2021-2022

جامعة البعث

الكلية التطبيقية – السنة الرابعة – تقنيات الحاسوب

الفصل الثاني 2021-2022

Networks Security

Lecture 2

:SUPERVISED BY

ENG. ALI MUSTAFA

Academic Year 2021-2022

Layer 2 Security … *Continue*

❖ VLAN Attacks

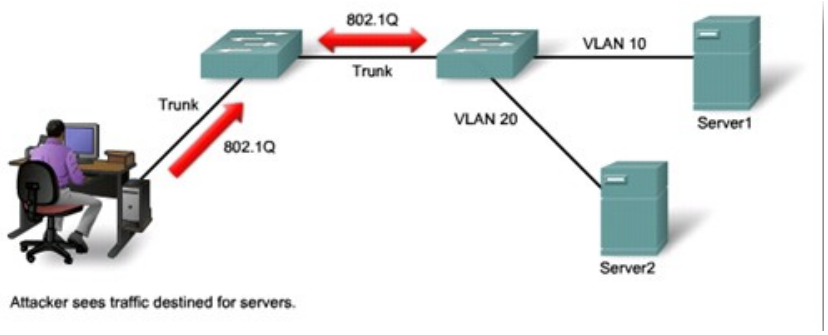
يهدف هذا الهجوم إلى الوصول إلى VLANs غير متاحة للمهاجم أصلاً (لا يمكنه الوصول إليها) ويمكن أن يتم بإحدى طريقتين:

1. **Switch spoofing.**
2. **VLAN Hopping (Double-tagging VLAN) attack**

× هجوم المُبدّلة المزيّفة (Rogue Switch) أو Switch Spoofing

يمكن للمهاجم إعداد جهاز حاسوب (يمكن أن يكون جهازه الشخصيّ) وجعله يبدو كمُبدّلة Switch والإعلان عن نفسه على أنه قادر على استخدام بروتوكول 802.1Q أو ISL.

يصبح المُهاجم في حالة نجاحه بذلك عضوًا في جميع شبكات VLAN ضمن الشبكة المحليّة.



× هجوم القفزة بين ال VLANs (VLAN Hopping Attack or Double-Tagging)

يقوم مُهاجم موجود ضمن Access VLAN معينة بإرسال إطارات (Frames) تحوي وسمي 802.1Q (أي تحوي إثنين من ال VLAN ID) ضمن ترويساتها (in the frames Headers) للوصول إلى شبكة محلية افتراضيّة (VLAN) مُختلفة.

- **يجب أن تتوفّر العوامل التالية حتى تتم الهجمة:**

1. أن يكون المُهاجم متصلاً عبر منفذ access بالمُبدّلة.

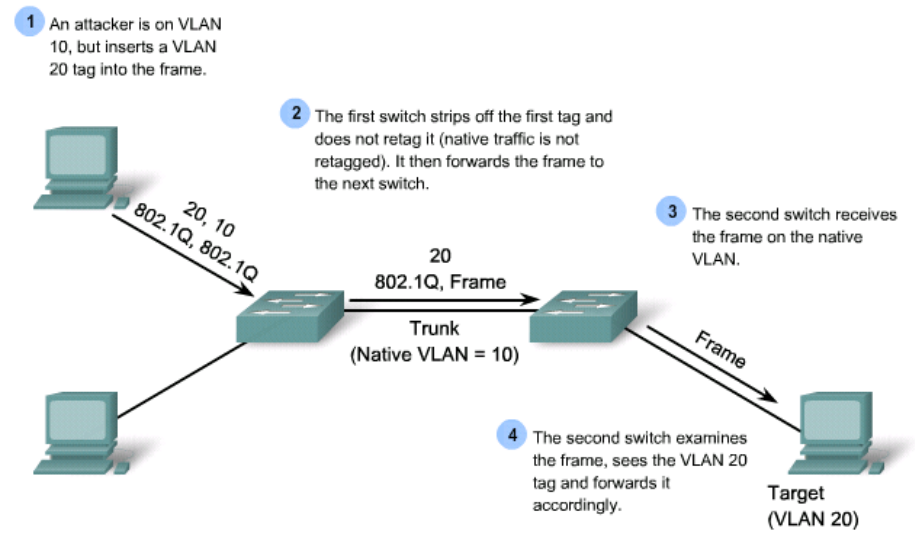
2. يجب أن تحوي هذه المُبدّلة (المُتصل معها المُهاجم) على وصلة 802.1Q trunk.

