Student:	Email:
Christian Barba	christianbarba527@gmail.com

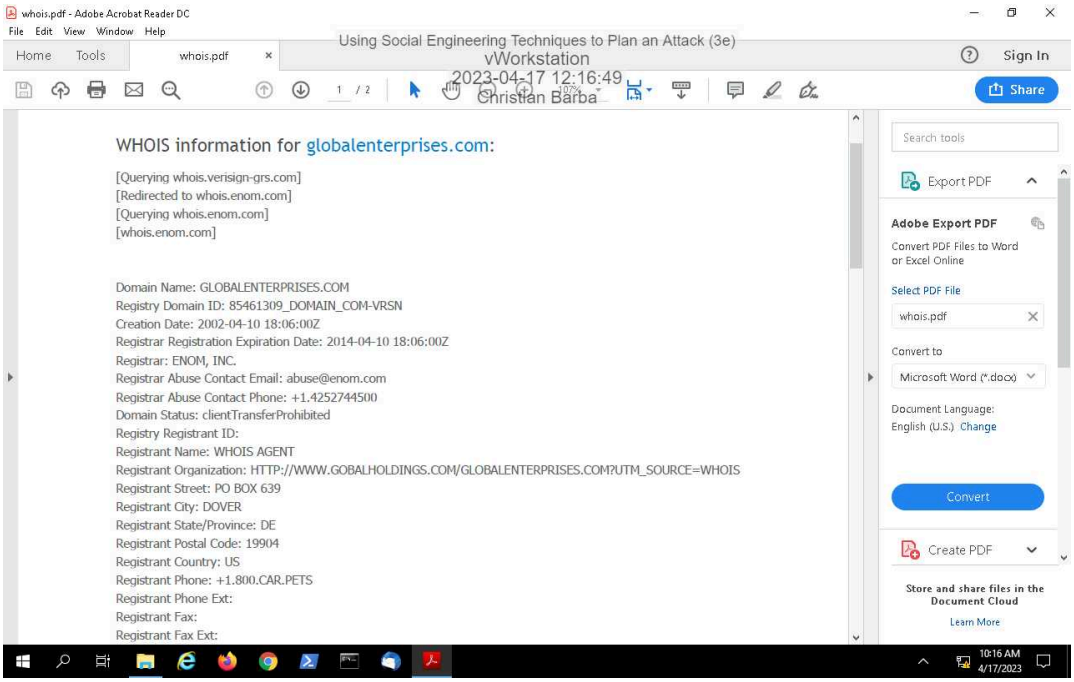
Time on Task:	Progress:
2 hours, 26 minutes	100%

