LABORATORY WORK NO. 11

Security Threats in Computer Networks

1. Objectives

At the end of the laboratory, students will be able to understand and analyze common security threats that occur in computer networks.

2. Common security threats

Network security in computer networking is a very broad domain and the security attacks can have different purposes, such as: service interruption, gaining elevated privilege for various services, data stealing, data corruption, etc. Security threats occur at every layer of the ISO/OSI model and networks must be secured with proper defenses against any possible attack.

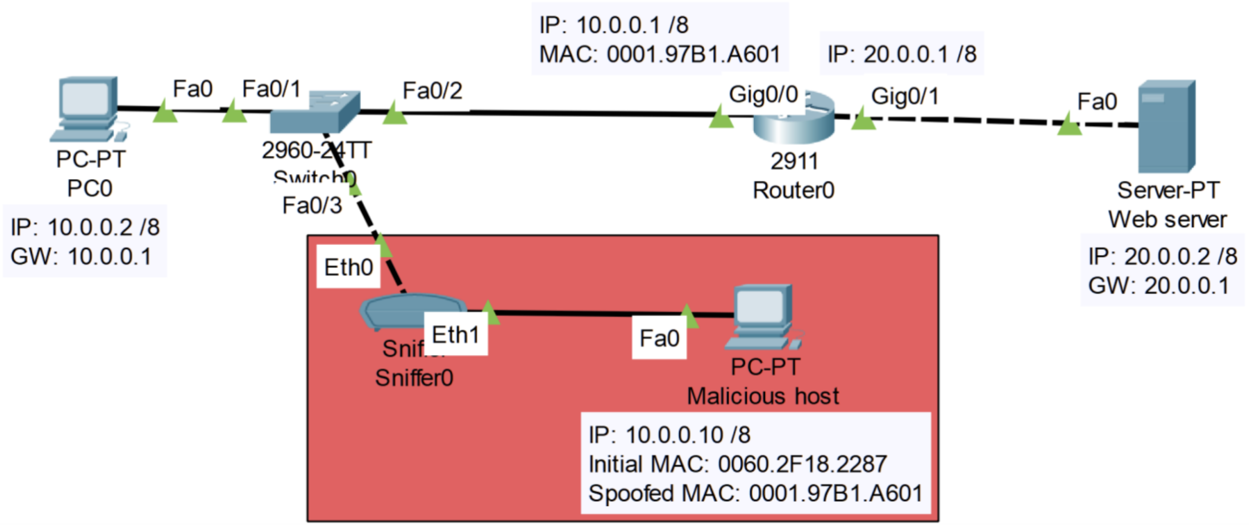
The current laboratory demonstrates the working principles of a few security threats using the Cisco Packet Tracer tool. In a real life scenario additional tools might be required to perform these attacks but the objective of this laboratory activity is academic only. The desired purpose is to understand how certain attacks are implemented and what are the best ways to prevent them from taking place.

The main concepts that are addressed in this laboratory are the following:

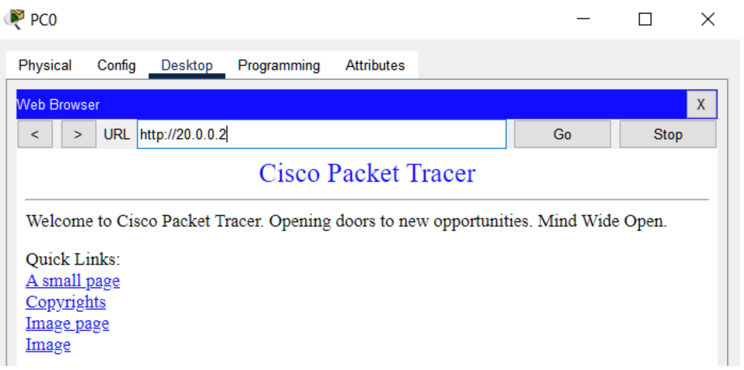
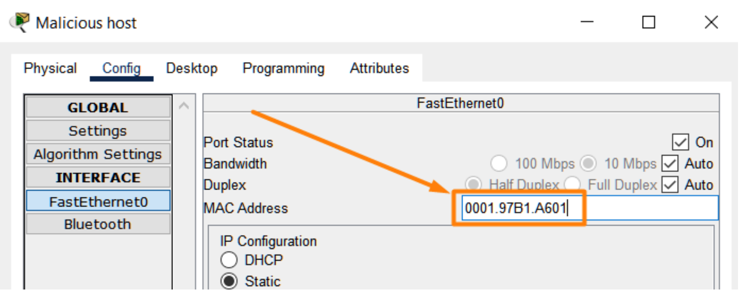
- **ARP spoofing**: This is the process in which a malicious device is spoofing its own MAC address, meaning it is masking its own MAC Address with a different MAC address that can belong to a different network device. In order to inform the other devices of the fake MAC address, the malicious device is sending a gratuitous ARP to the other network hosts informing them of the MAC address that resides at a specific IP Address. After each network host receives the ARP reply they will store the new pair of IP - MAC addresses in their own ARP cache table and when they will send a packet to the particular device, they will fill the Layer 2 header with the spoofed MAC address.
- **Network sniffer:** A network sniffer is a device that can intercept network traffic and records it using traffic monitoring tools.
- **Denial of Service (DoS):** This is a type of attack that has the purpose to restrict access to normal network functions.
- **Rogue server:** A rogue server does not belong to the institution (or stakeholder) that owns the network. Such a server can offer various services and invalid information to network devices with malicious intent.
    - **Rogue web server:** can offer web pages that look like a real website, but they are in fact copies of a real site
    - **Rogue DHCP server:** can offer invalid addressing, e.g. wrong default gateway for denying other hosts access to the internet, wrong DNS server to make hosts access invalid web server
    - **Rogue DNS server:** can provide fake mappings between URL - IP address with the purpose to force users to access a fake web server which apparently resides at a valid URL
- **Phishing:** A type of attack meant to steal information through a fraudulent message or web site.

