Student:	Email:
Stephen Asamoah	stephen.asamoah@howardcc.edu

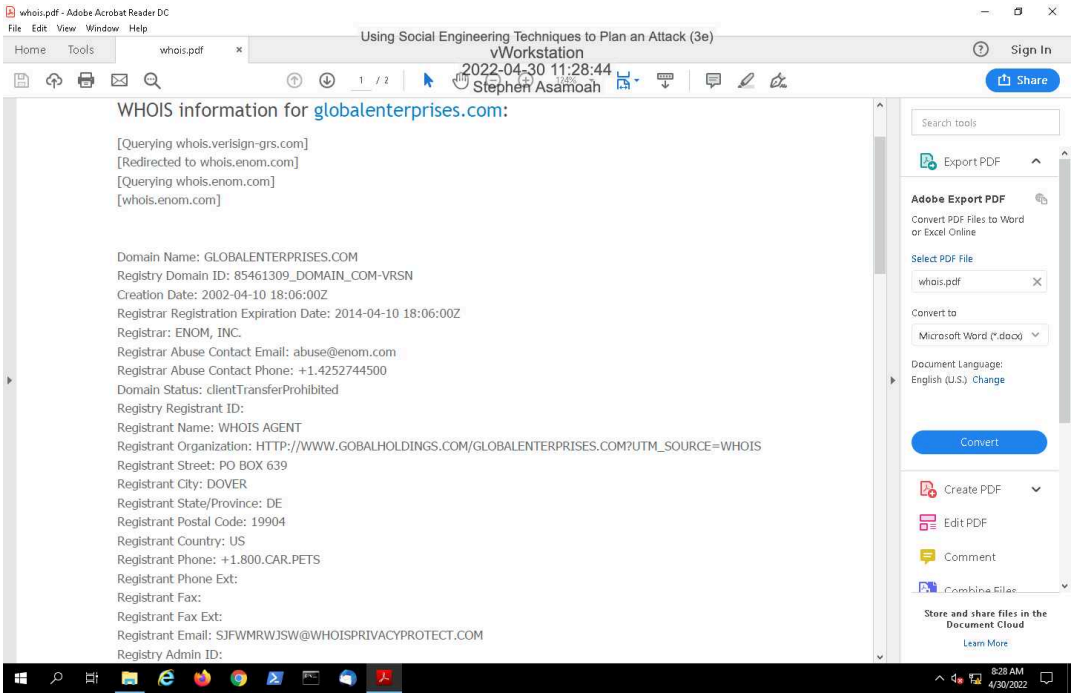
Time on Task:	Progress:
1 hour, 14 minutes	100%

