CYBER DEFENSE

❖ حسین ملک زاده

مشاور و تحلیل گر ارشد امنیت سایبری

کارشناس ارشد امنیت اطلاعات ازدانشگاه Sapienza Universityرم – ایتالیا

مدرس و عضو هیات علمی دانشگاه بین المللی نورث وست Northwest International University

مدرس و عضو هیات علمی دانشگاه نیوجرسی New Jersey International Open University

مدرس و عضو هیات علمی موسسه دانشگاهی DEI Institute - Online Universityآفریقا

دارای مدرک دکترا مدیریت امنیت سایبری DBA - Cyber Security Management از دانشگاه بین المللی نورث وست

ممیز و سرممیز امنیت اطلاعات ISMS ISO27001-2013

دارای مدارک سطح عالی امنیت اطلاعات CISSP , CISA

دارای مدرک مشاور ارشد امنیت سیستمی SSCP

طراح – مشاور و مجری پروژه¬های شبکه و امنیت اطلاعات ISMS , SOC , NOC

دارای بیش از ۲۴ سال سابقه آموزشی – اجرایی و مدیریتی درزمینه پروژه¬های شبکه و امنیت در داخل و خارج از کشور

مدرس دوره¬های تخصصی شبکه و امنیت با بیش از دوازده هزارساعت تدریس درموسسات داخلی و بین المللی

دارای تحصیلات و مدارک بین المللی :

MCSE , CCNA ,CCNA Security , CCNP , CEH , CISSP , CWNA , ISMS , SSCP, GSNA

عضوانجمن مهندسین کامپیوتر و فناوری آمریکا IEEE , ACM

مولف کتاب هنر هک کردن انسان در حوزه امنیت در مهندسی اجتماعی Social engineering

www.Hosseinmalekzadeh.com

Mobile: 09153133217

E-mail: Hoseeinmalekzadeh@Gmail.com

Telegram Channel : https://t.me/HosseinMalekzadeh

http://www.linkedin.com/in/hosseinmalekzadeh

@HOSSEINMALEKZADEH2015

@HOSSEINMALEKZADEH

By. Hossein Malekzadeh

Cyber Security Consultant and Manager

www.Hosseinmalekzadeh.com

Mobile : 09153133217

نقشه شبکه سازمان (دفتر مرکزی)

سناریوی سازمان

یک سازمان متوسط با حدود ۵۰۰ کارمند
دارای دفتر مرکزی و دو شعبه
خدمات اصلی سازمان شامل:

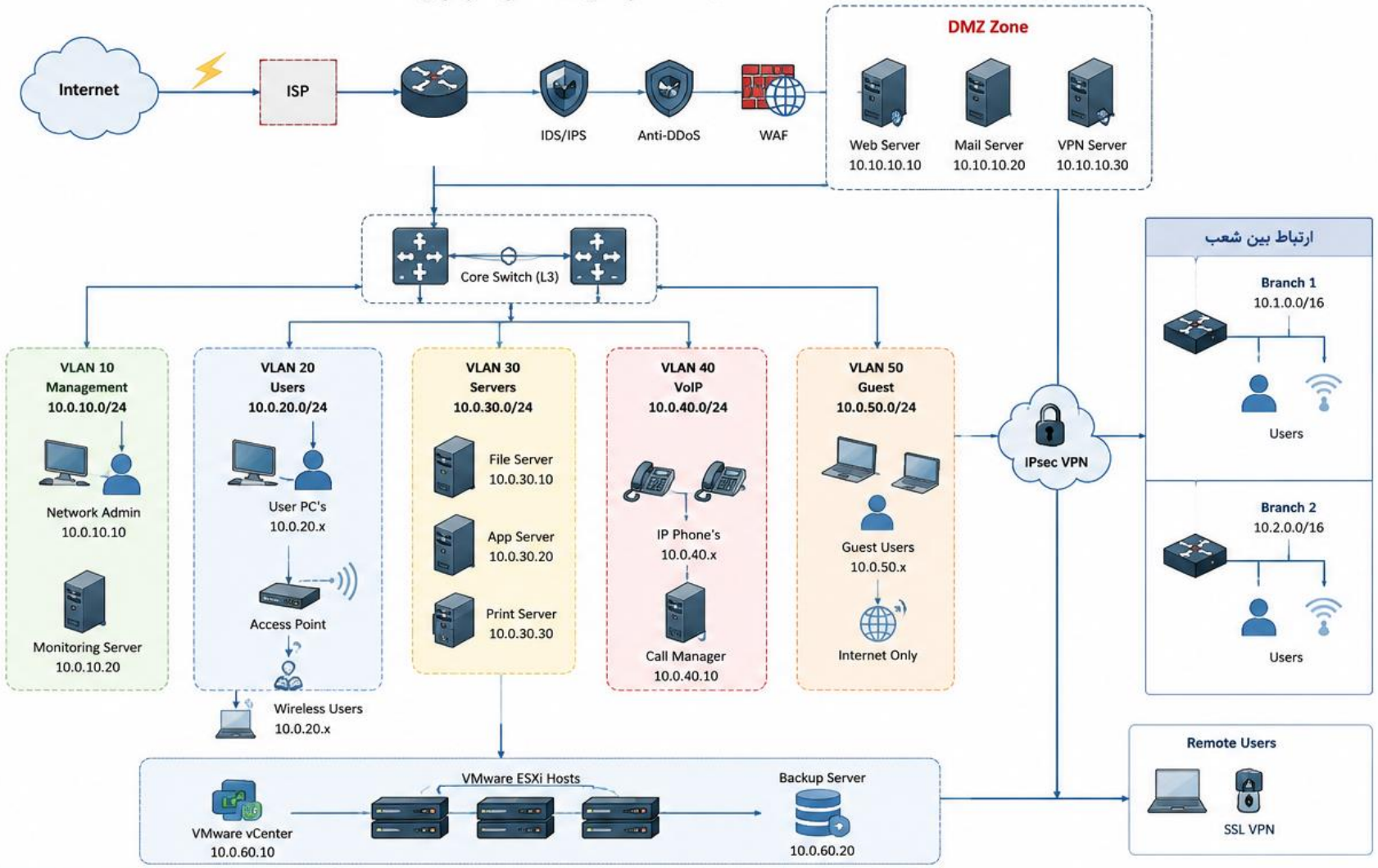
- سرویس های دایرکتوری (Active Directory)
- سرورهای فایل و پرینت
- سرور برنامه کاربردی تحت وب
- سیستم تلفنی تحت شبکه (VoIP)
- دسترسی کاربران به اینترنت
- ارتباط امن بین شعب از طریق VPN
- زیرساخت مجازی سازی با VMware

