حماية الشبكة المحلية

LAN Security

ماهوالـPortSecurity:

هو وضعية نقوم بأعداده على كل Interface تهدف لتحديد أجهزة الكمبيوتر التى يسمح لها بالأتصال من خلال هذا الـInterface وتتم العملية عن طريق ربط الـInterface بالـ Mac Address الخاص بكل جهاز كمبيوتر لديه الصلاحية للدخول على الشبكة وبهذه الطريقة نكون قد منعنا الأجهزة الدخيلة من المحاولة بالأتصال بالشبكة من خلال شبك الكمبيوتر بأحد مخارج السويتش كما يمكننا ردع هجوم ما يعرف بي mac flood من خلال تحديد عدد الأجهزة المتصلة بالـ Interface في حال لوكان عندنا hub مثلا

ماذا سوف يحدث في حال محاولة أحد الأشخاص الولوج إلى الشبكة

للـ Port Security ثلاث وضعيات يمكن أن يتخذها في حال تم شبك ماك ادريس لجهاز كمبيوتر غير مصرح به للدخول إلى الشبكة والحالات هي كالتالي

Mode	Description
Shutdown	في هذه الحالة سوف يقوم السويتش بإغلاق المنفذ بشكل مباشر وهذه الوضعية تعد الـ Default للـ Port Security

Protect	في هذه الحالة يقوم السوتش بعمل Drop لكل الترافيك القادم من الماك أدريس الغير مصرح به مع أبقاء المنفذ مفتوح للأجهزة المصرحة بها
Restrict	نفس الحالة السابقة لكن هنا يقوم السويتش بأحصاء كل الباكيت التى قام بعمل drop لها

طريقة ألأعداد :

طريقة أعداده تتم عن طريق أمرين فقط :

```
Switch# conf t
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
```

وبعدها نحتار mode access لكي نخبر السويتش أن هذا البورت متصل مع end device أو جهاز كمبيوتر
عندما نقوم بتفعيل الـ Port Security فالحالة الطبيعية التى يتخذها السويتش كما اوضحت سابقا هي أغلاق السويتش بالإضافة السماح لي Mac Address واحد كأقصى حد وبكلام آخر أول Mac Address سوف يتصل على البورت سوف يكون هو الوحيد القادر على الاتصال بالسويتش وهو يفيدنا في موضوع ردع هجوم الـ Mac Flooding في حالة لو أردنا ان نسمح لأكثر من ماك أدريس للأتصال بالسويتش نكتب الأمر التالي :

```
Switch(config-if)# switchport port-security maximum 3
```

وقد سمحت هنا بي 3 أجهزة للدخول الى السويتش من خلال هذا البورت ولو في حال أردت أن أقوم بتحديد ماك أدريس معين هو الوحيد الذي يستطيع الدخول إلى السويتش أقوم بكتابة الأمر التالي :

```
Switch(config-if)# switchport port-security mac-address 00-11-22-33-44-55-66
```

وممكن بدلا من ذلك أن تضع مكان كل ماك أدريس كلمة Sticky وهي تخبر السويتش بتسجيل الماك أدريس المتصل حاليا على البورت كا Address Static Mac وصيغة الامر تكون :

```
Switch(config-if)# switchport port-security mac-address mac-address sticky
```

وآخيرا لتغيير ردة الفعل التى سوف يتأخذها السويتش في حال تم حدوث أي تجاوز نكتب الأمر التالي

```
Switch(config-if)# switchport port-security mac-address violation ?
```

ونختار أحد الخيارات الثلاث الموضحة في الجدول السابق restrict , shutdown ,protect

ولأستعراض حالة البورتات على السويتش نقوم بكتابة الأمر التالي:

```
Switch#show port-security address
```

```
Switch#show port-security address
                Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports          Remaining Age
                                                                 (mins)
----    -----------       ----                  -----          -------------
1       000A.4145.6254    DynamicConfigured     FastEthernet0/1        -
1       000C.CFDE.C403    DynamicConfigured     FastEthernet0/1        -
1       00E0.F7DE.1C78    DynamicConfigured     FastEthernet0/3        -
1       00E0.8F2B.39B1    DynamicConfigured     FastEthernet0/4        -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#
```

كما هو واضح من الصورة قمت بالسماح للـ Interface 0/1 بأن يقبل أكثر من ماك أدريس وهذا يفسر لنا وجود أثنان ماك أدريس في القائمة

