Chapter 11
Social engineering

Outline

- The Social-Engineer Toolkit (SET)
- Example: Spear-Phishing Attacks
- Example: Web Attacks
- Example: Mass Email Attacks

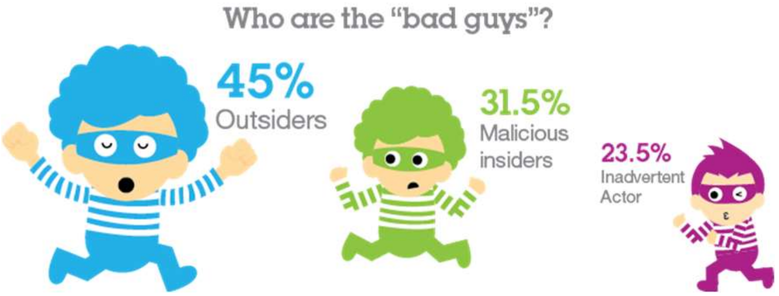
The Weakest Link

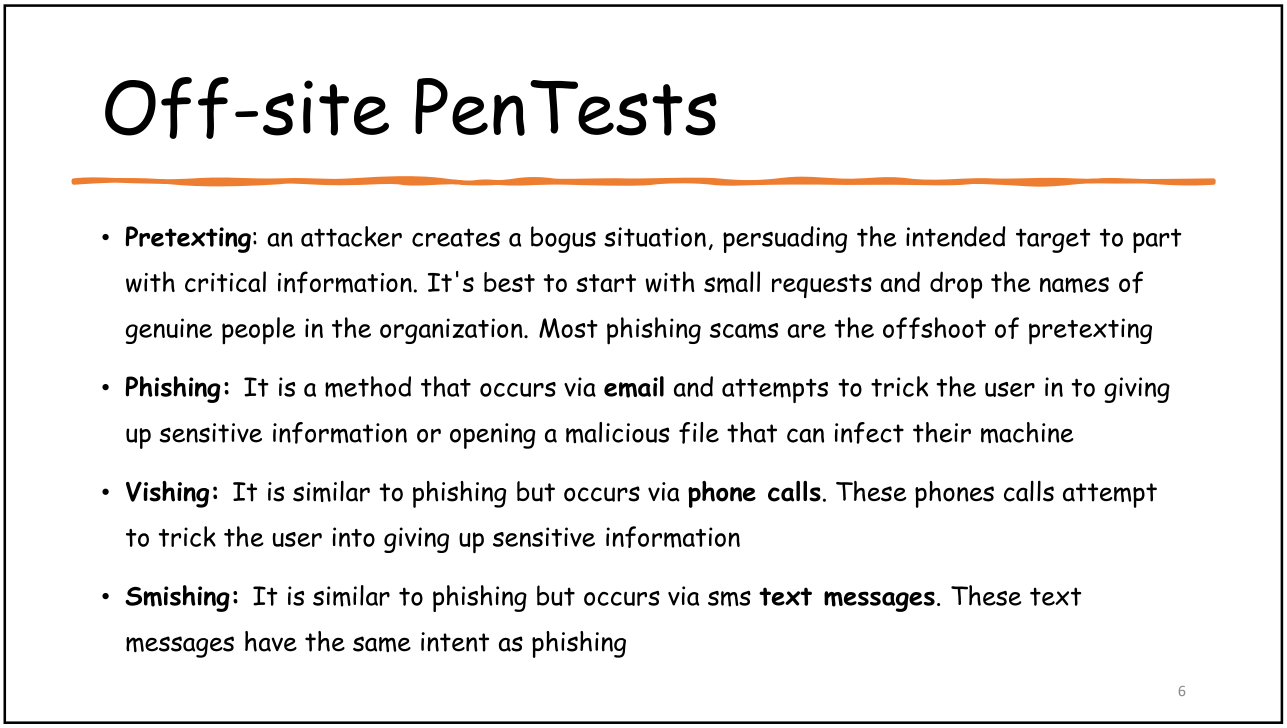
- No matter what technology we put in place, no matter how much money we spend on protections for the organization, we still have people and people are fallible. – Theodore Kobus, leader of BakerHostetler's Privacy and Data Protection team
  - It is a common saying in information security that users are the vulnerability that can never be patched
  - In fact, many of the most famous hacks include no system exploitation at all
- Social Engineering
  - An attack that exploits **human vulnerabilities**: a desire to be helpful, unawareness of security policies, and so on
  - Phishing attacks can be used to lure targets to visit **malicious sites** or download **malicious attachments**, among other things

Companies should put time and effort into training all employees about social-engineering attacks

Insider Attacks

- An **insider attack** is a security breach that is caused or facilitated by someone who is a part of the very organization that controls or builds the asset that should be protected.
- In the case of malware, an insider attack refers to a security hole that is created in a software system by one of its programmers.



