Мрежова сигурност на ниво 2

проф. д-р инж. Венета Алексиева,
проф. д-р инж. Христо Вълчанов

Основни моменти

- Защита с пароли
- Уязвимости на слой 2
- Сигурност на комутатори

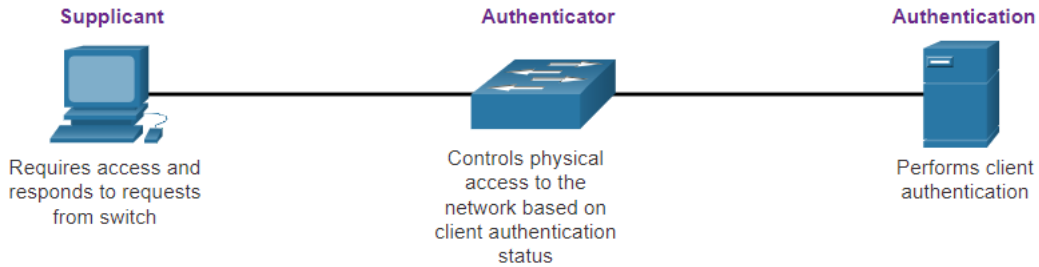
Автентикация с локална парола

- До крайно устройство – парола на устройството
- До мрежово устройство
  - За директен достъп - име и парола на конзолата, както и за различни режими за конфигуриране
  - За отдалечен достъп - име и парола на vty линиите и aux портовете
- Методът на локалната база данни има някои ограничения:
  - Потребителските акаунти трябва да бъдат конфигурирани локално на всяко устройство, което не е мащабируемо решение.
  - Методът не предоставя резервен метод за удостоверяване.

AAA

- Локално AAA удостоверяване:
  - Съхраняват се потребителски имена и пароли локално в мрежово устройство (напр. Cisco рутер).
  - Потребителите се удостоверяват спрямо локалната база данни.
  - Локалното AAA е подходящо за малки мрежи.
- Сървърно базирано AAA удостоверяване:
  - Мрежовите устройства имат достъп до централен AAA сървър, който съдържа потребителските имена и паролите за всички потребители.
  - За комуникация с AAA сървъра се използват се Remote Authentication Dial-In User Service (RADIUS) или Terminal Access Controller Access Control System (TACACS+).
  - Сървърно-базираното AAA е по-подходящо за големи мрежи.

IEEE 802.1X стандарт



- Стандартът IEEE 802.1X е базиран на контрол на достъпа през порт и протокол за удостоверяване.
- Протоколът ограничава неоторизираните работни станции да се свързват към LAN чрез публично достъпни портове на комутатора. Сървърът за удостоверяване удостоверява всяка работна станция, която е свързана към порт на комутатора, преди да направи достъпни услугите, предлагани от комутатора или LAN.
- Роли:
  - Клиент (заявител)
  - Суич или AP точка (Удостоверител) –посредник между клиента и сървъра за удостоверяване. Той изисква идентифицираща информация от клиента, проверява тази информация със сървъра за удостоверяване и предава отговор на клиента.
  - Сървър за удостоверяване – Сървърът потвърждава самоличността на клиента и уведомява комутатора или точката за безжичен достъп, че клиентът е или не е упълномощен за достъп до LAN.

Уязвимости на слой 2

- Ако слой 2 е компрометиран, всички слоеве над него също са засегнати.