والأمر التالي لأستعراض كل التفاصيل حول Interface معين

```
Switch#show port-security interface fastethernet 0/1
```

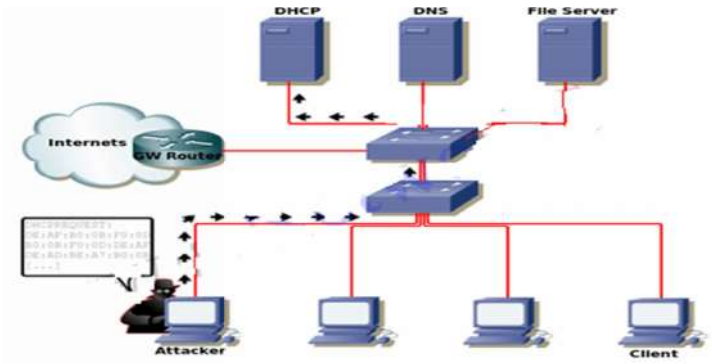
```
Switch#show port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000A.4145.6254:1
Security Violation Count   : 4
```

الهجمات على DHCP وطرق التصدي لها:

- DHCP Starvation -1
- DHCP Spoofing -2

- **DHCP Starvation :هو عبارة عن هجوم يستهدف الـ DHCP Serverو يعد احد هجمات الـ (DOS) Denial of service .**

- **يشكل هذا النوع من الهجوم خطرا كبيرا على الشبكة لانه يقوم بحجز كل IP الموجودة في سيرفر الـ DHCPوفيها يقوم المهاجم بأرسال عدد غير محدود من الرسائل إلى سيرفر الـ DHCPيطلب فيها تزويده بـ IP للجهاز الخاص فيه وعندما يتم أستلام الأعدادت من السيرفر وحجز IP له يقوم بأرسال طلب جديد إلى السيرفر لكن هذه المرة MAC ADDRESSمختلف وهكذا حتى يقوم المهاجم بحجز كل IP المتاحة على السيرفر وحتى لو كانت IP 10000 لان هذه العملية تتم بسرعة كبيرة والتى قد لاتستغرق بضع دقائق وبالتالي أي محاولة من أي جهاز آخر موجود على الشبكة للحصول على IP من السيرفر سوف تبدو بالفشل .**



طريقة التصدي لهذا الهجوم :
و يتم ذلك من خلال الـ Port Security وذلك بتحديد عدد معين من MAC ADDRESSالمسموح لها **بالدخول من خلال** هذا المنفذ وايضا يكمن اضافة بعض الاوامر له .

هجوم الـ DHCP Spoofing:

- **يعد هذا الهجوم احد الهجمات الخطيرة على الشبكة ويتم من خلال قيام المخترق بتشغيل سيرفر DHCPعلى جهازه يملك نفس المعلومات التى يقوم السيرفر الرئيسي بتزويدها للأجهزة لكن مع أختلاف بسيط جدا وهو الـ Gateway للشبكة فهو يقوم بتغييره بحيث يكون هو جهازه نفسه ومن خلال أحد البرامج مثل الـ ettercapيقوم بتحويل TRAFFIC المار عبر جهازه إلى الـ Gatewayالحقيقي للشبكة وبهكذا كل مايتم أرساله من خلال الأجهزة الموجودة على الشبكة سوف يعبر من خلال جهاز المخترق ومن خلال أحد برامج تحليل البيانات مثل الـ Wire Sharkسوف يشاهد كل تفاصيل TRAFFIC وطبعا هذه تعد كارثة كبيرة للشبكة وخصوصا أي هجمة تندرج تحت هجمات الـ MITM ولو أراد المهاجم أن يكون الهجوم كاملا فهو سوف يقوم أولا بتنفيذ هجوم الـ DHCP Starvationعلى السيرفر الرئيسي ويقوم بحجز كل ip الموجودة عنده وعندها سوف يضمن بأن كل الأجهزة الموجودة على الشبكة وعلى سويتشات آخرى بأنه سوف تلجأ إليه للحصول على المعلومات اللازمة للاتصال بالشبكة مما يزيد من كمية المعلومات المارة عبر جهاز المخترق وبالتالي دمار أكبر للشبكة**

هجوم الـ STP manipulationوطريقة التصدي له:

بروتوكول الـ Spanning Tree: STP له دورا كبيرا في الشبكة في منع مايعرف بي الـ loopأو Broadcast Stormويتم ذلك عن طريق أنتخاب سويتش واحد ليكون Root Bridgeويتم الأختيار حسب أقل Bridge IDموجود على الشبكة وبعدها يتم أختيار البورتات التى يجب أن تعمل أو تتوقف أعتمادا على الـ Costأو التكلفة للوصول للـ Root Bridgeوكل هذه الأمور تتم عن طريق (BPDU).