2.1. ARP spoofing for DoS and data sniffing

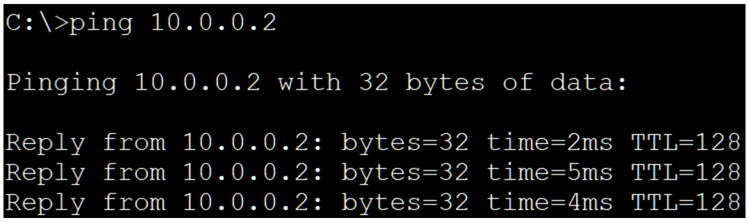
An example of ARP spoofing attack with the end goal to deny access to certain resources and to allow data sniffing can be seen in the figure below:



In order to perform the attack, configure the topology in Packet Tracer, then follow the steps described below.

1.	A web server resides at IP address 20.0.0.2. Accessing the default web page from PC0 having the IP address 10.0.0.2, the Cisco Packet Tracer view will look like the image on the right	 PC0 Physical Config Desktop Programming Attributes Web Browser X &lt; &gt; Go Stop URL http://20.0.0.2 Cisco Packet Tracer Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open. Quick Links: A small page Copyrights Image page Image
2.	The figure shows that the router's Gig 0/0 interface has the MAC address: 0001.97B1.A601 The malicious host can override its own MAC address with that of the router	 Malicious host Physical Config Desktop Programming Attributes GLOBAL Settings Algorithm Settings INTERFACE FastEthernet0 Bluetooth FastEthernet0 Port Status ☑ On Bandwidth ○ 100 Mbps ○ 10 Mbps ☑ Auto Duplex ○ Half Duplex ○ Full Duplex ☑ Auto MAC Address 0001.97B1.A601 IP Configuration ○ DHCP ● Static

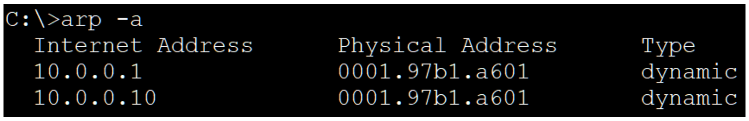
3. The next step for the malicious host is to inform the other network devices in the network that the MAC address of the router actually corresponds to the IP address of the malicious host. This can be done by generating continuous traffic in the network, e.g. using the ping command with the -t parameter



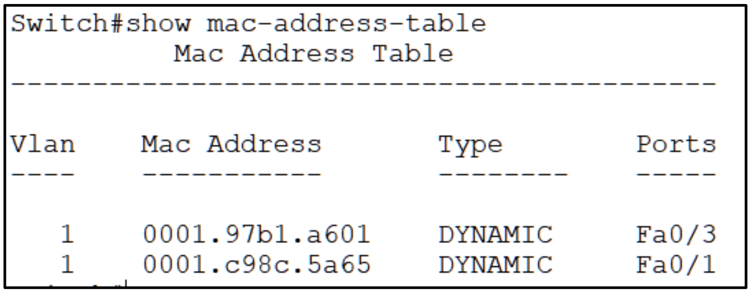
```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=2ms TTL=128
Reply from 10.0.0.2: bytes=32 time=5ms TTL=128
Reply from 10.0.0.2: bytes=32 time=4ms TTL=128
```