Report Generated: Saturday, April 30, 2022 at 12:36 PM

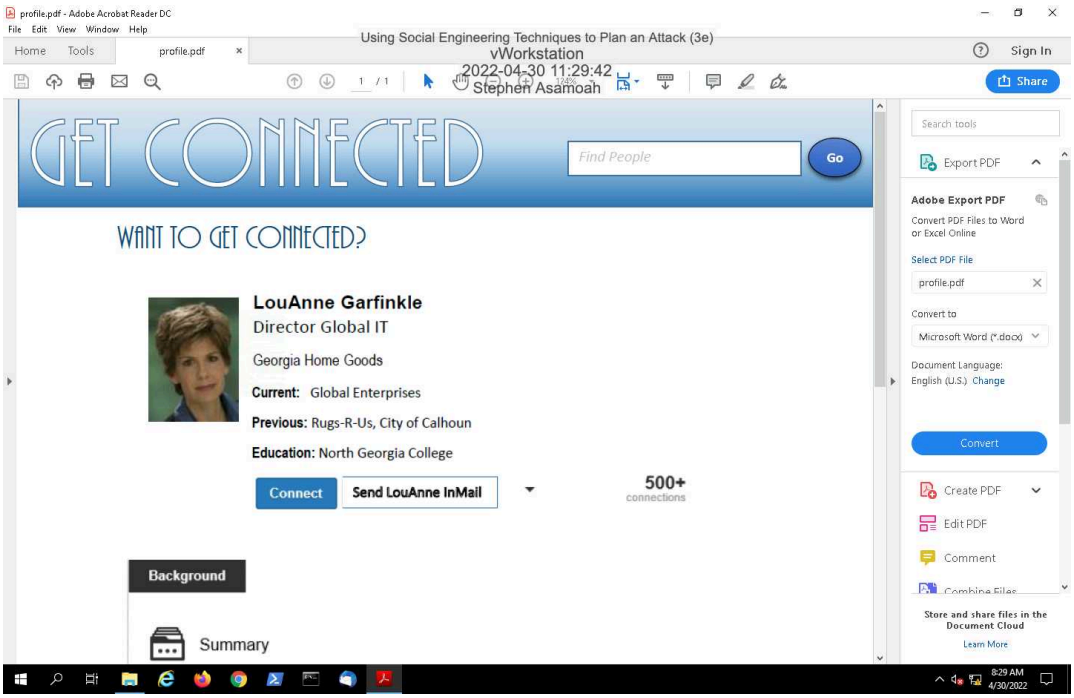
Section 1: Hands-On Demonstration

Part 1: Observe Targeted Social Engineering Research

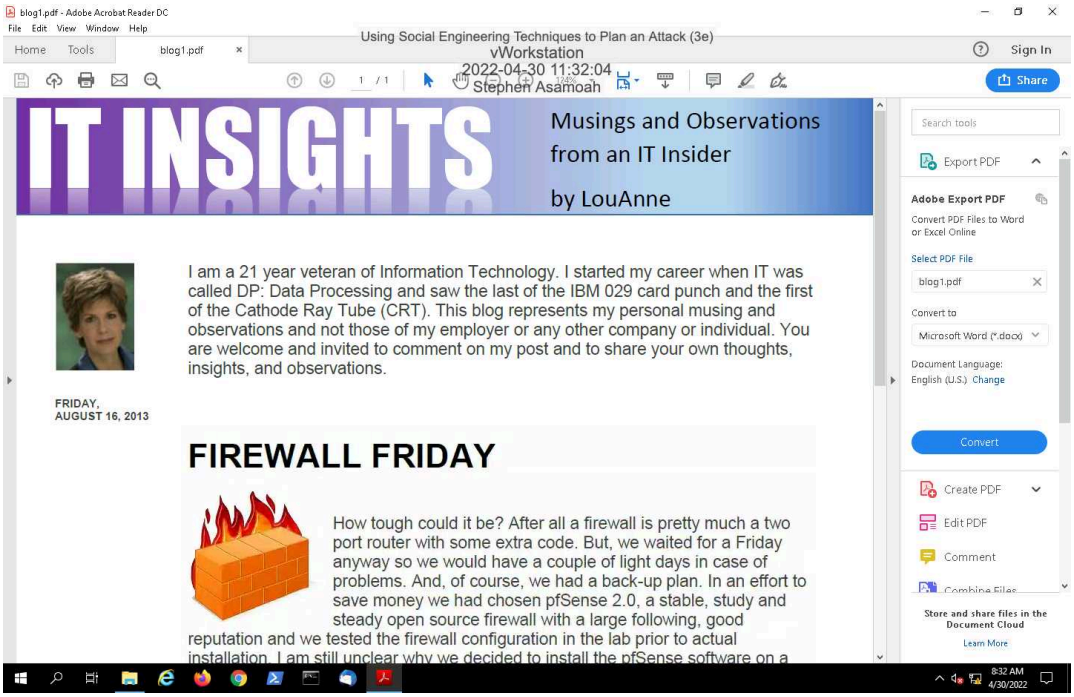
7. **Make a screen capture** showing the **whois information for Global Enterprises**.



