Steven Kim
Mr. Mason
Adv Cisco CCNP P1,2
10/15/13

Lab 3 – Layer 2 Attacks

Purpose

The purpose of this lab was to learn how to execute attacks performed in Layer 2 and mitigate them. We were required to do a total of 3 – 4 attacks to ensure a thorough understanding of the attacks.

Background Information on Lab Concepts

Layer 2 attacks are attacks formed in the Data Link Layer in the OSI model. The Data Link Layer is responsible for transferring da0.ta between networks and detecting any errors occurring in the previous layer, the Physical Layer. It uses protocols like PPP, HDLC, and ADCCP for local area networks, and hardware addresses (also known as mac-addresses)

Hackers find a way to attack the network in this Data Link Layer. Examples include: CAM Table Overflow, DHCP Attacks, ARP Attacks, VLAN Hopping, Spanning Tree Attacks, CDP Attacks and etc. I've executed and mitigated four attacks in my lab: DHCP Starvation, CAM Table Overflow, CDP, and ARP Poisoning.

CAM Table Overflow is an attack that generates counterfeit MAC addresses until the number of MAC addresses reaches the maximum number permitted in a cam table, and floods a certain port of a Switch. The Switch has to broadcasts every traffic throughout the network to pass any other incoming traffic, just like a hub, disabling the Switch from storing any additional MAC addresses. This type of broadcast allows the hacker to view private information that the user doesn't want to reveal.

DHCP Starvation is an attack that exhausts the available addresses on a DHCP server and prevents the user from receiving any addresses from it. When this attack is executed, the user is disconnected from the network, not being able to receive a valid address and connect with other devices/users in the network.

ARP Poisoning (Spoofing) is an attack in which a hacker to send counterfeit ARP messages into networks. The attacker disrupts traffic by forwarding packets onto unwanted networks, causing the user to experience network disabilities.

CDP Attack, or Cisco Discovery Protocol Attack, is an attack that allows the hacker to cause Cisco devices to malfunction, including running out of memory and crashes. The attack can be executed when CDP is enabled.

The program I used was Backtrack 5 r3, a program run on VMware. It allows numerous attack commands, the one previously mentioned, to be performed. The *yersinia –[alphabet]* command can also be issued so that the attacker can go to various attacking modes.

Lab Summary

In this lab I used a simple network topology consisting of a Router, 1-2 Switches, and two hosts. The Router acted as a DHCP Server for DHCP Starvation. To set up DHCP, create a pool that requires a default-router id, a DNS server, and a network number.

CAM Table Overflow

After setting up backtrack (see below for commands), I attempted to initiate CAM Table Overflow . I proved this by using Wireshark in which the attacking host received ping packets from the victim hosts. I also went to the MAC address table and found that there were over 5000 dynamic addresses assigned on a single switchport.

The mitigation necessary for this attack was port-security; I had to set up port-security on all the ports to prevent the ports from being overflowed. The port-security commands allowed a single MAC address to be assigned per port. To ensure that the mitigation worked successfully, I again checked the number of MAC addresses assigned on a switchport and saw that only one address was assigned per switchport.

DHCP Starvation

To execute a DHCP Starvation attack, I first went to Yersinia (see commands below). I launched the attack that created a disruption in the DHCP Server; after verifying that IP addresses could not be assigned automatically using the commands *ipconfig /release* and *ipconfig /renew*, I realized that the attack was successful.

I found out that the mitigation necessary for this attack was the exact same as that for CAM Table Overflow. Switchport security initiated a shutdown on the port if a violation occurred and allowed only 1 address per port. This feature of port security allowed a detection and an action against the attack, which was necessary for the mitigation.

ARP Poisoning

For executing the ARP Poisoning Attack, I went to Ettercap (see commands below) and clicked scan for hosts. After that, I clicked Mitm then ARP Poisoning, then Sniff remote connections to execute the attack. I verified that the attack worked by using Wireshark, seeing that the false ARP packets were sent by the attacker and confusing the network. The victim host was then not able to ping and therefore communicate throughout the network.

For mitigation, I set up DHCP Snooping, which is a technique that allows only hosts with a specific address (IP or MAC) to have access to the network. This unique characteristic of DHCP Snooping kept sending denial messages, saying that it dropped ARP since there were no previous records of an IP address that has been used by a host.