اهداف امنیتی

- حفاظت لایه به لایه از اطلاعات و سرویس ها
- جلوگیری از دسترسی غیرمجاز
- جلوگیری از حرکت جانبی مهاجم در شبکه
- مانیتورینگ و پاسخ به رخدادها
- پشتیبان گیری و تداوم کسب و کار

چالش ها / تهدیدات

- حملات اینترنتی (Brute Force, Exploit, DDoS)
- فیشینگ و مهندسی اجتماعی
- بدافزار و باج افزار
- تهدیدات داخلی و دسترسی بیش از حد
- نشت اطلاعات
- خرابی تجهیزات و از دسترس خارج شدن سرویس ها



راهنمای نمادها

اینترنت — کلاینت — فایروال / روتر
سیستم امنیتی — تلفن تحت شبکه — سوئیچ لایه ۳
دسترسی بی سیم — سرور

نکات طراحی امنیتی (Defense in Depth)

- لایه محیطی: فایروال, IDS/IPS, Anti-DDoS, WAF
- لایه شبکه: تقسیم بندی VLAN, Private VLAN, Private VLAN Security
- لایه سیستم: هاردنینگ سررورها و کلاینت ها، بروزرسانی Patch Management
- لایه هویت و دسترسی: Mtive Directory Security, Least Privilege Security
- لایه مانیتورینگ: جمع آوری و تحلیل لاگ ها در SIEM
- لایه داده: رمزنگاری: DLP, Backup منظم
- لایه پنجم پاسخ: Incident Response Plan و تمرین دوره ای

جدول آدرس دهی

VLAN	Network	Gateway	Description
10	10.0.10.0/24	10.0.10.1	Management
20	10.0.20.0/24	10.0.20.1	Users
30	10.0.30.0/24	10.0.30.1	Servers
40	10.0.40.0/24	10.0.40.1	VoIP
50	10.0.50.0/24	10.0.50.1	Guest
60	10.0.60.0/24	10.0.60.1	Virtualization/Backup
DMZ	10.10.10.0/24	10.10.10.1	DMZ Zone

بررسی امنیت در لایه ۲ شبکه

توپولوژی امن سازی لایه 2 و 3 با استفاده از سوئیچ و روتر

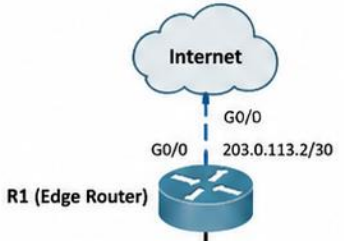
(برای پیاده سازی در Packet Tracer)

اهداف

- امن سازی لایه 2 با استفاده از قابلیت های سوئیچ
- امن سازی لایه 3 با استفاده از ACL روی روتر
- تفکیک شبکه با VLAN
- احراز هویت دسترسی به سوئیچ (SSH)
- جلوگیری از حملات رایج لایه 2

راهنما

- لینک اترنت
- لینک ترانک 802.1Q
- لینک سریال / WAN



امن سازی لایه 3 (روی روتر (R1)

- Extended ACL برای کنترل دسترسی بین VLAN ها
- فقط اجازه دسترسی به سرور از VLAN های مجاز
- مسدود کردن دسترسی بین VLAN های کاربری
- جلوگیری از دسترسی به شبکه مدیریت از بیرون
- NAT Overload برای دسترسی کاربران به اینترنت

شبکه ها و VLAN

VLAN 10 – USERS	192.168.10.0/24
VLAN 20 – SERVERS	192.168.20.0/24
VLAN 30 – GUESTS	192.168.30.0/24
VLAN 99 – MGMT	192.168.99.0/24

Gateway (SVI روی MLS1)

VLAN10:	192.168.10.1
VLAN20:	192.168.20.1
VLAN30:	192.168.30.1
VLAN99:	192.168.99.1

امن سازی لایه 2 (روی سوئیچ های دسترسی)

- خاموش کردن پورت های استفاده نشده
- Port Security (محدود کردن MAC Address
- BPDU Guard + Root Guard
- DHCP Snooping
- DAI (Dynamic ARP Inspection)
- جلوگیری از حمله CAM Table (Port Security + Shutdown)
- دسترسی امن به سوئیچ با SSH و غیرفعال کردن Telnet

VLAN 99 فقط برای مدیریت سوئیچ ها استفاده می شود
IP مدیریت سوئیچ ها در شبکه 192.168.99.0/24

مدیریت امن

- فقط از VLAN 99 و VLAN 9
- غیرفعال کردن HTTP و Telnet
- رمزنگاری رمزهای عبور
- Banner Login

سیاست‌های دسترسی (R1) روی (R1)

اجازه:

- فقط VLAN 10 به Server1 (192.168.20.10) و Server2 (192.168.20.20)
  VLAN 30 فقط به اینترنت

مسدود:

VLAN 30 به VLAN 10
VLAN 10 و VLAN 20 به VLAN

- هرگونه دسترسی به شبکه مدیریت (192.168.99.0/24) از بیرون
  سایر ترافیک های غیر مجاز

- اغلب کارشناسان، برقراری امنیت در لایه دو شبکه (Data-Link layer)را نادیده می گیرند. این در حالیست که لایه دو شبکه کلید دسترسی به سایر لایه هاست بنابراین در صورت امن نبودن این لایه، کل شبکه در معرض نفوذ قرار خواهد گرفت.

