Cary Co. Packet Analysis and Security Audit

Brea Spann, Chis Hooper, Keziah Rogers, Torrie Emery

Stevenson University

IS-232: TCP/IP Communication Protocol for Windows and Unix

Professor Redd

May 4, 2022

Executive Overview:

Cary Co is a highly regarded organization with valuable industry secrets. It has proven to be a strong competitor in the technological field. Unfortunately, Cary Co failed to employ a robust security protocol which allowed Cary Co's competitors to gain access to sensitive information. While the situation was unfortunate, Cary Co. took the necessary measures to rectify its weakened security front. Cary Co engaged a contractor to fully assess who, where, and how the security breaches occurred, along with recommendations to mitigate their vulnerabilities. Cary Co uses several unencrypted protocols, including Telnet, IMAP, POP, and FTP. More importantly, Cary Co was not using Secure Shell or Secure Socket Shell (SSH). The SSH protocol was constructed to deliver a secure alternative to unsecured remote shell protocols. It utilizes a client-server paradigm, in which clients and servers communicate via a secure channel.1 Employing SSH along with strengthening their password protocol, and other security measures will facilitate Cary Co in a long-term security solution.

Analysis:

During the time of packet collection, a multitude of interesting traffic and activities were discovered. To begin, a user named Ronald logged into a server via telnet with the password of golf. As telnet data is not encrypted, we can see all of the data transmitted to and from the server. We can see that there was no home directory listed for the user Ronald. Because of this, the user was sent to the root folder which contains a large amount of system files as well as directories for other users. The user then used the LS -l command which stands for list with the option long. This command lists all files and directories in the working directory; in this case the root directory. The user Ronald proceeded to try and create a new directory named "secretresearch" as seen in the following command excerpt: *$ mmkkddiirr sseecrcreettrreesseeaarrcchh.* You can see how the letters are duplicated in the test readout. This is because the server is confirming the entry of the specific character. The user was unable to create the directory because they did not have the proper permissions as seen with this return message from the server: *mkdir: Failed to make directory "secretresearch"; Permission denied.* Since the user was unable to make a directory, they created a text document named “secretresearch” using the VIM text editor program. Ronald then wrote the following into the ext document:

it.thhiiss iiss ttoo.

.this is t.

.this is iimmppoorrttaanntt ttoo JJiimm -- tteellll nnoooonnee!!

.

This is too

This is t

This is important to jim - tell noone

Interestingly, the user proceeded to exit vim forcefully without saving the content to the text file. This means that someone who views the text file will see nothing as the file remains blank. Finally, Ronald attempted to change their password however, the passwords entered did not meet minimum password requirements and so the user gave up and terminated the telnet session.

There was also a separate telnet session started with the user TOM logging into the server. Tom ran the commands $who , $uname -a, $uptime, and $ping 8.8.8.8. The who command displays the users currently logged into the system. The uname - a command shows information about a system including kernel, kernel version, operating system, and many others. The uptime command shows how long the server has been operating without a restart. And finally, the ping command is used to send a ICMP ping packet to a server to check if it is reachable. In this case the Google DNS server with IP 8.8.8.8 was contacted.

Moving away from telnet data streams, there were a multitude of email packets discovered using the IMAP, POP, and SMTP protocols. The contents of these emails included the mentioning of a key to the office under the front mat of the building. There was also a login for the account newb@carybarker.com with the password golf1 as seen in the following excerpt.

A001 LOGIN "newb@carybarker.com" "golf1"

A001 OK LOGIN Ok.

Finally, reviewing the FTP packets, there was a file uploaded to the FTP server. The name of the file was: *network wiring diagram.jpg.* The file was uploaded by the *backups@carybarker.com* account using the password edmond. The file's permissions were also changed by the same account to 644 which equated to read and write access to the owner, read access to the group, and read access to everyone else. This makes the file accessible to anyone who logs into the FTP server.