CDP

To execute a CDP Attack, I went to Yersinia. I clicked the CDP tab and then simply the flood CDP table. This allowed a disruption in the CDP table, as verified by the command *show cdp entry* and/or *show cdp neighbors*. The attack host was also able to gain information that can be shown using the command *show cdp neighbors* on the victim host.

For mitigation, I simply disabled CDP on both the global config mode and the interface mode. CDP is a protocol that is enabled by default; I realized that turning this unnecessary protocol will ensure security and therefore mitigate the CDP attack executed by the attacking host.

Lab Commands

Setting up the topology did not require many commands: I created VLAN 2, grouped all ports to it, and set IP addresses to *interface vlan 2*, interface fa0/1 , and hosts (for DHCP, I configured the pool). The commands required are *switchport mode access and switchport access vlan 2* on the interface mode. Before this, the command *vlan 2* had to be issued on the global config mode to create VLAN 2.

For DHCP Starvation setup, I issued the command *ip dhcp pool 1* on the global config mode to set up a DHCP pool. The commands network *10.0.0.0 255.255.255.0, dns-server 200.20.2.1,* and *default-router 10.0.0.1* were issued on the Router (config-dhcp)# mode.

To initiate Backtrack 5 rd3, I typed root for username and toor for the password. Then, I used the command *startx* to load the actual Backtrack applications.

The following are the commands for the attacks/mitigations:

1. CAM Table Overflow - Attack

   I used the command *macof* – 1 eth1 in the Backtrack command prompt, which is where the first screen that came up after issuing the command *startx*. This shows a large list containing a vast amount of randomly generated MAC addresses.

2. CAM Table Overflow – Mitigation

   The commands *switchport port-security*, *switchport port-security maximum 1*, *switchport port-security mac-address sticky*, and *switchport port-security violation shutdown* must be issued on the interface mode, on every interface. These commands enable Switchport Security against the attacks by allowing only 1 address per port, enabling sticky learning on the interfaces, and a shutdown of the interface when a violation is made.

3. DHCP Starvation – Attack

   The command Yersinia –G must be issued to enter Yersinia. Then, click the Launch Attack tab and send DISCOVER packets. Verify that the attack was successful by issuing the command *ipconfig /release* and *ipconfig /renew* on the command prompt. The victim host should not be receiving any IP addresses from the DHCP Server; it should display an error message instead.

4. DHCP Starvation – Mitigation

   The mitigation for DHCP Starvation, as mentioned earlier, is the same as that for CAM Table Overflow. Refer to the Mitigation commands in #2.

5. ARP Poisoning – Attack

   There are a series of clicks needed for the ARP Poisoning Attack on Ettercap:

   Before doing anything, verify that connectivity is ensured by clicking Scan for hosts on the top. Click Add to Target 1 or 2 to ensure that the Victim host is a target.
   Issue the command Ettercap –G to enter Ettercap mode. Click Mitm on the top then ARP Poisoning. Then, click Sniff remote connections to initiate the attack.
   Verify that the attack was successful by pinging and Wireshark. There will be a continuous loop on Wireshark while the victim host will receive *Destination Host Unreachable* messages.

6. ARP Poisoning – Mitigation

   There were several commands that were needed to be issued for mitigating an ARP Poisoning Attack:
   On the global config mode, type in the commands *ip dhcp snooping vlan 2, ip dhcp snooping, and ip arp inspection vlan 2*. As mentioned in the Lab Summary section, DHCP Snooping is a protocol that denies any unknown ARP requests. Then, on interface fa0/1 and fa0/3, issue the command *ip arp inspection trust*, which allows the Switch to trust an interface. Verify that the mitigation was successful by pinging the router.

