Security In Computing (CC5004NI)

Course Work 2

TOPIC CHOSEN: SECURITY IN NETWORKS

Submitted By: Manish Giri
Student ID Number: 16034959

Submitted To: Lecturer: Akchyat Bikram Joshi
Submission Date: 04/24/2018

ACKNOWLEDGEMENT

The success and final outcome of this project required a lot of guidance and assistance from many people and I am extremely privileged to have got this all along the completion of my project. All that I have done is only due to such supervision and assistance and I would not forget to thank them.

I respect and thank to **Mr. Akchyat Bikram Joshi** , for providing me an opportunity to do the project work in and giving us all support and guidance which made me complete the project duly. I am extremely thankful to him for providing such a nice support and guidance, although he had busy schedule managing the college affairs.

ABSTRACT

The fundamental subject of this coursework is to show about the vulnerabilites on Security in Network in detail. It depicts the issue, its motivation, dangers, Vulnerabilities and effects. The attack scenario and Problem situation has been investigated alongside its points and destinations. A basic DNS spoofing situation has been performed and the result has been screenshot and clarified

This project won't have been completed without the help of various research papers, journals, websites and EBooks. Therefore they are taken as the references.

TABLE OF CONTENTS

TABLE OF FIGURES

DNS SPOOFING(MAN IN THE MIDDLE ATTACK)

(Keycdn, n.d.)

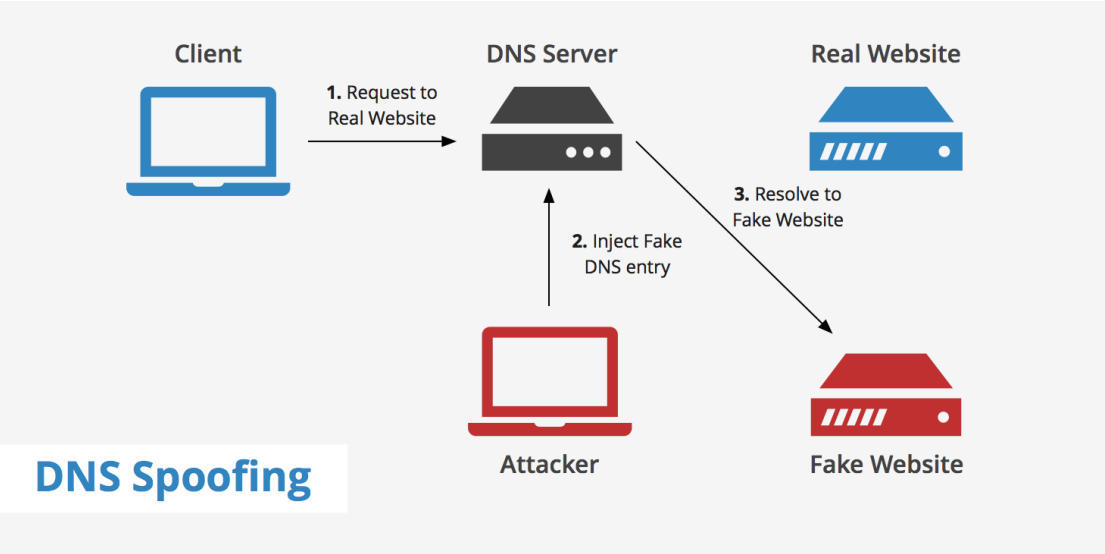


Figure 1 DNS SPOOF

INTRODUCTION

This report will be discussing vulnerabilities on Security in Networks and will mainly focus on the DNS spoofing attacks that exist throughout the network. The port 53 runs the Domain Name Server (DNS) service, however it is considered as the hackers first option to attack this refers to the importance of the DNS service as it is the heart of the internet infrastructure. DNS is the way the internet domain names are located and translated to Internet Protocol address, as domain names are meaningful and easy to remember by internet users.

Less than a month after the hack of United States Central Command (USCENTCOM or CENTCOM) Twitter and YouTube accounts, the hacker group that claimed responsibility for it has redirected visitors of the Malaysia Airlines (MAS) official website on Monday, January 26 to another site displaying the following (TrendMicro, n.d.):

404 - Plane Not Found
Hacked by Cyber Caliphate

Website owners are put in the limelight in cases of DNS spoofing and defacement such as this, even as the technical glitches or vulnerabilities was on the side of the service provider. As such, one proactive practice is to thoroughly research which service provider to trust. Website owners need to look into the

security measures observed by these providers when packaging web hosting services. They should also probe into the track record of potential providers, taking note to see how agile and accurate they are in cases of anomalies in the website (TrendMicro, n.d.).