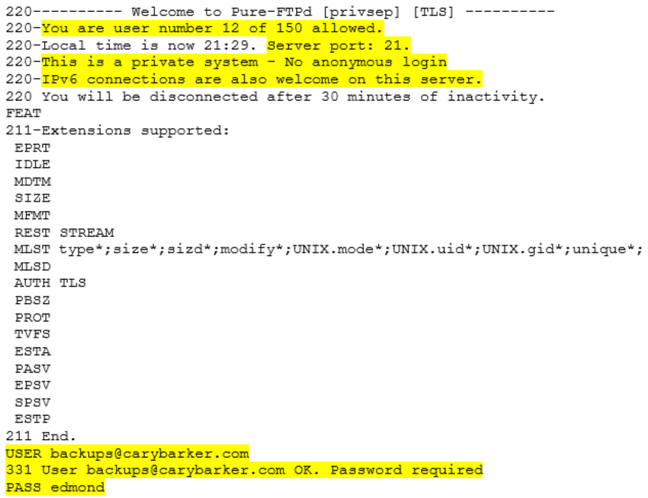
Security Analysis:

The insecurities identified included that the ports were not secure, the passwords were shown in the capture packets, weak passwords were used for the user accounts, there were no restricted directories listed when a user accessed the system, and the company used an obsolete version of a specific email software. These issues were easily noticed when the capture packets were searched. There was also malicious traffic when a specific user attempted to change their password more than once, and there was also suspicious activity when certain permissions were denied. It is obvious that the company did not monitor their systems' applications, they did not monitor the network traffic, and they did not encrypt the firewall. One of the biggest problems involved showed how sensitive information on the company's network was simple and not protected from attackers.

Discovered Sensitive Information

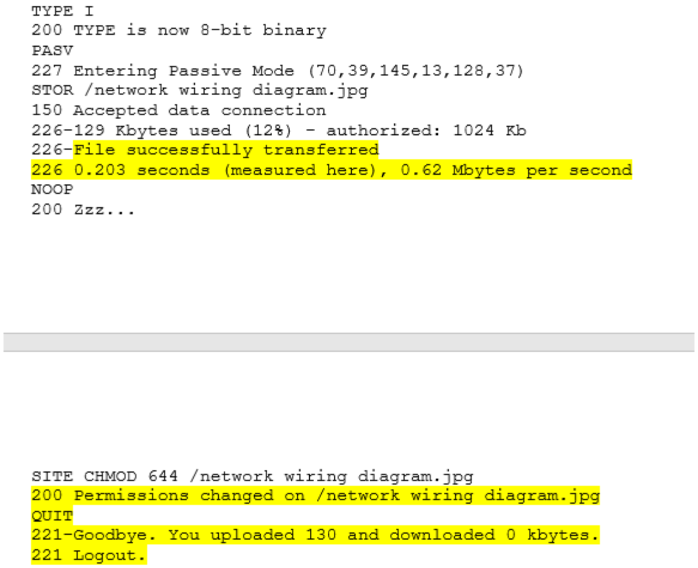
FTP Packet Analysis

The sensitive information that was seen in the traffic was employee login and password information. For example, in the FTP data 1 packet there is a user with the username "backups@carybarker.com" and the password was edmond. The data packets also showed port 21 being used, which is File Transfer Protocol (FTP), and this port allows connections to be made between hosts on the network **(See figure 1).** FTP data 1 also showed that network wiring diagram.jpg was sent across the network by the user caryba5 on March 21st. FTP data 2 shows that the user successfully transferred the file, but the permissions were changed. In other words, the network removed the restrictions and allowed the image to be uploaded by the user **(See figure 2).**



```
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 12 of 150 allowed.
220-Local time is now 21:29. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 30 minutes of inactivity.
FEAT
211-Extensions supported:
 EPRT
 IDLE
 MDTM
 SIZE
 MFMT
 REST STREAM
 MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*;
 MLSD
 AUTH TLS
 PBSZ
 PROT
 TVFS
 ESTA
 PASV
 EPSV
 SPSV
 ESTP
211 End.
USER backups@carybarker.com
331 User backups@carybarker.com OK. Password required
PASS edmond
```

