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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2012/2013
Übungsblatt 4

Abgabetermin: 05.12.2012 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email 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 9: (H) Allgemeine Vorgehensweise eines Angreifers

Das Vorgehen eines Angreifers lässt sich grundsätzlich in verschiedene Phasen gliedern:

1.Step: Reconnaissance, Footprinting & Social Engineering

2.Step: Scanning & Enumeration

3.Step: System Hacking

4.Step: Escalating privileges

5.Step: Creating Backdoor & Hiding Files

Beantworten Sie hierzu folgende Fragen:

a. Versetzen Sie sich in die Lage eines Angreifers. Im Rahmen der Reconnaissance versuchen Sie möglichst viele Informationen über ein Unternehmen und dessen IT-Infrastruktur in Erfahrung zu bringen. Scannen Sie die IP-Adresse 141.84.3.25 mit nmap. Verwenden Sie an dieser Stelle unterschiedliche Parameter, um z.B. das Betriebssystem oder die Service-Version zu bestimmen. Nennen Sie auch für Sie wichtige, nicht-technische Informationen, die Ihnen bei einem späteren Angriff nützlich sein könnten.

b. Vor kurzem wurde eine Lücke in MySQL bekannt. Bezeichnet wird diese Schwachstelle mit CVE-2012-2122. Beschreiben Sie diese Lücke knapp. Wie könnte ein Angreifer diese Lücke ausnutzen?

c. Ein befreundeter Hacker erzählt Ihnen, dass sich auf dem System mit der IP-Adresse 8D540319 ein für den in der vorherigen Teilaufgabe beschriebenen Angriff verwundbarer MySQL-Server befindet. Versuchen Sie die dort liegenden Datenbanken und Tabellen auszulesen. Welche Nutzer existieren dort und sind zugriffsberechtigt für die Datenbank(en)?

d. Sie arbeiten als Mitarbeiter in einem ServiceDesk. Zu Ihren Aufgaben gehört neben der Aufnahme von Störungen und Service-Requests das Zurücksetzen von Passwörtern. Beschreiben Sie eine mögliche Vorgehensweise um Social Engineering Angriffen, die auf das unberechtigte Erlangen von Credentials abzielen, wirkungsvoll zu begegnen.

Aufgabe 10: (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 jedem Angreifer, der sich im selben LAN-Segment befindet, möglich, ohne vorherige Authentifizierung beliebigen Code einzuschleusen und mit Systemrechten auszuführen.

Die NIST stellt einen CVSSv2-Calculator bereit (http://nvd.nist.gov/cvss.cfm?calculator&version=2). Geben Sie den zugehörigen Base-Metric-, Temporal- und Environmental-Wert an, so dass Ihre Score-Berechnung insgesamt nachvollziehbar ist.

a. Berechnen Sie für die beschriebene Schwachstelle den CVSSv2 Base-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 Base-/Temporal-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 Base-/Temporal-Score aus Aufgabe c)?

e. Glücklicherweise sind in ihrem Unternehmen erst 24% der Windows-Arbeitsplätze auf Windows 7 umgestellt. Wie beeinflusst dieser Umstand das CVSSv2-Scoring?