Fachhochschule Nordwestschweiz
Hochschule für Technik

Cyber Security Labor (cysL)

Theorieblock "Netzgestuetzte und lokale Attacken (technisch und nicht-technisch)"

Inhalt

Inhalt

Allgemeines

Der Normale Betrieb

Unterrichtsformen

- Unterrichtsblock (3 Lektionen Theorie)
  Lektionen 1, 6 und 13
- Laborblock (1 Lektion Theorie + 3 Lektionen reserviertes Labor für sie)
  Alle übrigen Lektionen

Informationen

- Im "AD"
- Drehbuch (Im AD)
- Die meisten PDFs sind verlinkt (das heisst, dass zugehörige Internet-Links wurden im Dokument hinterlegt) oder aber sie werden in das PDF-Dokument als Attachment eingebettet.

Aufgaben

- Sie arbeiten den Stoff jeweils vor!
- Sie verfassen die Berichte zu den Aufgaben.

Bewertung

- Über die beiden Aufgaben.

Allgemeines

Was dürfen sie erwarten

Inhalt

- Wir befassen uns mit cybertechnischen Angriffen und deren Abwehr.
  Sie dürfen im Cyberlab alle Angriffsformen, die sie wählen, auf ihre eigenen Infrastrukturen loslassen. Dies gilt auch für Formen, die Sie nicht vermittelt bekommen.
- Unser Labor ist vom Inhalt und Aufbau her fix. Vorschläge sind aber willkommen und erwünscht.
  Wir sind an den Beschrieb des Faches gebunden. Abhängig von Interessen können wir aber die Themen variieren.
- Es erwartet sie viel aber interessante Arbeit.

Einstellung

Keine Frage ist dumm und kein Ansatz zu trivial. Nichts ist unwesentlich. Wahre Eleganz liegt in einfachen Lösungen (gilt für Angriff wie auch für Abwehr).

(... und Kalendersprüche sind ab sofort tabu)

Allgemeines

Die Arbeitsweise

Wie arbeiten wir?

- Wir arbeiten jeweils ca. 1h im Schulzimmer und gehen anschliessend ins Lab (ausser in den reinen Theorieblöcken; da sind wir nur im Schulzimmer).
- Grundsätzlich erarbeiten Sie sich das Wissen selber (!) aber ich werde Sie jeweils mit Tipps und Buzzwords in der ersten Lektion versorgen, damit Ihnen die Lösung der Arbeiten leichter fällt.

Vorbereitung

Recherche

Machen sie eine Liste von Angriffen auf die Sicherheit eines Computersystems die kein Netzwerk-Zugriff auf ein System erfordern. Versuchen Sie die Liste in einem Raster zu kategorisieren. Welche Sichtweisen sind interessant aus der Sicht eines Angreifers und welche aus der Sicht eines Verteidigers? Sie müssen sich natürlich nicht nur am angegebenen Stoff orientieren.

Zum lesen oder anschauen ...

- Kodex CyberLAB
- Sicherheitsaspekte im Betriebssystem

Der Wikipedia-Artikel zu Social Engineering
TEDxSpeech über Social Engineering
TEDxSpeech über Taschendiebstahl

Begriffe

Informationssicherheit, Social-Engineering, Vulnerability-Thread-Control-Framework, Schutzziele, Schaden, Angreifer und Verteidiger.

Der Kodex

Unser Kodex

Unser Kodex gibt uns die Rahmenbedingungen vor unter denen wir arbeiten. Wir arbeiten hier mit spannenden Tools aber immer im Bereich des ethisch und gesetzlich vertretbaren.

Die Arbeitsweise im Labor

Was wir im CyberLAB tun werden

Das Drehbuch gibt uns ganz klare Vorgaben welche Ziele zu welchem Zeitpunkt erreicht werden müssen. Diese Ziele sind für uns bindend!

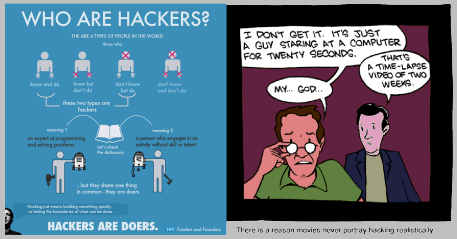
Eingebrachte Übungen

Es steht ihnen frei thematisch verwandte Aufgaben vorzuschlagen und, falls diese angenommen werden, sie anstelle einer oder mehrerer Übungen im Labor durchzuführen. Das ganze darf und soll Spass machen.

Spass mit Sicherheit

Die Definition eines Hackers

Was ein Hacker ist...



There is a reason movies never portray hacking realistically

Abbildung: Was sind eigentlich Hacker?

Allgemeines zur Sicherheit

Ein paar Begriffe

Identifikation

"Ich teile mit, wer ich bin"

Authentisierung

"Ich belege/beweise meine Identität mit vertrauenswürdigen Merkmalen."

Allgemeines zur Sicherheit

Ein paar Begriffe

Informationssicherheit

“Als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden (technischen oder nicht-technischen) Systemen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren beziehungsweise Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken.”

