Schutz vor ARP-Spoofing

Gereon Rütten und
Oliver Stutzke

Hamburg, 04.02.2004

ITELLIUM Systems & Services GmbH
der IT Dienstleister der KarstadtQuelle AG

Agenda

ITELLIUM let's do IT

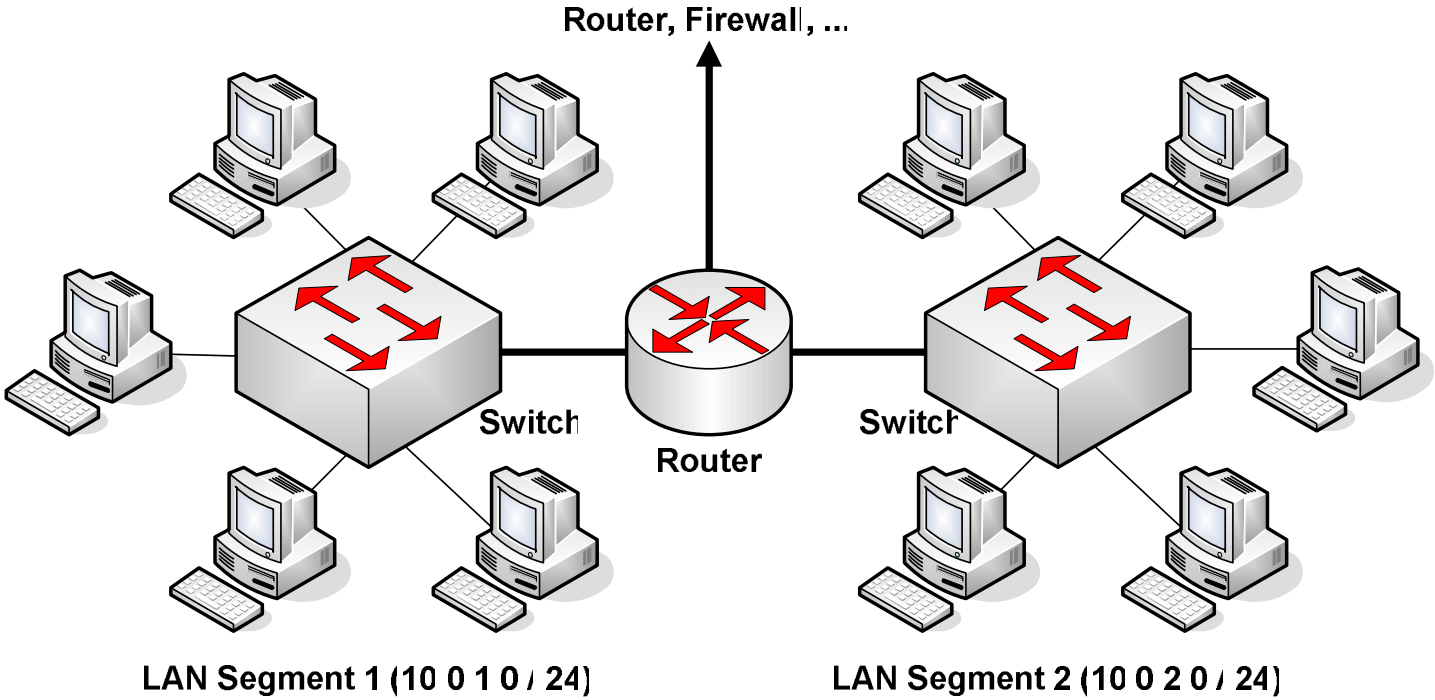
- Einleitung
- ARP-Spoofing
- Erkennung von ARP-Spoofing Angriffen
- Möglichkeiten zum Schutz vor ARP-Spoofing
- Zusammenfassung

Einleitung

- Vorrangiger Einsatz von Sicherheitssystemen zum Schutz vor Angriffen aus öffentlichen Netzen.
- Die Gefährdung durch Angriffe aus dem eigenen lokalen Netz wird häufig unterschätzt bzw. das Risiko derartiger Szenarien vernachlässigt.
- Es existieren zahlreiche Möglichkeiten die Sicherheit im LAN zu kompromittieren.
- ARP-Spoofing ist eine, auf Layer 2 des ISO / OSI-Modells basierende Möglichkeit Angriffe in lokalen Netzen durchzuführen.

Lokale Netze

- Ethernet ist die weltweit am häufigsten installierte LAN Technologie
- IPv4 ist in lokalen Netzen das Netzwerkprotokoll
- Sternförmige lokale Netze auf Basis von Ethernet-Switchen
- Entwicklung der Ethernet Technologie ohne Berücksichtigung sicherheitstechnischer Aspekte



- Das *Address Resolution Protocol,* kurz ARP (RFC 826)
  - ARP ist ein zustandsloses Protokoll
  - ARP-Request
  - ARP-Reply
- Lokale Verwaltung von MAC- / IP-Adressen-Zuordnung in einem dynamischen ARP-Cache
- Die Informationen eines ARP-Reply Paketes werden direkt in den ARP-Cache eingetragen