Report Generated: Thursday, April 20, 2023 at 12:59 PM

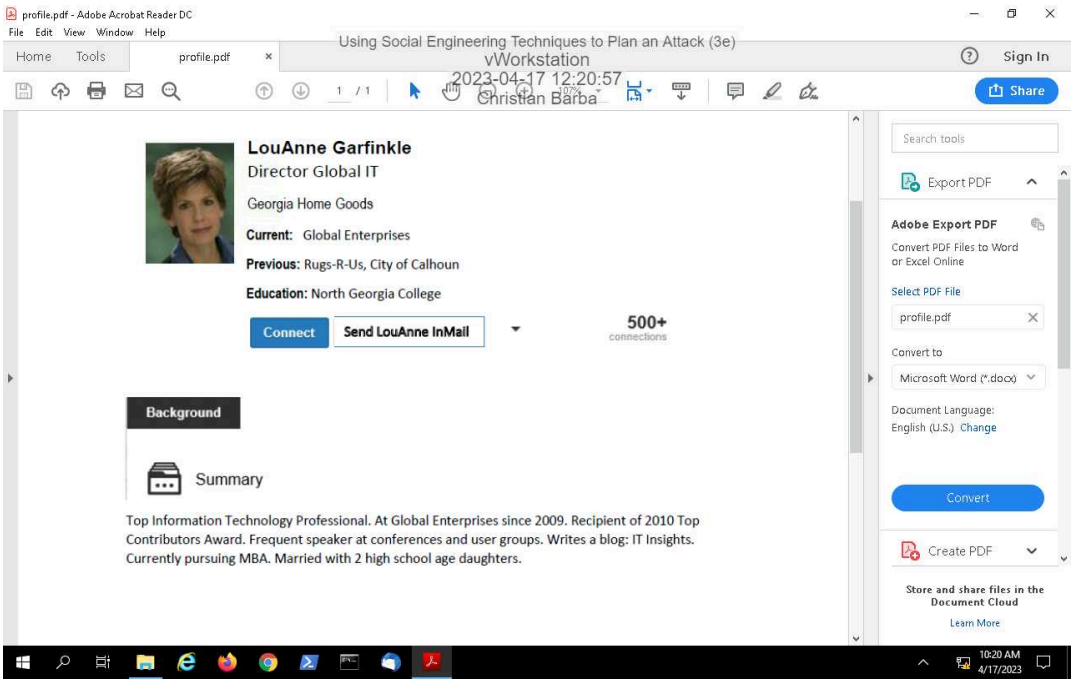
Section 1: Hands-On Demonstration

Part 1: Observe Targeted Social Engineering Research

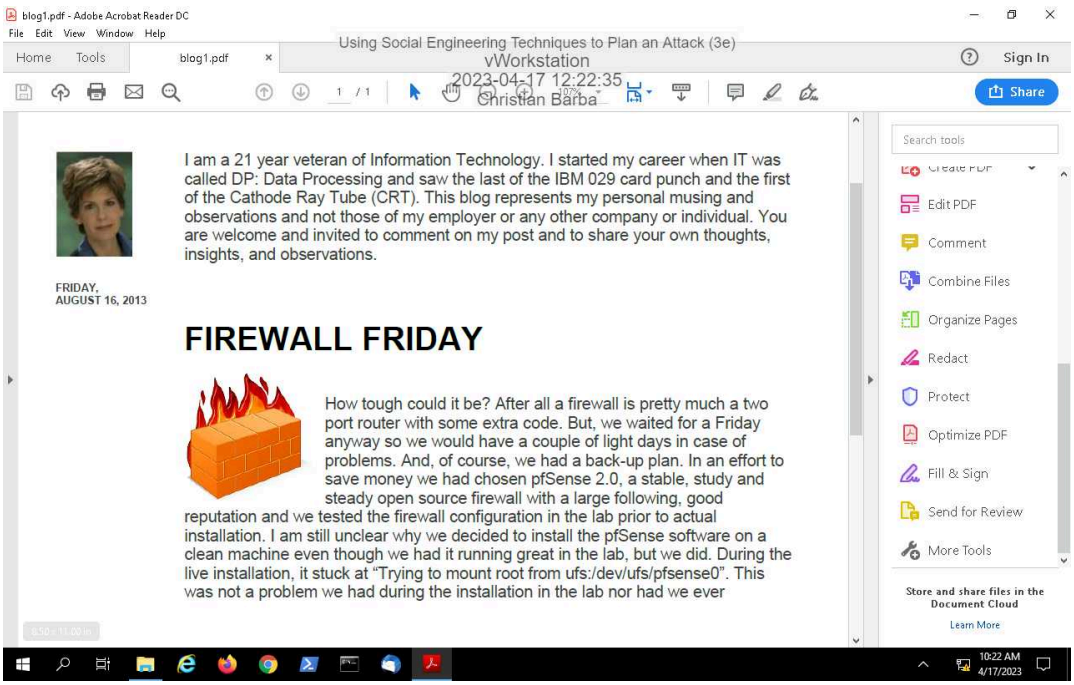
7. **Make a screen capture** showing the **whois information for Global Enterprises**.



