Honeypot Architectures for IPv6 Networks

Sven Schindler

Universität Potsdam
Institut für Informatik
Professur Betriebssysteme und Verteilte Systeme

Potsdam, den 9. Dezember 2016

Forschungsfragen

- Welche Ansätze verwenden Angreifer bei der Suche nach Maschinen?

Forschungsfragen

- Welche Ansätze verwenden Angreifer bei der Suche nach Maschinen?
- Wie kann ein IPv6-Adressraum beobachtet und darin interagiert werden?

Forschungsfragen

- Welche Ansätze verwenden Angreifer bei der Suche nach Maschinen?
- Wie kann ein IPv6-Adressraum beobachtet und darin interagiert werden?
- Befindet sich das Protokoll im Fokus von Angreifern?

/34 Darknet Experiment

- 15-monatige Beobachtung eines /34-Addressraums (01/2014 - 03/2015)
- Klassifizierte Angriffe in der Praxis beobachtbar?
- Erwartung: neue und intelligente **Scan-Ansätze**

/34 Darknet Experiment

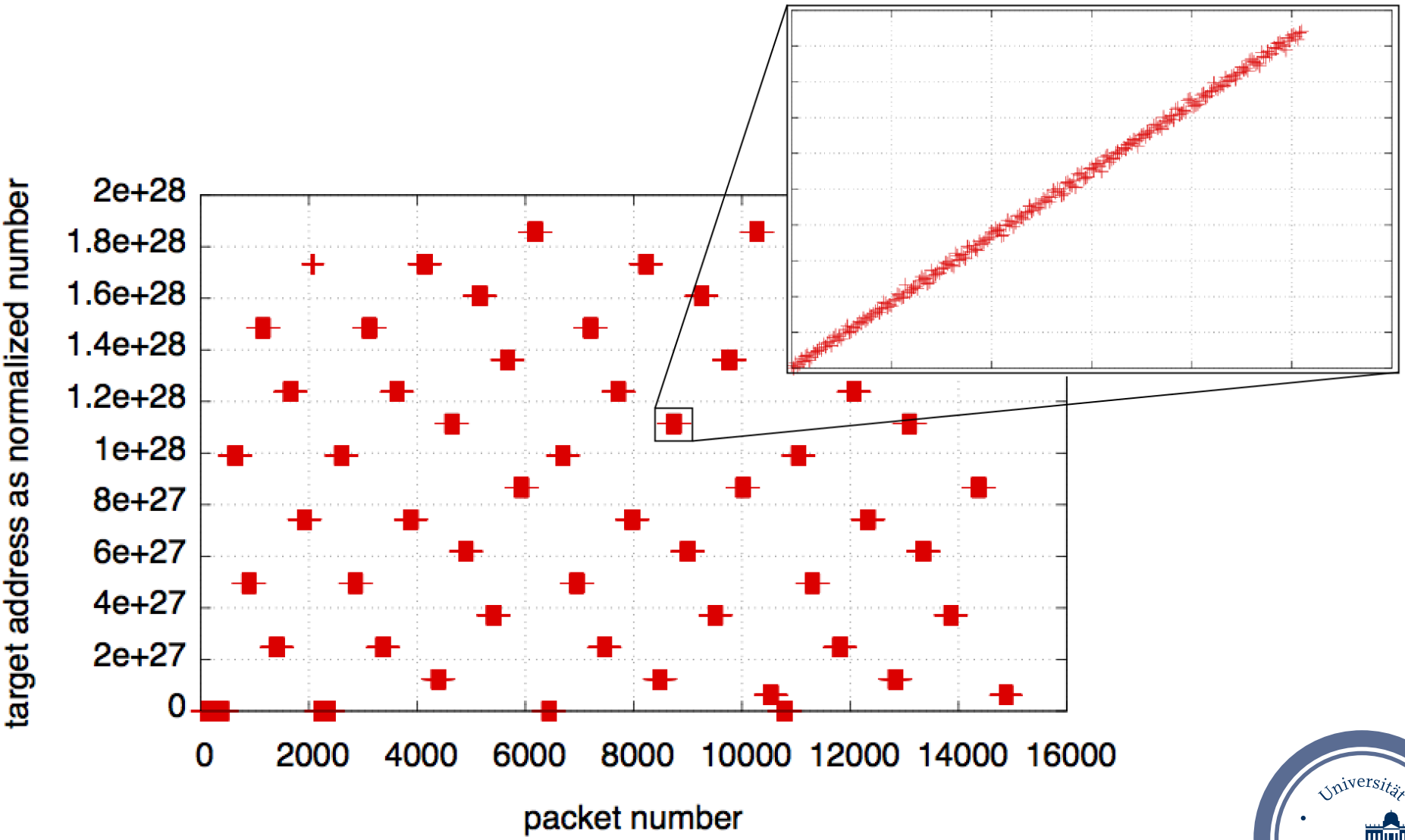
- 15-monatige Beobachtung eines /34-Addressraums (01/2014 - 03/2015)
- Klassifizierte Angriffe in der Praxis beobachtbar?
- Erwartung: neue und intelligente **Scan-Ansätze**
- Beispiele für intelligente Ansätze [4]:
  - Low-byte-Adressen (2001:db8::3)
  - Eingebettete IPv4-Adressen (2001:db8::93.184.216.34)
  - Adressen mit Worteinbettung 2001:db8::cafe or 2a03:2880:2110:df07:face:b00c:0:1
  - Auto-konfigurierte (SLAAC) Adressen (2001:1:1:1:1:11ff:fe11:1/64)

