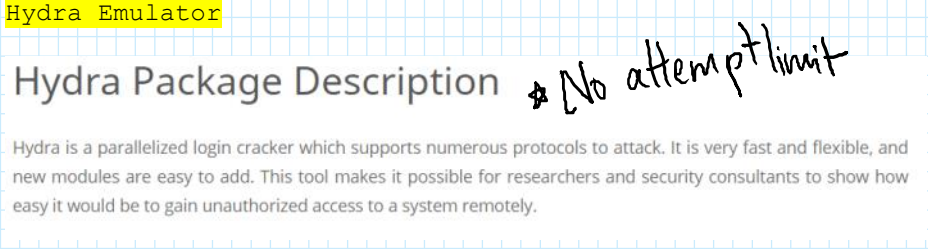
# Projects

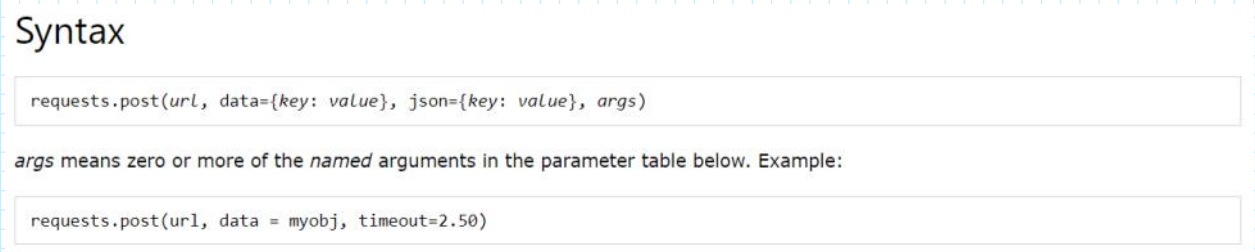
11 March 2021 17:17

1. Hydra Emulator




Screen clipping taken: 11-03-2021 17:23 source: https://tools.kali.org/password-attacks/hydra

Library used: requests




Screen clipping taken: 11-03-2021 17:30 source: https://www.w3schools.com/python/ref_requests_post.asp

How:

i. Send login data to server via a POST request. First try bruteforcing the username
ii. Analyze response. If response contains success string, move on to bruteforcing next parameter.
iii. Else: Try the next name in the dictionary.

2. CUPP Emulator


Screen clipping taken: 11-03-2021 17:33 Source: https://github.com/mebus/cupp.git

Library used: None, just strings and permutations

How:

i. Ask the user for information about the target, like name pet's name, fav sports team, date of birth, etc.
ii. Permute the strings received and generate a wordlist of all possible password combinations.
iii. Save it all to a text file.

Tool in action:

```
┌──(root💀BEESECHURGER)-[/mnt/d/College/python_in_hacking/Week4/cupp]
└─# python3 cupp.py -i
                         # Common
                         # User
                         # Passwords
                         # Profiler

                         [ Muris Kurgas | j0rgan@remote-exploit.org ]
                         [ Mebus | https://github.com/Mebus/]


[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Anthony
> Surname: Stark
> Nickname: Tony
> Birthdate (DDMMYYYY): 29051970


> Partners) name: Virginia Potts
> Partners) nickname: Pepper
> Partners) birthdate (DDMMYYYY): 10041972


> Child's name: Morgan
> Child's nickname: Stark
> Child's birthdate (DDMMYYYY):


> Pet's name: Jarvis
> Company name: Stark Industries


> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: ironman, arc reactor, AC/DC
> Do you want to add special chars at the end of words? Y/[N]: n
> Do you want to add some random numbers at the end of words? Y/[N]:
```

Screen clipping taken: 11-03-2021 17:39

This generates a text file called anthony.txt with a custom wordlist made out of all the details entered

