esse

Security for Systems Engineering – VO 10: Intrusion Detection & Intrusion Prevention

Florian Fankhauser

Agenda

- Grundlagen von Angriffserkennungssystemen
- IDS und IPS
  - Aufbau
  - Prinzipielle Arten
- Erkennungsmethoden für Angriffe
- Beispiele für Angriffe auf IDPS
- Beispiel für ein IDPS: Snort
- Honeypots und Honeynets

Aspekte der IT-Sicherheit

- Angriffe auf die IT-Sicherheit
- Sicherheitsmaßnahmen
- Schutzbedarf von Daten, Bedrohungs- und Risikoanalyse
- Implementierung, Test
- Betrieb
- Plan-Do-Check-Act (PDCA)

Sind wir nun sicher?

Sind wir nun sicher?

Wir wissen: 100%ige Sicherheit gibt es nicht.

Angriffe finden statt.

$\rightarrow$ *Erkennung von Angriffen*

Ziele von Angriffserkennungssystemen

- Unterstützung der Aufrechthaltung der IT-Sicherheit während des Betriebs
- Möglichst frühe und genaue Erkennung von möglichst vielen Angriffen/böswilligen Aktivitäten, d.h. Verletzungen der Security Policies, mit guter Darstellung der Incidents
  - z.B. Erkennung von Würmern, unautorisiertem Eindringen in ein Netzwerk oder in ein System, unautorisierte Benutzung von Systemen durch valide AnwenderInnen
- Dadurch Schadensreduzierung bei Angriffen
- Erkennung von Fehlkonfigurationen (z.B. von Firewalls)
- Abschätzung der Gefahrenlage für ein Unternehmen
- Abschreckung von AngreiferInnen, aber auch MitarbeiterInnen

