4

502470 - Einführung in Sicherheit und Privatheit
Übung: Angriffstechniken
— Diskussion der Lösung während der Übung: 17. Dezember 2018 —

1 Typische Angriffstechniken

Frage 1. Nennen und erläutern Sie kurz die in der Vorlesung vorgestellten Nährböden für Angriffe?

Frage 2. Was wird unter der typischen Bedrohungsabwehr verstanden? Nennen Sie die Schritte und geben Sie zusätzliche Beispiele.

2 Schadsoftware

Frage 3. Ein Nutzer sucht im Internet nach einem Programm zur Bearbeitung seiner Bilder. Nachdem er auf einer ihm seriös erscheinenden Webseite fündig geworden ist, lädt der Nutzer das typischerweise kostenpflichtige Programm plus Crack kostenlos herunter. Nach kurzem Zögern installiert der Nutzer beide Programme und bestätigt seinem Betriebssystem die Vertrauenswürdigkeit der Quelle. Kurz darauf stellt der Nutzer eine Flut an unerwünschter Werbung fest. Der Nutzer wundert sich über das Verhalten seines Browsers, da dieser stets andere Webseiten ansteuert als eingegeben. Wochen danach erhält der Nutzer eine ihm unerklärlich hohe Rechnung seines Internetproviders, da von seinem Anschluss aus kostenpflichtige 0900 Anrufe getätigt wurden.

Um welche Art von Schadsoftware (engl. malware) handelt es sich im dargestellten Beispiel? Beschreiben Sie zudem kurz was diese Schadsoftware kennzeichnet.

Frage 4. Trojaner können mit dem Programmstart oder durch eine logische Bombe aktiviert werden. Geben Sie in diesem Zusammenhang ein Beispiel für eine logische Bombe.

Frage 5. Nennen Sie unterschiedliche Bereiche eines Systems in denen Trojaner auftreten können.

Frage 6. Viren nutzen unterschiedliche Schutzmechanismen. Nennen und erläutern Sie kurz diese eigenen Schutzmechanismen von Viren.

Frage 7. In der Vorlesung wurden bereits mit dem Internet-Wurm (1988) und dem Wurm ILOVEYOU (2000) Beispiele für bekannte Würmer vorgestellt. Suchen Sie nach ähnlich

bekannten Würmern die zwischen 2003 und 2017 für aufsehen gesorgt haben. Beschreiben Sie anschließend kurz die Funktionsweise des Wurmes.

3 Bot-Netze

Frage 8. Erläutern Sie kurz das Prinzip eines Bot-Netztes sowie die geläufigen Abwehrstrategien gegen eben diese.

4 Alphanumerische Passwörter

Frage 9. In der Vorlesung wurde das Prinzip eines Wörterbuchangriffs erläutert. Salt stellt eine Gegenmaßnahme gegen einen solchen Angriff dar. Beschreiben Sie kurz was in diesem Zusammenhang unter Salt verstanden wird.

Frage 10. An kryptografische Hashfunktionen werden unterschiedliche Anforderungen gestellt. Unten aufgeführte Aussagen über die Hashfunktion H beschreiben diese Anforderungen zum Teil. Entscheiden Sie daher ob es sich um richtige Aussagen handelt. Kreuzen Sie diese an und korrigieren Sie ggf. falsche.

- ☐ Hashfunktion H besitzt die Eigenschaft einer Einwegfunktion
- ☐ Die Eigenschaft einer Hashfunktion H eine Einwegfunktion zu sein, wird auch als second preimage bezeichnet
- ☐ Schwache Kollisionsresistenz bedeutet, dass ein effizientes Verfahren existiert, um zu einer gegebenen Nachricht M eine Nachricht M' zu konstruieren, so dass diese dieselben Hashwerte liefert.
- ☐ Der Begriff second preimage charakterisiert häufig eine schwach kollisionsresistente Hashfunktion H
- ☐ Schwache Kollisionsresistenz besagt jedoch auch, dass es praktisch ausgeschlossen ist Paare zu finden deren Hashwerte kollidieren.
- ☐ Eine Hashfunktion H ist dann stark Kollisionsresistent, wenn schwache Kollisionsresistenz gegeben ist und es zunächst nicht effizient ist Paare, also zwei verschiede Eingabewerte M und M' deren Hashwerte übereinstimmen, zu finden.
- ☐ Starke Kollisionsresistenz ist schwerer zu garantieren als schwache.
- ☐ Ein Angreifer hat innerhalb der starken Kollisionsresistenz zwei Freiheitsgrade: beide Nachrichten M, M' können geändert werden, um gleiche Hashwerte zu finden.