MAS confirms that "its Domain Name System (DNS) has been compromised where users are re-directed to a hacker website when www.malaysiaairlines.com URL is keyed in" in a statement released on January 26 in its Facebook account January 26, 2015 (TrendMicro, n.d.)

AIM

The aim of this coursework is to demonstrate what an attack called DNS spoofing is and how we can prevent it so that we can maintain Security in Networks

OBJECTIVES

The main objectives are:

- To spread the dangers about DNS spoofing attacks
- To be clear about DNS Spoofing attack and how it works
- To be able to prevent any loss from such attacks by understanding preventive measures

ATTACK SCENARIO

DNS SPOOF ATTACK PROGRESSION

The initial aim of our attack is to successfully spoof a DNS response to a Windows 10 test machine under our control. Our initial attack will be very specific given the amount of knowledge we have about our own machine. Once a successful attack has been developed, the attack will be generalised to increase the likelihood of success against a foreign client. This process will also investigate how the Windows 10 DNS resolver matches responses to queries.

DNS spoofing occurs when a particular DNS server's records of "spoofed" or altered maliciously to **redirect traffic to the attacker**. This redirection of traffic allows the attacker to spread malware, steal data, etc. For example, if a DNS record is spoofed, then the attacker can manage to redirect all the traffic that relied on the correct DNS record to visit a fake website that the attacker has created to resemble the real site or a different site completely.

In this scenario, we will explore the use of the DNS spoofing attack in a typical corporate environment. Both the attacker, victim and DNS server are located on the LAN.

(Fund, n.d.)

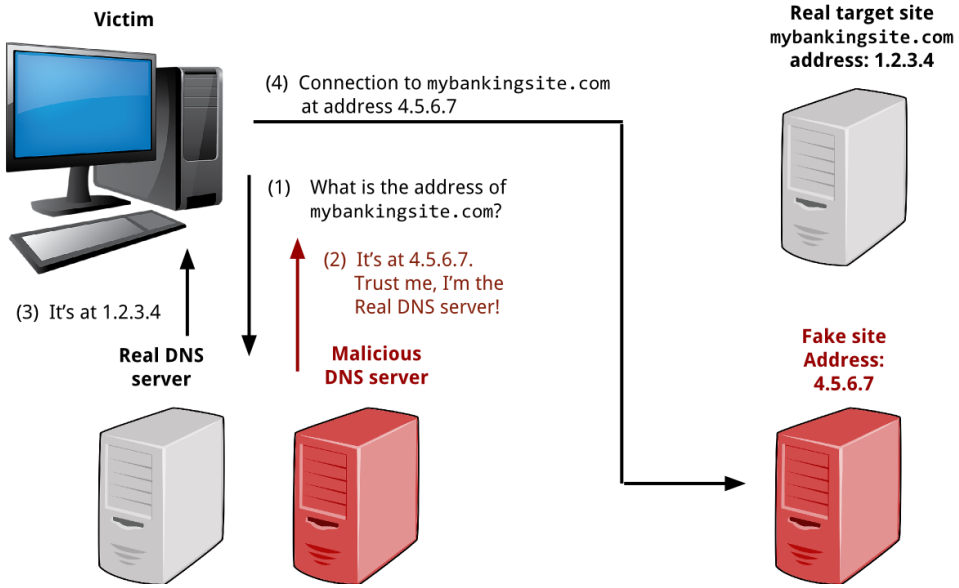


Figure 2 Attack Scenario

PROBLEM SCENARIO

In the year 2000, RSA Security, an Internet security firm, was the victim of a defaced web site. RSA Security is a major player in the security industry, so it was quite surprising to hear that their network was vulnerable to something like a web defacement attack (Fiore & Fran, n.d.).

The DNS hijacker rerouted RSA visitors to another URL that looked like the RSA site. The attacker created a fake web page and then redirected web traffic to that fake page by manipulating DNS IP addresses away from the real RSA Security. When site visitors saw the spoofed home page, they assumed that an intruder had cracked the real RSA Security web site (Fiore & Fran, n.d.).

When DNS is compromised, several things can happen. However, compromised DNS servers are often used by attackers one of two ways.

The first thing an attacker can do is redirect all incoming traffic to a server of their choosing. This enables them to launch additional attacks, or collect traffic logs that contain sensitive information. (Ragan, n.d.)