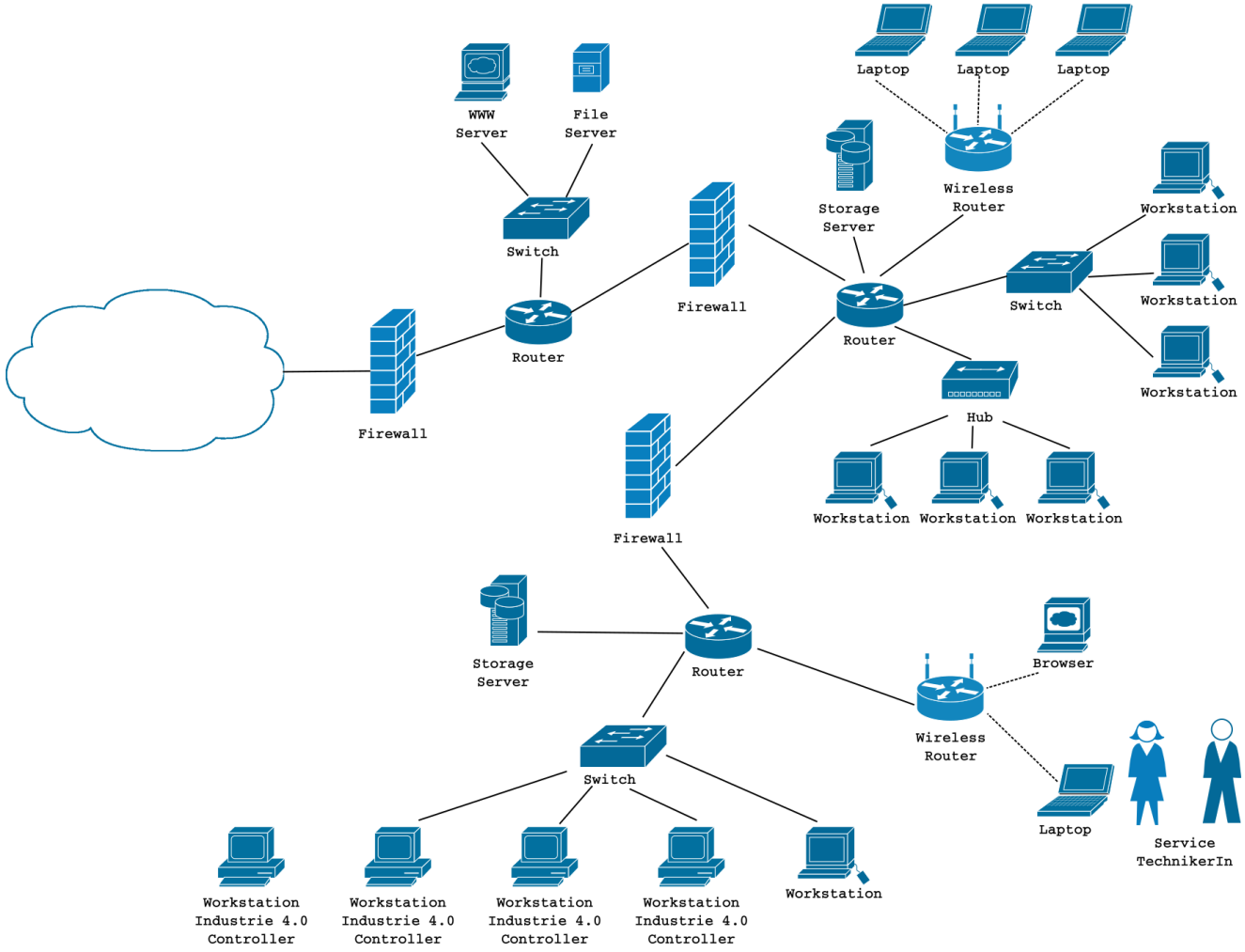
Wiederholung: IDS vs. IPS

- Intrusion Detection System (IDS)
  - Erkennung von Angriffen
    - Signaturen
    - Anomalie-Erkennung
  - Senden eines Alarms bei erkanntem Angriff
- Intrusion Prevention System (IPS)
  - Zusätzlich zur Erkennung: Automatische Ergreifung von Maßnahmen
    - z.B. Aktivierung einer Firewall-Regel
- Zusammengefasst immer wieder bezeichnet als Intrusion Detection Prevention System (IDPS)

Aufbau von IDS/IPS

- Ereigniskomponente
  - Aufnahme von Daten einer Umgebung über Sensoren
    - Auswahl der Daten, Platzierung der Sensoren
- Sicherungs- bzw. Aufzeichnungskomponente
  - Durchführung der Protokollierung der Erkenntnisse
- Analysekomponente
  - Analyse der gesammelten Daten und ggf. Auslösung eines Alarms
- Monitor- und Aktionskomponente
  - Aufbereitung und Durchführung von Aktionen
- $\rightarrow$ *(Manuelle) Reaktion auf Aktion*

Netzwerk-Plan: Platzierung der Sensoren



Prinzipielle Arten von IDPS

- Host-based IDPS (HIDPS)
  - Betrachtung der Eigenschaften und der Events eines einzelnen Hosts
- Network-based IDPS (NIDPS)
  - Betrachtung des Netzwerkverkehrs für Netzwerksegmente oder Geräte und Analyse der Netzwerk-, Transport- und Applikationprotokolle
- Network Behavior Analysis IDPS (NBA)
  - Betrachtung des Netzwerkverkehrs oder Statistiken über den Netzwerkverkehr und Analyse unerwarteter Netzwerkflüsse
- Wireless IDPS (WIDPS)
  - Betrachtung des Netzwerkverkehrs für WLAN-Netzwerke

