Advanced Security Features

Angriffe - Overview

DHCP Snooping, IP Spoofing und ARP Spoofing sind Angriffe innerhalb von geswitchten LANs, die die korrekte Weiterleitung von Ethernet Frames und IP Paketen manipulieren (**data plane**).

Exkurs: Einteilung von Angriffen/Sicherheitsmaßnahme auf Cisco

- **Management Plane**
  verarbeitet Datenverkehr an oder von Cisco Geräten, wie z.B. Telnet, SSH, SNMP, …
- **Control Plane**
  verarbeitet Datenverkehr, der zur Verwaltung der Netzwerkinfrastruktur verwendet wird, wie z.B. Routing Protokolle (EIGRP, OSPF, BGP), FHRPs, STP/RSTP, …
- **Data Plane**
  verarbeitet Datenverkehr, der zur Weiterleitung bestimmt ist.

Übersicht L2 Angriffsmethoden

.. in geswitchten LANs.

Angriff	Beschreibung	Vermeidung
Switch Device Attacks (management plane)		
CDP attacks	Ausspähen von CDP Informationen	CDP disable (port-based)
SSH and Telnet attacks	Mitlesen von Telnet Sessions	SSHv2 und Line-ACLs
MAC Layer Attacks (data plane)		
MAC flooding	Switch wird mit (falschen) MAC Adressen "bombadiert", wobei die MAC-Address Table überläuft → flooding aller Frames	Port Security (maximum 1) 802.1x
Spoofing Attacks (data plane)		
DHCP spoofing	Ausschöpfung des IP Addressraums; Übernahme des DHCP Dienstes	DHCP Snooping
MAC spoofing	Übernahme eine anderen (fremden) MAC	Port Security (mac-address)
ARP spoofing	Falsche ARP Replys (man-in-the-middle attacks)	DAI - Dynamic ARP Inspection
IP spoofing	Übernahme einer anderen (fremden) IP	DHCP Snooping/ IP Source Guard
VLAN Attacks (data plane)		
VLAN hopping	Kommunikation in (allen) VLANs durch Verwendung der entsprechenden VLAN ID	Trunk Configuration .. .. kein DTP, pruning Unbenutzte Ports .. .. in ein "unrouted VLAN"
STP Attacks (control plane)		
Rogue Device (Switch)	Rogue Switch wird Root Bridge	RootGuard
Rogue Device Hub	Potentielle Loops; Anschluß mehrerer Geräte an einem Port	PortFast with BPDUGuard PortFast mit BPDUFilter; Port Security (maximum 1),
Looping	Port-zu-Port Verkabelung	PortFast with BPDUGuard
VTP Attack (control plane)		
Bogus database	Rogue Device sendet falsche Infos	VTP Password

Spoofing Attacks

DHCP Spoofing

DHCP Spoofing heißt, das ein Angreifer einen **rogue DHCP Server** im Netzwerk implementiert, der anstelle des eigentlichen DHCP Servers auf Anfragen antwortet.

Dabei sendet der rogue DHCP Server manipulierte o. unbrauchbare Parameter.
Beispiele:Der rogue DHCP Server

- sendet für jeden Client eine IP aus einem anderen Netzbereich
  → die Clients können nicht miteinander kommunizieren
- sendet keine Default-GW Information
  → die Clients können nicht mit entferten Netzwerken kommunizieren
- sendet manipulierte Default-GW oder DNS IP Adressen
  → die Clients senden Datenverkehr an die falschen Geräte (**man-in-the-middle** attack), wo der Datenverkehr mitgeschnitten oder manipuliert werden kann.

IP Spoofing

Beim IP Spoofing verwendet der Angreifer falsche IP Adressen für die Kommunikation ..
.. z.B. um die Herkunft von **Denial of Service** Angriffen zu verschleiern.

Datenverkehr – zurück - an die gefälschten IP Adresse ist nicht zustellbar.

MAC-Spoofing/ARP-Spoofing

Beim ARP-Spoofing werden gefälschte ARP Pakete gesendet.
Dabei werden die ARP Tabellen auf allen Geräten im Netzwerk manipuliert: einer Ziel IP ist jetzt eine gefälschte MAC Adresse zugeordnet.

Datenverkehr an die entsprechende Ziel IP wird jetzt an den Angreifer zugestellt, der die Kommunkation abhören oder manipulieren kann.

