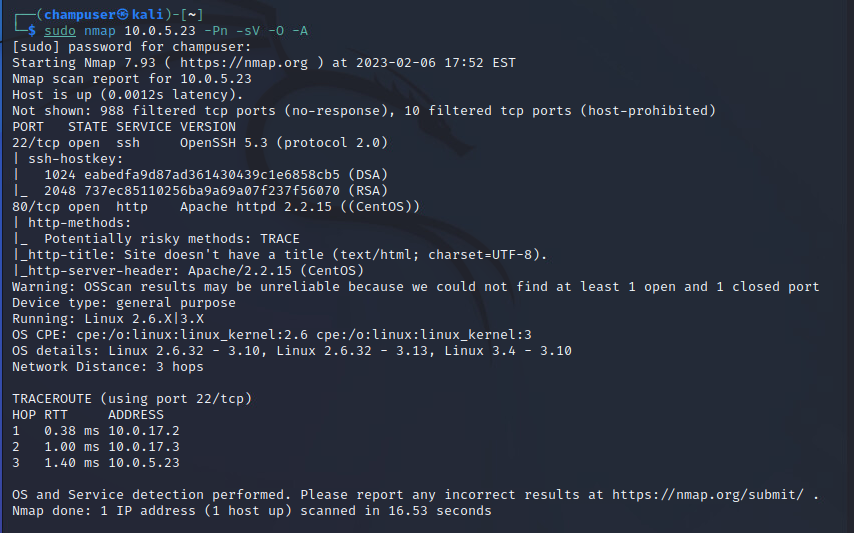
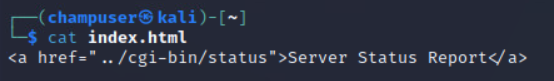
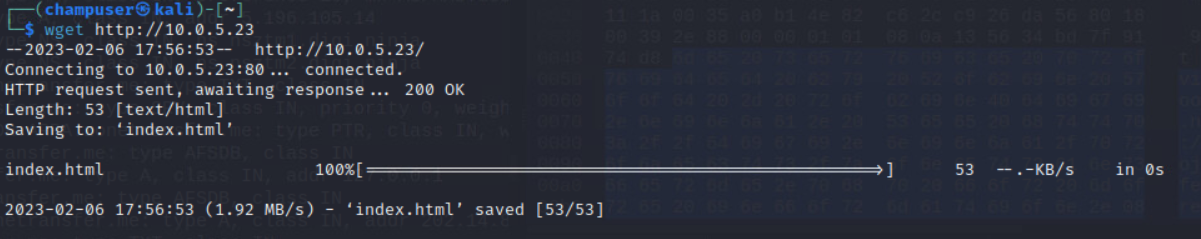
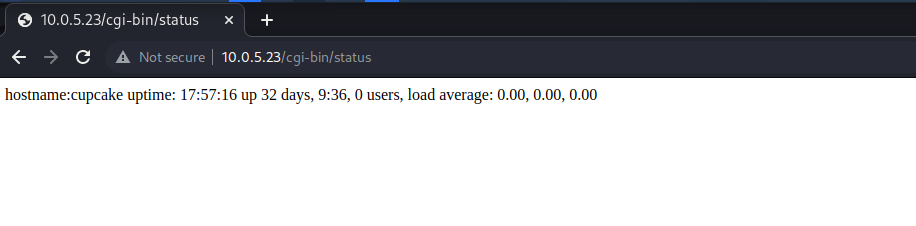
David Thomsen

Max Gallagher

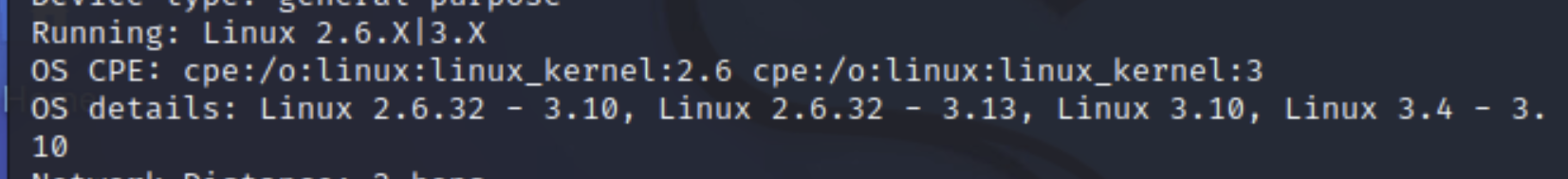
Deliverable 1. Provide a screenshot of your team's version detection scan(s).