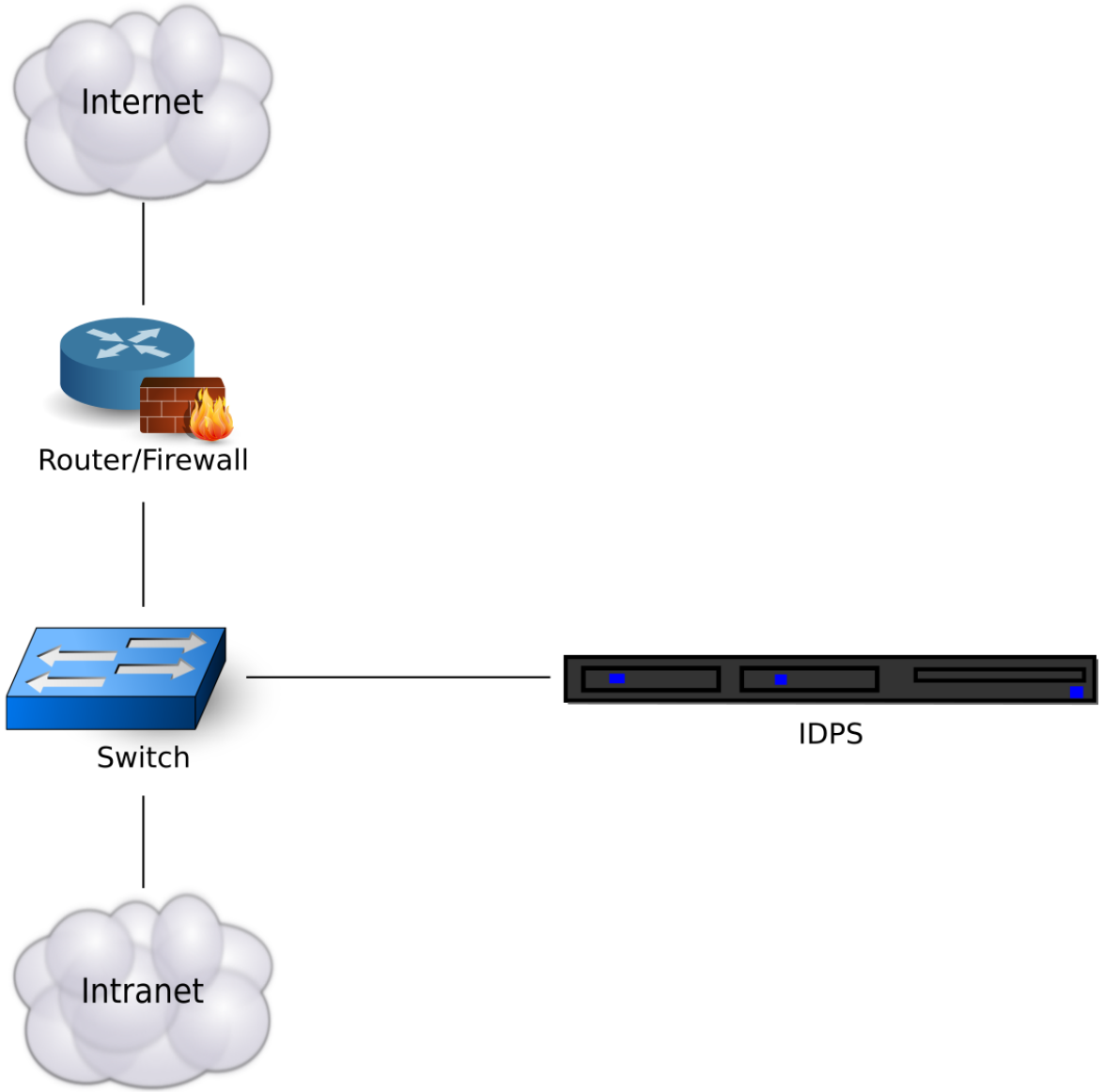
Host Based Intrusion Detection System (HIDS)

- HIDS ist direkt am Endsystem
- HIDS hat Sichtweise des Endsystems
- Monitoring von z.B.
  - Registry
  - Filesystem
  - Prozessen
  - Memory
  - System Calls
  - Logs
- Angriffe z.B. auf Signaturen, Deaktivierung HIDS

