

DDoS Detektion und Mitigation

Volker Tanger, Managing Security Consultant



Set-List

- 1 Deine Schuld
- 2 Out of the Frying Pan and Into the Fire
- 3 Beat It



Deine Schuld

Deine Schuld

Password, 1 2 3

- Admin-Schnittstelle mit Passwort im Internet erreichbar, srsly?
- Passworte: leer / Default / Dictionary / herleitbar (MAC) / einheitlich

Deine Schuld

Password, 1 2 3

- Admin-Schnittstelle mit Passwort im Internet erreichbar, srsly?
- Passworte: leer / Default / Dictionary / herleitbar (MAC) / einheitlich

Wer ander'n eine Backdoor gräbt

- „Versteckte“ Adminzugänge (Sercomm-Router)
- „geheime“ Admin-Passworte im ROM
- ILO, Seriell-Konsolen, Modems (Wardialing)...

Deine Schuld

Password, 1 2 3

- Admin-Schnittstelle mit Passwort im Internet erreichbar, srsly?
- Passworte: leer / Default / Dictionary / herleitbar (MAC) / einheitlich

Wer ander'n eine Backdoor gräbt

- „Versteckte“ Adminzugänge (Sercomm-Router)
- „geheime“ Admin-Passworte im ROM
- ILO, Wardialing, Seriell-Konsolen, ...

One-Way to Hell

- Nur 1 Leitung, keine Redundanz/Ausweichmöglichkeiten
- Alles in 1 Subnetz (Mastercard, eBay-DNS, .mil-DNS)

Out of the Frying Pan and Into the Fire

Out of the Frying Pan and Into the Fire

... und es hat ***KNACK*** gemacht

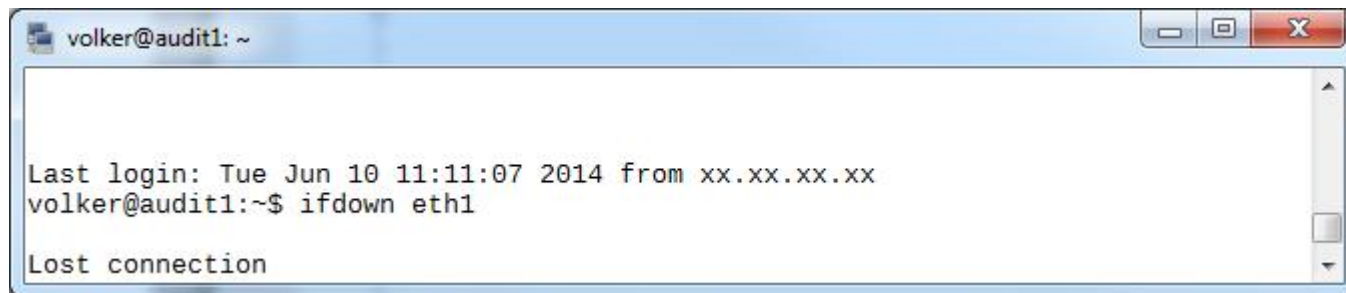
- Das ist Bodo mit dem Bagger und er baggert noch



Out of the Frying Pan and Into the Fire

... und es hat ***KNACK*** gemacht

- Das ist Bodo mit dem Bagger und er baggert noch
- Am falschen Ast gesägt



```
volker@audit1: ~  
  
Last login: Tue Jun 10 11:11:07 2014 from xx.xx.xx.xx  
volker@audit1:~$ ifdown eth1  
Lost connection
```

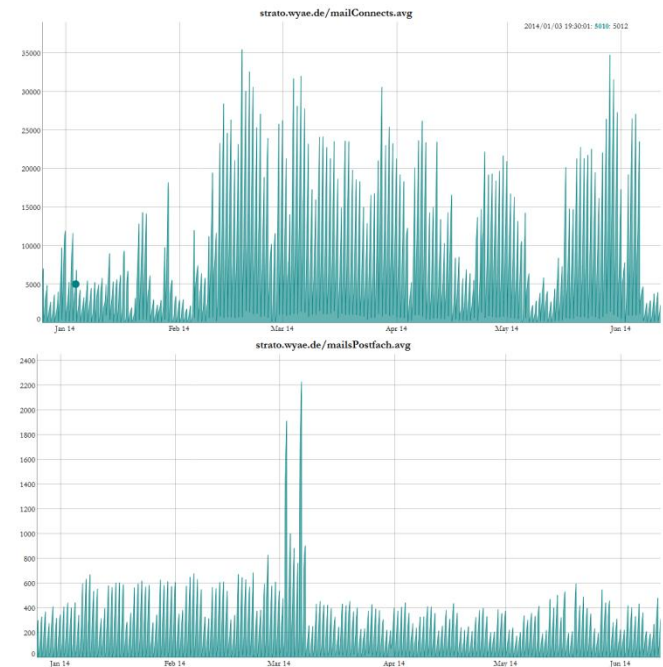
...oder auch ein Patch von Ferne aus einverspielt

Out of the Frying Pan and Into the Fire

... und es hat *KNACK* gemacht

Heute hier, morgen dort

- Spam-Wellen = Modeerscheinungen
- Ramp-Up über den Tag
- Ver-X-fachung der normalen Last
- Änderung über Wochen
- „normale“ Leistungsreserve reicht meist aus