7. CDP Attack – Attack

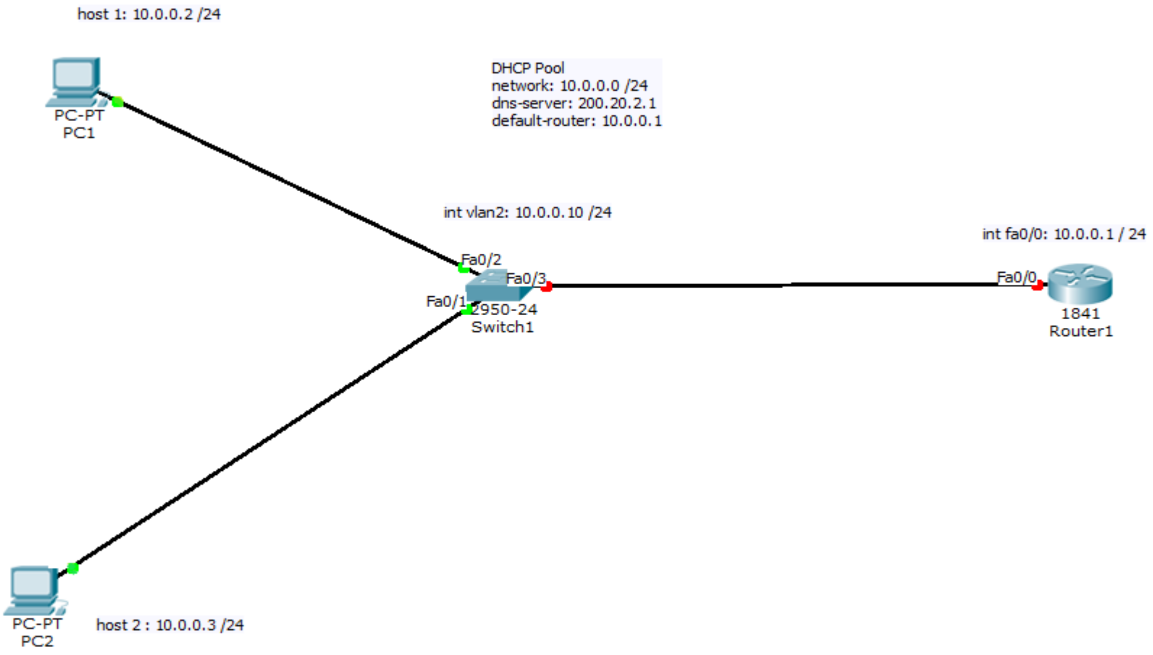
   The command Yersinia –G must be issued initially. Then, click Launch Attack and then the CDP. Click Flood CDP table there and verify that the attack was successful through Wireshark on the attacking host and *show cdp entries* and *show cdp neighbors* on the global config mode of the victim host.

8. CDP Attack – Mitigation

   The commands *no cdp run and no cdp enable* must be issued on the interface mode and the global config mode, respectively.

NOTE: All the mitigation commands were issued on the Switch.

Network Diagram with IPs



Configurations

DHCP Configuration before mitigation

Router 1

```
R1(config)#do sh run
Building configuration...

Current configuration : 1460 bytes
!
! Last configuration change at 15:28:05 UTC Thu Oct 10 2013
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
memory-size iomem 10
!
no ipv6 cef
ip source-route
ip cef
!
!
!
!
ip dhcp pool 1
 network 10.0.0.0 255.255.255.0
 default-router 10.0.0.1
 dns-server 200.20.2.1
!
!
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
!
license udi pid CISCO2901/K9 sn FTX1704Y03B
!
!
!
!
```

```
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
```

```
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin
lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

Switch 1

```
S1(config)#do sh run
Building configuration...

Current configuration : 2609 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
!
!
!
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
!
!
!
!
```

```
!
!
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard
misconfig
spanning-tree extend system-id
!
vlan internal allocation policy
ascending
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 10.0.0.10 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
```

Other Configurations before mitigation

Router 1 (Server)

```
R1(config)#do sh run
Building configuration...

Current configuration : 1460 bytes
!
! Last configuration change at 15:28:05
UTC Thu Oct 10 2013
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
memory-size iomem 10
!
no ipv6 cef
ip source-route
ip cef
!
!
!
multilink bundle-name authenticated
!
!
crypto pki token default removal
timeout 0
!
!
license udi pid CISCO2901/K9 sn
FTX1704Y03B
!
!
!
!
!
!
!
!
!
ip sla enable reaction-alerts
!
!
!
line con 0
line vty 5 15
!
end
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin
lapb-ta mop udptn v120 ssh
 stopbits 1
```

```
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
```

Cam Table Overflow Mitigation (show run)

Switch 1

```
S1(config)#do sh run
Building configuration...

