Concordia Institute for Information System Engineering(CIISE)

INSE 6961 – Graduate Seminar in Information and Systems Engineering

Graduate Seminar Report-1

Udemy Course: Learning Ethical Hacking from Scratch

Section Covered: Gaining Access – Client-Side Attacks – Social Engineering

Total Time covered for this Segment: 120 Mins

Submitted to:

Professor Ayda Basyouni

Submitted By:

Sai Chandra Sekhar Reddy Dwarampudi - 40189233

What is Social Engineering?

The term "social engineering" refers to a wide range of malevolent behaviors carried out through human relationships. Gathering information about the target is the most important task of social engineering. Gather information about the target as much as possible like website the target is searching, the target friends and try to build a strategy based on the gathered information. Finally make the target to run backdoor. Social Engineering is less technical and more about the strategy you are building and usage of the information to attack the target.

Introduction to Maltego:

Maltego is an information gathering tool that can be used to collect information about anything. Target can be anything like website, computer, company discover various entities associated with the entity. It is directly available in kali Linux in the application. Whenever you are logging in for the first time you will be asked for the credentials and activation link to the mail is sent. In the home page you can add more transformers to the tool which are used to gather information which will be asked to use certain API's. In the graph tab on the left side, you can find the entities, the graph, overview about the graph, detailed view, and property view to change the value of a property. Simply drag and drop the entity to the graph workplace you want to add. Personal information like a person's name, phone number and various social links like Facebook, GitHub, Instagram can also be added. The paid version is necessary to get more add-ons like to gather information from the target search engine.

Discovering websites, Links and Social Accounts:

Add a person to the graph and change the entity properties using the property view. Right click on the person and run the transforms like to website using search engine. You will be prompted to look for a specific domain, type space in the text boxes which means no specific domain. After running you will get the websites related to the target person's name. Double click on the Facebook website output, you will get the various profile URLs that are associated with the name. Open the various profiles using the browser and identify the right person URL you want to attack. After continuous checking we have identified an Udemy URL with the right target person we want to attack. In the Udemy website we found the links to various other websites like Facebook, linked-in and YouTube which can be used to go and get more information.

Discovering Twitter Friends and Associated Accounts:

In the Udemy page open the twitter link and, in the graph, add the twitter. Since the twitter entity is not default present to add it to the entity palette go to the manage entity select the twitter entity and drag and drop the twitter entity. Upon double clicking the entity you will various things about the things associated with the person like tweets posted, friends, retweets etc. Our main target is to find his friends. Now Maltego will ask to sign in to twitter and create and use the anonymous account for this purpose. Now we will be able to gather friends of the target. Emails will be sent to the friend's emails directly stating as the email was sent directly from his/her own friend. The person might think it as a genuine email from a friend and get spammed.

Discovering emails of the Targets Friends:

In the personal blog of the target, we found out the email id of the target and which will be added to the graph as an email entity. To get this email just simply run the email module from the website entity and you will get the email associated with it. Now if we run all the email addresses associated with the website, we will be able to get all the friends mail address and any other email addresses who are working for the same website. Now we will try to figure out some attack strategy which we will be going to be performed on the target.

Analyzing the Gathered Info and Building an Attack Strategy:

Try to reorganize the graph so that it will be easy to build an attack strategy. We identified that the target is a teacher at Udemy so we can send some beta program to target saying that it was sent only to the privilege user from the Udemy or some link which creates and UI like Udemy to ask the user to change his password since it was going to be expired and capture the actual password. Looking at the graph we can clearly tell that the target has many connections from isecurity company. We can try to send an email to the target such that it is coming exactly from one of his friends with some attachment of ebook. Now when the target opens the attachment some malicious code from the pdf will run on the target computer which will make us gain access to the target computer.

If nothing above works, we can hack the target friend's social media networks try to send some messages to the target send ultimately hack into the target system. This is the power of Maltego by simply knowing the name of the target we will be able to access such a huge amount of information.

Backdooring and Compiling any File Type

First, we must create a script which is sent to the target to open and in which we have the URLs we want the target to download like the backdoor file. Every file should be online and should contains and URL since the target should be able to download. Every URL should be separated by a comma. Change the file type from pdf to au3 and use the AutoIT code compiling software to compile the script. Choose the created script in the file and try to change the icon by downloading the icon you want to have using the IconArchive website. Download the icon and add the icon file in the AutoIT and just simply press convert, an executable file will be generated.

Spoofing .exe Extension to Any Extension:

Now we have created a file as per our analysis from the graph that the target is interested in. The main problem is that is file is ending with .exe extension. In most cases the windows operating system will not show the .exe extension but to make sure that the file is not sent with .exe extension which will make the target not to open the file we need to change the .exe extension to .jpg which is done through spoofing. If we simply rename the file by removing the extension to jpg the executable file will not work. So, we just simply add right to left override character before the reverse of the string that we want to read from right to left. For example, if we want the .jpg as extension to and gtr.exe file we just add the reverse of jpg which id gpj after gtr which becomes

gtrgpj.exe. The right to left override character is added at the starting of the second g so when properly read it will become gtrexe.jpg.

Some Brower's remove right to left overwrite while transferring the file. To eliminate this problem just simply archives before sending it to the browser. So now if we download the image from the browser and uncompressed it and open it, a backdoor and a reverse session will be created from the target machine to the Linux machine which we are using.

Spoofing Emails – Setting Up and SMTP Server:

Now that we understand how the trojan works and how it affects the target, we must consider how we should get it to the intended recipient. One of the best methods to do it is through the mail. The information we obtained at the beginning helps us locate the targeting person's mail as well as the mail of friends or coworkers. It might be a friend, a website, or an organization associated with the target. Based on the facts we obtained, we can continue in any of these ways. We can send fake emails using several web services.

Furthermore, because browsers have already detected them as spammers via servers, email sent through them ends up as spam, which is not what we want. Consequently, the SMTP Server is summoned to resolve the issue. This may be accomplished by employing sites that offer SMTP Server service. Sendinblue, for example, has a free plan.

Email Spoofing - Sending Emails as Any Email Account:

To send a false email, we must validate the transactional data (Username, Password, SMTP Server, Port) with the SMTP Server. We use the 'sendemail' application and a few Kali commands. The -xu and -xp options specify the username and password, respectively. The packed executable file may be uploaded to Google Drive or Dropbox, and an email with a link to download it can be sent.

Detecting Trojans Manually and Using a Sandbox:

The first thing to identify a trojan is to check the properties of the file just simply right click and check the properties. It will display the file type as an application instead of jpg. The second method to crack the trojan is to change the name of the downloaded file, change the name to identify the file type. In the resource tab you can identify all the open ports and the IP and ports on which the application is running. Just simply identify the IP that your malicious application was running on and try to search whether the IP is really a genuine website or not. If it is anyone personal computer, you will not be able to reach the IP. You can also do a reverse DNS lookup using the IP, it will tell you what website and which domain the IP belongs to.

Another way to detect the malicious files is to use sandbox. It is a place where the file will be executed to identify the ports to be opening, modify the registry entries or any other suspicious activities. It runs the scan, determines the file type and gives the report. Just go to the hybrid-analysis.com and select the file. In the network analysis part of the report, we can identify the IP addresses to which the application is being connected and to which port. We can simply do the reverse DNS for the above IP addresses. The file will be completely executed on a different server not on the local system.

Reference: https://concordia.udemy.com/course/learn-ethical-hacking-from-scratch/learn/lecture/5308842#overview

Course Instructor: Zaid Sahib (Ethical Hacker, Computer Scientist and CEO of zSecurity)