4. Next, the ARP cache entries on the other network devices can be verified (on PC0 having the IP address 10.0.0.2 and on the switch)

Viewing this information it can be seen that the computer will add the same MAC address when generating traffic towards the gateway or the malicious host, but the switch will as well redirect the traffic on the Fa 0/3 interface which links towards the malicious host (if the MAC address table does not change, use the *#clear mac-address-table* command)

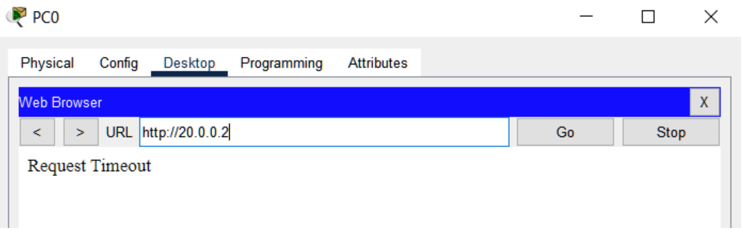


```
C:\>arp -a
  Internet Address      Physical Address      Type
  10.0.0.1              0001.97b1.a601        dynamic
  10.0.0.10             0001.97b1.a601        dynamic
```



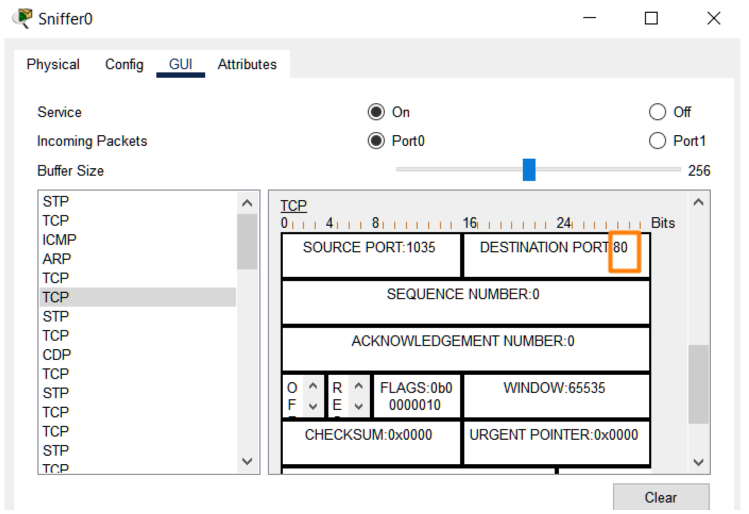
```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.97b1.a601    DYNAMIC     Fa0/3
   1    0001.c98c.5a65    DYNAMIC     Fa0/1
```

5. Next, when PC0, having IP address 10.0.0.2, tries to access the web server, it will create a packet having the correct MAC address of the network gateway (interface Gig 0/0 on the router), but the switch will redirect this packet towards the malicious host through the network sniffer



URL http://20.0.0.2

Request Timeout

6.	The sniffer can also be opened and inspect its GUI. The TCP traffic that is generated from the computer towards the web server can be inspected. Not much information is seen in this Cisco Packet Tracer example, but a real life test can reveal multiple traffic flows being generated from the targeted PC	 Sniffer0 Physical Config GUI Attributes Service ● On ○ Off Incoming Packets ● Port0 ○ Port1 Buffer Size 256 STP TCP ICMP ARP TCP TCP STP TCP CDP TCP STP TCP TCP STP TCP TCP 0 4 8 16 24 Bits SOURCE PORT:1035 DESTINATION PORT:80 SEQUENCE NUMBER:0 ACKNOWLEDGEMENT NUMBER:0 OF RE FLAGS:0b0 0000010 WINDOW:65535 CHECKSUM:0x0000 URGENT POINTER:0x0000 Clear

After analyzing the entire sequence of steps, the ARP spoofing attack was successful with the outcome of denying the service to the web server and eavesdropping on the traffic generated by the computer.