- اغلب سازمان ها معمولا به دنبال تامین امنیت و جلوگیری از حملات از سمت Outside به Inside و DMZ هستند حال اینکه در جهت خلاف این مسیر یعنی از Insideو DMZبه سمت Outsideتمهیدات و پیکربندی های امنیتی انجام نمی شود یا بطور ناقص انجام می پذیرد.

- این مورد می تواند باعث ایجاد حفره های امنیتی در شبکه و سیستم های یک سازمان، فراهم ساختن امکان نفوذ به شبکه برای هکرها و مهاجمان سایبری و در نهایت تحمیل خسارت های جبران ناپذیری به سازمان یا مختل شدن شبکه سازمان شود.

- تصور کنید کاربری ناآگاهانه ایمیلی حاوی یک تروجان را باز می کند، این تروجان روی سیستم کاربر اجرا شده و شروع به اسکن سیستم کاربر و سپس کل IP range شبکه جهت شناسایی شبکه و رسیدن به سایر مقاصد مخرب خود می کند. همین شرایط و شرایط مشابه نیز توسط مهاجمان Insider می تواند اتفاق بیفتد.

- شاید در اینجا این موضوع اغلب با نصب یک آنتی ویروس قدرتمند قابل حل است و مرتبط به لایه هفت شبکه می باشد اما با کمی تامل درمیابیم اسکن IP range شبکه و شناسایی منابع شبکه و سایر سیستم ها در لایه دو، سه و چهار مدل OSI رخ می دهد

تفاوت سویچ های لایه ۲ و ۳

سوئیچ لایه سه	سوئیچ لایه دو
در لایه Network فعالیت می‌کند	در لایه Data Link فعالیت می‌کند
از آدرس IP برای مسیردهی پکت‌ها استفاده می‌کند	فریم‌ها را براساس مک آدرس به مقصد ارسال می‌کند
توابع هر دو سوئیچ لایه دو و لایه سه را اجرا می‌کند	فقط با مک آدرس کار می‌کند
برای پیاده سازی VLANS استفاده می‌شود	برای کاهش ترافیک LAN استفاده می‌شود
سرعت بالایی ندارد	سرعت بالایی دارد
دامنه پخش چندگانه دارد	دارای یک دامنه پخش واحد است
در داخل و خارج شبکه ارتباط برقرار می‌کند	در داخل یک شبکه ارتباط برقرار می‌کند

مهمترین تهدیدات سایبری در لایه 2

- **VLAN Hopping**

- همانطور که می دانید دسترسی از یک VLAN به VLAN دیگر در لایه دو امکان پذیر نیست و تنها در لایه سه با استفاده از روتر و VLAN Routing این امکان فراهم می شود.

- VLAN Hopping نوعی از حملات است که توسط آن هکر می تواند در لایه دو شبکه از یک VLAN به VLAN دیگر دسترسی پیدا کند. این حملات به دو شیوه Switch spoofing و Double Tagging قابل اجراست.

• MAC Flooding

- از آنجایی که MAC پروتکلی است که در لایه دو مورد استفاده قرار می گیرد، بدون در نظر گرفتن تمهیدات امنیتی برای این پروتکل، یک هکر می تواند با هدف قرار دادن CAM Table سوئیچ ها باعث بوجود آمدن CAM Overflow شده در نتیجه می تواند به شنود ترافیک شبکه بپردازد.

- این ترافیک می تواند حاوی اطلاعات حساس شرکت از جمله اطلاعات مالی، ترافیک صدا در شبکه، پسورد سیستم ها، سرورها، تجهیزات و ... باشد.

- **DHCP Attacks**

- DHCP Starvation و Rogue DHCP در این حملات، مهاجم با برادکست نمودن درخواست های DHCP توسط آدرس های مک جعلی و ساختگی باعث استفاده شدن تمام آدرس های DHCP Address Pool می شود در نتیجه DHCP آدرسی برای اختصاص به سایر درخواست های DHCP ندارد.

- اینجاست که هکر با راه اندازی یک DHCPجعلی (Rogue DHCP)براحتی می تواند سیستم های یک شبکه را مورد سوء استفاده قرار دهد.

• ARP Table Poisoning

- همه ما با نحوه عملکرد پروتکل ARP در شبکه آشنایی داریم اما یک نکته جالب در مورد این پروتکل وجود دارد و آن اینست که هر کلاینت اجازه دارد یک ARP Reply را بدون اینکه کلاینتی ARP Request بفرستد بصورت برادکست ارسال کند در اصطلاح به این فریم ارسالی Gratuitous ARP گفته می شود و صرفا جهت معرفی آدرس مک کلاینت توسط خود کلاینت به سایر کلاینت ها استفاده می شود.

- یک هکر می تواند از این ویژگی استفاده کند و خود را به عنوان یک کلاینت دیگر در شبکه بطور مثال گیت وی شبکه معرفی کند در نتیجه آدرس مک هکر به جای آدرس مک گیت وی شبکه در ARP Table کلاینت ها قرار می گیرد.
- بدین ترتیب درخواست کلاینت ها به جای ارسال به گیت وی به سمت هکر هدایت می شود. با این روش ترافیک شبکه که می تواند حاوی اطلاعات حساس از جمله پسورد سیستم ها و ... باشد توسط هکر مورد شنود قرار گیرد.

- Spoofing Attacks

- MAC Spoofing

- تکنیک استفاده از آدرس مک سیستمی درگیر در شبکه جهت مقاصد خراب کارانه تحت عنوان MAC Spoofing شناخته می شود.

