ARP / DNS-Spoofing mit SSL-Side-Attack

Arne Köller, Benedikt Sielaff und René Hosch
Master IT-SEC WS 17/18

Inhalt

1. ARP-Protokoll und -Spoofing
2. DNS-Protokoll und -Spoofing
3. SSL-Side-Attacks und Vorführung Angriff
4. Fazit

1.

Adress Resolution Protocol

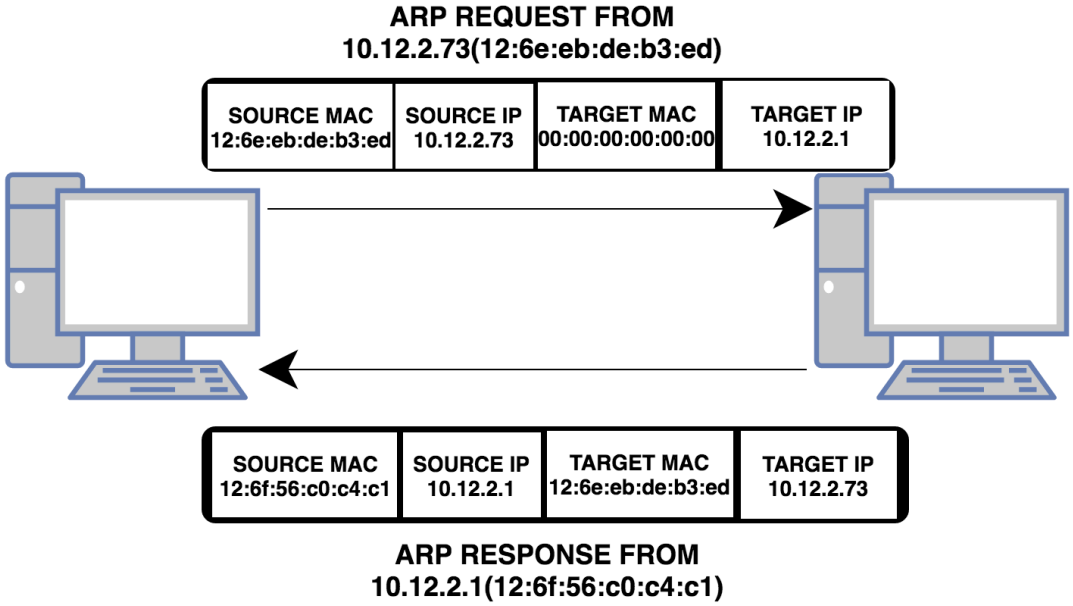
Definition ARP

- Ist ein Netzwerkprotokoll
- Ordnet eine Netzwerkadresse eine Hardwareadresse zu
- ARP-Tabellen
- Fast ausschließlich zur Ermittlung von MAC Adressen zu einer IP Adresse
- OSI Schicht 2

Ablauf ARP

- ARP Request wird gesendet (MAC und IP)
- Gesucht wird der Computer mit einer speziellen IP Adresse
- ARP Request wird an die Broadcast Adresse gesendet
- Match der IP Adresse => eine ARP Antwort wird generiert
- Kombination wird in die ARP Tabelle eingetragen

