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 2015/2016
Übungsblatt 6

Abgabetermin: 08.12.2015 bis 12:00 Uhr

Achtung: Die Übung am 01.12.2015 muss leider entfallen. Für die Bearbeitung dieses Übungsblattes sind daher zwei Wochen angesetzt.

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.

Bei Fragen zu Übungsaufgaben sowie generellen Anregungen, Verbesserungsvorschlägen, ... zum Übungsbetrieb wenden Sie sich bitte per Email an **`uebung-itsec@lrz.de`**.

Aufgabe 16: **(H)** Allgemeine Vorgehensweise eines Angreifers (4 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 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.

b. 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 17: (H) Portscanning mit Nmap (6 Punkte)

Der Portscanner Nmap ist ein häufig verwendetes Tool um festzustellen, welche Dienste auf welchen Hosts in einem Zielnetzwerk laufen.
Das LRZ ist für die in der Aufgabe 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.

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 das 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 00:23:61:89:A2:12 zu verwenden?
   (iv) die OS-Detection als auch die Service Versionen zu bestimmen?
   (v) anstelle von TCP-Ports, UDP-Ports zu scannen? Wie erwarten Sie, dass sich die Laufzeit eines Scans ändert, wenn anstelle von TCP, UDP verwendet wird?

   Geben Sie für jeden oben genannten Scan die entsprechende Kommandozeile, also insgesamt 5 Zeilen(!), an.

b. Was versteht man bei der Verwendung des Portscanners *Nmap* unter *Nmap decoys*? Welchen Zweck erfüllen diese? Beschreiben Sie, warum ein XMAS-Scan weniger auffällig ist als ein SYN-Scan. Geben Sie außerdem mindestens 3 weitere Optionen an, die einen Scan weniger auffällig machen.

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.

Aufgabe 18: (H) Einfache Chiffriermethoden & Steganographie & One Time Pads (7 Punkte)

Eines der zentralen Themen in der Informationssicherheit ist die Kryptographie. Neben den bekannten symmetrischen und asymmetrischen Verfahren gibt es zahlreiche, auch sehr einfache und dennoch effektive Methoden, die Vertraulichkeit von Informationen sicher zu stellen.

a. Ein sehr altes kryptographisches Verfahren ist *Skytale*, welches auch als Spaltentransformation bezeichnet wird. Der Geheimtext nach Anwendung der Transposition lautet FNABAIHUESNAFNSDUGKEESAL. Entschlüsseln Sie diesen und verwenden Sie hierbei eine Skytale mit einem Umfang U=5.

b. Neben additiven Chiffren (Caesar-Chiffre) existieren auch multiplikative Chiffren. Hierbei wird einem Buchstaben erst eine Zahl zugeordnet und anschließend mit einem Schlüsselwert k multipliziert. Das Ergebnis gibt die entsprechende Position im Alphabet (A-Z) an. Verwenden Sie den Wert $k = 2$. Der Buchstabe O soll dabei auf den Buchstaben D abgebildet werden. Geben Sie die Berechnungsvorschrift an und berechnen Sie die passenden Werte für alle Buchstaben. Was fälllt Ihnen bei dieser Substitution auf? Wie sollten Sie den Parameter k wählen, damit dieser Effekt nicht auftritt?

c. Auf der Vorlesungswebseite finden Sie im Abschnitt *Übung* eine Bild-Datei. In diese wurden mit den Steganographie-Werkzeug *Outguess* (Linux/Mac OS) bzw. *Steghide* (Linux/Windows) eine geheime Information eingebettet. Downloaden Sie das für ihr Betriebssystem geeignete Werkzeug und versuchen Sie den versteckten Nachrichtentext aus dem Bild zu extrahieren. Verwenden Sie das Ergebnis aus Teilaufgabe a) als Schlüssel. Der Schlüssel enthält keine Leerzeichen. Achten Sie darauf, dass ihre Lösung nachvollziehbar ist (z.B. Angabe der verwendeten Befehlszeile, Screenshots, . . .).

d. One-Time-Pad gilt derzeit als eine der sichersten Verschlüsselungsmethoden. Geben Sie das Chiffrat für die Eingabe HALLOWELT an. Verwenden Sie als Pad die Information, die Sie aus dem Bild im Rahmen der vorherigen Teilaufgabe extrahiert haben.

Aufgabe 19: (K) Rechtliche Randbedingungen der IT-Sicherheit

In der Vorlesung haben Sie sich auch mit einigen rechtlichen Rahmenbedinungen auseinander gesetzt. Beantworten Sie dazu folgende Fragen:

a. Beschreiben Sie die Unterschiede zwischen Nutzungsdaten (§15TMG), Bestandsdaten (§14TMG) und Inhaltsdaten (BDSG, LDSGe).

b. (2) Sie arbeiten in einem Consulting-Unternehmen, das Kunden auch in IT-Sicherheitsthemen berät. Um Ihren Kunden die Brisanz dieses Themas zu verdeutlichen, sind Sie im Besitz eines sogenannten Sniffer-Werkzeugs, um damit Datenpakete aus einem WLAN-Netz zu empfangen, d.h. auch Daten, die eigentlich für andere Empfänger bestimmt sind. Mithilfe dieser Datenpakete und einem weiteren, speziellen Tool kann der Zugangscode des WLAN entschlüsselt werden. Wie beurteilen Sie diese Situation strafrechtlich im Hinblick auf die Paragraphen §202b StGB und §202c StGB?

c. (1) Das in Teilaufgabe a) beschriebene Werkzeug ist auf einer ausländischen Internetseite als Open Source Programm frei zugänglich und kann von dort herunteregeladen werden. Sie geben dem Sicherheitsbeauftragten eines Kunden den Link zu dieser Internetseite. Wie beurteilen Sie diesen Tatbestand nach §202c StGB?