Man-in-the-Middle-Attacken auf Schicht 2

Johannes Weber | TÜV Rheinland i-sec GmbH

Agenda

- Vorstellung

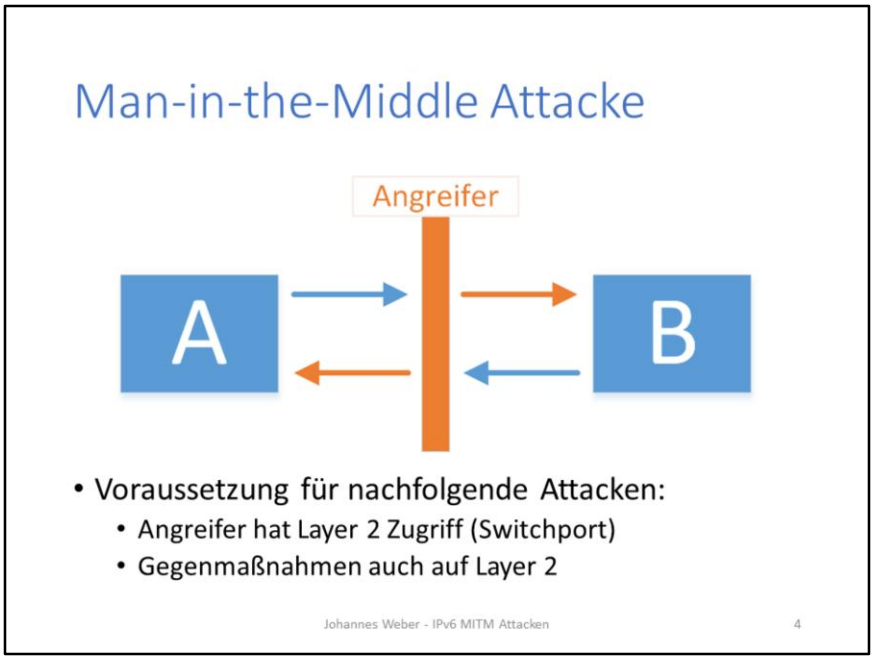
- MITM-Attacken
- Router Advertisement Spoofing
- Neighbor Advertisement Spoofing
- Rogue DHCPv6 Server

- Fazit

Vorstellung

- Johannes Weber
- Masterarbeit
  - IPv6 Security Test Laboratory
  - IPv6 Attacken
  - Firewalls im Labor getestet (Cisco, Juniper, Palo Alto)
- Technical Specialist Network Security
  - TÜV Rheinland i-sec GmbH (Consulting)

- Die Masterarbeit hat drei große Kapitel: 1) Einführung in IPv6, 2) IPv6 Security Attacken, 3) Testlabor mit Testergebnissen der Firewalls
- TÜV Rheinland i-sec GmbH: Consulting u.a. im Bereich Netzwerksicherheit (http://www.tuv.com/informationssicherheit)



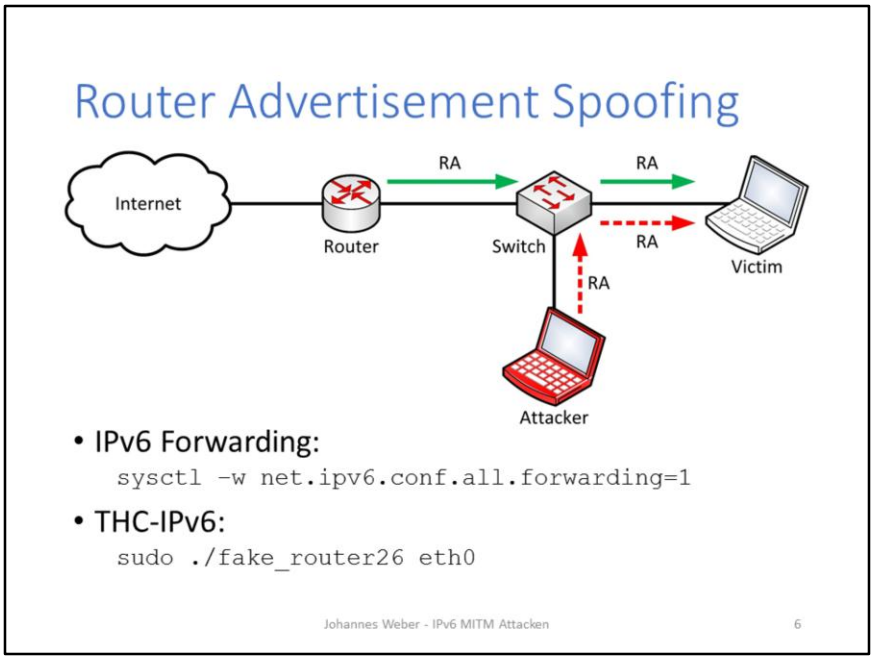
- Angreifer positioniert sich physikalisch/logisch zwischen den Kommunikationspartner (bzw. Victim = Opfer):
    - Er sieht den kompletten Datenverkehr und kann ihn entsprechend auswerten, zB Passwörter im Klartext, aufgerufene URLs, …
    - Er kann den kompletten Verkehr manipulieren, um zB TLS/SSL Verschlüsselungen aufzubrechen.
    - Physikalisch: Angreifer platziert sich wirklich zwischen A und B, zB mit einem eigenen Switch.
    - Logisch: Angreifer fälscht Forwarding-Tabellen beim Opfer, zB ARP Cache, Neighbor Cache, Routing Tabelle.
- Bei Angriffen auf Layer 2 müssen die Gegenmaßnahmen auch auf Layer 2 implementiert werden, sprich: eine Firewall am Übergang vom Firmennetz zum Internet bringt hier nichts.