Sven Schindler, Bettina Schnor, and Thomas Scheffler. Hyhoneydv6: A hybrid Honeypot Architecture for IPv6 Networks. *International Journal of Intelligent Computing Research (IJICR),6(2):570–578, 2015, ISSN: 2042-4655.*

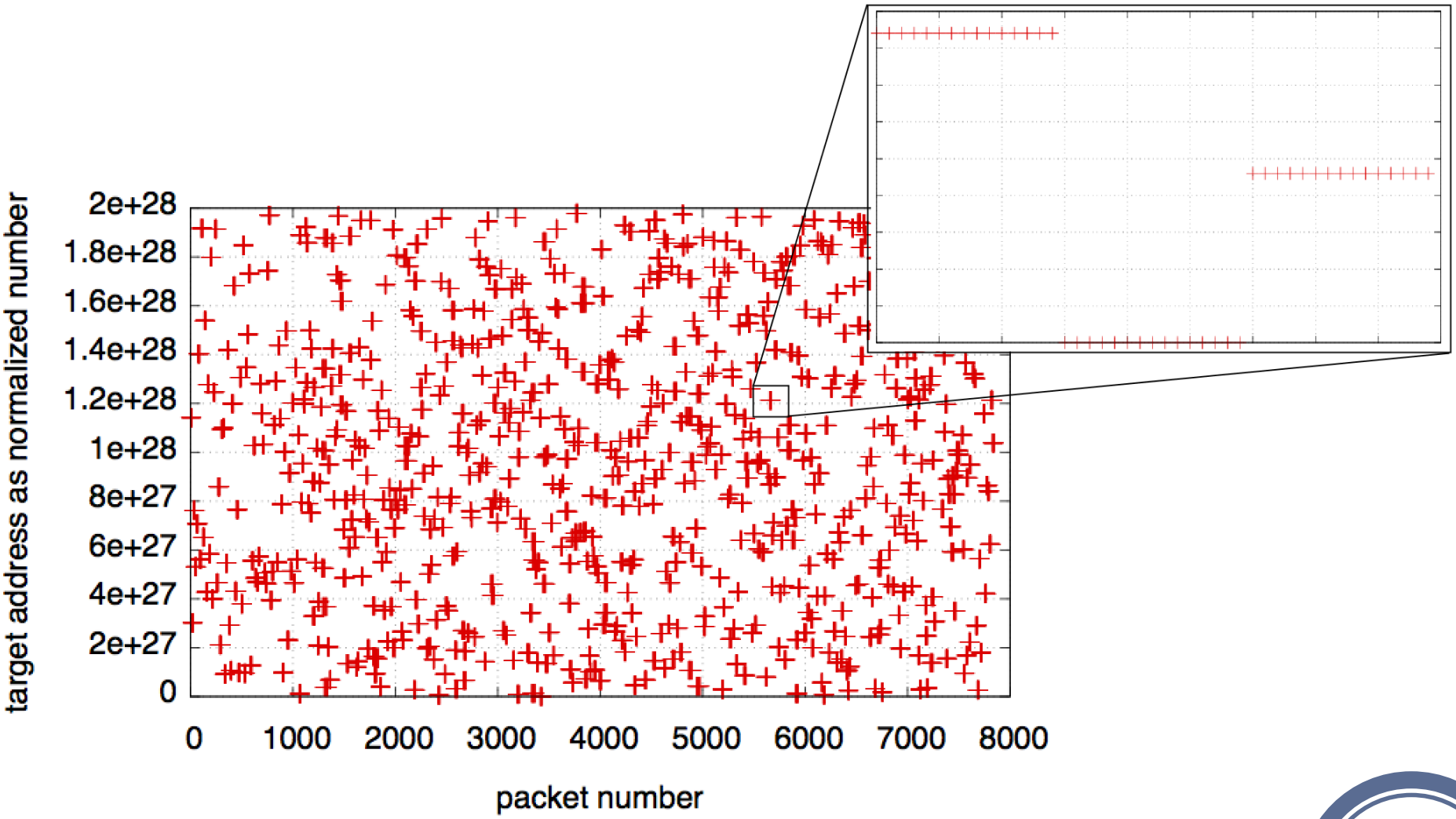
Ergebnisse des Darknet Experiments

- Hauptsächlich großräumige ICMPv6- und TCP-Netzwerkscans von Forschungsinstituten
- Weitestgehend Low-byte-Adressen