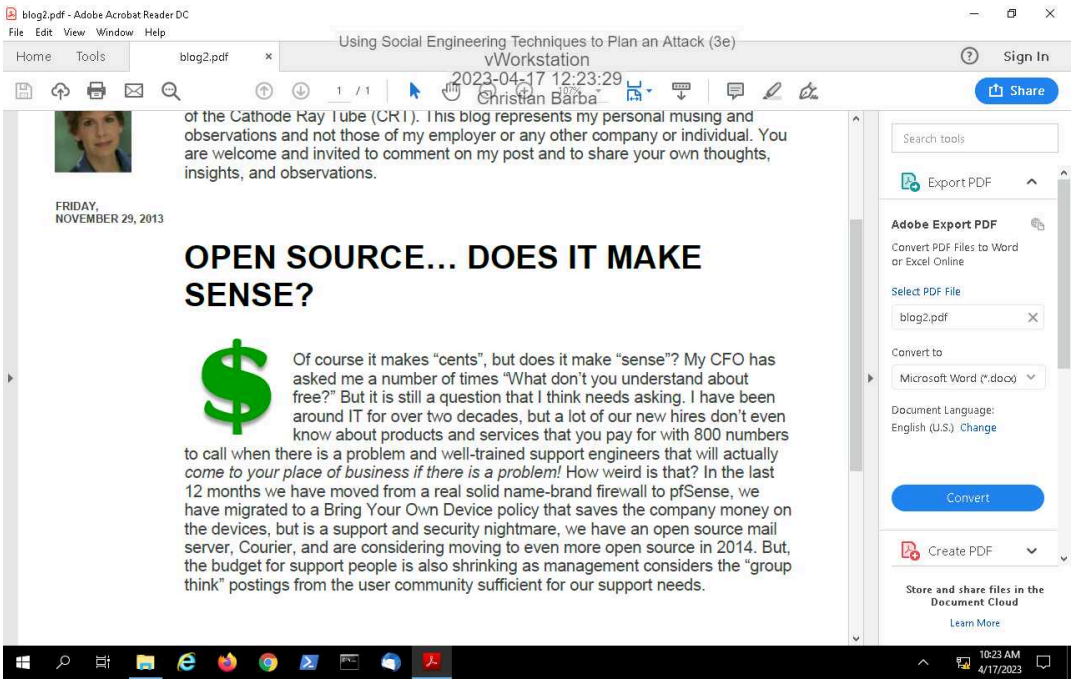
12. **Make a screen capture** showing **LouAnne's GetConnected profile**.



