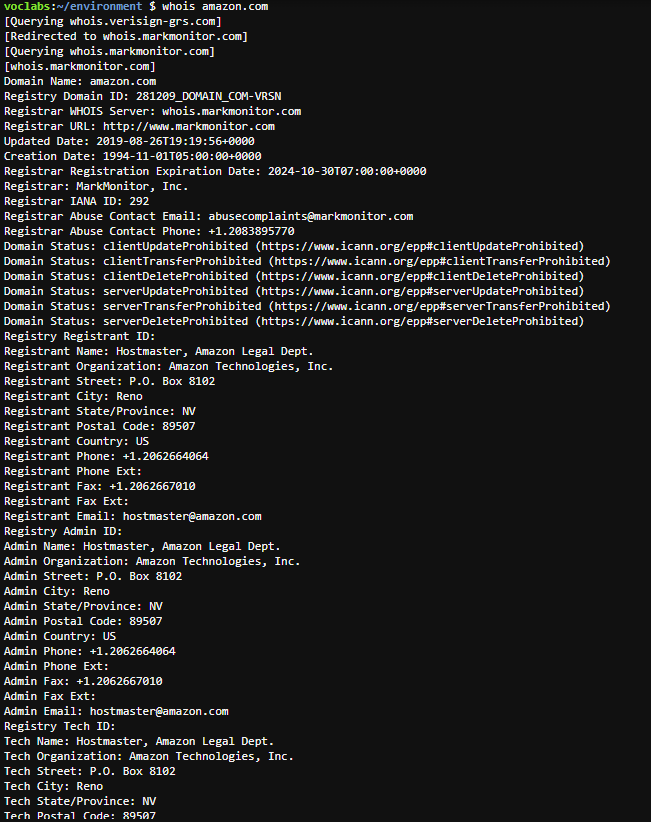
# Cybersecurity

## Activity 2.1.2 Passive Analysis

Copy and paste screenshots and/or answer questions from the activity.

#16 Screenshot of the results of the whois command.



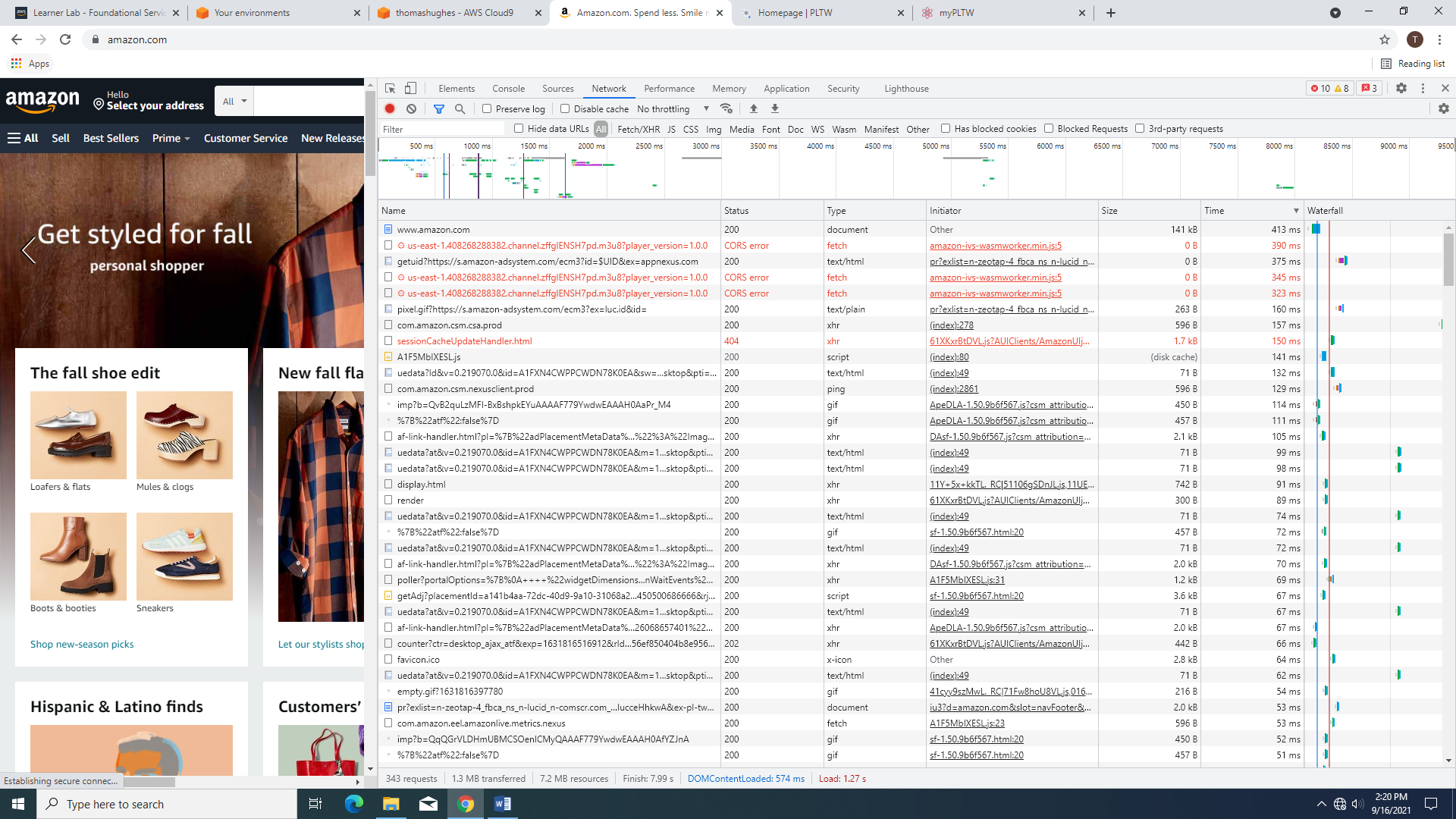
In your own words, describe the tasks you completed in the 1st 16 steps…what did you

