Penetration Test Project

ECE 222 Development

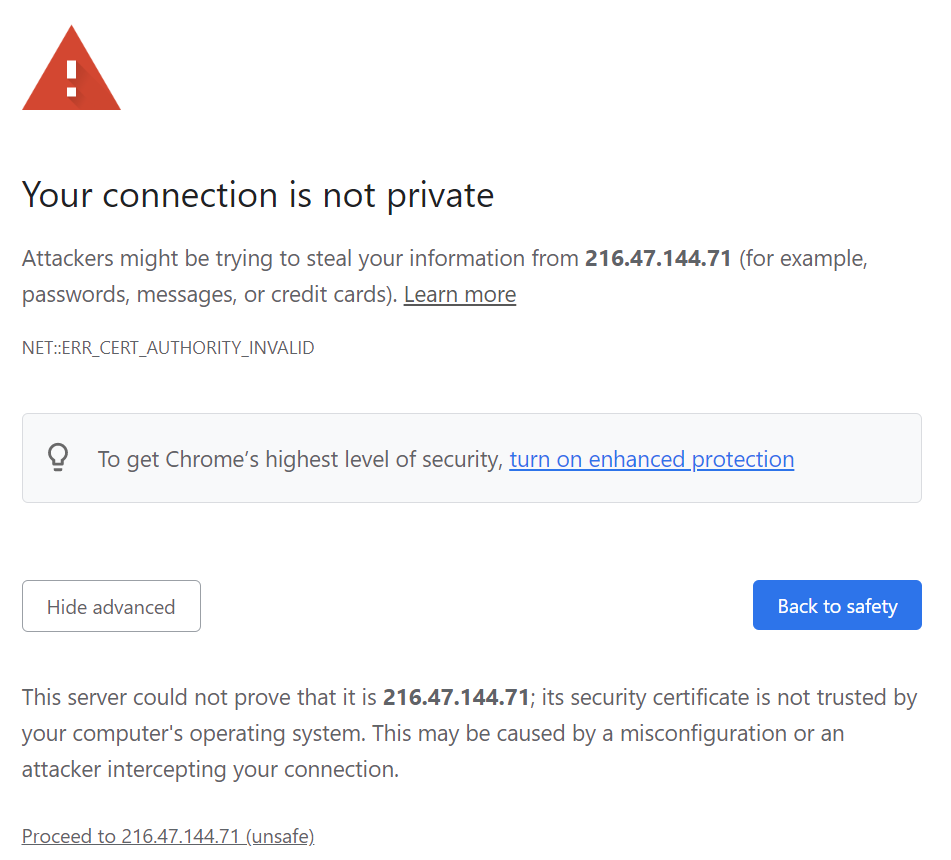
Spring 2023

# Student Objectives

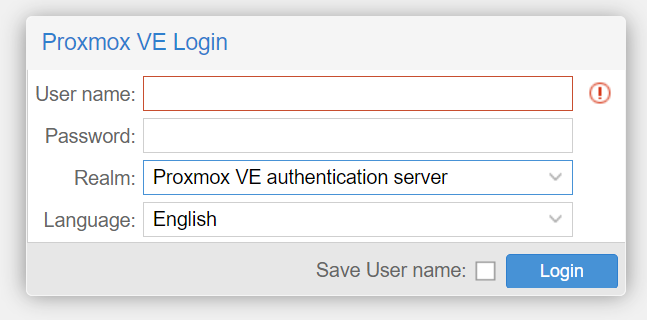
Students will apply the basic principles of a Penetration Test. Students should be able to conduct basic scans of a target machine in order to identify weak spots. After completing the necessary scans, research will be conducted to identify exploits to gain access to the target machine. Proof of access should be provided through the contents of a file on the target machine.

# Environment Access

In order to access the project environment, please navigate to <https://216.47.144.71> (at the moment we don’t have a domain name assigned to this machine). Since we don’t have an SSL certificate you will get a message from your browser warning you about the connection, but please just proceed.