Figure 1



```
TYPE I
200 TYPE is now 8-bit binary
PASV
227 Entering Passive Mode (70,39,145,13,128,37)
STOR /network wiring diagram.jpg
150 Accepted data connection
226-129 Kbytes used (12%) - authorized: 1024 Kb
226-File successfully transferred
226 0.203 seconds (measured here), 0.62 Mbytes per second
NOOP
200 Zzz...
```

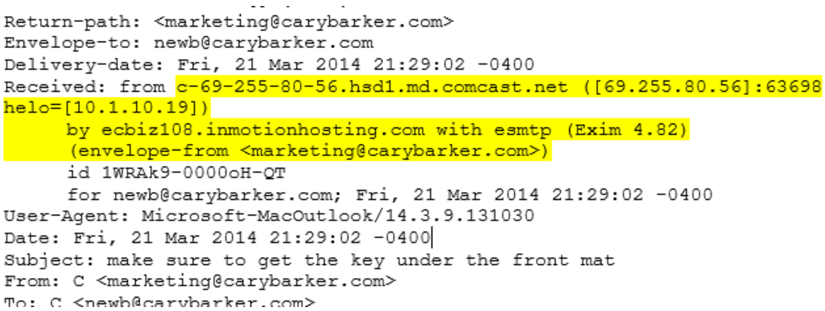
```
SITE CHMOD 644 /network wiring diagram.jpg
200 Permissions changed on /network wiring diagram.jpg
QUIT
221-Goodbye. You uploaded 130 and downloaded 0 kbytes.
221 Logout.
```

Figure 2

IMAP Packet Capture Analysis

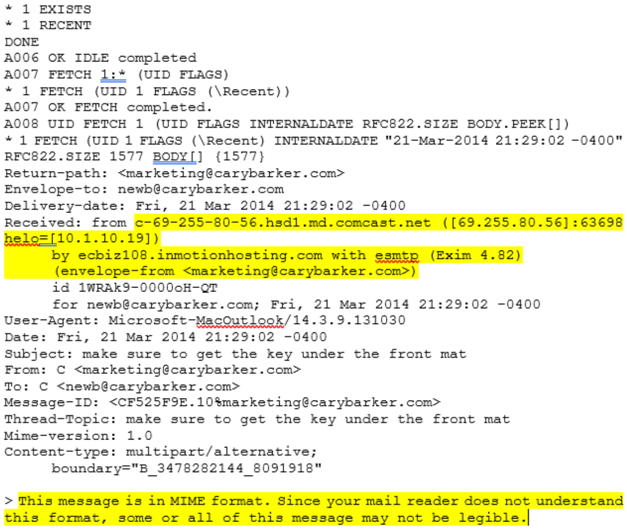
IMAP data 1 displays that the email message was received from c-69-255-80-56.hsd1.md.comcast.net with an IP address of 69.255.80.56. After researching this address, it is determined that the domain is comcast.net, the ISP is Comcast Cable Communications LLC, the address is a Unicast, the region is Maryland, and the country is the United States (*69.255.242.38 IP address geolocation lookup demo*). The address was also followed by 10.1.10.19 which is a private IP address, and it was sent by “ecbiz108.inmotionhosting.com with esmtp (Exim 4.82)” **(See figure 3).** The problem identified is that Exim 4.82 was used to send information because it is outdated (Project., *Exim internet mailer*). It is not encouraged that companies use expired software because they would be prone to easily receiving attacks, their information would not be secure, they would not have access to the necessary features for the software to be properly executed, and the performance of the software might not be adequate with the companies' systems.