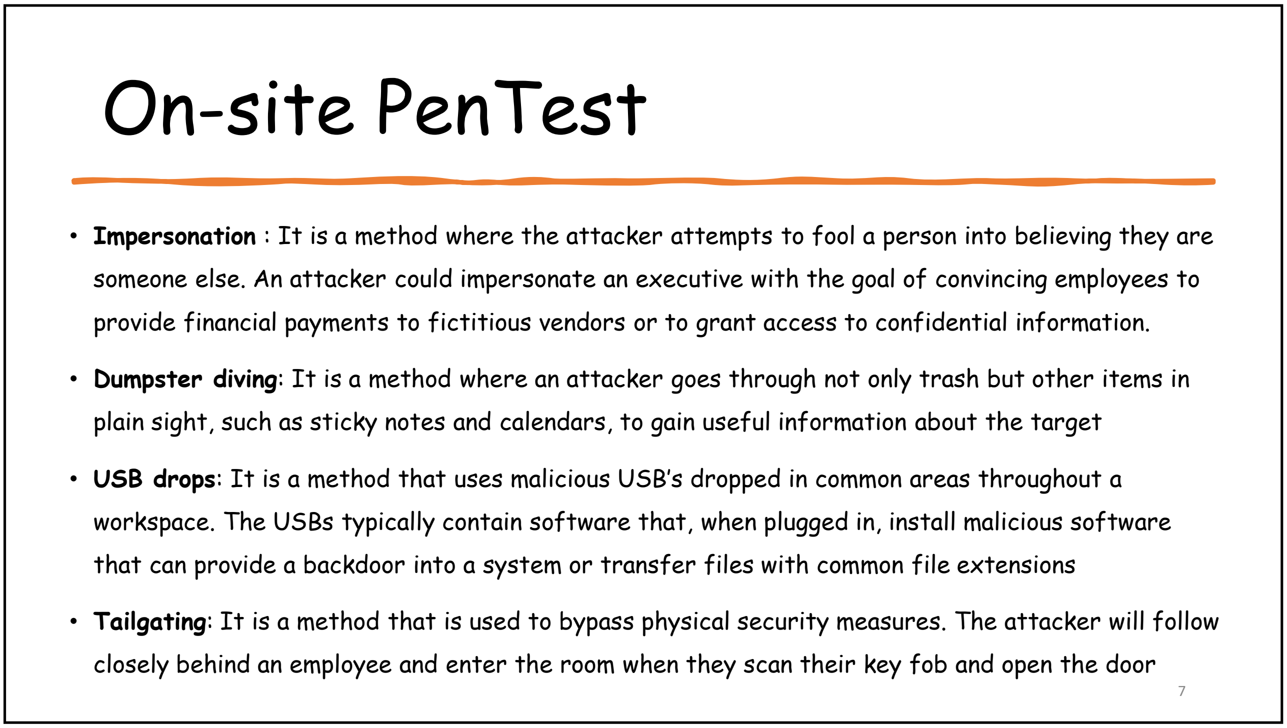


Off-site PenTests

- **Pretexting**: an attacker creates a bogus situation, persuading the intended target to part with critical information. It's best to start with small requests and drop the names of genuine people in the organization. Most phishing scams are the offshoot of pretexting
- **Phishing:** It is a method that occurs via **email** and attempts to trick the user in to giving up sensitive information or opening a malicious file that can infect their machine
- **Vishing:** It is similar to phishing but occurs via **phone calls**. These phones calls attempt to trick the user into giving up sensitive information
- **Smishing:** It is similar to phishing but occurs via sms **text messages**. These text messages have the same intent as phishing

6

6

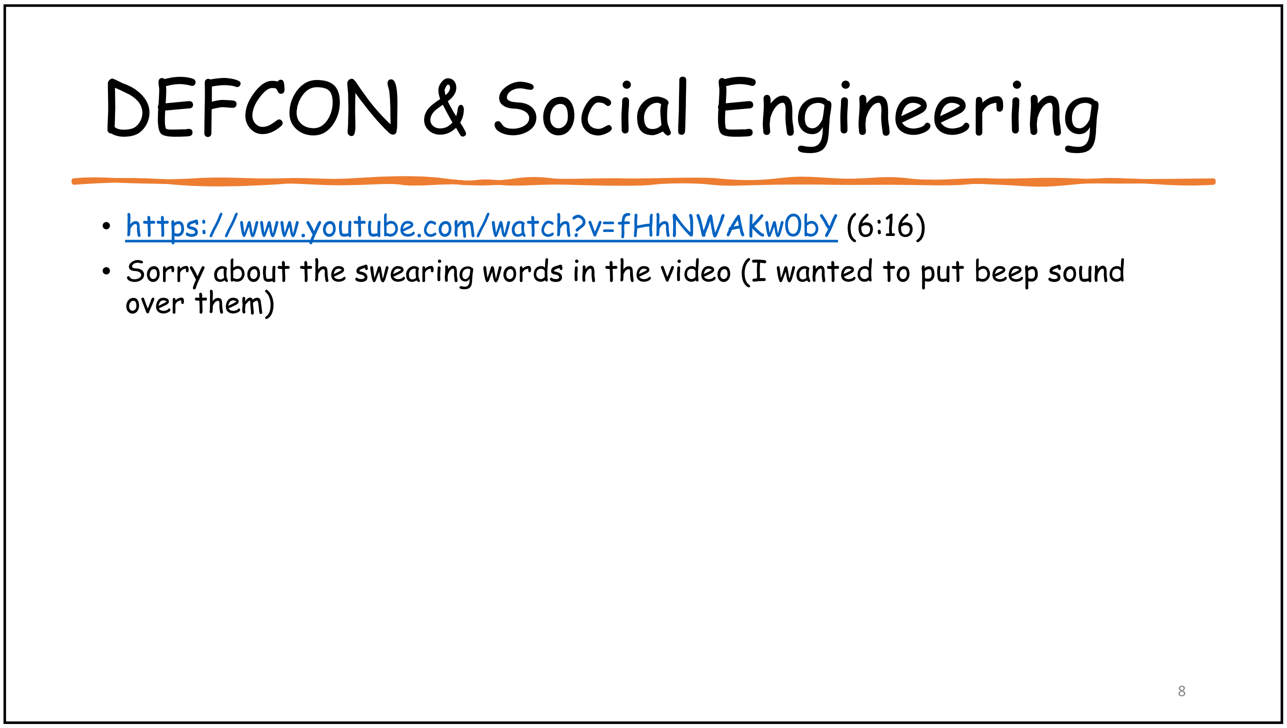


On-site PenTest

- **Impersonation** : It is a method where the attacker attempts to fool a person into believing they are someone else. An attacker could impersonate an executive with the goal of convincing employees to provide financial payments to fictitious vendors or to grant access to confidential information.
- **Dumpster diving**: It is a method where an attacker goes through not only trash but other items in plain sight, such as sticky notes and calendars, to gain useful information about the target
- **USB drops**: It is a method that uses malicious USB's dropped in common areas throughout a workspace. The USBs typically contain software that, when plugged in, install malicious software that can provide a backdoor into a system or transfer files with common file extensions
- **Tailgating**: It is a method that is used to bypass physical security measures. The attacker will follow closely behind an employee and enter the room when they scan their key fob and open the door