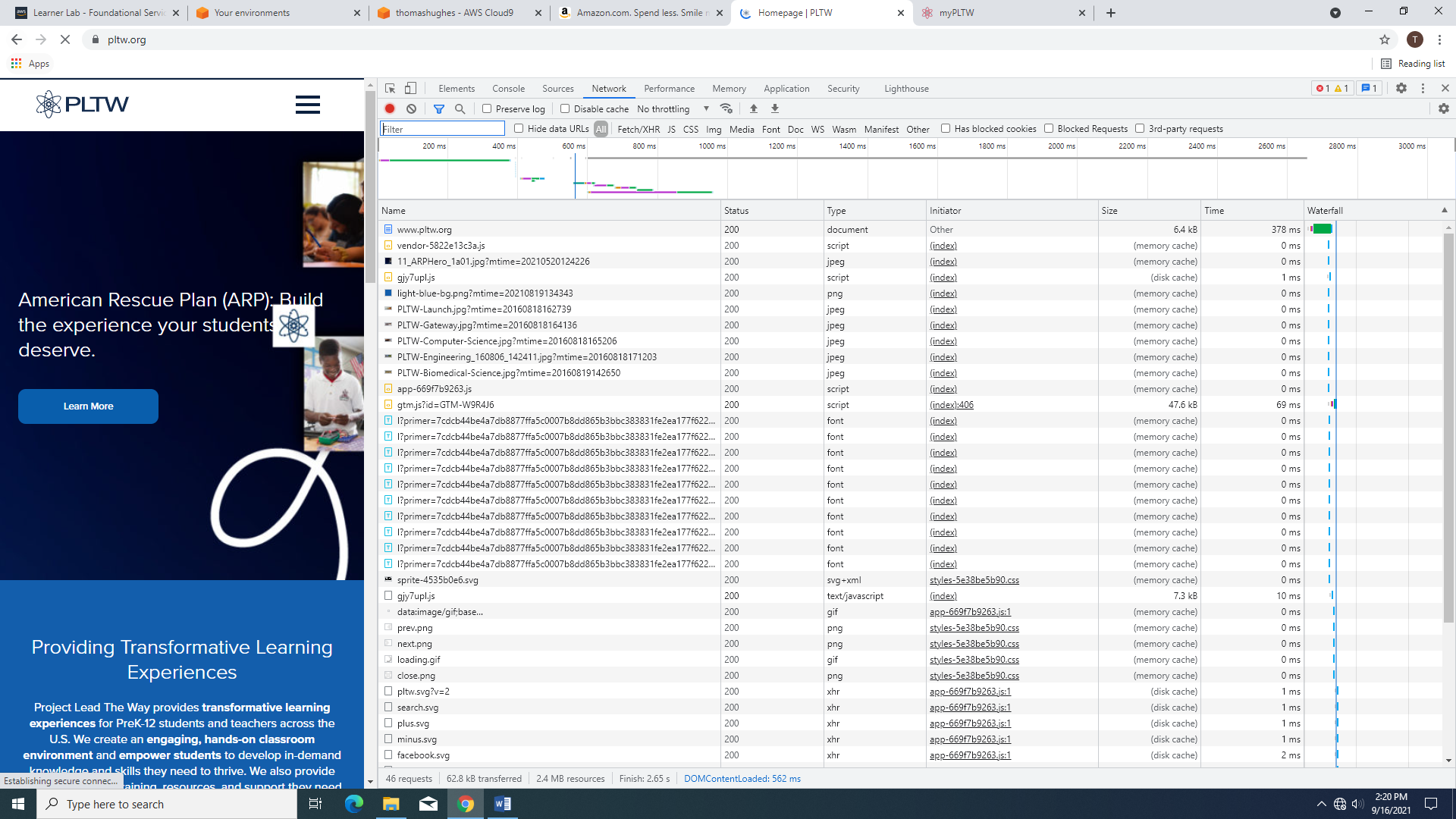
accomplish? Why are we using an AWS student account? What is cloud9? What does the