IMAP data 1 shows that the email message used MIME (Multipurpose Internet Mail Extension) format to be sent across the network. MIME is a transferable and encoded file format that is used by email services. MIME also allows images, audio files, and different file attachments to be sent on a network (Cnet). The message about MIME stood out in the packet because it also stated "Since your mail reader does not understand this format, some or all of this message may not be legible" **(See figure 4)**. This was a problem because the receiver of the message could open a corrupt file, they might not understand the sender's true intentions, and they could potentially load a virus onto their computer that could spread to other systems. Another data packet also showed that the company's email service did not accept bulk email which is wise to have because it prevents attackers from overloading a system with malware located in multiple emails.



```
Return-path: <marketing@carybarker.com>
Envelope-to: newb@carybarker.com
Delivery-date: Fri, 21 Mar 2014 21:29:02 -0400
Received: from c-69-255-80-56.hsd1.md.comcast.net ([69.255.80.56]:63698
helo=[10.1.10.19])
      by ecbiz108.inmotionhosting.com with esmtp (Exim 4.82)
      (envelope-from <marketing@carybarker.com>)
      id 1WRAk9-0000oH-QT
      for newb@carybarker.com; Fri, 21 Mar 2014 21:29:02 -0400
User-Agent: Microsoft-MacOutlook/14.3.9.131030
Date: Fri, 21 Mar 2014 21:29:02 -0400
Subject: make sure to get the key under the front mat
From: C <marketing@carybarker.com>
To: C <newb@carybarker.com>
```

Figure 3



```
* 1 EXISTS
* 1 RECENT
DONE
A006 OK IDLE completed
A007 FETCH 1:* (UID FLAGS)
* 1 FETCH (UID 1 FLAGS (\Recent))
A007 OK FETCH completed.
A008 UID FETCH 1 (UID FLAGS INTERNALDATE RFC822.SIZE BODY.PEEK[])
* 1 FETCH (UID 1 FLAGS (\Recent) INTERNALDATE "21-Mar-2014 21:29:02 -0400"
RFC822.SIZE 1577 BODY[] {1577}
Return-path: <marketing@carybarker.com>
Envelope-to: newb@carybarker.com
Delivery-date: Fri, 21 Mar 2014 21:29:02 -0400
Received: from c-69-255-80-56.hsd1.md.comcast.net ([69.255.80.56]:63698
helo=[10.1.10.19])
      by ecbiz108.inmotionhosting.com with esmtp (Exim 4.82)
      (envelope-from <marketing@carybarker.com>)
      id 1WRAk9-0000oH-QT
      for newb@carybarker.com; Fri, 21 Mar 2014 21:29:02 -0400
User-Agent: Microsoft-MacOutlook/14.3.9.131030
Date: Fri, 21 Mar 2014 21:29:02 -0400
Subject: make sure to get the key under the front mat
From: C <marketing@carybarker.com>
To: C <newb@carybarker.com>
Message-ID: <CF525F9E.10%marketing@carybarker.com>
Thread-Topic: make sure to get the key under the front mat
Mime-version: 1.0
Content-type: multipart/alternative;
      boundary="B_3478282144_8091918"

> This message is in MIME format. Since your mail reader does not understand
this format, some or all of this message may not be legible.
```

Figure 4

Recommendations:

Cary Co's security is not the best, so it is not surprising that sensitive information is being leaked to competitors. There are multiple ways that Cary Co can improve the network's security. The company uses Telnet, IMAP, POP, and FTP. All of the protocols used are unencrypted. This makes all information in transit insecure. All data including passwords are sent as clear text over the network. Cary Co can implement encryption by using Secure Shell (SSH). "SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network" (Loshin, 2021). Secure Shell was created to replace insecure terminal emulation or login programs such as Telnet, remote login, and remote shell. SSH also replaces file transfer programs such as File Transfer Protocol (FTP) and remote copy.