The second thing an attacker can do is capture all in-bound email. More importantly, this second option also allows the attacker to send email on their behalf, using the victim organization's domain and cashing-in on their positive reputation. Making things worse, attackers could also opt for a third option, which is doing both of those things (Ragan, n.d.).

BACKGROUND

PRE-REQUIREMENTS AND TOOLS

REQUIREMENTS

This attack requires us to know to how to work with basic Kali Linux and the command line.

- **Kali Linux**: Its a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

TOOLS USED ON KALI LINUX

Kali Linux is an operating system developed by linus which includes all the penetration testing application in one single package

Applications required that are included in Kali Linux

- **ETTERCAP**

STEPS INVOLVED

Step 1 (Configuration) : First we need to edit the Ettercap configuration file since it is our application of choice for today. Let's navigate to /etc/ettercap/etter.conf and open the file with a text editor like gedit and edit the file. We can use Terminal for that.

Step 2 (Using Ettercap): Then we run Ettercap to basically sniff the live connection and traffic while filtering the content to find out target and make ready for the next step.

Step 3 (Setting Up EtterCap): First we edit another file in the Ettercap folder i.e . This etter.dns file is the hosts file and is responsible for redirecting specific DNS requests. Basically, if the target enters facebook.com they will be redirected to Facebook's website, but this file can change all of that.

Step 4 (Redirecting Traffic) : Redirect traffic from any website you would like to your Kali machine. We basically change the IP address of the websites to our Kali's IP address. Then we start Apache Service to accept the incoming traffic.

Step 5 (Setting Up Fake Website): The html file in the location **/var/www/html** is where we will find the **index.html** page which is needed to setup to look like the website which we are spoofing.

Step 6 (Finalising Attack): The final thing left to do here is to start the attack. Go back to Ettercap and select **Start** > **Start sniffing** and that should do it.

DEMONSTRATION

The current scenario is as follows Two system are connected on a LAN . **Kali linux** and **Windows 10**

The system **Kali** Linux has IP address **192.168.153.135** The system **Windows 10** has IP address 192.168.153.140 and we have the same default gateway that is **192.168.153.2.**

In this scenario the attacker knows the IP of the victim and is connected in the LAN so that the attack can be performed easily

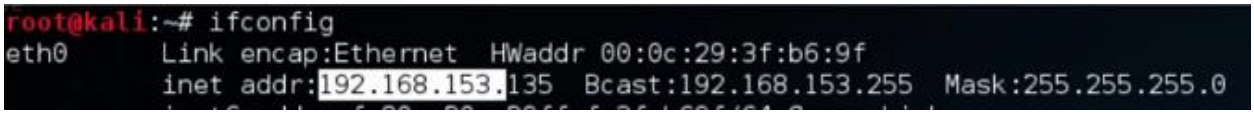


Figure 3 Kali IP address

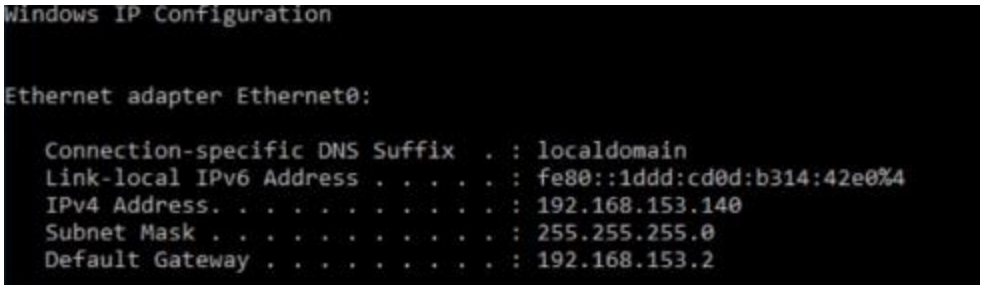


Figure 4 Windows 10 ip addresss

CONFIGURING ETTERCAP

We now need to edit the Ettercap configuration file since it is our application of choice. Let's navigate to **/etc/ettercap/etter.conf** and open the file with a text editor like gedit and edit the file. We can use Terminal for that.