Видове атаки	Пример
MAC Table Атаки	MAC address flooding
VLAN Атаки	VLAN hopping VLAN double-tagging Атака на устройства в една VLAN
DHCP Атаки	DHCP starvation DHCP spoofing
ARP Атаки	ARP spoofing ARP poisoning
Address Spoofing Атаки	MAC address spoofing IP address spoofing
STP Атаки	Spanning Tree Protocol manipulation

Решения за защита на слой 2

- Port Security
  - Предотвратява атаки като MAC address flooding, DHCP starvation
- DHCP Snooping
  - Предотвратява атаки като DHCP starvation, DHCP spoofing
- Dynamic ARP Inspection (DAI)
  - Предотвратява атаки като ARP spoofing, ARP poisoning
- IP Source Guard (IPSG)
  - Предотвратява атаки като MAC address spoofing, IP address spoofing

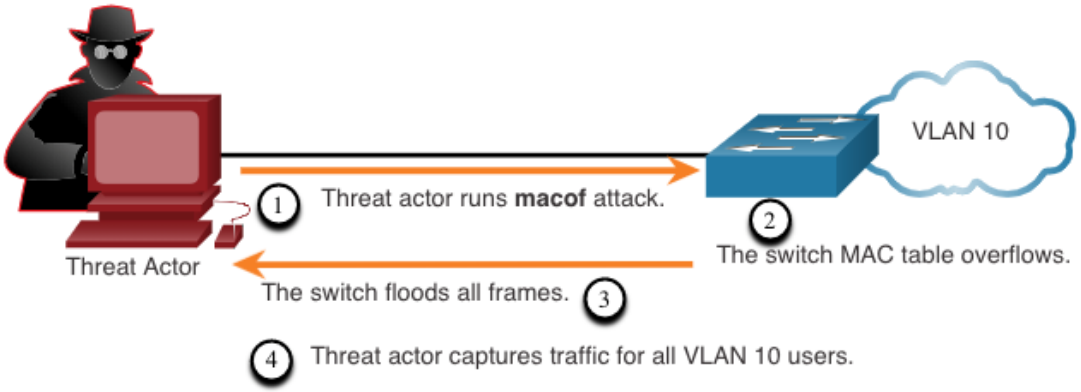
Защита на слой 2

- Винаги да се използват защитени варианти на протоколи за управление като SSH, Secure Copy Protocol (SCP), Secure FTP (SFTP), and Secure Socket Layer/Transport Layer Security (SSL/TLS).
- Да се използва отделна VLAN за управление, където не се пренася нищо друго освен трафик за управление.
- Да се използват ACL за филтриране на нежелан достъп.