3. يجب أن تحوي هذه الوصلة على شبكة ال VLAN للمُهاجم كشبكة محلية افتراضيّة أصلية (Native VLAN).

في المثال أدناه:

تقوم المُبدّلة الأولى بإزالة ال Tag الأول (ال VLAN ID الأول) من الإطار وتُوجّه هذا الإطار.

ثم تقوم المُبدّلة الثانية بإعادة توجيه الرزمة (الإطار) إلى الوجهة بالاعتماد على شبكة VLAN المُحدّدة في ترويسة 802.1Qالثانية.



Note: This attack works only if the trunk has the same native VLAN as the attacker.

✓ Mitigating VLAN Attacks

للتنصّل من هجمات VLAN، تأكّد من تمكين الوضع trunk فقط على المنافذ التي تتطلّب trunk (بين المُبدّلات مثلاً).

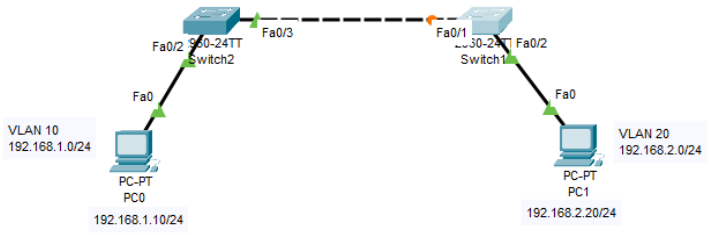
تأكّد أيضًا من تعطيل مفاوضات بروتوكول **DTP** (إلغاء تفعيل الوضع الأوتوماتيكيّ auto trunking) وإعداد وصلات ال Trunk يدويًا.

للتنصّل من هجمة VLAN Double Tagging، يجب عليك دائمًا إعداد وصلات ال Trunk بعناية باتباع الخطوات التالية:

الخطوة 1: إعداد ال VLAN الأصلي (native VLAN) ضمن وصلة trunk ما على أنها VLAN زائفة أو غير مستخدمة.

الخطوة 2: حذف شبكة ال VLAN هذه من طرفي وصلة ال Trunk.

مثال: **Mitigating VLAN Attacks**



نُطبّق التعليمات التالية على المُبدّلة Switch2

```
Switch(config)#vlan 1000
Switch(config-vlan)#name bogus_native_vlan
Switch(config-vlan)#exit
Switch(config)#interface f0/3
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch(config-if)#switchport trunk native vlan 1000
Switch(config-if)#switchport trunk nativ
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (1000),
with Switch Fa
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (1000),
with Switch FastEthernet0/1 (1%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent
peer vlan id 1 on FastEthernet0/3 VLAN1000.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/3 on VLAN1000. Inconsistent local
vlan.


Switch(config-if)#switchport trunk allowed vlan remove 1000
Switch(config-if)#ex
Switch(config)#do wr
Building configuration...
[OK]
```

كما ونُطبّق التعليمات التالية على المُبدّلة Switch1

```
Switch(config)#vlan 1000
Switch(config-vlan)#name bogus_native_vlan
Switch(config-vlan)#exit
Switch(config)#inter
Switch(config)#interface f0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with
Switch F
Switch(config-if)#switchport trunk native vlan 1000
Switch(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on
VLAN1000. Port consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001. Port
consistency restored.


Switch(config-if)#
Switch(config-if)#switchport trunk allowed vlan remove 1000
Switch(config-if)#do wr
Building configuration...
[OK]
```

