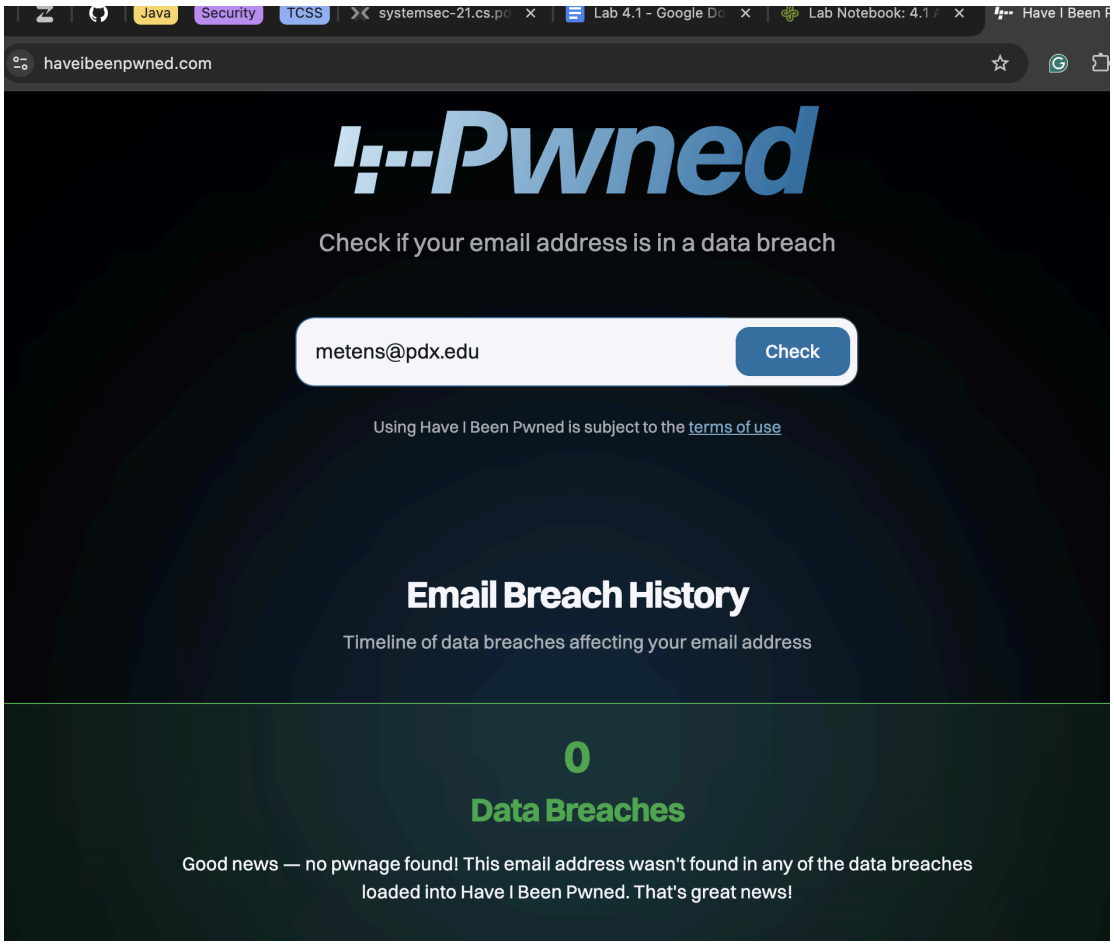
Lab 4.1

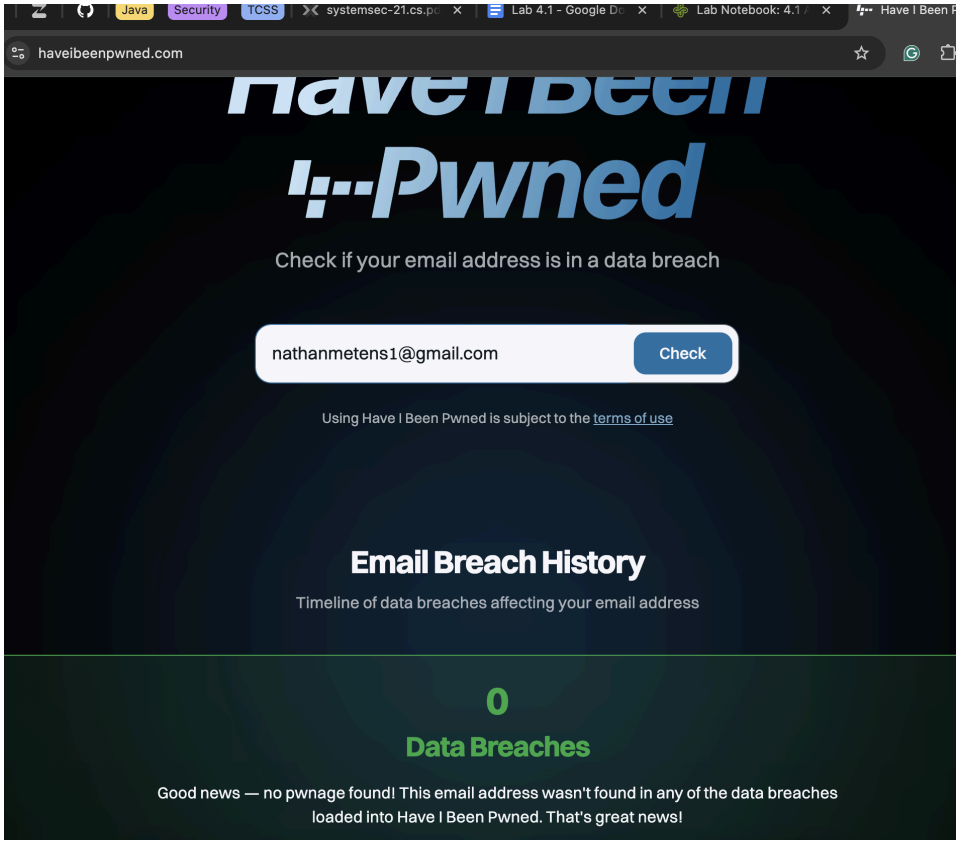
By: Nathan Metens (metens@pdx.edu)