- Zwei verschiedene Scan-Ansätze: Linear und anscheinend zufällig
- Keine offensichtlich bösartigen Aktivitäten

Scan-Ansatz I



Scan-Ansatz II



Honeyd

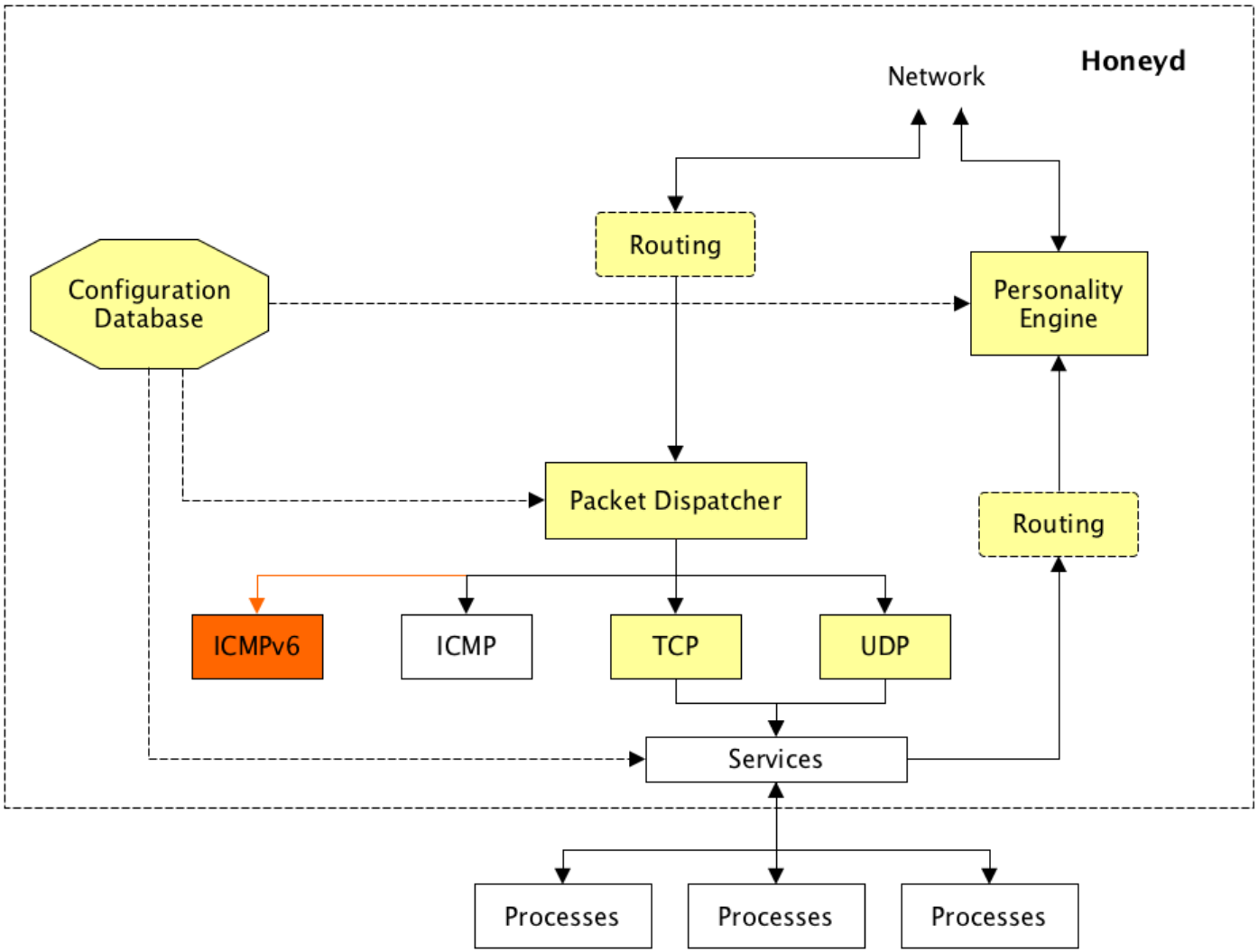
- Open-Source Low-interaction-Honeypot von Niels Provos
- Implementiert eigenen Netzwerk-Stack
- Simulation **großer Netzwerke** mit **tausenden von Maschinen** möglich
- Stellt Framework für Service-Skripte bereit
- Neueste Version v1.5c bietet keine IPv6-Unterstützung

