Lab 1: Creating Doppelgangers

Disclaimer: All information/techniques/scripts and other intellectual materials shared as part of this course and labs are meant teach you the techniques used by social engineers. Feel free to use them on any legal engagement/contract. I do not condone doing anything you learned for illegal purposes, and can ensure you if you do, you will likely end up in jail – you've been warned.

Objectives

To create an alternate persona that can be used in soliciting and gaining trust in the person(s) you are targeting in a Social Engineer engagement. Alternate sources should include:

- Personal email address – gmail or yahoo
- LinkendIn account – join groups associated w/ target. Become a 1st level connection with target
- Facebook account – friend target
- Any other social media site that makes sense: pintrest, Instagram, Twitter….. the list is endless.

The alternate persona you create needs to work on the various levels of trust/friendship the higher up the trust pyramid the better.

Materials Required

This lab requires the following:

- PC with Internet connectivity

Activity

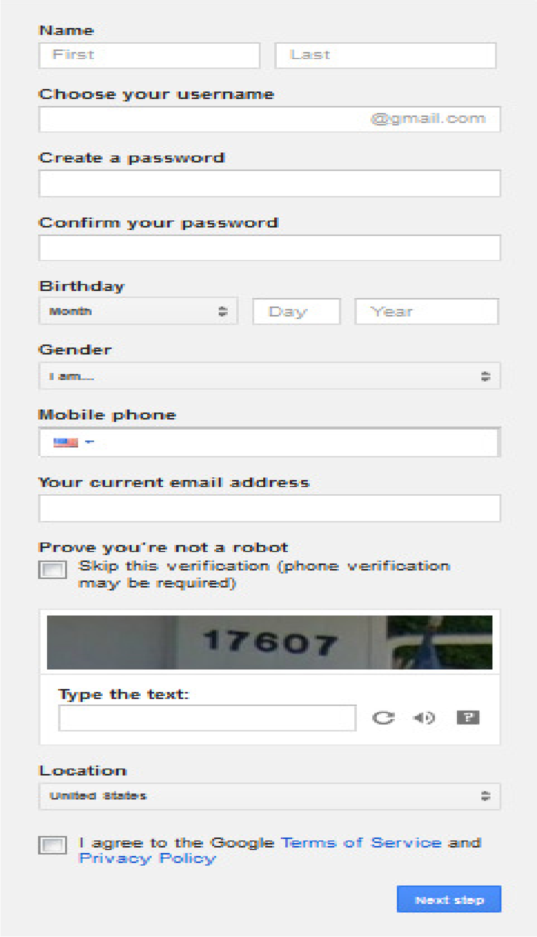
Estimated completion time: 10-15 minutes

In this lab, we will start by creating an alternate email account. While the lab will walk you through creating a gmail account, it is recommended that multiple accounts from the popular email services be created (Yahoo, Microsquish, etc.). We will then use this account to create a Linkedin account.

Stage 1: Creating a gmail account.

1. Open a browser and navigate to gmail.com. ***Note:*** *if you already have a gmail account you may need to log off prior to creating a new account.*
2. You will be presented with the account creation page. From there you will need to fill out the following information:
   a. Name
   b. UID
   c. Password
   d. DoB
   e. Gender
   f. Mobile Number

g. Existing email.



Name

First Last

Choose your username

@gmail.com

Create a password

Confirm your password

Birthday

Month Day Year

Gender

I am...

Mobile phone

Your current email address

Prove you're not a robot

□ Skip this verification (phone verification may be required)

17607

Type the text:

Location

United States

□ I agree to the Google Terms of Service and Privacy Policy

Next step

Figure 1 Gmail create account form.