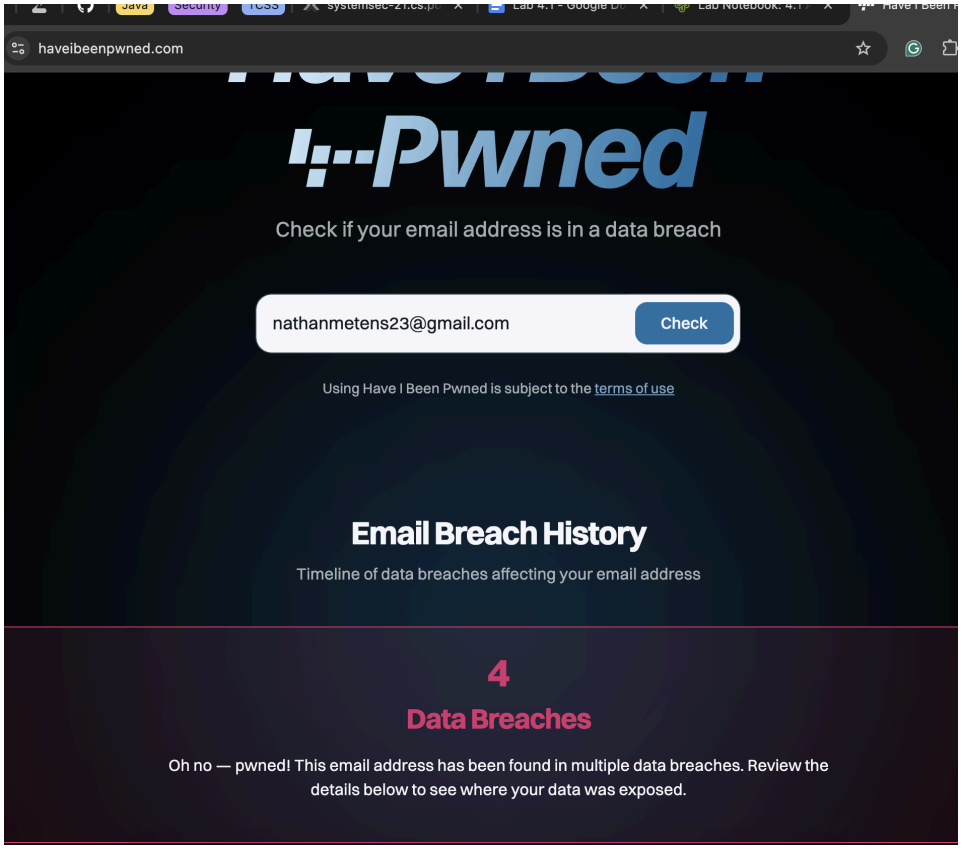
***Note**: My laptop was unable to connect to PSU Secure WiFi or PSU Guest for about 3 hours after class. I had to redownload the Kali VM on ProxMox, where I'm doing DevOps with Kevin, so I was using the "student" account instead of my Kali Linux account. I included a notepad with my Odin ID on the bottom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

1. HaveIBeenPwned

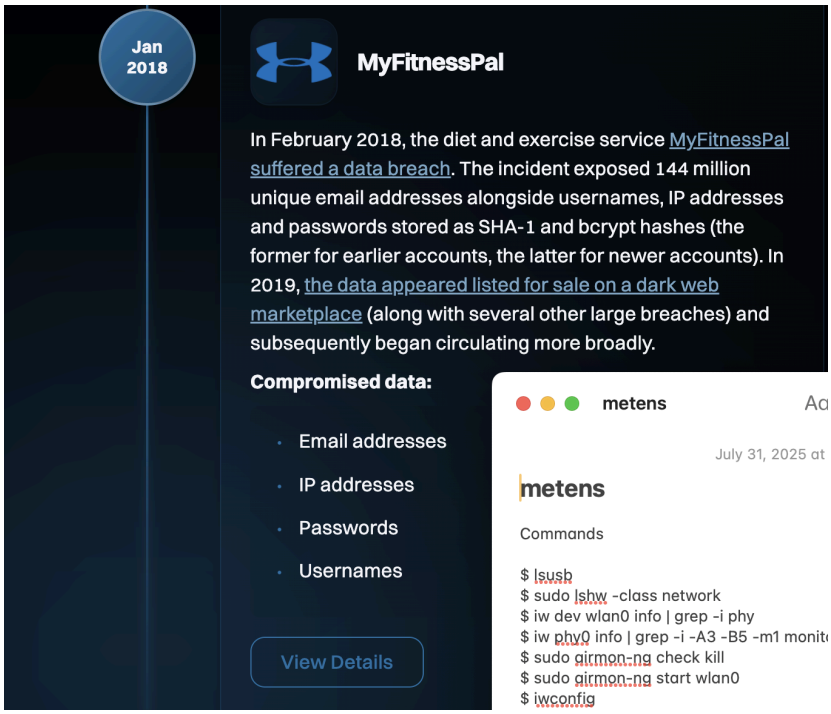
I visited https://haveibeenpwned.com/ and typed in three of my emails: metens@pdx.edu, nathanmetens1@gmail.com, and nathanmetens23@gmail.com. Out of those 3, only nathanmetens23@gmail.com was breached:

