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 4

Abgabetermin: 23.11.2011 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 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. Beim Reconnaissance versucht ein Angreifer, so viele Informationen wie möglich über ein Unternehmen in Erfahrung zu bringen. Hierzu verwendet er im Allgemeinen Informationen, die auf öffentlich zugänglichen Webauftritten stehen, aber auch spezielle Werkzeuge wie *NS-Lookup*, *traceroute* und *whois*. Versuchen Sie Informationen (Kontaktinfos, Telefonnummern, Netzwerkblöcke,. . .) über die LMU in Erfahrung zu bringen, die Ihnen bei einem Angriff u.U. nützlich sein könnten. Verwenden Sie hierzu u.a. die genannten Methoden.

b. Ziel-IP-Adressen, die in Web-Links, welche Angreifer z.B. per E-Mail an Mitarbeiter senden, werden oftmals verschleiert dargestellt. Die IP-Adresse 192.168.10.5 lautet in Dezimalschreibweise 3232238085 und in IP Hex C0A80A05. Wie lautet die IP Hex-Darstellung der IP-Adresse 129.187.254.231? Achten Sie darauf, dass Ihr Rechenweg nachvollziehbar ist.

c. Zu den Standardaufgaben eines ServiceDesk-Mitarbeiters gehört das Zurücksetzen von Passwörtern. Welche Maßnahmen schlagen Sie hierzu vor, um Angriffe im Social Engineering zu verhindern?

d. Mithilfe des OS-Fingerprintings versuchen Sie Informationen über das auf einem System installierte Betriebssystem zu erhalten. Man unterscheidet zwischen aktivem und passivem Fingerprinting. Erläutern Sie den Unterschied und nennen Sie einen Vor- und Nachteil für das passive Verfahren.

Aufgabe 10: (H) crypt & Passwort-basierte Authentifizierung

Bei älteren Unix-Systemen werden Nutzerpasswörter per *crypt* verschlüsselt gespeichert.

a. Welche Punkte der folgenden Beschreibung sind falsch? Korrigieren Sie den Text entsprechend.

   Beim Anlegen eines neuen Nutzerkontos legt der Administrator (root) das Passwort für einen Nutzer initial fest. Beim ersten Login wird dieser aufgefordert, das Passwort zu ändern. Der Nutzer root ist aber auch nach dieser Änderung in der Lage, das per crypt und damit per AES verschlüsselte und in der Datei /etc/passwd gespeicherte Nutzerpasswort zu entschlüsseln. Um Wörterbuch-Attacken zu erschweren, wurde ein Salt eingeführt, der insgesamt 16 Bit lang ist. Der Salt bildet die letzten 2 Ziffern im verschlüsselten Passwort, welches als 20 Bit langer String gespeichert ist. Die Verschlüsselung von crypt ist auch bei heutiger Rechenleistung als sicher zu bezeichnen.

b. Oftmals findet sich in der Datei /etc/passwd statt des verschlüsselten Passwort-Strings der Wert *x*. Was bedeutet dieser Wert und welchen Vorteil hat dieser gegenüber der herkömmlichen Methode?

c. Welche Regeln empfehlen Sie für die Wahl eines guten Passwortes?