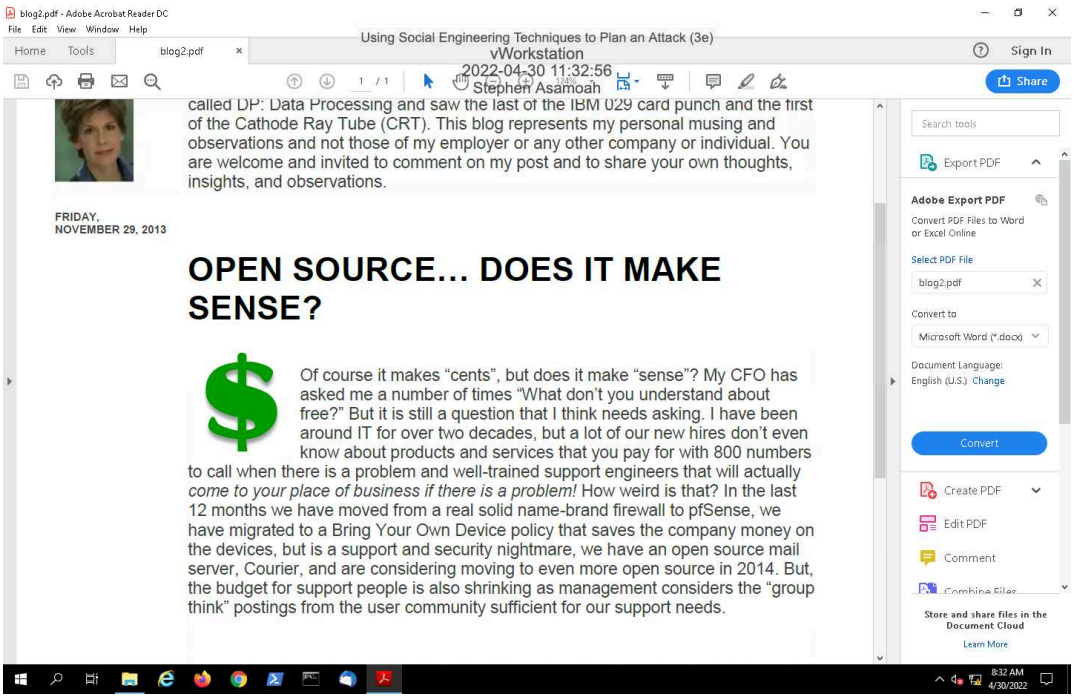
12. **Make a screen capture** showing **LouAnne's GetConnected profile**.



15. **Make a screen capture** showing the **first blog entry**.



18. **Make a screen capture** showing the **second blog entry**.

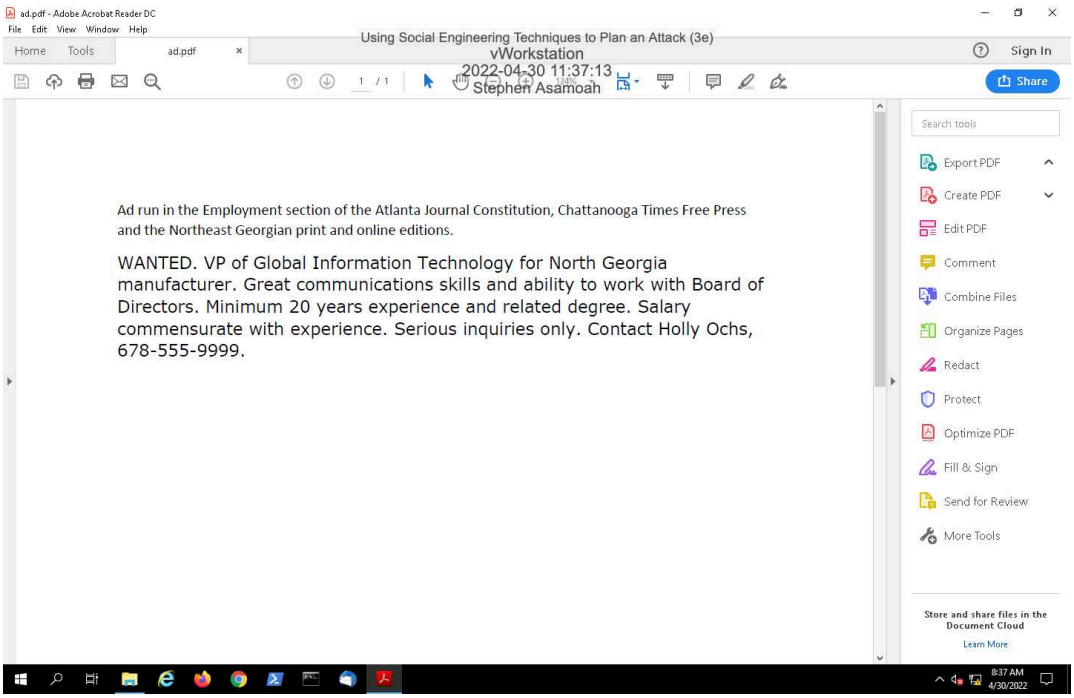


22. **Record** the **current firewall software version number**.

