# Cybersecurity

## Activity 2.3.3 Server Attacks

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

#9 Go to Packet 484 and record the Destination MAC address.

ff:ff:ff:ff:ff:ff

#11 Provide a Screenshot

Graphical user interface, text, table

Description automatically generated

#12 Save a screenshot of your Wireshark window.

00:22:fa:1c:eb:e6

Graphical user interface, text, application, table

Description automatically generated

#15 a. What are the two IP addresses that performed the handshake?

Graphical user interface, text, application, email

Description automatically generated

64.14.192.236 & 192.168.1.64

b. How long did the handshake take?

0.000127000 seconds

#16 How do the ip.addr and ip.src filters differ?

Ip.addr applies to the source and destination while ip.src only looks at the source address

#19 Do you think it would be harder to spoof (fake) a TLSv1 handshake than a TCP handshake? Why or why not?

A TLSv1 would be harder to spoof due to it requiring an extra layer of security that builds on top of TCP

#24 Save a screenshot of the full URI.\

A picture containing Teams

Description automatically generated

#25 What is the purpose of this website?

“A complete curriculum solution for cybersecurity education”

#28 Using a web browser, is the site a safe and reliable source for embedding scripts in a web page? Why do you think you needed to validate that ajax.googleapis.com is not suspicious or malicious?

You need to validate ajax because

Show the entire script in the Details pane and save a screenshot of your Wireshark window.

Graphical user interface, text

Description automatically generated

#35 a. How many different log-in attempts were made on this website? Approximately

how close together did these packets arrive (in seconds or minutes, not milliseconds)?

5 at ~ 0.005 seconds apart

b. Observe the values for the usernames and passwords. Do you think this data

represents a legitimate log-in attempt or a brute force attack? Justify your answer.

Brute force, they use the same username with different variations of the same password

#37 The response appears after the from content. What is that response?

“username and/or password incorrect”

#38 When you selected Follow > HTTP Stream data earlier, what Wireshark really did was to

create a filter for you. What is the filter?

Tcp.stream eq 12

Save a screenshot of your Wireshark window.

Text

Description automatically generated