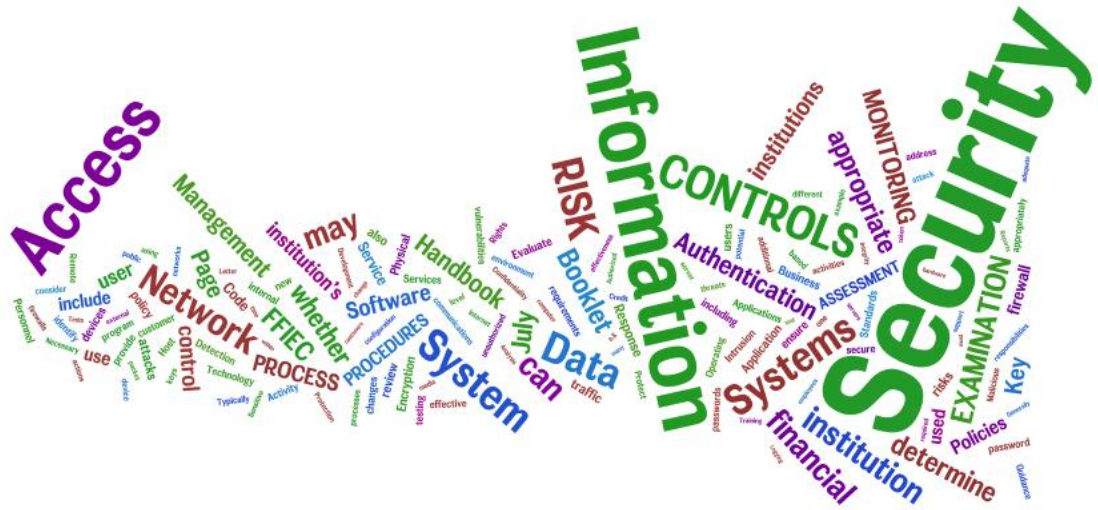

Angriffe auf ein System

Aufgabe Block 1-5

25HS

Inhaltsverzeichnis

1 Aufgabenstellung

In den Blöcken 1-5 erhalten sie einen groben Überblick über die Angriffe, die generisch auf ein System erfolgen können. Diese Angriffe lassen sich in die folgenden Gruppen unterteilen:

- Social Engineering
- Privilege Escalation
- DoS/DDoS

Entwerfen sie einen Angriff aus (so spezifisch wie möglich und sinnvoll) oder eine Sicherheitstechnische Verbesserung, der nicht zur Klasse des "Social Engineering" gehört, und befassen sie sich mit ihm vertieft, verfassen sie einen Bericht darüber, wie er im Detail funktioniert. Es soll explizite *kein Nachbau einer Attacke nach einem Howto im Internet* sein.

1.1 Vorgehen

Sie sollten sich bei der Wahl des Themas unbedingt an Ihren bestehenden Fähigkeiten orientieren. Am besten beginnen Sie damit, dass Sie sich fragen, was Sie bereits gut können und was Sie beruflich tun. fragen Sie sich entweder, wie ein solches System besser geschützt oder analysiert werden könnte. Oder wie man es Angreifen könnte. Beim Letzteren orientieren sie sich am besten an Angriffen, die sie von anderen Vorgehensweisen her kennen.

Wenn Sie einen bestehenden Angriff wählen: Zeigen Sie die Gefahren und Risiken auf und entwerfen sie detaillierte Abwehrszenarien für den von ihnen gewählten Angriff. Erläutern sie, wie weit sie den Angriff mit diesen Abwehrszenarien erschweren und welche Nachteile die getroffenen Massnahmen haben.

Hierzu folgendes Beispiel (kann nicht gewählt werden):

- Voraussetzung: Sie haben schon aktiv Bufferoverflows auf Windows 7 ausgenutzt und würden sich gerne mit DEP befassen.
- Gewählter Angriff: Buffer Overflow
- Eine vorgeschlagene Massnahme: DEP
- Beispiel: Windows 7 SP1 mit einem kurzen C-Programm und detaillierten Angaben wie DEP dieses Problem lösen kann (oder auch nicht).

Oder ein anderes Beispiel (kann auch nicht gewählt werden):

- Voraussetzung: Sie Sie haben einen Beruf bei dem Sie viel mit Kreditkarten arbeiten und Sie stellen fest, dass es zunehmend Diebstähle gibt, die die "Kontaktlos"-Funktion ohne Kartendiebstahl missbrauchen.
- Gewählter Angriff: Relayattacke bei Kreditkarten

- Eine vorgeschlagene Massnahme: Einsatz eines zusätzlichen Buttons auf der Karte um Angriffe ohne physischen Zugriff zu unterbinden.
- Beispiel: Statt generischer Smartcard soll ein Smarttoken von Gemalto mit Button eingesetzt werden

Alternativ dazu können Sie einen Sicherheitsrelevanten Patch für ein Opensource-Projekt einreichen. Für die Wahl des Projektes und Patches gelten die selben Vorgaben wie für einen reinen Bericht (Rücksprache mit dem Dozenten, Wahl und Termine).

