L7 - DNS Spoofing Threat

Recently, suspicions have arisen regarding a potential security vulnerability in a network where access to sensitive platforms such as banking applications is provided. Users have reported encountering suspicious web pages or experiencing unexpected redirections when attempting to access a known banking website, such as www.banka.com. Instead of the expected secure banking interface, they have encountered content that appears different or unexpected.

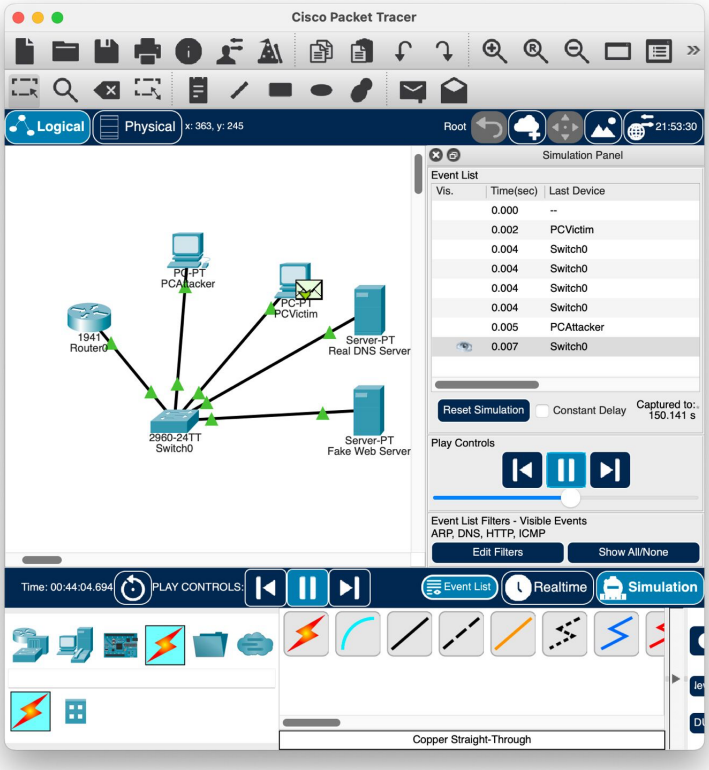
Expected Behavior: When accessing www.bank.com, the actual bank's IP address (192.168.1.10) should be resolved, and the legitimate bank website should load.
Observed Problem: When the user navigated to www.bank.com, a fake IP address (192.168.1.20) was resolved, and a fraudulent "phishing" web site loaded instead.
Primary Suspicion: This situation suggests that the DNS resolution mechanism on the network has been manipulated, indicating a DNS Spoofing attack has occurred.

Router CLI commands for interface configuration (GigabitEthernet0/0) and DHCP server setup, including DNS server assignment;

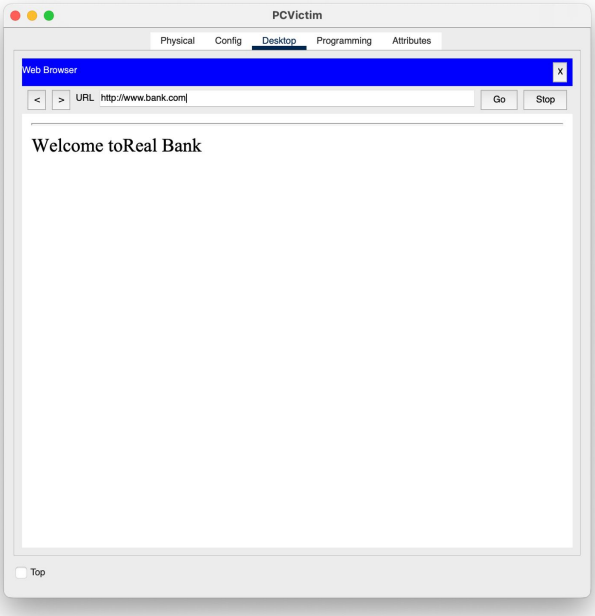
```
Router(config)#
Router(config)#
Router(config)#
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.5
Router(config)#p dhcp pool VLAN1
% Ambiguous command: "p dhcp pool VLAN1 "
Router(config)#ip dhcp pool VLAN1
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.10
Router(dhcp-config)#exit
Router(config)#write memory
               ^
% Invalid input detected at '^' marker.

Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Router#
```

The network topology for the DNS Spoofing simulation, showing active connections and the Packet Tracer Simulation Panel.



Victim PC's web browser successfully accessing www.bank.com and displaying the legitimate 'Welcome to Real Bank' page before the attack.



This problem primarily falls under OSI Layer 7 (Application Layer), as DNS (Domain Name System) is an application-layer protocol.