Penetration Testing Lab

IST 451: Network Security

PENNSTATE

Creators/Authors

Brad Witmer - brw5171

Table of Contents

Introduction

Penetration testing is the evaluation of an IT infrastructure's security by trying to expose potential vulnerabilities within a predisposed window of limitation. A pen test helps assess the overall quality of an employing entity's equipment/resource security through the attempt of gaining access to an entity's resources without normal means of access. For example: a bank may employ a security firm to implement a penetration test trying to exploit their security through gaining access to their employee information without actually using the information against the bank; the security firm will close out the attack with a report of the bank's security, providing information on weak and strong points within the IT infrastructure. The difference between the penetration testing and a real hack attack is permission by the entity that owns the IT infrastructure. An important part of this practice in network security is that the employed firm performing the penetration tests is keeping a detailed record about how the tests were performed, which vulnerabilities were found, and where the strength points were. The compromise points that the performers of the penetration test focuses on are: "servers, endpoints, web applications, wireless networks, network devices, mobile devices and other points of exposure" (Core).

Kevin Mitnick, author of *The Art of Intrusion,* wrote

"Companies spend millions of dollars on

firewalls, encryption and secure access devices,

and it's money wasted, because none of these measures address the weakest link in the security chain."

Objectives

In this lab exercise, you will complete the following tasks:

- Use OpenPuff to successfully send hidden data
- Hide a .txt file within a .mp3 file
- Use the LAN Messenger Application to secretly transmit the file to another computer

Visual of Lab

Task 1: Information Gathering

Step 1 Boot onto your penetration testing machine and log into the administrator account

Step 2 Make sure that the target machine is also booted up, if not boot the device up

Step 3 On the target machine, open a terminal window and type the command ipconfig

Step 4 When the download has completed, open the zip and find the OpenPuff.exe file, click this and

Step 5 Now from the Windows Start Panel open up Notepad and create a text file

a. Write down any message that you want to secretly send to another user

b. From the menu bar click "Save As"

c. For the sake of this lab we will name this file "secret" (no quotes) to help us remember that this will be the file we hide within our carrier file

d. Set the save destination as the desktop

e. Make sure the file is going to be saved with a .txt extension and click "Save"

Locate the provided .mp3 or .jpeg carrier file

Task 2: Setting up the Message's Cryptographic Parameters

Step 1 Now that the lab environment is setup it is time to begin hiding the secret.txt file within the

Step 2 With OpenPuff up and running select "Hide" from the main menu

Step 3 Deselect the check boxes "B" and "C"

Step 4 Now look over to the "(2)Data Max" section of the page and select "Browse", from their a

Step 5 From the Windows file browser find and select your message "secret.txt" file

Step 6 The application will respond to these changes by outputting the size of the file

Step 7 Now look over to the *"(3)Carrier Selection"* section of the page and select browse

Step 8 From the Windows file browser find and select your carrier file

Step 9 Look over to the "(4) Bit selection options" portion of the page and make sure that you take note

Step 10 Finally click the "Hide Data!" button and select a destination for the generated file to go

Task 3: Sending the Secret Message

Step 1 Open up the Lan Messenger Application (to do this go to the task bar on and right click on the

Step 2 Locate the contact that you wish to send the message to. (For this example we will be selecting

Step 3 Once the conversation window open select "Send a File"

Step 4 Select the carrier file and click send

Task 4: Unhiding the Secret Message

Step 1 Open the application OpenPuff on the receiving machine

Step 2 From the main menu select the "Unhide" button

Step 3 The application will open up the Unhide menu

Step 4 From this menu enter the password that was used to encrypt the carrier message into the password text field

Step 6 Uncheck the check boxes for passwords "B" and "C"

Step 7 Identify the carrier by clicking "Add Carriers" in the carrier selection portion of the page

Step 8 Select the carrier file giving to you from the other user

Step 9 Now find the Bit Options that the sender has given you in the "(3) Bit Options" portion of the page, this is a crucial step in the process

Step 10 Finally click the button "Unhide!"

Step 11 Select a destination for the file that you wish to unhide from the carrier and click "OK"

Step 12 Now find the file from the destination you just specified, it will open the secret message

Further Learning

If you are interested in learning more about Steganography try these.
These tutorials are for **Python**, **Java**, and another **Open Source Tool**:

- https://www.youtube.com/watch?v=q3eOOMx5qoo
- http://www.dreamincode.net/forums/topic/27950-steganography/
- http://null-byte.wonderhowto.com/how-to/hacks-mr-robot-hide-data-audio-files-0164136/

Additional Tools

These are some of the best tools to perform steganography:

- **Image Steganography** - http://imagesteganography.codeplex.com/
- **StegHide** - http://sourceforge.net/projects/steghide/files/
- **Cryture** - http://sourceforge.net/projects/crypture/
- **SteganographX Plus** - http://www.bestfreewaredownload.com/freeware/t-free-steganographx-plus-freeware-yeipgmrk.html
- **rSteg** - http://www.softpedia.com/get/Security/Security-Related/rSteg.shtml

Bibliography

1.Source:

Kessler, Gary C. "Steganography: Hiding Data Within Data." *Steganography*. N.p., n.d. Web. 25 Jan. 2016. <http://www.garykessler.net/library/steganography.html>.

2.Source:

Andrei, Mihai. "Cicada 3301: A Puzzle for the Brightest Minds, Posted by an Unknown, Mysterious Organization." *ZME Science*. N.p., 28 Apr. 2014. Web. 03 Mar. 2016.

<http://www.zmescience.com/other/feature-post/cicada-3301-puzzle-brightest-minds-posted-unknown-mysterious-organizationt/>

3.Source:

Steganography - OpenPuff v3 Demo. EmbeddedSW, 24 Feb. 2014. Online Video.

4.Source

Barker, Keith. "How to Use OpenPuff Steganography to Send Sensitive Info Securely." *Search Security*. N.p., 27 Jan. 2014. Web. 25 Jan. 2016. <http://searchsecurity.techtarget.com/video/How-to-use-OpenPuff-steganography-to-send-sensitive-info-securely>.

5.Source:

"OpenPuff 4.00 - Yet Not Another Steganography SW." *OpenPuff*. Advanced Embedded Solutions, n.d. Web. 04 Mar. 2016. <http://embeddedsw.net/OpenPuff_Steganography_Home.html>

7.Source:

Hussain, Mehdi, and Mureed Hussain. "A Survey of Image Steganography Techniques."*CiteSeerX-A Survey of Image Steganography Techniques*. CiteSeerX, May 2013. Web. 3 Mar. 2016. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.364.3275&rep=rep1&type=pdf.>

8.Source:

Schoen, Seth. "Secret Code in Color Printers Lets Government Track You." *Electronic Frontier Foundation*. N.p., 17 Oct. 2005. Web. 04 Mar. 2016. <https://www.eff.org/press/archives/2005/10/16>.

9.Source:

Shakdhar, Pavitra. "Best Tools to Perform Steganography - InfoSec Resources." InfoSec Resources Best Tools to Perform Steganography Comments. N.p., 08 June 2015. Web. 19 Apr. 2016. <http://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/>.