Snort – Quo vadis?

Kurzer Überblick über aktuelle Entwicklungen rund um das Open Source IDS Snort

Edin Dizdarević, System Developer (edin.dizdarevic@interActive-Systems.de)
www.interActive-Systems.de/security

Snort – Quo vadis?

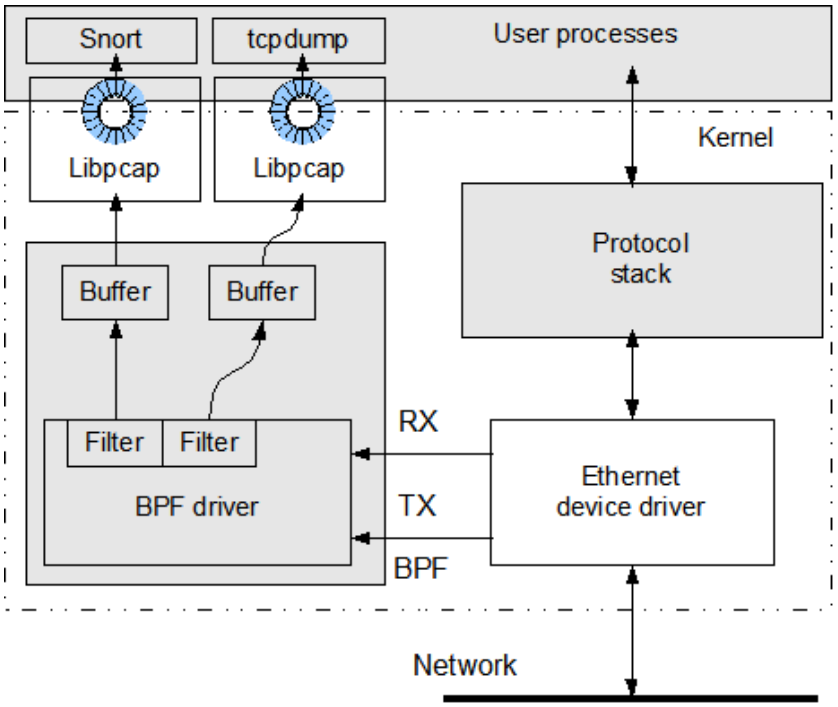
Der Ursprung

- Martin Roesch – Hauptentwickler von Snort, Gründer von Sourcefire Inc.
- Motivation:
  - Paket-Sniffer/Netzwerk-Analyse-Tool
    - Tcpdump-Ersatz mit lesbarerer Ausgabe
  - Paket-Logger
    - Netzverkehr „mitschneiden“ (verschiedene Output-Formate)
  - NIDS
  - IPS – Snort Inline (ab Snort 2.3.0)
  - Lightweight
- Aktuelle Version: 2.3.0

Snort – Quo vadis?

Basics: Snort als NIDS

- Libpcap-/Libnet-Basierend
  - Unter Linux: BPF/LSF BSD Packet Filter/ Linux Socket Filter
  - Am TCP/IP-Stack des Kernels vorbei Netzwerkpakete empfangen/erzeugen
- Signaturbasiert
  - Beispielsignatur:




```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS \
(msg:"WEB-ATTACKS /bin/ps command attempt"; \
flow:to_server,established; uricontent:"/bin/ps"; \
nocase; classtype:web-application-attack; sid:1328; rev:6;)
```

Snort – Quo vadis?

Basics: Snort-Subsysteme

- Präprozessoren
  - Aufbereitung des Datenstroms (der TCP/IP-Stack)
  - Traffic Normalization (HTTP, telnet)
  - Protocol Anomaly Detection
  - Zustandsinformationen einer Verbindung (Flow)
  - Sfportscan (Portscan-PP)
  - Weitere…
- Detection Engine (Pattern Matching Engine)
  - Erledigt die Kernaufgabe
- Output Stage – Ausgabe
  - Alerting
  - Logging
- Snort-Inline: Intrusion Prevention-Funktionalität
- Flexresp-Modul – „Quasi Intrusion Prevention“
- Analyse und Auswertung:
  - Gehört nicht zu Snort

Snort – Quo vadis?