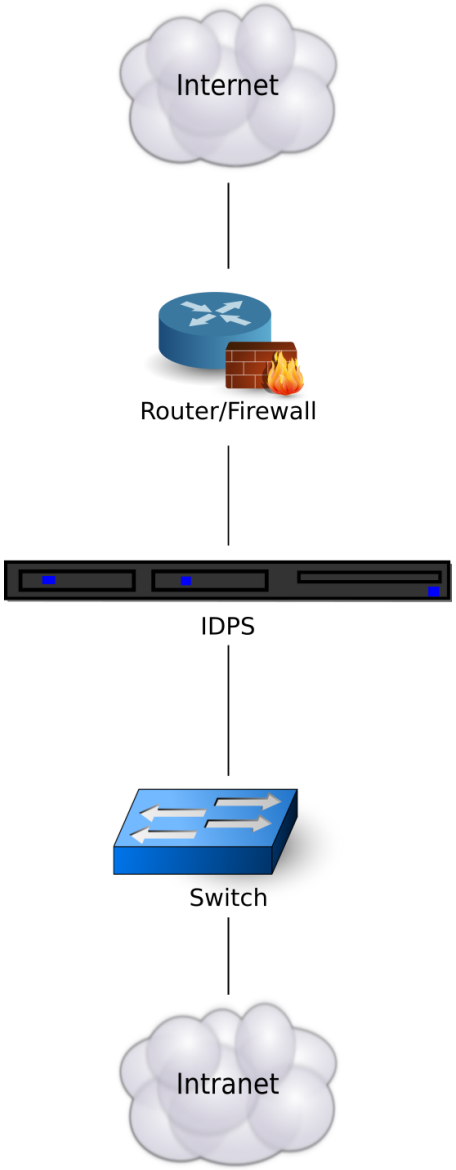
Network Intrusion Detection System (NIDS)

- Analyse des gesamten Traffics im Netz („Mitlauschen“)
- Sichtweise des gesamten Netzwerkes
- Portscans, Hostscans, Zugriffe auf spez. Ports
- Herausforderung der Positionierung
- End-2-End Verschlüsselung als Problem
- Abhängig vom Traffic hohe Last, welche zu Sicherheitsproblemen führen kann!

Passives IDS/IPS



In-Line IDS/IPS



Erkennungsmethoden für Angriffe

- Signature-based detection: „Signature-based detection is the process of *comparing signatures* against observed events to identify possible incidents.“
- Anomaly-based detection: „Anomaly-based detection is the process of comparing definitions of what *activity* is *considered normal* against observed events to identify significant deviations.“
- Stateful Protocol Analysis: „Stateful protocol analysis is the process of comparing predetermined profiles of *generally accepted definitions of benign protocol activity* for each protocol state against observed events to identify deviations.“

(Vergleiche Scarfone und Mell)

Signatur-basierte Erkennung

- Erkennung von Angriffen an Hand von bekannten Signaturen
- Eine Signatur ist ein Pattern, das einen Angriff identifiziert
- Vorteil
  - Weit verbreitet und einfach zu implementieren
- Nachteile
  - Für jeden Angriff muss eine Signatur erstellt werden
  - Erkennung von unbekannten Angriffen mit Signaturprüfung nicht möglich
  - Viele False Positives und False Negatives, wenn Signaturen nicht korrekt sind

Anomalie-basierte Erkennung

- Modelle von einem erwarteten Verhalten von Usern oder Systemen
- Jede Abweichung von diesem Modell wird als Angriff interpretiert
- Vorteil
  - Erkennung von unbekannten Angriffen
- Nachteile
  - Oft hohe False Positive Rate
  - Definition von „normalem“ Systemverhalten, um Anomalien zu erkennen, ist aufwändig
  - Angriffe mit „normalem“ Systemverhalten werden nicht erkannt

Anomalie-basierte Erkennung – Beispiel

- Beispiel übliche User-Aktivität:
  - Login am System zwischen 09:00-10:00 Uhr
  - Abruf von Mails
  - Lesende Datenbankzugriffe
  - Pause zwischen 12:00-13:00 Uhr
  - Zugriffe auf das Filesystem

Anomalie-basierte Erkennung – Beispiel

- Beispiel übliche User-Aktivität:
  - Login am System zwischen 09:00-10:00 Uhr
  - Abruf von Mails
  - Lesende Datenbankzugriffe
  - Pause zwischen 12:00-13:00 Uhr
  - Zugriffe auf das Filesystem
- Beispiele für Anomalie-Erkennung:
  - User-Login erst ab 18:00 Uhr
  - Start von Debugger und Compiler
  - ...