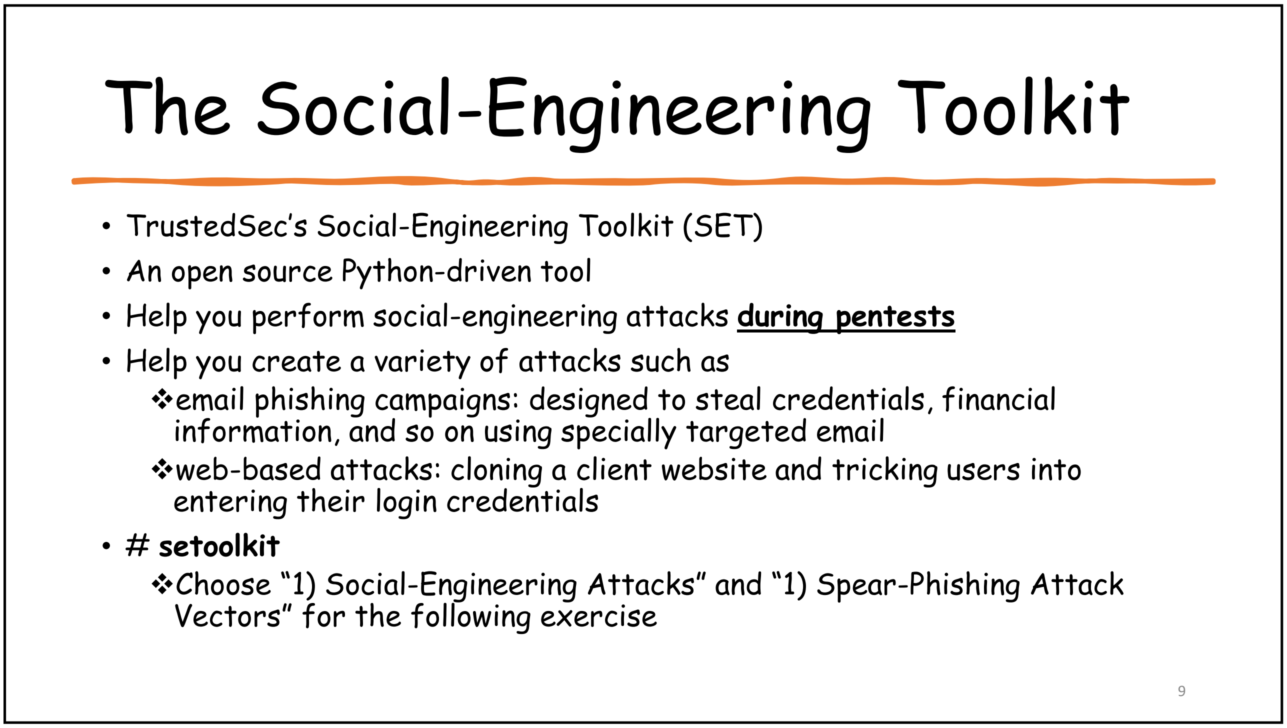
7

7



DEFCON & Social Engineering

- https://www.youtube.com/watch?v=fHhNWAKw0bY (6:16)
- Sorry about the swearing words in the video (I wanted to put beep sound over them)



The Social-Engineering Toolkit

- TrustedSec's Social-Engineering Toolkit (SET)
- An open source Python-driven tool
- Help you perform social-engineering attacks **during pentests**
- Help you create a variety of attacks such as
  - ❖email phishing campaigns: designed to steal credentials, financial information, and so on using specially targeted email
  - ❖web-based attacks: cloning a client website and tricking users into entering their login credentials
- **# setoolkit**
  - ❖Choose "1) Social-Engineering Attacks" and "1) Spear-Phishing Attack Vectors" for the following exercise

Troubleshooting setoolkit

- When **setoolkit** is working endlessly (more than 5min), but not giving you the output;

- apt-get update
- apt-get upgrade

- If it still doesn't look good,
- echo deb http://http.kali.org/kali kali-bleeding-edge main contrib non-free >> /etc/apt/sources.list
- apt-get update
- apt-get upgrade

Spear-Phishing Attacks

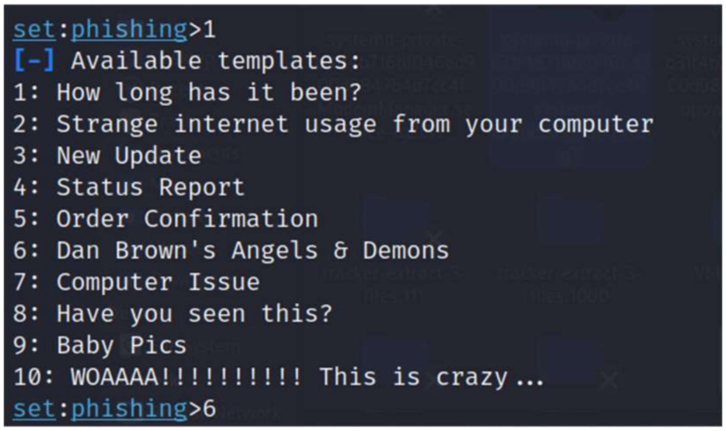
- Choose "1) Perform a Mass Email Attack"
- Choosing a Payload
  - ❖Select "14) Adobe util.printf() Buffer Overflow"
  - ❖Select "2) Windows Meterpreter Reverse_TCP"

CVE-2008-2992

- Setting Options
  - ❖SET should prompt for the relevant options for the payload
  - ❖set > IP address for the payload listener: <Kali IP address> & port
- Naming Your File
  - ❖Next you should be prompted to name your malicious file
- Single or Mass Email
  - ❖Now to decide whether to have SET send our malicious file to a single email address or a list of addresses

Spear Phishing Templates

- Are you familiar with some of these email title?