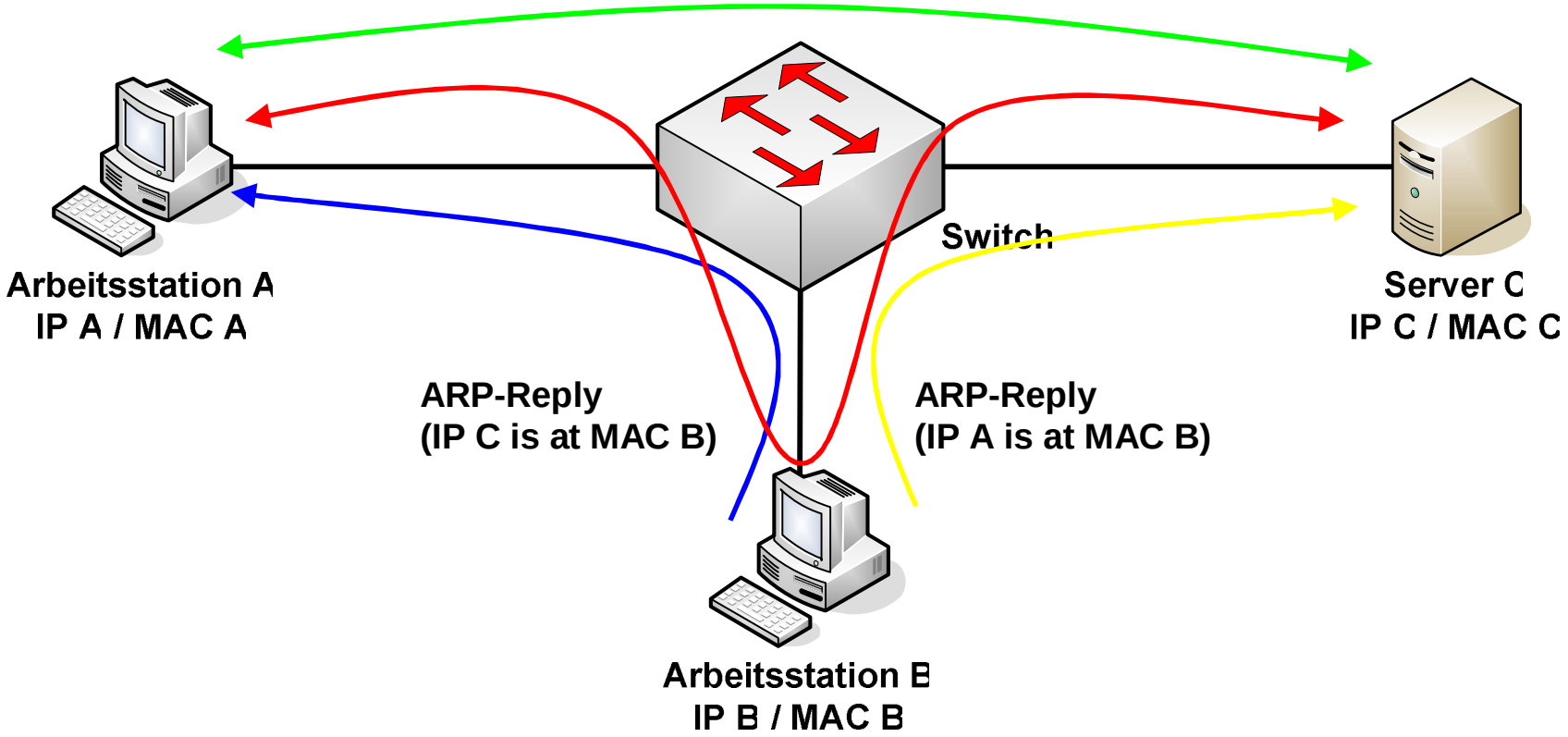
ARP-Spoofing

- Gezielte Manipulation der ARP-Caches durch Versenden von „ *falschen*“ ARP-Reply Paketen (ARP-Poisoning)

```
arp-reply
1:(Src: MAC B / Dst: MAC C / IP A is at MAC B)
2:(Src: MAC B / Dst: MAC A / IP C is at MAC B)
```

- Kein Hinzufügen von neuen Einträgen, sondern eine Aktualisierung des ARP-Cache
- ARP-Spoofing Angriffe sind:
  - nur innerhalb einer Broadcast-Domain möglich
  - die Grundlage für viele Angriffe auf Anwendungsebene
  - unabhängig von den im LAN eingesetzten Betriebssystemen

ARP-Spoofing



- Angreifer B hat eine klassische Man-in-the-Middle Situation hergestellt
- Umleitung der gesamten IP-basierten Kommunikation zwischen A und C über Arbeitsstation B