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



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

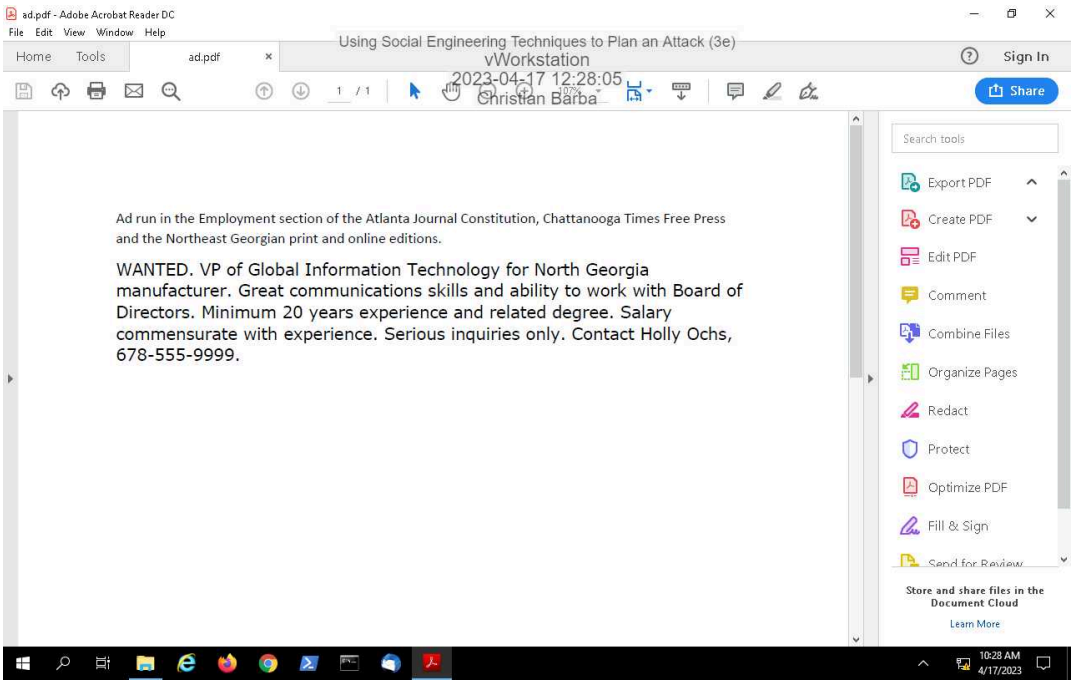


22. **Record** the **current firewall software version number**.

The current firewall software version number is 6.2.

Part 2: Observe a Targeted Reverse Social Engineering Attack

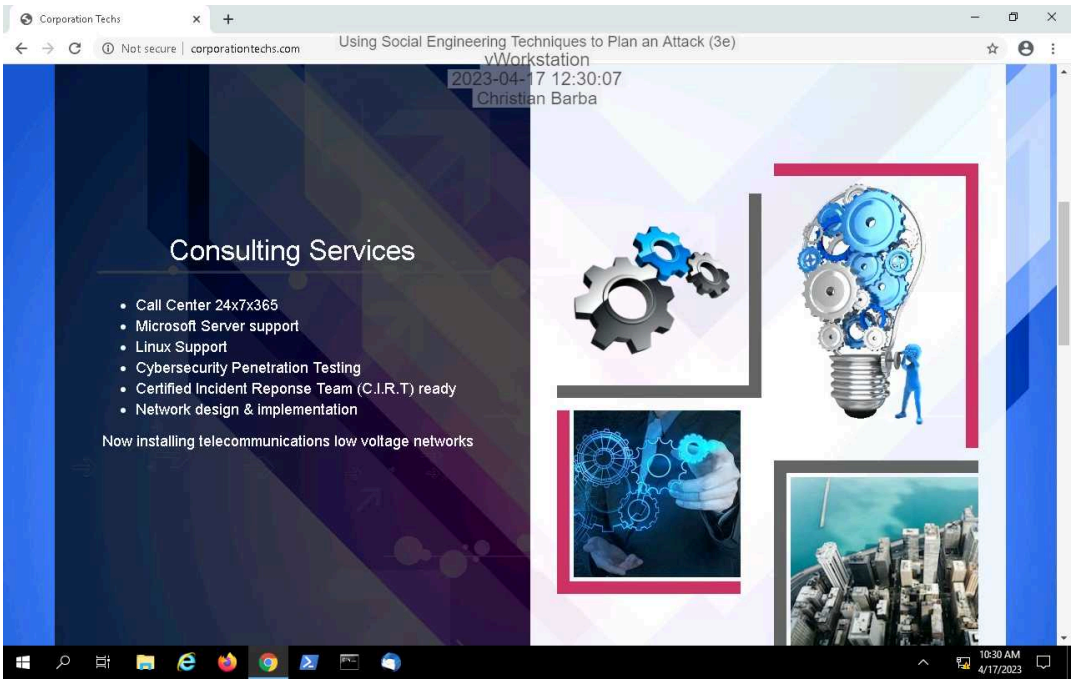
2. **Make a screen capture** showing the **fake job ad**.