Current configuration : 2609 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
!
!
!
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard
misconfig
spanning-tree extend system-id
!
vlan internal allocation policy
ascending
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address
sticky
 switchport port-security mac-address
sticky acf2.c555.9788 vlan access
!
interface FastEthernet0/2
```

```
end
```

Switch 1

(Same as DHCP)

```
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address
sticky
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address
sticky
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 10.0.0.10 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
!
ip sla enable reaction-alerts
!
!
!
line con 0
line vty 5 15
!
end
S1(config)#do sh run
Building configuration...

Current configuration : 2609 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
!
!
!
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
!
```

```
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard
misconfig
spanning-tree extend system-id
!
vlan internal allocation policy
ascending
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address
sticky
 switchport port-security mac-address
sticky acf2.c555.9788 vlan access
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address
sticky
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address
sticky
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 10.0.0.10 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
!
ip sla enable reaction-alerts
!
!
!
line con 0
line vty 5 15
!
end
```

DHCP Starvation Mitigation (show run)

Switch 1

```
S1(config)#do sh run
Building configuration...

Current configuration : 2609 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
!
!
!
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard
misconfig
spanning-tree extend system-id
!
vlan internal allocation policy
ascending
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address
sticky
 switchport port-security mac-address
sticky acf2.c555.9788 vlan access
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address
sticky
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address
sticky
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 10.0.0.10 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
!
ip sla enable reaction-alerts
!
!
!
line con 0
line vty 5 15
!
end
```

ARP Poisoning Mitigation (show run)

Switch 1

```
S1(config)#do sh run
Building configuration...

Current configuration : 2609 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
!
!
!
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard
misconfig
spanning-tree extend system-id
!
vlan internal allocation policy
ascending
!
!
!
ip dhcp snooping vlan 2
ip dhcp snooping
ip arp inspection vlan 2
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
 ip arp inspection trust
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
 ip arp inspection trust
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 10.0.0.10 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
!
ip sla enable reaction-alerts
!
!
!
line con 0
line vty 5 15
!
end
```

CDP Attack Mitigation (show run)

Switch 1

```
S1(config)#do sh run
Building configuration...

Current configuration : 2609 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!
hostname S1
!
boot-start-marker
boot-end-marker
!
!
!
!
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
!
!
!
!
no cdp enable
no cdp run
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access

!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 10.0.0.10 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
!
ip sla enable reaction-alerts
!
!
!
line con 0
line vty 5 15
!
end
```

Problems

Overall, I had 2 main problems in this lab: the burdensome research that was necessary for executing and mitigating the attacks and my inadequate planning for the video and the lab itself.

The research involved in this lab was tremendous and crucial. Since my peers and I did not have a clear background of Layer 2 Attacks, Mr. Mason required us to initially watch a video from a cisco website regarding Layer 2 Attacks. In addition to this video, I had to research every command that was not on the video; it was difficult to find how port security did not resolve every attacks that were performed. I also did not research enough information for performing and mitigating the attacks, such as not finding out which commands were necessary for initiating backtrack or not knowing which mitigation commands were appropriate.

My inadequate planning for the video also served as an impediment. Initially, I thought that I could hastily finish the video without practicing the filming beforehand. I was wrong: I could not finish the video for the very first attack after 2 hours. I did not realize how much time I would've saved had I not gone the vast amount of trial and errors. The process of filming that I went through was done impromptu: I had only a vague sense of how to even perform the mitigations before filming a video. As time came, it became obvious that careful planning is another crucial factor for efficiency.

Conclusion

Although I had undergone numerous time-consuming processes throughout this lab, the overall result was satisfactory. I created a cisco video using Camtasia for the very first time. Not only that, I had the opportunity to familiarize myself with common Layer 2 attacks, a part of "hacking" that I've always been interested in, that are still prevalent in many network fields. Such familiarization includes learning how to defend my networking devices from future Layer 2 attacks, a skill that is crucial to network engineers.

For more information, check the following URL which is linked to the Video I created:

http://www.youtube.com/watch?v=Rh1P0MjxmbQ