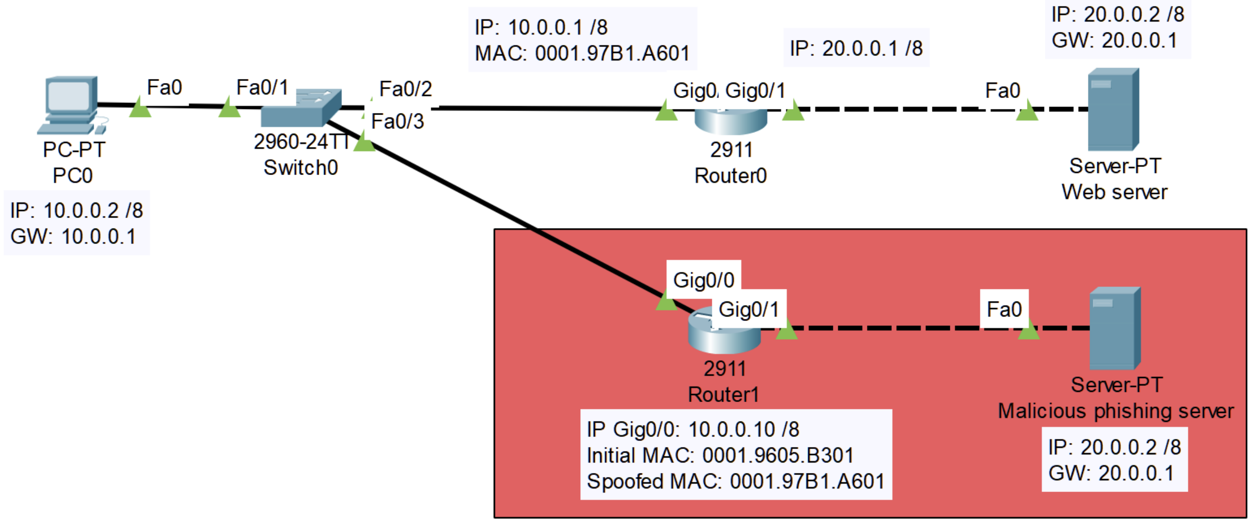
Possible ways to overcome these security threats include (but are not limited to):

- Limiting the number of allowed MAC addresses per switch port
- Configuring inspection of MAC - IP address consistency

Research other mechanisms to prevent ARP spoofing.

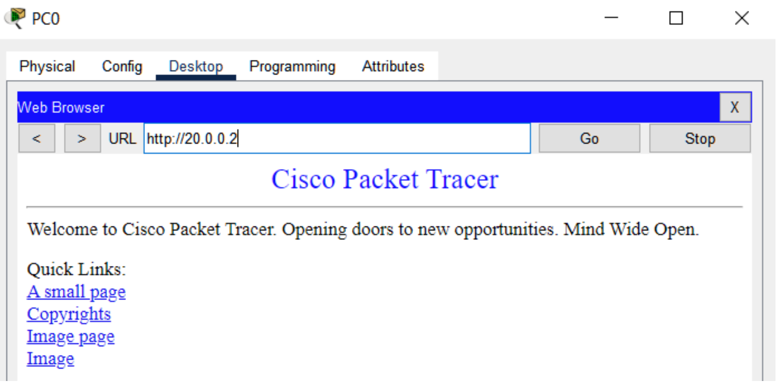
2.2. ARP spoofing for phishing

An example of a phishing attack from a web server can be seen in the figure below where an attacker is connecting to the network with a router (with a static IP address) and a web phishing server in the network behind the connected router:



In order to perform the attack, configure the topology in Packet Tracer, then follow the steps described below.

1. A web server resides at IP address 20.0.0.2. Accessing the default web page from PC0 having the IP address 10.0.0.2, the Cisco Packet Tracer view will look like the image on the right



URL http://20.0.0.2

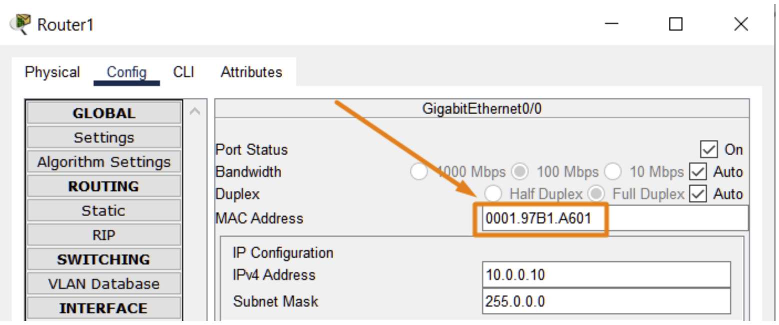
Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

2. The figure shows that Router0's Gig0/0 interface has the MAC address: 0001.97B1.A601

The threat actor connects to the network with a router where the MAC address is overridden with the MAC address of Router0