Beispiel: man-in-the-middle attack

Um Datenverkehr zwischen Host A und Host B abzuhören, sendet ein Angreifer manipulierte, unaufgeforderte ARP-Nachrichten (gratuitous ARP) an beide Hosts:

- Host A wird mitgeteilt, das die IP Adresse von Host B über die MAC Adresse des Angreifers zu erreichen ist,
- Host B wird mitgeteilt, das die IP Adresse von Host A über die MAC Adresse des Angreifers zu erreichen ist

Sämtlicher Datenverkehr zwischen Host A und Host B läuft jetzt über das Gerät des Angreifers, das als proxy für die Kommunikation zwischen den beiden Hosts agiert, und kann vom Angreifer ohne Probleme eingesehen oder manipuliert werden (**man-in-the-middle** attack).

Bei ARP Spoofing kann eine Angreifer auch die Rolle des **Default-Gateways** übernehmen, so kann sämtlicher Datenverkehr in entfernte Netzwerke vom Angreifer mitgeschnitten werden.

Abwehrmechanismen Spoofing Attacks auf Cisco - Überblick

- **DHCP Snooping**
  - verhindert DHCP Spoofing
  - vermeidet z.B. Man-in-the-middle Angriffe
    .. ein angreifender Rougue DHCP (gibt sich als DHCP Server aus) vergiebt gefälschte Parameter (z.B. falsches Default GW) und kann so Datenverkehr umleiten.

- **IPSG - IP Source Guard**
  - verhindert IP Spoofing
  - vermeidet z.B. DoS Angriffe
    .. ein angreifendes Gerät stellt in kurzer Zeit viele TCP SYN Segmente mit jeweils unterschiedlichen SRC IP Adressen im IP Header – sendet aber keine ACKs und kann so Server Dienste überlasten.

- **DAI - Dynamic ARP Inspection**
  - verhindert ARP Spoofing, MAC Spoofing
  - vermeidet z.B. Man-in-the-middle Angriffe
    .. ein angreifendes Gerät gibt sich durch gefälschte MAC und/oder IP Adressen als ein anderes Gerät aus (z.B. als Default GW) und leitet so Datenverkehr um.

Verfügbarkeit der Features auf Cisco Platformen und GNS3

	DHCP Snooping	**IPSG**	**DAI**
2950/60	JA	NEIN	NEIN
3550/60	JA	JA	JA
3750/60	JA	JA	JA
GNS3	JA	JA	JA

DHCP Snooping

Mit DHCP Snooping werden Ports auf einem Access Layer Switch wie folgt aufgeteilt

- **trusted port(s)** → Uplink zu einem DHCP Server
  alle DHCP Nachrichten werden weitergeleitet

- **untrusted port(s)** → alle anderen Ports
  nur DHCP Anfragen werden weitergeleitet (DHCP Discover, DHCP Request)

Default Einstellung für alle Ports: untrusted

Falls eine DHCP Antwort (DHCPOffer) an einem untrusted port empfangen wird, wird der Port in den **err-disable state** (shudown) geschaltet.

DHCP Snooping erstellt zusätzlich Tabellen über DHCP bindings, die aus der DHCP Kommunikation zwischen dem legitimen Server und dem Client erzeugt werden.
Diese **tracking database** beinhaltet alle Informationen, die der Client vom Server erhalten hat.

Schutz

- DHCP Snooping filtert untrusted DHCP Nachrichten - eine DCHP Antwort (DHCPOffer), die der Switch von einem über einen untrusted port empfängt - aus und schützt so vor **DHCP Spoofing Attacken**: ein "Angreifer" DHCP Server sendet falsche Default GW Informationen, worauf sämtlicher Datenverkehr (erst) an das "**Man-in-the-middle**" Default GW gesendet wird.
- Durch die Möglichket eine zulässige Anzahl von DHCP Anfragen innerhalb einer Sekunde festzulegen (**limit rate**), schützt DHCP Snooping ebenfalls for DHCP **DoS Attacken**.

DHCP Option 82
DHCP Snooping kann auch derart konfiguriert werden, dass er die DHCP Option 82 (die DHCP Relay Agent Option, RFC 3046) verwenden kann.

Dies ist sinnvoll, wenn der Switch als Relay-Agent arbeitet.