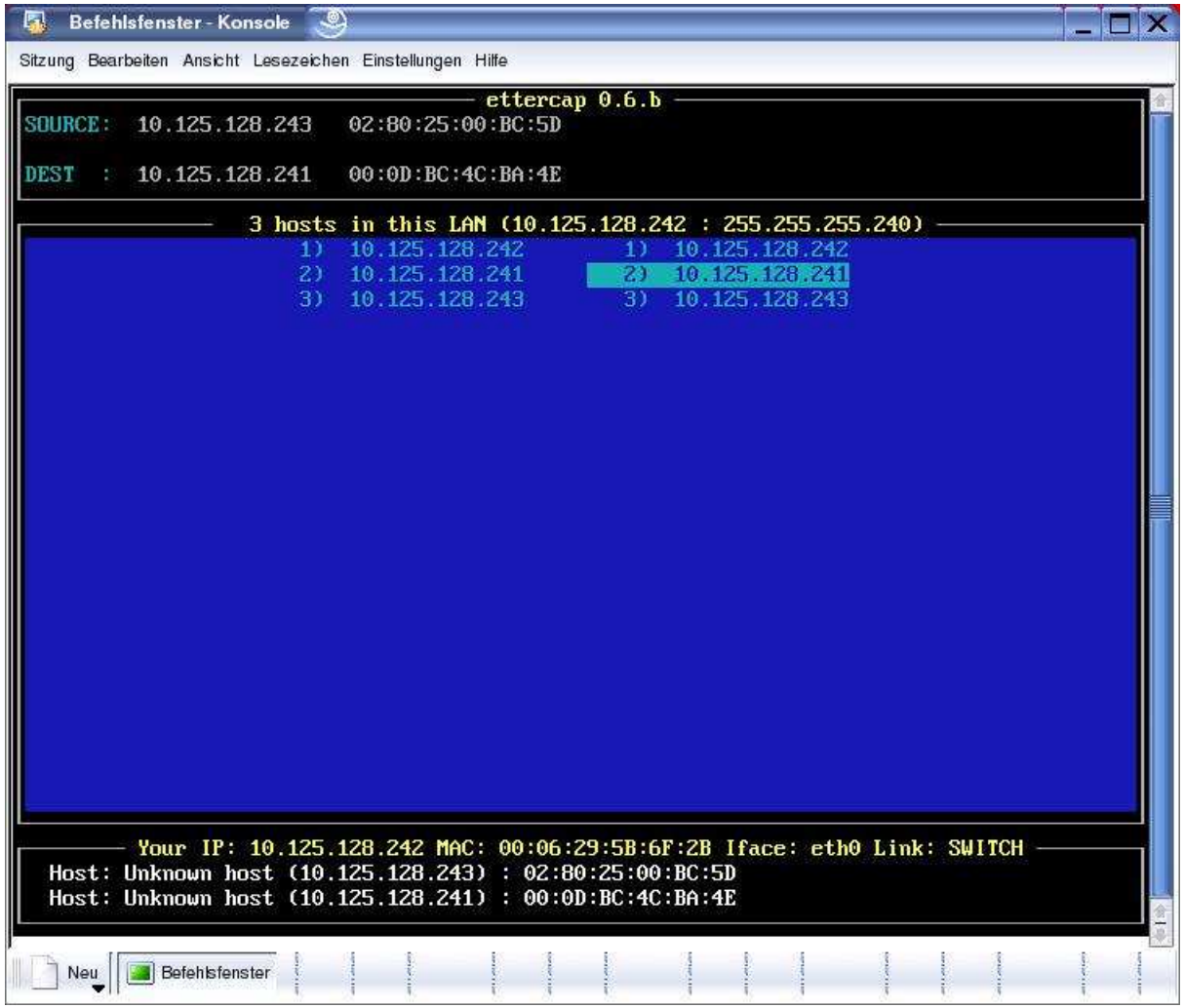
Wozu kann ARP-Spoofing genutzt werden

ITELLIUM let's do IT

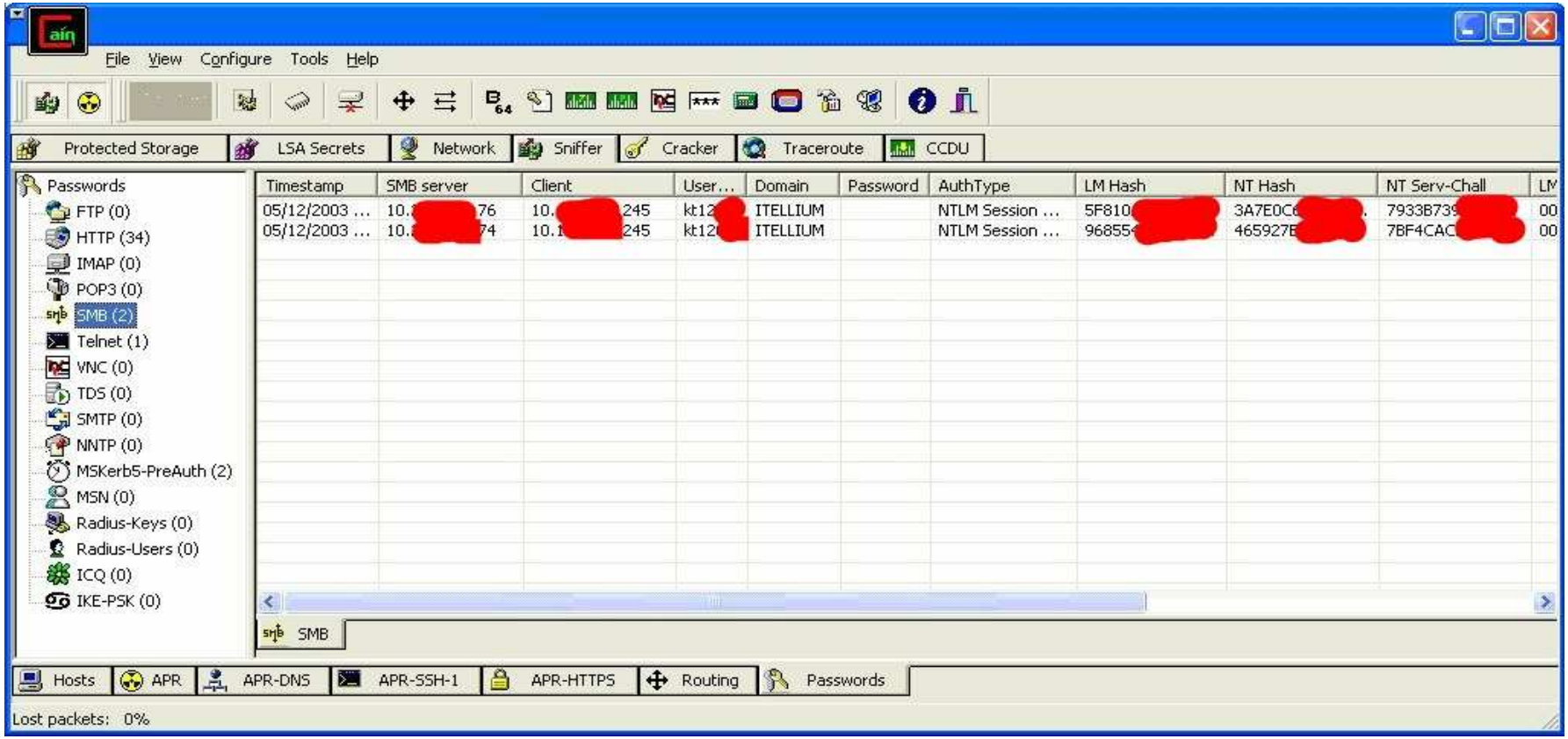
- Denial-of-Service Angriffe gegen einzelne Benutzer oder LAN-Segmente
- Schaffen und Ausnutzen einer Man-in-the-Middle Position
- Manipulation von Daten durch Verwendung von Anwendungsfiltern, z.B.
  - dns
  - http / https
- Analyse von Kommunikationsbeziehungen
- Abhören von Inhalten und Informationen
- Mitlesen von Passwörtern (telnet, ftp, http, ...)

