

Using Social Engineering Techniques to Plan an Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Supplemental Lab 03

Student:	Email:
Dillen Dela Cruz	dillen.delacruz@my.utsa.edu

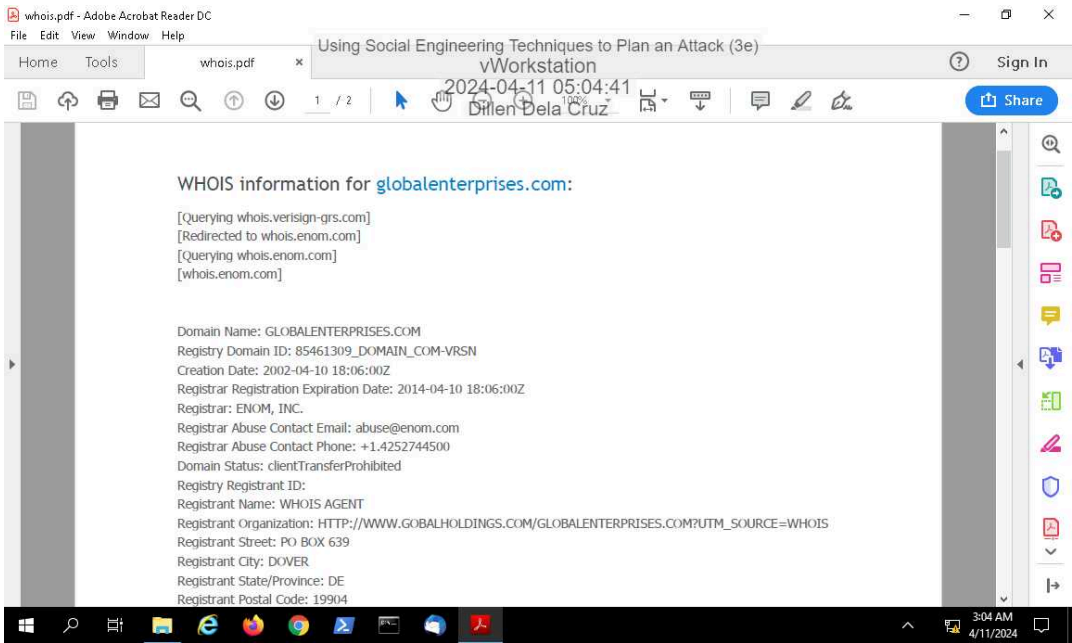
Time on Task:	Progress:
25 hours, 42 minutes	100%

Report Generated: Thursday, April 18, 2024 at 7:40 PM

Section 1: Hands-On Demonstration

Part 1: Observe Targeted Social Engineering Research

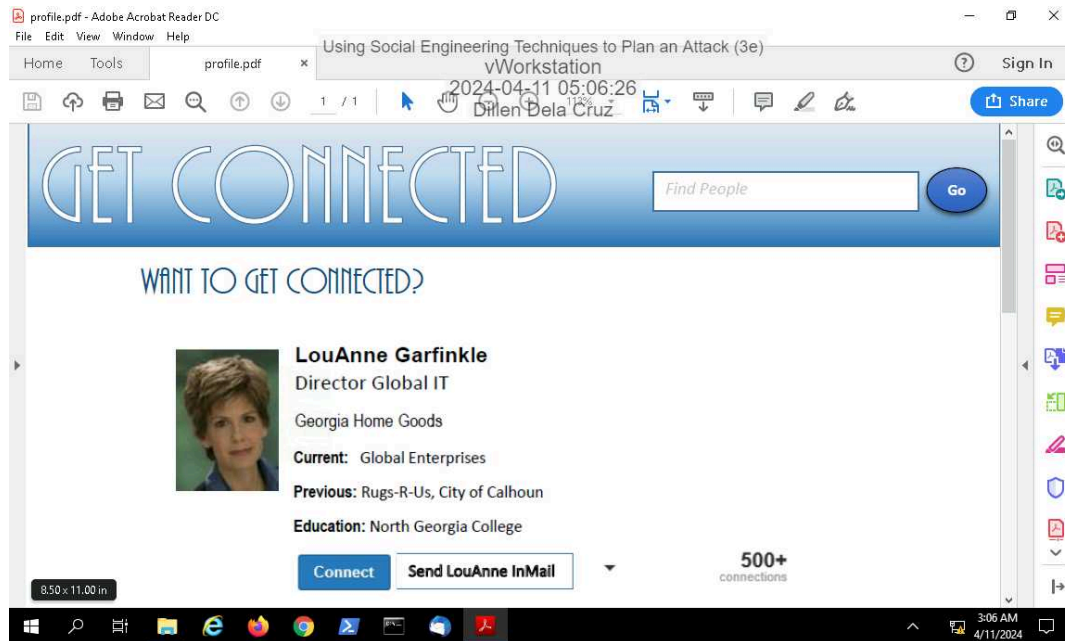
7. Make a screen capture showing the whois information for Global Enterprises.