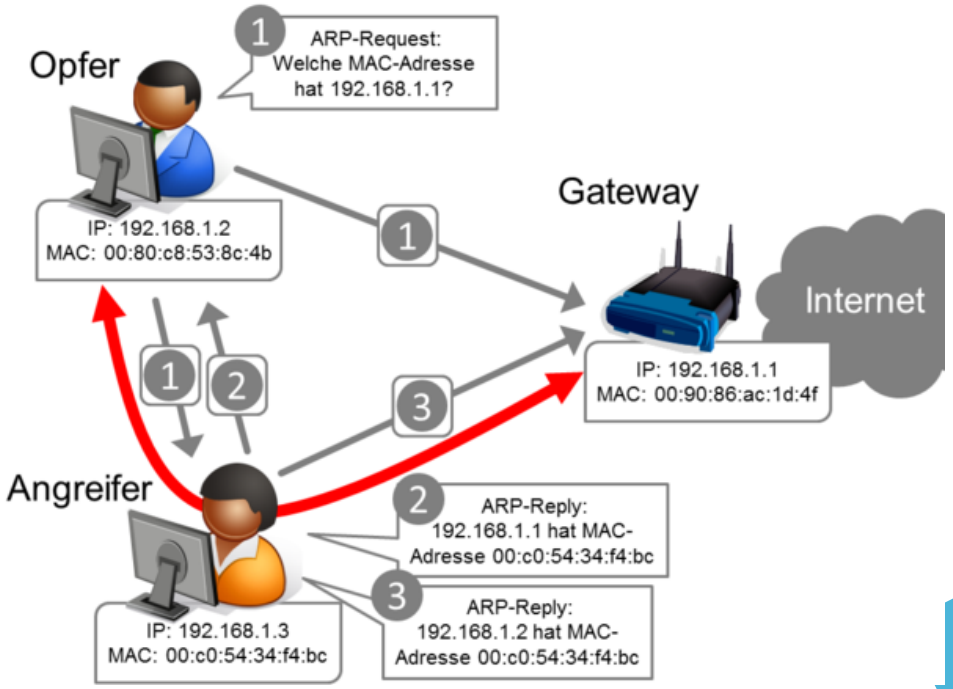
Ablauf ARP


ARP REQUEST FROM
10.12.2.73(12:6e:eb:de:b3:ed)
SOURCE MAC
12:6e:eb:de:b3:ed
SOURCE IP
10.12.2.73
TARGET MAC
00:00:00:00:00:00
TARGET IP
10.12.2.1
SOURCE MAC
12:6f:56:c0:c4:c1
SOURCE IP
10.12.2.1
TARGET MAC
12:6e:eb:de:b3:ed
TARGET IP
10.12.2.73
ARP RESPONSE FROM
10.12.2.1(12:6f:56:c0:c4:c1)

ARP Spoofing

- Bezeichnet das senden von gefälschten ARP Paketen
- ARP Tabellen verändern
- Anschließend soll der Datenverkehr abgehört oder manipuliert werden können
- Man-in-the-middle Angriff

ARP Spoofing



Gegenmaßnahmen

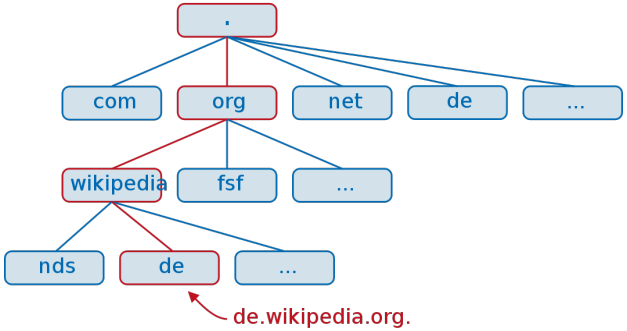
- Statische ARP-Tabellen (ist stark beschränkt).
- Monitoring Programme (arpwatch, ARP-Guard).
- Generell ist ARP jedoch anfällig.
- Ipv6 Neighbor Discovery Protocol.

2.
Domain Name System

Definition DNS

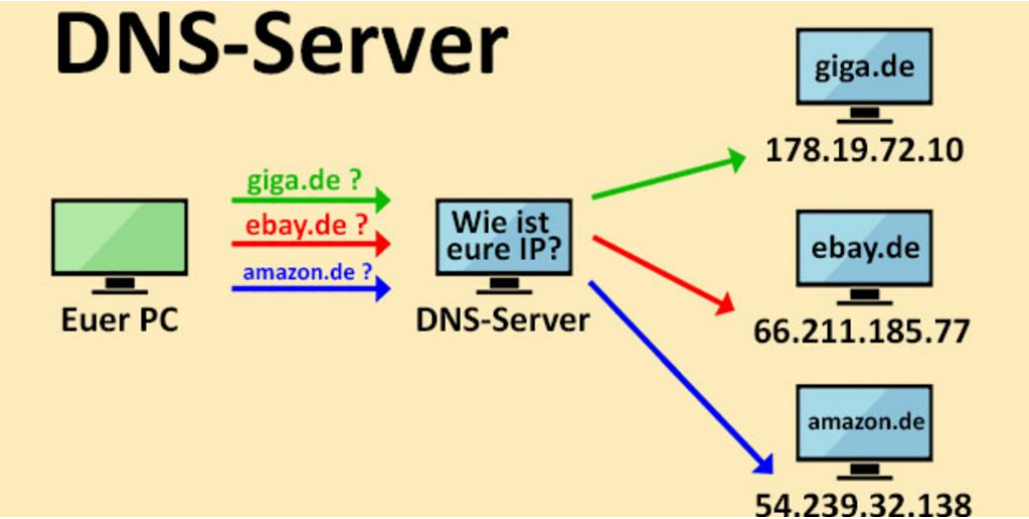
- Beantwortung von Anfragen zur Namensauflösung
- Funktioniert wie ein Telefonbuch
- User kennt den Domain Namen bspw. www.hs-bochum.de
- Forward lookup und Reverse lookup
- OSI Schicht 7

Ablauf DNS



- Schaut in der lokalen Host Datei
- Eintrag im Cache vorhanden ?
- Anfrage an den Root-Nameserver
- Beispiel de.wikipedia.org
- Abschließend wird die IP Adresse geliefert