تحتوي BPDUعلى المعلومات التالية:

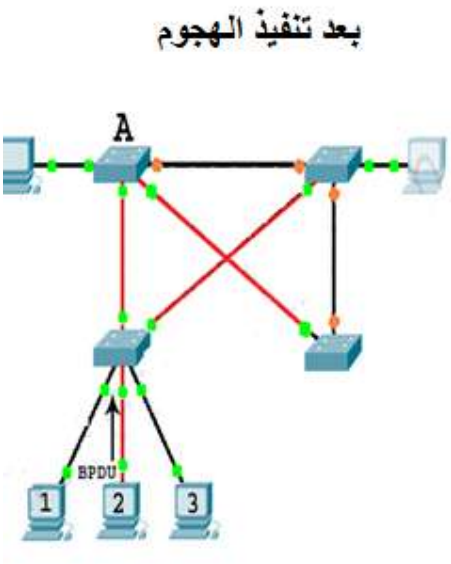
- Bridge IDللجهاز الذي يعتبر نفسه Root
- تكلفة المسار وصولا الى Root
- Bridge IDللذي يرسل اطار BPDU
- عمر الرسالة Age
- Port IDللمنفذ الذي يرسل BPDU

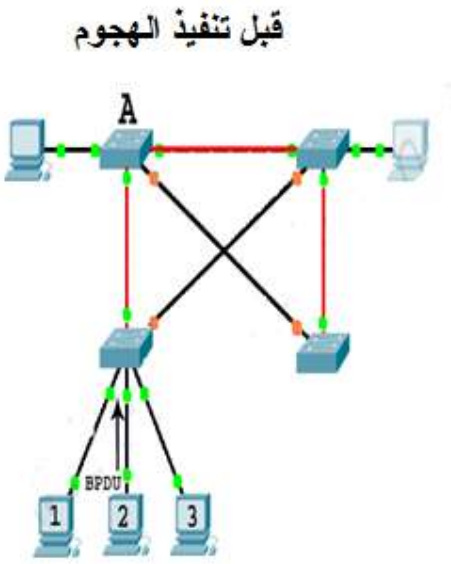
كيف يتم هذا النوع من الهجوم :

يتم عن طريق أرسال BPDUمزور يخبر فيه المهاجم السويتش الذي يرتبط معه بأنه يملك أقل Bridge IDعلى الشبكة وبانه يجب ان يكون هو الـ Root Bridgeوبالتالي سوف تتم أعادة توزيع البورت على كل السويتشات وهذه بعض الصور لتبسيط الموضوع

الصورة الاولى نرى فيها التوزيع الطبيعي للشبكة ونرى أيضا أن السويتش Aهو الـ Root Bridgeعلى الشبكة والخطوط الحمراء خاصة بي الـ STPونرى أن المهاجم الموجود على الجهاز رقم 2 يقوم بأرسال BPDUمزور إلى السويتش.

وفي الصورة الثانية نلاحظ ان كل شيء قد تغيير وأصبح كل الترافيك الذي يعبر عبر الشبكة يمر عبر الشخص المهاجم وبالتالي أصبح عندنا الهجوم الذي يعرف بي MITMأو Man In The Middle





كيفية التصدي لهذا الهجوم :

هناك ثلاث طرق للحماية :

1- **BPDU Guard: خاصية تخبر فيها البورت أن لا يستقبل أي نوع من رسائل الـ BPDUوفي حال أستلام البورت لاي BPDUسوف يقوم بتحويل حالة البورت إلى errdisableأي سوف يتم اغلاق البورت بشكل كامل.**

ويتم اعدادها على الشكل التالي : ندخل أولا على البورت الغير أمن ونكتب فيه الأمر التالي:

Switch(config)#spanning-tree bpduguard enable

2- BPDU Rootفي هذه الخاصية أخبر السويتش بأن هذه البورت لن يكون أبدا Root Bridgeوتتم من خلال هذا الأمر

