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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2024/2025
Übungsblatt 5

Besprechung: Do, 28.11.2024 um 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.

Aufgabe 1: (T) Social Engineering

In der Vorlesung wurde ausführlich das Thema *Social Engineering* vorgestellt.

a. Ein vom Social Engineer häufig angewandtes und in der Praxis erfolgreiche Vorgehensweise ist das *Phishing*. Erläutern Sie die Vorgehensweise und die Unterschiede der Phishing-Varianten *Clone phishing*, *Spear phishing* und *Whaling*.

b. Nennen Sie mindestens 4 Dinge, die eine Phishing-E-Mail aufweisen sollte, damit der Social Engineer sein Ziel, d.h. das Erlangen sensibler Informationen, z.B. Zugangsdaten, erreicht.

c. Als wirkungsvollste Maßnahme gegen Social Engineering Angriffen gilt nach wie vor, Mitarbeiter:innen zu sensiblisieren. Der Aufbau eines erfolgreichen Security Awareness Programms ist aber eine Herausforderung. In der vom SANS-Institut herausgegebenen *Top 20 Security Controls* Liste wird auch das Control *Implement a Security Awareness and Training Program* angeführt. Wie sollten Sie demnach beim Aufbau eines Awareness-Programms vorgehen?

Aufgabe 2: (T) Rechtliche Randbedingungen der IT-Sicherheit

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

a. Der Branchenverband BITKOM hat einen praktischen Leitfaden für die Bewertung von Software im Hinblick auf den §202c StGB (Hackerparagraph) veröffentlicht. Obwohl der Verband die Regelung grundsätzlich begrüßt, sieht er dennoch eine Problematik bei deren strikter (im Wortlaut) Anwendung?

b. Erläutern Sie das im BITKOM-Leitfaden definierte, dreistufige Bewertungsschema, inwieweit der Umgang mit einer Software als tatsächlich strafbar zu bewerten ist.

c. Wenden Sie das Bewertungsschema auf einen *Passwort Cracker*, *Schwachstellenscanner* und ein in der Softwareentwicklung häufig eingesetztes *Code Analyse Werkzeug* exemplarisch an.

Aufgabe 3: **(T)** Pentesting

Die Durchführung von Penetrationstests oder kurz *Pen-Tests* ist ein verbreiteter Ansatz von IT-Sicherheitsexperten.

a. Welche Ziele haben Penetrationstests? Welche Risiken bergen sie?

b. Welche Eigenschaften und Qualifikationen sollte ein Pen-Tester mitbringen?

c. Was kann man aus Pen-Test-Ergebnissen lernen? Ist deren Durchführung sinnvoll?

d. Wie unterscheiden sich Pen-Test und Vulnerability Scan?

e. Was sind Blackbox- bzw. Whitebox-Tests? Wann sollte welches Modell angewandt werden?

Aufgabe 4: **(H)** Social Engineering

Beim *Social Engineering* richten sich die Angriffe nicht direkt gegen technische Systeme, sondern auf ihre Benutzer.

a. Beschreiben Sie fünf gängige Angriffstechniken des Social Engineerings.

b. Welche davon erscheinen für welche Zielsetzung am erfolgsversprechenden?

c. Welche Maßnahmen lassen sich (aus Unternehmenssicht) gegen die verschiedenen Techniken etablieren? Wie kann man sich (als potentielles Opfer) im Alltag schützen?

Aufgabe 5: (H) Ablauf von Penetrationstests

a. Nennen Sie den Unterschied zwischen Ethical- (White-Hat) und Black-Hat-Hacker? Geben Sie eine Definition von "Hackerän.

b. Beschreiben Sie kurz den Ablauf eines Pen-Tests anhand des 5-Phasen-Modells des BSIs. (`https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=3`)

c. Wie lassen sich Pen-Tests klassifizieren? Beschreiben Sie das Klassifizierungsschema des BSIs. (`https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=3`)

d. Kann der Einsatz von *Social Engineering* im Rahmen eines Pen-Tests auch negative Auswirkungen auf die Mitarbeiter haben? Geben Sie ein Beispiel an.

e. Was ist der Unterschied zwischen einem Port-Scan und einem Schwachstellenscan?