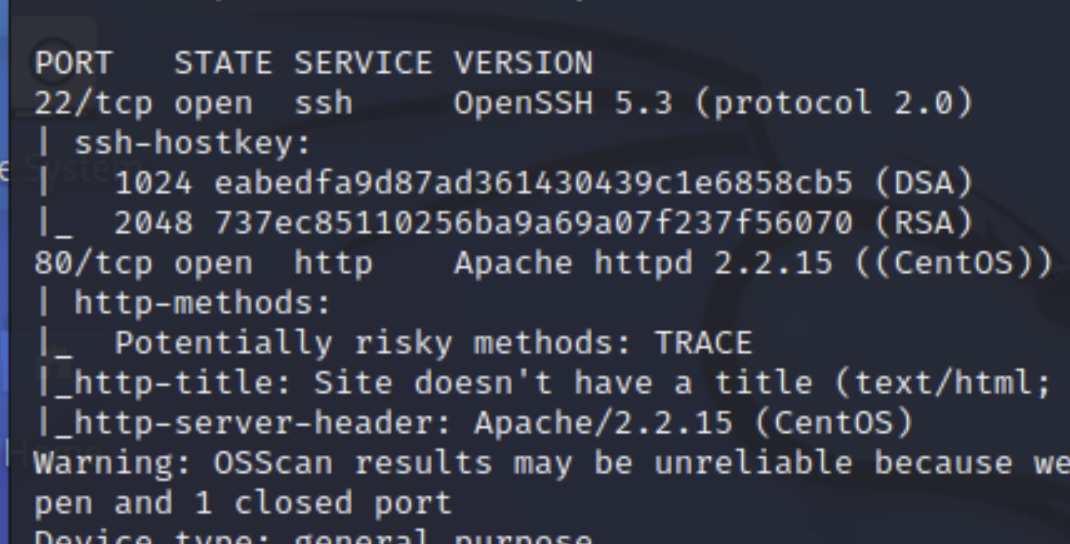
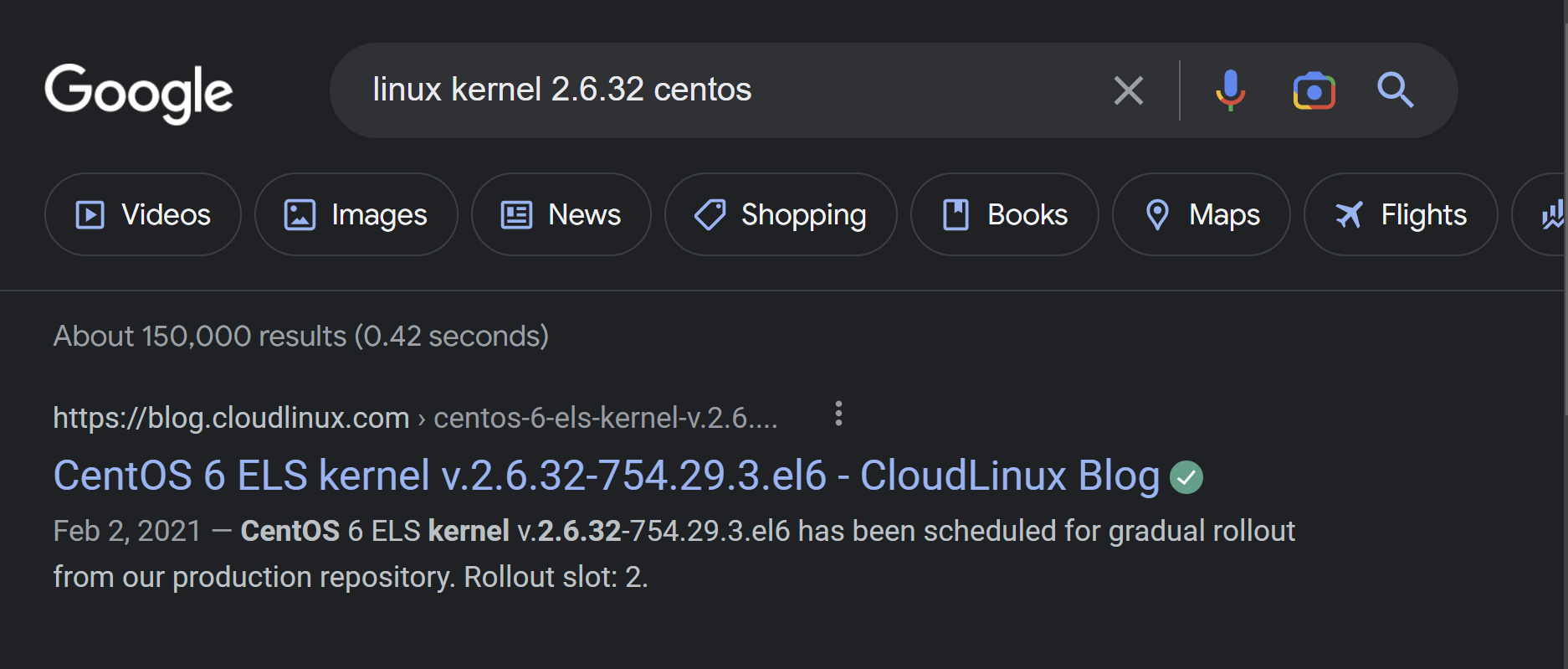


Deliverable 2. Examine any applications that are publicly accessible. What did you find?