Switch(config-if)#spanning-tree guard root

3- BPDU Filteringهذه الخاصية هي نفس الخاصية الأولى تماما والفرق الوحيد هو أن هذه الخاصية تتيح لك أن تحدد ماذا تريد للبورت أن يفعل في حال أستلم BPDUبعكس الـ BPDU Guardالذي سوف يقوم بأغلاق البورت بشكل مباشر وطريقة الأعداد هي كالتالي:

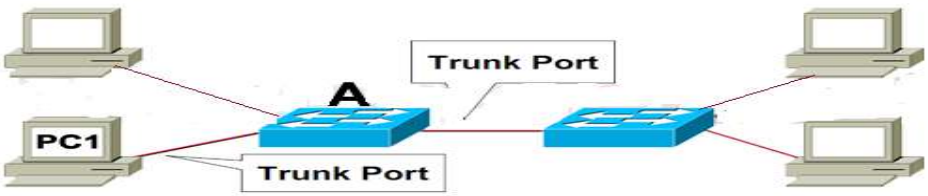
على البورت

Switch(config-if)#spanning-tree bpdufilter enable

هجوم الـ Vlan Hopping وكيف التصدى له ؟

هذا النوع من الهجمات تستهدف الـ Layer 2 Devices وتدعى Vlan Hopping وتقوم فكرة هذا الهجوم باختراق قواعد الـ Vlan على الشبكة وذلك بالسماح لشخص معين موجود على Vlan2 مثلا بالدخول على Vlan 3 والأتصال بكل الأجهزة الموجودة هناك لأننا كما نعلم أن أحد مميزات الـ Vlan هي عزل الأجهزة عن بعضها البعض

من انوع الهجمات المطبقة عليه :
Spoofing Switch:



حيث أن وظيفة الـ Trunk Port هي السماح بالأتصال بين جميع الـ Vlans

الموجودة في السويتش مع نفس الـ Vlans الموجودة على سويتش آخر وذلك بوسم كل Traffic ذاهب الى السويتش الآخر برقم الـ Vlan التى أرسلت منه وهذا بدوره يعطي الـ Trunk Port القدرة على الأتصال بكل الـ Vlans الموجودة على الشبكة
لنتخيل أول حالات هذه الهجوم
يقوم العابث الموجود على PC1 بعمل سويتش وهمي أو يقوم بوصل سويتش حقيقي على الجهاز مخبر السويتش Aبأنه Trunk Port وهذا بدوره يعطي العابث الصلاحيات في الوصول إلى كل الأجهزة الموجودة على الشبكة بالأضافة إلى أمكانية التنصت على كل الباكيت المرسلة بين الـ Vlansوالسبب طبعا لان البورتات الموجودة في السويتش A تكون في حالة auto مع الطرف الآخر فهو يستجيب لك أذا أخبرته أنك سويتش وأنك Trunk Port
وللتصدي لهذا النوع تقوم بكتابة أمر واحد على كل Interface موصول مع Host

```
SwitchA#conf t
SwitchA(config)#interface fastethernet 0/1
SwitchA(config-if)#switchport mode access
```

بهذا الأمر نكون قد أوقفنا نصف الهجوم لان السويتش يحوي ثغرة آخرى تتم عن طريق بروتوكول الـ DTP أو Dynamic Trunk Protocol وظيفة هذا البروتوكول بأختصار هي تحديد نوع الـ Trunk Protocol الذي يجب أستخدامه بشكل أوتماتيكي أي تحديد هل يجب أستخدام Q802.1 أو ISL وهو يعمل Be default على كل البورتات الموجودة على السويتش وهذا مايستغله العابث بشكل جيد فهو يقوم بأرسال Packet DTP إلى السويتش مخبرا ايأه بأنه ييستخدم بروتوكول Q802.1 مثلا ليتحول الـ Port إلى Trunk Port بشكل أوتماتيكي حتى لو كنا قد طبقنا الأمر السابق ولأيقاف هذه البروتوكول عن العمل نقوم بتنفيذ الأمر التالي

```
SwitchA(config)# interface fastethernet 0/1
SwitchA(config-if)# switchport mode trunk
SwitchA(config-if)# switchport nonegotiate
```

وفيه أخبر البورت بأن لايقوم بالتفاوض مع الطرف الآخر حول نوع الروتوكول الذي يجب أستخدامه