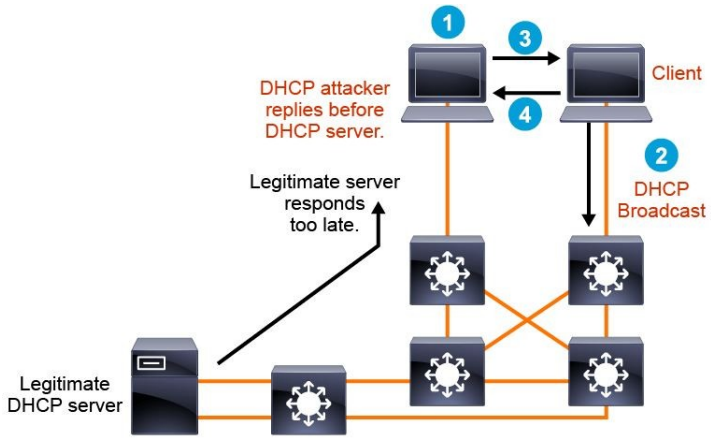
× هجمة DHCP Spoofing

يوجد نوعان من هجمات DHCP:

- **DHCP spoofing**
- **DHCP starvation**

يتم في هجمات DHCP Spoofing وضع مُخدّم DHCP مُزيّف لنشر العناوين إلى الزبائن.

أما DHCP Starvation فغالباً ما يتم استخدامها قبل هجمة DHCP Spoofing من أجل منع الخدمة والوصول إلى المُخدّم الأصليّ.

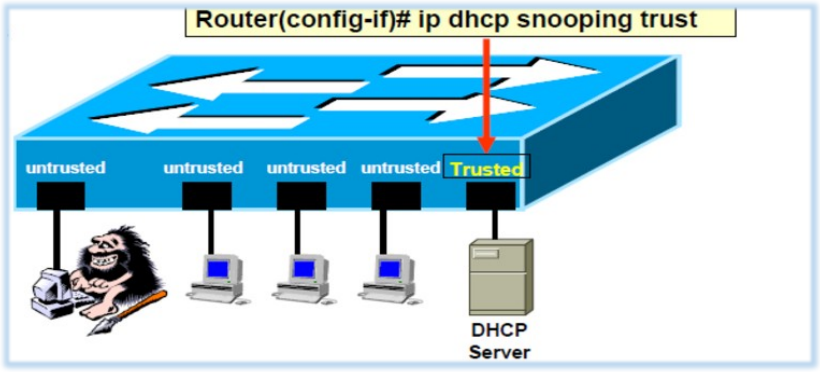


✓ التنصّل من هجمة DHCP Spoofing (DHCP Snooping)

يتم هنا تحديد منافذ المُبدّلة التي بإمكانها الاستجابة لطلبات ال DHCP (تحديد المنافذ الموثوقة فقط).