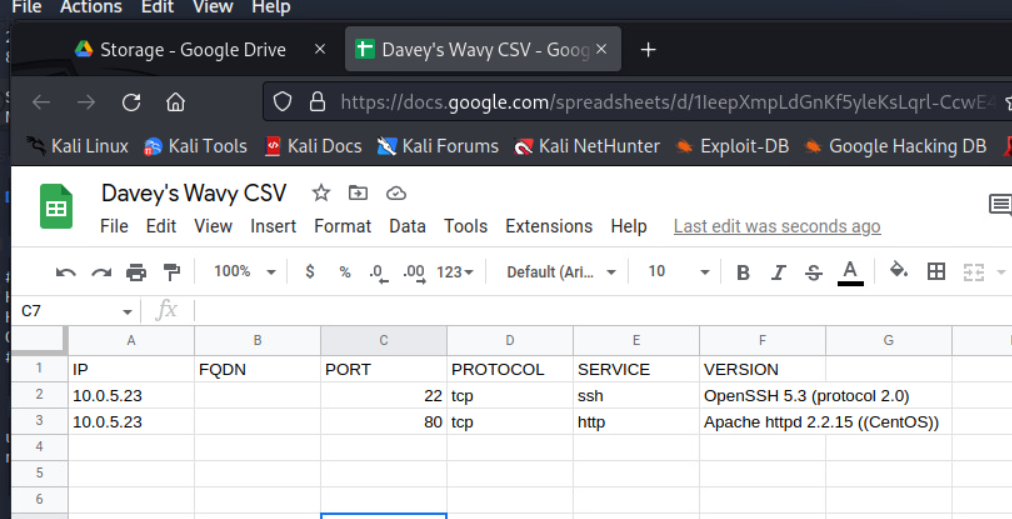
Deliverable 3. You should have the versions of at least two applications. Go ahead and hit the internet and see if your group can find:

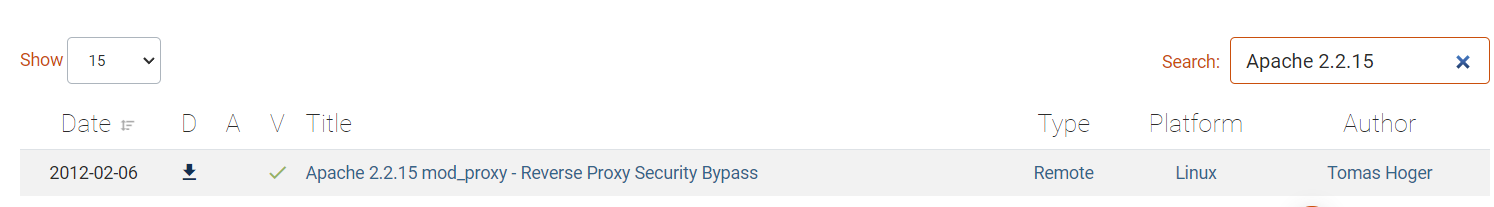
1. The operating system (this is easy)

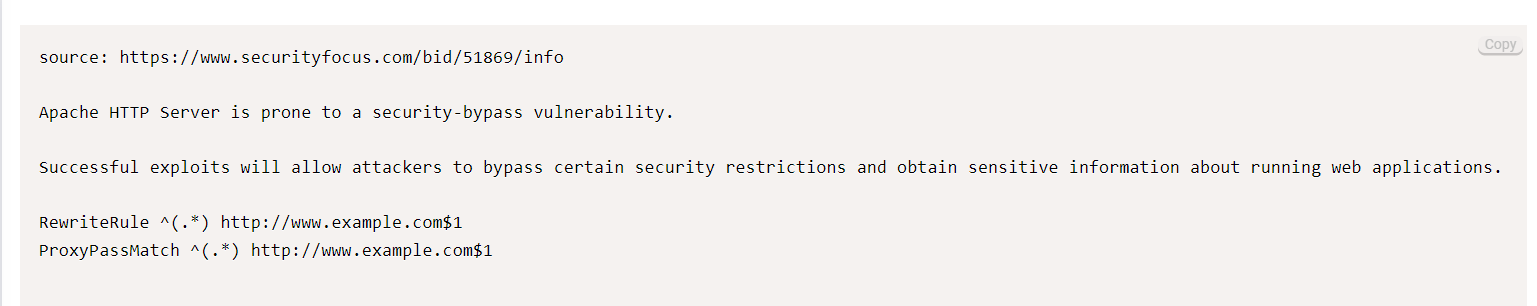


1. release (a bit harder).
   1. Centos 6~
   2. 
   3. 
2. What did you find and how did you find it? Be prepared to share your findings with the rest of the class.
   1. (**Shared in class**)

Deliverable 4. Provide a screenshot similar to the one below that shows your exported google sheet of nmap scan data against cupcake. Note, the scan in the demo did not show version detection. See if you can figure out how to do that. You will have at least two ports.



Deliverable 5. What potential remote vulnerabilities did your team find? 



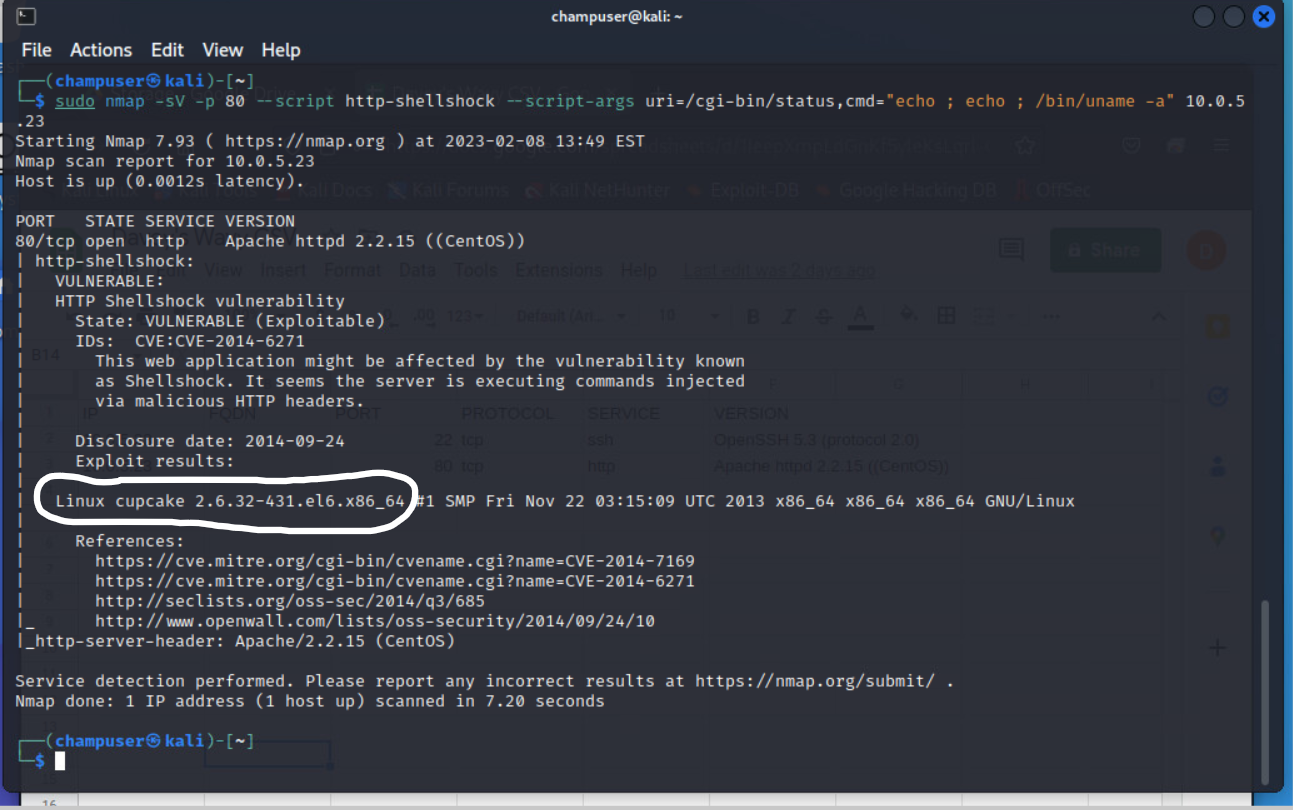
[**https://www.cvedetails.com/vulnerability-list/vendor\_id-45/product\_id-66/version\_id-459994/Apache-Http-Server-2.2.15.html**](https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-459994/Apache-Http-Server-2.2.15.html)

[**https://www.cvedetails.com/vulnerability-list/vendor\_id-97/product\_id-585/version\_id-462753/Openbsd-Openssh-5.3.html**](https://www.cvedetails.com/vulnerability-list/vendor_id-97/product_id-585/version_id-462753/Openbsd-Openssh-5.3.html)

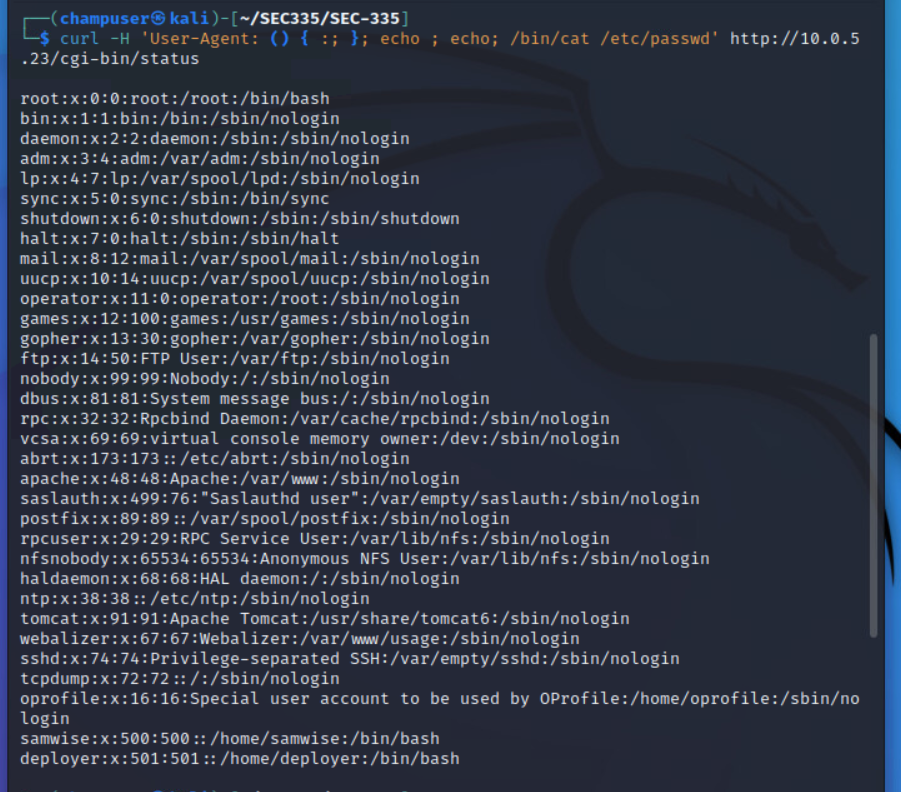
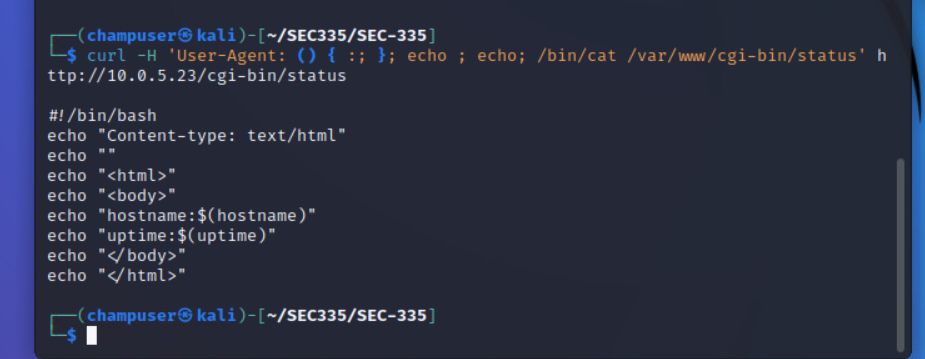
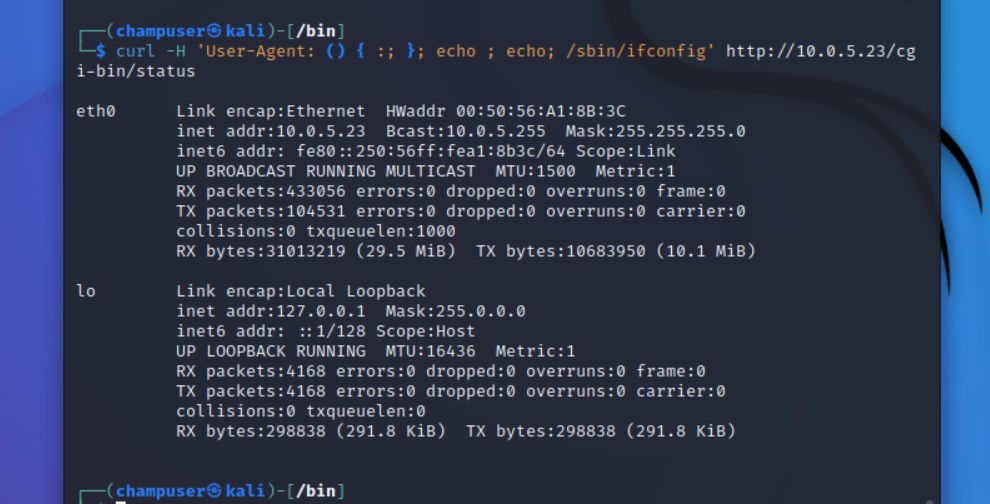
* **The First link as well as the screenshot attached are exploits that relate to the Apache 2.2.15 vulnerabilities. There were multiple different vulnerabilities that were found and the link rates them based on how much potential impact they can have on a system. This is similar to OpenSSH 5.3 where there is a list of known exploits that are all ranked based on how much damage can be done to the PC being exploited.**
* **The first screenshot shows an exploit with Apache 2.2.15 that allows the person using the exploit to bypass security on files within the directory of the apache web server.**

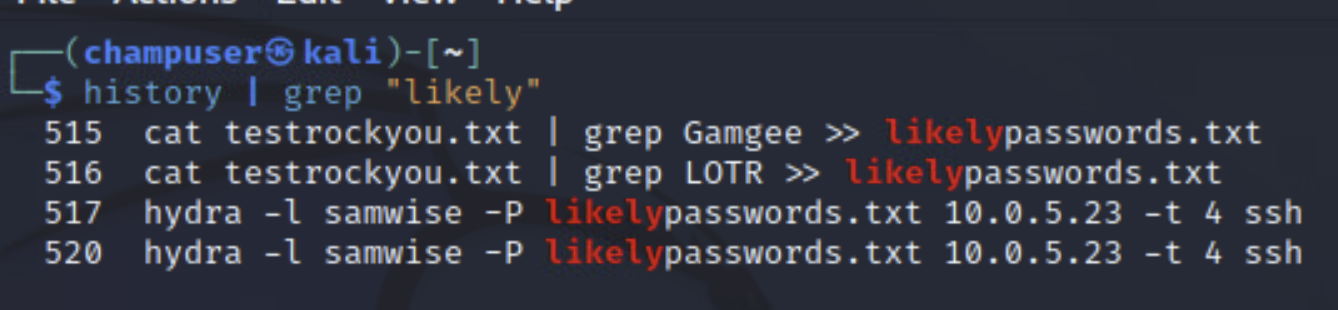
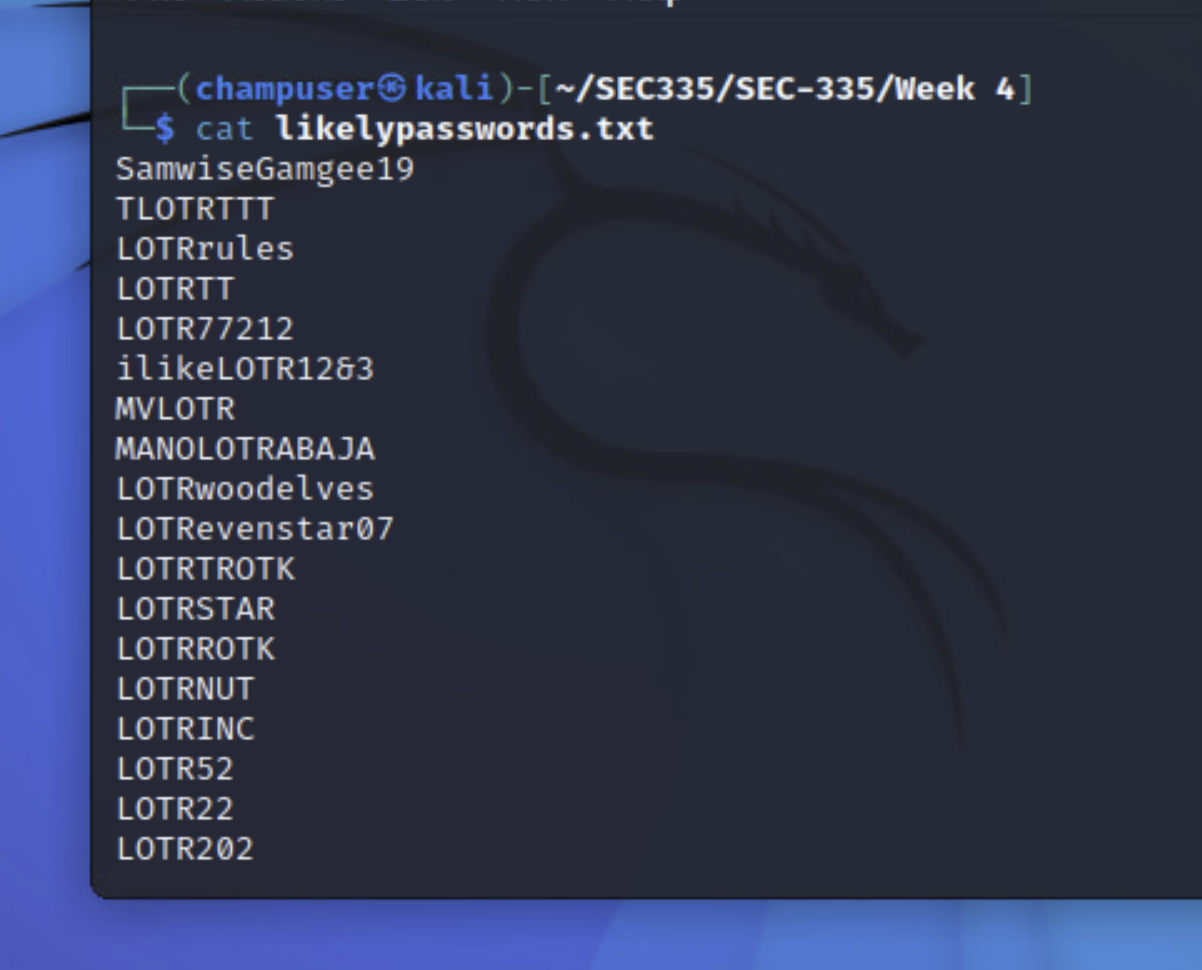
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

David Thomsen

Deliverable 6. Using the following screenshot as a point of departure. Determine what the target's running kernel version (you would use the uname command for this). Provide a screenshot that shows the major and minor release of the kernel.

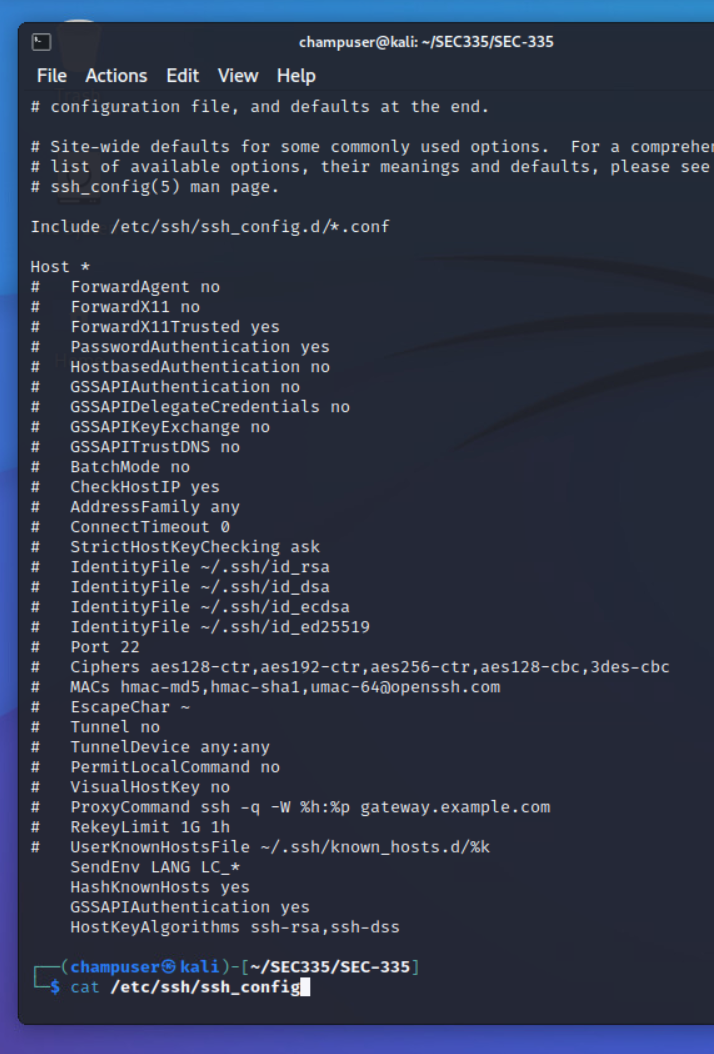
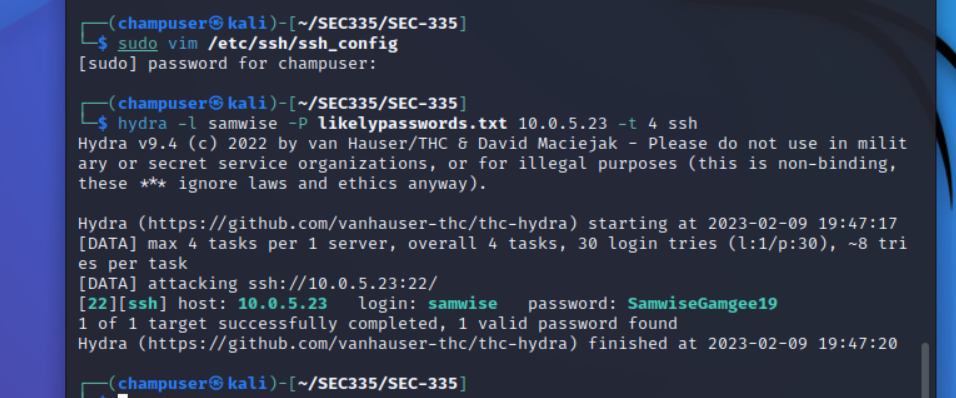
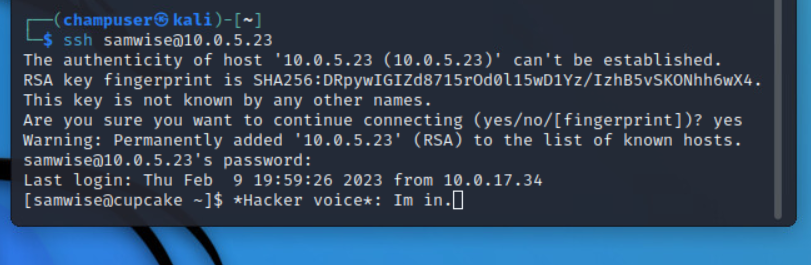
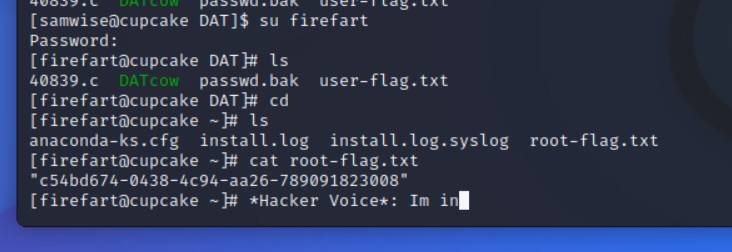
Deliverable 7. The following technique exposes the OS release. Show similar screenshots that show:

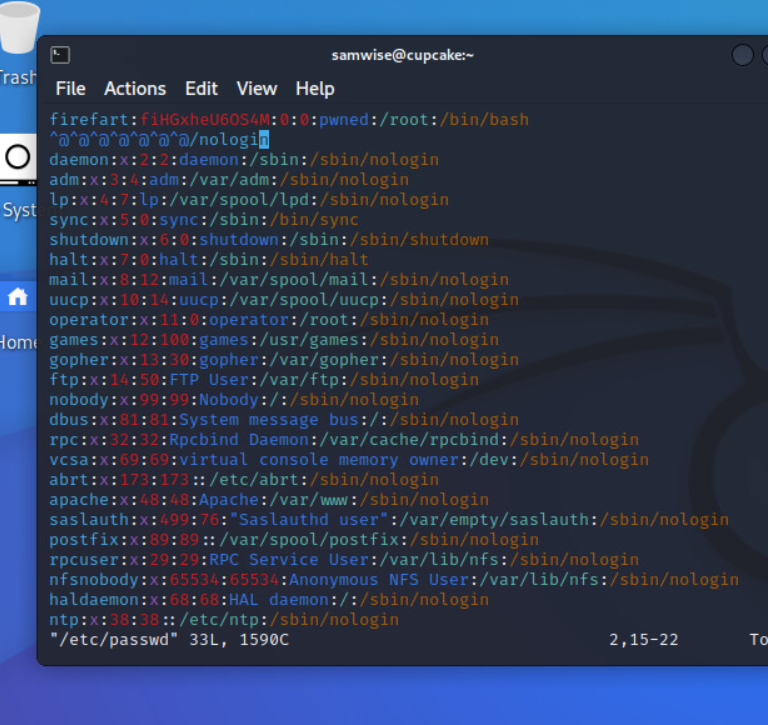
* the contents of /etc/passwd
* 
* the code behind the status cgi
* 
* the results of running ifconfig
* 
* <https://askubuntu.com/questions/120628/ifconfig-command-ifconfig-is-available-in-sbin-ifconfig>

Deliverable 8. Armed with the contents of /etc/passwd, let's see if we can build a list of likely passwords for the target account. You should end up with 28 passwords in your list. Provide a screenshot that shows how you generated the list as well as the list contents 

Deliverable 9. Show a screenshot of your hydra session as well as a ssh login session using the targeted account. Also dump the contents of user-flag.txt using cat or more.



* Error due to the server being down. Same command shown working below with an additional fix (on Git under *Troubles Encountered*)Deliverable 9. Show a screenshot of your hydra session as well as a ssh login session using the targeted account. Also dump the contents of user-flag.txt using cat or more.
* 



Deliverable 10. Provide a screenshot that shows the results of the id command as well as the contents of root-flag.txt similar to the one below.