Tools zum ARP-Spoofen

- Ettercap (Windows, Linux, ...)
- Cain & Abel (Windows)
- dsniff (Linux)



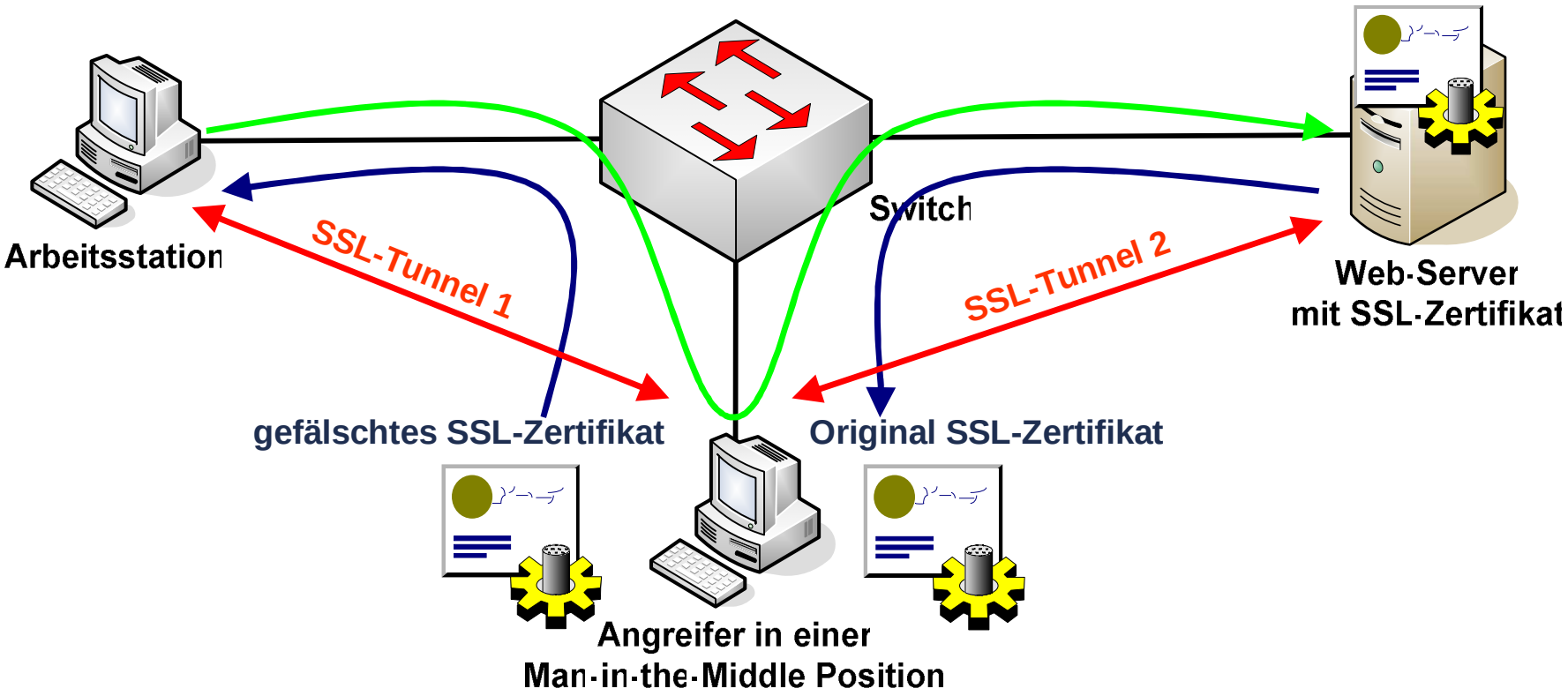
Anwendungsbeispiele - Passworte



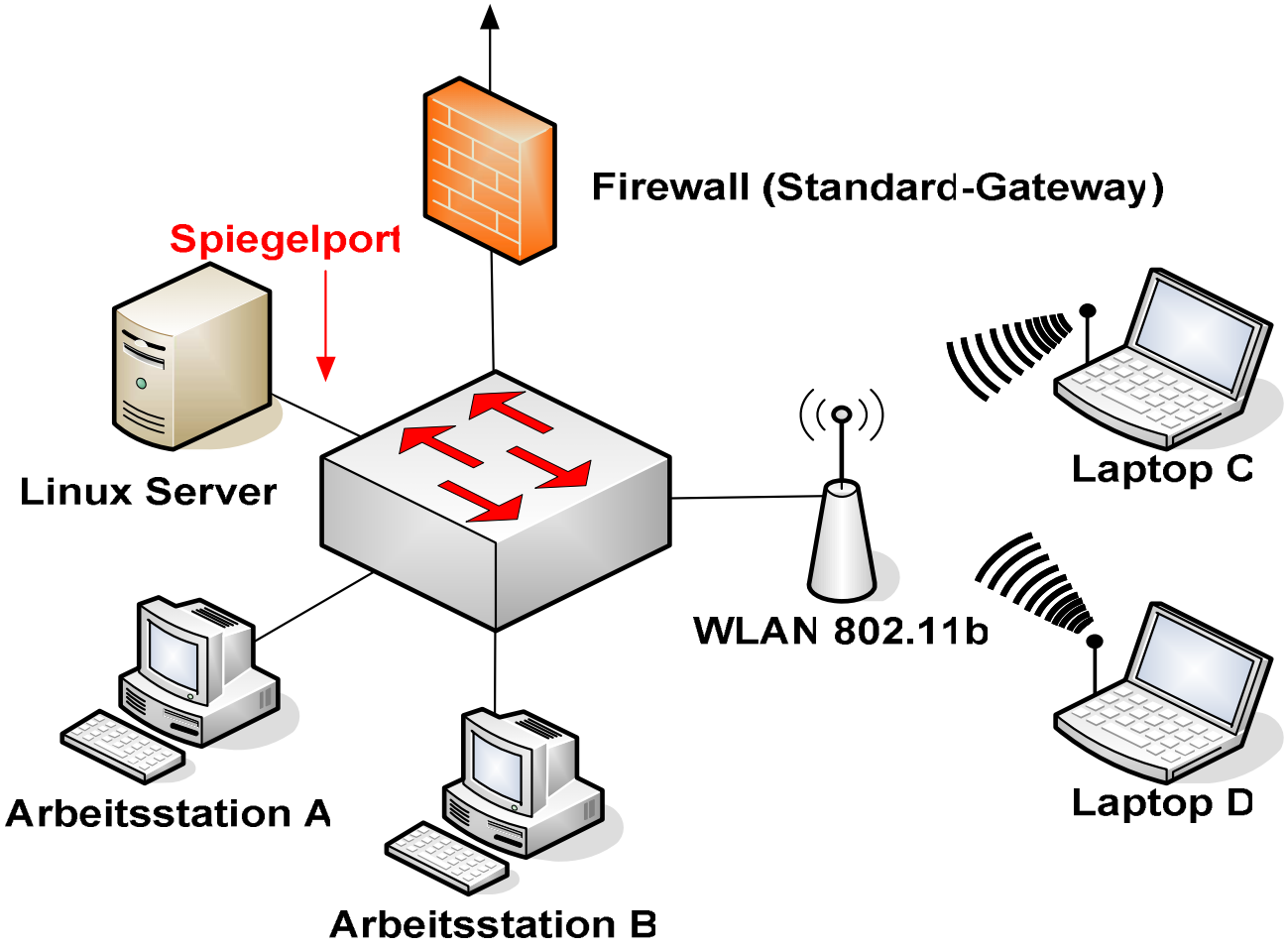
- Möglichkeit z.B Domain-Logins, SMB-Authentifikation abzuhören und direkt an einen Passwort-Knacker zu übergeben
- ssh Version 1, eine Schwäche in der Implementierung des Protokolls ermöglicht das direkte Auslesen und Entschlüsseln des Passwortes

Anwendungsbeispiel – https

- Abfangen des originalen ssl-Zertifikates und Austausch durch ein gefälschtes ermöglicht dem Angreifer das Aufbrechen der verschlüsselten Verbindung



Test-Labor



- Ergänzung der folgenden Techniken zur Erkennung und Abwehr von ARP-Spoofing Angriffen durch praktische Ergebnisse aus dem Test-Labor

Grundlage für Schutzmaßnahmen

ITELLIUM let's do IT

- Erkennung von ARP-Spoofing Angriffen
- Überwachung
  - des ARP-Cache
  - der ARP-Pakete im LAN
  - auf Endgeräten
  - auf und mit Netzkomponenten

Erkennung von ARP-Spoofing im Netz

ITELLIUM let's do IT

- Voraussetzung ist, alle ARP-Meldungen in einem LAN Segment durch an Spiegelports angeschlossene Netzsensoren zu überwachen
- IDS Systeme wurden in erster Linie zur Erkennung von Angriffen auf Layer 3 bis 7 entwickelt
- Erkennung von ARP-Angriffen durch darauf spezialisierte Systeme
  - ARPwatch
  - ARP-Guard
- IDS Module auf Netzkomponenten