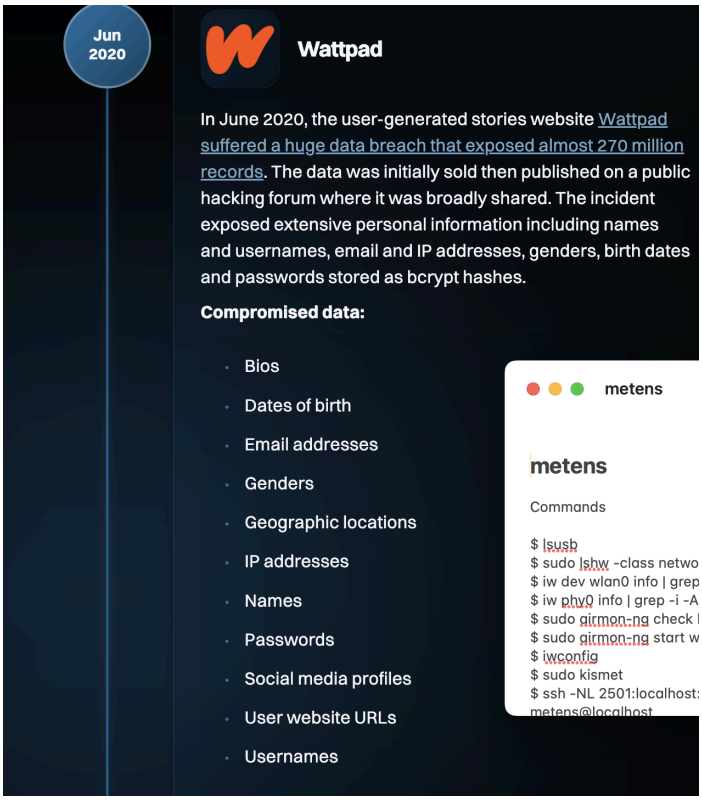


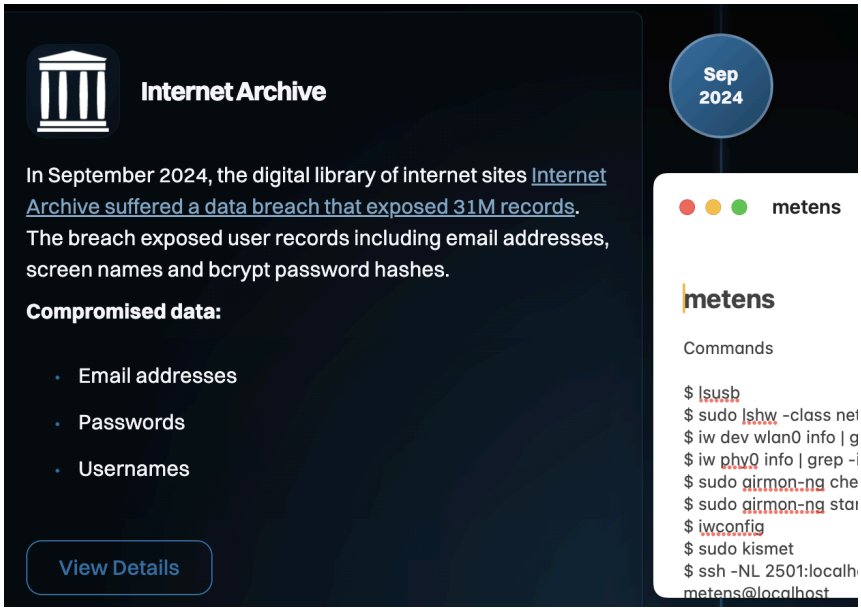

haveibeenpwned.com
Have I Been Pwned
Check if your email address is in a data breach
nathanmetens1@gmail.com
Check
Using Have I Been Pwned is subject to the terms of use
Email Breach History
Timeline of data breaches affecting your email address
0
Data Breaches
Good news — no pwnage found! This email address wasn't found in any of the data breaches loaded into Have I Been Pwned. That's great news!

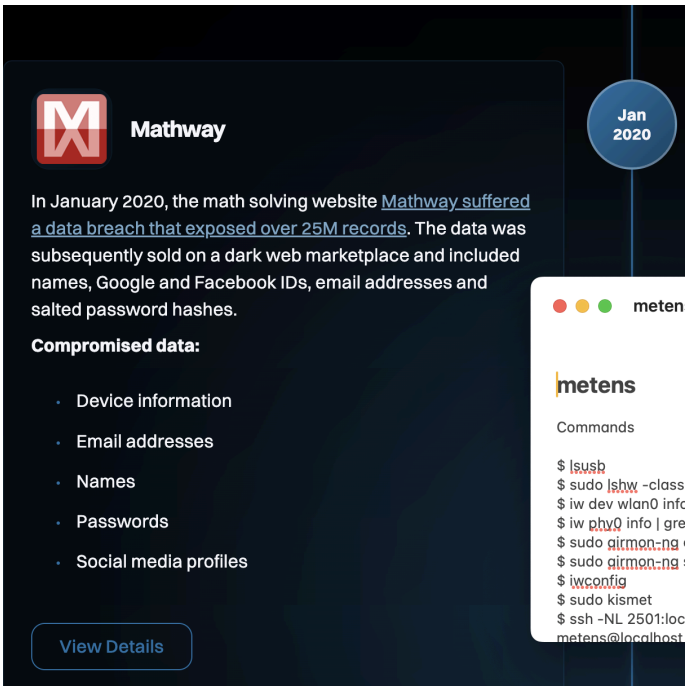

haveibeenpwned.com
Have I Been Pwned
Check if your email address is in a data breach
nathanmetens23@gmail.com
Check
Using Have I Been Pwned is subject to the terms of use
Email Breach History
Timeline of data breaches affecting your email address
4
Data Breaches
Oh no — pwned! This email address has 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:







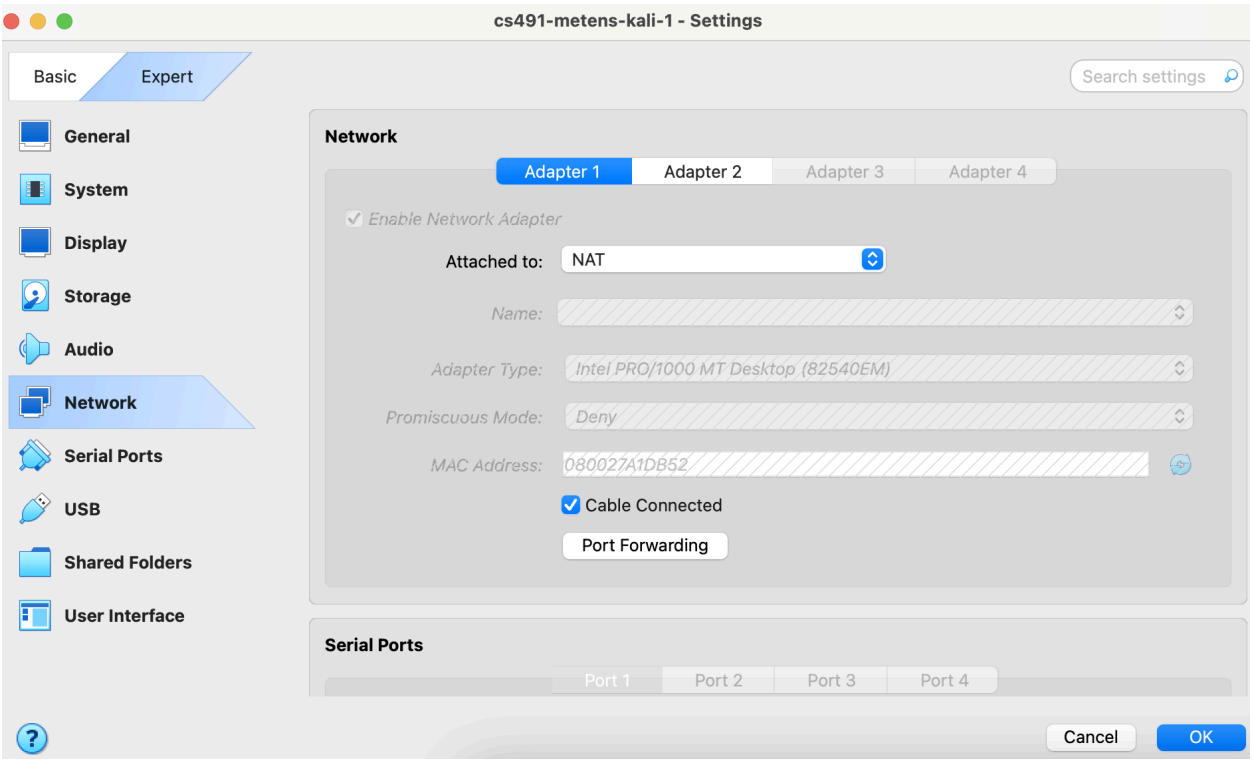


Next, I visited https://haveibeenpwned.com/Passwords and looked up the following passwords:

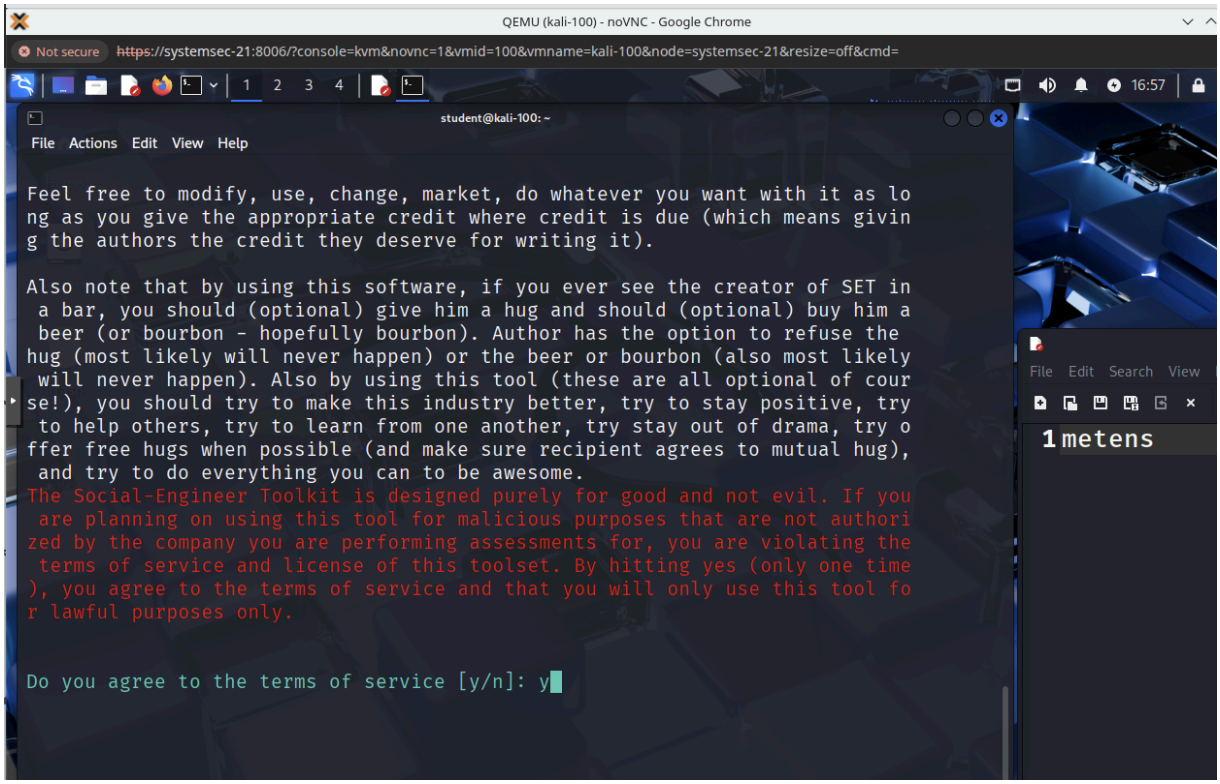
1. 111111 -> This password has been seen **9,054,376** times before in data breaches!
2. 1234567890 -> This password has been seen **10,236,756** times before in data breaches!
3. Iloveyou -> This password has been seen **49,387** times before in data breaches!
4. qwerty123 -> This password has been 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.