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

Spear-Phishing Attacks – Cont'd

- Creating the Template
  - ❖When crafting the email, we can use one of SET's email templates or enter text for one-time use in the template
    - Ex) Emails appear to come from a company executive or the IT manager, announcing new website functionality or a new company policy
- Setting the Target
  - ❖Now SET should prompt you for your target email address and a mail server for use in delivering the attack email
  - ❖When prompted, enter the email address and password for your Gmail account
    - SET should attempt to deliver the message

*** Gmail SMTP is filtering these emails out these days. You need your own mail server to send this**

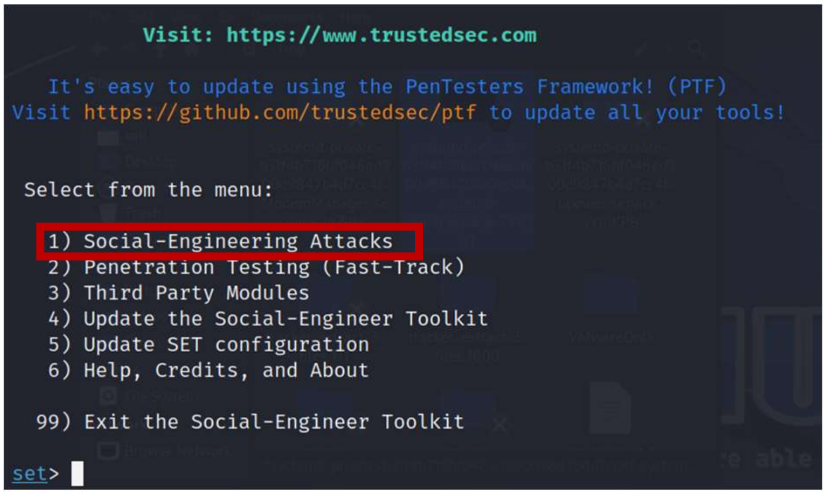
Spear-Phishing Attacks – cont'd

- Setting Up a Listener
  - ❖You can have SET set up a Metasploit listener to catch our payload if anyone opens the email attachment
  - ❖It automatically selects a module and a payload and inputs proper values to options

14

14

Web Attacks

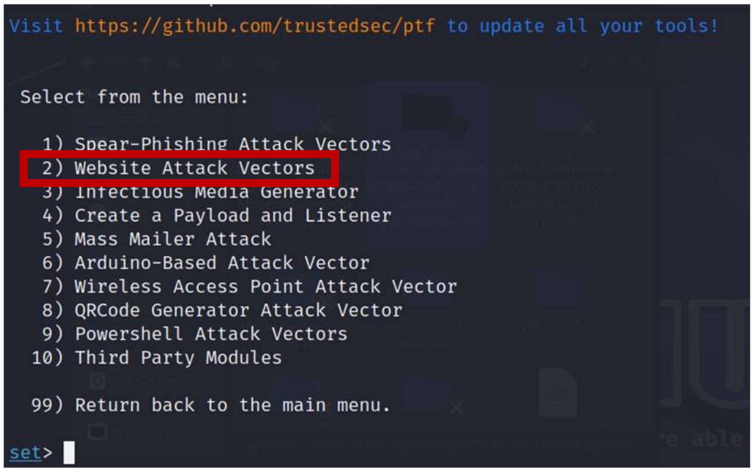


```
          Visit: https://www.trustedsec.com

   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>
```

15

15

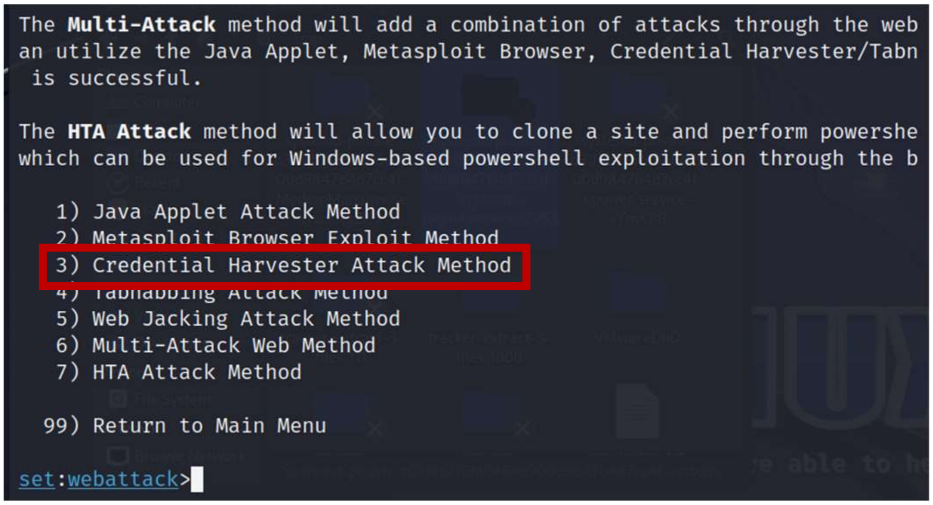
Website Attack Vectors



```
Visit https://github.com/trustedsec/ptf to update all your tools!

 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 Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set>
```

16

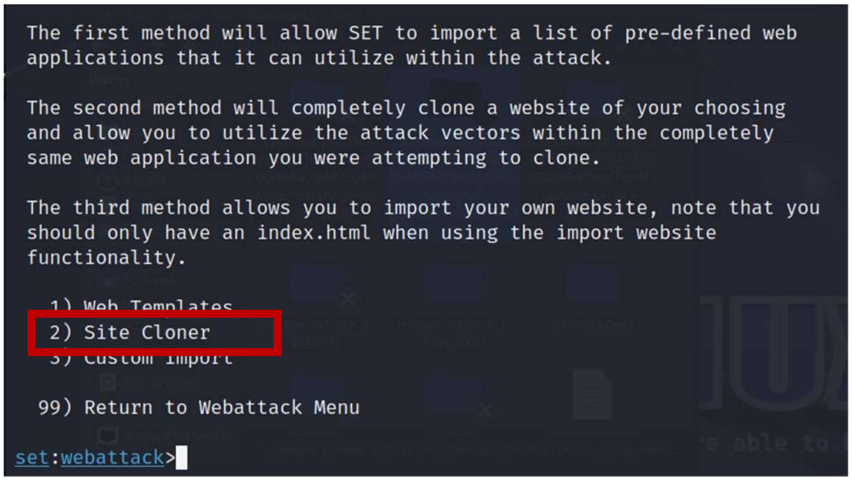
Credential Harvester Attack



```
The Multi-Attack method will add a combination of attacks through the web
an utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabn
 is successful.

The HTA Attack method will allow you to clone a site and perform powershe
which can be used for Windows-based powershell exploitation through the b

   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>
```

