### **set1.pcap**

**1. What application protocol was used to transfer files from PC to server?**  
FTP (file transfer protocol) was used to transfer these files

**2. Briefly describe why the protocol used to transfer the files is insecure?**  
Everything was transmitted in plaintext. There is a security flaw with FTP that all information, including usernames, passwords, and files are sent over the network as plaintext. Because it is not encrypted, anybody can read the credentials and reconstruct the files.

**3. What is the secure alternative to the protocol used to transfer files?**The secure alternative to FTP is FTPS that uses SSL to encrypt data transmitted over the network. Another secure alternative to FTP is SFTP. It encrypts both credentials and content.

**4. What is the IP address of the server? (be careful)**  
192.168.1.215

**5. What was the username and password used to access the server?**  
Username: wallstreetbets  
Password: MoneyIsTheMostImportantThingInTheWorld

**6. How many files were transferred from PC to server?**   
7 files (2 PDF, 5 JPG)

**7. Extract all the files that were transferred from PC to server. VERY IMPORTANT: each file MUST have proper file extension. These files must be part of your submission!  How were you able to determine the type of each file?**  
I saved these files from wire shark to my computer in raw format. Then I used terminal and command ‘file [name]’ to check for file extension.

### **set2.pcap**

**8. How many packets are there in this set?**  
76409

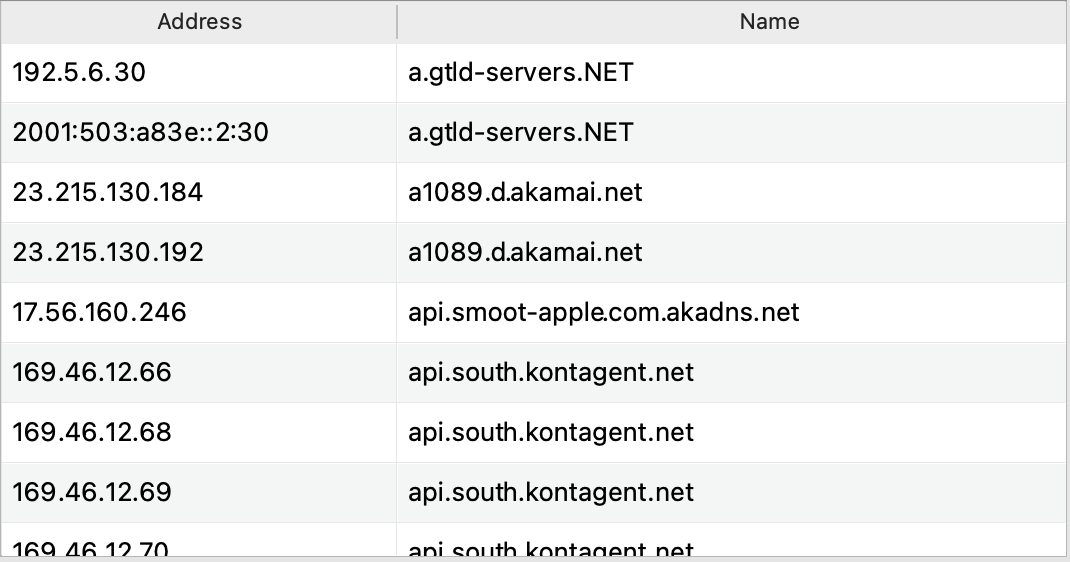
**9. How many plaintext username-password pairs are there in this packet set? Please do not count accounts such as "anonymous" or "cisco".**2 pairs

USER: wbgapp31216 **PASS:** Q827wO6656!nW99\_a1  
USER: ventas@wekiguatemala.com.gt **PASS:** "$Alesgt1.1"

**10. For each of the plaintext username-password pair that you found, identify the protocol used, server IP, the corresponding domain name if possible (e.g., google.com), and port number.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Packet # | protocol used | server IP | domain | port |
| 18488 | HTTP | 176.58.103.138 | Worldboardgames.com | 80 |
| 27142 | HTTP | 176.58.103.138 | icloud.com | 80 |
| 5430 | HTTP | 176.58.103.138 | Hotmail.com | 80 |

**11. Of all the plaintext username-password pairs that you found, how many of them are legitimate? That is, the username-password was valid, access successfully granted? Please do not count any anonymous or generic accounts.**  
The username-password pairs are valid. The HTTP login is successful by looking at what happened after each packet (HTTP 401 Auth) the next response from the web server was a 200 OK status

**12. Provide a listing of all IP addresses with corresponding hosts (hostname + domain name) that are in this PCAP set. Describe your methodology.**Use the statistics tool in Wireshark and find "Resolved Address". The snapshots of few of the items from the list below, as I wasn’t able to copy/paste the entire list from Wireshark and Ming confirmed it was sufficient to take few snapshot as prove.  
  
****  
****

**  
**

### **set3.pcap**

**13. How many plaintext username-password pairs are there in this packet set?**Three   
(YnJvZGdlcnM6VGhleVBsYXllZFdpdGhHcmVhdENoYXJhY3Rlcg==)( ZG1veWVzOklBbUFGb290YmFsbEdlbml1cw==)(YW91cnNsZXI6SWQxMHRFeHBlcnQ=)

**14. For each of the plaintext username-password pair that you found, identify the protocol used, server IP, the corresponding domain name if possible (e.g., google.com), and port number.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Packet # | protocol | server IP | domain | port |
| 60 | HTTP | 130.64.23.35 | www.eecs.tufts.edu | 80 |
| 138 | HTTP | 130.64.23.35 | www.eecs.tufts.edu | 80 |
| 163 | HTTP | 130.64.23.35 | www.eecs.tufts.edu | 80 |

**15. Of all the plaintext username-password pairs that you found, how many of them are legitimate?**  
None of them are legitimate. They all have this note “ This server could not verify that you

are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required”

### **General Question**

**16. Based on PCAP sets 1 - 3, what advice would you give to the owners of the username-password pairs that you found so their account information would not be revealed "in-the-clear" in the future?**  
It is better to use HTTPS and SFTP, as a secure protocol, when using any passwords or sensitive information. This will ensure encryption and more difficult to read/steal data. Also, try to use SSL/TLS when you have to get access to emails with IMAP to secure usernames and passwords. To be extra safe, don’t use public Wi-Fi networks for any personal data that are not utilized by WPA encryption. The VPN tool can also be used.