whois command show us?

------------------------ CAN BE COMPLETED WITHOUT YOUR AWS ACCOUNT------------------------

#20 Screenshot of browser load times





#21 What do you find after comparing the load times of each site?

Amazon: 49 seconds

PLTW: 41 seconds

#23

c. Use your down-arrow key to quickly scroll through the resource Name list and record at least five unique remote IP addresses.

184.87.221.178:443

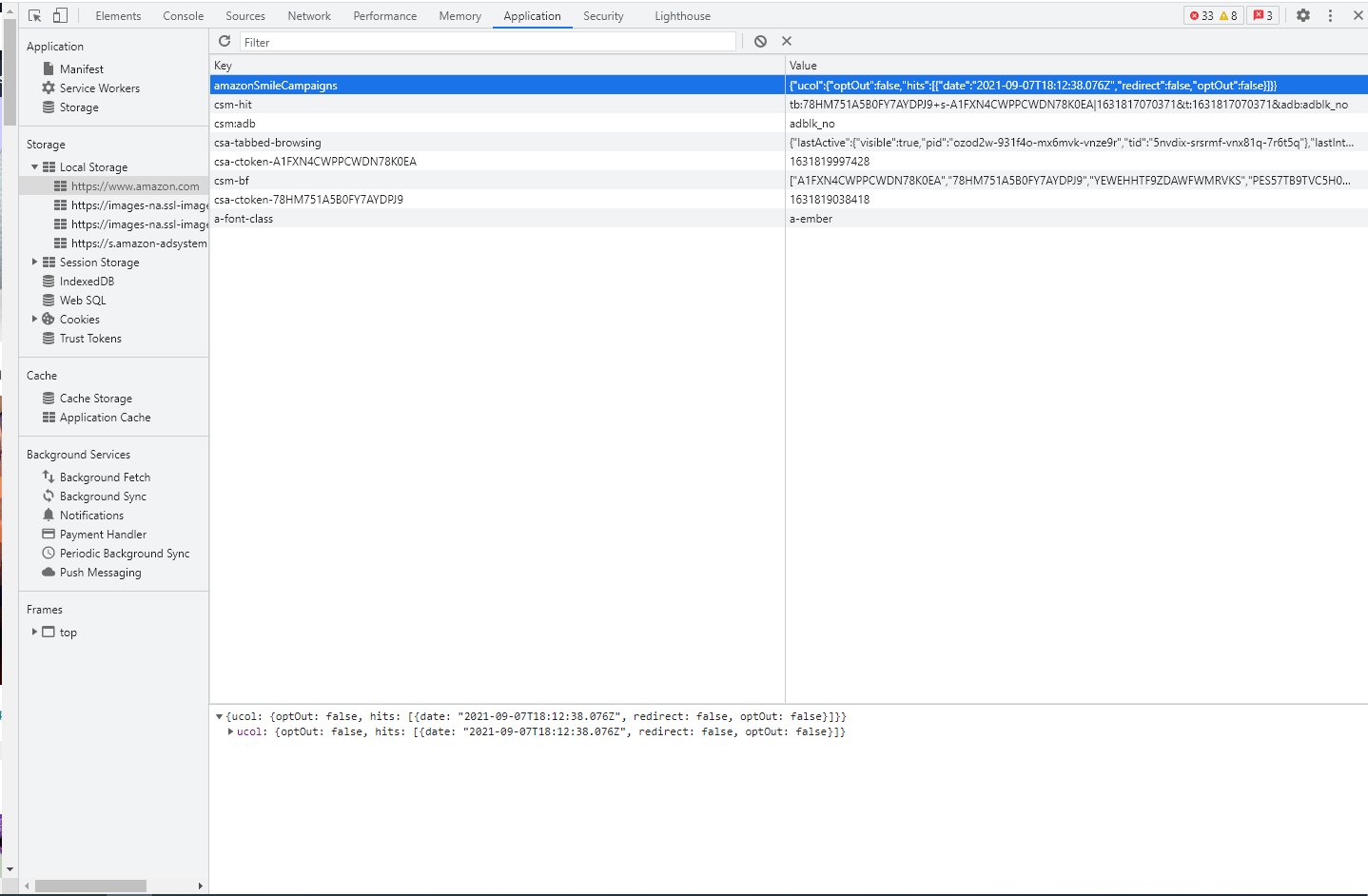
99.84.246.92:443

52.94.232.195:443

104.18.226.225:443

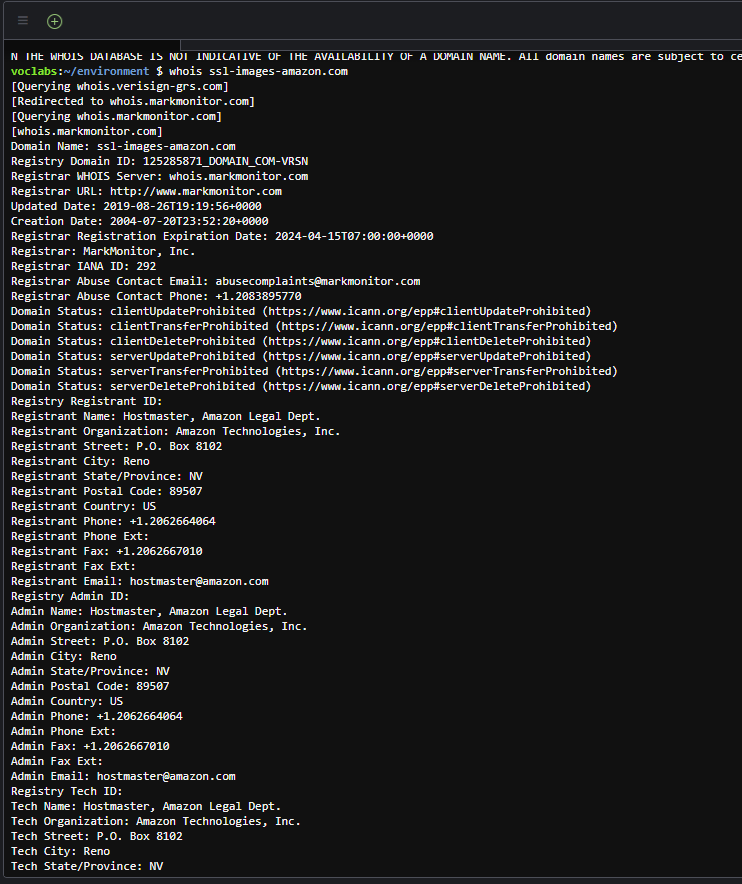
104.123.153.11:443

#26 Record the URLs listed.