Honeyd

- Open-Source Low-interaction-Honeypot von Niels Provos
- Implementiert eigenen Netzwerk-Stack
- Simulation **großer Netzwerke** mit **tausenden von Maschinen** möglich
- Stellt Framework für Service-Skripte bereit
- Neueste Version v1.5c bietet keine IPv6-Unterstützung
- **Ziel: Implementation eines IPv6-Netzwerkstacks**

Sven Schindler, Bettina Schnor, Simon Kiertscher, Thomas Scheffler, and Eldad Zack, HoneydV6: A low-interaction IPv6 honeypot. *10th International Conference on Security and Cryptography (SECRYPT), Reykjavik, Iceland, 2013.*

Honeydv6-Architektur [8]



Random Request Processing für große IPv6-Adressräume

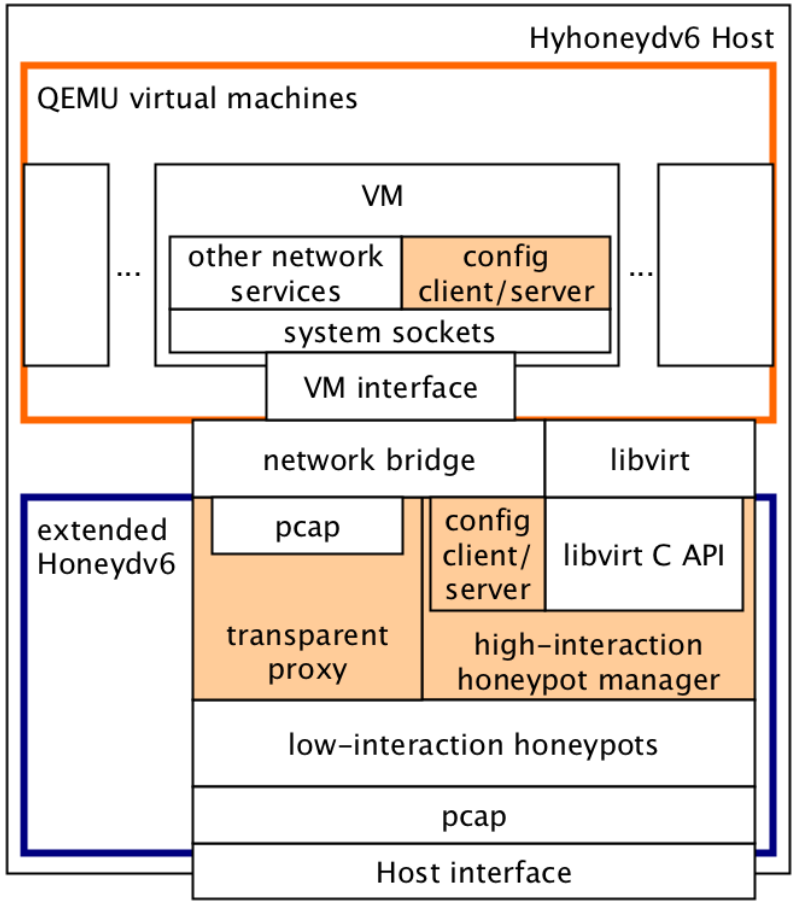
- Honeydv6 implementiert **dynamische Erstellung von virtuellen Maschinen auf Anfrage**
- Konfigurierbare Anzahl und Wahrscheinlichkeit von zu erstellenden Maschinen
- Logging aller Verbindungsversuche