Router Advertisement Spoofing

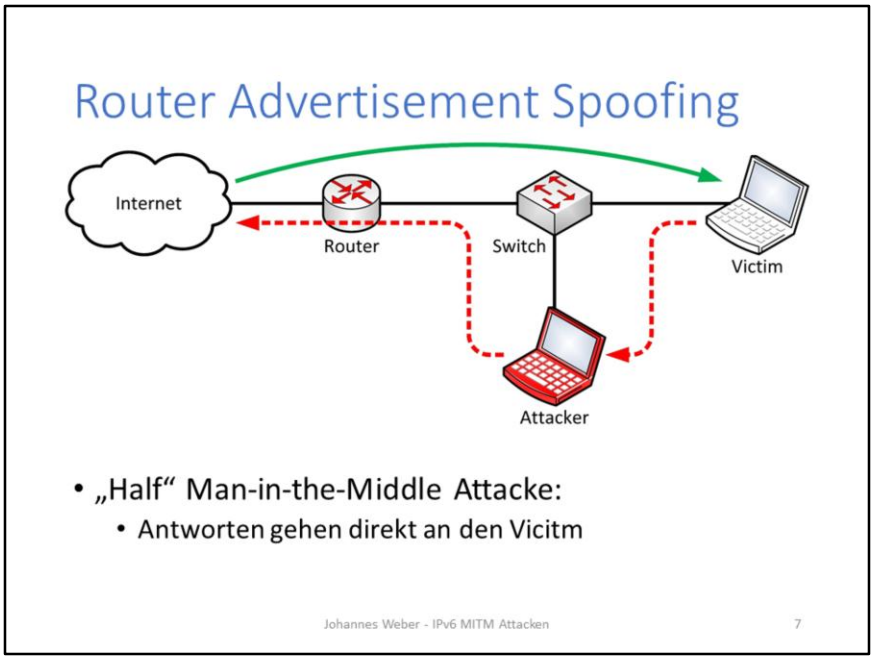
- Einstiegsfrage: Darf es immer nur einen Default Router pro Netzwerk geben?

→ Nein: Jeder Router kann/darf RAs senden. IPv6 Nodes erzeugen entsprechende Adressen (SLAAC) und tragen Routen ein.

- Zweite Einstiegsfrage, die ich aus Zeitgründen rausgelassen habe: Nicht nur Nodes, sondern auch Router verändern ihre Routing-Tabelle wenn ein RA von einem weiteren Router empfangen wird? (Falsch: Router ignorieren RAs von anderen Routern.)

