von Tarpits und Honeypot

DarkNET vs. TOR – Ist die Welt gefährlicher?

- 1. anonymes Surfen durch TOR
- 2. es gibt versteckte TLD .onion / hidden services
- 3. anonymes Suchen durch disconnect.me oder grams

Cloud - CaaS - Crime as a Service

- Webinterface
- Konfigurationassistent
- PayPal, VISA
- Widerrufsrecht
- Zufriedenheitsgarantie
- Schadsoftware entwickeln ist KEINE Straftat

Ziel der Angriffe

- Geld
- Botnetze aufbauen
- Schaden/Sabotage
- Mal gucken was geht …
- Ruhm

Aktuelle Angriffeszenarien

- Viren
- Trojaner
- Malware
- **Exploits**
- **Ransomware**
- Phishing
- …

Ist eine SPI-Firewall überfordert?

- Filter basiert nur auf MAC, IP, Port, …
- Nächster Schritt ist Contentfilterung
- Aber wie scanne ich verschlüsselte Pakete?

- Aber man fühlt sich sicher!

Wegwerfen, Ablenken, Bremsen und Untersuchen

- Fragwürdige Pakete sind noch keine Gefahr
- Doch was soll damit geschehen?

Blackhole-Route

VERWERFEN

- Pakete weitergeleitet und letztlich verworfen
- Angreifer bekommt keine Benachrichtigung

Tarpits - Teergrube

ABLENKEN und BREMSEN

- Verbreitungsgeschwindigkeit von Würmern verringern
- täuschen große Netzwerke vor
- verlangsamen oder behindern so beispielsweise die Verbreitung von Internetwürmern oder die Durchführung von Netzwerkscans
- offene Proxyserver emulieren und – falls jemand versucht, Spam über diesen Dienst zu verschicken – den Sender dadurch ausbremsen, dass sie die Daten nur sehr langsam übertragen.

HoneyPot - Grundkonzept

ABLENKEN und UNTERSUCHEN

- Als Honigtopf oder auch englisch honeypot wird eine Einrichtung bezeichnet, die einen Angreifer oder Feind vom eigentlichen Ziel ablenken soll oder in einen Bereich hineinziehen soll, der ihn sonst nicht interessiert hätte. Der Ursprung stammt aus der Überlegung, dass Bären mit einem Honigtopf sowohl abgelenkt als auch in eine Falle gelockt werden könnten.

- Köder oder Ablenkung
- JEDER Nutzer eines HoneyPot ist ein Angreifer

Low Interactive HoneyPot

- Simulation von Diensten
- Simulation von Hosts
- Simulation von Netzen

- Geringer Aufwand
- Leicht zu erkennen

- Idee: Verstecke einen Baum in einem Wald

Nmap – Fingerprints vs. RFCs

- Die FIN probe
- Der BOGUS flag Test
- Sammeln von TCP Sequenznummern
- Don't Fragment bit
- TCP Initial Window
- ACK Sequenznummern
- ICMP Error MessageQuenching
- ICMP Message Quoting
- Integritaet von Antworten auf ICMP-Fehlermeldungen
- Type of Service
- Die Behandlung von Fragmenten
- TCP Optionen
- Ausnutzen der zeitlichen Abfolge
- Widerstandsfaehigkeit gegen SYN gegen Flooding

Hight Interactive HoneyPot

- Komplette virtualisierte oder physische Strukturen
- Angreifer sind ausdrücklich Willkommen
- Zusätzliche Strukturen zur Beobachtung und Dokumentation

Installation - Simulation vs. Virtuell vs. Physisch

- Art der Implementierung

- Tiefe der Darstellung

Klassische Zielgruppe - **Kunden**

- Eindringlinge / Gefahren erkennen
- IDS / IPS

Klassische Zielgruppe – **Security Anbieter**

Next Generation Firewall

- FW analysiert und reagiert nicht allein
- Synchronized Security
- Heatbeat-Technologie zwischen Host und Firewall
  - Endpoint testen sich selbst
  - Bedrohungen werden der FW gemeldet
  - Firewall sperrt den Client aus

- Gartner …
- Sophos XG Firewall und Central Endpoint = Sophos Intercept X.