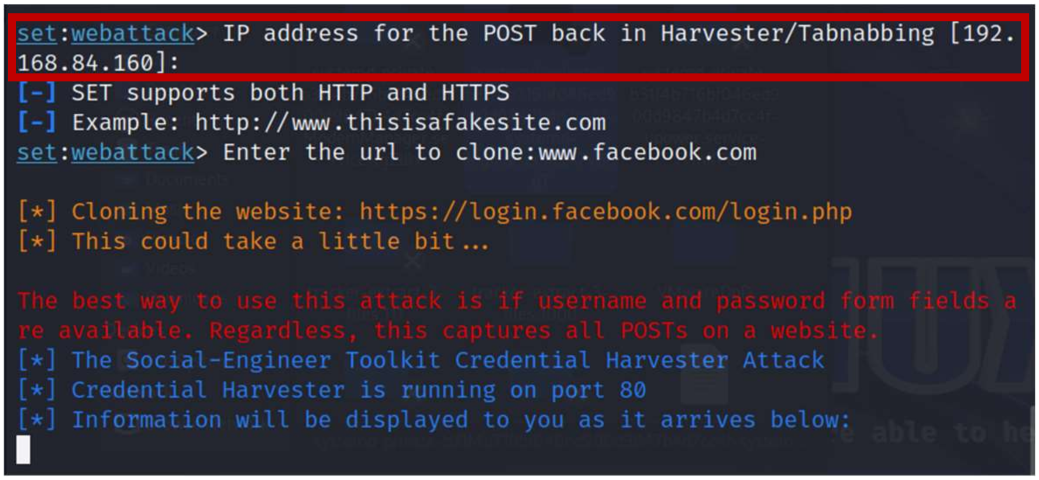
17

Site Cloner



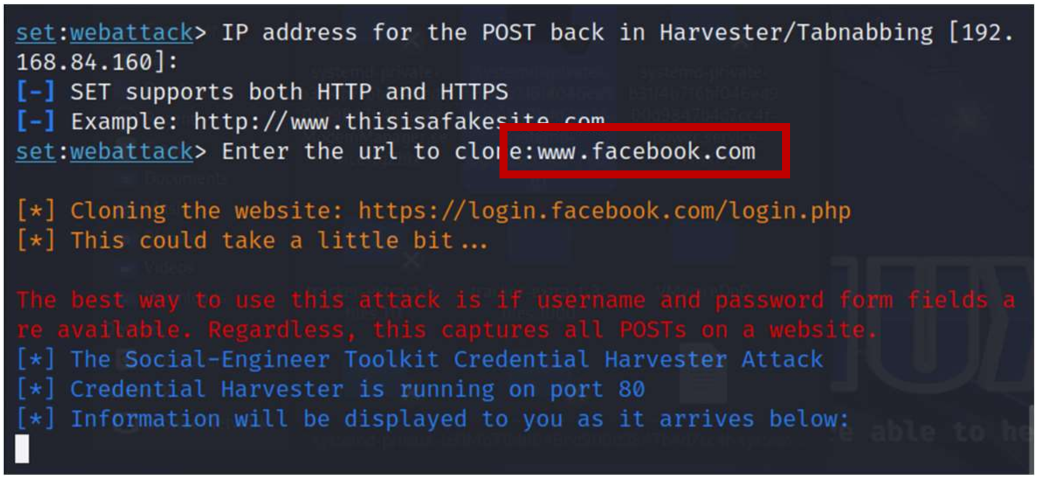
```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

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>
```

Set Attacker Machine's IP Address



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.
168.84.160]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields a
re available. Regardless, this captures all POSTs 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:
```

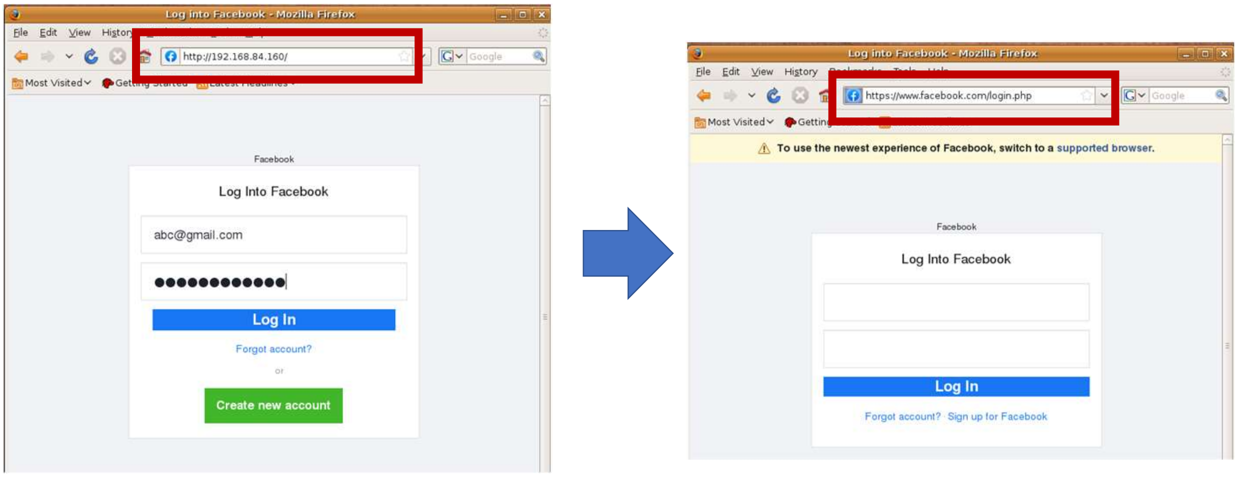
Set the Victim Website



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.
168.84.160]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields a
re available. Regardless, this captures all POSTs 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:
```