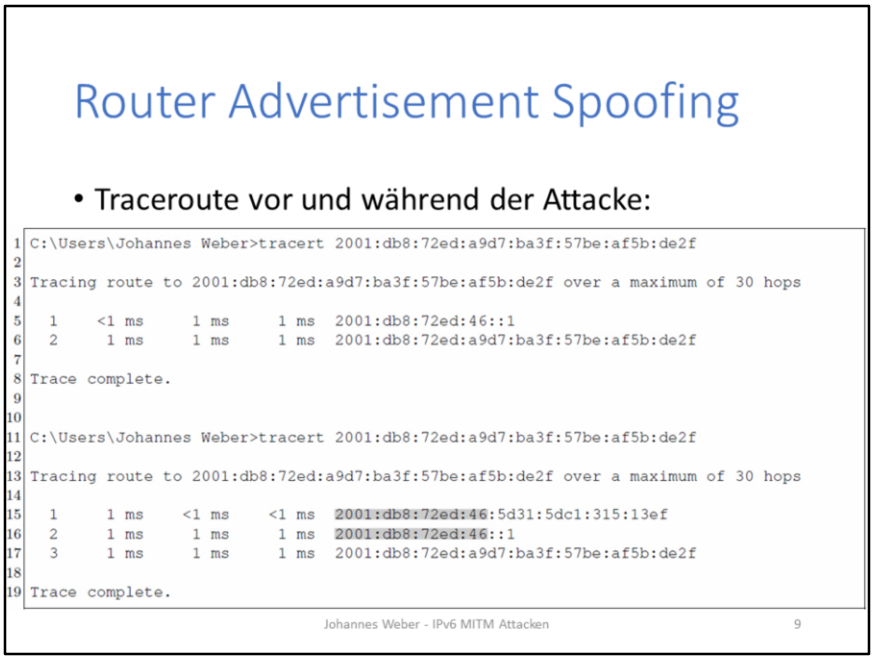


- Normalfall: Nur der richtige Router schickt Router Advertisements ins Netzwerk.
- Angriffsfall: Auch der Angreifer schickt RAs. Diese haben die höchste Priorität für die Default Route. → Die Victims im Netzwerk speichern den PC des Angreifer als Default Router ab.
- Die beiden Befehle jeweils am PC des Angreifers ausführen. 1) PC wird zum Router, 2) PC sendet RAs mit höchster Priorität und eigener MAC als Link-Layer Adresse.
- Es werden keine weiteren IPv6 Adressen per SLAAC bei den Nodes erzeugt. Es wird nur die Routing-Tabelle verändert. (Es wird also kein weiterer Präfix in den RAs bekannt gegeben.)
- In den Routing-Tabellen der Victims befinden sich nun zwei Default Router, wobei mindestens der des Angreifers die höchste Priorität hat:
    - Windows: netsh interface ipv6 show route
    - Linux: ip -6 route show

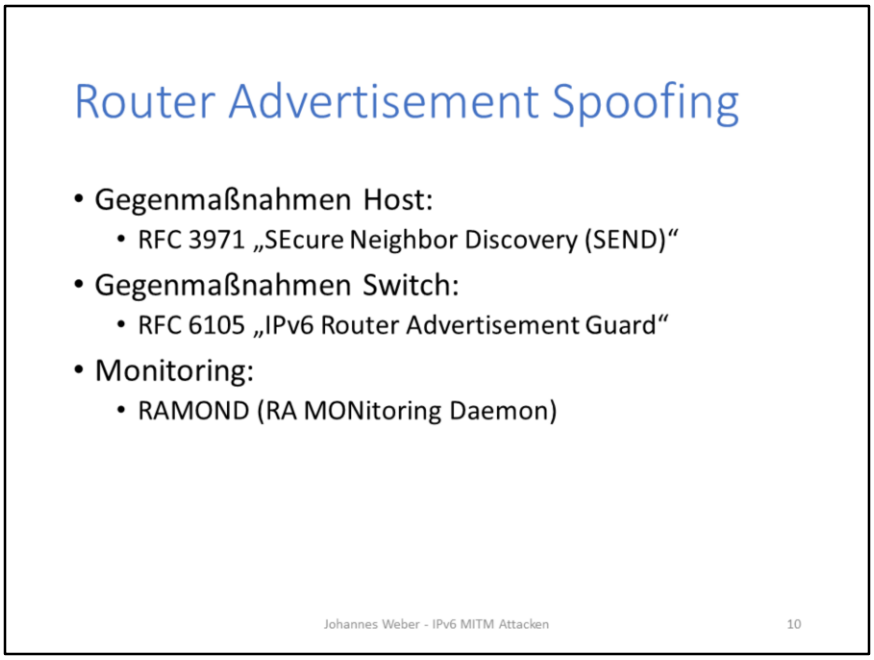


- „Half“ Man-in-the-Middle Attacke: Der zurückkommende Verkehr wird vom Router DIREKT an den Victim gesendet (grüner Pfeil), weil der Router bei dieser RA Spoofing Attacke seinen Zustand NICHT ändert. Wenn er ein IPv6 Paket bekommt, welches an einen IPv6 Node im direkt angeschlossenen Netzwerk gehen soll, schickt er es direkt raus.

- Bei der zweiten Ausführung sind zwei Default Router (::/0) vorhanden, wobei der neuere des Attackers eine kleinere Metrik (höhere Priorität) hat.



