Seunghyuk Baek

[Sbaek44@vt.edu](mailto:Sbaek44@vt.edu)

ECE5480 Project 7.

**Objective**

This lab is to demonstrate the DNS attack in 3 different ways. First DNS attack is placed with assumption that the victim’s system is already compromised by a hacker, so the hacker has all privileges to modify victim’s system. Second DNS attack simulates when a hacker is using same private network with victim and can steal traffic between the victim and DNS server. Last scenario is to simulate when the traffic between DNS server and other authoritative DNS servers is captured and modified by a hacker.

**Lab Environment Setup**

To simulate such scenarios, three linux virtual machines were set up in a private NAT network. Each of these VM takes role of hacker, user and DNS server. If all VMs are set up correctly, each VM machine can connect to internet.

A screenshot of a cell phone

Description automatically generated

Next, we need to set up one VM as dns server. Which will result in

A screenshot of a cell phone

Description automatically generated

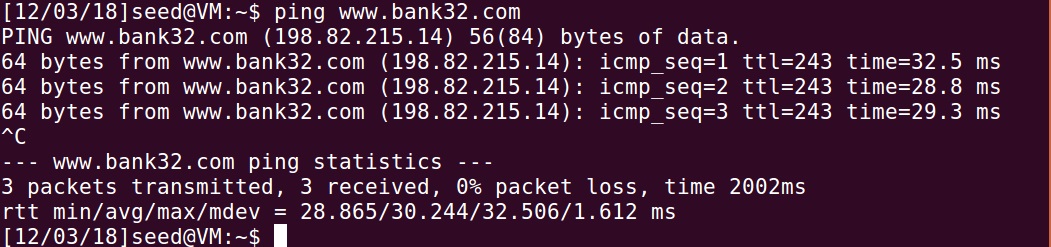
**Task 1.**

If victim’s computer is compromised by a hacker, the hacker can modify HOST file which serves as local lookup and preferred over remote DNS lookups.

A close up of text on a black background

Description automatically generated

[www.bank32.com](http://www.bank32.com) ip address is changed from 184.168.221.58 to 198.82.215.14.



**Task 2.**

In this task, a hacker sniffs the packet between the user and the local DNS server. When the user asks for service to local DNS server, the hacker intercept user’s query can send malicious response to the user.

A screenshot of a cell phone

Description automatically generated

Above is the result of dig [www.example.com](http://www.example.com) before hacker attack

A screenshot of a cell phone

Description automatically generated

Above is dig [www.example.com](http://www.example.com) command after successful hacker attack by sniffing transaction between user and DNS server. Note that ip address of example.com and the name of DNS server had been changed.

**Takas3.**

In this task, the hacker poisons local DNS server so any user who connects to this DNS can be affected by hacker. To do this, hacker intercept the traffic between local DNS and remote DNS. Once, local DNS receives spoofed query from the hacker, the DNS saves spoofed ip address in cache and uses it for other queries.

A screenshot of a cell phone screen with text

Description automatically generated

Above picture is screenshot of user after DNS poisoning attack is successful.

A screenshot of a cell phone

Description automatically generated

Above is dumped cache from DNS server.

**Conclusion.**

By attacking DNS, hacker can lead victims to malicious web site without notice. DNS attack is especially effective when a user’s system is already compromised to a hacker. Therefore, it is needed to check whether DNS is indeed valid authority. For NAT network, network administrator’s care is needed to avoid DNS attack by hacker. Also, it is much easier for a hacker to attack from the inside network. Therefore, effective user control is needed. For this assignment, setting up VMs and each systems according to their role was hardest part. It took around 8 hours to finish this lab.