Aus Wikipediartikel “Informationssicherheit”

↳ Hauptziel ist es Risiken respektive die Schäden, die daraus resultieren, zu minimieren

Allgemeines zur Sicherheit

Ein paar Begriffe

Schutzziele

Klassisch gibt es drei Schutzziele

- Vertraulichkeit (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)

Die häufig ergänzt werden mit:

- Authentisierung (Authentication)
- Nachweisbarkeit (non-repudiation)
- Prüfbarkeit (Auditability)

Allgemeines zur Sicherheit

Ein paar Begriffe

Asset

Als “Asset” in der IT-Sicherheit wird alles bezeichnet was einen Wert hat. Beispiele sind:

- Hardware (Computer, Tablets, Scanner, Netzwerke usw.)
- Software (Firmware, Betriebssysteme, Standard- und Spezial-Programme usw.)
- Daten (Dateien, Datenbanken, Sicherheitsmerkmale, Firmengeheimnise usw.)

Der Wert dieser Assets ist häufig nicht eindeutig bezifferbar und subjektiv. Er kann unter anderem beeinflusst werden durch…

- die Ersetzbarkeit
- das Alter
- den potentiellen Schaden, der damit angerichtet werden kann.

Allgemeines zur Sicherheit

Klassifikation von Ereignissen

Ereignisse

Es gibt mehrere Möglichkeiten Ereignisse zu Klassifizieren. Gängigerweise werden sie aufgeteilt wie folgt:

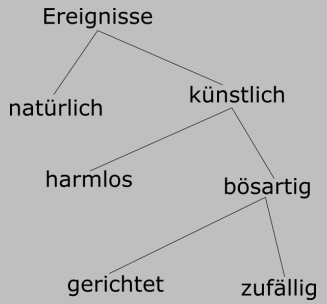


Abbildung: Klassifizierung von Ereignissen

Allgemeines zur Sicherheit

Klassifikation von Angreifern

Angreifer

- Amateure
  - Oportunisten
  - Script-Kiddies
- Hacker (harmlos?)/Cracker (bösartig?)
  - Personen mit einem Sicherheitsauftrag
  - Kriminelle
  - Organisierte Kriminalität
  - Cyber-Terroristen oder Hacktivisten
  - Staatlich finanzierte “Informationskrieger” und Spione

Allgemeines zur Sicherheit

Abwehrstrategien

Abwehrstrategien

- Angriff verhindern
- Angriff erschweren
- Angriff ableiten
  - Intern oder extern
- Schaden kontrollieren
- Angriff entdecken
  - Während aber auch im Nachhinein
- Vom Angriff erholen

Allgemeines zur Sicherheit

Die Grundvoraussetzungen für einen Angreifer

Grundvoraussetzungen

- Methode
  - Fähigkeiten
  - Hilfsmittel
- Möglichkeiten
- Motiv

Ein paar lokale Angriffsformen

Nicht technische Angriffe

Social Engineering

Üblicherweise wird bei Social-Engineering versucht die Realität im Sinne des Angreifers zu formen. Dies geschieht üblicherweise über:

- Ausnutzen von Automatismen und “normalem” Verhalten.
- Prozessausnutzung
  Kann (muss aber nicht) auch mit gefälschten Artefakten erfolgen.
- Ausnahmesituation
  - Dringlichkeit (“Ich benötige dringend…”)
  - Wichtigkeit (“Der Chef will…”)
  - Einschränkungen (z.B. Gehstöcke, Rollstuhl oder “Im Moment kein Zugriff”)

Die verwendeten Angriffsvektoren sind üblicherweise:

- Physisch
- Per üblicher Kommunikation (z.B. Telefonisch, Email, Brief oder FAX)
- Über Dritte (z.B. Managementpersonen sind häufig Türöffner)

Ein paar lokale Angriffsformen

Technische, lokale Angriffe

Einsatz spezieller Hardware

Wenn spezielle Hardware zum Einsatz kommt wird üblicherweise das lokale Vertrauensverhältnis von Hardware ausgenutzt:

- Spezielle Speichersticks (z.B. mit CD-ROM-Emulation, Tastaturen oder Soundkarten)
- Netzwerk- oder Tastaturen-Traps

Ein paar lokale Angriffsformen

Technische, lokale Angriffe

Einsatz von Software

Bei Software wird entweder eine Schwachstelle bei der Plattform oder beim Benutzer ausgenutzt:

- Der Benutzer wird zu schädigendem Verhalten animiert (einräumen von Admin-Rechten bei der Installation).
  - Eine “coole” App auf dem Telefon installieren.
  - Der Benutzer soll sich selber schützen und deshalb Dateien löschen (?)
- Die mangelhafte Prüfung einer Grenze wird ausgenutzt (typischerweise Exploit). Beispiele hierfür sind:
  - Buffer Overflows
  - Zip-Bomb
  - External entity attack

Repetition und Aufgabe

Nächster Block

Labor "Lokale Attacken"

Nächster Termin

Einreichen Übung 1 vor Beginn der Lektion 8 am 04.11.2025 (in 49 Tagen)