Basics: Präprozessoren

- Aufbereitung des Datenstroms
  - TCP-Stream Reassembly (stream4)
    - Telnet, SSH, …
  - Defragmentation (frag2)
  - Traffic Normalization
    - HTTP-Decoding (http_decode, http_inspect)
    - Telnet-Decoding (telnet)
    - …
  - Protocol Anomaly Detection
    - Fehler beim Defragmentieren (z.B. Fragmentation Overlap-Angriff)
    - Unsinnige Flag-Kombinationen bei TCP-Paketen (SYN+FIN, …)
    - ...
  - Portscans
    - …

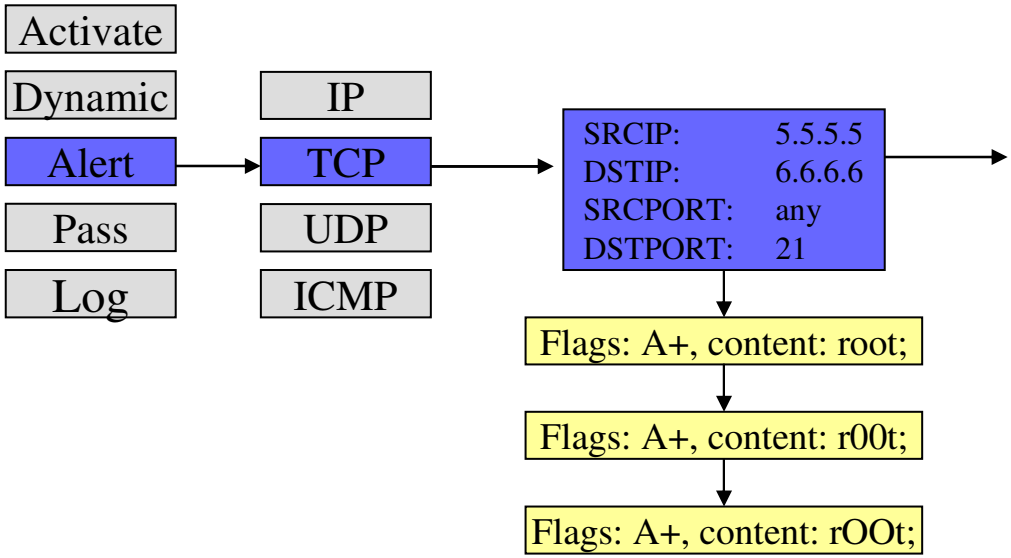
Snort – Quo vadis?

Basics: Pattern Matching Engine

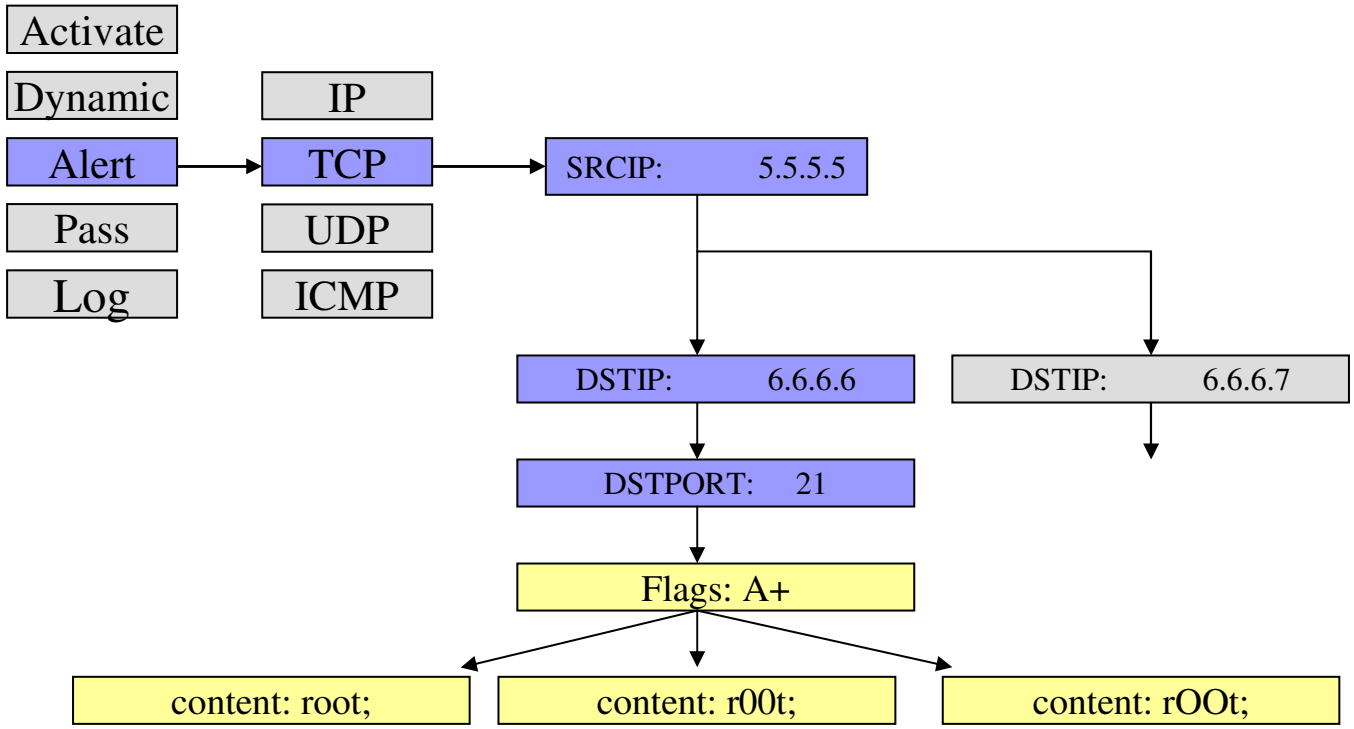
- Multiple Alerts per Packet/Stream
  - Event Queue
    - Max_queue, log, order_events
  - Thresholding
    - Limit, threshold, both
- Detection Plugins – modular (ip_same_check, isdataat,…)
- Verschiedene Suchalgorithmen implementiert (config searchmethod:)
  - Modified Wu-Manber (mwm, Default)
  - Aho-Corasick (ac, evtl. schneller aber Speicherintensiv)
  - Boyer-Moore (lowmem, für kleine Regelsätze gut)
- Discrete Options
  - Sofortiger Abbruch der Suche bei Nicht-Übereinstimmung
    - Ack, dsize, flags, icode, itype, ...