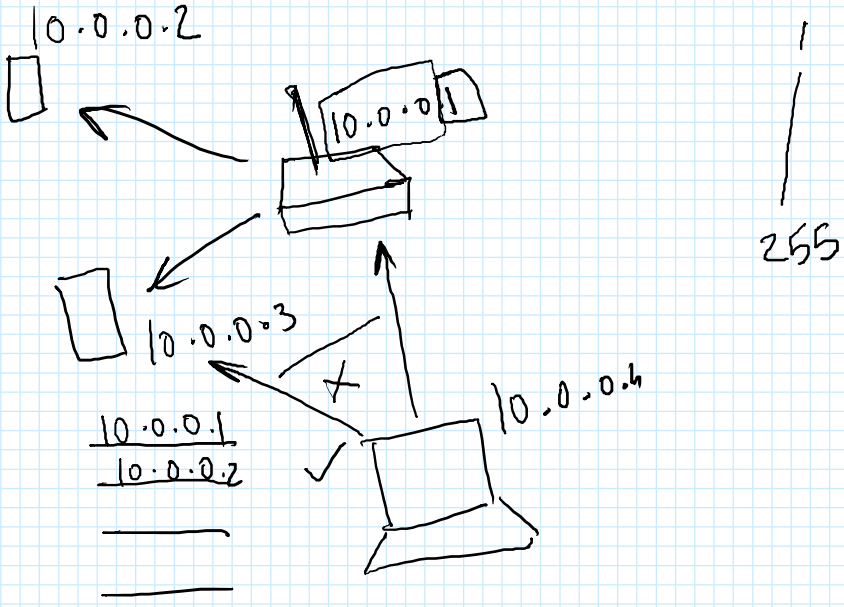
3. Network Scanner

Scan a network, tells what IP addresses are up

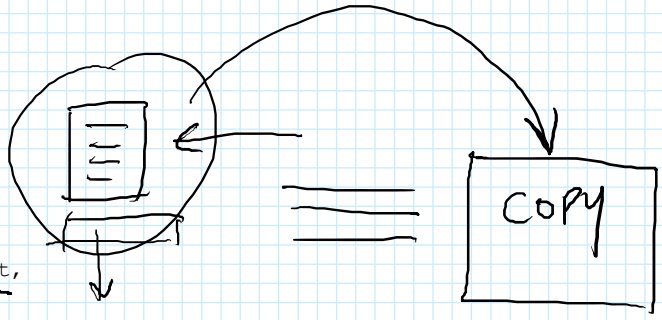
Library used: Sockets or networkscan

How:

i. Ask user to enter network ID (IP address of the network, last digit is zero)
   a. Example of network ID: 192.168.1.0, 10.0.0.0
ii. In a given network, hosts IP addresses have last number between 1 and 254
   a. Example: 192.168.0.1 to 192.168.0.254
iii. Iterate over all IPs in the network, and ping each one.
iv. If there is a response, that IP is up. Else, it is down.
v. Print all the IP addresses that are up.



4. Important Files Copier

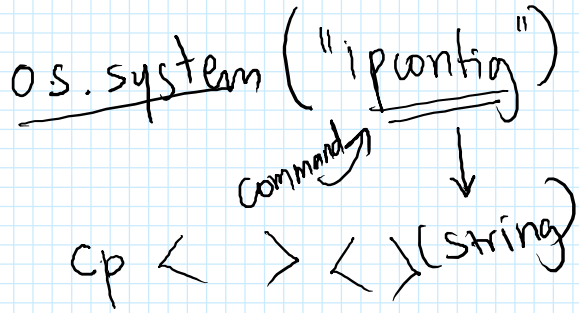



Just like Assignment 1, but instead of searching all files for interesting information, check file names!

Library used: os, regex (optional)

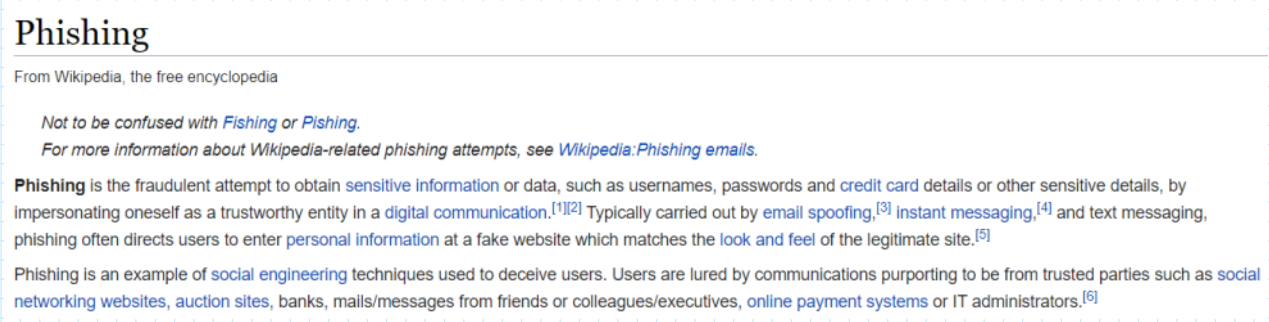
How:

i. Have a list of interesting file names (password.txt, do_not_open.txt, etc.)
ii. Perform recursive file traversal and read names of all files in all directories, check if that file name exists in your list.
iii. If exists, copy that file to a designated directory. Copying can be done two ways (possibly more):
   a. Use the shutil library:
      ```
      from shutil import copyfile
      copyfile(src, dst)
      ```
   b. Use os.system() to execute commands on the command prompt. You must have used the cp command in your Python Lab.