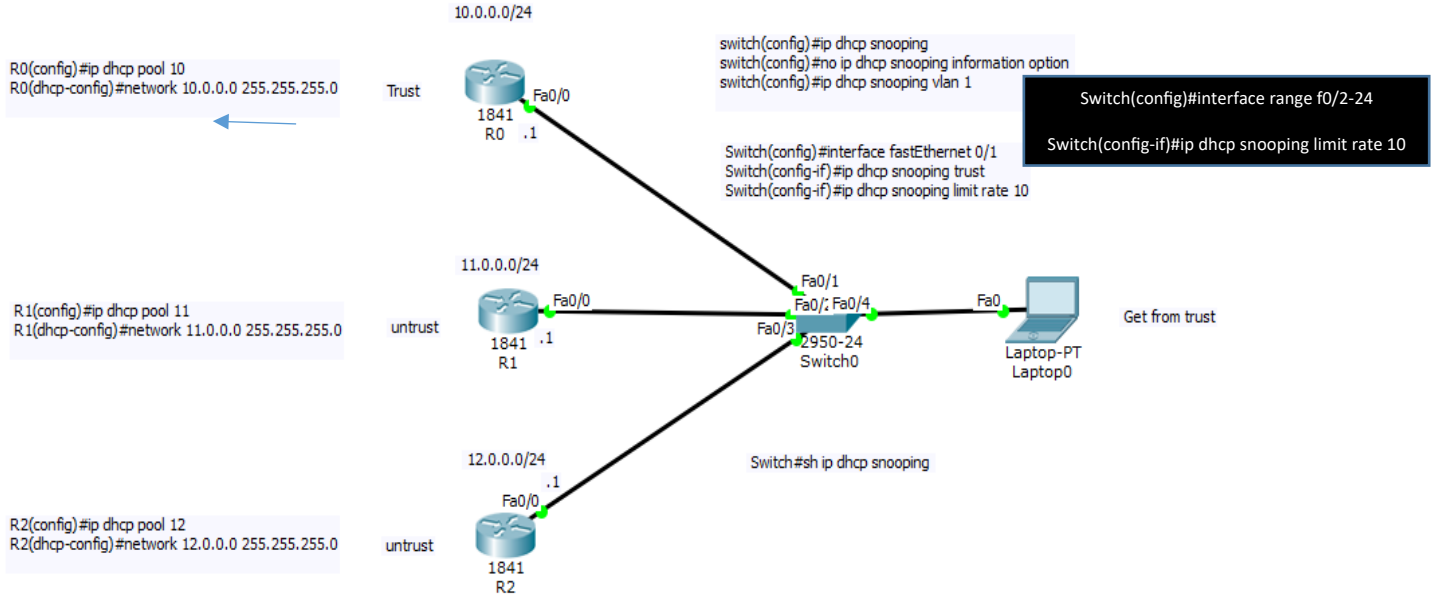
لا ننسى أن نقوم أولاً بتفعيل DHCP Snooping ضمن الوضع configuration mode:

```
Router (config) # ip dhcp snooping
Router (config) # ip dhcp snooping vlan vlans-IDs or ranges
```



تقوم هذه التقنية ببناء جدول يُدعى DHCP Binding Table يحوي العنوان المنطقيّ IP لجهاز المستخدم وعنوانه الفيزيائيّ MAC ورقم المنفذ المتصل به هذا المستخدم ورقم ال VLAN (VLAN ID) التي ينتمي لها المستخدم.