- Beispiel Funktionsweise der Detection Engine:
  - 3 ähnliche Regeln:
    - alert tcp 5.5.5.5 any -> 6.6.6.6 21 (Flags: A+, content: root;)
    - alert tcp 5.5.5.5 any -> 6.6.6.6 21 (Flags: A+, content: r00t;)
    - alert tcp 5.5.5.5 any -> 6.6.6.6 21 (Flags: A+, content: rOOt;)

- Detection Engine Snort 1.x:



- Detection Engine Snort 2.x:



- snort_inline
  - Empfängt Pakete von Netfilter (Queue)
  - Zusätzliche Aktionen für Regeln:
    - Drop, reject, sdrop
  - Kann mit Einschränkungen Pakete modifizieren
  - Arbeitet zustandsorientiert
  - Anpassung der Regeln erforderlich (SnortConfig, Oinkmaster)
  - Neue Regelordnung:
    - ->activation-> dynamic-> drop-> sdrop-> reject-> alert-> pass-> log
  - Kann auf einer Bridge auf Layer 2 arbeiten
  - Erfordert Libnet 1.0.2 (veraltet)

- Flexresp – Flexible Response
  - Keine „echte“ Intrusion Prevention
  - Versucht Verbindungen durch TCP-Reset und ICMP-Fehlermeldungen zu desynchronisieren / beenden
  - Die „bösen“ Pakete kommen u. U. trotzdem durch
    - Je nach Angriff reicht u. U. bereits ein Paket aus (Slammer)

Snort – Quo vadis?

Snort: Interessante Add-Ons

- Hogwash
  - „Paketschrubber“
  - Kann auf einer Bridge arbeiten
  - Bait & Switch für Honeypots
  - Wird nicht weiterentwickelt (Snort 1.8.1)
- SnortSam
  - Intrusion Prevention-Lösung mit Snort
  - Patch für Snort und Firewall-Modul
  - Arbeitet mit Iptables, EBtables, IPchains, Checkpoint, Cisco, ...
- Snort Wireless
  - Fügt Snort das WIFI-Protokoll hinzu
  - Kann Rogue-APs, AdHoc-Netze und Netstumbler erkennen

Snort – Quo vadis?

Snort: Output-Plugins

- Unified (Binär), sehr schnell,
  Einsatz mit Barnyard oder Mudpit (Postprocessing)
- Tcpdump
- ASCII
  - Syslog
  - Alert
- Unix_sock
- Unix_sock_db: FLoP
  - Das mächtigste Output-Plugin
  - Sehr schnell
  - Für professionellen Einsatz mit
    vielen Sensoren sehr gut geeignet

Snort – Quo vadis?