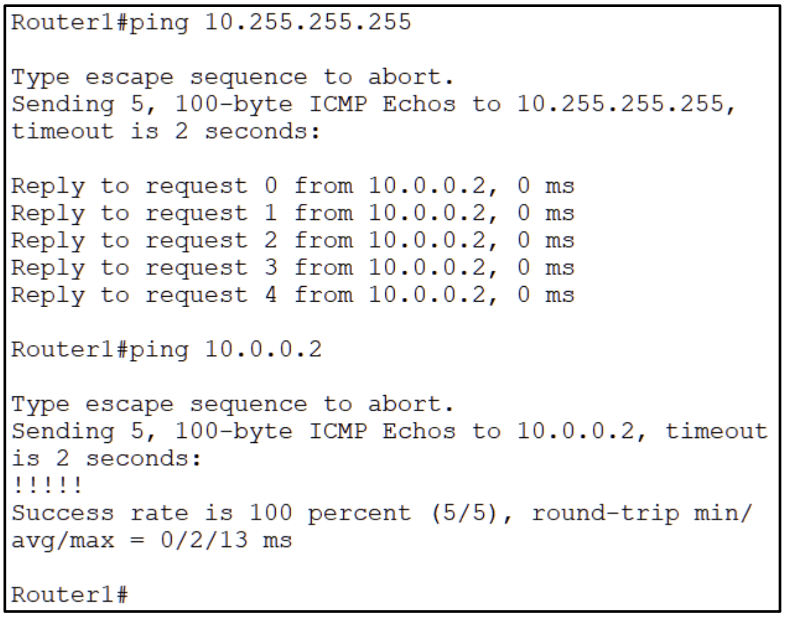


GigabitEthernet0/0

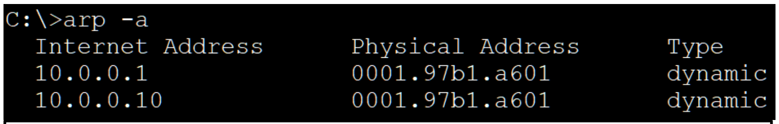
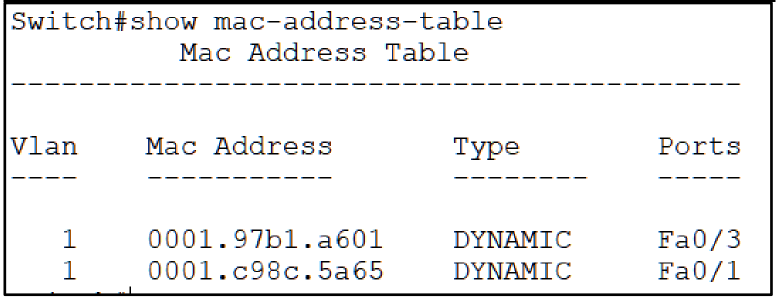
Port Status ☑ On
Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address 0001.97B1.A601

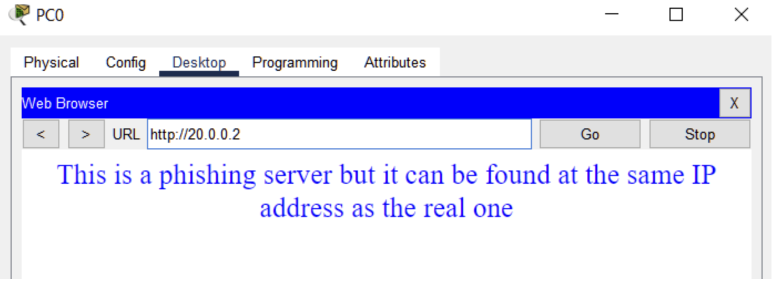
IP Configuration
IPv4 Address 10.0.0.10
Subnet Mask 255.0.0.0

3. The next step for the threat actor is to inform the other network devices in the network that the MAC address of Router0 actually corresponds to Router1 (the malicious router). This can be done by generating continuous traffic in the network, e.g. using the ping command from the Router1's CLI as shown in the image on the right



```
Router1#ping 10.255.255.255

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.255.255.255,
timeout is 2 seconds:

Reply to request 0 from 10.0.0.2, 0 ms
Reply to request 1 from 10.0.0.2, 0 ms
Reply to request 2 from 10.0.0.2, 0 ms
Reply to request 3 from 10.0.0.2, 0 ms
Reply to request 4 from 10.0.0.2, 0 ms

Router1#ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/
avg/max = 0/2/13 ms

Router1#
```

4.	Next, the ARP cache entries on the other network devices can be verified (on PC0 having the IP address 10.0.0.2 and on the switch)
	Viewing this information it can be seen that the computer will add the same MAC address when generating traffic towards the gateway of Router1, but the switch will as well redirect the traffic on the Fa 0/3 interface which links towards Router1 (if the MAC address table does not change, use the *#clear mac-address-table* command)
		