Figure 5 Configuring Ettercap

So now we want to edit the **uid** and **gid** values at the top to make them say **0** so go ahead and do that.:

```
#  (at your option) any later version.                                  #
#                                                                       #
#                                                                       #
#########################################################################

[privs]
ec_uid = 0                # nobody is the default
ec_gid = 0                # nobody is the default

[mitm]
arp_storm_delay = 10          # milliseconds
arp_poison_smart = 0          # boolean
arp_poison_warm_up = 1        # seconds
arp_poison_delay = 10         # seconds
arp_poison_icmp = 1           # boolean
arp_poison_reply = 1          # boolean
arp_poison_request = 0        # boolean
arp_poison_equal_mac = 1      # boolean
dhcp_lease_time = 1800        # seconds
port_steal_delay = 10         # seconds
port_steal_send_delay = 2000  # microseconds
```

Figure 6 Uid and Gid to 0

Now scroll down until you find the heading that says **Linux** and under that remove both the # signs below where it says "if you use iptables".

```
#--------------
#     Linux
#--------------

# if you use ipchains:
   #redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port
   #redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %por

# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport

#--------------
#    Mac Os X
#--------------

# quick and dirty way:
   #redir_command_on = "ipfw -q add set %set fwd 127.0.0.1,%rport tcp from any
   #redir_command_off = "ipfw -q delete set %set"

# a better solution is to use a script that keeps track of the rules interted
```

Figure 7 Removing the # sign

USING ETTERCAP

We first have to launch the **ETTERCAP** and we will be using **Unified Sniffing** from the **Sniff** menu

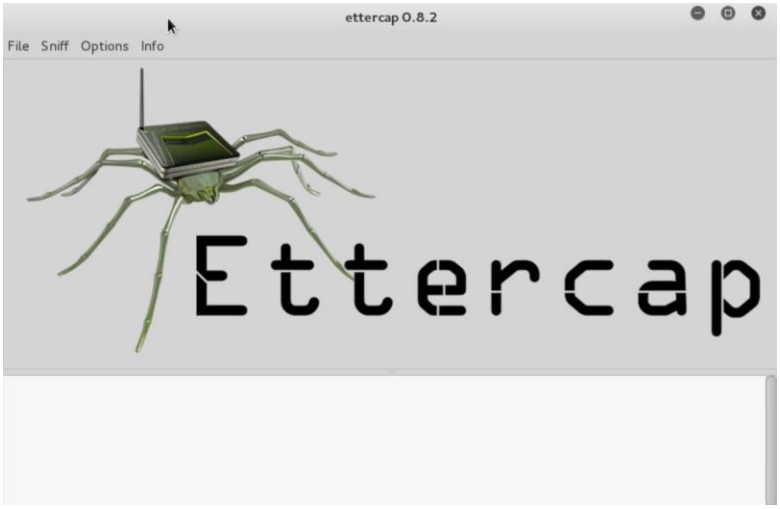


Figure 8 Ettercap

First select **Sniff** > **Unified sniffing**… > (Select the interface connected to the internet) > **OK**

Then swiftly do **Start** > **Stop sniffing** because it automatically starts sniffing after we press **OK** and we don't want that.

Now we want to scan for targets on our network and pick one. To do this, we go to **Hosts** > **Scan for hosts** and wait until it does the scan. It should only take a few seconds depending on the size of our network

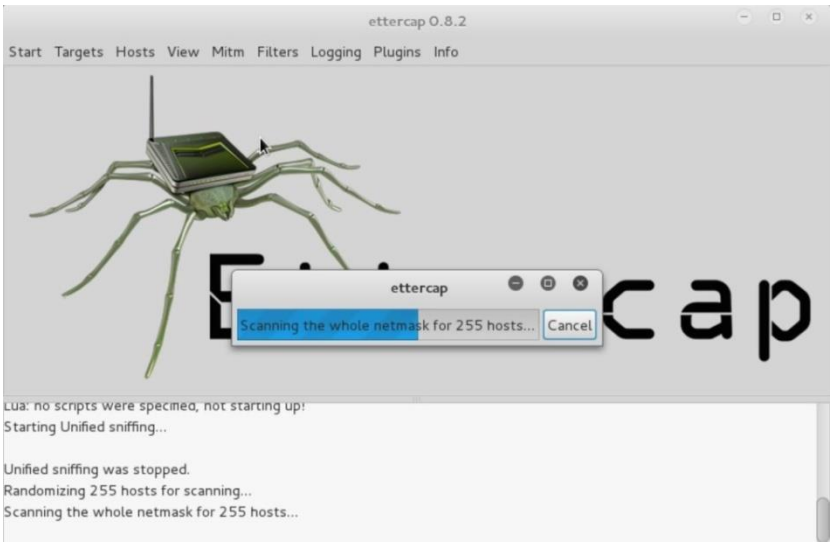


Figure 9 Ettercap Scanning

We'll, go back to **Hosts** and select **Host list** to see all the targets that Ettercap has found.

