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

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

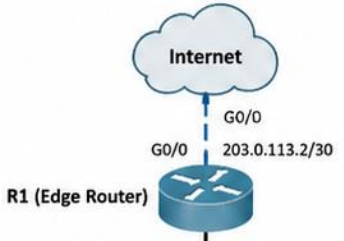
(برای پیاده سازی در Packet Tracer)

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

- **زمانی که tracert میگیرم از داخل سازمان مثلا tracert8.8.8.8**
- اولین چیزی که نشون میده ایپی روتر من هست اگر اولین step باشه و بعد ایپی های بقیه روتر ها اینجا میخوام ایپی روتر من نشون داده نشه ولی روتینگ انجام بشه امکانش هست ؟

- شما میخواید وقتی از داخل سازمان **tracert 8.8.8.8** میگیرید، اولین hop (که آی‌پی اینترفیس روتر شماست) دیگه تو خروجی tracert دیده نشه، اما مسیر و روتینگ کار خودش رو بکنه درسته!؟
- **پس یعنی:**
- دیتا رد بشه
- اینترنت وصل باشه
- ولی آی‌پی اولین روتر در tracert لو نره

- وقتی توی traceroute TTL=1 هست، اولین دستگاه (روتر شما) وقتی TTL صفر بشه باید طبق استاندارد یک ICMP Time Exceeded جواب بده. این جواب باعث میشه IP روترت تو tracert نشون داده بشه.

- باید روی اینترفیس داخلی روترت که کاربرا بهش وصلن، این دستور رو بزنی:

- interface GigabitEthernet0/1
- no ip unreachables

- یا اگر دقیق‌تر بخوای فقط ICMP Time Exceeded رو بلاک کنی:

- ip access-list extended BLOCK_TRACEROUTE
- deny icmp any any time-exceeded
- permit ip any any
- !
- interface GigabitEthernet0/1
- ip access-group BLOCK_TRACEROUTE in

- حالا وقتی کسی توی سازمان tracert بگیره،
- اولین hop یا timeout میشه Request timed out یا رد میشه بدون اینکه آی‌پی نشون بده.

- دیتا و روتینگ (مثل ارتباط با اینترنت) کاملاً درست کار میکنه.
- نمونه خروجی traceroute من رو بعد از این تغییر ببین:

- قبل از تغییر:

- 1 192.168.1.1 1ms 1 ms 1 ms
- 2 10.1.1.1 10 ms 11 ms 10 ms

- بعد از تغییر:
- **1Request timed out.**
- 2 10.1.1.1 10 ms 11 ms 10 ms

- اولین IP مخفی شد ولی مسیر ادامه داره.

- سر یه پروژه ای ما نیاز داشتیم روی پورت ها port fast رو فعال کنیم
- ولی چون متاسفانه تو مسیر باز از سوئیچ های کوچیک چند پورت استفاده میشد **bpduguard** پورت رو خاموش میکرد ولی سوال من اینجاس تو **show** نشون نمیداد که من این پورت هارو خاموش کردم

- جهت یادآوریت باید بگم که وقتی روی یه پورتی **portfast** رو فعال میکنی و همزمان **bpduguard** هم فعال باشه، اگر **BPDU** دریافت بشه، پورت errdisable میشه و خاموش میشه.

- توی show run یا show interface status مستقیم نمی‌بینی که "این پورت به خاطر bpduguard خاموش شده.

- باید بری از یه دستور خاص‌تر استفاده کنی:
- دستور:
- **show interfaces status err-disabled**
- نشون میده کدوم پورت‌ها به خاطر چه دلیلی errdisable شدن.
- یا
- **show errdisable recovery**
- میگه کدوم ارور باعث شده پورت غیرفعال بشه

- **یا دستور**

- **show logging | include BPDU-Guard**
- لاگ دقیقی میده که BPDU-Guard مثلا روی پورت Xعمل کرده و پورت رو خاموش کرده.
- مثلا خروجی
- **show interfaces status err-disabled**
- شبیه این میشه :

- Port Name Status Reason
- Gi1/0/5 err-disabled bpduguard

سناریو بعدی

- روی یکی از سوئیچ‌هامون یه ترافیک مشکوک داریم، فقط وقتی یه دستگاه خاص وصل میشه، نصف شبکه داون میشه. نه لاگ درست، نه خطایی، نه چیزی...
- روی سوئیچی که گفته بودن، یه پورت گیگ مشکوک.
- **اول یه چک سریع با TDR می زنیم**

- **test cable-diagnostics tdr interface gig1/0/24**

- بعد چند ثانیه:
- **show cable-diagnostics tdr interface gig1/0/24**

- دیدم طول کابل نرماله ولی یه impedance mismatch روی Pair C هست!
- یا کابل داغونه، یا یه چیزی داره لایه فیزیکی رو خراب می‌کنه...