Snort: Output-Plugin FLoP

- Entwickelt und gepflegt von Dirk Geschke
- Sehr ausgereift (Aktuelle Version 1.4.1)
- Patch für Snort und eine Programmsuite
- Nimmt Snort viel Arbeit ab
- Loggt viele Infos (MAC-Addressen)
- Alerts und Logs schnell und mit wenig Overhead auf die zentrale DB übertragen
- Pakete aus der DB wieder herstellbar (Ethereal)
- Automatisierte Mailbenachrichtigung
- Kann auf Diskless-Sensoren eingesetzt werden
- Resistent gegen Alert-Flooding
- ...

Snort – Quo vadis?

Snort: Policy-Management

- IDS Policy Manager (Win)
- Oinkmaster (mächtiges Perl-Skript mit GUI)
- SnortCenter (Enterprise-Lösung)
- SneakyMan (Regeleditor)

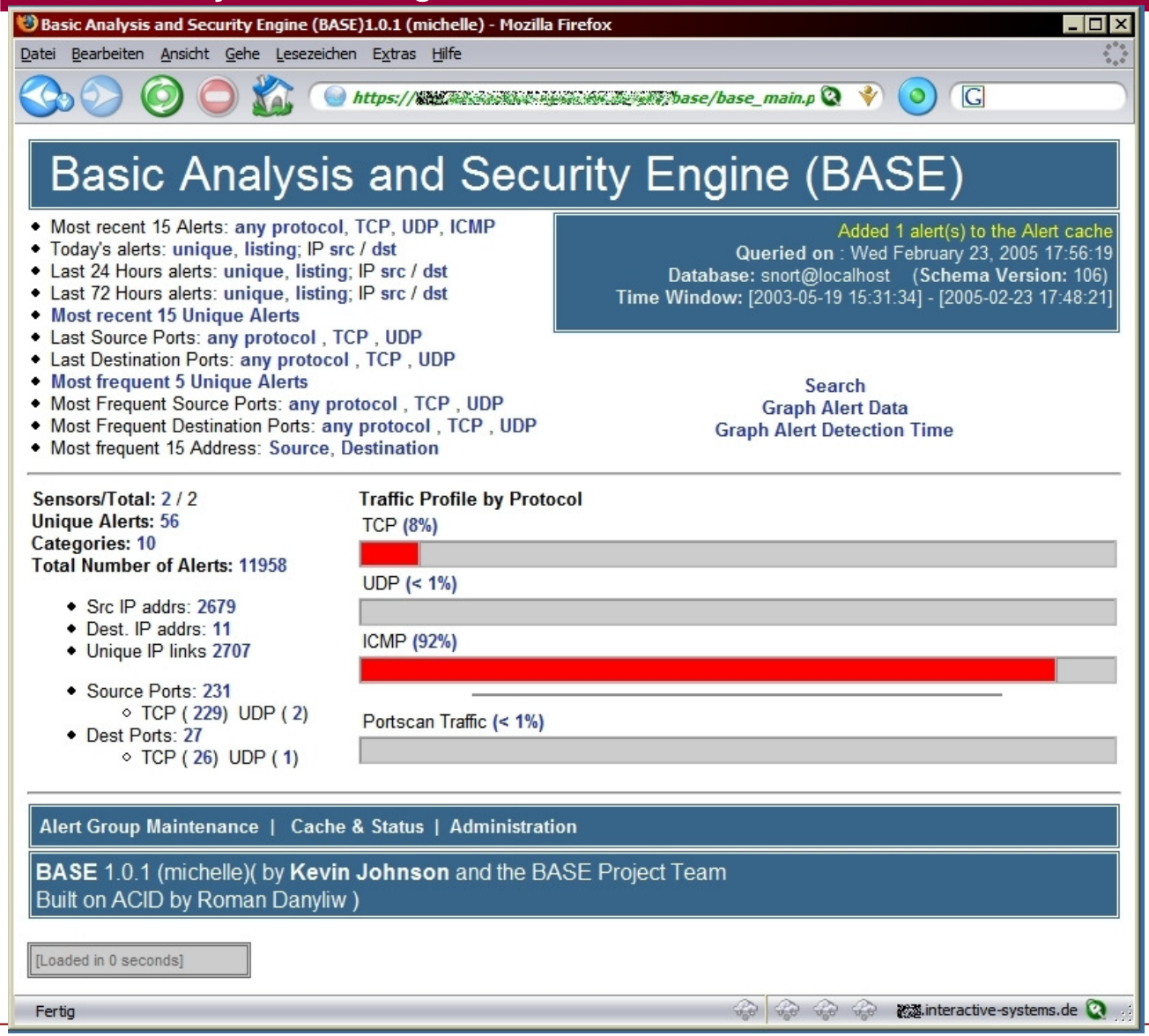
Snort – Quo vadis?