Now what we want to do is add our **victim machine** to **Target 1** and our **network gateway** to **Target 2** since we know both of their IP addresses.

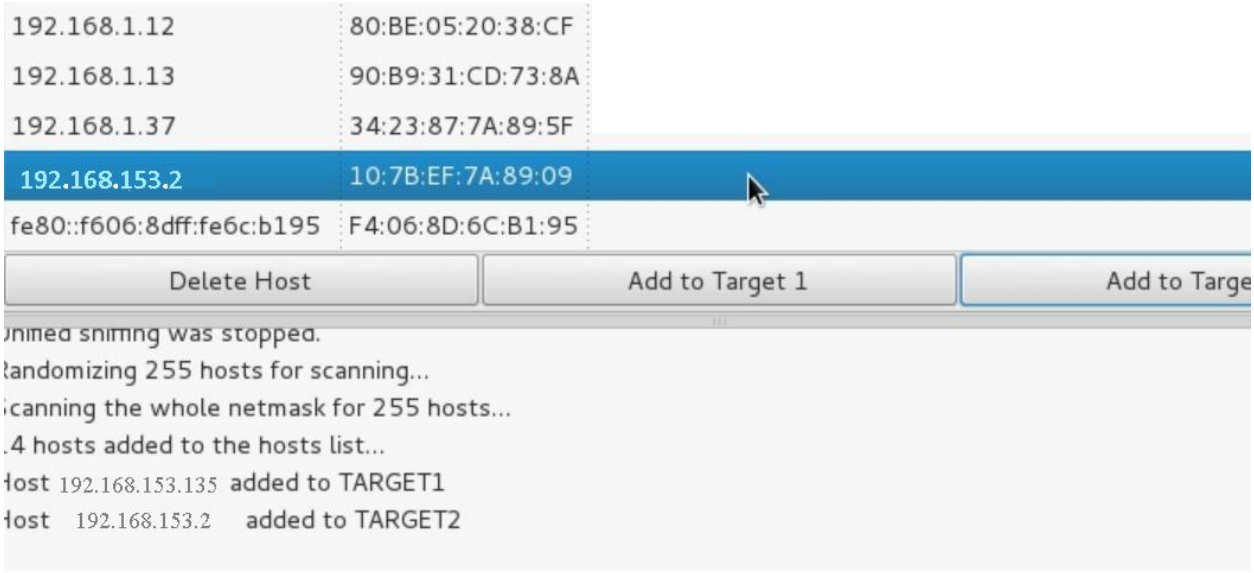


Figure 10 Targeting Victin

SETTING UP ETTERCAP

Go to the **MITM** tab and select **ARP poisoning**, choose **Sniff remote connections** and press **OK**. Now go to **Plugins** > **Manage the plugins** and double click **dns_spoof** to activate that plugin.

We now need to edit another file in the Ettercap folder.

Figure 11 Editing etter.dns

This **etter.dns** file is the hosts file and is responsible for redirecting specific DNS requests. Basically, if the target enters facebook.com they will be redirected to Facebook's website, but this file can change all of that.

Figure 12 Traffc redirecting

```
#                                                                              #
# or for TXT query (value must be wrapped in double quotes):                   #
#    google.com TXT "v=spf1 ip4:192.168.0.3/32 ~all"                           #
#                                                                              #
# NOTE: the wildcarded hosts can't be used to poison the PTR requests          #
#       so if you want to reverse poison you have to specify a plain           #
#       host. (look at the www.microsoft.com example)                          #
#                                                                              #
################################################################################

###############################
# microsoft sucks ;)
# redirect it to www.linux.org
#

microsoft.com      A   107.170.40.56
*.microsoft.com    A   107.170.40.56
www.microsoft.com  PTR 107.170.40.56      # Wildcards in PTR are not allowed
facebook.com       A   192 . 168 . 153.135
*.facebook.com     A   192 . 168 . 153.135

#########################################
# no one out there can have our domains...
#

www.alor.org  A 127.0.0.1
www.naga.org  A 127.0.0.1
www.naga.org  AAAA 2001:db8::2

#########################################
# dual stack enabled hosts does not make life easy
# force them back to single stack

www.ietf.org   A    127.0.0.1
www.ietf.org   AAAA ::

www.example.org  A    0.0.0.0
www.example.org  AAAA ::1
```

Figure 13 Etter.dns

Now we need to start Apache to accept incoming traffic.

```
root@Kali:~# service apache2 start
```

Figure 14 Starting apache server

SETTING UP FAKE WEBSITE

The html file in the location **/var/www/html** is where we will find the **index.html** page which is needed to setup to look like the website which we are spoofing.