Angriffe auf IDPS: Netzwerk-Ebene

- Tiny Fragment Attack (z.B. Port # im 1. Fragment nicht vorhanden)
- Fragment Overlap Attack (z.B. Port # im 1. Fragment unauffällig, im 2. überschrieben)
- Stealth Scans

Angriffe auf IDPS: Applikations-Ebene

- Kleine Änderungen, die inhaltlich keine Auswirkungen haben, aber Signatur ändern
  - GET /AllDasIstUninteressantUndKommtWeg/../cgi-bin/test.cgi
  - GET /cgi-bin\test.cgi
  - GET /CGI-BIN/test.cgi
- Langsame, kleine Änderungen

Varianten von Angriffserkennungen bei IDS/IPS

- Richtige Erkennung
  - True Positive
  - True Negative
- Falsche Erkennung
  - False Positive
  - False Negative

Maßnahmen bei einer Erkennung eines Angriffs

- Senden eines Alarms (e-mail, sms,. . .)
- Löschung von böswilligen Paketen
- Reset der Netzwerk-Verbindung
- Blockierung des gesamten Traffics
- Abänderung von Paketen

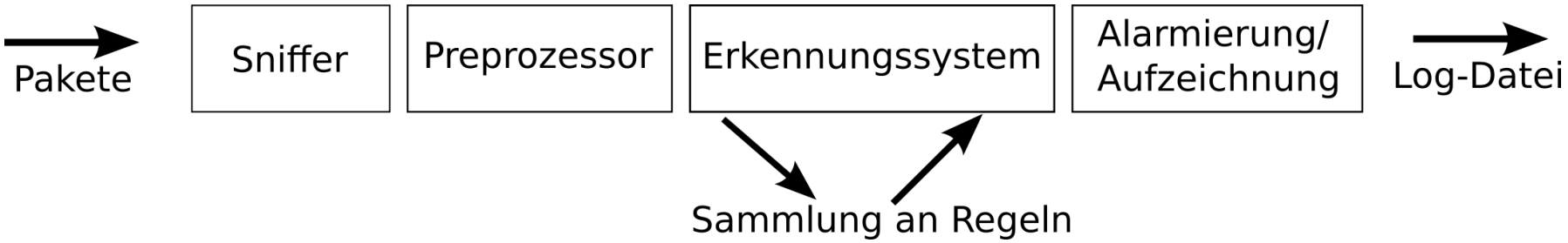
Top 5 IDS-Fehler

- Das [N]IDS kann nicht den gesamten Netzwerk-Datenverkehr sehen.
- Das IDS wurde richtig eingesetzt, aber niemand sieht nach den Alarmen, die es generiert.
- Es gibt keine IDS-Reaktionsregelung.
- Das IDS ist nicht auf seine Umgebung abgestimmt.
- Die Beschränkungen, die der NIDS-Technologie anhaften, werden nicht berücksichtigt.

(Vergleiche Peikari und Chuvakin)

Beispiel: Snort

- Martin Rösch – 1998
- SNORT – `http://www.snort.org/`
- Plattformunabhängiges NIDS bzw. NIPS
- Architektur:



Snort: Regeln

- Zustand oder Bedingung in einem Netzwerk und eine Aktion
- Per Definition besteht eine Regel aus 2 Teilen:
  - Rule Header: Aktion, Pakettyp, Quell- und Ziel-IP-Adresse und einem Quell- und Ziel-Port
  - Rule Option: besteht aus mehreren Options, die den Inhalt eines Pakets überprüfen
- Definition + Beispiel:

action proto src_ip src_port direction dst_ip dst_port (options)

alert tcp $HOME_NET any -> $EXTERNAL_NET 80

Snort-Regeln: Beispiele für Aktionen

- alert: Generierung eines Alarms und Loggen des Pakets
- log: Loggen des Pakets
- pass: Weiterleitung eines Pakets ohne weitere Prüfung
- drop: Blockierung und Loggen des Pakets
- reject: Blockierung, Loggen und TCP-Reset oder ICMP Port Unreachable-Nachricht

Snort-Regeln: Optionen

- Eine oder mehrere Options sind möglich und mit Beistrich getrennt
- Die Regel trifft nur zu, wenn ALLE Options erfüllt sind
- Beispiele:
  - msg: Titel der Rule in Log-Einträgen (nur Beschreibung)
  - content: Pattern im Payload suchen
  - offset: Durchsucht den content erst ab Position offset
  - ...