Атаки към MAC таблицата

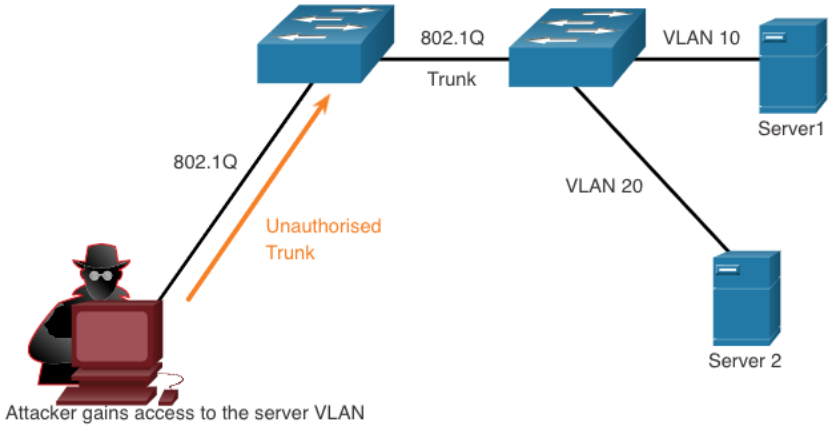
- Всички MAC таблици имат фиксиран размер.
- Атаките за наводняване на MAC адрес се възползват от това ограничение, като бомбардират комутатора с фалшиви MAC адреси на източника, докато таблицата с MAC адреси на комутатора се запълни.
- Тогава суичът третира фрейма като неизвестен уникаст и го изпраща по всички портове на тази VLAN.
- Това позволява на атакуващия да прихване всички фреймове, изпратени от един хост на друг в локалната LAN или локалната VLAN.
- Инструмент: macof

```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```



VLAN Hopping атака

- VLAN hopping атака позволява трафикът от една VLAN да бъде видян от друга VLAN без помощта на рутер.
- Тази атака конфигурира хоста да действа като комутатор, за да се възползва от функцията за автоматичен trunk порт с 802.1Q, активирана по подразбиране на повечето портове на комутатора.
- Така атакуващият хост има достъп до всички VLAN на комутатора и може да изпраща и получава трафик на всяка VLAN.



VLAN Double-Tagging атака

- Атакуващият слага скрит 802.1Q таг вътре във фрейма, който вече има 802.1Q таг. Този таг позволява на фрейма да отиде до VLAN, която оригиналният 802.1Q таг не е посочил.
- Стъпка 1: Атакуващият изпраща двойно маркиран 802.1Q кадър към комутатора. Външният хедър има VLAN тага на заплахата, който е същият като конфигурирания VLAN на порта на суича.
- Стъпка 2: Комутаторът препраща фрейма през всички свои VLAN портове след отстраняване на VLAN тага. Фреймът не се маркира повторно, защото е част от този VLAN. В този момент вътрешният VLAN етикет все още е непокътнат и не е бил проверен от първия комутатор.
- Стъпка 3: Фреймът пристига във втория суич. Native VLAN трафик не се маркира от изпращащия суич, както е посочено в спецификацията 802.1Q. Вторият суич разглежда само вътрешния 802.1Q таг, който е останал и изпраща фрейма към дестинацията по MAC адрес или я праща на всички в този VLAN, в зависимост от това дали има съществуващ запис в таблицата с MAC адреси за дестинацията.

VLAN Double-Tagging атака

- Атаката с двойно маркиране на VLAN е еднопосочна и работи само когато атакуващият е свързан към порт, намиращ се в същата VLAN като собствената VLAN на trunk порт.
- Двойното маркиране позволява на атакуващия да изпраща данни до хостове или сървъри във VLAN, които иначе биха били блокирани от някакъв тип конфигурация за контрол на достъпа.
- Предполага се, че обратният трафик също ще бъде разрешен, като по този начин ще даде възможност на атакуващия да комуникира с устройства в иначе блокираната VLAN.

Предотвратяване на VLAN атаки

- Деактивира се трънкинга на всички портове за достъп.
- Деактивира се автоматичния трънкинг на trunk връзки, така че те да се активират ръчно.
- Native VLAN да се използва само за trunk връзки.

ARP атаки

- Хостовете изпращат бродкастни ARP заявки за определяне на MAC адреса на хост по IP адрес. Всички хостове в подмрежата получават и обработват ARP заявката. Хостът със съвпадащия IP адрес в ARP заявката изпраща ARP отговор. Клиент може да изпрати непоискан ARP отговор, наречен „ gratuitous ARP“. Другите хостове в подмрежата съхраняват MAC адреса и IP адреса от него в своите ARP таблици.
- Атакуващият може да изпрати gratuitous ARP съобщение, съдържащо фалшив MAC адрес, до суич и той ще актуализира своята MAC таблица. Атакуващият изпраща нежелани ARP отговори до други хостове в подмрежата с MAC адреса си и IP адреса на gateway, като така настройва атака „man in the middle".

STP атака

- Това е атака чрез подправяне на root bridge и промяна на топологията на мрежата с цел атакуващият да прихване целия трафик за този домейн.
- За да проведе STP манипулираща атака, атакуващият хост излъчва broadcasts STP bridge protocol data units (BPDUs) , съдържащи промени в конфигурацията и топологията, които ще предизвикат преизчисляване на spanning-tree.
- BPDU, изпратени от атакуващия хост, обявяват по-нисък приоритет на суича в опит да бъдат избрани като root bridge.
- Тази STP атака се смекчава чрез прилагане на BPDU Guard на всички портове за достъп.

Въпроси ?

Благодаря за вниманието !