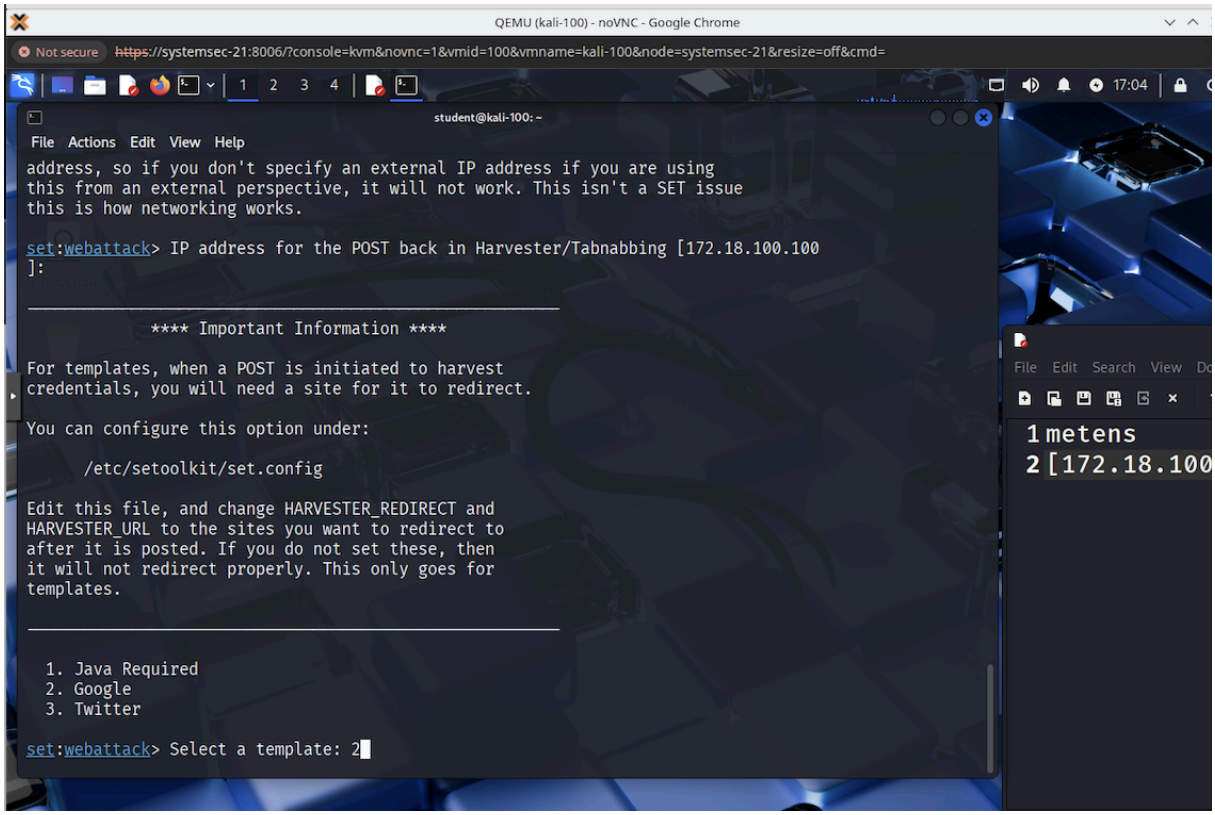
2. Social Engineer Toolkit (SET) - Google



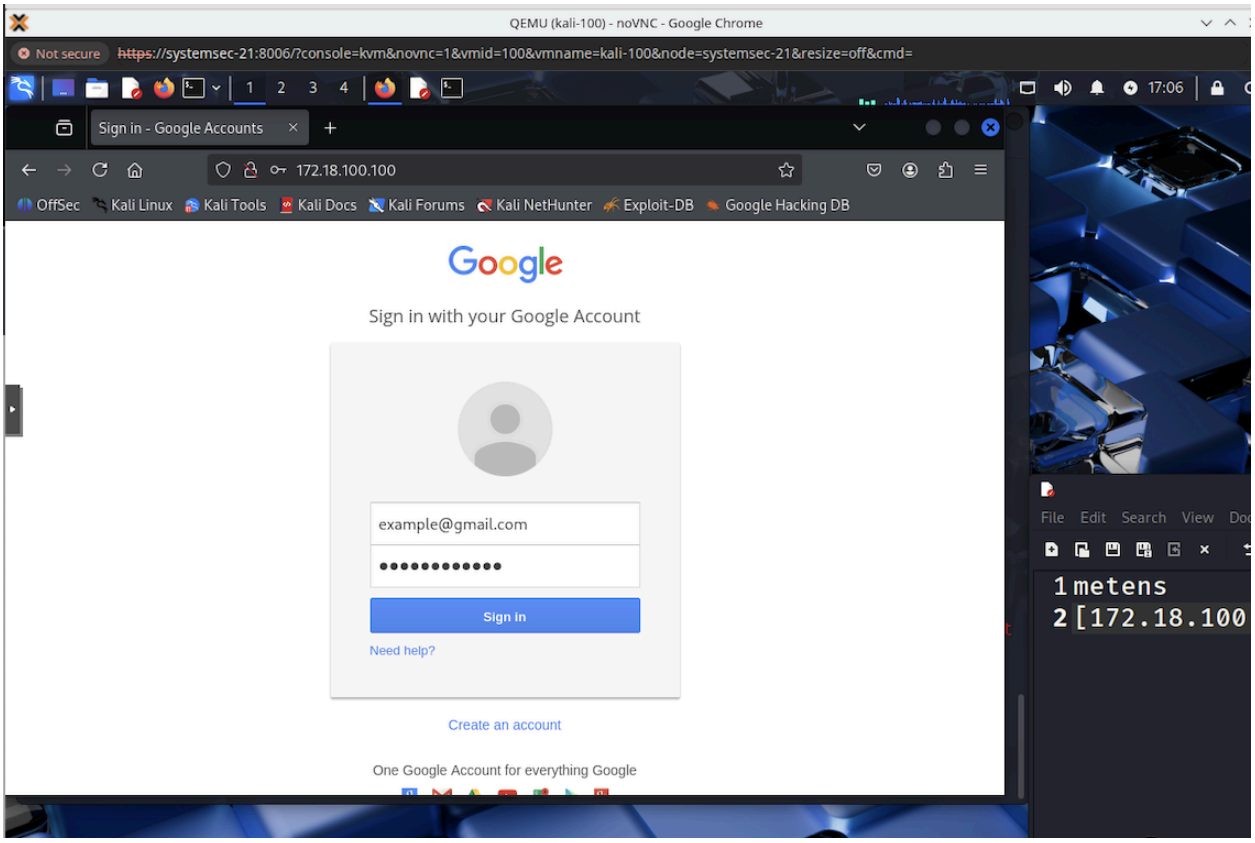
To get `setoolkit`, I first installed it in my Kali VM, then ran `sudo setoolkit`. I acknowledge the terms and conditions:

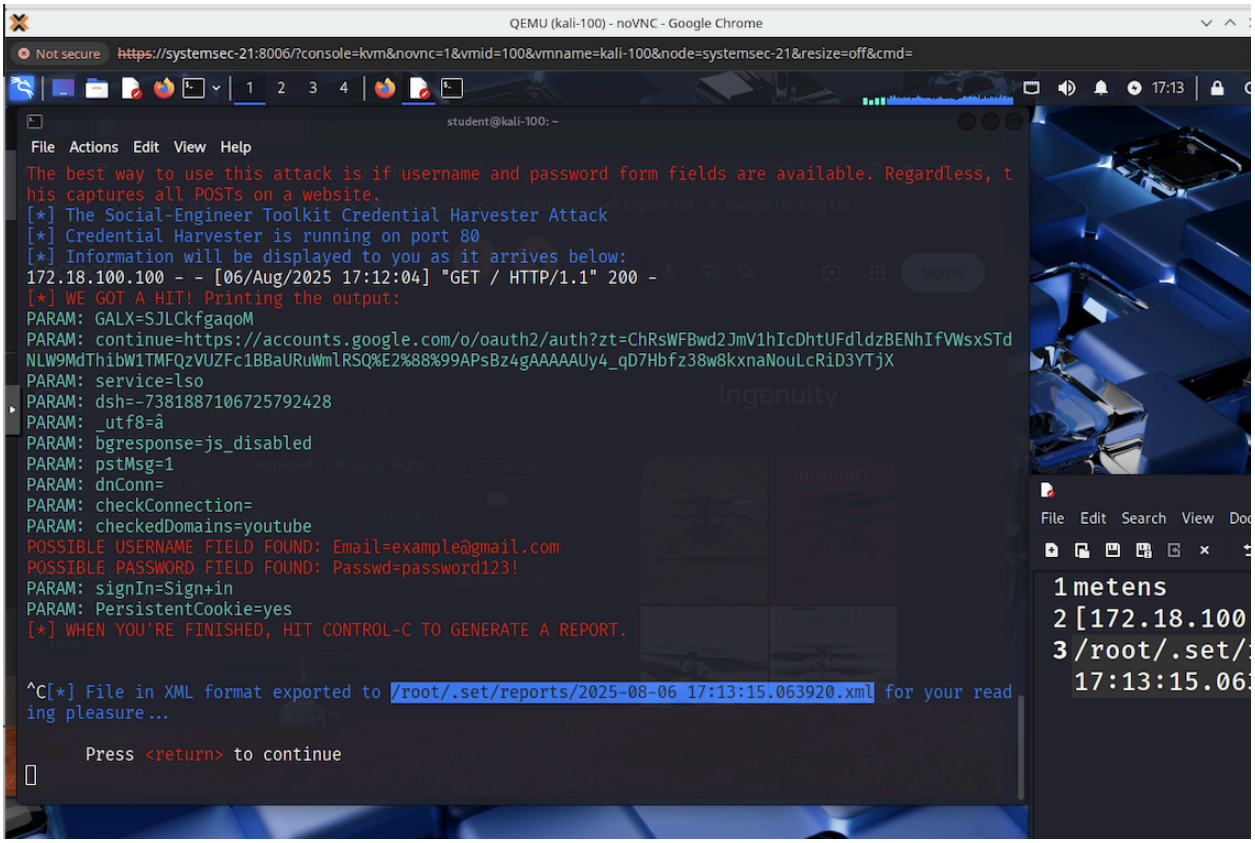


I navigated to the right spit in the toolkit:

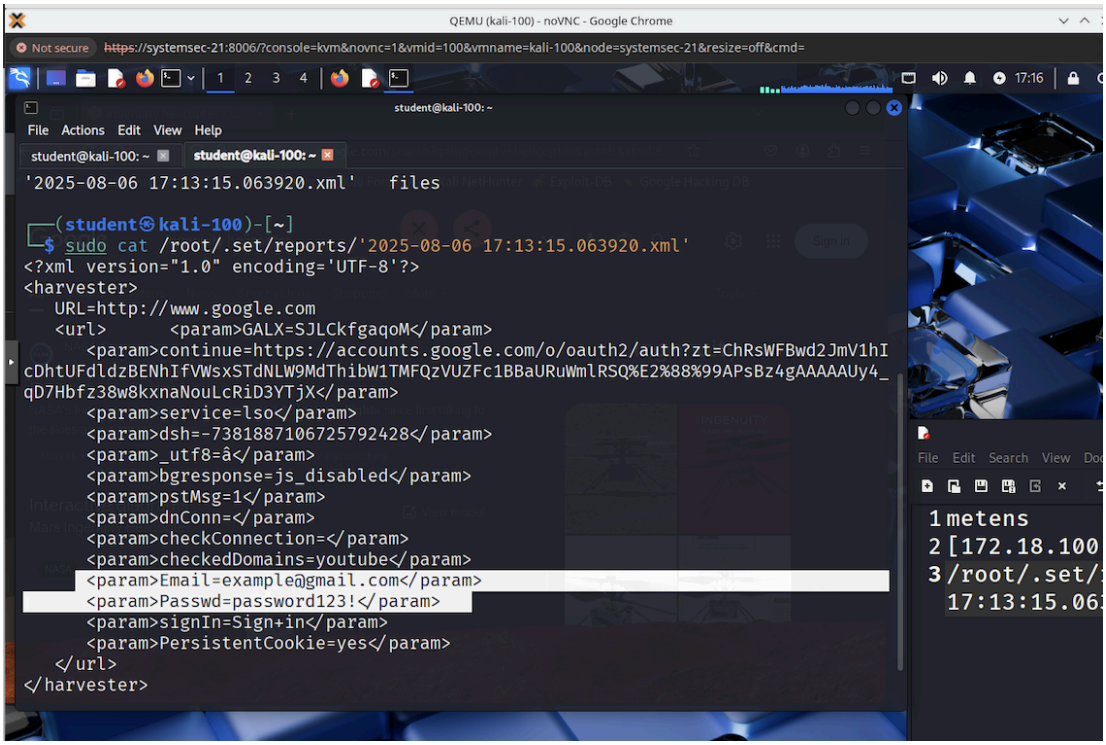


I navigated to the URL `172.18.100.100`:


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=
Sign in - Google Accounts
172.18.100.100
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Google
Sign in with your Google Account
example@gmail.com
Sign in
Need help?
Create an account
One Google Account for everything Google
17:06
File Edit Search View
1 metens
2 [172.18.100