Snort: Ersetzung von Paketinhalten

- Nur im In-Line Mode möglich
- Vorsicht: Bei der Ersetzung darf die Content-Length nicht verändert werden
- Beispiel:

```
alert tcp any any <> any 80 (msg: "tcp replace"; content:"
    GET"; replace:"BET";)

alert udp any any <> any 53 (msg: "udp replace"; content: "
    yahoo"; replace: "xxxxx";)
```

Wiederholung: Honeypot und Honeynet

- Honeypots sind eine *ergänzende* Sicherheitsmaßnahme
- Definition
  - „A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.“ (Spitzner)
  - „A security resource who's value lies in being probed, attacked or compromised.“ (Spitzner)
- Kein Produktionssystem
- Kein legitimer Zugriff
- Leichtere Analyse von auftretendem Traffic
- Honeynet ist ein Netzwerk von Honeypots

Honeypots

- 2 grundlegende Arten von Honeypots
  - Honeypots mit geringer Interaktivität --> Simulation
  - Honeypots mit hoher Interaktivität --> reale Systeme

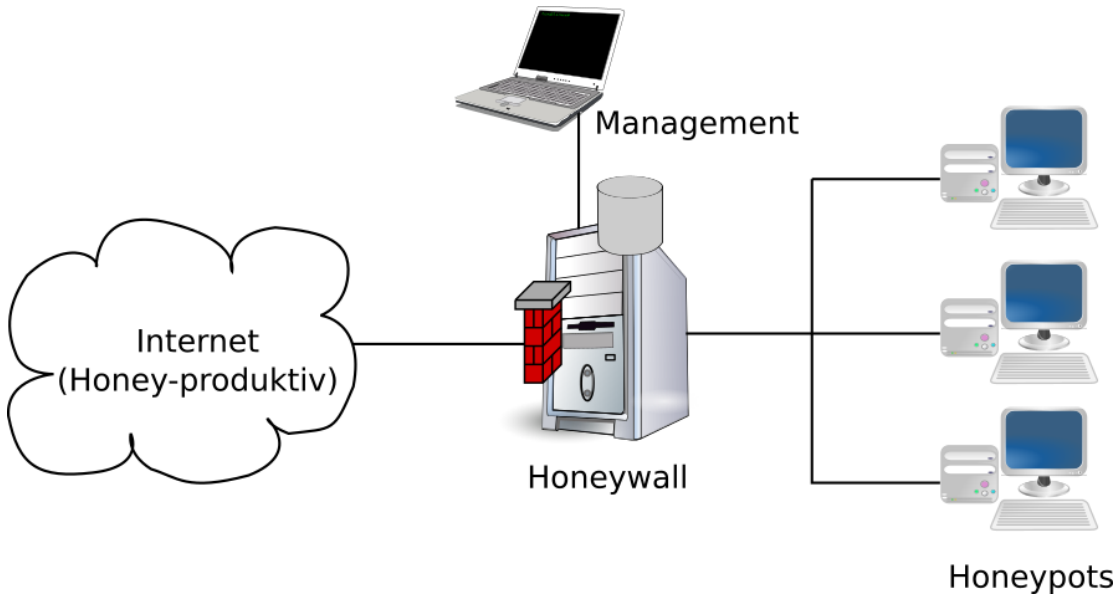
- Honeypot ist ein (reales) System (mit Diensten) z.B. Debian Linux mit FTP Server, Cisco Router mit IOS, Simulation z.B. mit honeyd (`http://www.honeyd.org/`)

Vor- und Nachteile von Honeypots/Honeynets

- Vorteile
  - Eine geringe Datenmenge mit hoher Bedeutung
  - Erkennung neuer Werkzeuge und Taktiken
  - Guter Einsatz in der Forschung
  - Umleitung von verdächtigem Traffic aus Produktion zu Honeypots
- Nachteile
  - Beschränkte Sicht
  - Risiko
  - Aufwand für Überwachung und Analyse