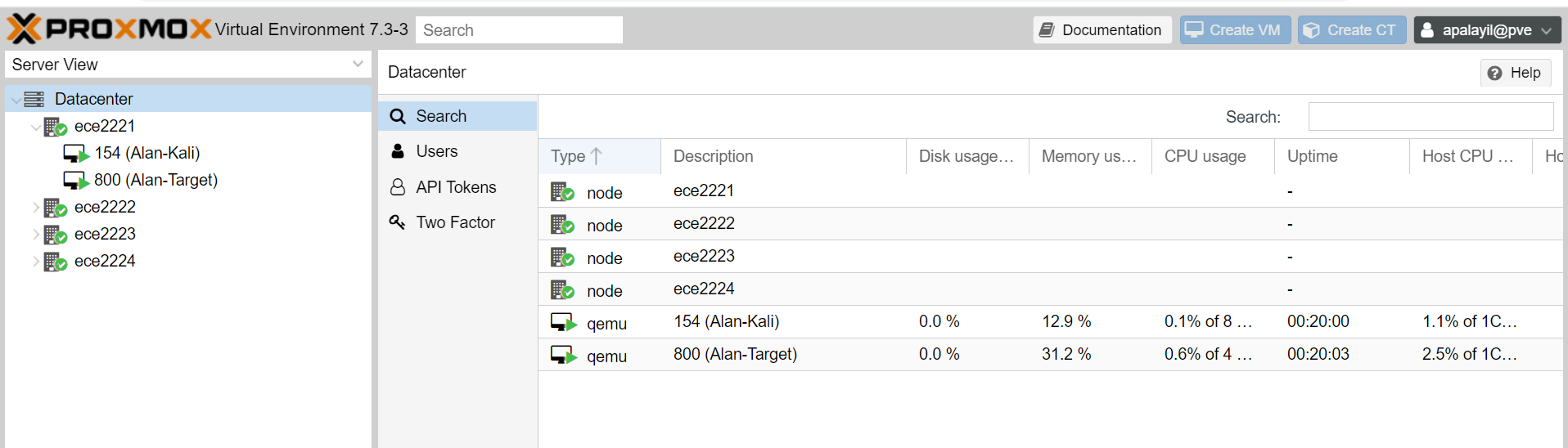
After proceeding to the website, you’ll be greeted with the login page like this:



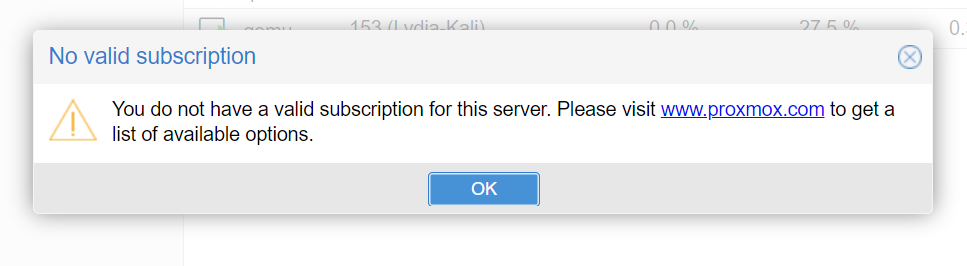
Change the “Realm” to “Proxmox VE authentication server” and enter your credentials (this is being added for ECE 497, in the future the students will be directly contacted with their credentials)

|  |  |  |  |
| --- | --- | --- | --- |
| Username | Password | Kali Machine IP | Target IP |
| mostrowski | 2W3E3ZqdxJ | 10.10.10.12 | 10.10.10.2 |
| apalayil | WNAgksuQm9 | 10.10.10.14 | 10.10.10.4 |

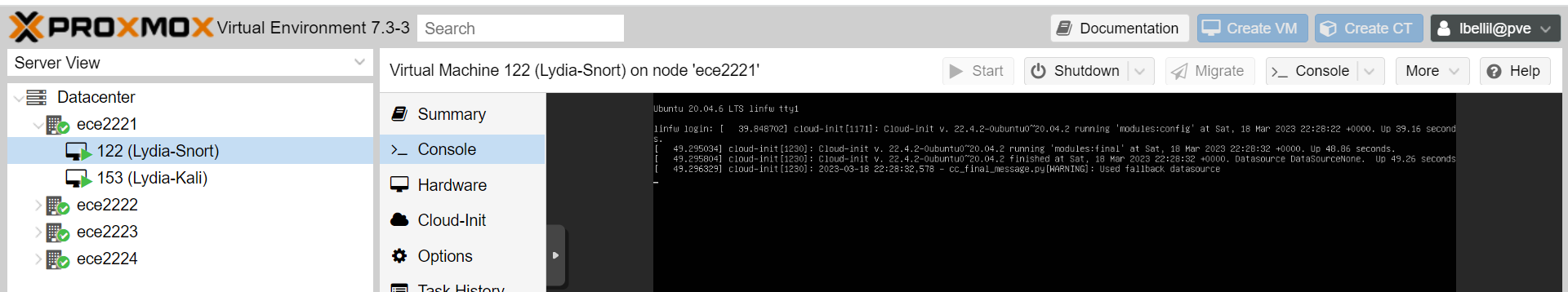
After logging in, you should see something like this:



If it warns you that you don’t have a subscription, just click OK.



In order to access your environments, you’ll do everything via the browser (so note that you won’t be able to copy and paste from the terminal). To get there, just click on the machine you want to work on and then go to “console” (you can get a full screen version by double clicking).



# Instructions

1. Log into your Kali Linux machine and conduct an nmap scan of the target
   1. Kali Linux Credentials:
      1. Username – kali
      2. Password – kali
   2. Suggested nmap scan

nmap -T4 -A -Pn <ip>

* 1. Take a screenshot of the scan results and consider:
     1. What ports are listening?
     2. What are the services that nmap has identified?

1. Based on your results from step 1, start to investigate the services and ports listed. What if you see the following?
   1. FTP Server – can you log in anonymously?
   2. Website – Is there a login portal? Is it running a known software (like Jenkins?)?
      1. If you don’t see anything initially what tools are useful to enumerate the potential domain names?
   3. Samba File Share – can you log in anonymously?
2. Hints for Alan & Matt (won’t be distributed to the students):
   1. Alan –
      1. Is there anything interesting in the FTP server?
      2. If so, where can you use the information that’s provided?
      3. If you can transfer a file to the target, how can you get it to spawn a shell for you?
   2. Matt –
      1. What are the services that you’ve enumerated and do they return anything via searchsploit?
      2. If you find a script to exploit a vulnerability, what are potential ways you need to modify it or use the -h function to find out different command line arguments?
      3. NOTE – the exploit in your case uses a swear word, please communicate with me and we’ll work on blurring that in your final video.
3. After gaining initial access to the machine, look for the file /tmp/flag.txt and take a screenshot
4. Also, if you don’t have root, how would you go about escalating your privileges?

# Deliverables

Students in ECE 222 will be required to submit a report that includes the following:

* Introduction
  + Discuss the steps in a Penetration Test
  + Provide a description of the tools you used during your Penetration Test
* Scanning and Enumeration
  + Provide a screenshot of your nmap scans of the target
  + Discuss the listening ports identified by nmap
    - If a service is identified, what is it responsible for?
    - What potential exploits are associated with the vulnerability
* Exploitation
  + What steps did you take to gain access to the target?
    - If applicable, where did you find the exploit?
    - Did you need to make any modifications to the exploit?
  + Provide a screenshot of the contents of the file /tmp/flag.txt

**Students in ECE 497 should do the following:**

* Follow the *Environment Access* and *Instructions* sections to familiarize yourself with the steps our ECE 222 students will need to complete.
  + Take notes regarding your experience:
    - Was it easy to get into the environment?
    - Are the instructions clear and were you able to follow them?
    - What suggestions for improvement do you have?
  + We’ll discuss your notes and feedback as a group near the end of the semester.
* Record an introductory video explaining how to access the environment and completing the necessary steps as part of the project. Your video should include:
  + How to access the environment
  + How to interact with your Kali machine
  + How to scan the target
  + How to conduct research based on the scan results
  + How to use Metasploit or manual exploits to gain access to the target
  + Gaining access to the target and obtaining the /tmp/flag.txt flag