

Cyber Security Labor (cysL)



Inhalt

Vorbereitung

Spass mit Sicherheit

der Blaster-Wurm

Nicht mehr ganz so aktueller Anlass

Die Key Reinstallation und Coppersmith Attacke

Die (D)DoS-Angriffe

Die Angriffsarten

Die Smurf-Attacke

Die DNS-Flooding-Attacke

Der CIH-Virus

Repetition und Aufgabe

Vorbereitung

Spass

Blaster-Wurm

Almanal

Krack

(D)DoS-Angriffe

Angriffsarten

Smurf

DNS-Flooding

CIH

Repetition

Recherche

Es ist relativ einfach eine DDoS-Attacke durchzuführen. Überlegen sie sich mögliche Szenarien eine solche abzuwehren.

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.

Vorbereitung

Spam

Blaster/Worm

Alkaloid

Krack

0Day-Exploit

Aggraffieren

Smurf

DNS-Flooding

CRH

Regulation

Spass mit Sicherheit

der Blaster-Wurm

der Blaster Wurm (2003)

```

0 00 00-6D 73 62 6C mshl
0 6A 75-73 74 20 77 ast.exe I just w
9 20 4C-4F 56 45 20 ant to say LOUE
0 62 69-6C 6C 79 20 YOU SAN!! billy
0 64 6F-20 79 6F 75 gates why do you
3 20 70-6F 73 73 69 make this possi
0 20 6D-61 6B 69 6E ble ? Stop makin
E 64 20-66 69 78 20 g money and fix
7 61 72-65 21 21 00 your software!!
0 00 00-7F 00 00 00 ♠ ♡ ▶ H △
0 00 00-01 00 01 00 ♠_♠_ @ @ @
0 00 00-00 00 00 46 á@ L F
C C9 11-9F E8 08 00 ♦ jêèù- r f p
0 00 03-10 00 00 00 +▶ H ` @ ♠ ♡ ▶
3 00 00-01 00 04 00 b♥ Õ ♠ ♡ @ ♦

```

Abbildung: Programmieren mit Google

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

Sicherheit

Spam

Blaster-Worm

Alsmat

Krack

@Duck-Agilla

Agg@Barten

Smurf

DNS-Flooding

CBH

Regulation

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=0h4WURZoR98>

Vorbereitung

Spam

Blaster/Worm

Alkali

Krack

0Day-Agents

Angreifer

Sensor

DNS-Flooding

CBH

Regulation

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.

Angriffsarten

- ▶ Aushungern von Ressourcen
 - ▶ 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”.

Vorbereitung

Spam

Blaster/Worm

AbuseIT

Krack

DDoS-Angriffe

Angriffsarten

Smurf

DNS-Flooding

CRIT

Reputation

Die SMURF-Angriffe

Die Smurf Attacke ist eine traditionelle Amplifikator-Angriffe.

- ▶ 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.

Vorbereitung

Spam

Blaster/Worm

Stuxnet

Keack

Stuxnet

AngryFlooder

Smurf

DNS-Flooding

CRIT

Regulation

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 Amplifikator 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.

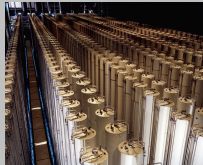


Abbildung: Eine vergleichbare Analge der Ukraine

Quelle: Aus Wikimedia (PD)

Nächster Block

Theorieblock “Mail und DNSSEC”

Nächster Termin

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

Vorbereitung

Spam

Blaster/Worm

Attacks

Crack

00Hack-Agents

Angreiferarten

Smurf

DNS-Flooding

CSF

Repetition