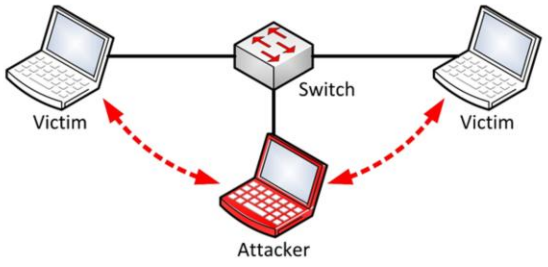
- Im zweiten Teil sieht man, dass ein weiterer Router im Pfad zu dem gleichen Ziel vorhanden ist (Erster Hop). Dieser befindet sich im gleichen Netzwerk-Segment, was für normales Routing untypisch ist.



- SEND: Über einen Zertifizierungspfad kann der IPv6 Host feststellen, ob er mit einem legitimen Default Router spricht. Der Host muss natürlich vorher ein entsprechendes vertrauenswürdiges Root Zertifikat haben, anhand dessen er dann feststellen kann, ob der Zertifizierungspfad des Routers ebenfalls vertrauenswürdig ist. Nachteil: Alle Hosts im Netz müssen VORHER entsprechend konfiguriert werden bevor sie ins gesicherte Netzwerk können. → Heute noch nicht abzusehen, ob das alles „sauber“ funktionieren wird. (zB: Hat jeder kleine Drucker SEND korrekt implementiert?)
- RA Guard: Ein Switch blockt RAs die von Ports kommen, an denen nur Hosts sitzen. Der Admin muss also vorher an den Switchports, an denen legitime Router sitzen, diese Schutzfunktion herausnehmen, bzw. als Router-Ports deklarieren.
- RAMOND: Ein einfacher Sniffer auf dem Netzwerk, der Alarm schlägt sobald unbekannte RAs auftauchen. Könnte man auch selber mit tcpdump oder ähnlichen Tools nachbauen.

- Ein Switch kann/könnte Listen führen, bei denen er per Port speichert, welche Multicast Gruppen dahinter „lauschen“ (ähnlich einem Router bei Nutzung von Multicast Gruppen). Der Switch kann das wissen, da jeder Host für alle Multicast Gruppen entsprechende Multicast Listener Report Nachrichten versendet. Diese Funktionalität haben aber nur „große“ Switche implementiert (MLD Snooping).

Neighbor Advertisement Spoofing



- IPv6 Forwarding:

```
sysctl -w net.ipv6.conf.all.forwarding=1
```

- THC-IPv6:

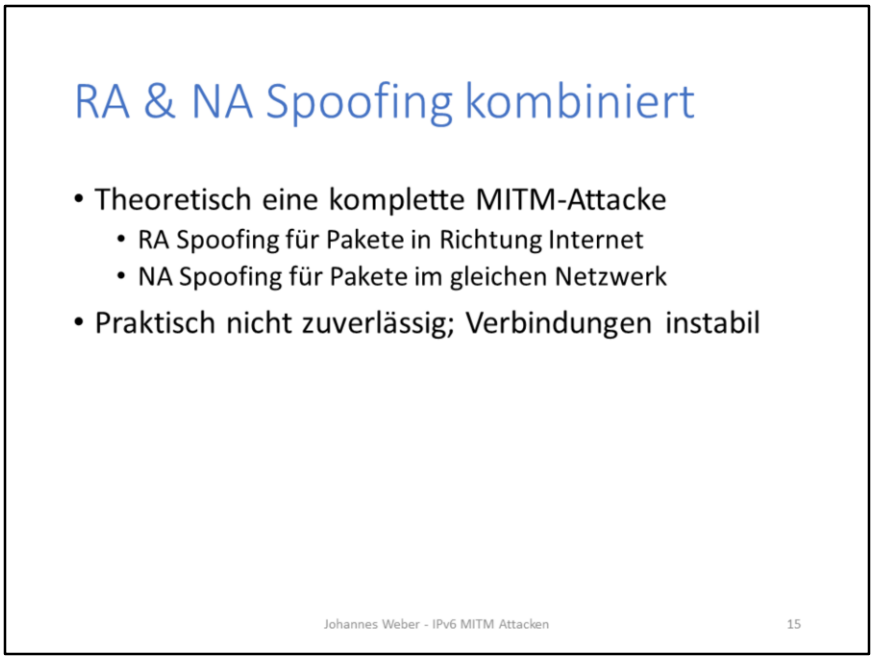
```
sudo ./parasite6 eth0
```

Johannes Weber - IPv6 MITM Attacken 12

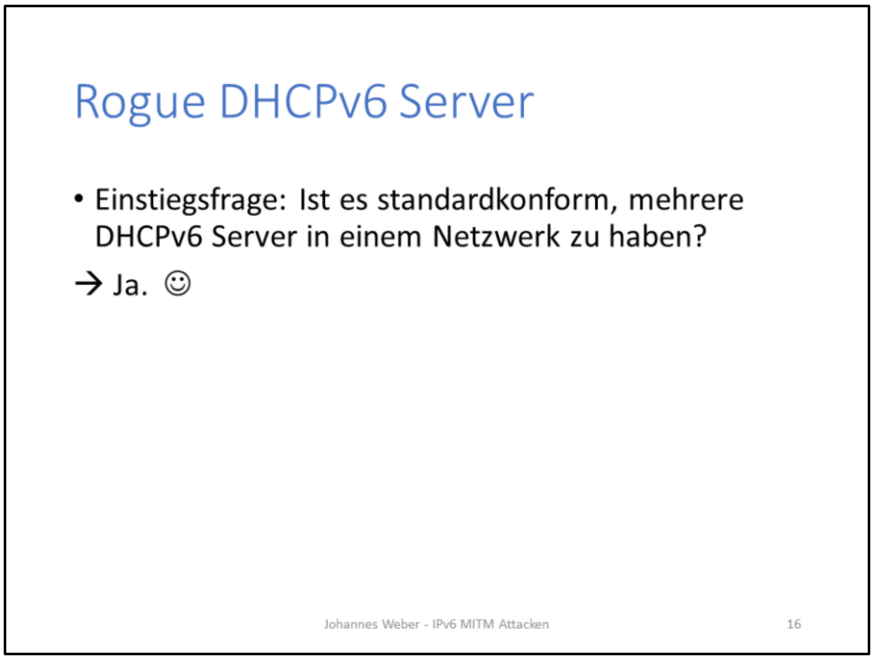
- Dieser Angriff ist das Pendant zu einem ARP Spoof in IPv4.
- Wenn Victim A mit Victim B kommunizieren möchte (und ein NS sendet), schickt der Angreifer ein NA mit der IPv6 Adresse von Victim B aber seiner eigenen MAC Adresse (!) an Victim A. Somit schickt Victim A seinen Traffic an die MAC Adresse des Angreifers. Bei Nachrichten von Victim B zu A entsprechend genau so.
- Parasite6: Vorsicht, es ist ein KOMPLETTER Neighbor Advertisement Spoof im Netzwerk. Wenn viele Hosts vorhanden sind, dann wird sehr viel gespooft. Für eine Einschränkung der Attacke kann man zB das na6 Tool vom SI6 Toolkit verwenden, welches Filter für die ausgehenden NA zulässt (http://www.si6networks.com/tools/ipv6toolkit/).
- Während der Attacke kann man sich den Neighbor Cache anschauen und feststellen, dass die Link-Layer Adresse von dem Angreifer im Cache steht:
    - Windows: netsh interface ipv6 show neighbor
    - Linux: ip -6 neighbor show
- Per Traceroute an einen Host im gleichen (!) Netz kann man sehen, dass das Paket über einen Router geleitet wird, der ebenfalls im gleichen Netzsegment sitzt. Im Normalfall zeigt ein Traceroute zu einem Host im gleichen Netz keinen Zwischenrouter an, da das Paket direkt an den anderen Host gleitet wird.

- Zu der gleichen IPv6 Adresse wurde eine andere MAC Adresse in den Neighbor Cache des Windows 7 Rechners geschleust.