مرحله بعدی شکارگر شبکه

- یه SPAN ساده می زنیم رو همون پورت مشکوک :
- monitor session 1 source interface gig1/0/24
  monitor session 1 destination interface gig1/0/1

- پورت مقصد وصله به یه لپتاپ تحلیلگر با Wireshark.
- ولی بعد ۳۰ ثانیه، دیدم حجم ترافیک عجیبه... یه چیزی درست نیست.

- هر لحظه MAC شو عوض می‌کرد و سوئیچ هی MAC Table رو flush می‌کرد
- راه حل : استفاده MAC Secure + Storm Control

- interface gig1/0/24
- switchport port-security
- switchport port-security maximum 2
- switchport port-security violation restrict
- storm-control broadcast level 0.10
- storm-control multicast level 0.10
- storm-control action trap

- دستمزد این کار چقدر بود؟!
- ۱۰ میلیون تومان

فایلها در یک شبکه مثل CRM بازنمیشوند

همه چی اوکیه... ولی ترافیک از Subnet مالی رد نمی‌شه.

```
ping 10.3.3.25 source 192.168.33.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos...
.....
Success rate is 0 percent (0/5)
```

- یا مشکل از DNS هست یا ترافیک شبکه از طریق ACL بسته شده
- بررسی اینترفیس
- show run interface GigabitEthernet0/1
- ip address 192.168.33.1 255.255.255.0
- ip access-group KILL-SWITCH in

- کالبدشکافی

- show access-lists KILL-SWITCH

- Extended IP access list KILL-SWITCH
- 10 deny ip 192.168.33.0 0.0.0.255 any
- 20 permit ip any any

- به جای حذف کل ACL (که باعث drop لحظه‌ای می‌شه)، با sequence بازی کنیم

- ip access-list extended KILL-SWITCH
- no 10
- 5 permit ip 192.168.33.0 0.0.0.255 any

- **نکته مستنداتی:**
- خب ACLهای شماره‌دار (standard/extended)رو می‌شه با sequence number دقیق مدیریت کرد.
-
- ترتیب ruleها مهمه؛ اولین matchاجرا می‌شه.
-
- همیشه permit قبل از deny باشه اگه قصد استثنا داری.
-
- بهتره ACLها رو به‌صورت named ACL بسازی تا بعداً بتونی اصلاح‌شون کنی بدون حذف کامل.

- بررسی بعد از اصلاح

- show access-lists KILL-SWITCH

- Extended IP access list KILL-SWITCH
- 5 permit ip 192.168.33.0 0.0.0.255 any
- 20 permit ip any any

- و بعدش:

- ping 10.3.3.25 source 192.168.33.1
- Success rate is 100 percent (5/5)

- ویژگی کمترین طول پسورد در IOSسیسکو
- IOSسیسکو توانایی اجبار به استفاده از رمزهای عبور با حداقل طول برای کاربران را دارد. این سیاست قابل اعمال به رمزهای عبور زیر میباشد:

- user password
- enable password
- enable secret
- line password

- این ویژگی از طریق دستور زیر یم تواند به کار گرفته شود:

- **Router(config)#** security passwords min-length length

- وقتی این دستور اجرا شود، هر پسوردی با طول کمتر از مقداری که در این دستور در نظرگرفته شده، مردود میباشد.

- **محدود کردن تعداد دفعات ورود**
- برای مقابله با حمله دیکشنری میتوان یک تأخیر بین هر دو درخواست ورود تعریف کرد. این کار باعث کاهش سرعت حمله، افزایش زمان مورد نیاز برای موفقیت حمله و افزایش بازه زمانی برای تشخیص رفتارهای غیرعادی میشود.
- در IOS سیسکو برای اعمال تاخیر بین درخواستهای ورود پی در پی میتوان از دستور login delay استفاده
- کرد. به طور پیشفرض یک ثانیه تأخیر برای این منظور در نظر گرفته شده است:

- Router(config)# login delay <seconds>

- **محدود کردن تعداد دفعات ورود ناموفق در یک بازه زمانی مشخص**
- برای مقابله با حمله دیکشنری میتوان تعداد دفعات درخواستهای ورود ناموفق به تجهیز را در یک بازه زمانی معین، محدود کرد. این کار باعث کاهش سرعت حمله، افزایش زمان مورد نیاز برای موفقیت حمله و افزایش بازه زمانی برای تشخیص رفتارهای غیرعادی میشود
- در IOS سیسکو برای تعریف حداکثر تعداد دفعات تلاش برای ورود به دستگاه در یک بازه زمانی مشخص، به طوری که بعد از آن دستگاه برای یک زمان معین اجازه وارد شدن را ندهد، از دستور زیر میتوان استفاده کرد:

- Router(config)# login block-for seconds attempts tries within seconds

- همچنین در سیستم عامل نرم افزاری سیسکو میتوان یک ACL استثناء برای سیستمها و شبکه های مورد اعتماد و مجاز، با استفاده از دستور زیر تعیین کرد:
- در مثال زیر روتر به گونه ای پیکربندی شده است که اگر در بازه زمانی ۱۰۰ ثانیه تعداد دفعات تلاش برای وارد شدن به تجهیز از ۱۵مرتبه تجاوز کند، دستگاه برای یک بازه زمانی ۱۰۰ ثانیه ای اجازه هیچگونه وارد شدن به دستگاه برای سیستمهایی که در ACL 10تعریف شده اند را نمیدهد:

- **Router(config)#** access-list 10 permit host 172.26.150.206
- **Router(config)#** login block-for 100 attempts 15 within 100
- **Router(config)#** login quiet-mode access-class 10

- محدودیت تعداد دفعات لاگین اشتباه در یه بازده زمانی خاص
- Router (config) #login block-for 30 attempts 5 within 10
- در کد بالا اگر کاربری در ۱۰ ثانیه ۵ بار اشتباه پسورد را وارد کند به مدت ۳۰ ثانیه بلاک می شود.

- **مخفی کردن فایل Boot**

- جهت بالابردن امنیت تجهیزات سیسکو ، فایل bootخود را با استفاده از دستور بالا می توانید مخفی کنید.
- Router(config)#secure boot-image

- ایجاد پشتیبان مخفی از کانفیگ تجهیزات
- Router(config)#secure boot-config

تمام collision domain های اترنت باید به صورت سوئیچینگ باشد یعنی چی ؟

- منظور این است که هر دستگاه باید در یک Collision Domain مجزا باشد و ارتباطات هم صرفا از طریق سویچ انجام شود

- در سویچ هر پورت یک Collision Domain مستقل است

- برای مشاهده Collision از دستور :
- # show interfaces | include collision
- که این مقدار باید صفر یا نزدیک به صفر باشد .

- میزان ترافیک روی هیچکدام از لینک های WANنباید بیشتر از ۷۰ درصد ظرفیت آن باشد.
- برای برسی این میزان از دستور :
- Show interface serial 0/0
- یا
- Show interface gig 0/0

- خروجی گزارش :
- 5 minute input rate 45 mbps
- 5 minute output rate 20 mbps
- اگر ظرفیت لینک ۱۰۰ باشد ۴۵ درصد استفاده شده است

- نحوه محاسبه : اگر ظرفیت لینک ۱۰۰۰ یا گیگ باشد خروجی
- 5 minute input rate 350000 sec
- یعنی 350 mbps
- 350/1000 *100 = 35%
- یعنی ۳۵ درصد ظرفیت لینک استفاده شده است

- مانیتورینگ CPU :
- Show interface summary
- Show processes cpu sorted
- مقدار پیشنهادی کمتر از ۷۰٪ (به این دلیل که روتر یا سویچ در شرایط غیر عادی بتواند افزایش ناگهانی بار را تحمل کند)

- اگر CPU بالای ۷۰٪ باشد چه اتفاقی می‌افتد؟
- در تجهیزات Cisco بسیاری از پردازش‌ها توسط CPU انجام می‌شوند:

- Routing Protocol ها (OSPF, BGP, EIGRP)
- STP
- HSRP/VRRP
- SNMP
- Syslog
- SSH
- NetFlow
- Control Plane Processing

- اگر CPU دائماً روی ۸۰٪ تا ۹۰٪ باشد

- در این حالت ممکن است:
- SSH کند شود یا قطع شود.
- Routing Protocol ها Neighbor را از دست بدهند.
- HSRP Failover اتفاق بیفتد.
- Packet Drop ایجاد شود.
- شبکه ناپایدار شود

محدوده‌های پیشنهادی در ممیزی

وضعیت	میانگین CPU
عالی	0% تا 40%
خوب	40% تا 60%
قابل قبول	60% تا 70%
نیاز به بررسی	70% تا 80%
هشدار	80% تا 90%
بحرانی	بالای 90%