**PROBLEM STATEMENT:**

4. Install Social Phish tool from GitHub and try to execute the tool for phishing page and perfrom in lab setup only .

**SOLUTION:**

**WHAT IS PHISHING?**

**Phishing** is probably one of the biggest issues for most organizations today, with network and endpoint defensive technology getting better and better, the bad guys aren’t trying to go after the though route and instead of going for the low hanging fruit. Phishing is one of those issues where training the employees is your best defence – try your best to make sure they can spot a malicious email and make sure that they can report it easily so that appropriate action can be taken as quickly as possible. The train of thought behind saying this is that – it’s beneficial to depend on multiple nodes of human intelligence to spot a potential threat, because even if one person spots and reports a phishing mail, it’s possible to run mass searches and find who all were targeted by a campaign.

**STEPS:**

Shellphish is fairly straight forward to install. It can be done on your Linux of choice, we will be using Kali. We fire up our Kali Linux and use the terminal to navigate to the desktop.

|  |  |
| --- | --- |
| **1** | **cd Desktop** |

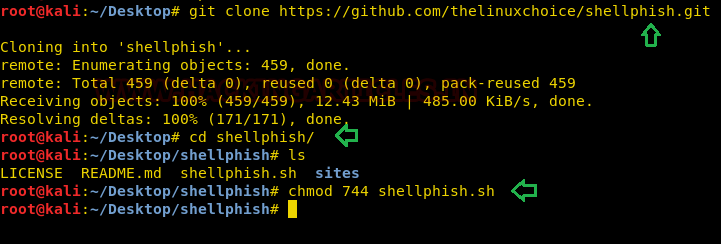
We need to clone the ShellPhish from GitHub, the download link is provided below.



|  |  |  |  |
| --- | --- | --- | --- |
| 1 | **git clone** [**https://github.com/thelinuxchoice/shellphish.git**](https://github.com/thelinuxchoice/shellphish.git)**.**  **This makes a folder named “shellphish” on our desktop. Let’s check the folder and its contents.**     |  |  | | --- | --- | | 1  2  3 | ls  cd shellphish/  ls | |

The next step is to change the permissions of the shellphish.sh file so that we as the admin can use it. We don’t want everyone to have open access to it.

|  |  |
| --- | --- |
| 1 | chmod 744 shellphish.sh |



And that’s it, now we can launch our phishing tool



|  |  |
| --- | --- |
| 1 | ./shellphish.sh  SOCIAL2.png  **Exploring Templates:**  ShellPhish offers us 18 prebuilt templates, we will look through 3 of them to get an idea of what someone on the receiving end looks at when they get a link generated by this tool.  Get the Instagram page. The platform needs no introduction. We can see what the malicious link leads to, the page it shows is very convincing and might easily fool someone who isn’t paying attention.  SOCIAL3.png |

Similarly, you can generate another duplicate page i.e NETFLIX as shown below.