Zielgruppe – Warum nicht auch eine CISCO NetAcademy?

- Thema kann den Teilnehmern nah gebracht werden
- Angreifbare komplexe Struktur ohne Aufwand
- Ideal für Netzwerkanalyse
- Schutzstrukturen schaffen und testen
- (win)honeyd 1.5

Install … honeyd 1.5c … Niels Provos … 2007

- winhoneyd … inkl. GUI …. Oder
  - WinPcap 3.1 installieren
  - WinHoneyd v1.5c installieren
  - nmap.prints evtl. bearbeiten (Fingerprints)
  - Honey.conf bearbeiten
  - runhoneyd.cmd bearbeiten
  - Honeyview installieren
- Honeyd

  Linux installieren

  # apt-get install honeyd farpd
  /etc/default/honeyd …
  /etc/honeypot/honeyd.conf …
  # /etc/init.d/honeyd start

edit the INTERFACE and NETWORK
Hauptkonfigurationsdatei

Konfiguration … WindowsHost

Windows NT4 web serverserver
Create windows
Set windows personality"Windows NT 4.0 Server SP5-SP6“
Add windows tcp port 80 „perl scripts/iis-0.95/iisemul8.pl“
Add windows tcp port 139 open
Add windows tcp port 137 open
Add windows udp port 137 open
Add windows udp port 135 open
Set windows tcp action reset
Set windows default udp action reset

bind 10.0.1.51 windows
bind 10.0.1.52 windows

Konfiguration … LinuxHost

FTP Linux server template

create linuxftp

set linuxftp personality "Linux 2.4.7 (X86)"

set linuxftp default tcp action reset

set linuxftp default udp action block

set linuxftp default icmp action open

add linuxftp tcp port 21 "sh /usr/share/honeyd/scripts/unix/linux/suse8.0/proftpd.sh $ipsrc $sport $ipdst $dport"

bind 192.168.1.50 linuxftp

Konfiguration … CISCO Router

```
### Cisco Router
create router
set router personality "Cisco IOS 11.3 - 12.0(11)"
set router default tcp action reset
set router default udp action reset
add router tcp port 23 "/usr/bin/perl scripts/router-telnet.pl"
set router uid 32767 gid 32767
set router uptime 1327650

bind 10.0.0.100 router
bind 10.0.1.100 router
bind 10.1.0.100 router
bind 10.0.0.200 router
bind 10.2.0.100 router
bind 172.20.254.1 router
```

Konfiguration … Network

First Router

route entry 10.0.0.100 network 10.0.0.0/16

Link dahinter

route 10.0.0.100 link 10.0.1.0/24

Weiterer Router

route 10.0.0.100 add net 10.1.0.0/16 10.0.1.100

Links dahinter

route 10.0.1.100 link 10.1.0.0/16

Lets SCAN and PROTECT

Netze, Hosts, Services, fake oder real?

Quellen

http://bruteforcelab.com/getting-started-honeyd.html

http://www.honeyd.org/configuration.php

http://www.honeyd.org/config/honeyd.conf.networks

http://www.faz.net/aktuell/wirtschaft/macht-im-internet/verbrechen-4-0-crime-as-a-service-14510568.html

https://www.heise.de/newsticker/meldung/Europol-warnt-vor-Crime-as-a-Service-aus-der-Cloud-3341301.html

https://www.tutonaut.de/anleitung-wie-komme-ich-ins-darknet/

https://www.pressebox.de/pressemitteilung/sophos-gmbh/Praedikat-Leader-Sophos-UTM-ueberzeugt-mit-neuen-Technologien-auch-Gartner/boxid/813644

https://partian.co/Downloads/Fortinet/magic_quadrant_for_unified_t_269677.pdf