5. Phishing page

Create a phishing page for any website of your choice.



# Phishing

From Wikipedia, the free encyclopedia

*Not to be confused with Fishing or Pishing.*
*For more information about Wikipedia-related phishing attempts, see Wikipedia:Phishing emails.*

**Phishing** is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details or other sensitive details, by impersonating oneself as a trustworthy entity in a digital communication.[1][2] Typically carried out by email spoofing,[3] instant messaging,[4] and text messaging, phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.[5]

Phishing is an example of social engineering techniques used to deceive users. Users are lured by communications purporting to be from trusted parties such as social networking websites, auction sites, banks, mails/messages from friends or colleagues/executives, online payment systems or IT administrators.[6]

Screen clipping taken: 11-03-2021 18:02

Library used: flask, requests

How:

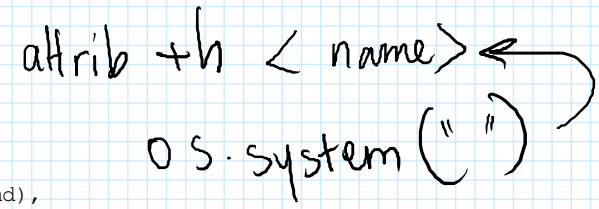
i. Create a web server using flask in python. (Source code put up on Microsoft Teams)


ii. The web page must have a login form that looks like that of your target.
iii. When a user enters their credentials in the fake page, your server will receive it. Print the credentials to your screen / save it to a text file.
iv. Redirect the user to the actual website.

6. Prank - Hide all files in the current directory

This is a prank that will hide all the files in the current directory. This will have the user believe that those files have been deleted.

Library used: os




How:

i. Get a list of all the files inside the target directory using os.walk().
ii. Now, there are two ways to go:
   a. If you are a Windows user, hiding a file in Windows can be done using the command (on cmd),
      Attrib +h <file/folder name>

Once you have a list of all files, you can iterate over them, and use the os.system() function to execute the above command for each file.

b. If you are using Linux, any file whose name starts with a . (dot) is hidden. So all you have to do is rename each file.
You can do that using two ways:
   i. Using os.rename()
      os.rename(file_name, new_file_name) will rename a file called file_name to new_file_name.
   ii. Using the terminal command mv:
      mv old_name new_name will rename a file called old_name to new_name.

.bashrc

a.txt → .a.txt

7. Prank - Shut down the system

This is a slightly more complicated tool, as it will require knowledge of bash / batch scripting, depending on your target os.

Library used: os, batch/bash scripting (not a library)

How:
i. Find out what's the command to shut down a system in your target system.
   a. Linux: sudo init 0 (or) shutdown <options>
   b. Windows: shutdown /s
   You can play around with the options to shut down the system at a certain time, or after a certain duration.
ii. Then you gotta figure out how to run this script every time the system boots.
iii. WARNING: DO NOT run this on your host machine, use a vm in case you don't configure the shutdown time properly and your computer shuts down right after you boot it.
iv. Fun: In Windows, you can show alert messages before shutdown the machine, kinda like the low battery warnings. For extra effect, you can play around with that!

Shutdown now → IMMEDIATELY

8. Anything done in class

Your project can be any tool we discussed in class. But, it should:
i. Have a presentable output
ii. Handle errors gracefully
iii. Validate input

] MUST

Additionally, you can make anything else too!

Grading:
20 Marks for Presentation
20 Marks for Content → Where use?
60 Marks for the Project → Skill + execution

Submission:
On Microsoft Teams
Submit a video as:
a. Direct upload
b. Drive link
c. Compressed zip file containing the video

You can Google stuff, but do not copy stuff as is, either from Google, your peers, or the code uploaded on Teams. Plagiarism is not allowed

1th March – 17th March