- تصور کنید در شبکه ای یک هکر آدرس مک خود را به آدرس مک یکی از سیستم ها در شبکه تغییر دهد در این شرایط CAM table سوئیچ نیر تغییر می کند. با این عمل، ترافیک شبکه به آن سیستم خاص به سیستم هکر هدایت شده و در این صورت هکر می تواند ترافیک ارسالی به سیستم مورد نظر را بطور موقت شنود کند

• STP Attacks

- در شبکه همواره لینک های Redundant از اهمیت ویژه ای برخورد بوده اند این اهمیت در لینک های Redundant بین سوئیچ ها نیز کاملا محسوس است. اما در این شرایط امکان ایجاد لوپ در شبکه وجود دارد بنابراین پروتکلSTP برای جلوگیری از Loop در لایه دو شبکه بوجود آمد. این پروتکل در صورت نادیده گرفتن تمهیدات امنیتی در این لایه براحتی می تواند مورد سوء استفاده قرار گیرد.

- بطور خلاصه پروتکل STP در شبکه برای تعیین سوئیچ Root bridge و تعیین لینک فعال بین لینکهای Redundant از پروتکل BPDU استفاده می کند. Root bridge سوئیچی است که ترافیک شبکه از طریق این سوئیچ به سایر بخشهای شبکه منتقل می شود.

- حال تصور کنید یک هکر در شبکه سیتسم خود را به عنوان یک سوئیچ در شبکه معرفی کند و در نهایت با ارسال فریم های BPDU با پارامترهایی خاص، خود را به عنوان Root Bridge می شناساند بنابراین قادر به شنود ترافیک شبکه خواهد بود.

- **CDP Attacks**

- در واقع از پروتکل CDP نه برای حمله بلکه جهت کسب و جمع آوری اطلاعاتی در خصوص شبکه (CDP Sender, IP Address, Software Version, Device Model,...) و توپولوژی شبکه مورد استفاده قرار می گیرد. علاوه بر جمع آوری اطلاعات، این پروتکل در IOSهای سیسکو در ورژن های قبل از ۱۲،۱(۱۰،۱) آسیب پذیر بوده طوری که با ارسال پکت های بی شمار CDPبه یک سوئیچ(CDP Flooding)، سوئیچ Crashکرده و نیاز به ریستارت داشته است.

حمله MAC Flooding

- حمله MAC address flooding یا حمله CAM table flooding نوعی حمله به شبکه سازمان ها می‌باشد که در آن حمله‌کننده به یک سوئیچ در شبکه متصل است و این سوئیچ را با بسیاری از Ethernet Frame ها که تماماً دارای MAC Address های جعلی می‌باشند، پر می‌کند.
- از این پس سوئیچ بدلیل پر شدن جدول CAM خود نمی تواند MAC جدید را دریافت کند؛ در نتیجه سوئیچ بسته های دریافتی که آدرس مقصد آنها را در جدول CAM ندارد، روی تمام پورت ها ارسال می کند.
- سیستم حمله کننده نیز این Frameها را دریافت کرده و می‌تواند به‌راحتی به Capture کردن این ترافیک‌ها بپردازد و اطلاعات حساسی نیز از این بررسی‌ها به دست آورد.

- **پر شدن جدول CAM دو مشکل به وجود می آورد:**

- باعث ایجاد ترافیک بیشتر در شبکه می شود که در نتیجه آن، تجهیزات شبکه نیز مجبور به پردازش این ترافیک اضافه می شوند و حتی باعث از کار افتادن تجهیزات به خاطر ترافیک زیاد خواهد شد.

- ترافیک چون روی همه پورت ها ارسال می شود سیستمی که مقصد ترافیک نیست نیز این ترافیک را دریافت می کند در نتیجه محرمانگی اطلاعات در این حالت از بین می رود.

S1

```
S1#show mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
cc02.1478.0000          Self        1     Vlan1
0050.56c0.0008          Dynamic     1     FastEthernet1/0
c201.1a90.0000          Dynamic     1     FastEthernet1/2
0050.56c0.0001          Dynamic     1     FastEthernet1/1

S1#
```

- در مرحله بعد با ساختن MAC آدرس جعلی و ارسال آن به سمت CAM، جدول از داده های جعلی اشباع می شود.

```
root@kali: ~/Desktop
File  Edit  View  Search  Terminal  Help
9594067(0) win 512
b8:98:eb:7c:bf:ee 42:83:e8:26:ff:13 0.0.0.0.55687 > 0.0.0.0.25808: S 761779879:7
61779879(0) win 512
c2:16:80:20:da:fb 74:8f:5c:4c:d9:8a 0.0.0.0.29810 > 0.0.0.0.30351: S 519706600:5
19706600(0) win 512
7a:f7:60:55:d3:28 94:11:54:76:15:80 0.0.0.0.42368 > 0.0.0.0.64499: S 946440424:9
46440424(0) win 512
37:23:d7:b:f5:56 43:5d:45:51:38:d9 0.0.0.0.50210 > 0.0.0.0.17533: S 826711423:82
6711423(0) win 512
f7:8b:34:5c:8:6 6c:22:a0:21:fc:43 0.0.0.0.38112 > 0.0.0.0.34131: S 981290977:981
```

- در تصویر زیر تعداد MACهای داخل جدول قبل و بعد از حمله در قسمت Total MAC address قابل مشاهده است.

```
S1#show mac-address-table count
NM Slot: 1
--------------

Dynamic Address Count:                     6841
Secure Address (User-defined) Count:       0
Static Address (User-defined) Count:       0
System Self Address Count:                 1
Total MAC addresses:                       6842
Maximum MAC addresses:                     8192

S1#show mac-address-table count
NM Slot: 1
--------------

Dynamic Address Count:                     7326
Secure Address (User-defined) Count:       0
Static Address (User-defined) Count:       0
System Self Address Count:                 1
Total MAC addresses:                       7327
Maximum MAC addresses:                     8192
```

- روش مقابله با حمله MAC flooding
- به منظور مقابله با حمله MAC flooding می توان قابلیت امنیتی Port Security را بر روی سوئیچ فعال کرد.