		C:\>arp -a
		  Internet Address Physical Address Type
		  10.0.0.1 0001.97b1.a601 dynamic
		  10.0.0.10 0001.97b1.a601 dynamic
		
		Switch#show mac-address-table
		          Mac Address Table
		--- 	
		Vlan Mac Address Type Ports
		---- ----------- -------- -----
		   1 0001.97b1.a601 DYNAMIC Fa0/3
		   1 0001.c98c.5a65 DYNAMIC Fa0/1

5.	Next, when PC0 will try to access the web server, it will create a packet having the correct MAC address of the network gateway (interface Gig 0/0 on Router0), but the switch will redirect this packet towards Router1. After the packet reaches Router1, the threat actor has already set up in place a simulated network which mimiques the same IP addresses as in the real network but creates a phishing website showing different content, but which is still accessible on the same IP address	 PC0 Physical Config Desktop Programming Attributes Web Browser X < > URL Go Stop http://20.0.0.2 This is a phishing server but it can be found at the same IP address as the real one

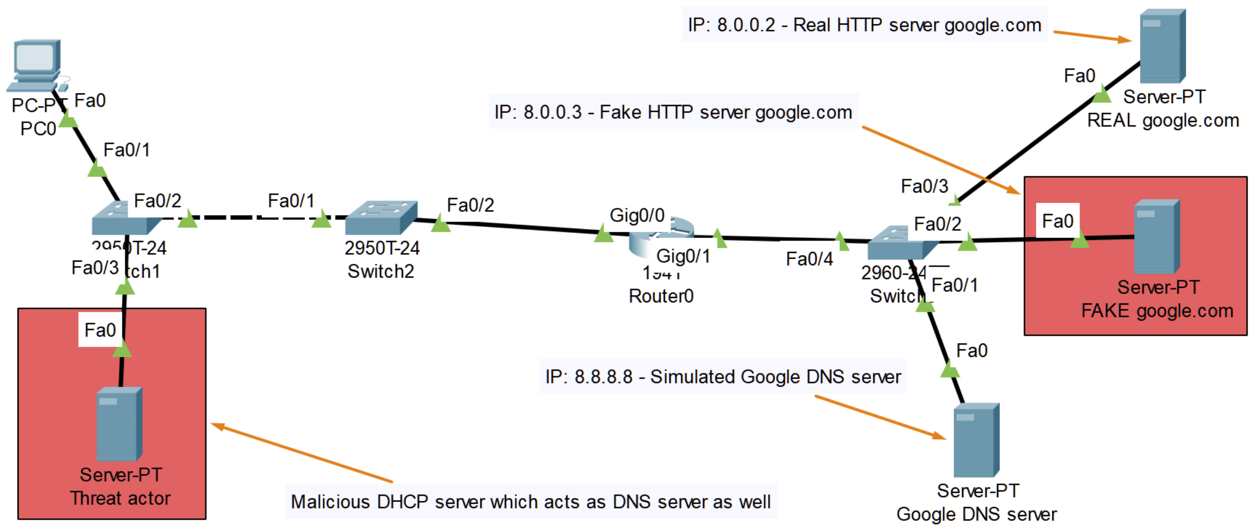
After analyzing the entire sequence of steps, the ARP spoofing attack was successful with the outcome of making the targeted host access a fake server that can accomplish phishing scenarios if configured to e.g. accept credentials input.

One of the best advised ways to overcome this issue is to prevent/avoid it entirely by not accessing unsecured websites from untrusted networks or by not introducing sensitive credential information when present in an untrusted network.

Research other mechanisms to prevent ARP spoofing and phishing.

2.3. Rogue DHCP and DNS servers for phishing

An example of a phishing attack which is performed with the help of a rogue DHCP and DNS server can be seen in the figure below:



IP: 8.0.0.2 - Real HTTP server google.com

IP: 8.0.0.3 - Fake HTTP server google.com

IP: 8.8.8.8 - Simulated Google DNS server

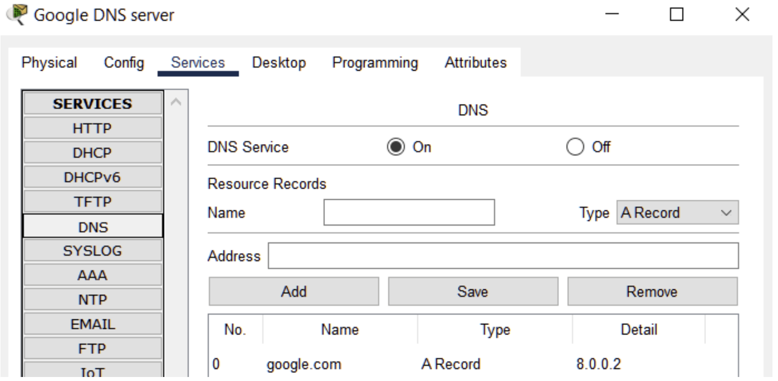
Malicious DHCP server which acts as DNS server as well

The threat actor connects to the network with a server providing false DHCP addressing information (the DNS server configuration being the most important addressing information in this example). When the computers inside the network use the false DNS server to access the IP address of a web server, they will be redirected to the phishing server instead of the real one.