Bei Verwendung der DHCP Option 82

- sendet der Switch, bei Weiterleitung des DHCP Requests, der über einen untrusted Port empfangen wurde zusätzliche Informationen an den Server:
  - remote ID - MAC Adresse des Switches
  - circuit ID - die Port ID des Ports, über die die Anfrage erhalten wurde

- Wenn der DHCP Server, der das Paket empfängt, die Option 82 Informationen auswerten kann, verwendet er die remote ID und/oder die circuit ID um die korrekte IP Informationen für den anfragenden Client zu ermitteln und zu versenden.
  In jedem Fall wird der Server in seiner Antwort die Option 82 Informationen unverändert zurückgesenden.

- Der Switch überprüft bei Erhalt der Antwort die Informationen im Option 82 Feld auf Richtigkeit, entfernt sie und leitet die Antwort an den Client weiter.

ACHTUNG: wenn eins der beteiligten Geräte (DHCP Relay oder DHCP Server) die Option 82 nicht auswerten kann, wird die DHCP Anfrage nicht beantwortet.

Konfiguration DHCP Snooping

DHCP Snooping wird NUR auf **Access Layer** Switches konfiguriert.

Globale Aktivierung von DHCP Snooping auf Access Layer Switches – notwendig!

(config)# **ip dhcp snooping**

Aktivierung von DHCP Snooping für ein VLAN oder einen Bereich von VLANs – notwendig!

(config)# **ip dhcp snooping vlan** *vlan-id* [*last-vlan-id*]

Festlegung eines Interface als trusted (default: untrusted) .. da geht's zum DHCP Server.
HINWEIS: falls ein L3 Port zum DHCP Server führt, muss bzw. kann dieser nicht als trusted Port eingestellt werden (.. L3 Ports sind default "trusted").

(config-if)# **ip dhcp snooping trust**

Optional – aber empfehlenswert: Festlegung der maximalen Anzahl von DHCP Requests, die auf dem untrusted Interface innerhalb einer Sekunde empfangen werden können. Empfohlen ist ein rate-limit **nur für untrusted interfaces**, um eine Flut von DHCP Requests (DoS attack) abzufangen.

(config-if)# **ip dhcp snooping limit rate** *pps*

ACHTUNG: Option 82 (default gesetzt)
der Switch erweitert die DHCP Nachricht in der default-Einstellung mit der **Option 82**,
die folgende Informationen enthält:

- Eingehender Port des DISCOVER auf AccessLayer Switch
- MAC Adresses des AccessLayer Switch

.. und **zusätzlich** wird i.d. **GIADDR** Feld im DHCP Header die **0.0.0.0** eingetragen (ist generell für die IP eines DHCP Relay Agent vorgesehen, die der AccessLayer Sw nicht kennt).

ACHTUNG: mgl. wird eine DHCP Nachricht mit einem Wert von 0.0.0.0 im GIADDR Feld von einem DHCP Relay oder DHCP Server NICHT aktzeptiert und/oder weitergeleitet ..
.. dann sollte die Aktzeptanz mit folgendem Kommando eingestellt werden.
NUR auf Cisco Relay Agent oder Server notwendig – im SubConfiguration Mode des "ip-helper" Interfaces:

(config-if)# **ip dhcp relay information trusted**

Anstelle dessen (nicht empfohlen) kann dem Access Switch auch das Einfügen der Informationen verboten werden:

(config)# **no ip dhcp snooping information option**

Troubleshooting

show ip dhcp snooping
show ip dhcp snooping binding
show ip dhcp snooping statistics
show ip source binding

debug ip dhcp snooping events

IPSG - IP Source Guard (mit DHCP Snooping)

Nomalerweise hält der Switch die MAC Adressen angeschlossener Geräte zusammen mit der Port Nurmmer in seiner MAC Table, d.h. er hat keine Kenntniss, welche IP Adressen den jeweilingen MACs zugeordnet sind.

IPSG wertet die Einträge in der **IP DHCP Snooping Binding Table** aus, die folgende Informationen zu einem Client enthält: MAC Addresse, IP Adresse, VLAN ID und Port ID.

Dann wird auf diesem Port **nur Datenverkehr von der zulässigen Source IP Adresse** (und optional der zulässigen MAC) weitergeleitet.

HINWEIS: Wenn Clients statische IP Adressen verwenden, kann adminstrativ ein Eintrag für die IP DHCP Snooping Binding Table konfiguriert werden.

Arbeitsweise

1. An einem IPSG aktiven Port ist nach "link up" nur DHCP Datenverkehr möglich, bis ein entprechender Eintrag für den Port in der IP Source Binding Table existiert.
2. Nachdem IPSG einen Eintrag in der Binding Table gefunden hat, wird automatisch eine Port ACL (PACL) für das Interface erzeugt und aktiviert, die nur Datenverkehr von der entprechenden IP Adresse (und optional auch MAC Adresse) über diesen Port zulässt.