*It works like DNS cache poisoning

Access from Victim machine



Log into Facebook - Mozilla Firefox

http://192.168.84.160/

Facebook

Log Into Facebook

abc@gmail.com

●●●●●●●●●●●●●

Log into Facebook - Mozilla Firefox

https://www.facebook.com/login.php

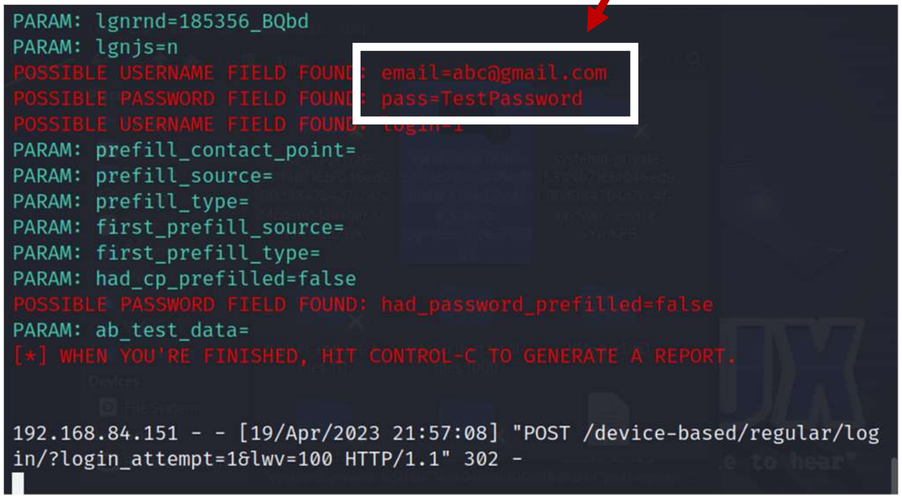
To use the newest experience of Facebook, switch to a supported browser.

Facebook

Log Into Facebook

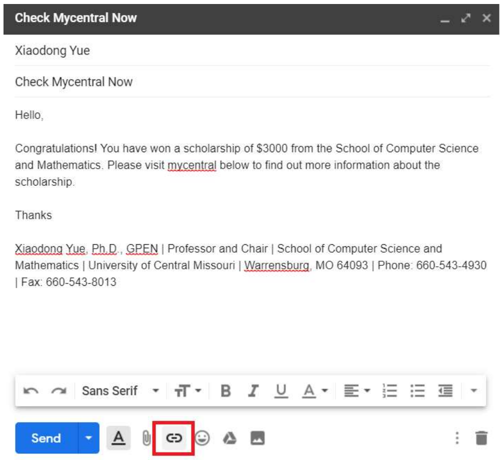
Attacker's Screen

Login Credential Harvesting



```
PARAM: lgnrnd=185356_BQbd
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=abc@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=TestPassword
POSSIBLE USERNAME FIELD FOUND: login=1
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.84.151 - - [19/Apr/2023 21:57:08] "POST /device-based/regular/log
in/?login_attempt=1&lwv=100 HTTP/1.1" 302 -
```

Composing a Phishing Email



Check Mycentral Now

Xiaodong Yue

Check Mycentral Now

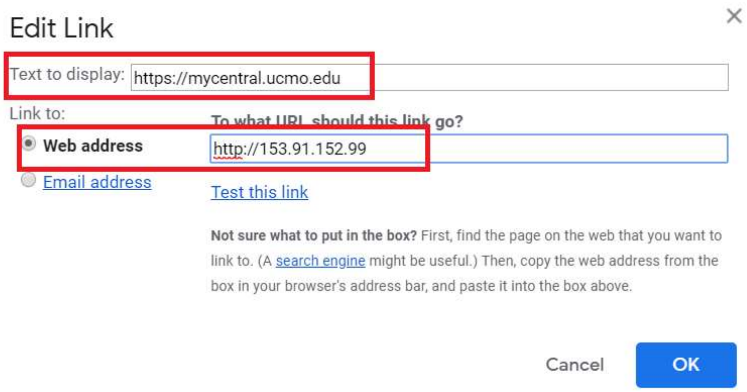
Hello,

Congratulations! You have won a scholarship of $3000 from the School of Computer Science and Mathematics. Please visit mycentral below to find out more information about the scholarship.

Thanks

Xiaodong Yue, Ph.D., GPEN | Professor and Chair | School of Computer Science and Mathematics | University of Central Missouri | Warrensburg, MO 64093 | Phone: 660-543-4930 | Fax: 660-543-8013

Construct the Fake Link



Edit Link

Text to display: https://mycentral.ucmo.edu

Link to:

● Web address

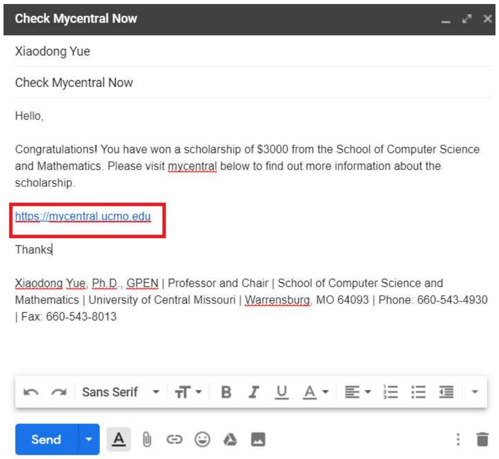
○ Email address

To what URL should this link go? http://153.91.152.99

Test this link

Not sure what to put in the box? First, find the page on the web that you want to link to. (A search engine might be useful.) Then, copy the web address from the box in your browser's address bar, and paste it into the box above.

