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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2014/2015
Übungsblatt 6

Abgabetermin: 02.12.2014 bis 12:00 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 (über Uniworx als Einzelabgabe). Während des Semesters werden vier Übungsblätter ausgewählt, korrigiert und bewertet. Bei vier als korrekt bewerteten Lösungen (mind. 75% der erreichbaren Punkte) 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 14: (H) Allgemeine Vorgehensweise eines Angreifers (10 Punkte)

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. Sie, in der Rolle eines Angreifers konnten im Rahmen der Reconnaissance sehr viele Informationen über ein Unternehmen sammeln. So wissen Sie beispielsweise, dass auf dem Großteil der dort vorhandenen IT-Systeme als Betriebssystem Linux- bzw. Unix installiert ist.
Sie konnten mit etwas Geschick und Glück, ein für einen gezielten Angriff geeignetes System identifizieren, von dem sie aber bislang nur die IP-Adresse (138.246.6.16) kennen.
Wie würden Sie den Portscanner *nmap* konfigurieren, um

   (i) einen möglichst unauffälligen XMAS-Scan durchzuführen?

   (ii) als Source-IP die IP-Adresse 187.156.23.12 zu verwenden?

   (iii) die MAC-Adresse 00:23:67:89:A2:12 zu verwenden?

   (iv) die OS-Detection als auch die Service Versionen zu bestimmen?

Das LRZ ist für die genannte IP-Adresse zuständig, es befindet sich jedoch kein reales IT-System dahinter, d.h. Sie brauchen es nicht mit Nmap zu scannen. Beachten Sie außerdem dass Portscans als Angriffsversuche angesehen werden, insofern bitten wir Sie auch keine anderen IP-Adressen zu scannen.

Geben Sie für jeden oben genannten Scan die entsprechende Kommandozeile, also insgesamt 4 Zeilen(!), an.

b. Was versteht man bei der Verwendung des Portscanners *Nmap* unter *Nmap decoys*? Welchen Zweck erfüllen diese?

c. Nmap erlaubt Ihnen den Aufruf spezieller Scripte, die gezielt versuchen Schwachstellen auszunutzen. Wie lautet der Nmap-Aufruf für die unter Teilaufgabe a) genannte IP-Adresse, wenn Sie die *common Scripts* ausführen wollen. Manche dieser Scripte erfordern die Angabe von Username und Passwort. Erstellen Sie eine entsprechende Script-Argument-Datei und ergänzen sie vorherigen Nmap-Aufruf um die Argument-Datei.

d. Sie arbeiten als Mitarbeiter in einem ServiceDesk in einem Unternehmen. Zu Ihren Aufgaben gehört neben der Aufnahme von Störungsmeldungen (Incidents), deren Lösung im Rahmen von 1st-Level-Support auch explizit das Zurücksetzen von Passwörtern. Definieren Sie stichpunktartig eine sinnvolle Vorgehensweise, insbesondere ein Verfahren, um die Gefahr hierbei durchgeführter Social Engineering Angriffen, die auf das unberechtigte Erlangen von Credentials abzielen, wirkungsvoll zu begegnen.

e. Ein Grund, warum Social Engineering Angriffe erfolgreich verlaufen, ist das Ausgeben als eine Autoritätsperson, z.B. eines Vorgesetzten. Nennen Sie weitere, *mindestens 4* Gründe, warum SE-Angriffe immer wieder funktionieren.

Aufgabe 15: (H) Common Vulnerability Scoring System (CVSS) (6 Punkte)

Das DFN-CERT informiert ans DFN angeschlossene Einrichtungen über einen automatischen, E-Mail-basierten Warndienst über aktuelle Schwachstellen.

a. Mitarbeiter des LRZ Abuse-Response-Teams erhielten am 25.09.2014 eine E-Mail (DFN-CERT-2014-1258), in der auf mehrere Schwachstellen in GNU Bash hingewiesen wurde. Beschreiben Sie die damit verbundenen Schwachstellen CVE-2014-6271 und CVE-2014-7169 so, dass Sie die damit verbundenen, verschiedenen CVSSv2-Scores in den folgenden Teilaufgaben berechnen können.

b. Berechnen Sie mithilfe des unter http://nvd.nist.gov/cvss.cfm?calculator&version=2 verfügbaren CVSSv2-Calculators für die in der vorherigen Teilfaufgabe beschriebene Schwachstelle in GNU Bash den CVSSv2 Base-Score.

c. Nehmen Sie nun an, dass sich die Schwachstelle nur dann ausnutzen lässt, wenn eine Race Condition in einem sehr engen Zeitbereich auftritt? Wie verändert das den Base-Score?

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

e. Bereits am nächsten Tag tauchte in einschlägigen Foren ein Exploit für diese Schwachstelle auf. Dieser besitzt keine besonderen Voraussetzungen und ist somit in jeder Situation funktional. Wie verändert sich dadurch der Base-/Temporal-Score aus Aufgabe c)?

f. Glücklicherweise sind in ihrem Unternehmen nur 77% der IT-Systeme Linux-/Unix-basiert und somit betroffen. Wie beeinflusst dieser Umstand das CVSSv2-Scoring?

Hinweis: Bei den Berechnungen eines Base-Scores mit dem CVSSv2-Calculator verwenden Sie für Temporal und Environmental Scores jeweils den Wert *Not defined*.