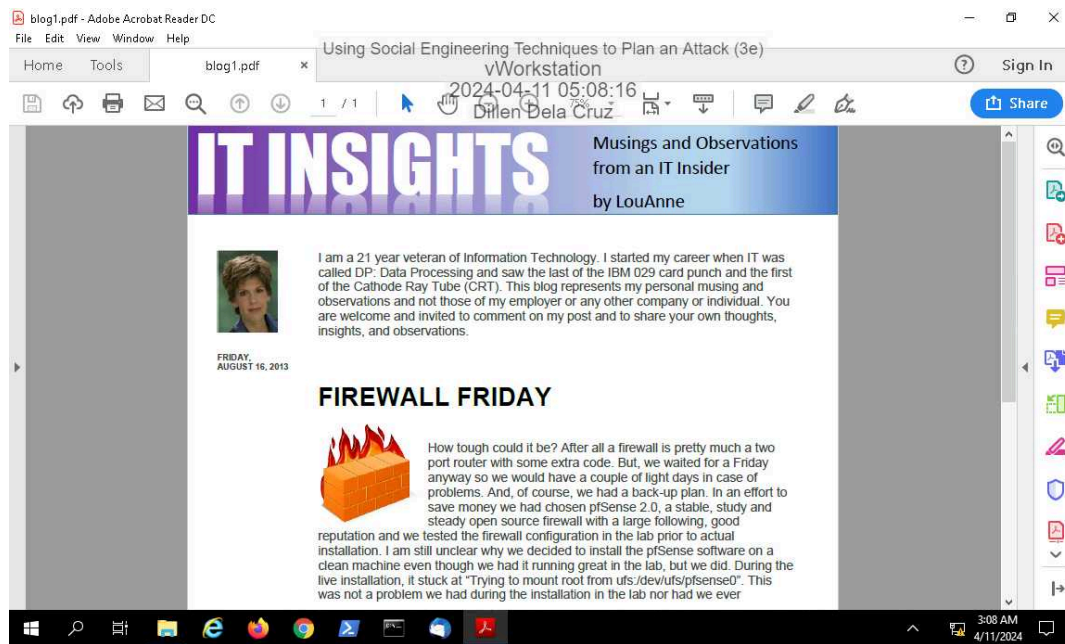
Using Social Engineering Techniques to Plan an Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Supplemental Lab 03

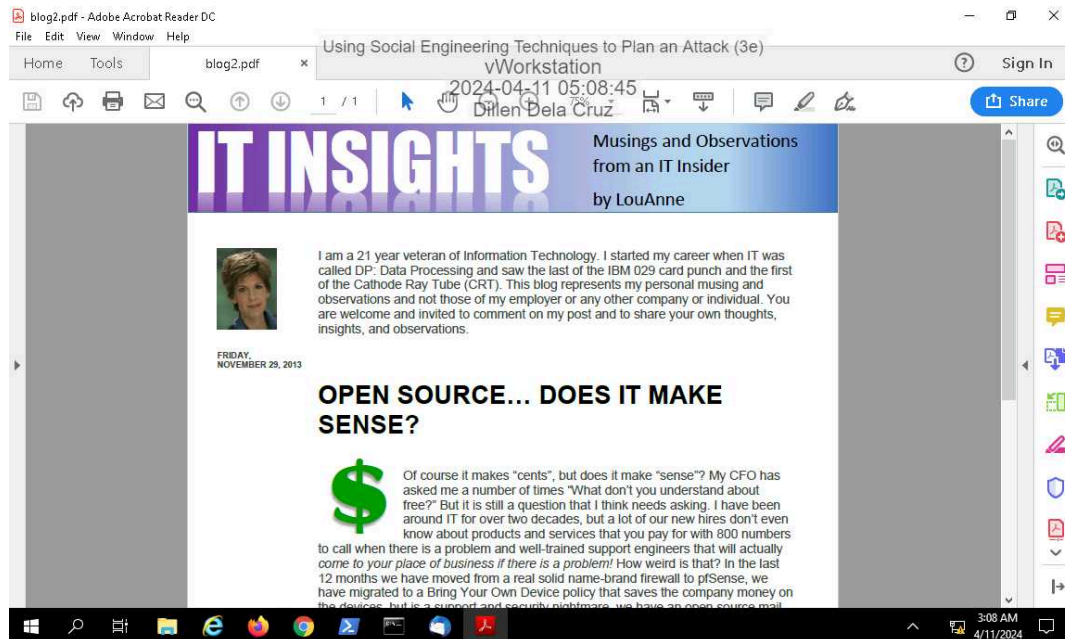
12. Make a screen capture showing LouAnne's GetConnected profile.



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.

Based on my external research, I've found that there's no one-size-fits-all answer when it comes to the firewall versions used by global enterprises. However, some commonly chosen versions include Fortinet FortiGate. Currently, the installed version is FortiGate / FortiOS 7.4, which was last updated in April 2024.

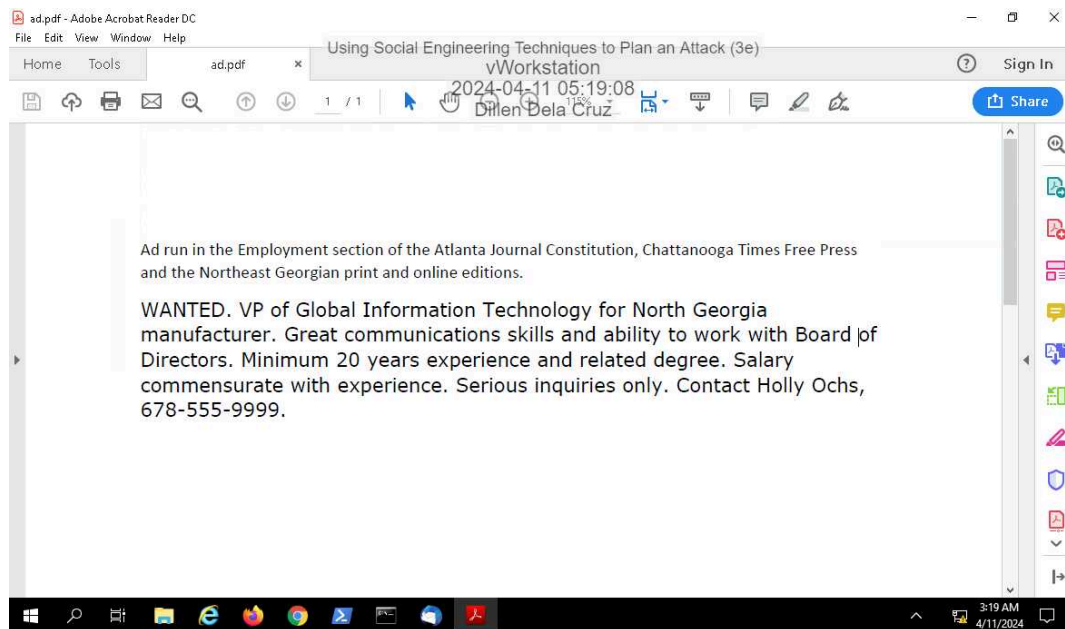
Works Cited Fortinet. "FortiGate / FortiOS 7.4." Fortinet Document Library, <https://docs.fortinet.com/product/fortigate/7.4>. Accessed 18 April 2024. SoftwareG. Wikipedia, <https://softwareg.com.au/blogs/internet-security/what-version-of-firewall-did-global-enterprises-install>. Accessed 18 April 2024.

Part 2: Observe a Targeted Reverse Social Engineering Attack

Using Social Engineering Techniques to Plan an Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Supplemental Lab 03

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



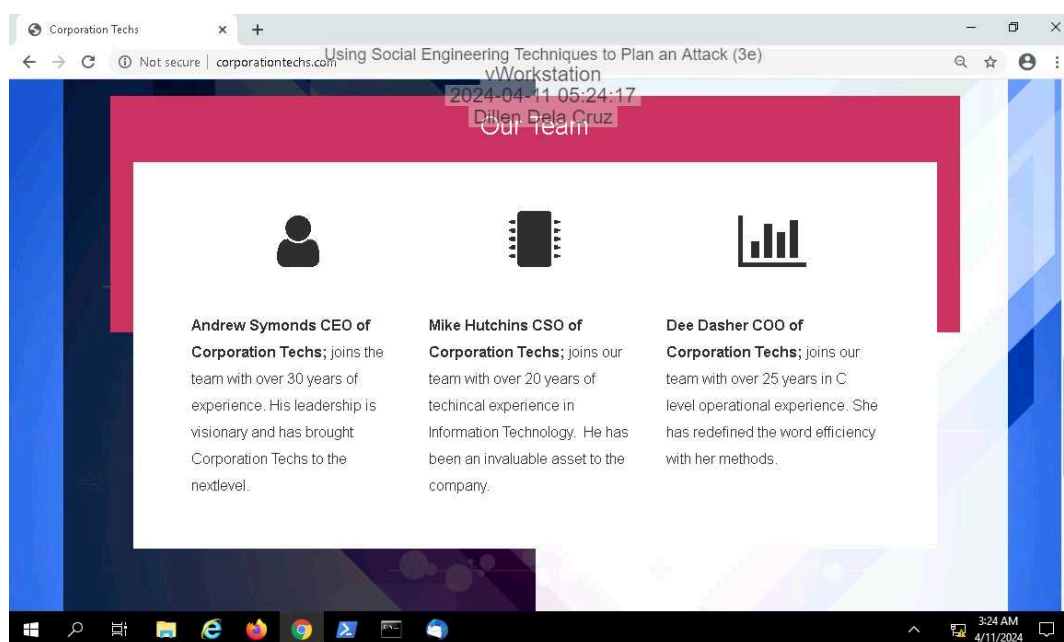
Section 2: Applied Learning

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?

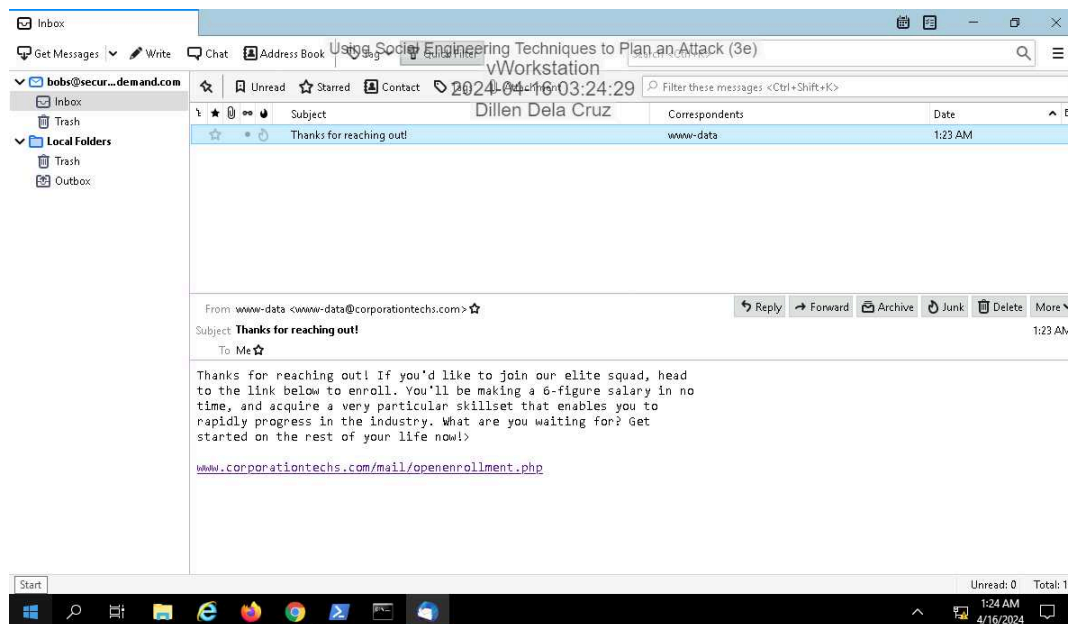
Andrew Symonds attended San Diego State University for his college education, though the specific years are unspecified in the "Education" section of his LinkedIn profile. He currently resides in Addison, Texas. In terms of employment history, Andrew has served as a sales executive for 13 years and 11 months with Wodash Incorporated.

Mike Hutchins pursued his college education at Virginia Tech from 1992 to 1996. Similar to Andrew, he resides in Addison, Texas. Mike's longest period of previous employment was as a security officer for 7 years and 4 months with Aegis Secured.

Dee Dasher graduated from Texas State University, spanning the years 1985 to 1989. Like Andrew and Mike, Dee also lives in Addison, Texas. Her longest period of previous employment was in Operations for 8 years and 7 months with Dante's Inc.

Part 2: Perform a Targeted Social Engineering Attack

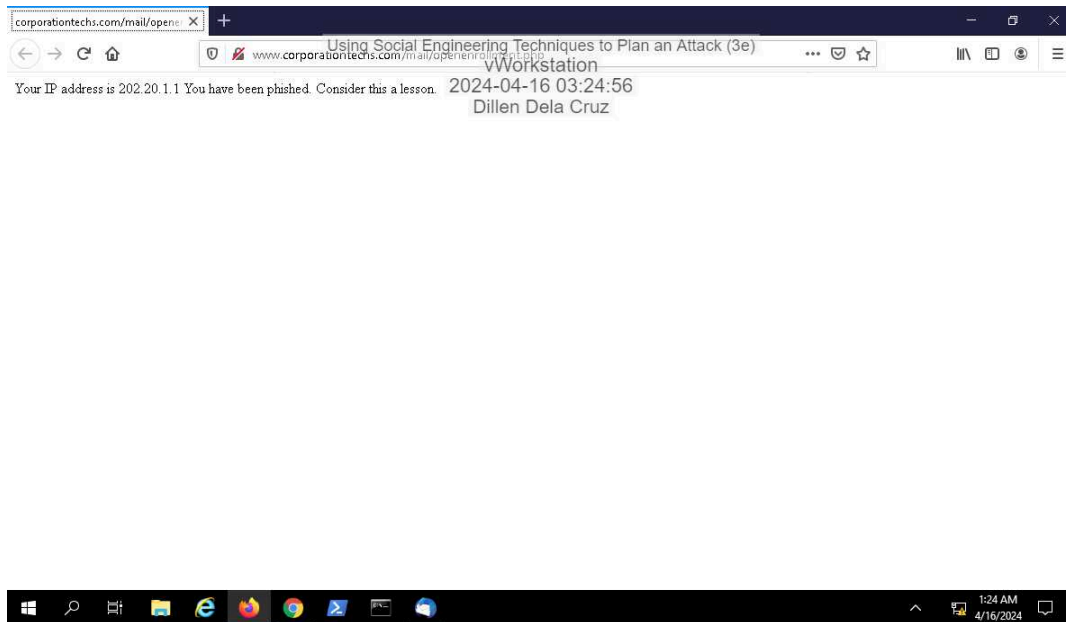
3. Make a screen capture showing the contents of the email.



Using Social Engineering Techniques to Plan an Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Supplemental Lab 03

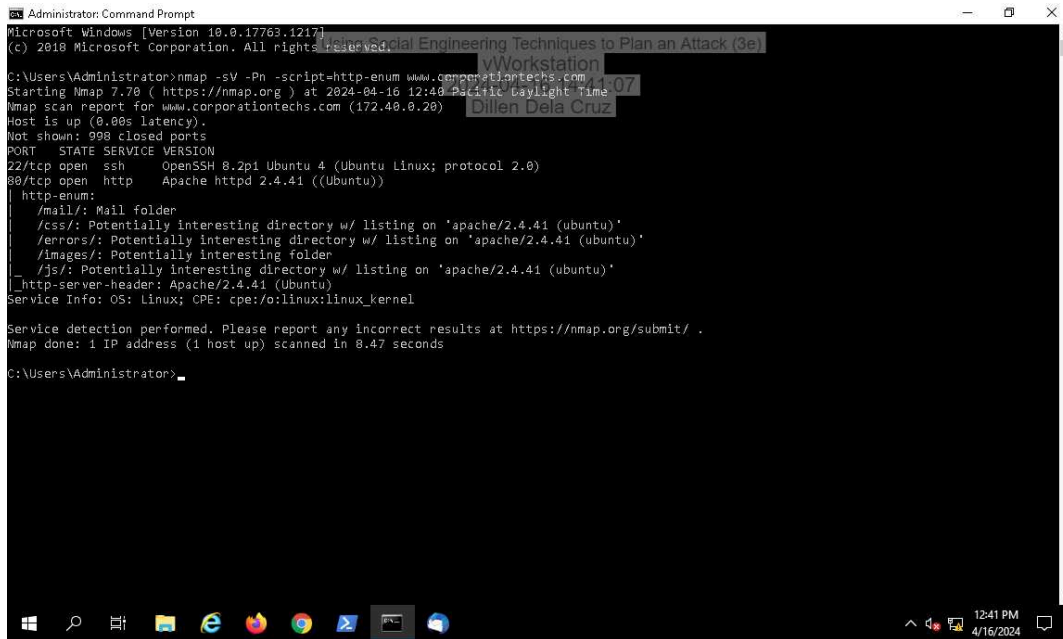
5. Make a screen capture showing the resulting web page.



Section 3: Challenge and Analysis

Part 1: Investigate a Data Leak

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



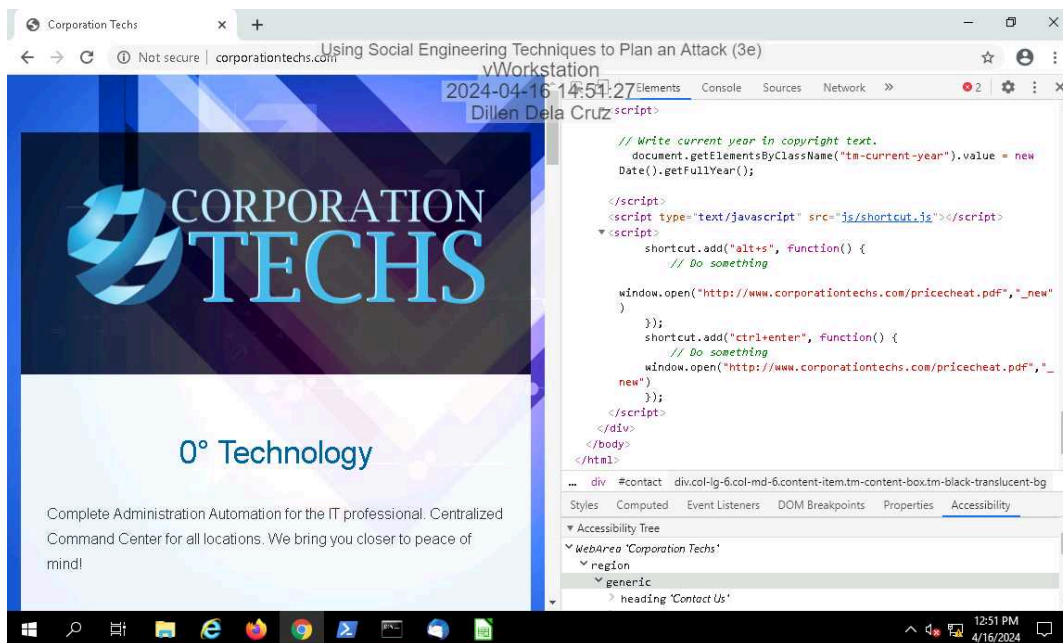
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1217]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nmap -sV -Pn -script=http-enum www.corporationtechs.com
Starting Nmap 7.70 ( https://nmap.org ) at 2024-04-16 12:48 Pacific Daylight Time
Nmap scan report for www.corporationtechs.com (172.48.0.20)
Host is up (0.00s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
http-enum:
  /mail/: Mail folder
  /css/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
  /errors/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
  /images/: Potentially interesting folder
  /js/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
  _http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.47 seconds