IPSG schützt vor **IP Spoofing DoS Attacken** .
IPSG kann nur auf switchports (access und trunk links) konfiguriert werden (nicht auf routed ports). Empfohlen ist die **Konfiguration auf untrusted access links NUR auf Access Layer Switches.**

Konfiguration IP Source Guard mit Source IP Filter .. nur Validierung der Src IP
→ IP DHCP Snooping muss aktiviert sein.

```
(config-if)# ip verify source
```

Konfiguraiton IP Source Guard mit Source IP and MAC Filter .. Validierung von Src IP u. MAC
→ IP DHCP Snooping muss aktiviert sein.
→ Cisco Switchport Security muss aktiviert sein
(sonst sind alle MACs zulässig → # sh ip verify source)

```
(config-if)# switchport port-security
(config-if)# ip verify source port-security
```

Optional: Manuelle Erzeugung eines IP Source Binding Eintrages

```
(config)# ip source binding MAC-address vlan vlan-id IP-address \
             interface if-type if-number
```

Troubleshooting

```
# show ip verify source
# show ip source binding
# show ip dhcp snooping binding

# debug ip verify source
```

Konfigurationsbeispiel: IP Source Guard mit Source IP und Source MAC Filter

```
!
ip dhcp snooping
ip dhcp snooping vlan 10
!
interface fa 0/2
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security mac-address 0001.abcd.efab
 ip dhcp snooping limit rate 100
 ip verify source port-security
!
```

DAI - Dynamic ARP Inspection (mit IP DHCP Snooping)

Dynamic ARP Inspection überprüft die Richtigkeit (korrekte IP-to-MAC Zuordnung) von ARP Nachrichten innerhalb eines Netzwerks.

.. und bietet so einen Schutz vor ARP spoofing und man-in-the-middle attacks.

Arbeitsweise

1. Der Switch unterbricht (eingehende) ARP Replys an untrusted ports
2. Der Inhalt der ARP Nachricht wird dann vom Switch auf Richtigkeit überprüft. Dies geschieht mit Hilfe der IP DCHP Snooping Binding Table.
3. Erst nach erfolgreicher Validierung erfolgt eine Update des internen ARP Cache und die Weiterleitung der ARP Nachricht.
4. War die Vallidierung nicht erfolgreich wird die ARP Nachricht gedroppt und eine Log-Meldung generiert (? und in den error-disable state geschaltet ?)

Guidelines

- DAI ist ein **ingress security feature**, d.h. es überprüft Frames nur wenn sie eingehen (ingress) und nicht wenn sie ausgehen (egress).

- DAI kann konfiguriert werden auf:
  - **access ports**
  - **trunk ports**
  - **Etherchannel ports**
  - **pVLAN ports**

- DAI sollte wie folgt auf Access Layer Switches konfiguriert werden
  - **untrusted** auf (allen) **access ports**
    Ports mit angeschlossenen Clients sollten validiert werden
  - **trust** auf (allen) **trunk ports**
    Auf Switch-to-Switch Verbindungen sollte und braucht keine Validierung (mehr) stattfinden.

- DAI benötigt **aktiviertes IP DCHP Snooping**, da es die Einträge innerhalb der DHCP snooping binding database verwendet.

  In Umgebungen ohne DHCP können **ARP ACLs** verwendet werden:
  Wenn Hosts mit statischen IP Adressen angebunden sind, und keine Einträge in der IP DHCP Binding Table existieren, kann eine statische ARP ACL mit notwendigen Einträgen adminstrativ erzeugt UND an den DAI Prozess angebunden werden.

  Wenn ARP Replys an einem Port eintreffen, überprüft der Switch zuerst die ARP ACL, wenn kein Eintrag existiert, wird die IP DHCP Snooping Table verwendet – mit static wird nur die ACL überprüft, dann greift das IMPLICIT DENY am Ende der ACL.

Konfiguration DAI

Globale Aktivierung von ARP Inspection für ein VLAN oder einen Bereich von VLANs.
Auch Angabe einer VLAN Liste möglich.

(config)# **ip arp inspection vlan** *vlan-id* [*vlan-id*]

Alle Interfaces (incl. trunks) des entsprechenden VLANs sind nach Aktivierung von ARP Inspection **default untrusted**. Verbindungen zu anderen Switches sollten trusted sein.