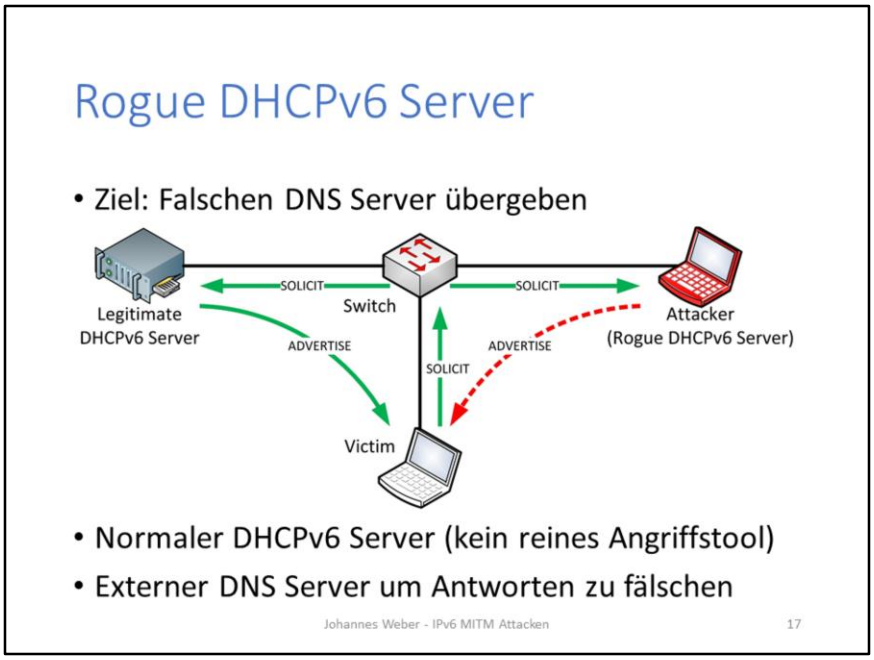
- Race Condition: Das Opfer bekommt zwei NAs: Das Richtige vom Kommunikationspartner und das Falsche vom Angreifer. Ja nach dem welches als erstes ankommt, bzw. wie der IPv6 Stack programmiert ist, funktioniert der Angriff mal mehr mal weniger gut. Es kann also sein, dass dieser Angriff keine 100 % Wirkung hat, bzw. „per Zufall“ mal nicht genau so funktioniert wie erwartet.
- SEND: IPv6 Nodes erzeugen sich eine CGA IPv6 Adresse (Cryptographically Generated Address, RFC 3972). Über ein Public-Private Key Paar kann ein IPv6 Node seine Neighbor Solicitation Message signieren und somit beweisen, dass er die dazugehörige Adresse wirklich besitzt. Problem: SEND wird heutzutage noch fast nicht eingesetzt, bzw. ist nicht auf allen Geräten implementiert.
- HIPS: Jeder Victim empfängt im Angriffsfall mindestens zwei verschiedene NAs mit verschiedenen MAC Adressen. Dies kann er feststellen und entsprechende Warnungen/Alarme ausgeben, wobei er nicht sicher sagen kann, welche NA jetzt die Richtige ist. HIPS Software muss zusätzlich installiert werden.
- ND Snooping: Der Switch lernt, welche IPv6 Adresse mit welcher MAC Adresse an welchem seiner Ports angeschlossen ist. Wenn ein Angreifer gefälschte NAs schickt, kann der Switch entsprechend den Port des Angreifers blocken.
- NDPMon: Snifft auf dem Netzwerk mit und stellt fest, wenn Anomalien auftreten (so wie in diesem Angriff der Fall).



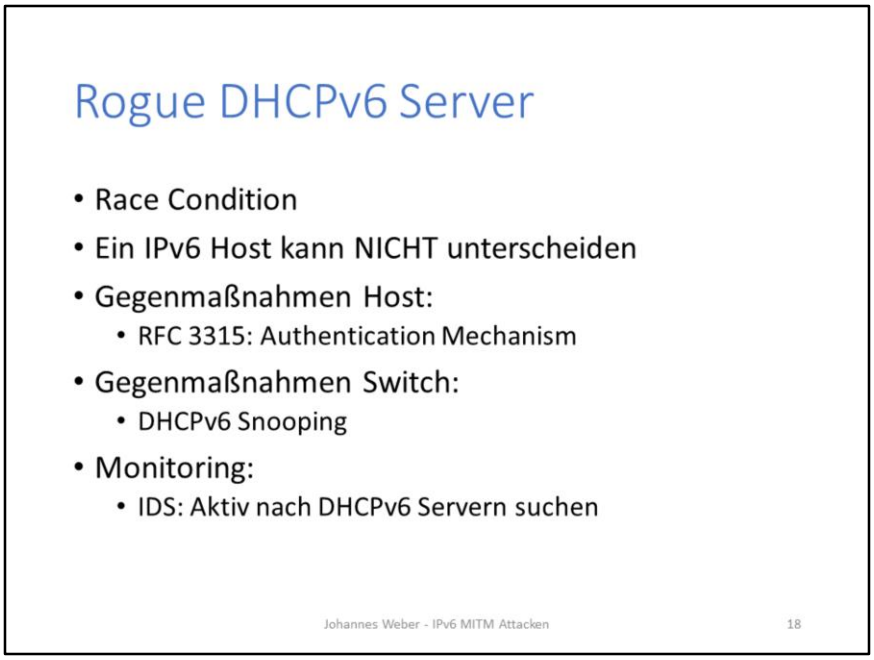
- Das hier ist nur meine eigene praktische Erfahrung! Eventuell treten durch die gleichzeitige Anwendung beider THC Tools irgendwelche Nebeneffekte auf. Vermutlich liegt das Problem aber in der Race Condition von den NAs.