- یکی از تکنیک های مهم ادمین های یک شبکه اعمال سیاست های خاص مطابق با توپولوژی آن سازمان هست محدود کردن یک پورت یا اینترفیس سویچ به یک سری سیاست ها حائز اهمیت است

- برای اینکه پورت های فیزیکی یک سویچ از لحاظ اتصالات و دسترسی امن باشد و از دسترسی های غیرمجاز جلوگیری شود یکی از این سیاست ها اعمال port security در سویچ می باشد

- Switch(config)# interface interface_id
- Switch(config-if)# switchport mode access
- Switch(config-if)# switchport port-security
- Switch(config-if)# switchport port-security mac-address sticky
- Switch(config-if)# switchport port-security maximum value
- Switch(config-if)# switchport port-security violation {restrict | shutdown}
- Switch(config-if)# end

- برای SECURITY VIOLATION اقدام (Action) می توانید مشخص کنید که عبارتند از:
- Protection: هنگامی که یک Violation ایجاد شود پورت به کارکرد خود ادامه می دهد. آدرس های MAC مجاز به درستی کار می کنند ولی آدرس های غیر مجاز drop می شوند. ویژگی اصلی این حالت این است که شما به عنوان مدیر شبکه به شما اطلاع داده نمی شود که یک نقض امنیتی رخ داده است.

- Restriction: هنگامی که یک violationایجاد شود پورت به کار خود ادامه می دهد آدرس های MACمجاز به درستی کار می کنند ولی آدرس های غیر مجاز drop می شوند.در این حالت به شما اطلاع داده می شود که تخلف امنیتی رخ داده است و SNMP Trap ارسال می شود، یک پیام syslog ایجاد می شود و شمارنده نقض نیز افزایش می یابد. تمام این موارد یک نقض امنیت در پورت سوئیچ به شما اطلاع می دهد.

- Shutdown: نقض امنیت پورت باعث می شود که اینترفیس بلافاصله غیرفعال err-disable شود و همچنین چراغ پورت را خاموش می کند. SNMP trap را ارسال می کند، شمارنده را افزایش می دهد و پیام syslog را نیز ارسال می کند. هنگامی که یک پورت در حالت خطا err-disable قرار دارد می توانید با shut و no-shut کردن آن را دوباره فعال کنید. این حالت به صورت پیش فرض فعال است.

- : Port Security Monitoring
- به منظور بررسی و مانیتورینگ وضعیت پورت های Secure می توان از دستور زیر استفاده کرد :
- **Switch# show port-security interface**

```
Switch# show port-security address
           Secure Mac Address Table
-----------------------------------------------------------------
Vlan    Mac Address        Type                  Ports    Remaining Age
                                                            (mins)
----    -----------        ----                  -----    -------------
   1    0004.00d5.285d     SecureDynamic         Fa0/18        -
-----------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024

Switch# show port-security interface fa0/18
Port Security                          : Enabled
Port Status                            : Secure-up
Violation Mode                         : Shutdown
Aging Time                             : 0 mins
Aging Type                             : Absolute
SecureStatic Address Aging             : Disabled
Maximum MAC Addresses                  : 1
Total MAC Addresses                    : 1
Configured MAC Addresses               : 0
Sticky MAC Addresses                   : 0
Last Source Address                    : 0004.00d5.285d
Security Violation Count               : 0

Switch#
```

Configuring the Router for SSH

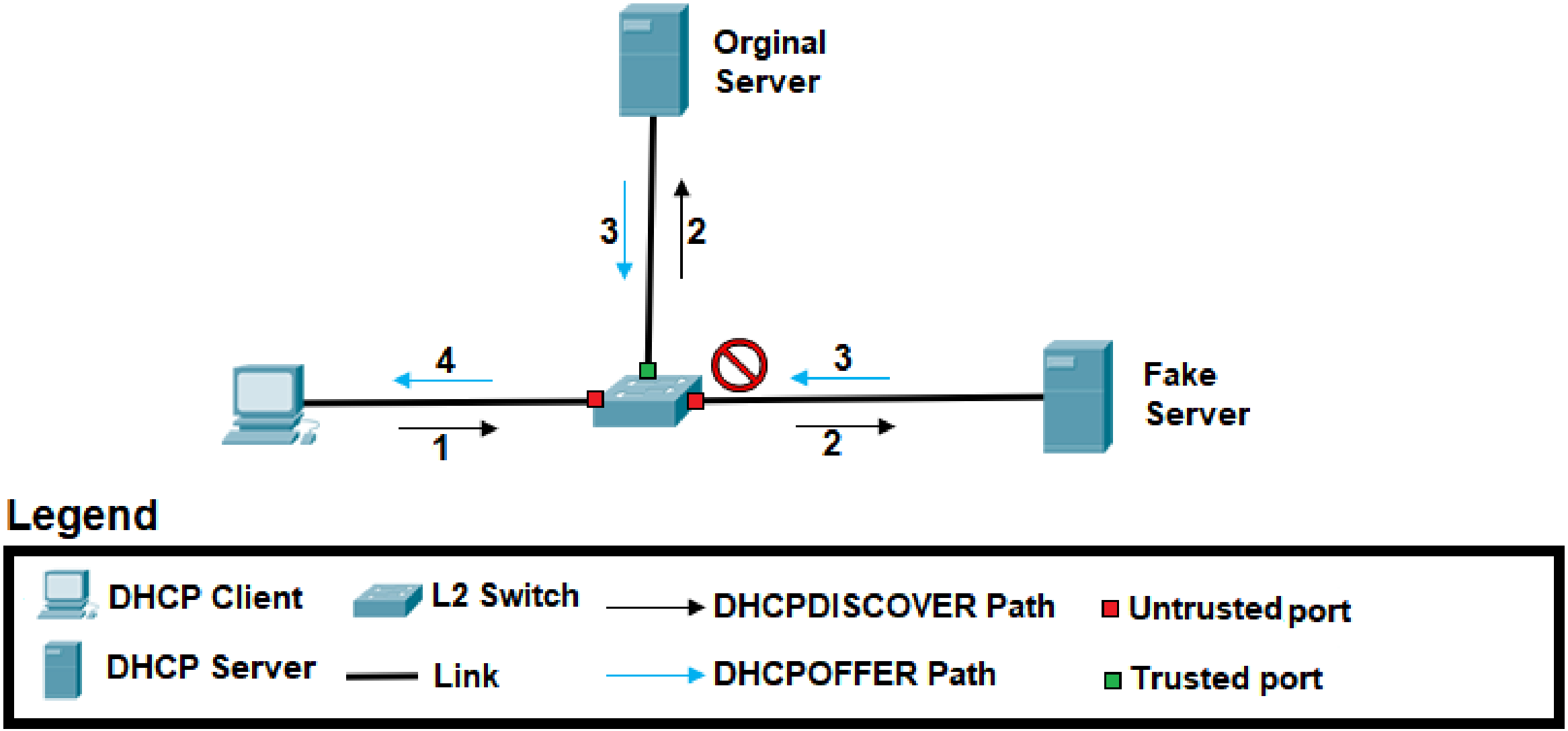
```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