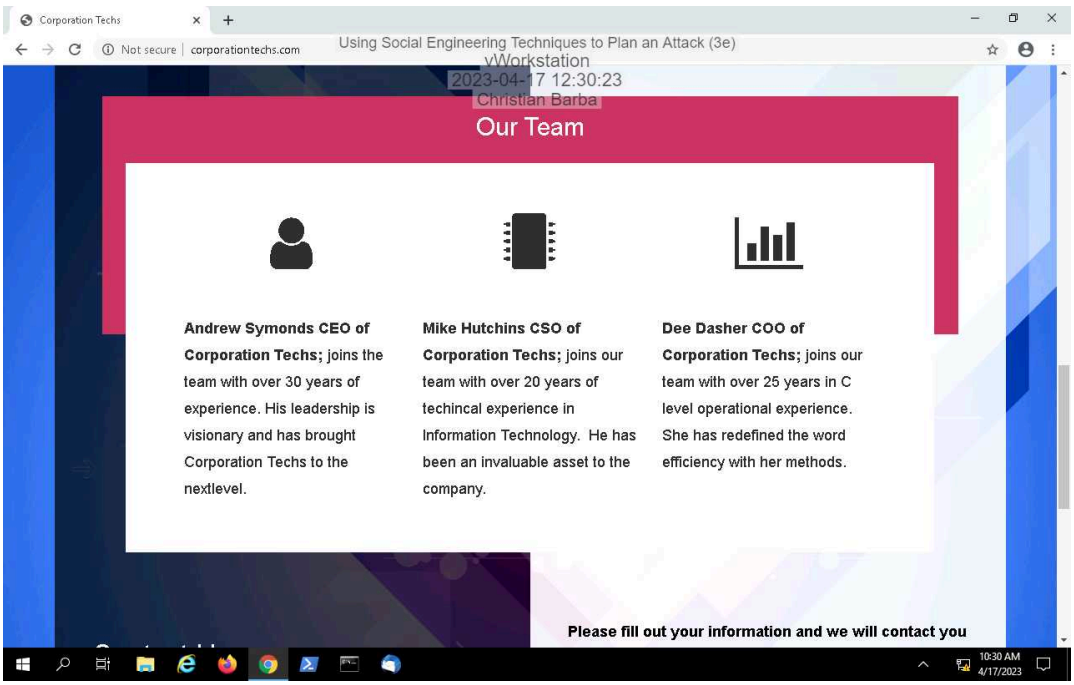
Section 2: Applied Learning

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**.

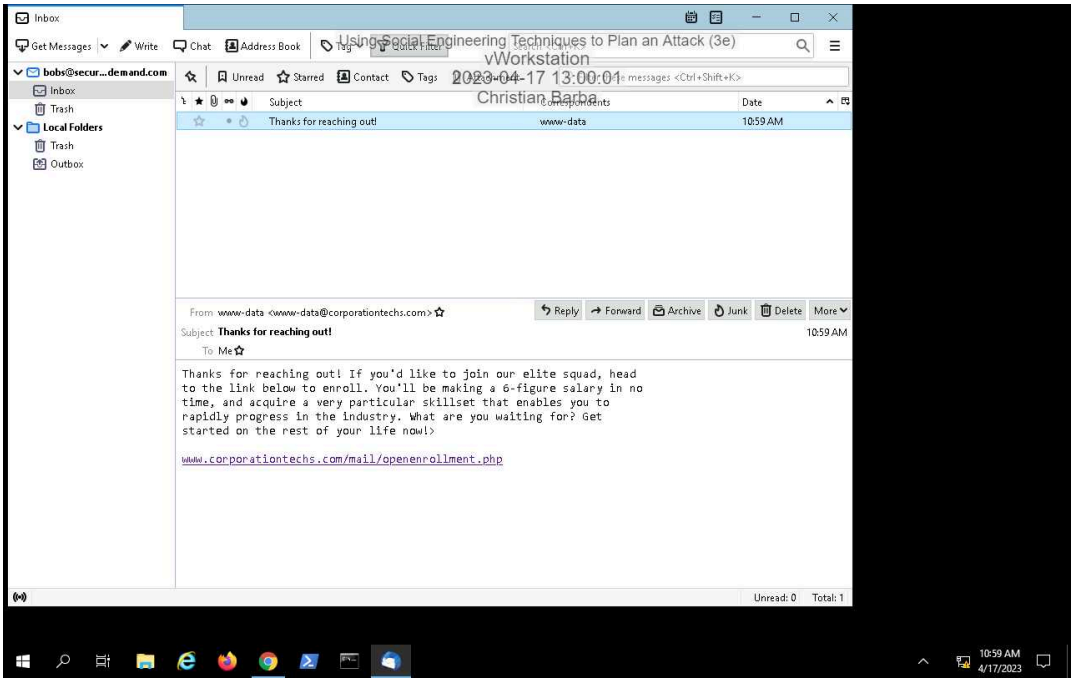
    - Which college or university did each officer attend, and for which years?
    - Where does each officer live?
    - Not including Corporation Techs, where did each officer work the longest?