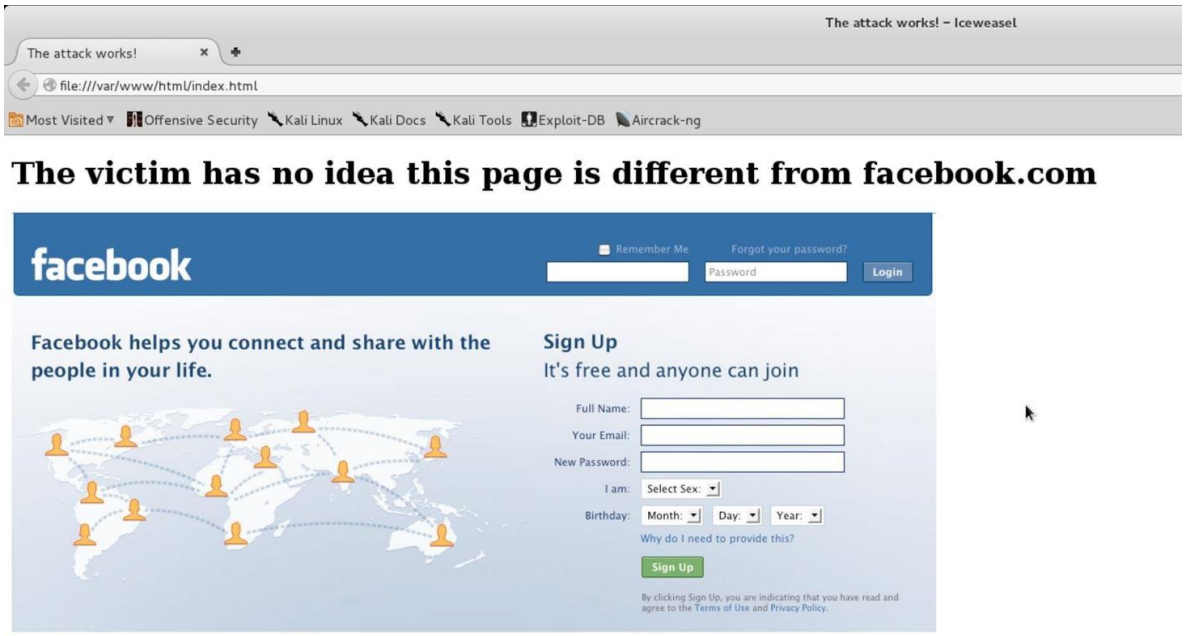


Figure 15 Fake Facebook

The final thing left to do here is to start the attack. Go back to Ettercap and select **Start** > **Start sniffing** and that should do it.

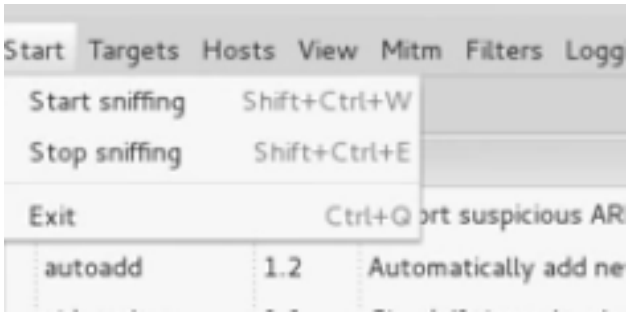


Figure 16 Started Sniffing

Now on **windows 10** if we go to the website facebook.com

Figure 17 Victim redirected to fake website

PREVENTION AND RECOMMENDATIONS:

Many cache poisoning attacks against DNS servers can be prevented by being less trusting of the information passed to them by other DNS servers, and ignoring any DNS records passed back which are not directly relevant to the query.

There are some consideration that will help to prevent DNS spoofing:

- **Implement DNS spoofing detection mechanisms** – it's necessary to implement DNS spoofing detection computer code. product like XArp facilitate product against arp cache poisoning by inspecting the info that comes through before transmitting it (Keycdn, n.d.).

- **Use encrypted data transfer protocols** – Using end-to-end encryption via SSL/TLS will help decrease the chance that a website / its visitors are compromised by DNS spoofing. This type of encryption allows the users to verify whether the server's digital certificate is valid and belongs to the website's expected owner (Keycdn, n.d.).