(config-if)# **ip arp inspection trust**

Wenn Hosts mit statischen IP Adressen angebunden sind kann eine statische ARP ACL mit notwendigen Einträgen adminstrativ erzeugt UND an den DAI Prozess angebunden werden.
.. mit static wird nur die ACL überprüft, dann greift das IMPLICIT DENY am Ende der ACL.

(config)# **arp access-list** *acl-name*
(config-acl)# **permit ip host** *IP* **mac host** *MAC* [**log**]

(config)# **ip arp inspection filter** *acl-name* **vlan** *vlan-id* [**static**]

Es werden default nur IP und MAC im ARP Reply (Nutzlast) überprüft
→ wird gegenüber den Einträgen innerhalb der IP DHCP Snooping Binding Table überprüft

Die Überprüfung kann sich optional aber auch zusätzlich für den ARP Reply verwendete Adressinformationen erstrecken:

- SRC MAC und/oder DST MAC im Ethernet Header
- und/oder SRC und DST IP im IP Header

→ wird genüber der Felder im ARP Reply (Nutzlast) überprüft

(config)# **ip arp inspection validate** { [**src-mac**] [**dst-mac**] [**ip**] }

src-mac	→ Src-MAC im Ethernet Header = MAC Adresse im ARP Reply
dst-mac	→ Dst-MAC im Ethernet Header = Target MAC im ARP Reply
ip	→ Src-IP im IP Header = IP im ARP Request
	→ Dst-IP im IP Header = Target IP im ARP Reply

Troubleshooting

show ip arp inspection interfaces
show ip arp inspection vlan *vlan-id*
show ip dhcp snooping binding

debug dai packet

Konfigurationsbeispiel
IP DHCP Snooping, IP Source Guard (incl. MAC Validierung) und Dynamic ARP Inspection

```
!
ip dhcp snooping
ip dhcp snooping vlan 10
no ip dhcp snooping information option
ip arp inspection vlan 10
!
interface fa 0/2
 description client link
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security mac-address 0001.abcd.efab
 ip dhcp snooping limit rate 5
 ip verify source port-security
 ip arp inspection limit rate 5
!
interface fa 0/2
 description switch-to-switch link
 switchport mode trunk
 ip dhcp snooping trust
 ip arp inspecton trust
!
```

Konfigurationsbeipiel: DHCP Snooping, IPSG, DAI

.. auf einem Access Layer Switch:

- Ports 1–10 → access VLAN 10 (10.1.10.0/24)
- Ports 11–20 → access VLAN 20 (10.1.20.0/24)
- Ports 23,24 → trunk zum Distribution Layer Switch (.. Verbindung zum DHCP Server)

- Endgeräte an den Ports 1 und 11 haben eine feste IP
  - IPSG → statischen Einträge in der IP Source Binding Table
  - DAI → ARP ACL
- Endgeräte an den Ports 2-10 und 12-20 beziehen die IP über DHCP Server

DHCP Snooping

```
!
ip dhcp snooping
ip dhcp snooping vlan 10,20
no ip dhcp snooping information option
!
int range fa 0/23 – 24
  ip dhcp snooping trust
!
int range fa 0/1 – 20
  ip dhcp snooping limit rate 5
!
```

IP Source Guard .. und für fa 0/1 auch Überprüfung der Source MAC (neben der SRC IP)

```
!
ip source binding 00ca.1234.aaaa vlan 10 interface fa 0/1
ip source binding 00ca.1234.bbbb vlan 10 interface fa 0/11
!
int range fa 0/2 – 20
  ip verify source
!
int fa 0/1
  switchport port-security
  switchport port-security mac-address 00ca.1234.aaaa
  ip verify source port-security
!
```

DAI .. SRC MAC im Ethernet Hdr. wird bei ARP Replys auch geprüft (nebst Infos im ARP Hdr.)

```
!
ip arp inspection vlan 10,20
ip arp inspection validate src-mac
!
int range fa 0/23 – 24
  ip arp inspection trust
!
int range fa 0/1 – 20
  ip arp inspection limit rate 5
!
arp access-list STATIC
  permit ip host 10.1.10.10 mac host 00ca.1234.aaaa log
  permit ip host 10.1.20.10 mac host 00ca.1234.bbbb log
!
ip arp inspection filter STATIC vlan 10,20
```

!