Complete the Email



Check Mycentral Now

Xiaodong Yue

Check Mycentral Now

Hello,

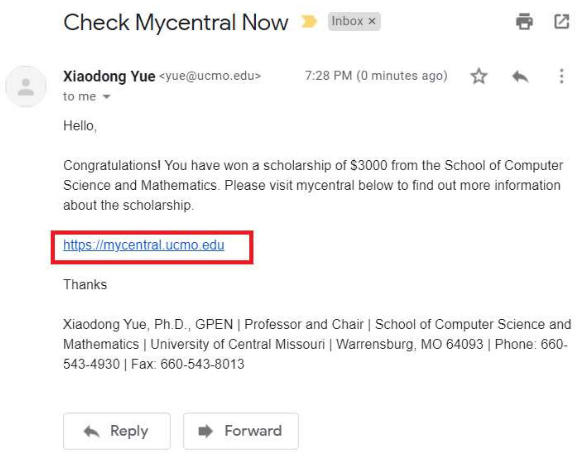
Congratulations! You have won a scholarship of $3000 from the School of Computer Science and Mathematics. Please visit mycentral below to find out more information about the scholarship.

https://mycentral.ucmo.edu

Thanks

Xiaodong Yue, Ph.D., GPEN | Professor and Chair | School of Computer Science and Mathematics | University of Central Missouri | Warrensburg, MO 64093 | Phone: 660-543-4930 | Fax: 660-543-8013

Receive the Email



Check Mycentral Now

Xiaodong Yue <yue@ucmo.edu> 7:28 PM (0 minutes ago)
to me

Hello,

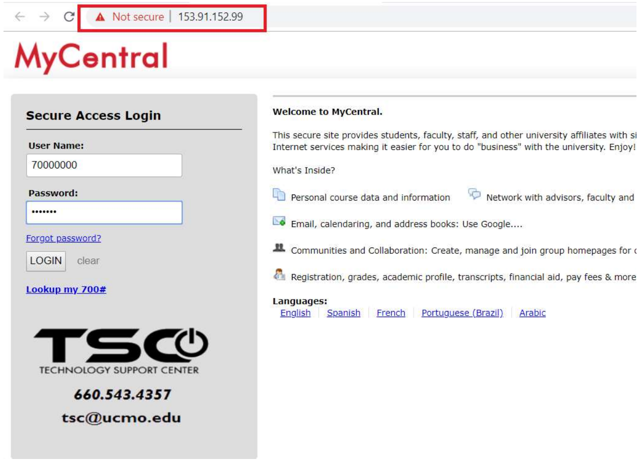
Congratulations! You have won a scholarship of $3000 from the School of Computer Science and Mathematics. Please visit mycentral below to find out more information about the scholarship.

https://mycentral.ucmo.edu

Thanks

Xiaodong Yue, Ph.D., GPEN | Professor and Chair | School of Computer Science and Mathematics | University of Central Missouri | Warrensburg, MO 64093 | Phone: 660-543-4930 | Fax: 660-543-8013

Visit the Cloned Site



Secure Access Login

User Name: 70000000

Password: •••••••

Forgot password?

Lookup my 700#

660.543.4357

tsc@ucmo.edu

Welcome to MyCentral.

This secure site provides students, faculty, staff, and other university affiliates with si
Internet services making it easier for you to do "business" with the university. Enjoy!

What's Inside?

Personal course data and information

Network with advisors, faculty and

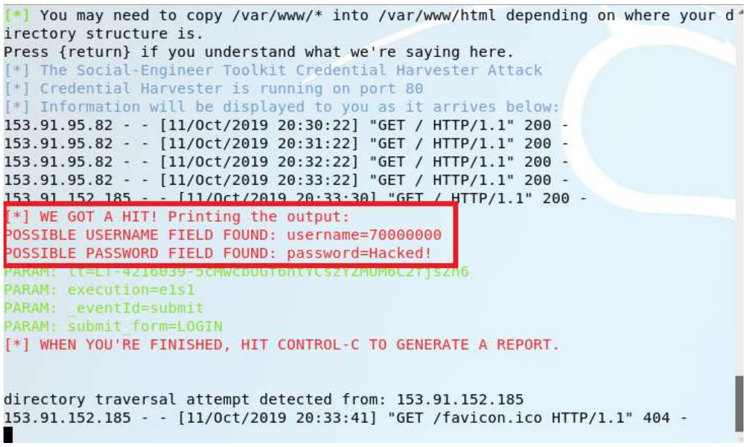
Email, calendaring, and address books: Use Google....

Communities and Collaboration: Create, manage and join group homepages for c

Registration, grades, academic profile, transcripts, financial aid, pay fees & more