- **Use DNSSEC** – DNSSEC, or Domain Name System Security Extensions, uses digitally signed DNS records to help determine data authenticity. DNSSEC is still a work in progress as far as deployment goes, however was implement in the Internet root level in 2010. An example of a DNS service that fully supports DNSSEC is Google's Public DNS (Keycdn, n.d.).

DEMONSTRATION

MANUALLY CHECKING ARP CACHE ON REGUALAR BASIS.

STEPS INVOLVED

Step 1 (Configuration) : First we need to note down the Mac Address of the Default Gateway (i.e our router) and keep checking the ARP cache

Step 2 (Terminal): To check the ARP cache, go to the Terminal and type **arp -a** and you will see several entries like this:

Figure 18 Preventing

USING SOME EXISTING SOFTWARES

There are some softwares which exist for detection of ARP poisioning detection which provide and alternative for checking the arp command manually on a regular basis.

1. **XArp**

A GUI advanced ARP spoofing detection and active probing software. It is designed for this kind of job and works on both Windows and Linux (configurable for OS X as well).

2. **Snort**

You most probably know Snort for its IDS amazingness, but I'm sure you haven't heard that it also detects ARP spoofing (you may have).

3. **ArpON**

This is a portable handler daemon for securing ARP against spoofing and cache poisoning.

CONCLUSION

According the report the DNS Spoofing attack is a huge threat with much vulnerability which is difficult to deal. It can access the network and victims within the network by running some of the command and sniff the data that is transferring in network through victims and default gateway.

Since we cannot eliminate the DNS spoofing attack completely we can try to minimize the possibilities of this attack onto the network. Some of these security measures include host hardening i.e. operating systems onto the network should be upgraded, network designing from security point of view, network devices and the computers onto the network should be updated periodically and the patches should be installed regularly.

REFFERENCES

Anon., 2017. *cisco*. [Online] Available at: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html.

Anon., 2017. *keycdn*. [Online] Available at: https://www.keycdn.com/support/dns-spoofing/.

Anon., 2017. *Networks*. [Online] Available at: http://www.valencynetworks.com/articles/cyber-attacks-explained-man-in-the-middle-attack.html.

Cisco, 2017. *ARP Poisoning Attack and Mitigation Techniques - Cisco*. [Online] Available at: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html.

club, 2017. *club*. [Online] Available at: http://www.thewindowsclub.com/man-in-the-middle-attack.

Fernandez, C., 2016. *Youtube channel*. [Online] Available at: https://www.youtube.com/watch?v=bEMwES6TQUw.

Finley, D.R., 2011. *http://alienryderflex.com*. [Online] Available at: http://alienryderflex.com/man_in_the_middle/.

Fiore, F. & Fran, J., n.d. *http://www.informit.com/*. [Online] Available at: http://www.informit.com/articles/article.aspx?p=29015&seqNum=2.

Fund, F., n.d. *witestlab.poly.edu*. [Online] Available at: https://witestlab.poly.edu/blog/redirect-traffic-to-a-wrong-or-fake-site-with-dns-spoofing-on-a-lan/.

Huang, X., 2010. *IEEE*. [Online] Available at: http://0-ieeexplore.ieee.org.emu.londonmet.ac.uk/xpls/icp.jsp?arnumber=5635945.

INCAPSULA, n.d. *www.incapsula.com*. [Online] Available at: https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html.

Keycdn, n.d. *keycdn.com*. [Online] Available at: https://cdn.keycdn.com/support/wp-content/uploads/2017/02/dns-spoofing.png.

Khanse, A., 2016. *TheWindowsClub*. [Online] Available at: http://www.thewindowsclub.com/man-in-the-middle-attack.

MICE, M.&., 2017. *DNS Spoofing | Men & Mice*. [Online] Available at: https://www.menandmice.com/resources/dns-spoofing/.

Networks, V., 2017. *Article : Cyber Attacks Explained: Man In The Middle : Ethical Hacking, Pen Test Pune,India - Valency Networks*. [Online] Available at: http://www.valencynetworks.com/articles/cyber-attacks-explained-man-in-the-middle-attack.html.