Andrew Symonds went to San Diego University before the year 1983 because that is when his first job started. He currently lives in Addison, Texas, and the longest job he had was a Sales Executive position for Wodash Incorporated for 13 years.
Mike Hutchins went to Virginia Tech from 1992-1996, and he currently lives in Addison, Texas. His longest job prior to Corporation techs was at Aegis secured for 7 years and 4 months.

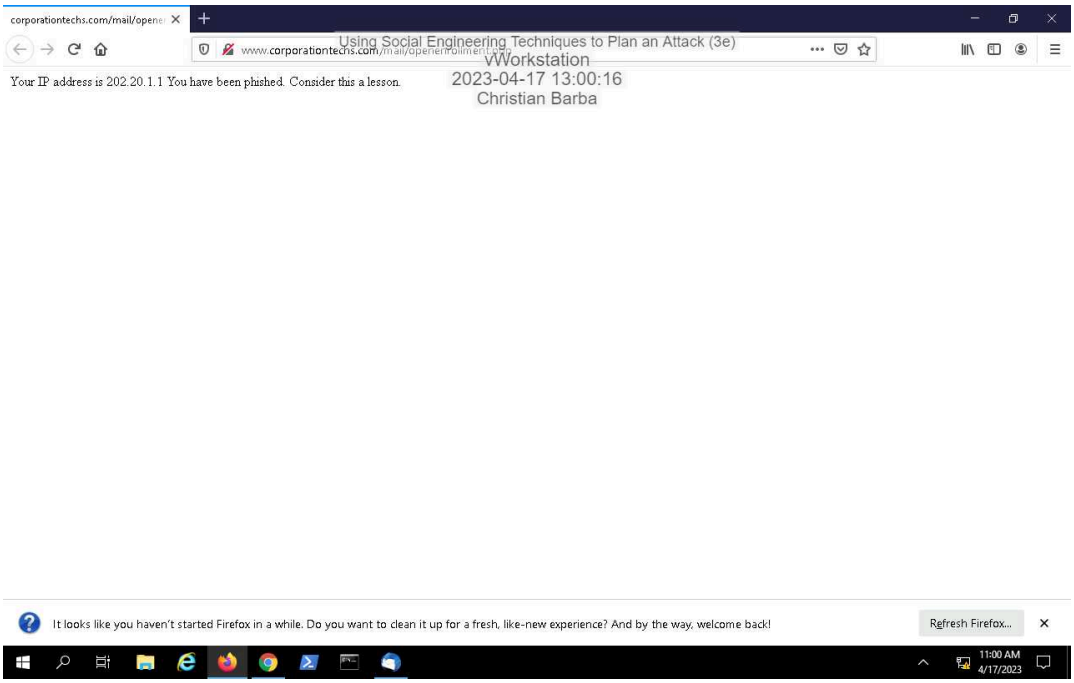
Lastly, Dee Dashher attended school at Texas State University from 1985-1989, and currently lives in Addison, Texas. She worked at Dante's Inc for 8 years and 7 months and this was the longest she had worked a position prior to Corporation Techs.