Configure the topology in Packet Tracer, then follow the steps described below.

<table>
<tr>
<td>1.</td>
<td>Initial configuration steps:
- Leave the threat actor unconfigured (or remove its link to the switch)
- Configure DHCP on Router0 and ensure that it provides a valid DNS server in the addressing information (as seen on the right)
- Configure the simulated Google DNS server as seen on the right side</td>
<td>

```
ip dhcp pool pool1
 network 10.0.0.0 255.0.0.0
 default-router 10.0.0.1
 dns-server 8.8.8.8
```

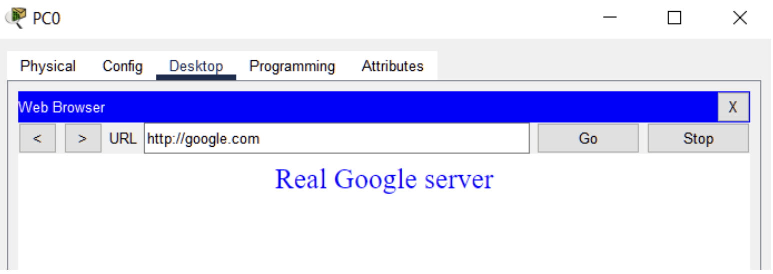


DNS
DNS Service ● On ○ Off
Resource Records
Name
Type A Record
Address

No.	Name	Type	Detail
0	google.com	A Record	8.0.0.2

</td>
</tr>
</table>

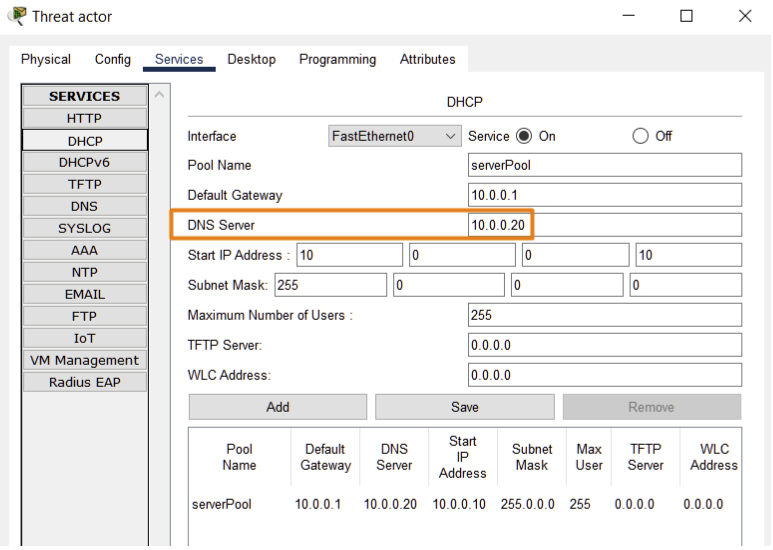
2. A simulated Google server resides at the server having the 8.0.0.2 IP address. Accessing this server from PC0, the Cisco Packet Tracer view will look like the image on the right.



URL http://google.com

Real Google server

3. Connect the threat actor to the network and configure its DHCP service as seen in the image on the right side. Notice the different DNS server which in fact corresponds to the threat actor’s static IP address.



DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name serverPool

Default Gateway 10.0.0.1

DNS Server 10.0.0.20

Start IP Address : 10 0 0 10

Subnet Mask: 255 0 0 0

Maximum Number of Users : 255

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

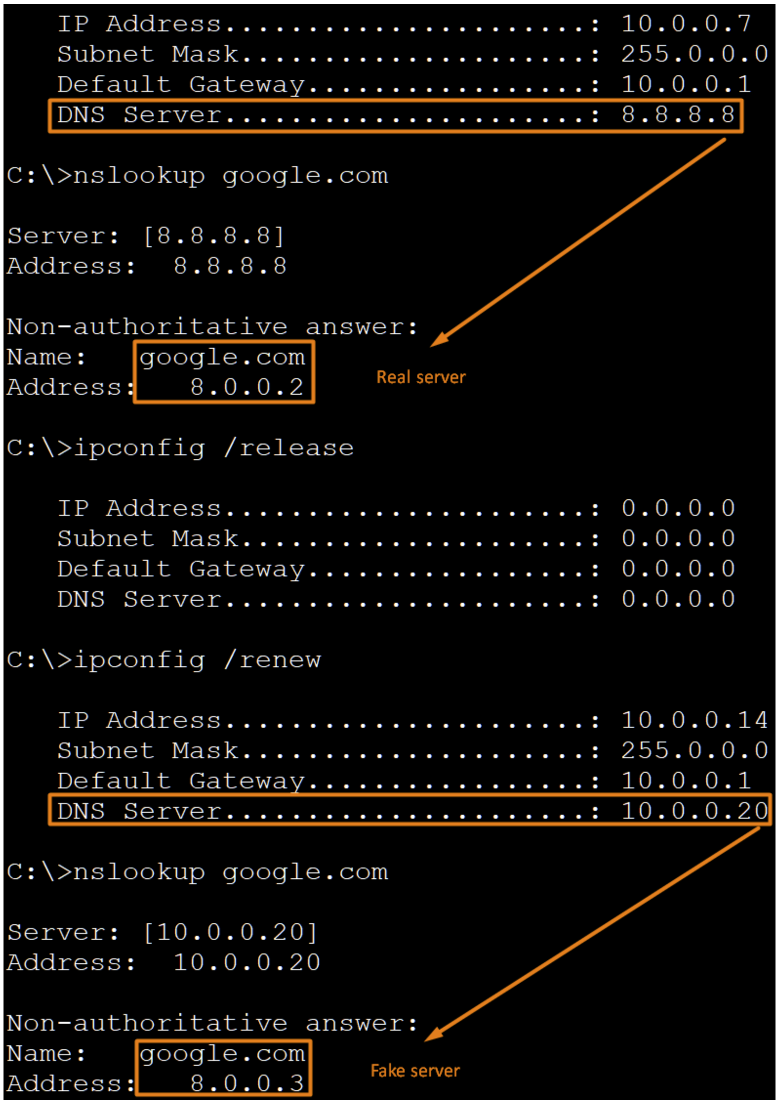
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	10.0.0.1	10.0.0.20	10.0.0.10	255.0.0.0	255	0.0.0.0	0.0.0.0

4. At some point, PC0 will have to update its addressing information by requesting a new lease from the DHCP server. This step can be manually simulated as seen on the right side.

   Notice how the DNS server has changed, meaning that PC0 receives the lease from the threat actor and not from Router0.

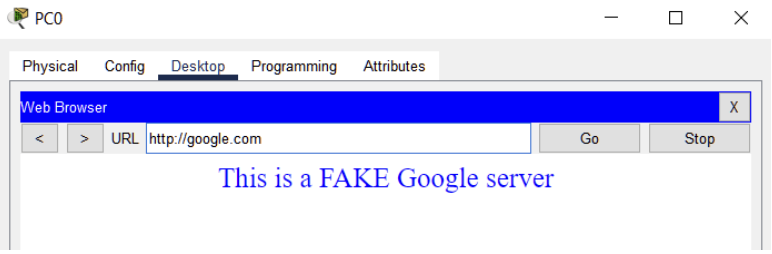
   Investigate how this happens by using the Simulation tool provided by Cisco Packet Tracer.

   It is obvious that the DNS server configured on the threat actor's server will not match the "google.com" URL to the correct IP address, it will match the URL to the fake server's IP address as seen in the topology. Running an nslookup command on PC0 will prove this.



```
   IP Address......................: 10.0.0.7
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: 10.0.0.1
   DNS Server......................: 8.8.8.8

C:\>nslookup google.com

Server: [8.8.8.8]
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Address:    8.0.0.2

C:\>ipconfig /release

   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Server......................: 0.0.0.0

C:\>ipconfig /renew

   IP Address......................: 10.0.0.14
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: 10.0.0.1
   DNS Server......................: 10.0.0.20

C:\>nslookup google.com

Server: [10.0.0.20]
Address:  10.0.0.20

Non-authoritative answer:
Name:    google.com
Address:    8.0.0.3
```

5. After PC0 has been compromised, accessing the google.com web page will redirect to the fake server showing a different page.



URL http://google.com

This is a FAKE Google server

After analyzing the entire sequence of steps, this phishing attack was successful and it can trick the user into entering his credentials on a fake web page having a seemingly valid URL.

Research mechanisms to prevent rogue servers to provide false network services and mechanisms to prevent phishing attacks.