---------------------­­­­­­­­­­­­­­­­­­­----------------------------------------------------------------------------------------------------------

#27



b. Compare this output to your screenshot of whois amazon.com . Does the data for the new URL confirm that any unknown domains are part of the Amazon website and others are not? What are some clues?

#28 (the numbers are wrong in the directions…you should be looking at step #23 and step #26)

…Why are do you get a forbidden message, a blank page, or an error?

#30

1. Do you see a pattern in the domain names? In what way are they similar to amazon's domain? To each other?
2. Depending on the IP addresses you chose, some nslookups may return “Non-existent domain”. Why do you think that happens?
3. Save a screenshot of your PowerShell window with its results.

NSLOOKUP AND TRACEROUTE DON’T WORK!!!

#32 Save a screenshot of the results of traceroute

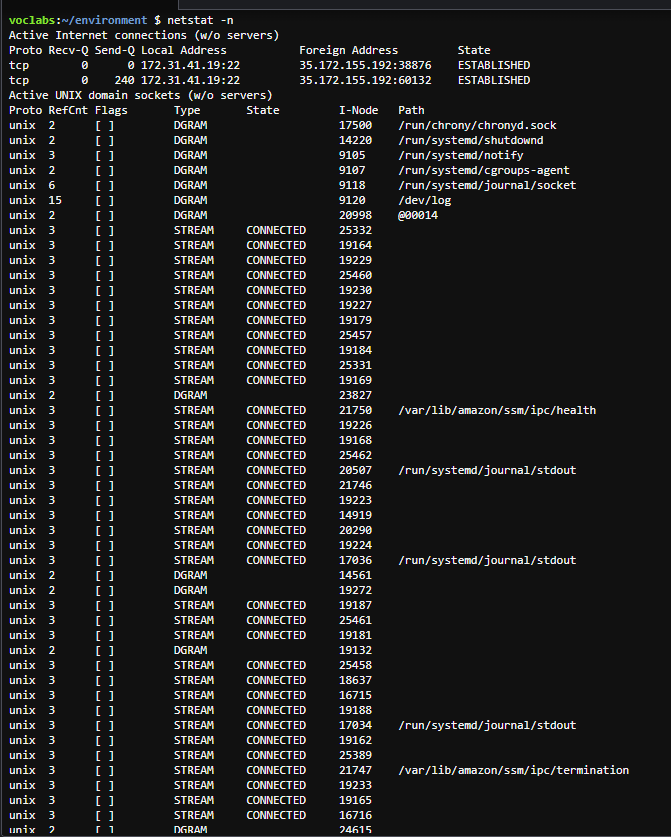
NSLOOKUP AND TRACEROUTE DON’T WORK!!!

In your own words, explain what the traceroute command does.

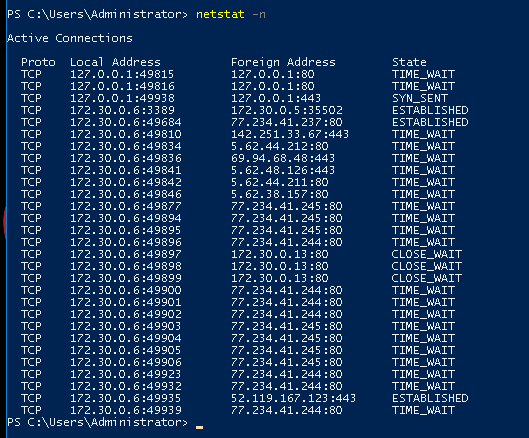
I DON’T KNOW I DIDN’T USE IT

#34 Save a screenshot of your PowerShell window with your latest netstat data

#36 Save a screenshot of your PowerShell window with your latest netstat data



#37 Record the full foreign address of the CTS website



#39 Describe what service is associated with each of these ports. Then describe which parts of

the network (CTS or your security lab) are using those services.

NO

Conclusion

1. Work through the following scenario: suppose you are the victim of a malware attack and you suspect a spoofed website is the problem. Summarize how each tool could help you in your investigation of the website.

* Whois
  1. Tells you the name and address of a domain
* Nslookup
  1. Learn the domain names of web addresses
* Traceroute
  1. Report the host names of different servers
* Netstat
  1. Check the port status of connected servers