Beispiele aus dem Test-Labor

ITELLIUM let's do IT

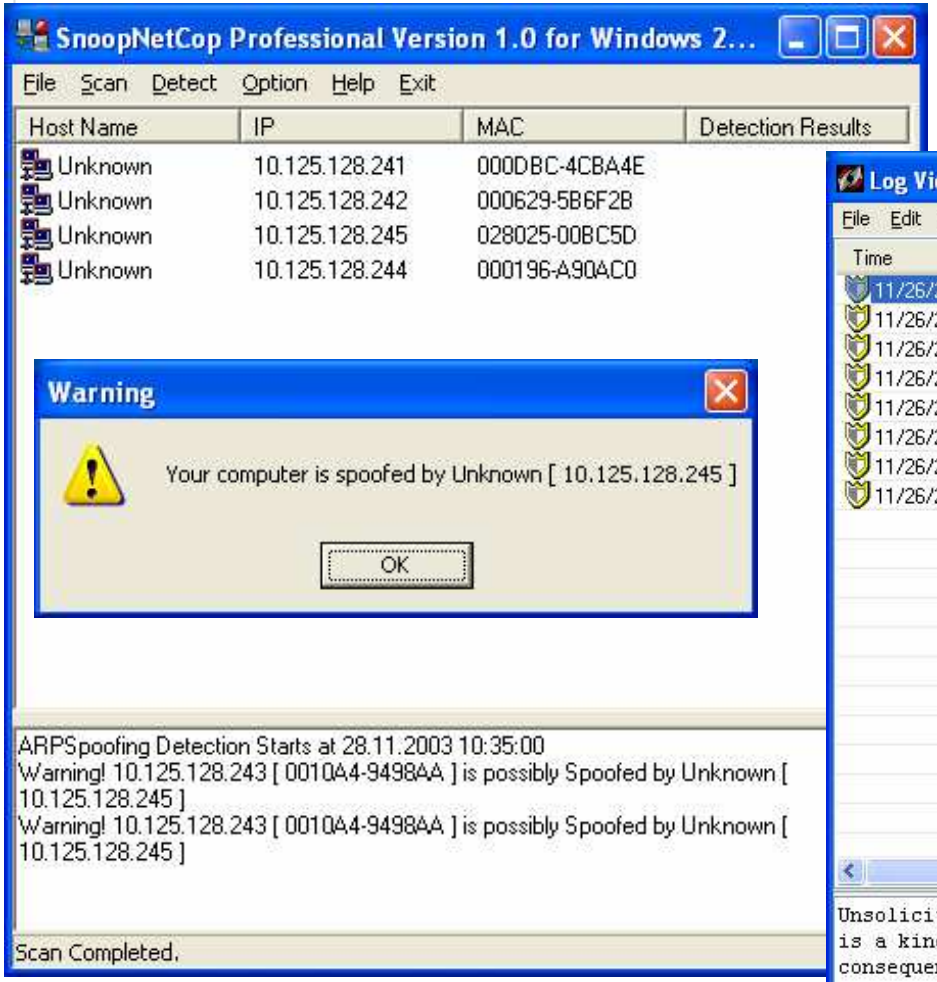
- Snort
  - `preprocessor arpspoof`
    Ende des Angriffs:
    ```
    11/14-12:02:15.850358 [**] [112:2:1] (spp_arpspoof)
    Ethernet/ARP Mismatch request for Source [**]
    ```
  - `preprocessor arpspoof`
    `preprocessor arpspoof_detect_host: <IP A> <MAC A> , ...`
    Start des Angriffs:
    ```
    11/14-09:49:03.994100 [**] [112:4:1] (spp_arpspoof)
    Attempted ARP cache overwrite attack [**]
    11/14-09:49:34.010568 [**] [112:2:1] (spp_arpspoof)
    Ethernet/ARP Mismatch request for Source [**]
    ```
- Cisco PIX Firewall
  - Erkennung eines IP- / MAC- Zuordungsproblems unter der Voraussetzung, dass die Zuordung des angegriffenen Rechners im ARP-Cache der PIX vorhanden ist
  - Integriertes IDS Modul der PIX erkennt zur Zeit keine ARP-Angriffe

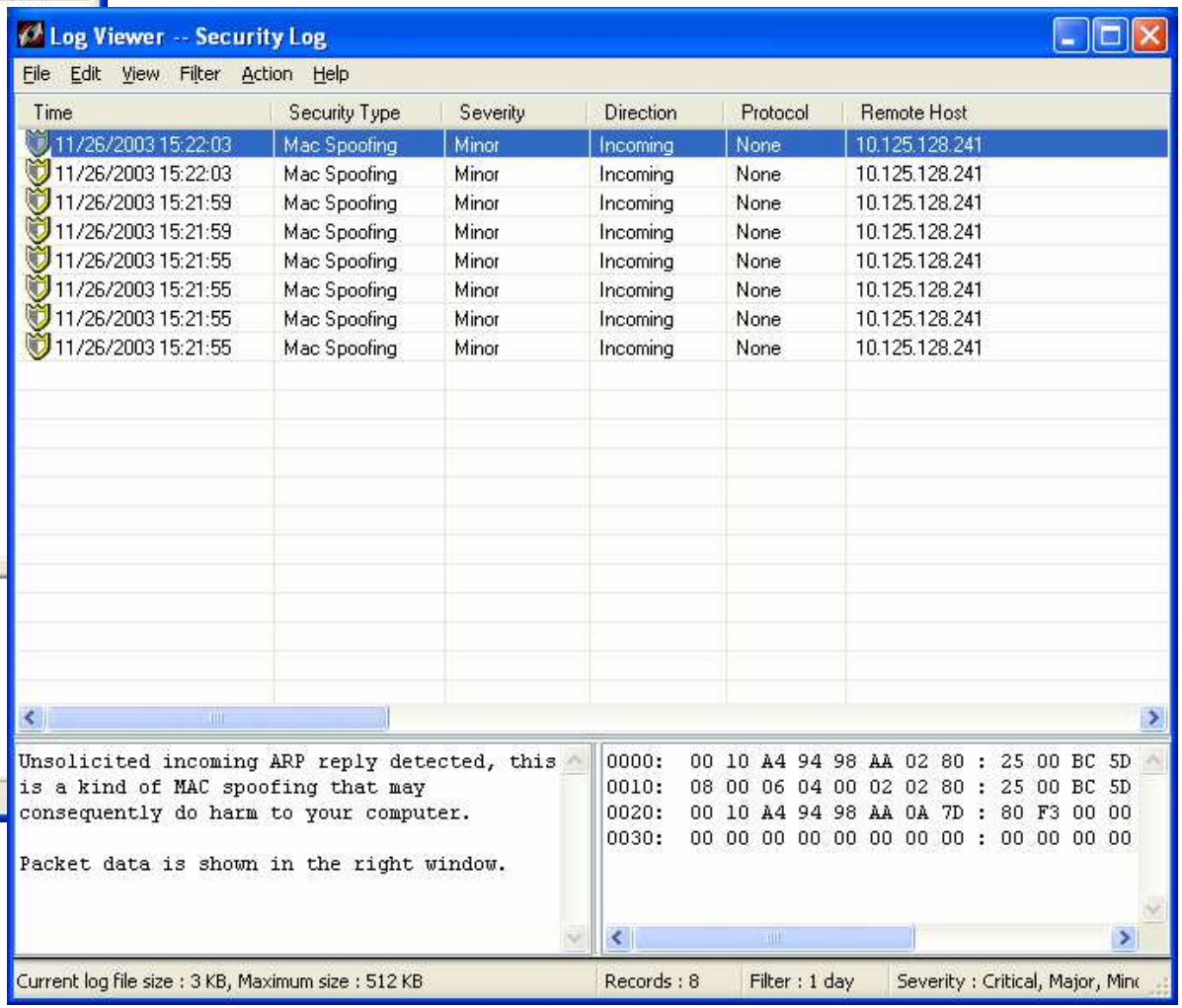
Erkennung von ARP-Spoofing auf Endgeräten