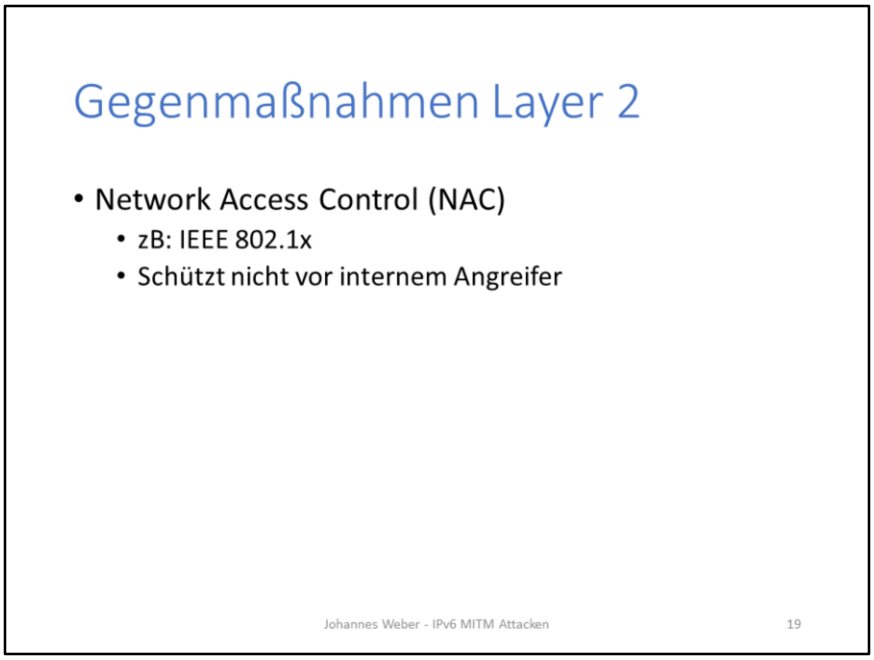
- Alle DHCPv6 Server und Clients unterscheiden sich durch eine eindeutige DHCP Unique Identifier (DUID).



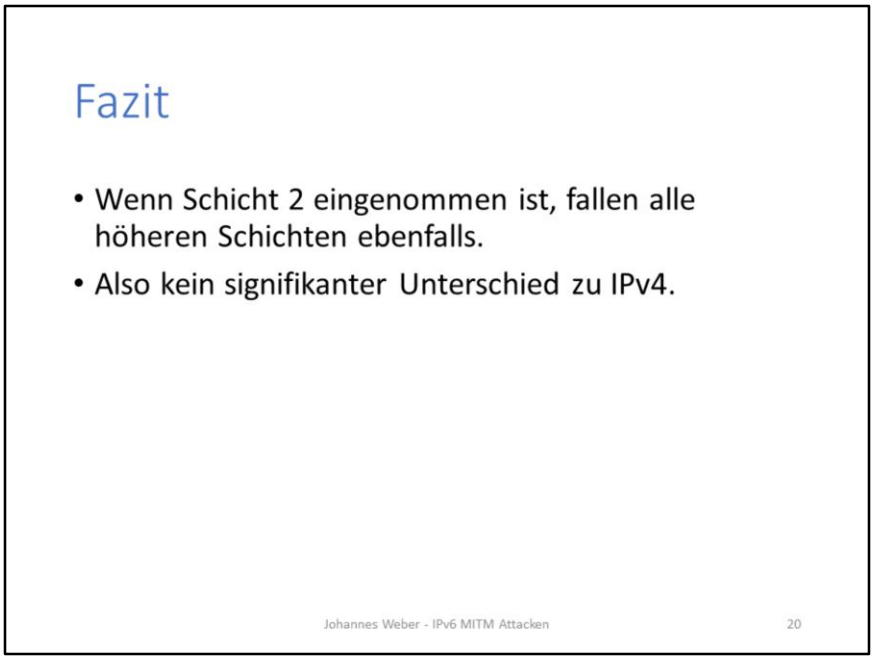
- Bei dieser Attacke wird nicht der gesamte IPv6 Traffic im LAN über den Angreifer geleitet (wie bei den vorherigen Attacken), sondern nur der DNS Server Eintrag bei den Victims gefälscht.
- Es geht NICHT darum, den DHCPv6 Server im stateful Modus zu betreiben um den Opfern weitere IPv6 Adresse zuzuweisen, sondern NUR um die Zuweisung eines gefälschten DNS-Servers (stateless DHCPv6).
- Der Angreifer muss zusätzlich einen eigenen DNS Server betreiben, der gefälschte IP Adressen bei angefragten DNS Namen herausgibt (DNS Spoofing, bzw. DNS Poisoning).



