Concordia Institute for Information System Engineering
(CIISE)

Concordia University

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:

Nithish Reddy Yalaka – 40164619

Social Engineering:

What is Social Engineering?

Exploiting human flaws to get access to personal information and secure systems is known as social engineering. Instead of hacking computer systems to get access to a target's account, social engineering depends on manipulating individuals. Social engineering is used by criminals since it is usually easier to exploit your natural tendency to trust than it is to figure out how to hack your system.

A social engineer's purpose is to deceive someone into providing important information or access to it. In the vast majority of cases, the attacker never sees the victim, but they nearly always gain the information or access they need to accomplish fraud. Some of the types of Social Engineering attacks are Phishing, pretexting, baiting, vishing, Spear Phishing, tailgating, Scareware, Quid Pro Quo, and piggybacking.

Maltego, an Information Gathering Tool

For this, we have a tool called MALTEGO. The type of information we're looking for can be anything from living to non-living. This tool is accessible for download and usage on our respective systems via the internet. It prompts us to log in with the username and password once we've installed it on our PC (if we have one). Otherwise, we must first register before utilizing it. As soon as we log in, a popup appears with pre-existing templates for collecting data. We can use any of them or dismiss the popup. Then we visit Maltego's homepage, which has a number of plugins that assist us collect information about the target and even allows us to add more.

We have a plus option on the top left of the screen to acquire a new graph when we go to Maltego's primary workplace. The graph is essentially where the data is shown and on the right side of the graph, we have an overview, a detail view, and properties windows. Details about the object that aren't visible in the main graph window are displayed in the detail view. We also have an entity palette to the left of it, which groups entities into categories based on their type. The required entity must be dragged and dropped onto the graph. We may also replace the default properties with the relevant properties to begin collecting data. After gathering information, the next step is to devise an offensive strategy. So, before we proceed, we must first gather sufficient data as information gathering is the primary and most important task of any social engineering attacks.

Maltego, Hands ‘on:

To get a feel for this tool, let's look at an example. In the event that we need to gather information about a person based on their name. In the personal category in the entity palette on the left of the graph window, we have an entity named person that can be utilized for this purpose. By double-clicking at the desired location after it's been dragged onto the graph, we may replace the default properties (Full name, First name, and Surname) with the target properties. When we're finished, right-click on the object and select the paterva category, we'll see a list of transforms to run based on the data we want to collect. We may use the 'To Website' transform to acquire the websites related with the target name. When we choose that option, it prompts us to enter a domain name and, if we don't have one, to replace it with a space. In this approach, we can find all of the

websites that are linked to the target name we've specified. We can do same technique with websites associated with the name like Twitter, LinkedIn, Facebook, udemy.com, YouTube, and have to verify and check which of these websites exactly are the target users.

Discovering Twitter Friends & Associated Friends using Maltego:

Let's pretend we found the target person's Twitter account and email address while perusing the web. To explore what we can pull out of Twitter, we'll need to drag and drop the Twitter item from the palette's social network category. The palette did not contain all of the entities. When we go to entities at the top and then manage entities, we may find some of them. We can discover the Twitter entity there, and we can click the checkbox next to the palette in advance settings to find it on the entity palette. We can now drag and drop it onto the graph, replacing the default values with the target properties we saw via the Twitter account link, such as Name, Link, and Username. Now, if we right-click on the entity and select Transforms, we can view the many data points that may be gathered from that Twitter account. We can reach out to the target's Twitter followers to see if they can help us compile the data. Now, as we can see the friends and useful information about the victim via Maltego, there is a very high chance of the victim responding to actions when the attackers pretending to be his friend or the website he often follows.

Discovering Emails of the Target's Friends:

Next, we can drag and drop the email address entity into the personal category of the entity palette, replacing the default properties with the data of the target individual. We can acquire websites associated with the email, and in turn, we can find emails related to the website, using the same approach we used for Twitter. This manner, if we have anything in common, such as work colleagues, we can get information that ties to the information we got on Twitter. By doing so, we got all the information that is enough to build a strong attack strategy on the target.

Analyzing the Information Collected in Order to Formulate an Attack Strategy:

Now is the time to remove any entities that are no longer useful and correlate the information we obtained from Twitter with the target person's email address. It is time to match the dots that was obtained in the previous steps by matching the email ids and people we found and relate them according to name, email and organization for better understanding and strategy. We can also target and hack their friends account and try directly reach out to the main victim. If the Target's friend is not security oriented and knowledgeable it'll be very easy to manipulate them.

Spoofing an .exe extension into a Zip file:

The file we wanted as a trojan was ready, but it has a.exe extension, indicating that it is an executable file to the target person. The.exe file will no longer function as an executable file if we rename it with the required file extension. We need to spoof it in order to replace it with the desired extension (the extension of the content in it, such as.jpg or.png in the event of an image or.pdf in the case of a pdf, etc.) and make it work like an executable file. We'll need to utilize the right-to-left override character for this. As a result, whenever we

insert that character, everything that follows it is read from right to left. On the system, we'll require a character's application. We'll be able to copy and paste a right to left override character from it when we open it and search for one in our case, we are renaming it. We convert the file to a zip and deliver it to the target individual because few browsers recognize this character. When the target person extracts the zip file, it functions exactly as it did previously. We can spoof the.exe extension with the appropriate extension this way.

Spoofing Emails - Setting Up an SMTP Server:

Now it is clear that how the trojan works and how exactly it works on target , but now we need to see how we should send it to the target individual. The mail is one of the greatest ways to convey it. The information we gathered at the start aids us in locating the target person's mail as well as the mail of friends or colleagues. It could be posing as a buddy, a website, or an organization connected to the target. We can proceed in any of these ways based on the information we gathered. We can send bogus emails using a variety of online sites. Even so, because the browsers have already identified them as spammers through servers, the mail sent through them ends up in spam, which is not what we want. As a result, the SMTP Server is brought in to solve the problem. We can accomplish this by utilizing sites that provide SMTP Server service. Sendinblue is one such platform that offers a free plan.

Email Spoofing - Sending Emails as Any Email Account:

Now that we have a free smtp server as Sendinblue, we need to validate the transactional data (Username, Password, SMTP Server, Port) with the SMTP Server to send a false mail, so we register. We utilize the 'sendemail' software and a few commands in Kali. -xu specifies the username and -xp specifies the password. -s to specify the server, followed by a port separated by a colon, -f to specify the email address from which we want to send the email, -t to identify the email address to which we want to send the email, -u to specify the title, -m to define the email content, and a message header. The packaged executable file can be posted to Google Drive or Dropbox, and the link to download it can be sent via email.

Email Spoofing Using Web Hosting:

Web hosting can also be used to send fake emails. We can opt for cheap web hosting providers to get start going. Once we have a web hosting account, we can upload the 'send.php' file by renaming it and from the resources folder to the website's file management, and by adding the extension /send.php to the link, we will be able to send an email to the target person just like we did with the SMTP Server. Make the necessary changes to the from email account, name field and test it beforehand. Spoofing emails can be done using either of the two approaches, we can use this if other one's doesn't give us the required outputs.

References:

https://concordia.udemy.com/course/learn-ethical-hacking-from-scratch/learn/lecture/5369454#overview

Instructor : Zaid Sabih