- Überwachung auf jedem Endgerät im LAN Segment notwendig
- Software zur Überwachung des lokalen ARP-Cache bzw. der ARP-Pakete durch
  - Personal Firewalls
  - Spezielle *Anti-ARP-Spoofing* Software
  - IDS Hostsensoren
- Aufklärung der Benutzer über das Gefährdungspotential von ARP-Spoofing

Beispiele aus dem Test-Labor

ITELLIUM let's do IT

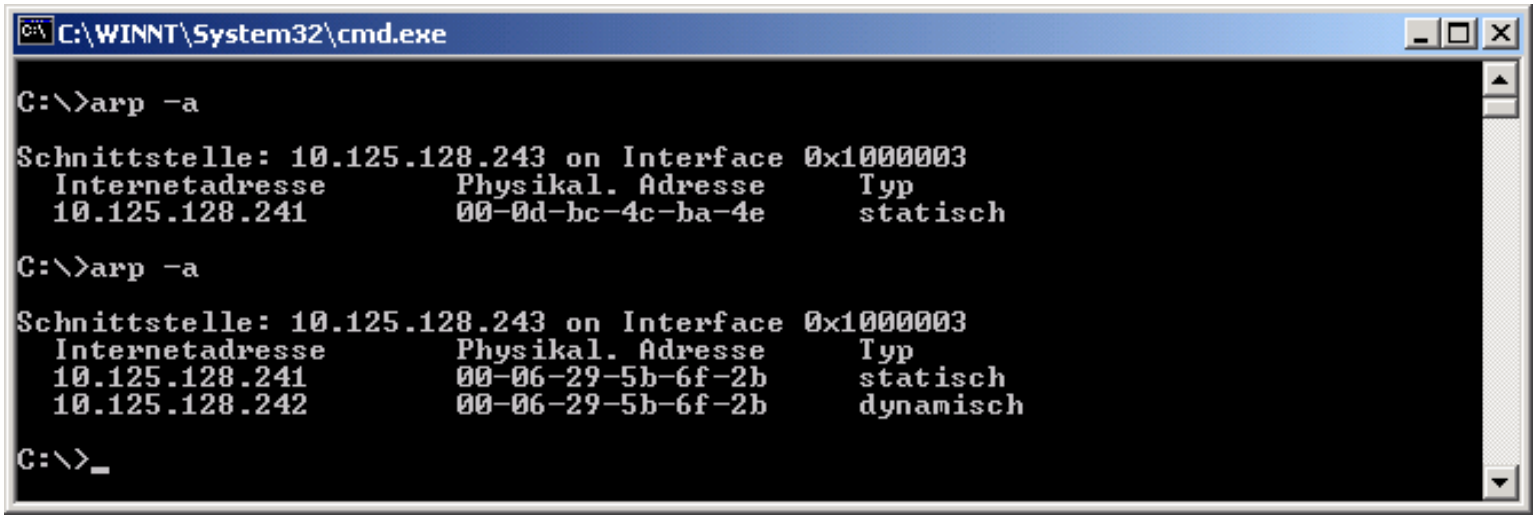




Präventive Schutzmaßnahmen vor ARP-Spoofing

ITELLIUM let's do IT

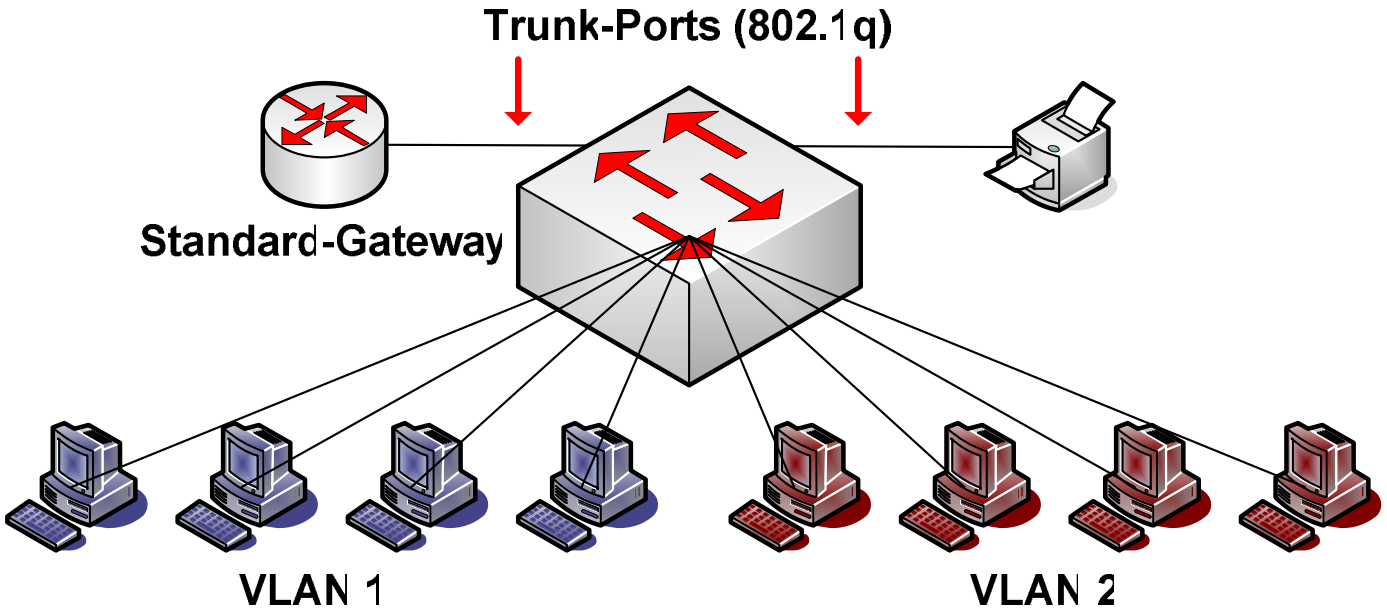
- Organisatorische Maßnahmen
  - Installation von Software durch Benuzter unterbinden
- Statische IP- / MAC–Zuordnung im ARP-Cache
  - `arp –s <IP-Adresse> <MAC-Adresse>`
  - bei Microsoft erst ab XP möglich
  - erhöhter administrativer Aufwand
  - in DHCP Umgebungen nicht realisierbar
  - statische IP- / MAC-Zuordung des Standard-Gateways auf allen Arbeitsplatzrechnern im LAN Segment