Part 2: Perform a Targeted Social Engineering Attack

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



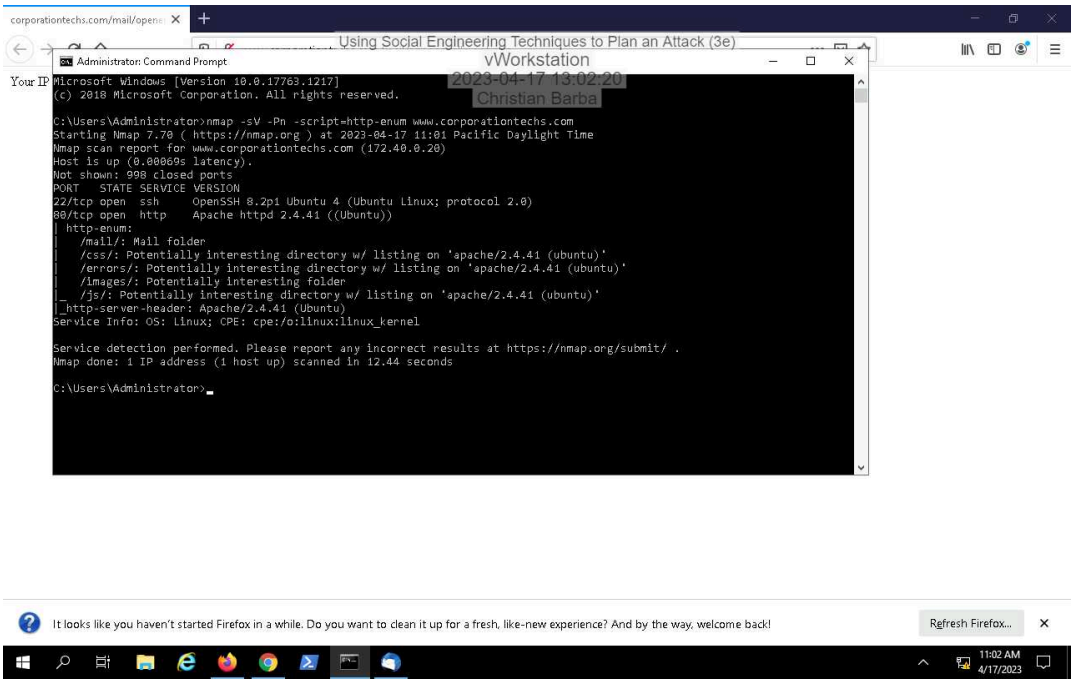
5. **Make a screen capture** showing the **resulting web page**.