GB-OS 2

Part 2: Observe a Targeted Reverse Social Engineering Attack

2. **Make a screen capture** showing the **fake job ad**.

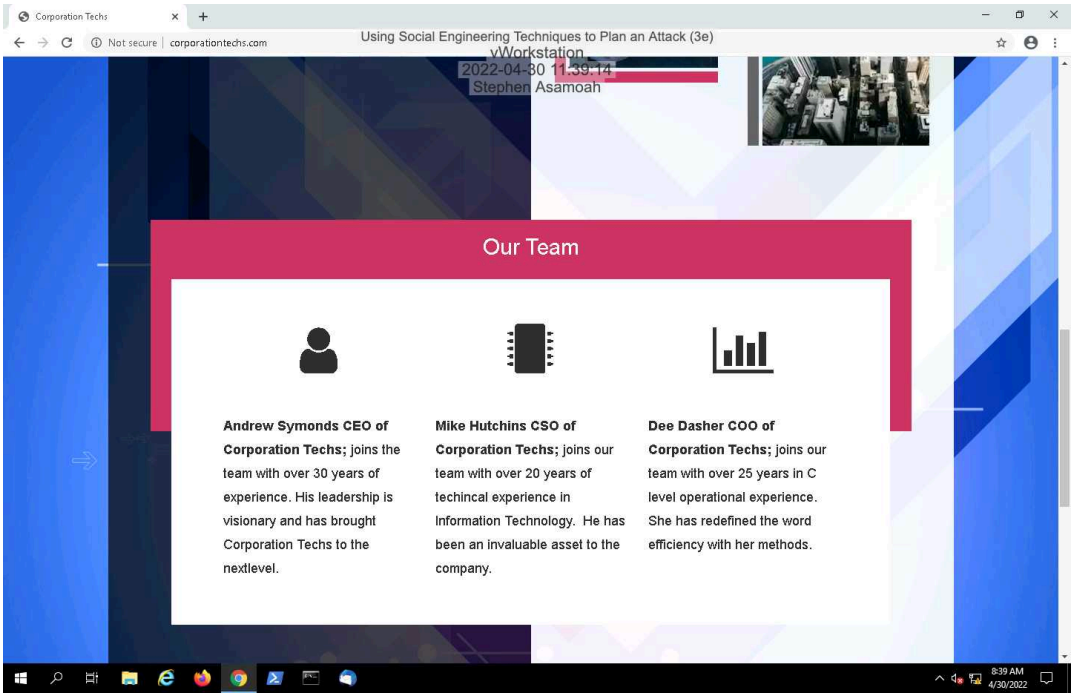


Section 2: Applied Learning

Part 1: Perform Targeted Social Engineering Research

2. **Make a screen capture** showing the **services offered by Corporation Techs**.

3. **Make a screen capture** showing the **Corporation Techs corporate officers**.



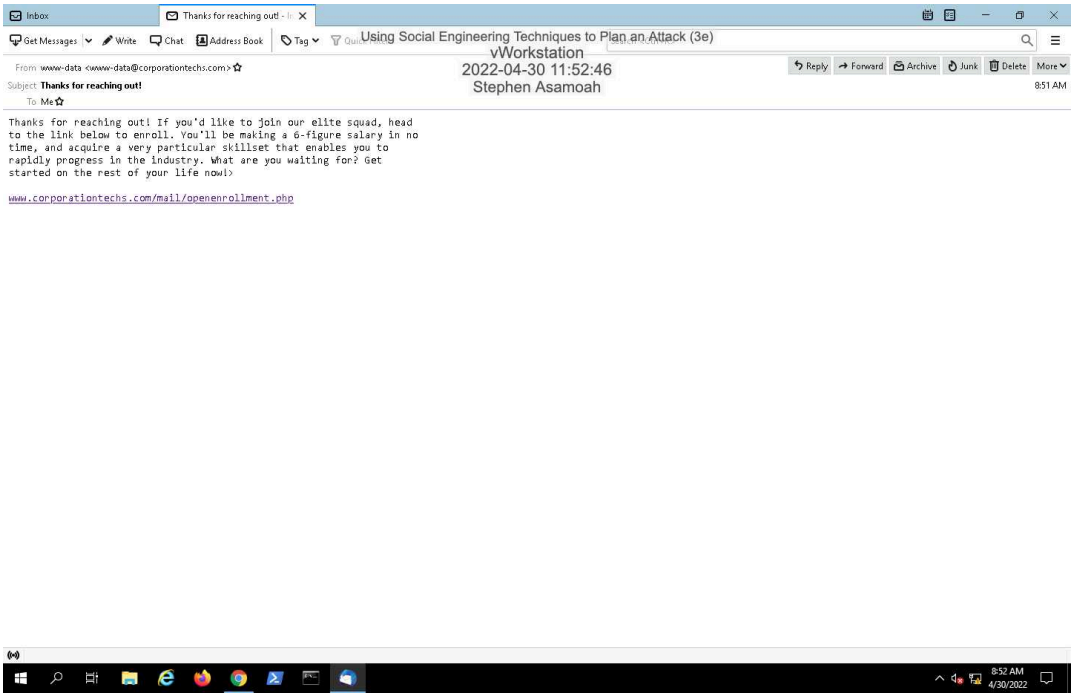
6. **Review** the **LinkedIn profiles** and **answer the following questions**.