Präventive Schutzmaßnahmen vor ARP-Spoofing

ITELLIUM let's do IT

- Möglichkeit ohne den Einsatz von Tools die Sicherheit zu erhöhen
  - Konfiguration von kleinen, logisch getrennten Netzsegmenten
  - innerhalb der Netzsegmente besteht **kein** Schutz vor ARP-Angriffen
  - Reduzierung der Anzahl angreifbarer Komponenten
  - erhöhte Anforderungen an Netzkomponenten
  - erhöhter administrativer Aufwand



Schutzmaßnahmen im LAN

- Voraussetzung ist die Erkennung von ARP-Angriffen
- Automatische Benachrichtigung des Administrators
  - manuelle Prüfung
  - keine Reaktion in Echtzeit
- Einsatz von Scripten zur Erkennung eines Angreifers und automatische Deaktivierung seines Switch-Ports
  - False-Positive Problematik
- Einsatz von Sicherheitsfunktionen auf Netzkomponenten, z.B. bei Cisco
  - `port` oder `switchport protected`
    → Isolation von Ports auf Switchen
  - `port security`
    → Limitierung der MAC-Adressen pro Port

Schutzmaßnahmen auf Endgeräten

- Einsatz von Software zur Erkennung von ARP-Angriffen
  - Benutzer müssen über Gefährdungslage informiert sein
  - Benutzer müssen instruiert sein
  - Pflege der Software
  - Schutz für Mobile User
- Statische ARP-Einträge (wenn möglich)
  - in DHCP Umgebungen nicht möglich
  - statischer Eintrag des Standardgateways

Kryptographische Schutzmaßnahmen

- Schutz der transportierten Daten und Informationen durch Verwendung von Verschlüsselung
  - auf Netzebene durch VPN-Technologien (z.B. IPSec, ssh mit Port Forwarding)
  - auf Anwendungsebene (z.B. PGP, S-MIME)
  - https nur in Verbindung mit lokal gespeicherten SSL-Zertifikaten
- Nachteil ist die Installation, Konfiguration und Pflege der Software
- Benutzer müssen die Lösung akzeptieren

Schutz vor ARP-Spoofing - Überblick

ITELLIUM let's do IT

Schutzmaßnahme	Erkennung vorausgesetzt	Einsatzgebiet im Netz	Einsatzgebiet auf Endgeräten	Benutzer involviert
Statische ARP Einträge			X	
Einsatz von Script-basierter Port-Deaktivierung	X	X		
Warnung der Benutzer vor der Verwendung von ARP-Spoofing Tools	X	X	X	X
Sicherheitsfunktionen auf Netzkomponenten		X		
Kleine Netzsegmente		X		
Verwendung starker Verschlüsselung			X	X

Weitere Layer-2 Angriffsmöglichkeiten

- CAM-Table Overflows
  - Methode: Überflutung der CAM-Table eines Switch
  - Ziel: Broadcasten **aller** Pakete in einem VLAN
- MAC-Address Cloning
  - Methode: Übernehmen von fremden MAC-Adressen
  - Ziel: Aushebeln von auf MAC-Adressen basierten Sicherheitsmassnahmen (z.B. ACL‘s)
- VLAN Hopping
  - Methode: Manipulation von VLAN Tags
  - Ziel: Pakete in fremde VLANs verschicken (z.B. für DoS-Angriffe)

Fazit

- Es existiert zur Zeit keine universelle Lösung zum Schutz vor ARP-Spoofing Angriffen
- Es existieren zahlreiche Möglichkeiten, die über statische ARP-Einträge und den Einsatz von ARPwatch hinausgehen
- Es ist sinnvoll, verschiedene Schutzmöglichkeiten zu kombinieren
- Die Entscheidung über den Einsatz von Schutzmaßnahmen muss je nach Art der Infrastruktur, dem angestrebten bzw. geforderten Sicherheitsniveau, den finanziellen Möglichkeiten und dem vorhandenen Know-How der Administratoren getroffen werden.

Kontakt

Itellium Systems & Services GmbH
Theodor-Althoff-Strasse 2
45133 Essen

Gereon Rütten: gereon.ruetten@itellium.com

Oliver Stutzke: oliver.stutzke@itellium.com

Vielen Dank für Ihre Aufmerksamkeit