```
R1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication
retries: 3
R1#
R1# conf t
Enter configuration commands, one per line.  End
with CNTL/Z.
R1(config)# ip ssh version 2
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
R1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication
retries: 2
R1#
```

DHCP snoopingچیست و چگونه راه اندازی می شود؟

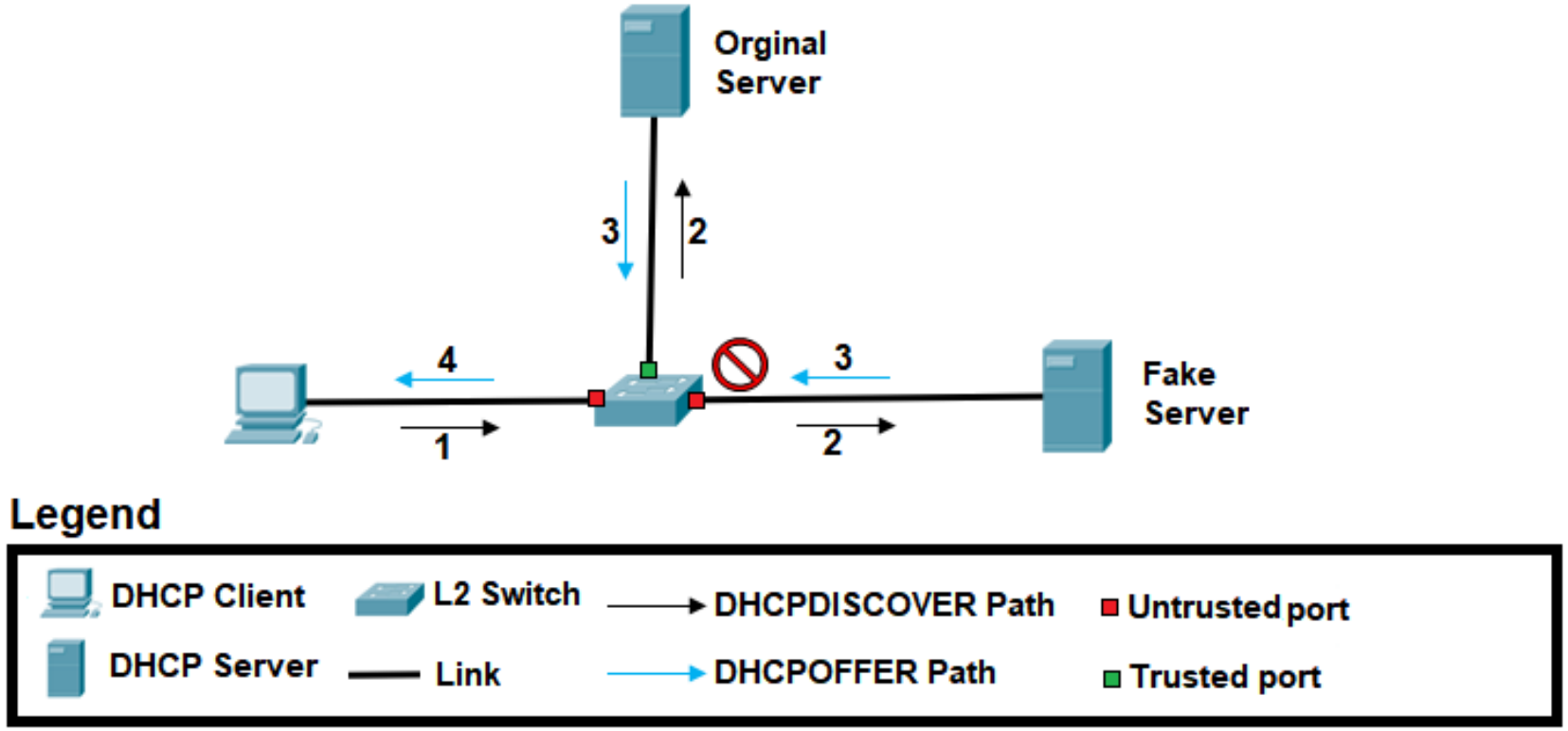


- قابلیت DHCP-Snooping در سوئیچ های سیسکو برای مدیریت حملات جعل هویت DHCP سرور استفاده می شود.

- با استفاده از این مکانیسم پورت های سوئیچ در دو حالت مختلف تنظیم می شود:

- حالت قابل اعتماد (trusted)
- حالت غیر قابل اعتماد (untrusted)

- اگر پورت پیکربندی شده باشد در حالت trusted باشد می تواند پاسخهای DHCP responses را دریافت کند.
- ولی اگر یک پورت در حالت untrusted باشد مجاز به دریافت پاسخ های DHCP نخواهد بود و اگر روی یک پورت rouge DHCP یا DHCP سرور جعلی وجود داشته باشد با دریافت پیام های DHCP responses اون پورت غیر فعال می شود.



- پیکربندی کلیه پورت های سوئیچ برای حالتهای مورد اعتماد و غیر قابل اعتماد، کار طولانی و کسل کننده ای خواهد بود، بنابراین فقط پورت سوییچ متصل به DHCP سرور نیاز است که به صورت مورد اعتماد پیکربندی شود.
- اگر پورت به عنوان پورت قابل اعتماد تنظیم نشده باشد به طور پیش فرض پورت غیر قابل اعتماد محسوب می شود. برای پیکربندی این قابلیت باید قابلیت DHCP Snooping را در مود Global فعال کنیم:

```
Switch1(config)#ip dhcp snooping
```

- ما این امکان را داریم که فقط برای تعدادی از VLAN ها این قابلیت را فعال کنیم. برای این کار لازم است دستور زیر را در مود Global واردکنیم:

- Switch1(config)#ip dhcp snooping vlan 10-15

- این دستور قابلیت DHCP snoopingرا برای vlan های ۱۰ تا ۱۵ فعال می کند.

- پیکر بندی پورت DHCP-Server در DHCP snooping:
- فقط فعالسازی این قابلیت کافی نیست و ما باید برخی از پورت های سوئیچ را که به DHCP-Server متصل هستن به صورت Trust با استفاده از دستورات زیر پیکربندی کنیم:

- Switch1(config)#interface eth 0/3

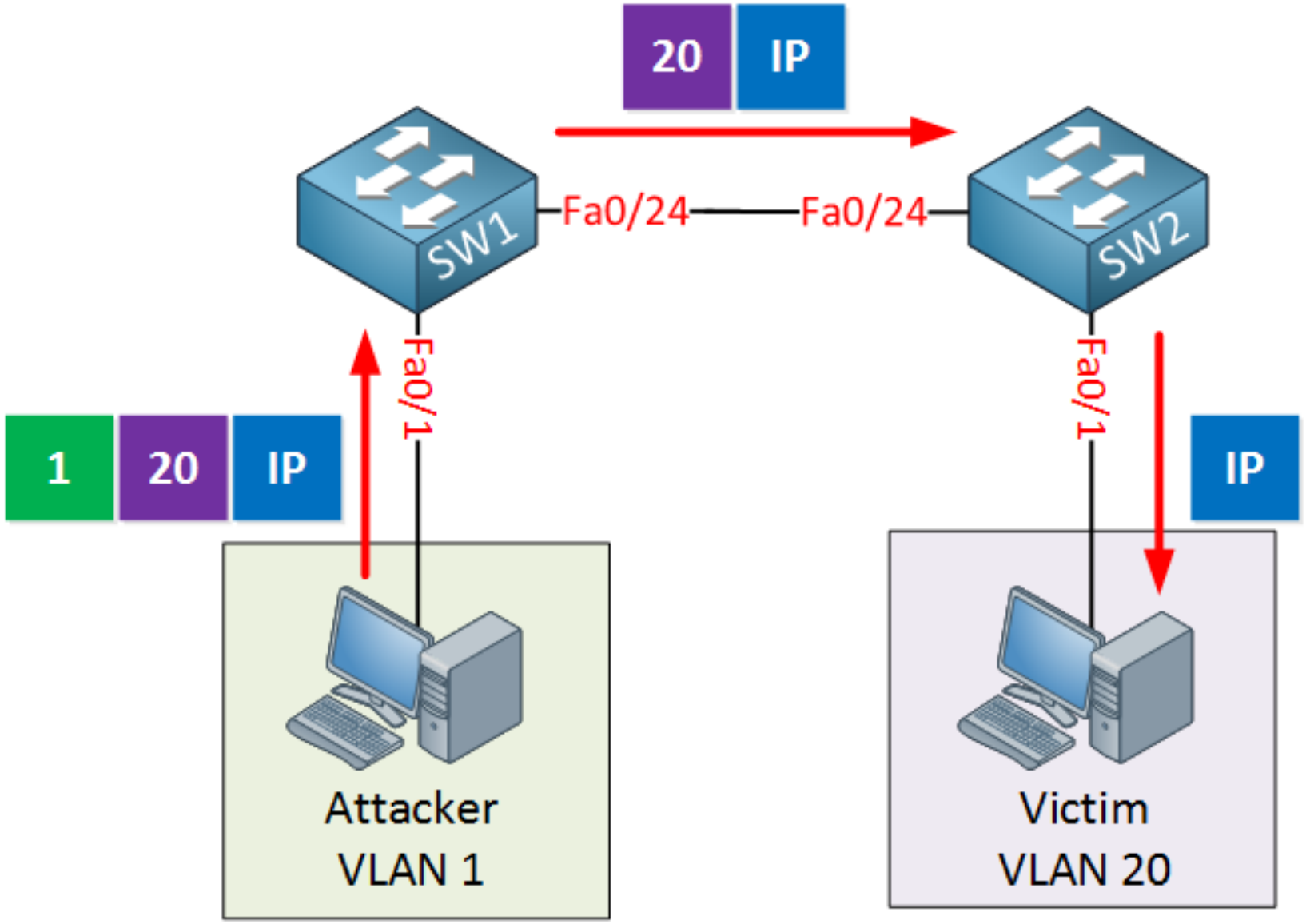
- Switch1(config-if)#ip dhcp snooping trust

- **تنظیم محدودیت های پیام های DHCP روی پورتهای سوییچ**
- حمله DoS به سرور DHCP نوع دیگری از حمله است که نفوذگر می تواند با یک تکنیک خاص آن را کند و یا از کار بی اندازد.
- این حمله با ارسال درخواستهای بسیار برای IP انجام میشود و DHCP-Server نیز همه آنها را پردازش کرده و پاسخ می دهد.
- برای برطرف کردن این نوع حمله می توان این ویژگی امنیتی لایه ۲ را تنظیم کرد تا تعداد پیام های DHCP در ثانیه را که مجاز به عبور از پورتهای سوئیچ هستند را محدود کند.
- در این روش ما مانع از جاری شدن سیل درخواست های DHCP غیر واقعی خواهیم کرد. برای تعیین حد مجاز پیام های DHCP در یک پورت به پنج پیام در هر ثانیه از این دستور استفاده می کنیم:

- Switch1(config)#interface eth 0/0

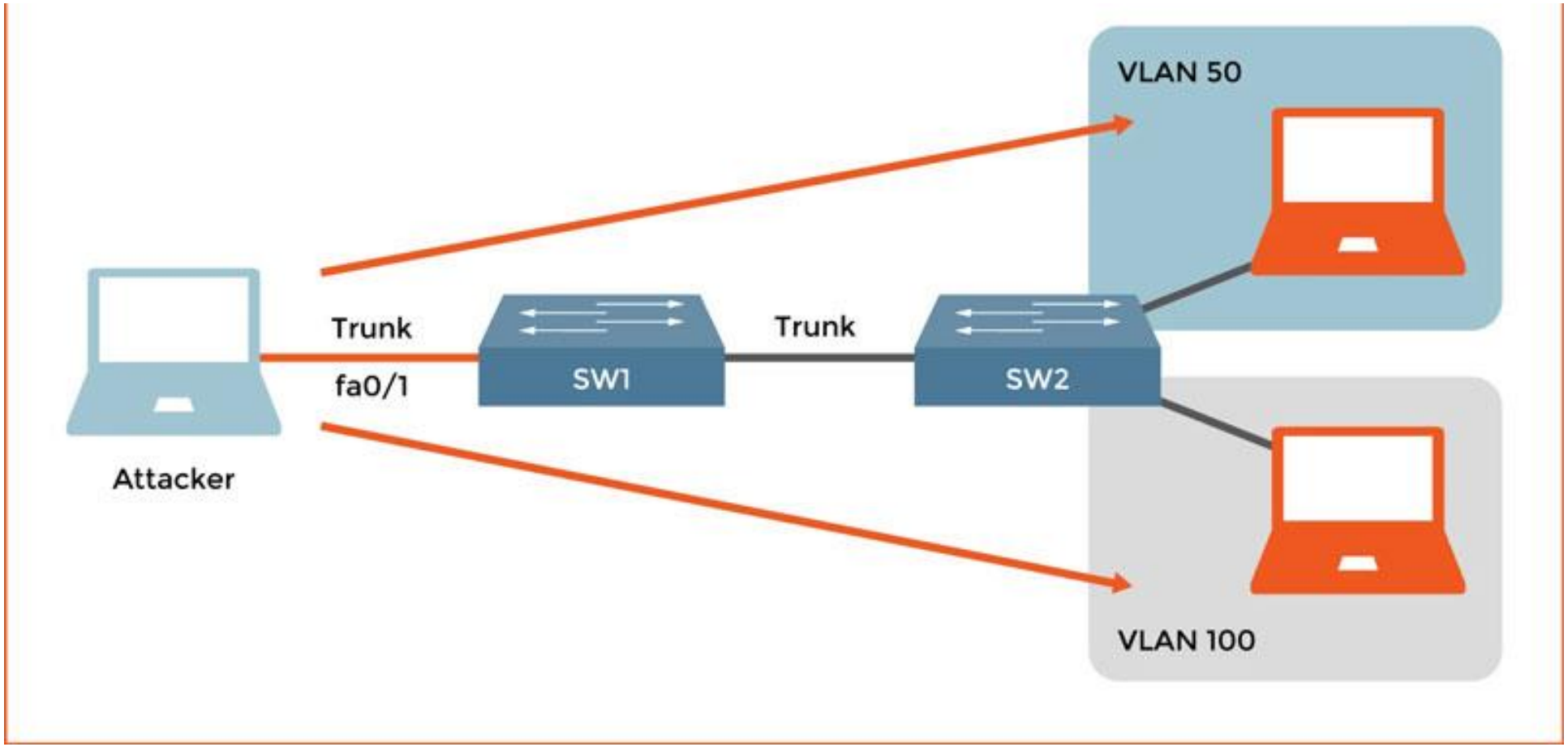
- Switch1(config-if)#ip dhcp snooping limit rate 5

حمله VLAN hopping چیست و چگونه میتوان از آنها جلوگیری کرد؟