Wiederholung: Aufbau eines Honeynets

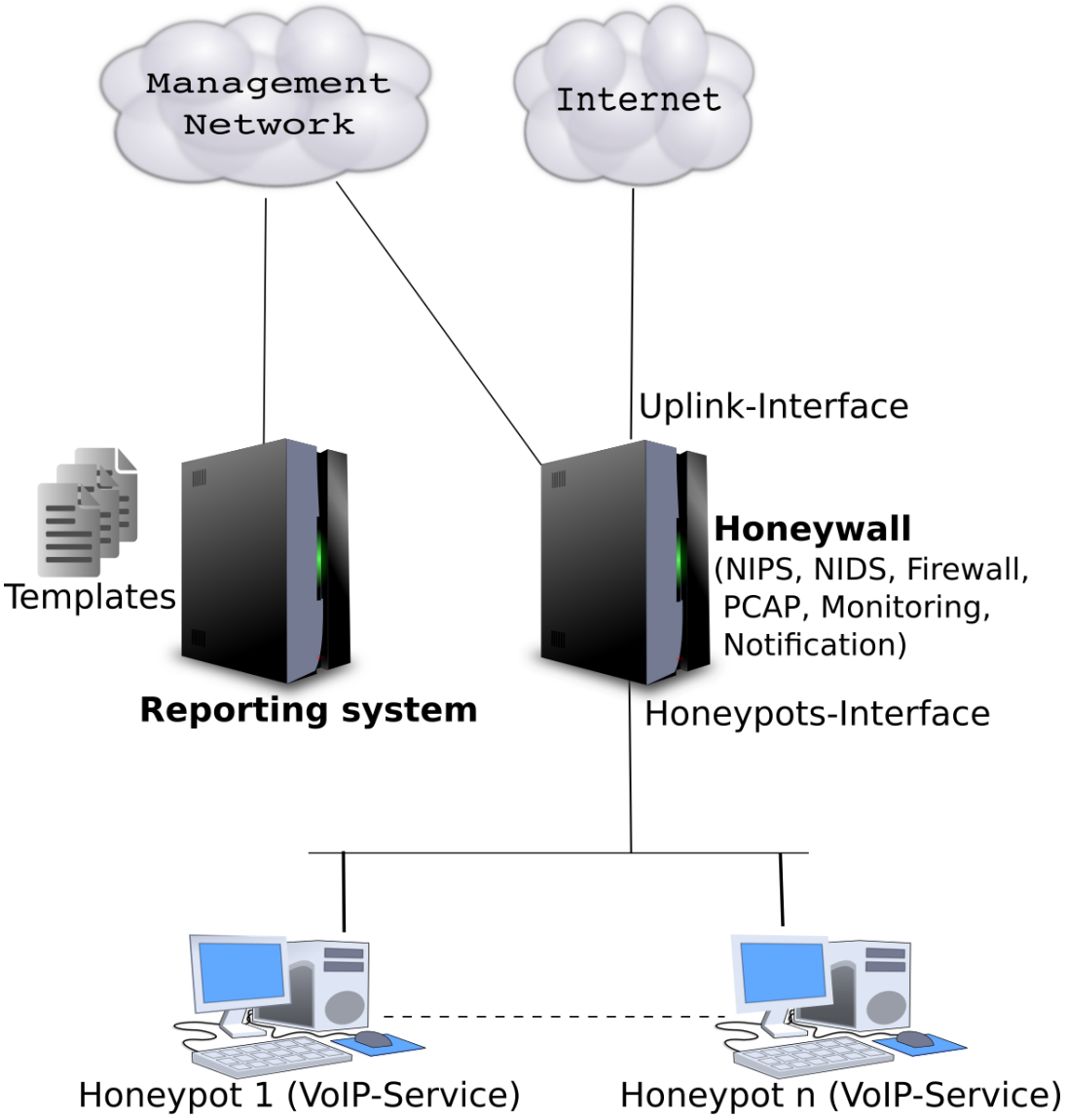
- So etwas wie eine Firewall bzw. ein Gateway (*Honeywall*)
- Verbund von Honeypots mit diversen Diensten