    - Which college or university did each officer attend, and for which years?
    - Where does each officer live?
    - Not including Corporation Techs, where did each officer work the longest?

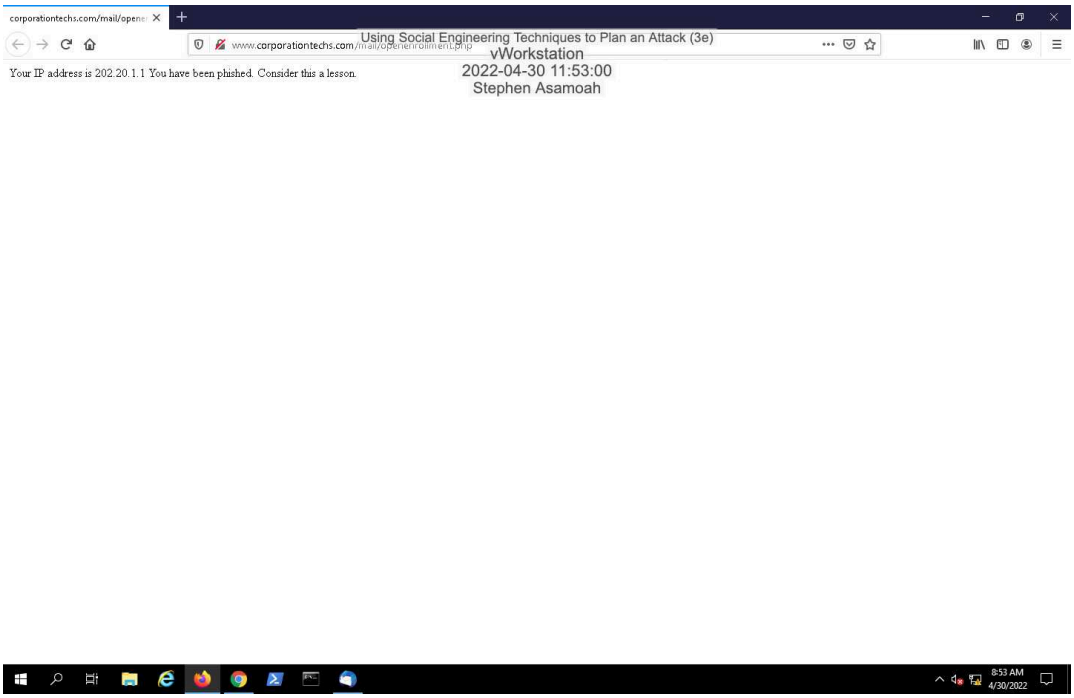
Andrew went to San Diego State University, Mike went to Virginia Tech and Dee went to Texas State University. They all live in Addison, Texas. Andrew, Mike and Dee worked the longest at Wodash Incorporated, Aegis Secured and Dante's Inc respectively.