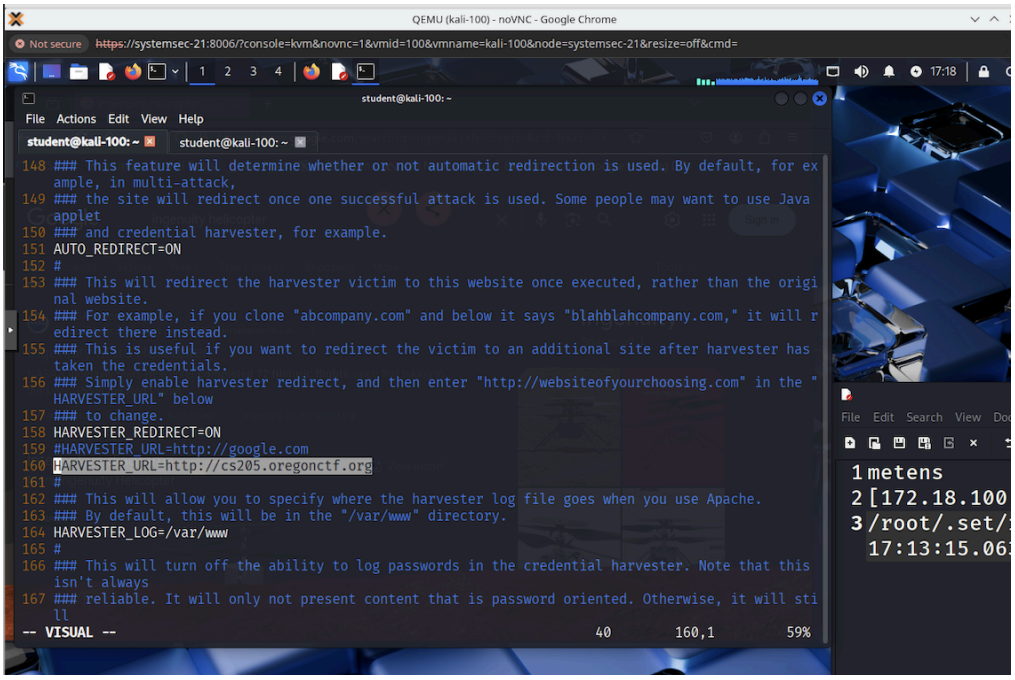

QEMU (kali-100) - noVNC - Google Chrome
Not secure
https://systemsec-21:8006/?console=kvm&novnc=1&vmid=100&vmname=kali-100&node=systemsec-21&resize=off&cmd=
17:13
student@kali-100: ~
File Actions Edit View Help
The best way to use this attack is if username and password form fields are available. Regardless, t
his 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:
172.18.100.100 - - [06/Aug/2025 17:12:04] "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=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTd
NLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7318887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=example@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=password123!
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
^C[*] File in XML format exported to /root/.set/reports/2025-08-06 17:13:15.063920.xml for your read
ing pleasure...
Press <return> to continue
File Edit Search View
1 metens
2 [172.18.100
3 /root/.set/
17:13:15.06