Honeynet in einer Forschungsumgebung

- Ziel: Sammlung so vieler Informationen wie möglich über ein Forschungsgebiet
- Forschungsgebiet ist z.B. Voice over IP (VoIP)
- Schnelle Erkennung von neuen Angriffsmustern durch Aufzeichnung des gesamten Traffics
- Ständig in Betrieb und in Weiterentwicklung

Honeynet in einer Forschungsumgebung – Architektur



Honeynet in einer Forschungsumgebung – Signatur-Verbesserungen

- Reporting-System unterstützt, um Angriffe auswerten zu können
- Verwendung aller Informationen des IDS sowie der Honeypots
- Ableitung von neuen Signaturen
  - Welche Angriffsmuster wurden verwendet?
  - Erkennung von Abweichungen zum „normalen“ Verhalten
- Neue Angriffe vs. Aktualisieren der Signaturen

Honeynet in einer Forschungsumgebung – Ergebnisse

- User-Agents, die für einen Großteil der Angriffe verantwortlich sind
- Untypisches Verhalten:
  - Senden von CANCEL- oder BYE-Paketen vor einem INVITE-Paket
  - Verhalten, nachdem ein Account geknackt wurde
  - ...
- Fazit: Mit Hilfe eines Honeynets kann man sehr viel über die AngreiferInnen und deren Verhalten lernen

Literatur/Quellen – 1/4

- Ross Anderson. *Security Engineering. A Guide to Building Dependable Distributed Systems*. Wiley Publishing, Inc., 2. Auflage, 2008. ISBN 978-0-470-06852-6. `http://www.cl.cam.ac.uk/~rja14/book.html`
- Bruce Schneier. Managed Security Monitoring: Network Security for the 21st Century. *Computers & Security*, 20(6):491–503, 2001
- Richard A. Kemmerer und Giovanni Vigna. Intrusion detection: a brief history and overview. *Computer*, 35:27–30, 2002. ISSN 0018-9162. doi: 10.1109/MC.2002.1012428

Literatur/Quellen – 2/4

- Karen A. Scarfone und Peter M. Mell. SP 800-94 Rev. 1. Guide to Intrusion Detection and Prevention Systems (IDPS). Technischer Bericht, Gaithersburg, MD, United States, 2012. `http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf`
- Andy Oram und John Viega, (Hrsg.). *Beautiful Security*. O'Reilly Media Inc., 2009. ISBN 978-0-596-52748-8
- Cyrus Peikari und Anton Chuvakin. *Kenne deinen Feind. Fortgeschrittene Sicherheitstechniken. Dt. Übers. v. Peter Klicman, Andreas Bildstein und Gerald Richter*. O'Reilly, Köln, 2004. ISBN 3-89721-376-1

Literatur/Quellen – 3/4

- Matt Bishop. *Introduction to Computer Security*. Pearson Education, Inc, 2003. ISBN 0-321-24744-2
- BSI. BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen, 2002. `https://www.bsi.bund.de/DE/Publikationen/Studien/IDS02/index_htm.html`
- Michael Meier. *Intrusion Detection effektiv!* Springer, Berlin Heidelberg New York, 2007
- Honeynet Project. Know Your Enemy: Honeynets. What a honeynet is, its value, and risk/issues involved, 2005. `http://old.honeynet.org/papers/honeynet/`
- Olu Akindeinde. *Security Analysis And Data Visualization*. 2009

Literatur/Quellen – 4/4

- Markus Gruber, Florian Fankhauser, Stefan Taber, Christian Schanes, und Thomas Grechenig. Trapping and Analyzing Malicious VoIP Traffic Using a Honeynet Approach. In *The 6th International Conference on Internet Technology and Secured Transactions (ICITST)*, Seiten 442 –447, Dezember 2011
- `http://www.snort.org/`
- *Die Slides enthalten Teile aus der VO im SS2014 von Markus Gruber.*

Zusammenfassung

- Grundlagen zu Angriffserkennungssystemen
- IDS vs. IPS
- Aufbau, Arten von IDPS
- Erkennungsmethoden für Angriffe
- Beispiele für Angriffe auf IDPS
- Beispiel für ein IDPS: Snort
- Honeypots & Honeynets

Vielen Dank!

https://security.inso.tuwien.ac.at/