Part 2: Perform a Targeted Social Engineering Attack

3. **Make a screen capture** showing the **contents of the email.**



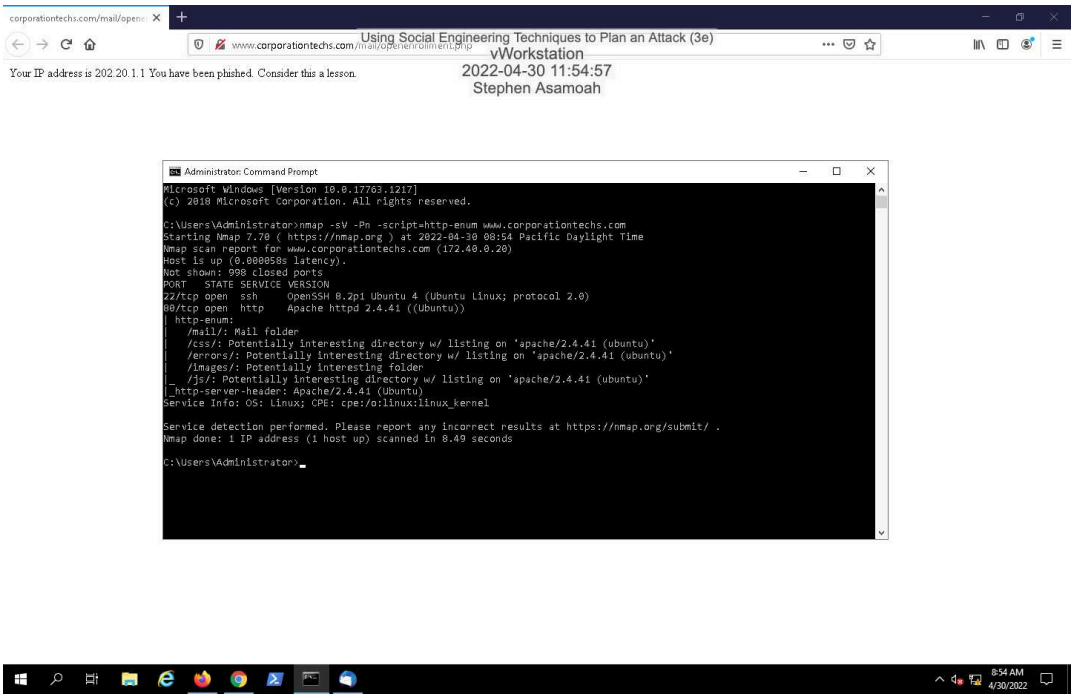
5. **Make a screen capture** showing the **resulting web page**.