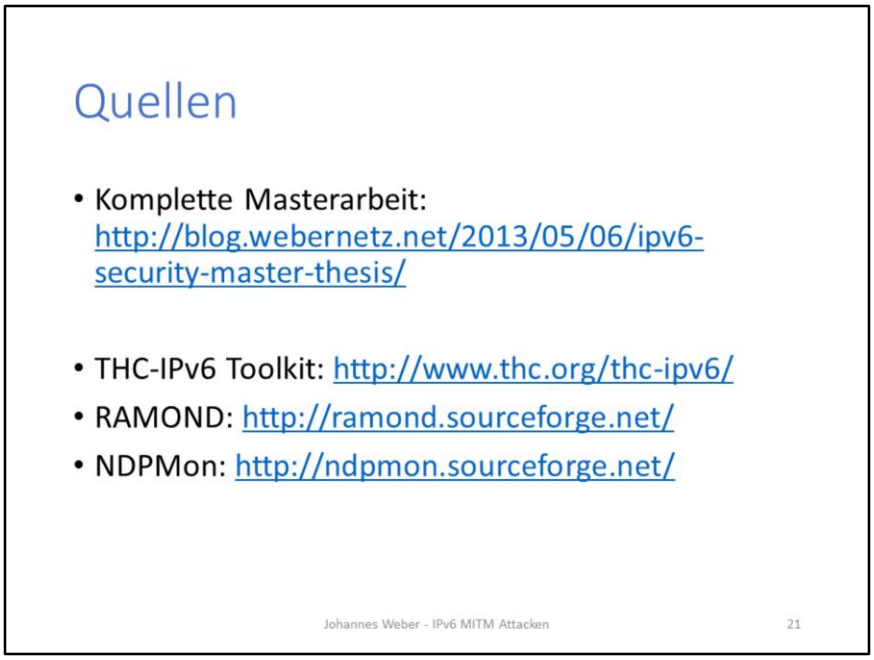
- Race Condition: Auch bei dieser Attacke kommt es darauf an, welche ADVERTISE Nachricht als erstes beim Opfer eintrifft: Entweder die des echten DHCPv6 Servers, oder die des Angreifers. Ebenso ist es abhängig von der IPv6 Implementation, welche Nachricht akzeptiert ist. Erfahrungsgemäß wird die erste Nachricht akzeptiert und alle weiteren einfach verworfen.
- DHCPv6 Authentication: DHCP-Option, die die komplette DHCP Nachricht signiert. Dadurch wird die Nachricht als auch der Sender der Nachricht authentisiert (message authentication, entity authentication). Nachteil: Man braucht (vorher ausgelieferte) Schlüssel.
- DHCPv6 Snooping (ähnlich dem RA Guard): Beim Switch muss konfiguriert sein, von welchen Ports DHCPv6 Server Nachrichten eintreffen dürfen. Kommt eine solche Nachricht von einem „Access“ Port, wird dieser zB blockiert.
- IDS: Per DHCPv6 Probes (SOLICIT) nach weiteren DHCPv6 Servern suchen. Dadurch werden auch fehlkonfigurierte DHCPv6 Server gefunden.



- Per NAC kann man zumindest den externen Angreifer fernhalten.
- Aber entsprechenden Statistiken sollten bekannt sein: Mindestens die Hälfte aller Angriffe kommt von Innen!



- Sprich: Wenn der Angreifer am Switch hängt, sieht es schlecht aus…



- In der Masterarbeit sind sehr viele IPv6 Attacken detailliert erklärt (Skizzen, tcpdumps, …). Außerdem wurde ein Testlabor aufgebaut, in dem drei Firewall getestet wurden (Cisco ASA, Juniper SSG, Palo Alto PA). Eine ausführliche Tabelle mit allen IPv6 Security Attacken ist ebenfalls vorhanden.

Vielen Dank fürs Zuhören ☺

- Bei Fragen/Anmerkungen:
  - johannes.weber@i-sec.tuv.com

- Meine Visitenkarte ;)