaufgabe a) nicht erfolgreich lösen konnten, die Nachricht lautete: 2312170154441A312416273061144502.

c. Verwenden Sie das Ergebnis aus Aufgabe b) als initialen Rundenschlüssel für den Rijndael-Algorithmus (AES) und verschlüsseln damit folgende Klartext-Nachricht. Beachten Sie, dass die Multiplikationen in $GF(2^8)$ durchzuführen sind. Das zugehörige irreduzible Polynom lautet $x^8 + x^4 + x^3 + x + 1$. Benennen Sie die jeweilige Phase des AES-Algorithmus, berechnen Sie den Wert des 1. Bytes nach Ablauf der 1. AES-Runde. Geben Sie alle relevanten Zwischenergebnisse an, damit Ihr Rechenweg nachvollziehbar ist!

Klartext: $\begin{pmatrix} 11 & 22 & 33 & 44 \\ 33 & 22 & 44 & 11 \\ 33 & 44 & 11 & 22 \\ 44 & 11 & 22 & 33 \end{pmatrix}$ Spaltenmixmatrix: $\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$

Verwenden Sie für die Substitution die folgende S-Box:
S-BOX:

	0	1	2	3	4	5	6	7	8	9	A
0	0x00	0x10	0x20	0x01	0x18	0x19	0xB4	0x45	0x2C	0xCB	0xE7
1	0xCB	0x25	0xE1	0xCA	0x10	0x13	0xA7	0x3B	0x1A	0x37	0x76
2	0xD2	0xA1	0x40	0x89	0x9D	0x34	0x12	0x5E	0x2D	0x45	0x18
3	0x38	0x40	0x2C	0x29	0x02	0x27	0xF1	0x01	0x89	0x61	0x37
4	0x43	0xF2	0x20	0x30	0x40	0x02	0xD8	0x7B	0x6A	0x12	0x7F
5	0x3C	0xCB	0x28	0x34	0xA2	0x09	0x7F	0x4D	0xC2	0x8D	0x10
6	0x15	0x62	0x7D	0xE1	0xB6	0xD3	0x34	0x81	0xC6	0x9A	0x1F
7	0x26	0x5D	0xA1	0xD8	0x32	0x89	0x12	0x01	0xC0	0x1F	0x8E

Nach der ersten Key Expansion wurde folgender Rundenschlüssel berechnet:

1. Rundenschlüssel: $\begin{pmatrix} 1A & 5A & EE & 18 \\ B7 & 87 & 26 & B4 \\ 41 & 51 & 43 & 45 \\ 19 & 39 & CA & 18 \end{pmatrix}$