Languages:
English | Spanish | French | Portuguese (Brazil) | Arabic

Harvest the Credentials

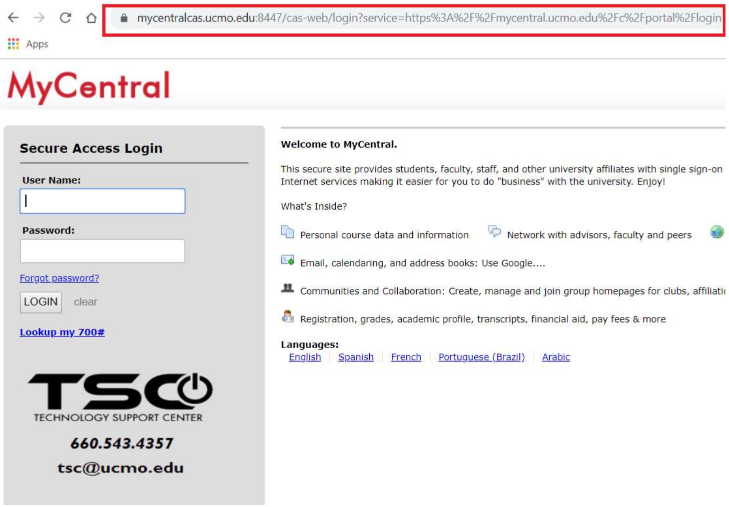


```
[*] You may need to copy /var/www/* into /var/www/html depending on where your d
irectory structure is.
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
153.91.95.82 - - [11/Oct/2019 20:30:22] "GET / HTTP/1.1" 200 -
153.91.95.82 - - [11/Oct/2019 20:31:22] "GET / HTTP/1.1" 200 -
153.91.95.82 - - [11/Oct/2019 20:32:22] "GET / HTTP/1.1" 200 -
153.91.95.82 - - [11/Oct/2019 20:33:22] "GET / HTTP/1.1" 200 -
153.91.152.185 - - [11/Oct/2019 20:33:30] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=70000000
POSSIBLE PASSWORD FIELD FOUND: password=Hacked!
PARAM: lt=LT-4216039-5cMWcbUGT6ntYCs2YZMUM6C2Tjs2h6
PARAM: execution=e1s1
PARAM: _eventId=submit
PARAM: submit_form=LOGIN
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


directory traversal attempt detected from: 153.91.152.185
153.91.152.185 - - [11/Oct/2019 20:33:41] "GET /favicon.ico HTTP/1.1" 404 -
```

28

28

User Redirected



mycentralcas.ucmo.edu:8447/cas-web/login?service=https%3A%2F%2Fmycentral.ucmo.edu%2Fc%2Fportal%2Flogin

MyCentral

Secure Access Login

User Name:

Password:

Forgot password?

Lookup my 700#

TSC
TECHNOLOGY SUPPORT CENTER
660.543.4357
tsc@ucmo.edu

Welcome to MyCentral.

This secure site provides students, faculty, staff, and other university affiliates with single sign-on Internet services making it easier for you to do "business" with the university. Enjoy!

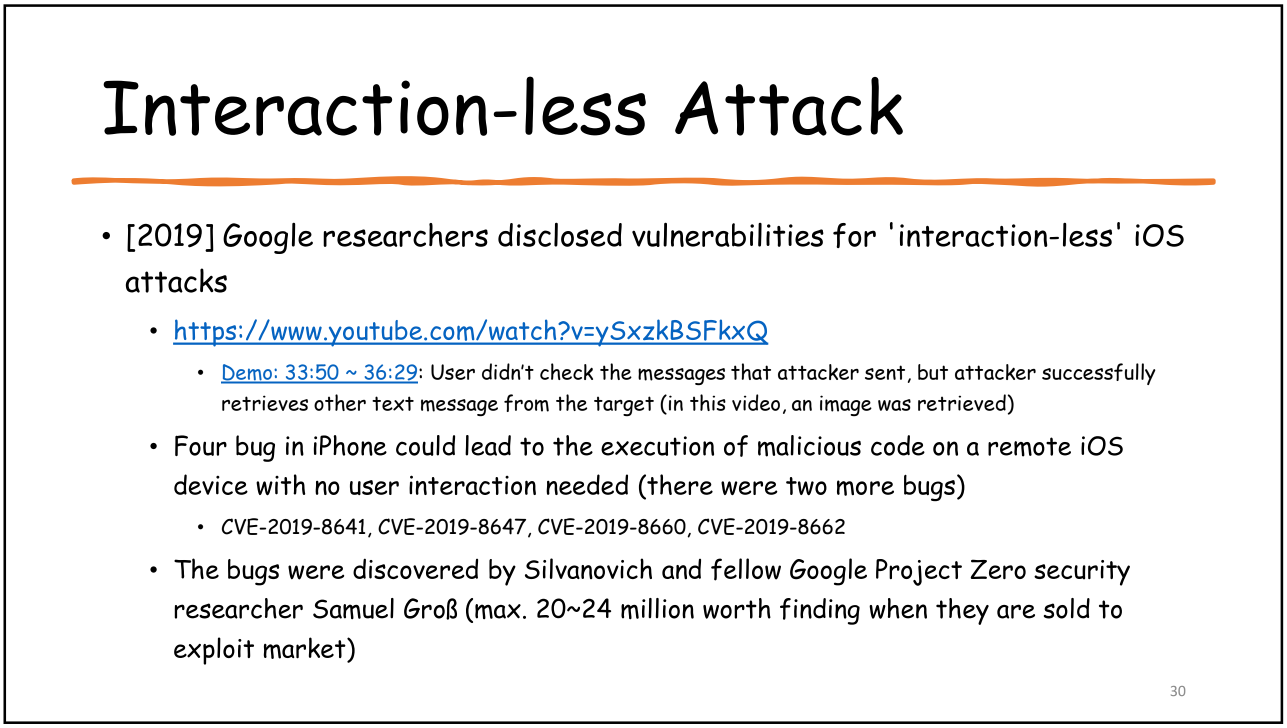
What's Inside?

- Personal course data and information
- Network with advisors, faculty and peers
- Email, calendaring, and address books: Use Google....
- Communities and Collaboration: Create, manage and join group homepages for clubs, affiliati
- Registration, grades, academic profile, transcripts, financial aid, pay fees & more

Languages:
English | Spanish | French | Portuguese (Brazil) | Arabic

29

29



Interaction-less Attack

- [2019] Google researchers disclosed vulnerabilities for 'interaction-less' iOS attacks
  - https://www.youtube.com/watch?v=ySxzkBSFkxQ
    - Demo: 33:50 ~ 36:29: User didn't check the messages that attacker sent, but attacker successfully retrieves other text message from the target (in this video, an image was retrieved)
  - Four bug in iPhone could lead to the execution of malicious code on a remote iOS device with no user interaction needed (there were two more bugs)
    - CVE-2019-8641, CVE-2019-8647, CVE-2019-8660, CVE-2019-8662
  - The bugs were discovered by Silvanovich and fellow Google Project Zero security researcher Samuel Groß (max. 20~24 million worth finding when they are sold to exploit market)

30