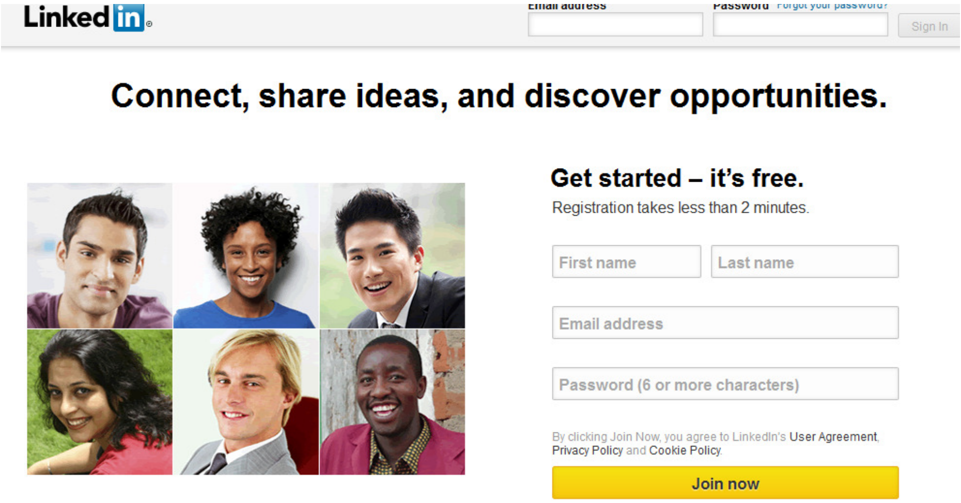
Food for Thought: *What type of person would be most effective gaining trust with your target? Male/Female? Age? Marital Status? Work level? – all of these go into creating a good secondary persona. It makes it easier if you have a person (real or not) to model your persona off of.*

3. Click on "Next Step" to
4. Next you will be presented with a "Create Google+" account – if you need one go ahead. No will suffice for the lab.
5. You're done step 1 – new account setup and created.

For more privacy you may want to stack your accounts or use throw away mobile numbers.

Stage 2: Creating a LinkedIn Account

1. In your browser navigate to www.linkedin.com
2. On the main screen you will be presented with options to create an account. Fill in the necessary information and click "Join Now". ***Note:*** *Use the same information used in the gmail account from stage 1.*



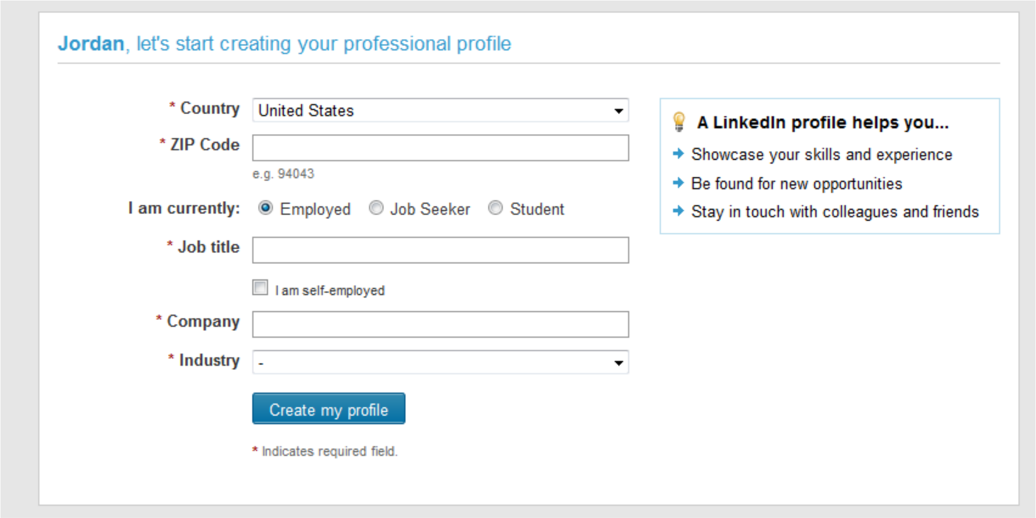
Connect, share ideas, and discover opportunities.

Get started – it's free.

Registration takes less than 2 minutes.

By clicking Join Now, you agree to LinkedIn's User Agreement, Privacy Policy and Cookie Policy.

3. You will be presented with geographical information as shown below. ***Note:*** *You should choose something relevant to the target(s) you are trying SE, or a generic address if just using for general info gathering/connecting.*



Jordan, let's start creating your professional profile

* Country: United States

* ZIP Code:

e.g. 94043

I am currently: ● Employed ○ Job Seeker ○ Student

* Job title:

□ I am self-employed

* Company:

* Industry: -

* Indicates required field.

A LinkedIn profile helps you...

- Showcase your skills and experience
- Be found for new opportunities
- Stay in touch with colleagues and friends

4. From there you will be taken to a variety of screens, to include email confirmation. None of these steps are required outside of confirming your email. In lieu of connecting gmail and linkedin opt for the send me confirmation email link. (you will have to go to your email and verify it). Skip all other steps – you can work on the profile later.

Food for Thought: *Creating a fictitious resume with work history that aligns with your target(s) or the industry you are info gathering for. Use this resume to update the profile- be sure to join groups, reach out to contacts, get contacts.*

5. Finished early? Need contacts/connections? Great –look over to the person to the left, right, front, back – basically all around you to start your contacts. This way you will be second degree to any of their contacts – instant way to gain connections.
6. Finding this is easy –good you may want to do the stretch lab later which will require

a linked premium account. Go ahead and make yours premium – its free for the first 30 days (good to have anyway).

Practice @Home

Great if you have gotten this far, you have a preliminary alternate account/persona started. Here is a list of things to do @Home:

1. Complete your Linkedin profile – getting as complete as possible, to include recommendations is key to making it look legit.
2. Join Groups – instant access to similar likes/dislikes of target.
3. Expand into other social media avenues.
   a. Create a Facebook account for your new self
   b. Create a twitter account and schedule regular tweets. Follow the target and those the target follows.
4. Announce change of job on all social media – helps "convince" someone you are targeting that you have mutual employer.

Lab 2 Phone Skills

Disclaimer: All information/techniques/scripts and other intellectual materials shared as part of this course and labs are meant teach you the techniques used by social engineers. Feel free to use them on any legal engagement/contract. I do not condone doing anything you learned for illegal purposes, and can ensure you if you do, you will likely end up in jail – you've been warned.

Objectives

One common social engineering attack vector is to call the target and obtain information that supports your effort. While it is unreasonable for all of to make cold calls, we will meet in groups to discuss possible scripts and present those to the class.

Materials Required

Nothing – although "google fu" may help. Keep an open mind that this will be a script to use on when calling the target organization.

Activity

Estimated completion time: 15 minutes to meet & 10 minutes to discuss

In this lab, you will meet with your team to come up with a script to be delivered via voicemail or in-person calls. The examples below taken from the Vulnerability Assessment framework http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html should assist you in your ideas. Although I hate the term I want the groups to "think outside the box".

> **Example 1:** - Pretend to be from the Helpdesk
> "Hi, it's Zoe from the helpdesk. I am doing a security audit of the network and I need to re-synchronize the Active Directory usernames and passwords.T his is so that your logon process in the morning receives no undue delay." Tips: If you are calling from a mobile number, explain that the helpdesk has been issued a mobile phone for 'on call' personnel.
>
> **Example 2:** - Pretend to be form Network Security
> "Hi, I'm the new guy in IT and I've been told to do a quick survey of users on the network. They give all the worst jobs to the new guys don't they? Can you help me out on this?" Get the following information; try to put a "any problems with it we can help with?" slant on it. Username, Domain, Remote access (Type - Modem/VPN), Remote email (OWA), Most used software? Any comments about the network? Any additional software you would like? What do you think about the security on the network? (Password complexity etc.) Now give reasons as to why they have complexity for passwords, try and get someone to give you their password

and explain how you can make it more secure. "Thanks very much and you'll see the results on the company boards soon."

You and your group will have 15 minutes to come up with a phone based scenario – each group will share their ideas to the entire class. The group will need to present the following information:

- Goal of phone call – getting info, confirming email addresses, gaining passwords, etc.
- The script – Present what your team came up with. Please limit the script to 2-3 minutes. This should be ample time to share your ideas.

Class examples will be given, that take it beyond the normal interactions.

Practice @Home

Public speaking, to include calling targets causes many people stress. There are some public speaking notes that will help you get over stress/anxiety. The biggest and simplest item to do is practice. I recommend practicing the following:

- What to say – know your script and what you are and the end goal of the call
- What they will say – prepare yourself for both compliant and non-compliant users
- Know when you are on track – you may get deviated from original course but still obtain the goal
- Know when you are off track – be able to quickly identify when you are off track. You may not be able to get to your goal on that call so adapt and set new goals (e.g. set up a follow on call).

Lab 3 Email Enumeration w/Demo

Disclaimer: All information/techniques/scripts and other intellectual materials shared as part of this course and labs are meant teach you the techniques used by social engineers. Feel free to use them on any legal engagement/contract. I do not condone doing anything you learned for illegal purposes, and can ensure you if you do, you will likely end up in jail – you've been warned.

Objectives

One of the most common Social Engineering attack vectors is via email (Phishing, Spear-Phishing, Whaling, etc.) however, before the first email is sent a list of contacts (email addresses) will have to be gathered. While this class is not an OSINT course, it will show you ways to effectively gather email accounts.

Materials Required

This lab requires the following:

- PC running a UNIX variant (We recommend Kali) with the following tools installed:
  - Burp web proxy tool
  - Python

Activity

In this lab, we will search Bing or LinkedIn for all employees associated with our target(s) and use that information to find possible email addresses. The instructions below are written from a Kali perspective but should provide the necessary fundamentals if you are using an alternate distro. ***Note:*** *This lab was built off the Phishbait tool suite that I highly recommend. I modified it slightly as I like the company search better.*

Estimated completion time: 15-45 minutes

FREE Lab Portion – Don't have a credit card/paypal account use this. This is the easier of the two. I encourage you to try both.

Stage 1: Launch ICE Waesel

1. Navigate to github and do a search for phishbait
2. Navigate to the phishbait github site
3. Select and copy the HTTPS clone URL

Stage 2: Launch a terminal window

1. Git clone the phishbait tools by issuing the following command
   a. Git clone https://github.com/hack1thu7ch/PhishBait.git
2. Cd to the phishbait directory

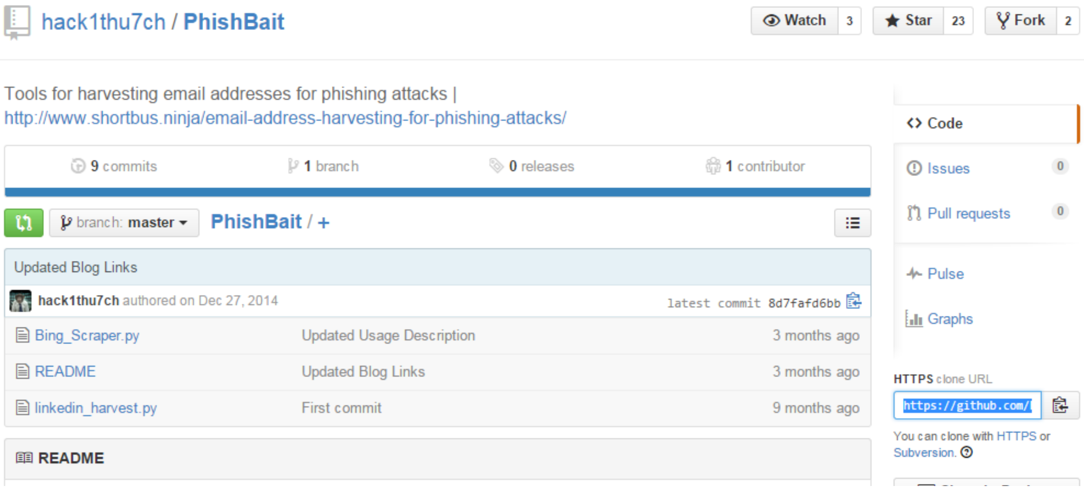
Stage 3: Use Phishbait Bing Scraper to get emails.

1. Type *python Bing_Scraper.py* to pull up the usage command
2. Re-run it with the correct syntax for the target you want

3. Enjoy – you now have quite a few emails

Stage 4 Optional: Merge your theHarvster emails with your phishbait emails and unique them

1. Run harvester and pipe output to file using tee command
    a. Theharvester –d victim.com –l 500 –b all |tee *file*
    b. Grep @ *file* > *harvesteremails*
    c. Cat harvesteremails >> phishbait email file
    d. Sort –u to unique them. Don't forget to > it to a file



Tools for harvesting email addresses for phishing attacks | http://www.shortbus.ninja/email-address-harvesting-for-phishing-attacks/

Updated Blog Links

hack1thu7ch authored on Dec 27, 2014 latest commit 8d7fafd6bb

Bing_Scraper.py	Updated Usage Description	3 months ago
README	Updated Blog Links	3 months ago
linkedin_harvest.py	First commit	9 months ago

STRETCH Lab Portion – Requires Linked premium account they are free first 30days but need you need to put in CC or Paypal. If you don't get a chance in class try it @Home.