- VLAN hoppingروشی برای حمله به شبکه با ارسال بسته ها به پورت است برای دسترسی به قسمت‌هایی از شبکه که به طور معمول از یک سیستم انتهایی مشخص قابل دسترسی نیستند.
- برای جلوگیری از این حمله و پورت‌هایی که نیاز نیست Trunkباشند را از حالت ترانک خارج کنیم.
- به صورت پیش فرض برخی از سوئیچ های سیسکو در حالت Auto Trunking قرار دارند. یعنی با دریافت فریم DTP روی پورت، آن پورت به صورت خودکار تبدیل به پورت ترانک میشود.
- این موضوع زمانی تبدیل به یک مشکل امنیتی می شود که نفوذگر پورت سوئیچ را به ترانک تبدیل کند و حملات VLAN-hopping را انجام دهد.

- VLAN hoppingمی تواند برای سرقت کلمه عبور و سایر اطلاعات حساس از مشترکین شبکه استفاده شود. این حمله همچنین می تواند برای تغییر،خرابکردن و یا حذف داده ها، نصب نرم افزارهای جاسوسی یا سایر نرم افزارهای مخرب و تبلیغ ویروس ها، کرم ها و تروجان ها در سراسر شبکه مورد استفاده قرار گیرد.



- جلوگیری از حمله VLAN hopping
- برای غیرفعال کردن امکان VLAN-hoppingمی توانید ترانک را روی تمام پورتهایی که به آن نیاز ندارند غیر فعال کنید. و همچنین قابلیت DTP را روی تمام پورتها غیر فعال کنید.

- **غیر فعال کردن ترانک:**
-

- Switch1(config)# interface gigabitethernet 0/3
- Switch1(config-if)# switchport mode access
- Switch1(config-if)# exit

- **جلوگیری از امکان DTP:**

- Switch1(config)# interface gigabitethernet 0/4
- Switch1(config-if)# switchport trunk encapsulation dot1q
- Switch1(config-if)# switchport mode trunk
- Switch1(config-if)# switch port nonegotiate