Fachhochschule Nordwestschweiz
Hochschule für Technik

Cyber Security Labor (cysL)

Inhalt

Inhalt

Vorbereitung

Recherche

Es ist relativ einfach eine DDoS-Attacke durchzuführen. Überlegen sie sich mögliche Szenarian eine solche abzufedern.

Zum lesen oder anschauen ...

Denial of Service
Eine Kurzeinführung in DDoS (Interessant sind vor allem die Seiten 25-37 und 44)

Begriffe

(Distributed) Denial of Service.

Spass mit Sicherheit

der Blaster-Wurm

der Blaster Wurm (2003)

Abbildung: Programmieren mit Google

Quelle: By admin - http://nuevovirus.info/virus-blaster/, Public Domain, https://commons.wikimedia.org/w/index.php?curid=17225105

Nicht mehr ganz so aktueller Anlass

Die Key Reinstallation und Coppersmith Attacke

Key Reinstallation Attacks

- Wesentlich schlimmer als die Schwäche ist der beiläufig entdeckte Bug im WPA-Supplicant. (Betrifft primär Linux und Android)
- Mehr Details unter `https://www.youtube.com/watch?v=Oh4WURZoR98`

Nicht mehr ganz so aktueller Anlass

Schwäche in den Infineon Chips

Return of the Coppersmith Attack

- Es wurde eine Schwachstelle in den Infineon-Chipsets identifiziert.
- Die Schwachstelle hat zur Folge, dass generierte RSA-Schlüssel gegenüber der Coppersmith-Attacke anfällig sind.
- Die Schwachstelle betrifft unter anderem viele TPM-Module und alle Pässe und IDs von Estland.

Die (D)DoS-Angriffe

Die Angriffsarten

Angriffsarten

- Aushungern von Resourcen
  - CPU
  - Disk
  - Netzwerkbandbreite
    Wird häufig über Bot-Netze oder Reflektions-Attacken erreicht. Reflektionsattacken betreffen typischerweise UDP- und ICMP-Dienste.
- Dienste Funktionsunfähig machen
  - PDoS
    Vor allem bei Netzwerk-Hardware angewandt. Über einen modifizierten Firmware-Upload wird typischerweise ein Gerät ge-“bricked”.

Die (D)DoS-Angriffe

Die Smurf-Attacke

Die SMURF-Attacke

Die Smurf Attacke ist eine traditionelle Amplifikator-Attacke.

- Ein Ping-Paket (mit falschem Absender) und grossem Payload wird an eine Directed-Broadcast-Adresse gesendet.
- Die Antwort wird von mehreren Teilnehmern in diesem Netz an das Ziel gesendet.

Die (D)DoS-Angriffe

Die DNS-Flooding-Attacke

Verschiedene DNS-Flooding-Attacken

Weil DNS via UDP funktioniert und häufig umfangreiche Antworten gibt sind sie nur schwer zu kontrollieren. Sie bilden einen guten Amplifikator für eine Attacke.
Es gibt zwei typische Vorgehen beim Fluten mittels DNS:

- Fluten eines Zieles mittels DNS-Antworten (DNS wird als Aplifikator verwendet)
- Fluten eines DNS mit (häufig negativen) Anfragen um die zugehörigen Dienste nachhaltig zu stören.

Die (D)DoS-Angriffe

Der CIH-Virus

CIH

War der Name eines der wenigen Spezies dieses Programmtyps, welche tatsächlich Hardware “bricken” konnte. Er überschrieb bei der Aktivierung teile des BIOS.

Stuxnet

Stuxnet war ebenfalls ein solcher Vertreter. Er zerstörte die Gaszentrifugen des Urananreicherungsprogrammes im Iran.

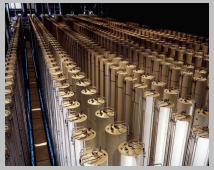

Abbildung: Eine vergleichbare Analge der Ukraine

Quelle: Aus Wikimedia (PD)

Repetition und Aufgabe

Nächster Block

Theorieblock “Mail und DNSSEC”

Nächster Termin

Einreichen Übung 1 vor Beginn der Lektion 8 am 04.11.2025 (in 82204 Tagen)