Stage 1: Launch Burp

1. Navigate to the Applications menu and select: *kali linux -> web applications ->web application proxies -> burpsuite*
    a. The Burp tool should launch
2. Configure the proxy portion of burp so that it intercepts web traffic (does not have to but may make it easier …)

Stage 2: Launch ICE Weasel (browser)

1. Ensure the bowser is configured to navigate through the Burp proxy.
    a. *Preferences ->advanced -> network ->settings ->manual proxy*
    b. Set it for all protocols
2. In your browser navigate to LinkedIn and login with the account created in Lab 1.
    a. Burp should be intercepting this traffic – it may benefit you to confirm that it is working
    b. **Note:** you will have to click to allow the traffic to pass through burp
3. From LinkedIn perform a search on People for everyone who works for

“target” (your target not the store they have had enough grief lately)

   a. To the left of the search bar is a person icon – click it to ensure you are searching for people.
   b. Fill out the company name of your target and select “People who work at…”
   c. This request should be logged by Burp – please confirm that it is.

Stage 3: Switch over to Burp

1. Navigate to the HTTP history tab (or the intercept tab within Burp if you still had intercept on) to identify the above to request.
2. Send the above request to Intruder (right click send to intruder)
3. You should see a pageID number in the request – this is the “position” we want to manipulate. Select *Clear* to clear all “positions” an select the pageID=# “position” by highlighting and selecting *add*
4. Select *Payloads* tab
   a. Under the Payload Sets select numbers
   b. Under the Payloads Option select *Sequential,* and choose 1 – 5 (need to keep simple – could have selected 100s if you wanted to, although if you do make sure you build in delays as not to get caught by LinkedIn as a robot –free burp has built in delays) for the *From* and *To* range.
   c. Enter “1” for *Step & Min/Max integer digits* and “0” for the *Min/Max fraction digits.*
   d. Run intruder by selecting *Start Attack* – this will automatically pull down the first 5 pages of “People who work for {target}”
   e. Highlight the results and right click to save them make sure to disable “base64” if it is enabled. Remember the file name as we will be cleaning it up in the next step

Stage 4: Launch a terminal window – We will need to manipulate the data we saved

1. Navigate to the directory where you saved the file. If you want you can view it by using cat or similar tool.
   a. Yes, I know this doesn’t have emails in it… don’t worry we are getting there.
2. The first phase of the cleanup will to get the people’s names extracted from the file we saved. To do this we will be using a series of SED commands. To save typing you can download the following SED commands from pastebin ():
   a. The first command gets us a unique list of names from the file and saves it to a file named: names1. Note to change YourSavedFile to the name of the file you just saved.

```
sed '/profileName=/!d;s//&\n/;s/.*\n//;:a;/&network/bb;$!{n;ba};:b;s//\n&/;P;D' | sort –u
YourSavedFile  >names1
```

   b. If you view the file names1 you should see something a little more useful – but it still needs some cleaning. To get rid of the + sign between the first and last name run the following SED command:
   `sed ‘s/\+/ /g’ names1 >names2`
   c. Now let’s look at names2 - depending on the people that work at your target company you may be done. But you may have to do some extra

scrubbing as well. In case you have to do extra scrubbing the following commands may help:

i. sed 's/%2C.*//g' *filename* – this gets rid of any commas after the last name (often people, myself included, will put certs after their name)

ii. grep –v % *filename* – this will get rid of all crazy apostrophes or other weird charaters in names (that may kill emailing programs.