In addition, Cary Co should start using SFTP instead of FTP as it is more secure. SFTP is used as organizations should be more security conscious as threats have expanded. SFTP can be used to transfer files while maintaining the C.I.A Triad.“Secure file transfer systems offer a basic way to get files from one place to another while safeguarding their confidentiality, integrity, and availability” (Scarfone, 2016). SFTP is also inexpensive and has been widely used for decades.

When it comes to the passwords being used at Cary Co, the current passwords are too simple. Having simple passwords makes it easy for someone to get into the network and access sensitive information. Cary Co should implement a password policy to defend the network as passwords are the first line of defense. “A well-defined password policy enables companies to layout password security best practices and recommendations while ensuring users understand password requirements and their role in keeping companies safe” (Kirvan, 2021). Password policies establish rules for password administration, penalties for violation of password rules, procedures for addressing invalid access attempts, and other security-related activities. The following are important guidelines for creating a strong and user-friendly password policy. Consider the use of one-time passwords. Use password management software to help users create, encrypt, store, and update passwords. Establish a password team within the security team. Consider using single sign-on to reduce required access steps for different systems. Provide periodic password awareness, education, and training activities to all employees. Lastly, make sure password policies have sufficient security requirements including a minimum length, the use of capital letters, lowercase letters, numbers, and special characters.

One of the employees left a key under a doormat and sent an unencrypted email to a coworker about it. This is mishandling of security because anyone can look under the doormat and get access to something that they shouldn’t. To prevent this, physical security needs to be implemented. “Physical security is the protection of personnel, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage to an enterprise, agency, or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism, and terrorism” (Cobb, 2021). Security measures should limit and control who has access to sites, facilities, and materials. Access control encompasses the measures taken to limit exposure of certain assets to authorized personnel only. ID badges, keypads, and security guards can be used to implement access control. Surveillance can be used to monitor the activity of locations and facilities. Examples of surveillance include patrol guards, heat sensors, cameras, and notification systems. Lastly, companies can use a log and trail to record what is accessed and who is accessing it when using keys and hardware.

Summary:

In summary, due to the lack of encryption and basic cybersecurity practices, Cary Co. had no security measures in place to block the hack. Some of the recommendations that should be put into place immediately include training staff on the protection of personnel, hardware, software, networks, and data from both physical and technical events that could cause serious loss or damage to the organization. Also, deploying access control systems to monitor and regulate who has access to sites, facilities, and materials. And finally, implementing a good security policy that includes regulations on passwords, file access, and physical security will help ensure that Cary Co. can minimize future cybersecurity incidents.

References

Cnet. (n.d.). *Download your free trial*. WinZip. Retrieved May 2, 2022, from https://www.winzip.com/en/learn/file-formats/mime/#:~:text=Multipurpose%20Internet%20Mail%20Extension%20or,character%20sets%20other%20than%20ASCII.

Cobb, Michael. (2021). *Physical Security*. TechTarget. Retrieved May 3, 2022, from https://www.techtarget.com/searchsecurity/definition/physical-security

Kirvan, Paul. (2021). *How to Create a Company Password Policy*. TechTarget. Retrieved May 3, 2022, from https://www.techtarget.com/searchsecurity/tip/How-to-create-a-company-password-policy-with-template

Loshin, Peter. (2021). *Secure Shell (SSH)*. TechTarget. Retrieved May 3, 2022, from https://www.techtarget.com/searchsecurity/definition/Secure-Shell

69.255.242.38 IP address geolocation lookup demo. IP2Location. (n.d.). Retrieved May 2, 2022, from https://www.ip2location.com/demo/69.255.242.38

Project., T. E. (n.d.). *Exim internet mailer*. Exim Internet Mailer. Retrieved May 2, 2022, from https://www.exim.org/

Scarfone, Karen. *Choosing Secure File Transfer Products for Your Enterprise*. TechTarget. Retrieved May 3, 2022, from https://www.techtarget.com/searchsecurity/feature/Choosing-secure-file-transfer-products-for-your-enterprise