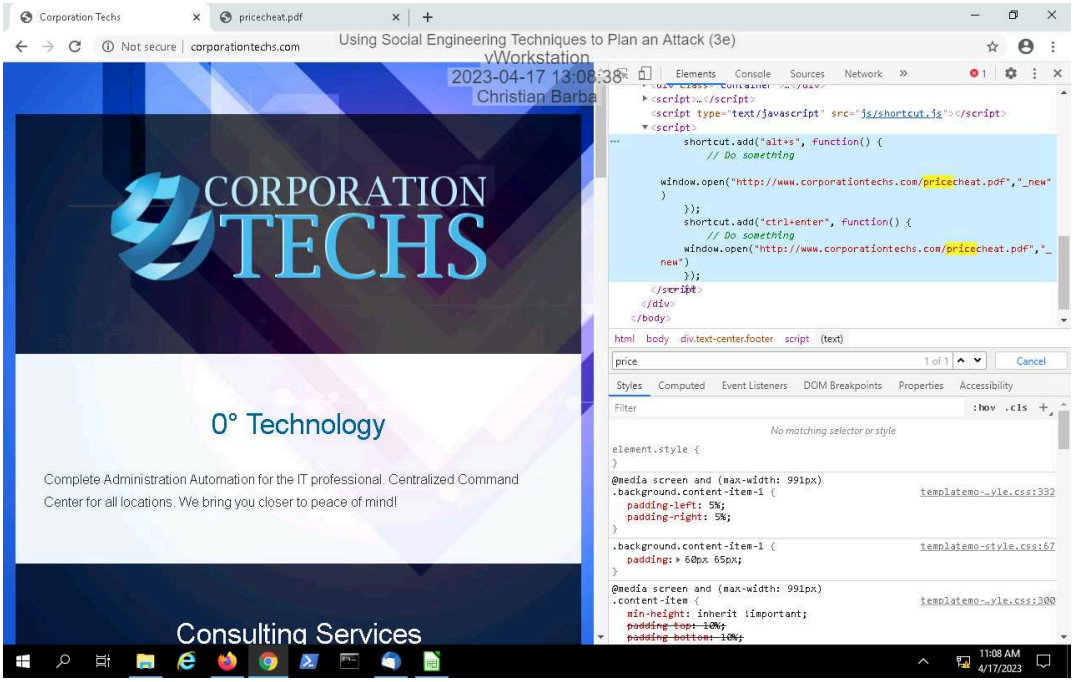
Section 3: Challenge and Analysis

Part 1: Investigate a Data Leak

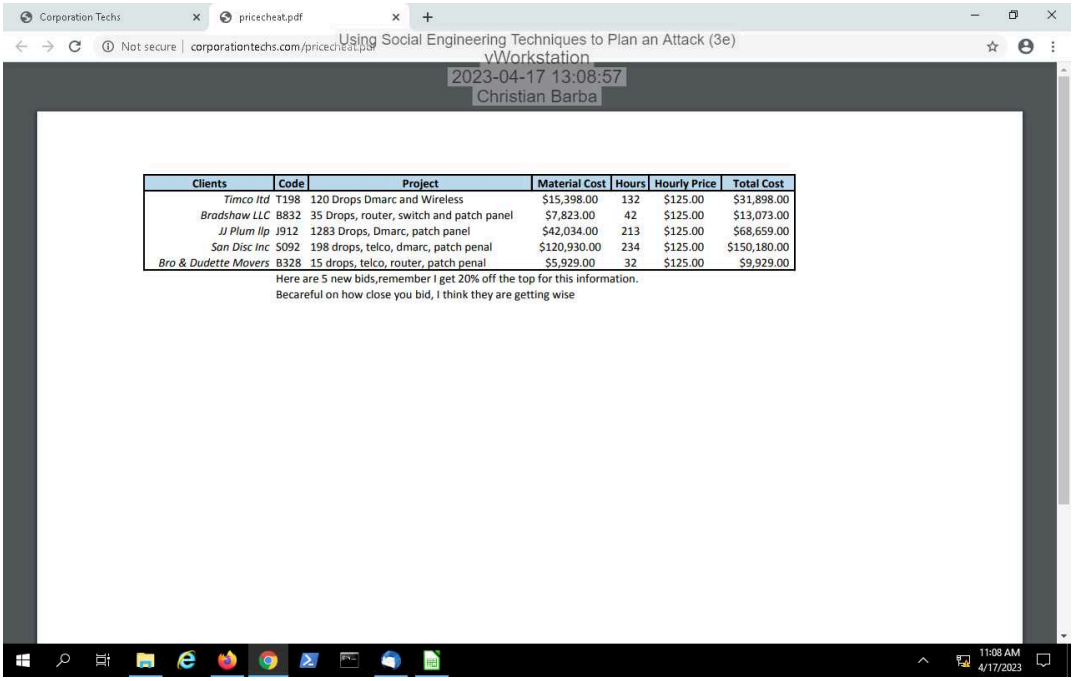
3. **Make a screen capture** showing the **results of the Nmap scan**.



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.

What I would do to continue my investigation would be to search through the logs to see if there were any commands ran similar to that of the GET command that they used to obtain our records. Before this however, I would make sure to take the script that led to this data leak out of my company's code to ensure this wouldn't happen again. I would rely mostly on technical measures because I think if the stealing was captured through the logs, the destination of these files would also be found. This could lead us to finding out who was in charge of stealing these documents or where these documents were sent. Either way, names will be popping up if we track down addresses that this attack was linked to. There is also a social engineering technique we could apply to this scenario. For example, if a company received our data leaks, signs could point us to an employee that used to work at this company in the past. This would show us that we have an insider threat that purposefully added bad code to our website to obtain easier access to our files. Lastly, it is also important to patch ports 22 and 80 as these are ports that attackers use to infiltrate a server. Ensuring that these ports are closed would also help keep our files safe.