مثال: DHCP Snooping and DHCP Limit Rate



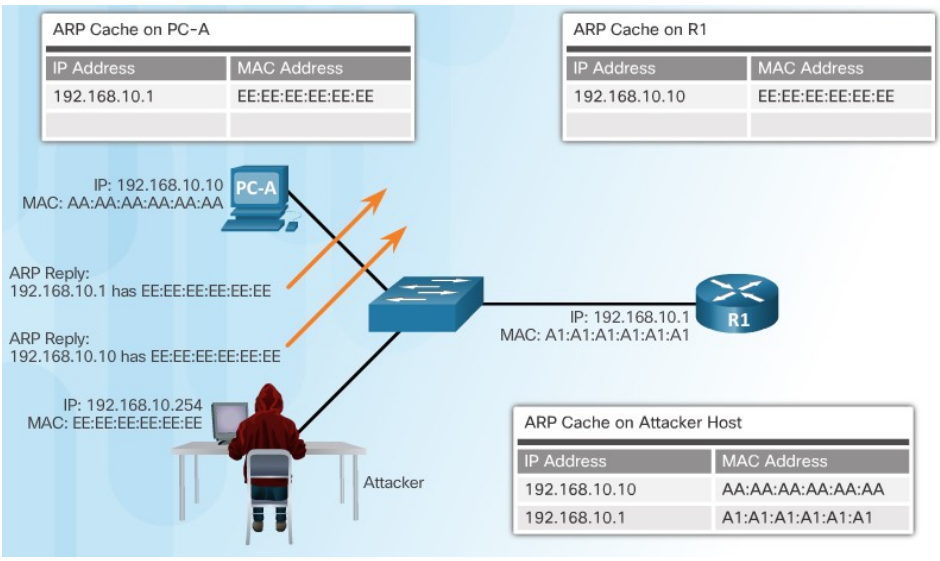
ARP Spoofing هجمة ×

يضيف المُهاجم ضمن هذه الهجمة سطر ARP مُزيّف إلى جدول ال ARP الخاص به، لبدء إعادة توجيه الرُزم إلى عنوان ال MAC المزيّف للمهاجم.

سيتم إعادة توجيه جميع الرُزم المُرسلة إلى عنوان ال IP المُرتبط بال MAC المُزيّف عبر جهاز المُهاجم.

يُعرف هذا الهجوم باسم تسميم ال ARP (ARP Poisoning) أو ARP spoofing، ويعتبر نوعًا من هجوم man-in-the-middle.

يمكن للمُهاجم إرسال رد ARP مزيّف عندما يسمع طلب ARP تم بثّه مُسبقاً ويحوي على عنوان ال MAC المزيّف نتيجة السطر المزيّف الذي أضافه المُهاجم.

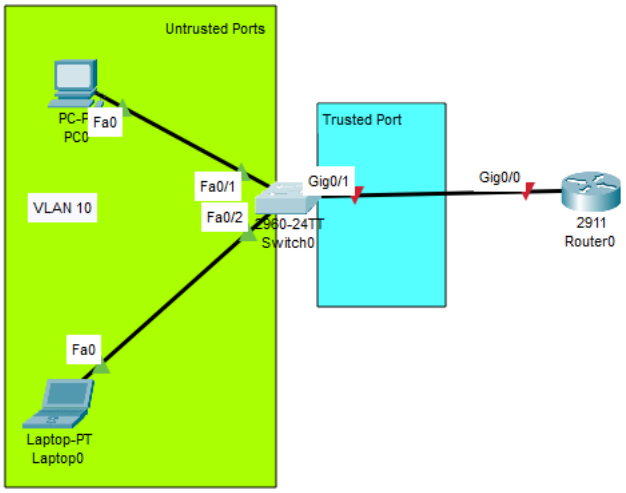


✓ **التنصّل من هجمة ARP: تقنية الفحص الديناميكيّ لل ARP (Dynamic ARP Inspection (DAI))**

يعمل **DAI** مثل DHCP snooping (حتى أنه يعتمد عليه) حيث يتم تصنيف جميع منافذ المُبدّلات على أنها موثوقة أو غير موثوق بها.

تقوم المُبدّلة باعتراض وفحص جميع رُزم ARP التي تصل إلى منفذ غير موثوق به؛ بينما لا يتم إجراء فحص على المنافذ الموثوقة.

مثال: إعداد DAI على المنافذ الموثوقة لمُبدّلة



وتكون الإعدادات على المُبدّلة **Switch0** كالتالي:

```
Switch(config)#vlan 10
Switch(config-vlan)#name V10
Switch(config-vlan)#exit
Switch(config)#interface range f0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#
Switch(config)#interface g0/1
Switch(config-if)#exit
Switch(config)#ip arp inspection vlan 10
Switch(config)#interface g0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip arp inspection trust
Switch(config-if)#
Switch(config-if)#do wr
Building configuration...
[OK]
```