1.2 Bewertung

Die Arbeiten werden im Wesentlichen nach folgenden Kriterien beurteilt:

- Eigene Kontribution (7x; Maximal 5 Punkte)
- Technisches Niveau (5x; Maximal 6 Punkte)
- Vollständigkeit und Tiefe (4x; Maximal 5 Punkte)
- Umfang und Praxisbezug (4x; Maximal 5 Punkte)
- Termingerechte Einreichung (3x; Maximal 3 Punkte)

Für eine 6 müssen Sie 105 Punkte erreichen. Die Skala ist linear.

Bitte beachten Sie, dass durch eine geschickte Auswahl der Aufgabe die Punkte massgeblich beeinflusst werden können.

2 Lieferobjekte

2.1 Wahl des Themas

Ein erster Vorschlag soll bis zum Ende der ersten Woche (Freitag 12:00) via Mail eingereicht sein. Spätestens bis zum Ende der 2. Woche haben sie ihr Thema definitiv gewählt (WARNUNG! Dieser Teil wird normalerweise massiv unterschätzt) und teilen dieses schriftlich (via Mail an den Dozenten) mit. Bei Themen, die abgelehnt werden oder präzisiert werden müssen, gibt es eine Frist von jeweils 2 Arbeitstagen.

Der Inhalt des Mails soll sein:

- Das Thema
- Was ist neu daran/Ihr Anteil
- Was Denken Sie? Kriegen Sie die gewählte Arbeit in 35 Ingenieurs-Stunden hin (Sie dürfen grössere Aufgaben wählen, aber es ist nicht notwendig).

Am besten wählen Sie Ihr Thema, anhand Ihrer Fähigkeiten und Interessen und fragen sich bei der Ausarbeitung der Aufgabe bereits, wie die Arbeit bewertet werden soll.

2.2 Abgabeform

Es soll ein Dokument abgegeben werden. Akzeptierte Formate sind (PDF-)LaTeX, Word, LibreOffice und PDF-Dokumente. Falls sie eine Lizenz wünschen empfehle ich Creative-Commons.org zu verwenden. Als Sprache können Sie Deutsch oder Englisch verwenden (das Modul wird nicht dem "Englischen Track" deswegen angerechnet).

Die Files sollen wie folgt benannt sein:

```
<email>_<YY><SS>_aufgabe2.<Dateierweiterung>
<email>    = Ihre Email-Adresse
<YY>       = Jahreszahl (zweistellig)
<SS>       = Semesterbezeichnung (FS=Frühjahrssemester; HS=Herbstsemester)
```

Beispiel:

```
Max.Muster@students.fhnw.ch_24HS_aufgabe1.docx
Max.Muster@students.fhnw.ch_24HS_aufgabe1.zip
```

2.3 Umfang und Inhalt

Der Umfang in Seiten wird nicht vorgegeben. Er soll sich am Thema orientieren. Rechnen sie damit, dass sie zur Aufbereitung des Berichtes *minimal* 35 Stunden aufbringen sollten. Wenn Sie sich ein Thema aussuchen, von dem Sie keine Ahnung haben können Sie das Erarbeiten eines Themas nicht in die 35h mit einrechnen.

2.4 Offenlegung

Bezüglich des Inhaltes gelten die üblichen Regeln speziell zu beachten ist, dass sie alle Quellen genau angeben müssen (inhaltlich, textuell oder auch bei Bildern und Illustrationen).

Die Textpassagen, die von einer KI generiert wurden (auch wenn sie nachträglich angepasst wurden) müssen als solche explizite kenntlich gemacht werden. Kam keine KI zum Einsatz muss dies ebenfalls deklariert werden. Sie können keine KI als Quelle für Inhalte oder Behauptungen angeben.

2.5 Termine

Das Thema muss am Ende der ersten Woche (Freitag 12:00) eingereicht sein.

Abgabe muss spätestens vor Beginn der 8. Lektion im cysL erfolgen. Abgabe muss elektronisch an martin.gwerder@fhnw.ch erfolgen. Der Erhalt der Arbeit wird binnen einem Arbeitstag elektronisch bestätigt.

2.6 Allgemeine Hinweise

Bitte beachten sie, dass ihr Bericht künftigen Studenten des CyberLAB in PDF-Form zur Verfügung gestellt wird. Sie werden sich auf andere Angriffe konzentrieren und versuchen Ihre Arbeiten teilweise als Grundlage zu verwenden.

Ich werde die Berichte durch ein Plagiats-Prüfsystem prüfen lassen. Wenn sie Quellen verwenden, dann müssen sie diese zitieren. Arbeiten, die sich als Plagiate entpuppen werden zurückgewiesen und abhängig nach Schweregrad mit der Note 1 Bewertet oder mit einem signifikanten Notenabzug zur Nachbesserung gegeben.