C:\Users\Administrator>
```

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



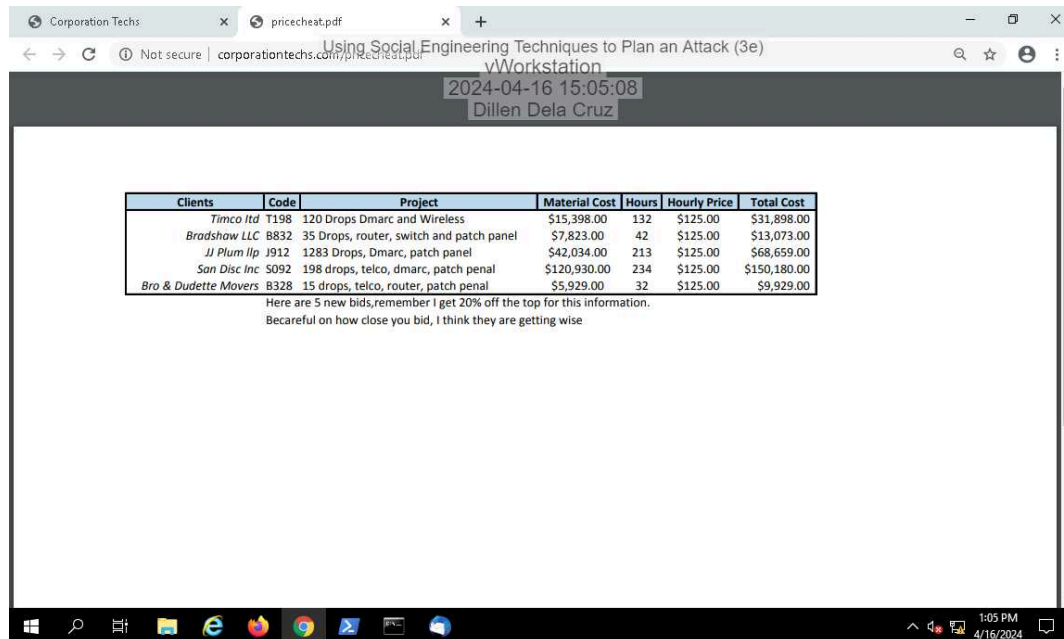
```
Corporation Techs
Using Social Engineering Techniques to Plan an Attack (3e)
2024-04-16 14:51:27
Dillen Dela Cruz
// Write current year in copyright text.
document.getElementsByClassName("tm-current-year").value = new
Date().getFullYear();

</script>
<script type="text/javascript" src="js/shortcut.js"></script>
<script>
  shortcut.add("alt+s", function() {
    // Do something

    window.open("http://www.corporationtechs.com/pricecheat.pdf", "_new"
  );
  });
  shortcut.add("ctrl+enter", function() {
    // Do something
    window.open("http://www.corporationtechs.com/pricecheat.pdf", "_
new");
  });
</script>
</div>
</body>
</html>

... div #contact div.col-ig-6.col-md-6.content-item.tm-content-box.tm-black-translucent-bg
Styles Computed Event Listeners DOM Breakpoints Properties Accessibility
v Accessibility Tree
v WebArea 'Corporation Techs'
  v region
    v generic
      > heading 'Contact Us'
```


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



Part 2: Continue the Investigation

Write a brief summary of your recommendations.

To continue the investigation and catch the culprit responsible for transferring data from the pricesheet.xlsx file to a competitor, a wide approach combining technical measures and social engineering techniques is essential. On the digital forensics front, it offers an important direction for analysis. By examining server logs, network traffic, and system activity, investigators can trace the origin of file transfers using tools such as packet sniffers and intrusion detection systems. Additionally, analyzing the metadata of transferred files provides valuable insights into their source and any alterations made, shedding light on the culprits identity and methods. Implementing endpoint monitoring software on corporate devices further enhances surveillance, enabling the tracking of user activity and detection of unauthorized access or file transfers. In addition to these you can add social engineering techniques such as crafting convincing emails designed to lure the culprit into revealing themselves or providing information about their actions can be particularly effective. For instance, sending emails disguised as legitimate requests for information related to the price sheet transfer may prompt a response from the culprit. By implementing a combination of technical and social engineering skills, investigators can significantly strengthen the investigation's success and increase the likelihood of identifying and catching the individual responsible for the data breach.