يمكن أن نطبّق الفحص على العنوان MAC للمصدر أو عنوان ال MAC للوجهة أو عنوان ال IP أو على جميعها:

```
S1(config)# ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address

S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)#
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)#
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)#
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

✓ التنصّل من هجمات انتحال العناوين (Mitigating Address Spoofing Attacks)

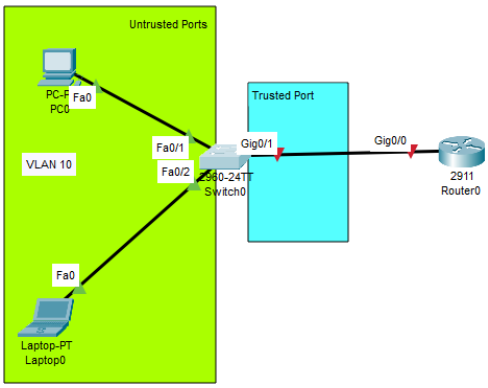
يمكن أن تستخدم مُبدّلات Cisco ميزة الحماية IP source guard لاكتشاف هجمات انتحال العناوين وتجنّبها -حتى إذا حدثت داخل نفس الشبكة الفرعية.

يقوم IP Source Guard بهذا من خلال الاستفادة من قاعدة بيانات DHCP Snooping وقائمة ربط (Binding) بين الأجهزة المصدر مع عناوينها ال IP وهي قائمة ربط ثابتة يُدخِلُها مدير الشبكة يدوياً.

ملاحظة:

يتم إعداد IP source guard على واجهات الشبكة Layer2 غير الموثوق بها (untrusted Layer-2 interfaces).

مثال (نفس مثال الفقرة السابقة): **إعداد IP Source Guard**



نطبّق الأوامر التالية على المُبدّلة **Switch0**:

```
Switch (config) # interface range fastethernet 0/1-2
Switch (config-if) # ip verify source
```

تصلُح الأوامر السابقة لوحدها في حال كانت الأجهزة تعتمد على مُخدّم DHCP فعّال على الشبكة للحصول على عناوينها وكانت DHCP Snooping فعّالة وبالتالي بإمكان المُبدّلة الاستفادة من قاعدة بيانات DHCP Snooping.

بينما في حال كانت الأجهزة لا تستخدم DHCP (كما هو الحال في مثالنا) عندها نقوم بإعداد قائمة ربط يدوياً حيث نُحدّد ضمنها عنوان ال IP وعنوان ال MAC ورقم المنفذ ورقم ال VLAN لكل من الأجهزة المتصلة بالمُبدّلة باستخدام الأمر التالي:

Switch (config) # **ip source binding** *mac_address* **vlan** *vlan_id ip_address* **interface** *interface_type interface_number*

وتكون التعليمات الواجب تطبيقها على المُبدّلة Switch0 كالتالي:

```
Switch (config-if) # ip source binding 0090.0CD9.A4EE vlan 10 192.168.1.10 interface fastethernet 0/1
Switch (config-if) # ip source binding 0000.0C12.4688 vlan 10 192.168.1.20 interface fastethernet 0/2
```

بعدها نفعّل Ip Source Guard:

```
Switch (config) # interface range fastethernet 0/1-2
Switch (config-if) # ip verify source
```

ملاحظة:

إن تعليمة ip verify source تفحص عنوان ال ip للمصدر فقط، ونستطيع إضافة الخيار port-security لفحص عنوان MAC المصدر أيضاً.

```
Switch (config) # interface range fastethernet 0/1-2
Switch (config-if) # ip verify source port-security
```

Note:

جميع التعليمات ضمن هذه الفقرة غير مُعرّفة ولا تعمل ضمن المُحاكي Packet Tracer، ويمكن تطبيقها على GNS 3 Emulator.

المراجع

- جامعة البعث -كلية الهندسة المعلوماتيّة -السنة الخامسة / مُقرّر أمن الشبكات الحاسوبيّة – مُحاضرة (Layer 2 Security) / **الدُكتورة زينب خَلوف.**

???Any Questions