Stage 5: Creating the emails

1. Now that we have a list of names in the format of Firstname Lastname, we need to create email address. For this I created my own little script that I built of the phishbait stuff. Download the following Python script: pastebin.com/ndvFHnwW
   a. wget http://pastebin.com/raw.php?i=ndvFHnwW
2. Run the script pacing in the names list (created by above steps) and the domain of the target. The script will create 3 output files one each of the following formats (feel free to add to it if you want):
   a. firstinitialLastname@victim.com
   b. Firstname.lastname@victim.com
   c. FirstnameLastname@victim.com

Practice @Home

Try new and interesting ways to automate gathering emails. The more the better

- Didn't get a chance to try the stretch lab – that's ok try it at home.
- There are many tools/ways to accomplish this – try scripting something that works for you.
- Emails are, IMHO, the best way to SE – don't have to worry about talking to folks and someone always clicks it (really about a good 30+% do)

Lab 4 Phishing

Disclaimer: All information/techniques/scripts and other intellectual materials shared as part of this course and labs are meant teach you the techniques used by social engineers. Feel free to use them on any legal engagement/contract. I do not condone doing anything you learned for illegal purposes, and can ensure you if you do, you will likely end up in jail – you've been warned. Only phish yourself or those you have legal permission to do so.

Objectives

In this lab you will familiarize yourself with the tools of the trade to send emails and ways to create successful campaigns. Demos of other tools will be given too.

Materials Required

This lab requires the following:

- PC running able to run JAVA programs
  - I have tested this on Kali but had to update my JDK first.

Activity

We will use the tool "ICE-Hole" to generate email messages to the Doppelganger you created and test the different templates. Time permitting; we will build additional templates to use.

Estimated completion time: 30-45 minutes

Stage 1: Getting ICE-Hole

1. I have copies on the CD but if you are too impatient you can get it by issuing a wget https://www.blackhat.com/docs/us-14/materials/arsenal/us-14-Manners-Ice-Hole-Tool.zip
2. Unzip it to a folder of your choice.

Stage 2: Launching ICE-Hole

1. If running on a windows platform then you need to click the bat file.
2. If running on linux you need to run the ice-hole.sh command

Stage 3: Playing with ICE-Hole – using graphics here cause it is easier than typing it all out.

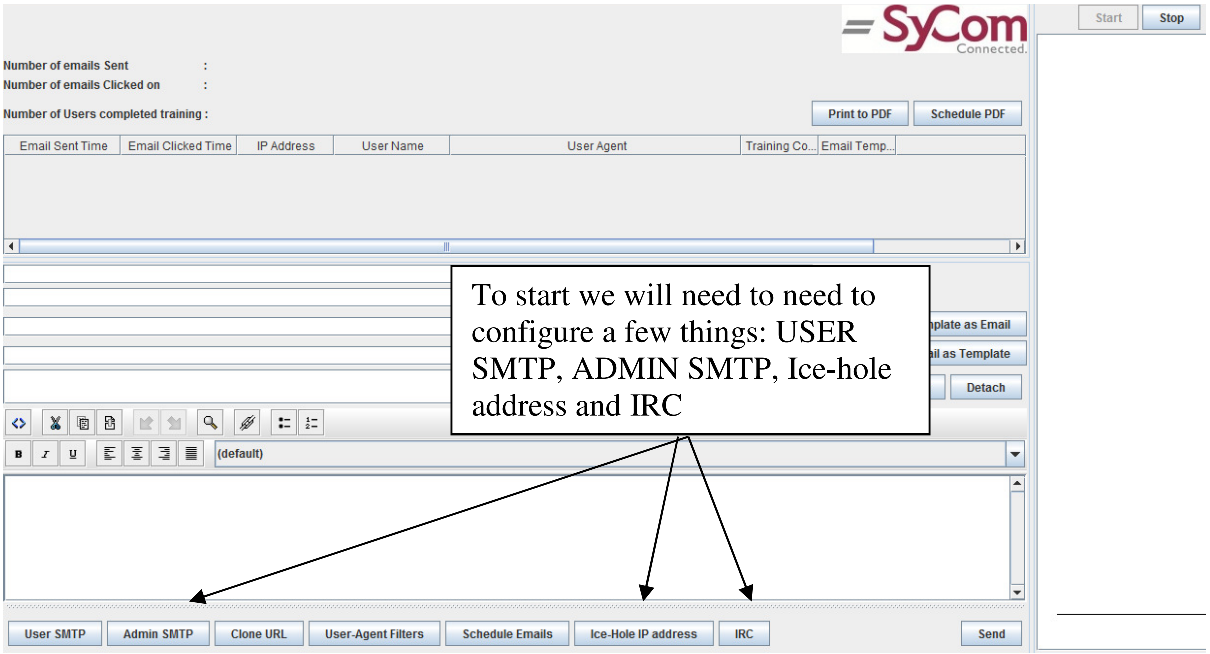
Note we will be disabling the IRC portion for the lab.