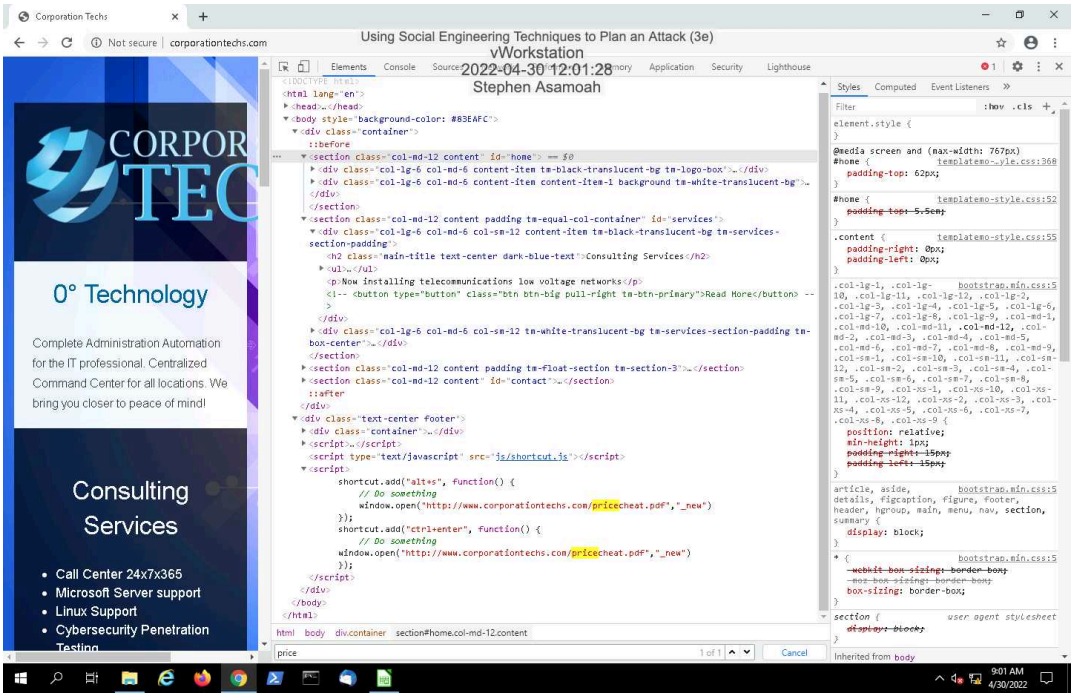
Section 3: Challenge and Analysis

Part 1: Investigate a Data Leak

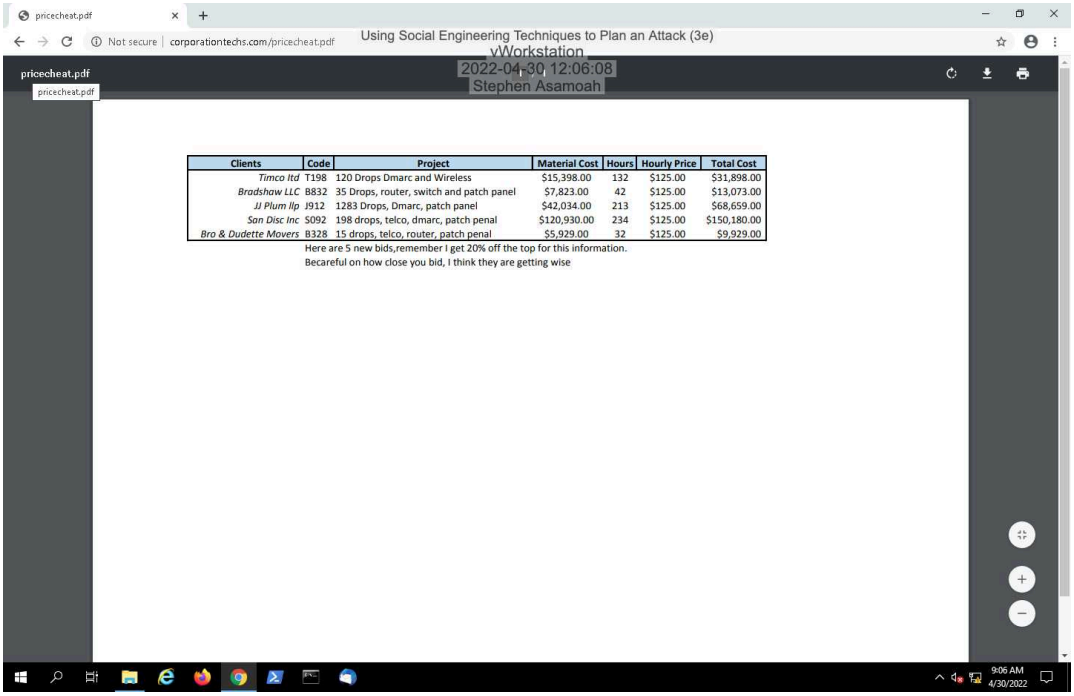
3. **Make a screen capture** showing the **results of the Nmap scan**.



15. **Make a screen capture** showing the **script that will open the file**.



19. **Make a screen capture** showing the **result of your actions**.



Clients	Code	Project	Material Cost	Hours	Hourly Price	Total Cost
Timco ltd	T198	120 Drops Dmarc and Wireless	$15,398.00	132	$125.00	$31,898.00
Bradshaw LLC	B832	35 Drops, router, switch and patch panel	$7,823.00	42	$125.00	$13,073.00
JJ Plum llp	J912	1283 Drops, Dmarc, patch panel	$42,034.00	213	$125.00	$68,659.00
San Disc Inc	S092	198 drops, telco, dmarc, patch penal	$120,930.00	234	$125.00	$150,180.00
Bro & Dudette Movers	B328	15 drops, telco, router, patch penal	$5,929.00	32	$125.00	$9,929.00

Here are 5 new bids,remember I get 20% off the top for this information.
Becareful on how close you bid, I think they are getting wise

Part 2: Continue the Investigation

Write a brief summary of your recommendations.

In my opinion, You can rely on digital forensics. You can check the IP address of the culprit and do reverse nslookup. This will give you the hostname and you can identify that person. Most organizations name workstations based on IP address. for example, 10.10.20.30 may be for computer HCC-LV1-DT4674. The naming convention can lead to the department, floor and the owner of that computer. Social Engineering could also be applied. You can act as the competitor and initiate a conversation with suspected culprit to see if you can catch him live