

Title:

Lining the Hook for Tactical Phishing

Abstract:

The first Seng360 lab entailed using the Social-Engineer Toolkit (SET) by Dave Kennedy to construct a Phishing website and send phishing emails to steal user data. We used a Linux environment and provided our own emails for this informational phishing practice. Overall, the attempt was successful and provided insight into social engineering, even without the phishing email being physically sent due to present email security features.

Aim:

The aim of the lab was to familiarize ourselves with common phishing tactics and how they are implemented. In short, we learned to appreciate the tools available to attackers that launch these social engineering attacks, such as phishing emails and cloned phishing websites.

Intro and Background:

The lab introduced SET which is an open-source Python-driven tool for penetration testing around social-engineering. What I found interesting was that the SET program has over two million downloads and is supported heavily within the security engineering community. Interestingly, the menu in SET offers multiple Spear Phishing Attack Options such as:

- (1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack

- 6) Arduino-Based Attack Vector
- 7) SMS Spoofing Attack Vector
- 8) Wireless Access Point Attack Vector
- 9) QRCode Generator Attack Vector
- 10) Powershell Attack Vectors
- 11) Third Party Modules
- 99) Return back to the main menu.

Here we chose options 2 and 5 for the lab but the other options, especially Wireless Access Point Attack Vector, offer interesting avenues to potentially explore further in future labs. Website attack vectors and mass mailer attacks allowed our lab group to construct and send phishing emails as well as set up websites that steal a user's data as they enter the information on to the site. We were also tasked with creating a phishing email template, which would be believable and entice users to open and think it is a genuine email and not a phishing attempt.

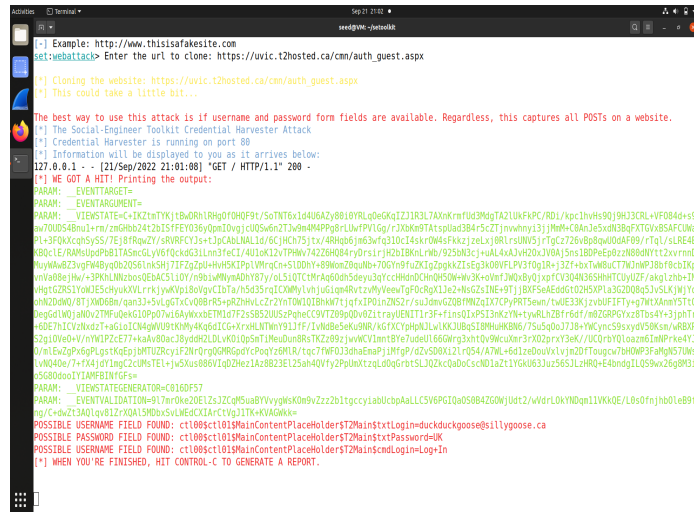
Method:

The tools used for this lab were the aforementioned SET tool kit, Ubuntu-Desktop setup (Via VirtualBox or VM cloud service), Website Attack Vector and Mass Mail Attacker SET options in the UVic Lab. We then used SET to create a phishing email and webpage for security knowledge purposes. We additionally utilized an html online editor to create a phishing template.

Results:


When creating the harvester to receive user data, we were able to obtain the email and password of a user who entered the site, which is displayed in the screenshot of the harvested info from the website. Due to the VM Cloud used for the virtual box, it was not possible to generate the xml report file, although the contents are still visible in this screenshot of the terminal.

Screenshot (Harvester receiving data from the site):



Secondly we were tasked with setting up, sending and creating a phishing email attack. The set up involved utilizing a template and selecting a mass or single email address as the target. The single email address allowed us to send an email using a fake username, however due to network and email security, the email was not actually sent to the target.

Screenshot (Phishing email setup):

 SSH-in-browser

```
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>1

Do you want to use a predefined template or craft
a one time email template.

1. Pre-Defined Template
2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Strange internet usage from your computer
2: Dan Brown's Angels & Demons
3: Have you seen this?
4: How long has it been?
5: Computer Issue
6: Baby Pics
7: WOOAAA!!!!!!!!!!!! This is crazy...
8: Order Confirmation
9: Status Report
10: New Update
set:phishing>7
set:phishing> Send email to: [redacted]@gmail.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com): PaulIsAwesome@HalaMadrid.com
set:phishing> The FROM NAME the user will see: PAUL WALL
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
```

Lastly, the creation of the phishing email template provided an avenue for creativity. I chose to have a World Cup 2022 phishing email set up, which offers free tickets to the tournament. The assumption being that since the World Cup is coming up in November, we have a believable and realistic email in order to attack a target and obtain their information.

Screenshot(Phishing email)

FREE WORLD CUP TICKETS TO QATAR!



GO TO THIS WEBSITE TO RECEIVE YOUR TICKETS: uvic.ca/you_got_phished

Save this link into your bookmarks and share it with your friends, they all get tickets too!!!

Enjoy!

Question: What is an open SMTP relay? Why is it problematic?

SMTP relay provides an interesting method to potentially send phishing emails. It allows emails to travel between multiple email servers before ending up in the target's inbox. Therefore, it allows a sender to send multiple emails through multiple servers, potentially bypassing email securities of targets and not be limited to a targets' safety measures [1]. This is a problem, since it allows phishing emails to be sent with a high rate of deliverability en masse and potentially go through multiple servers to reach their targets. It provides the ability for phishing emails to be sent more regularly, being received by more targets and therefore having a high volume of successful scams completed. In essence, it improves the "numbers game" and widens the target pool of potential targets to get phished.

References:

[1] A. Rahman, "SMTP Relay: What Is It and How Does It Work," *Mailmodo*, Apr. 11, 2022.
<https://www.mailmodo.com/guides/smtp-relay/> (accessed Sep. 23, 2022).