Stage 4: Ice-Hole holds all the config information in the mail.properties folder. You may need to update that (for example to switch the port numbers) directly from time to time.

Stage 5 : Updating JDK in Kali – you may have to do this if you are running this in kali and still using older Java.

1. Navigate to pastebin.com/MDgASRQi – copy link or follow along.

a. wget http://pastebin.com/raw.php?i=MDgASRQi

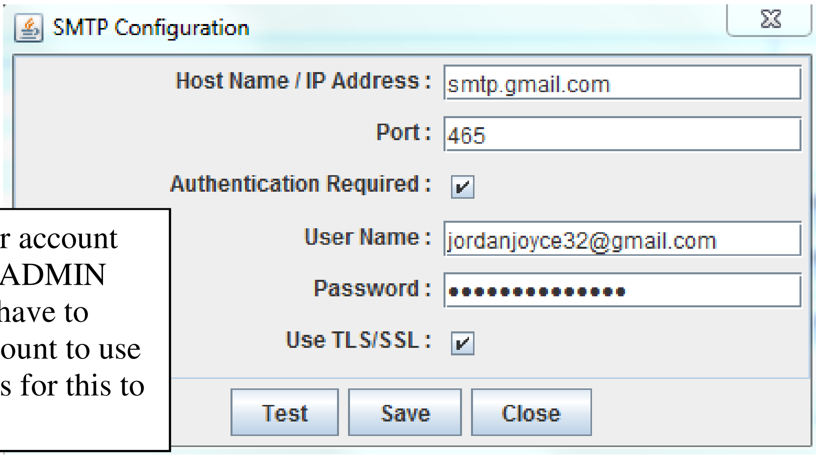


Number of emails Sent :
Number of emails Clicked on :
Number of Users completed training :

Email Sent Time	Email Clicked Time	IP Address	User Name	User Agent	Training Co...	Email Temp...

To start we will need to need to configure a few things: USER SMTP, ADMIN SMTP, Ice-hole address and IRC

Figure 2 The Ice-hole main screen



SMTP Configuration

Host Name / IP Address : smtp.gmail.com

Port : 465

Authentication Required : ☑

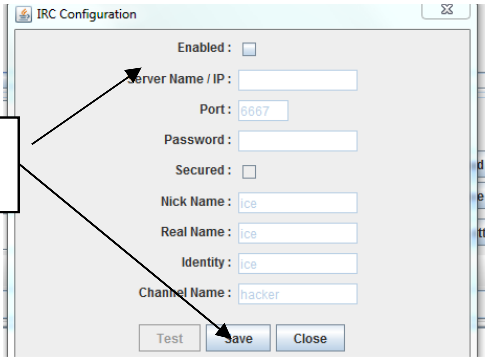
User Name : jordanjoyce32@gmail.com

Password : ••••••••••••••

Use TLS/SSL : ☑

Use your doppelganger account to configure USER & ADMIN SMTP. Note you will have to change your gmail account to use less secure applications for this to work.

Figure 3 SMTP Settings



IRC Configuration

Enabled : □

Server Name / IP :

Port : 6667

Password :

Secured : □

Nick Name : ice

Real Name : ice

Identity : ice

Channel Name : hacker

Uncheck the “Enabled” checkbox to disable IRC. Save changes

Figure 4 IRC Config

Ice-Hole will rewrite the templates with this info. Can use IP or DNS. For lab use 127.0.0.1 as we will be phishing ourselves.