Snort: Analyse-Werkzeuge

- ACID
- BASE
  - Fleißige ACID-Weiterentwicklung
  - Aktuell Version 1.0.2
- SGUIL
  - Zeitnahe Analyse und Auswertung von Alerts
  - Output-Plugin für Barnyard
  - Tcl/Tk-GUI
  - GUI-Server

Snort – Quo vadis?

Snort: Analyse-Werkzeuge



Snort – Quo vadis?

Snort: Aktuelle Entwicklung

- Neue Präprozessoren (Auswahl):
  - http_inspect
    - Löst http_decode und unicode ab
  - Frag3
  - Flexresp2
  - Sfportscan
  - ...

Snort – Quo vadis?

Snort: HTTP Inspect

- HTTP Inspect
  - Normalisiert HTTP (HEX, Unicode, …)
  - Profile Apache/IIS
  - Erkennt HTTP auf nicht typischen Ports
  - Erkennt (unerwünschte) Proxynutzung
  - Erkennt viele Evasion-Techniken (Siehe Literatur)
    - Hex Encoding: %41= „A“
    - Double Percent HE:%2541 = „A“
    - Double Nibble HE:%%34%31 = „A“
    - First Nibble HE: %%341 = „A“
    - …

- Frag3
  - Target Based IP-Defragmentation durch Profile
    - First (Win)
    - Last (Cisco)
    - Bsd (FreeBSD, IRIXe, OS/2, …)
    - bsd-right (HP JetDirect)
    - linux
  - Schneller als frag2 (bis zu 250%)
  - Besser (aber aufwändiger) konfigurierbar

Snort – Quo vadis?

Snort: Flexresp2

- Flexresp2
  - Neuentwicklung: Flexresp2 != Flexresp
  - TCP-Reset dest/src/both
  - ICMP net/host/port/all unreachable
  - Brute-Force TCP desync
  - Libdnet-Basierend
  - Z. Z. ein Patch für Snort

Snort – Quo vadis?

Snort: Sfportscan

- Sfportscan
  - Benötigt Informationen vom PP Flow
  - Kann viele Nmap-Basierte Scans erkennen
    - TCP/UDP/IP Portscans
    - Decoy Portscans
    - Distributed Portscans
    - Portsweeps
    - Filtered Portscans
  - Die „Empfindlichkeit“ einstellbar Low/Medium/High
  - Generiert ein Pseudo-Paket zum Loggen
  - Erlaubt weitgehendes Feintuning

Snort – Quo vadis?

Snort: Aktuell

- Aktuell:
  - SF-Regeln dürfen nicht mehr kommerziell weitervertrieben werden
- Martin Roesch:
  - New configuration parser and rules language
  - New action stage API
  - Development towards Target Based ID
  - Neue Policy ohne Neustart (far future)

Snort – Quo vadis?

Snort: Literatur

Literatur:

- R. W. Stevens, TCP/IP Illustrated, Vol. 1, The Protocols
- HTTP IDS Evasions Revisited, Daniel J. Roelker, Sourcefire Inc.
- Active Mapping: Resisting NIDS Evasion Without Altering Traffic, U. Shankar, V. Paxson, http://www.icir.org/vern/papers/activemap-oak03.pdf

Links (http://):

Snort:	www.snort.org
FLoP:	www.geschke-online.de/FLoP/
SnortSam:	www.snortsam.net
SnortConfig	www.shmoo.com
MMAPed Libpcap:	public.lanl.gov/cpw/
Mudpit:	www.fidelissecurity.com/techtalk/mudpit.asp
IDS-Tools:	www.forinsect.de/ids/ids-tools.html

Animation Suchalgorithmen:

Aho Corasick:	www-sr.informatik.uni-tuebingen.de/~buehler/AC/AC.html
Boyer Moore:	www-sr.informatik.uni-tuebingen.de/~buehler/BM/BM.html

Fragen?