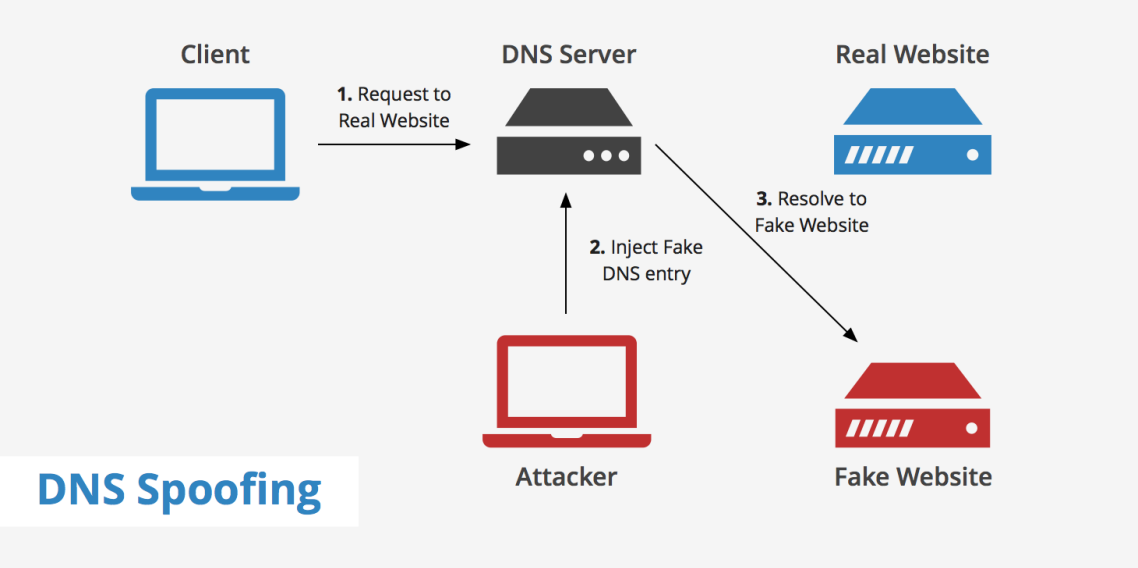
Ablauf DNS


DNS-Server
giga.de
178.19.72.10
giga.de ?
ebay.de ?
amazon.de ?
Wie ist eure IP?
Euer PC
DNS-Server
ebay.de
66.211.185.77
amazon.de
54.239.32.138

DNS Spoofing

- Angriff auf das DNS
- Datenverkehr soll unbemerkt umgeleitet werden
- Zuordnung zwischen Namensraum und IP soll gefälscht werden

DNS Spoofing



Gegenmaßnahmen

- Source Port Randomization
- 0x20-Bit Encoding
- Digitale Signaturen oder Message Authentication Codes
- Kryptographische Verfahren
- Bspw. DNSSEC

3.

SSL-Side-Attack und Vorführung Angriff

Ablauf Angriff

Bekannte SSL-Side-Attacks

1. Pre-HTTPS Intercept
2. HTTPS-Downgrade

Pre-HTTPS-Intercept

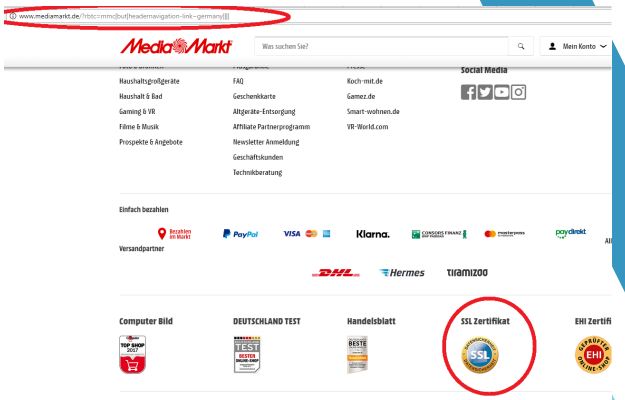
- Wir nutzen den Umstand, dass viele Webseiten erst ihre geschützten Bereiche SSL-Verschlüsseln und **nicht ihre gesamte Webseite**!

Code und Demo

https://github.com/bene77/IT-Sec

Vulnerable Websites: Pre-HTTPS Interce

- spiegel.de, faz.net, bild.de
- ikea.com
- mediamarkt.com
- karstadt.de
- hs-bochum.de, ruhr-uni-bochum.de
- sparda.de
- qvc.de
- deutsche-rentenversicherung.de
- Google-Suche: inurl:http://



HTTPS-Downgrade

Tool: sslstrip
In Kali enthalten.

Vulnerable Websites: HTTPS-Downgrade

- iberia.com

Gegenmaßnahmen SSL-Side-Attacks

- HTTPS Everywhere (gegen Pre-HTTPS Intercept)
- HSTS (gegen HTTPS-Downgrade)

4.
Fazit

Fazit

- ARP und DNS Spoofing sind immer noch eine große Sicherheitslücke.
- ARP Spoofing kann nicht komplett verhindert werden.
- DNS kann durch Sicherheitsmaßnahmen verhindert werden.
- SSL-Side-Attacks funktionieren oft!
- Social Engineering funktioniert nur durch die Naivität der User.

Vielen Dank für Ihre Aufmerksamkeit!

Quellen

- https://hosting.1und1.de/digitalguide/server/sicherheit/arp-spoofing-angriffe-aus-dem-internen-netzwerk/Ordnet eine Netzwerkadresse eine Hardwareadresse zu
- https://www.elektronik-kompendium.de/sites/net/1710251.htm
- https://de.wikipedia.org/wiki/Address_Resolution_Protocol
- https://de.wikipedia.org/wiki/Domain_Name_System
- https://avicoder.me/2016/02/22/SSLstrip-for-newbies/