Sven Schindler, Bettina Schnor, Simon Kiertscher, Thomas Scheffler and Eldad Zack. IPv6 network attack detection with HoneydV6. In Mohammad S. Obaidat and Joaquim Filipe, editors, E-Business and Telecommunications, volume 456, pages 252–269. Springer Press, 2014. ISBN: 978-3-662-44787-1.

Anforderungen an IPv6-Honeypots zur Analyse komplexer und proprietärer Netzwerk-Services

- **Bereitstellung authentischer Netzwerk-Services**
  - Keine Service-Simulation
  - Einfache Unterstützung von Protokollen mit Verschlüsselungsmechanismen
- **Abdeckung großer IPv6-Adressräume**
  - Brute-Force-Suche in IPv6-Netzwerken nicht realistisch [2]
  - Dynamische Instanziierung von Honeypots ähnlich zu Honeydv6
- **Kosten/Performanz**
  - Geringe Anzahl von benötigten Maschinen
  - Keine Abhängigkeiten zu Cloud-Anbietern

Hyhoneydv6-Architektur



Sven Schindler, Thomas Scheffler, and Bettina Schnor. Taming the IPv6 Address Space with Hyhoneydv6. In *Proceedings of the World Congress on Internet Security (WorldCIS), Dublin, Ireland, 2015, received Best Paper Award.*

Zusammenfassung

- IPv6-Netzwerke größtenteils frei von bösartigen Aktivitäten
- Eher naive Scan-Ansätze beobachtbar
- Honeydv6 ermöglicht Interaktion mit Angreifern in riesigen IPv6-Netzwerken
- Hyhoneydv6 verbindet Vorteile von Low- und High-Interaction Honeypots für IPv6-Netzwerke

Vielen Dank

Quellen

[1] Fabrice Bellard.
Qemu, a fast and portable dynamic translator.
In *Proceedings of the Annual Conference on USENIX Annual Technical Conference*, ATEC '05, pages 41–41, Berkeley, CA, USA, 2005. USENIX Association.

[2] T. Chown.
IPv6 Implications for Network Scanning.
RFC 5157 (Informational), March 2008.

[3] S. Deering and R. Hinden.
Internet Protocol, Version 6 (IPv6) Specification.
RFC 2460 (Draft Standard), December 1998.
Updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935, 6946, 7045, 7112.

[4] F. Gont and T. Chown.
Network Reconnaissance in IPv6 Networks - draft-ietf-opsec-ipv6-host-scanning-04, June 2014.

[5] Johanna Ullrich and Katharina Krombholz and Heidelinde Hobel and Adrian Dabrowski and Edgar Weippl.
Ipv6 security: Attacks and countermeasures in a nutshell.
In *8th USENIX Workshop on Offensive Technologies (WOOT 14)*, San Diego, CA, 2014. USENIX Association.

[6] M Tim Jones.
Anatomy of the libvirt virtualization library.
IBM developer Works, pages 97–108, 2010.

[7] K. Kishimoto, K. Ohira, Y. Yamaguchi, H. Yamaki, and H. Takakura.
An Adaptive Honeypot System to Capture IPv6 Address Scans.
In *Cyber Security (CyberSecurity), 2012 International Conference on*, pages 165–172, Dec 2012.

[8] Niels Provos and Thorsten Holz.
Virtual Honeypots - From Botnet Tracking to Intrusion Detection.
Addison-Wesley, 2008.

[9] Christian Seifert, Ian Welch, and Peter Komisarczuk.
Taxonomy of honeypots.
Technical report, Victoria University of Wellington, Wellington, 2006.