Project 1: Network Security Spring 2022

Due: February 22, 2022

February 11, 2022

Problem 1: Breaking 2 FA With MITM Attack [50 Points]

In this project we will implement the attack for breaking two factor authentication. At the end of this project we will be able to successfully execute a man-in-the-middle (MITM) attack for stealing username and password while at the same time bypassing any software based 2FA. We will use Evilginx (interested people please read about the implementation of Evilginx here: (`https://breakdev.org/evilginx-advanced-phishing-with-two-factor-authentication-bypass/`), which implements a phishing 2.0 framework for bypassing 2FA using a MITM attack (which was discussed in class). Evilginx provides a way to create phished webpages that can be used as landing pages for launching the attacks and also provides a way to create certificates for use in creating the HTTPS connection between the victim computer and the attacker machine. The project will involve the following steps:

- Each team will create an account on Reddit or LinkedIn or Twitter (or any other service supported by Evilginx see `https://github.com/kgretzky/evilginx2`). The account should have a username and a non-trivial password and should also have 2FA enabled. I would recommend creating a Reddit account as it is easier to create and operate. The team would then create and use a phishing link targeting the service selected (I will assume Reddit for the rest of the description).

- Upon clicking the phishing link, the user should be taken to the landing page which is created using Evilginx phishlets. The landing page will be the login page where the user will enter the username and password. This information exchange will happen over a HTTPS link. Evilginx enables the creation and use of the certificates required for creating the secure connection. After the username and password is created, the information is sent to the attacker machine where it can be read by the attacker. The attacker relays this information to the actual Reddit server, where the real authentication takes place and since 2FA has been enabled by the user, Reddit presents the user with the 2FA page and waits for the 2FA

information to be entered. The attacker intercepts this page and sends the same to the user.

- After the user enters the 2FA information, it is relayed by the attacker to Reddit servers where the final step of the authentication happens and the user is logged in. In response, the server sends the user a session cookie (which is intercepted by the attacker) and sends the user to the main Reddit landing page. The attacker, at this point intercepts the page and the cookie and sends the page to the user and stores the cookie.

- Finally the cookie is used by the attacker on a browser window to login to the user account and take over the account. Note that at this point the connection with the user can be broken as there is no need to keep the user logged in. In fact if the attacker changes the password of the user's account, they will be immediately logged out and locked out of the account with no further recourse to fix the problem.

Notes: In order to do this attack you will need to create a Reddit (or another service) account. Please do not use your personal account for this attack. The reddit account should be of the form cs465-xxxx where xxxx can be anything that you choose. The password should be a random sequence of letters and numbers and NOT something that you use on your accounts. You will also need to have a registered domain name where you will host the phishlets. You can get a domain for free from Namecheap (`https://www.namecheap.com/`) using GitHub student developer pack (`https://education.github.com/pack`) as shown and discussed in class. Please do not select auto-renew option if you have to use a card to get the free offer. You will need to host the domain on a server having a public facing IP. I would recommend using Digital Ocean for doing that and we have discussed this in class. You can get $ 100 credit on Digital Ocean from GitHub student developer pack `https://education.github.com/pack`). After you have created the Digital Ocean account create a "droplet" using Ubuntu and then map your domain to the IP of the droplet. Now SSH into the droplet and install Evilginx on it. Finally start your setup by following the videos by Luke Turvey available from `https://github.com/kgretzky/evilginx2` (yes, they are back after YouTube removed them but now hosted on his own server). We have also demonstrated the creation of the droplet in class, so you can refer to the lecture videos from there as well.

Submission: I have decided to have a demo from each team for this. The demo should show be the attack and the fact that you can steal the username and password and the session cookie.

Note: Please DO NOT use this attack on any one as this is illegal and you can go to jail for this. I am teaching this as a part of the course and NOT for using this against anyone. I or UAH will not be responsible if you use this attack on anyone and face the consequences of your actions.

Submission: You will submit a report with screenshots of each of the main steps showing how the credentials were finally stolen. You will also need to demo this to the TA.

Problem 2: John The Ripper [30 Points]

In this lab we will explore the use of John The Ripper (JTR) for password cracking. Note that JTR is a dictionary based password cracking tool and the time it takes to crack a password will depend on the complexity of the password. This part of the project is being set to make you familiar with the process of using a new tool, setting it up and learning to use the same for a penetration task. As it is not possible to teach everything in the class, my goal is to teach you enough so that you can explore your own and hence we have NOT shown any demos for this part of project 1. You will do the following:

1. Install Kali Linux on the Virtual Box or a hypervisor of your choice. Kali VMs can be downloaded from here `https://www.kali.org/get-kali/#kali-virtual-machines`. Make sure that Kali is working and that JTR is installed in Kali.

2. Create a password protected zip archive containing a text file having the sentence "Hello World". Use the following passwords one by one:

   (a) Password465
   (b) Ball2022Game
   (c) SuperBowl!Hooray
   (d) E$%!&dret5@!#@$@$
   (e) !123#UAH$Go

   For each of these cases, use JTR to break the password (if you can) and document the time taken by JTR to achieve the break. You will need to show that JTR can find the password. Document the cases (if any) where JTR fails to break the password. Note that we will NOT show you how to use JTR and you need to learn how to use JTR and will need to document the usage using a step-by-step howto document. During the demo, you will show JTR working on the password that was cracked in the shortest time. You will also submit a report with screenshots of each crack and the time it took to achieve the crack. Also document cases where JTR failed.

Problem 3: Exploring Passwords [20 Points]

For this part of the project, you will explore the passwords in the file "passwords.txt" available from the Canvas project 1 module. This is a dataset of breached passwords that is publicly available for research purposes. Please download this dataset and write a piece of code to explore this dataset to answer the following questions:

1. How many passwords are there in total? [5 Points]

2. How many of these passwords contain the substring "password". Note that you need to consider all forms of capitalization of the letters. [10 Points]

3. How many of these passwords are composed of a combination of letters [a-z,A-Z], numbers [0-9] and special characters [!,@,#,$,%, &]? [5 Points]