Out of the Frying Pan and Into the Fire

... und es hat *KNACK* gemacht

Heute hier, morgen dort

Die perfekte Welle – von unten ‘drunter

- Ramp-Up über 1-3 Stunden
- Start: Oft zu Arbeitsbeginn
- Dauer: einige Stunden, dann vorbei
- Oft: vom eigenen Marketing versenkt
- Twitter, Facebook, ... (Virales Marketing)
- Slashdot / Heise / Fefes Zeitbindernetzwerk
- Seltener: Online-Demo



Out of the Frying Pan and Into the Fire

... und es hat *KNACK* gemacht

Heute hier, morgen dort

Die perfekte Welle – von unten 'drunter

We're goin' down, down, down

- Gezielter Angriff (auch amplified), bis 400 Gbit/s
- Ramp-Up in wenigen Sekunden/Minuten
- Dauer: meist wenige Stunden bis Tage
- Billig zu haben (\$200 für 1 Tag 100.000 Zombies = 10-100Gbit/s)

Beat It

Beat It

Shadow on the Wall

- Projekte mit fehlenden Messwerten oder belastbaren Mengengerüsten
- Flurfunk zu kommenden „tollen“ Projekten / Leuchtturmprojekte
- Risikosysteme: „nicht anfassen!“ / „zu kritisch!“ / „nicht ersetzbar“
- Unbequem eng: fehlende Reserven / Redundanzen
„läuft doch...“ / „hat bisher immer gereicht...“

Einfach mal den Admin fragen?

Vorher?

Beat It

Shadow on the Wall

Drums of Doom

- Monitoring: Schwellwerte, Trends
- automatische, zeitnahe Logfile-Auswertung
- Alarme! **Alarme!!** Alarme!!!
- ggfs. automatische Abwurf- / Umschalt-Fahrten / Reboots

Beat It

Shadow on the Wall

Drums of Doom

PAL = Problem anderer Leute

- WWW gehostet / CDN
- DNS gehostet (hidden primary) – woanders!
- Mail über Filter (eleven, antispameurope, ...) oder extern (beliebt in den USA: Gmail)

Klassisches Outsourcing / Cloud-Lösungen

Beat It

Shadow on the Wall

Drums of Doom

PAL = Problem anderer Leute

TEAM = Toll, Ein Anderer Macht's

- Firewalling, SynFlood-Protection (auf Provider-Seite)
- Loadbalancing, Cluster, Reverse Proxy
- getrennte Server (WWW / Shop @ Ritter Sport)
- Backup-Leitungen (Shiften von einer auf die andere)
- Umrouten von (Sub)Netzen (BGP), Blackholing
- DNS-Umrouten / RoundRobin

Beat It

Shadow on the Wall

Drums of Doom

PAL = Problem anderer Leute

TEAM = Toll, Ein Anderer Macht's

Vorbereitung ist das halbe Leben

- Skalierbarkeit, Leistungsreserven (virtuell/umsteuerbar)
- vorbereitetes Peering/Routing,
- Abwurfplan / Anfahrplan, statische Kopie der Webseite, 4xx & 5xx Fehlermeldungen am HTTP-Server
- Filterbox / QoS-Drossel bei/mit Provider
- Hochlast-tauglich: optimierte Webseiten, Last-Test verifiziert, Cacheing, ...macht Sites auch schneller+attraktiver

Beat It

Shadow on the Wall

PAL = Problem anderer Leute

TEAM = Toll, Ein Anderer Macht's

Drums of Doom

Vorbereitung ist das halbe Leben

Friends Will Be Friends

- Verträge abklopfen / überprüfen, ggfs. wechseln
- Partner-Kontakte aufstellen & pflegen, *BEVOR* man sie braucht
- Notfall-Übungen / Tests => Verbesserungen
(extrem: Simian Army bei Netflix)

Set-List

Deine Schuld

- Password, 1 2 3
- Wer ander'n eine Backdoor gräbt
- One-Way to Hell

Out of the Frying Pan and Into the Fire

- ... und es hat *KNACK* gemacht
- Heute hier, morgen dort
- Die perfekte Welle – von unten 'drunter
- We're goin' down, down, down

Beat It

- Shadow on the Wall
- Drums of Doom
- PAL = Problem anderer Leute
- TEAM = Toll, Ein Anderer Macht's
- Vorbereitung ist das halbe Leben
- Friends Will Be Friends

DANKE!

Volker Tanger

HiSolutions AG

Bouchéstraße 12
12435 Berlin
tanger@hisolutions.com
www.hisolutions.com
+49 30 533 289-0



Weitere Informationen & Quellennachweise

Weitere Informationen

- Volker.Tanger@wyae.de
- <http://www.wyae.de/volker.tanger/papers/>

Fotos

- Bagger: http://de.wikipedia.org/wiki/Bagger#mediaviewer/Datei:CAT_325_Raupenbagger.JPG
- Terminal-Screenshot, Mail-Graphen (MoSShE): Volker Tanger
- Ritter Sport Mett
<http://www.ritter-sport.de/blog/2014/04/01/sonderedition-ritter-sport-mett-ab-sofort-erhaltlich/>
- Saturn MP3-Shop
<http://www.heise.de/newsticker/meldung/Saturns-MP3-Shop-dem-Ansturm-nicht-gewachsen-894193.html>

...mit der Bitte um Entschuldigung an:

- Die Ärzte, Galaxy feat. "The Voice" , AC-DC, Meatloaf , Klaus Lage , Mike Krüger , Hannes Wader , Juli , Bruce Springsteen , Michael Jackson , Mike Oldfield , Manowar , Queen
- Sprichworte und Sponti-Sprüche