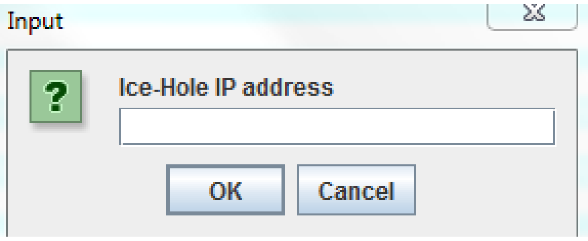
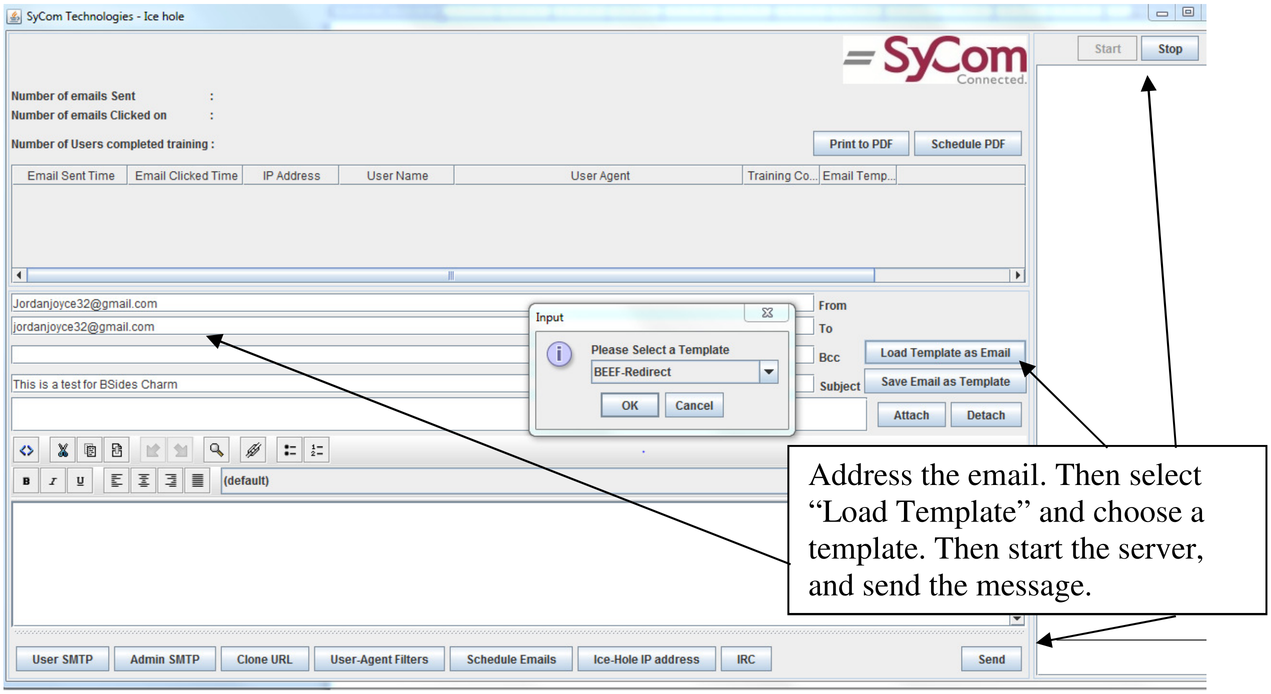


Figure 5 Configure Ice-Hole's Address



From: Jordanjoyce32@gmail.com

To: jordanjoyce32@gmail.com

Subject: This is a test for BSides Charm

Please Select a Template: BEEF-Redirect

Address the email. Then select “Load Template” and choose a template. Then start the server, and send the message.

Figure 6 Let's send an email...

Practice @Home

Run through all the available templates. Create your own (see next lab)

- My favorite is the yahoo keystroke logger.

Lab 5 Building Templates

Disclaimer: All information/techniques/scripts and other intellectual materials shared as part of this course and labs are meant teach you the techniques used by social engineers. Feel free to use them on any legal engagement/contract. I do not condone doing anything you learned for illegal purposes, and can ensure you if you do, you will likely end up in jail – you've been warned.

Objectives

To know what goes into building new templates and the logic around creating new ones.

Materials Required

This lab requires the following:

- PC running able to run Notepad (++, sumblime, leaf editor, etc.)

Activity

This lab is included if we have time; otherwise feel free to do it on your own @Home. You are limited to your own imagination. I will describe what I do, in hopes that it inspires you to think of clever ideas.

Estimated completion time: (Time permitting)On going… Keep developing these

Stage 1: Getting Samples

1. I like to know what kinds of samples the company may be getting spammed with and see if I can dupe those.
2. Get samples from those companies sign up on as many "lists" as possible.

Stage 2: View them as web page

1. Copy and Steal… I mean borrow.
2. Understand the tool and what it looks for modification.
    a. For example PhEmail wants a "{0}" that it searches for and replaces.
3. Many time it's better if it is not "forced"