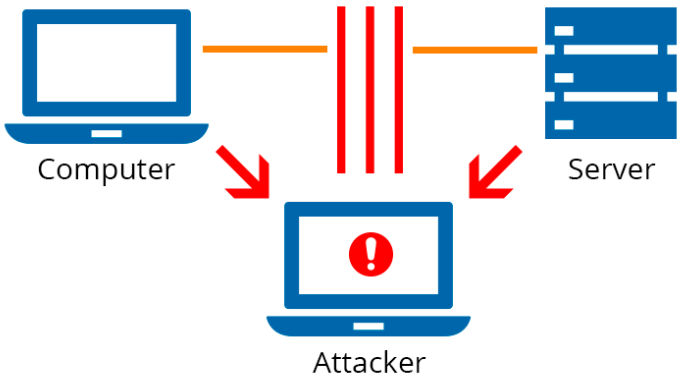
Ragan, S., n.d. *https://www.csoonline.com*. [Online] Available at: https://www.csoonline.com/article/2133916/malware-cybercrime/three-types-of-dns-attacks-and-how-to-deal-with-them.html.

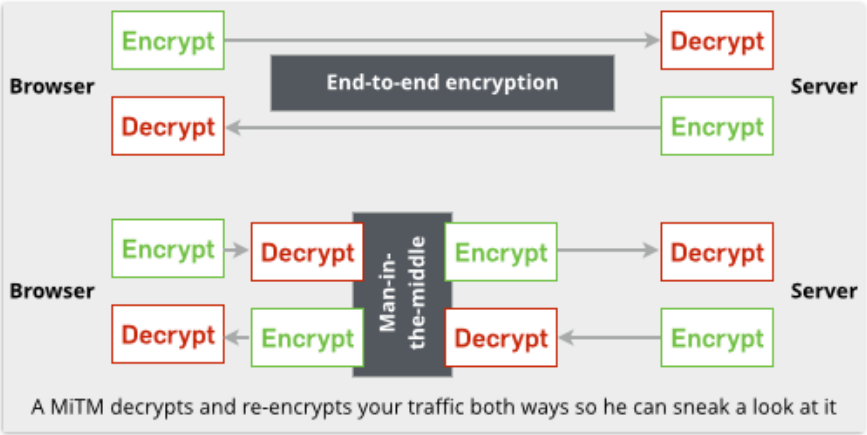
Seung Yeob Nam, D.K.J.K., 2010. *IEEE Communications Letters*. [Online] Available at: http://0-ieeexplore.ieee.org.emu.londonmet.ac.uk/document/5403629/.

Technologies, C., 2017. *Ca Technologies*. [Online] Available at: https://www.veracode.com/security/man-middle-attack.

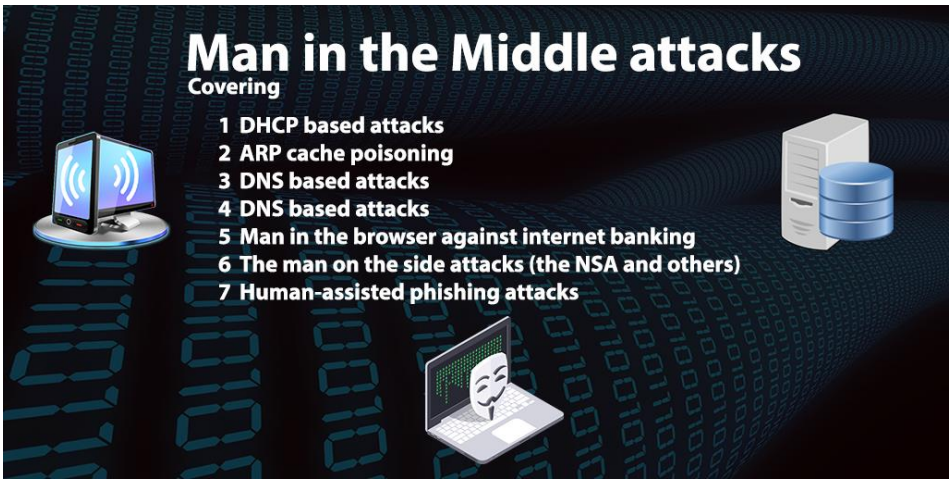
TrendMicro, n.d. *https://www.trendmicro.com/*. [Online] Available at: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/hacked-or-spoofed-digging-into-the-malaysia-airlines-website-compromise.

APPENDICES






FREE
WI-FI
Just
don't
mind
me!


Man in the Middle attacks
Covering
1 DHCP based attacks
2 ARP cache poisoning
3 DNS based attacks
4 DNS based attacks
5 Man in the browser against internet banking
6 The man on the side attacks (the NSA and others)
7 Human-assisted phishing attacks