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

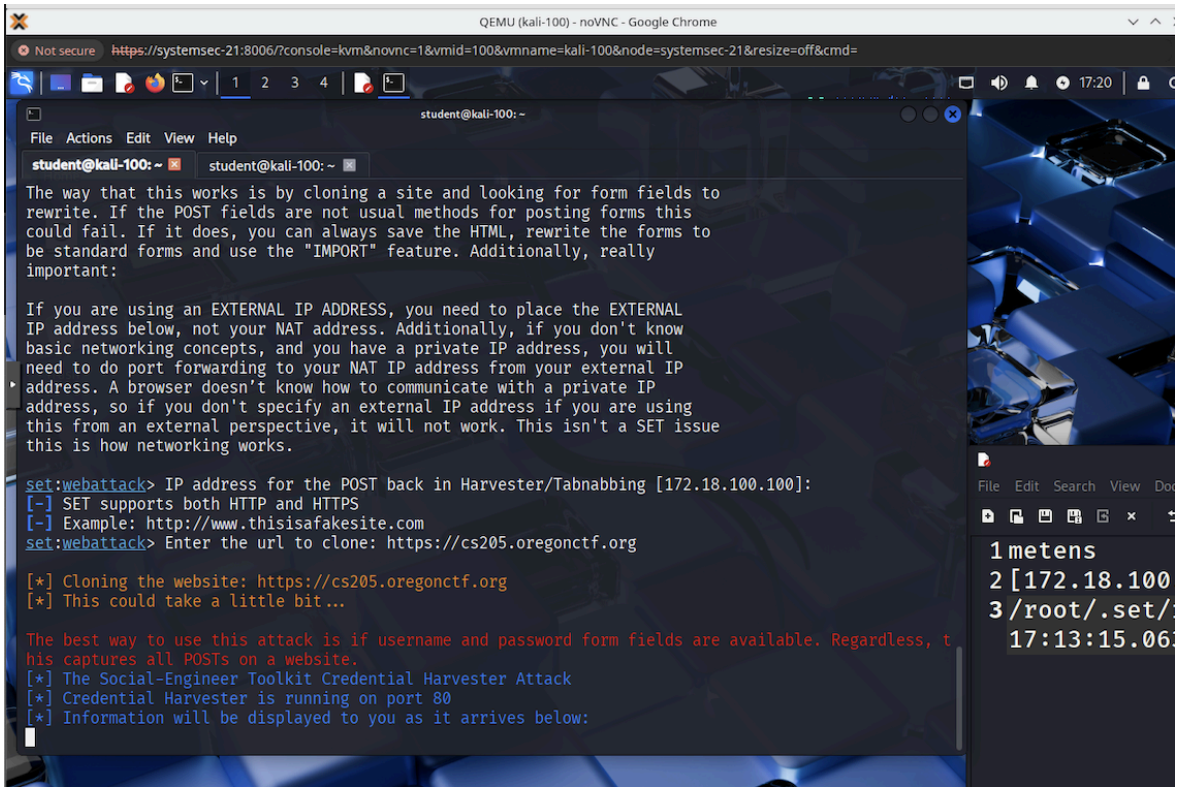


3. Social Engineer Toolkit (SET) – OregonCTF

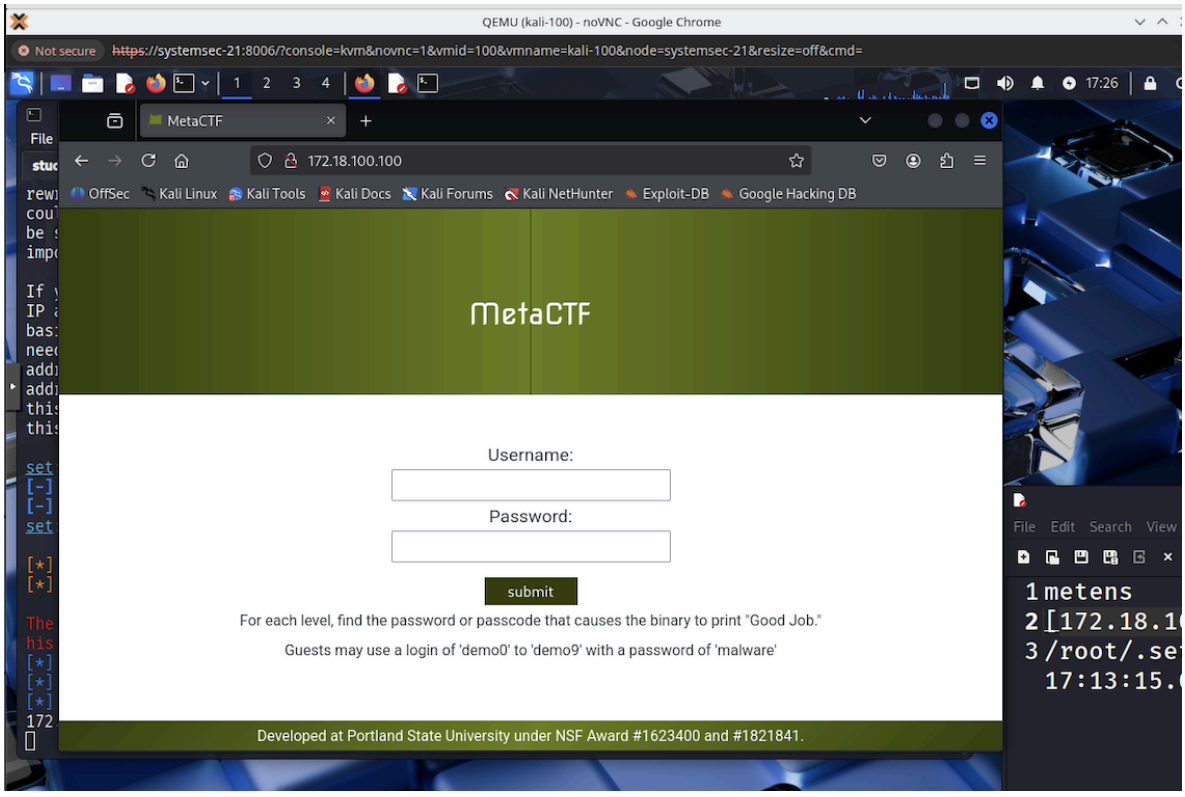
First, I changed the `/etc/setoolkit/set.config` file:



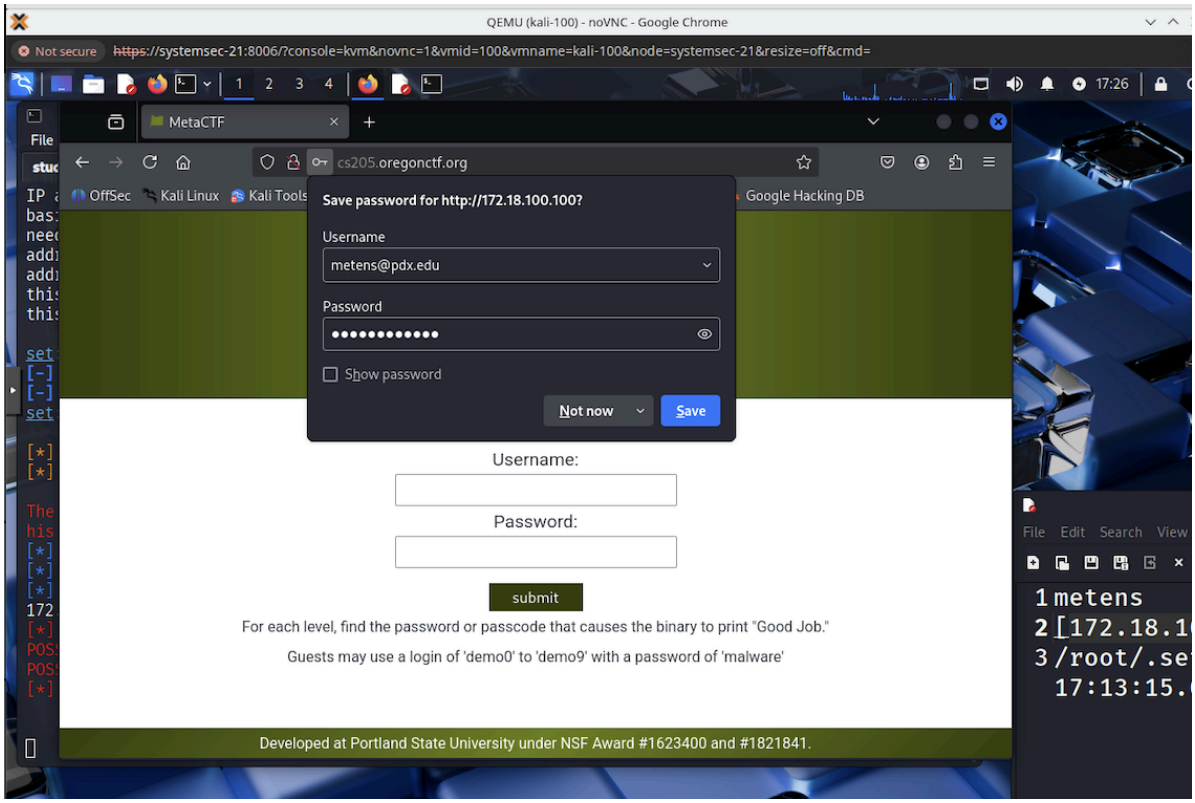
Then I navigated to the site cloner and imputed the oregonctf URL to clone:



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: