Barbara Garcia
ID: 011883626
1/15/2023

D482 – Secure Network Design Performance Assessment

A.

Business Requirements:

Company A deals with financial accounts and bank cards. Company B is involved in medical software with the potential to contain PHI and receives credit cards as payment. For both companies, business requirements dictate that it is critical to maintain confidentiality, integrity, and availability. Before the merger takes place, security and information problems need to be resolved to harden the company's network against attack by threat actors.

Company A Security Problems:

One security problem for Company A is that all users have local administrative passwords. This opens the network up to insider attacks and makes it more likely for a social engineering attack to be successful in gaining access to the network, as the adversary would only need to fool one user to gain access to admin capabilities. To prevent data access and exfiltration, administrative passwords should be limited to only the necessary users.

A second security problem for Company A are that 3 servers are running outdated versions of windows. The application server, file server and the server providing file transfer service and acting as an external web server are all running Windows 2012. Since these operating systems are no longer supported, they are no longer receiving updates and security patches and are therefore vulnerable to security breaches that could compromise the confidentiality, availability and integrity of personally identifiable information and financial data. All servers should be updated to a currently supported version of Windows.

Company A Infrastructure Problems:

One major problem with Company A's infrastructure is that major physical components of the network are no longer supported by the manufacturer. The Cisco 7600 border router and the Cisco 3750X switches are no longer supported by Cisco. Since the devices are no receiving firmware updates from the manufacturer, they are susceptible to attack. One example of this is documented incidents of Russian and Chinese threat actors exploiting unpatched Cisco routers (security week). To comply with business requirements, this out-of-date hardware needs to be replaced with up-to-date equipment and regularly updated with the latest available firmware.

Another flaw in Company A's infrastructure is the absence of a VPN connection for remote users to access the company's internal network. Data traveling between the user and the company network is therefore unencrypted and could be easily intercepted by threat actors. The sensitive nature of the data handled by the company necessitates encryption of data in motion.

Company B Security Problems

Company B also has security problems. One of these is that Telnet Port 23 is open. "When used over an unencrypted channel, things like usernames and passwords are transferred in clear text, allowing an attacker to eavesdrop on connections and discover confidential information" (Mike, 2021). Since Company B maintains credit card data and its software manages private personal and health information, it is important that confidentiality is maintained. Port 23 should be disabled, and the information sent through SSH via port 22.

Another security problem with Company B is that workstations and servers are running end of life operating systems. One server is running an outdated version of Apache Tomcat, and the company has workstations running Windows XP and Windows 7. Since these operating systems are no longer receiving updates and patches form Windows, they can contain weakness that can be exploited by threat actors.

Company B Infrastructure Problems

Company B has infrastructure problems that open it up to attack. The company's function of providing software to medical providers necessitates high availability, integrity, and confidentiality. One infrastructure problem is that there is no firewall between the web application servers and the internal network. This lack of separation makes the entire network

vulnerable to a threat actor compromising a web-facing server and then easily gaining access to the internal network.

Another infrastructure problem in Company B's network is that the Java RMI has default configuration settings making it vulnerable to remote code execution on the publicly facing server. Appropriate parameters need to be set on the virtualized device.

B1.

Company A Vulnerabilities

One vulnerability in Company A's network is that user accounts no longer required are not removed. Old accounts are often not monitored, and passwords not updated, so they can be used by a threat actor to access the network, potentially without being detected by the company.

A second vulnerability is that the company has port 21 for file transfer protocol open.

Company B Vulnerabilities

Company B also has vulnerabilities. One of these is related to Distributed Ruby which, "may permit unauthorized systems to execute distributed commands." (*Gain a Shell Remotely : Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities*, n.d.) These are referred to as Distributed Ruby (dRuby/DRb) multiple remote code execution vulnerabilities.

A second vulnerability in the network is that PostgreSQL admin is reachable from the internet.

B2.

Company A Impact, Risk & Likelihood

As to the vulnerability in Company A of user accounts no longer required not being removed, the risk is that these accounts can "quickly become a gateway for malicious hackers that can infiltrate sensitive systems and extract valuable information." (Stefan, 2023) The impact of an attack would be critical to business operations, especially given that all users have admin access. A bad actor who gained access to one of these user accounts would quickly have access

to the company's clients' personal and financial information. The likelihood for the vulnerability to be exploited is moderate. While it is an easily exploited vulnerability once discovered, the threat actor would need to be aware of the existence of these user accounts.

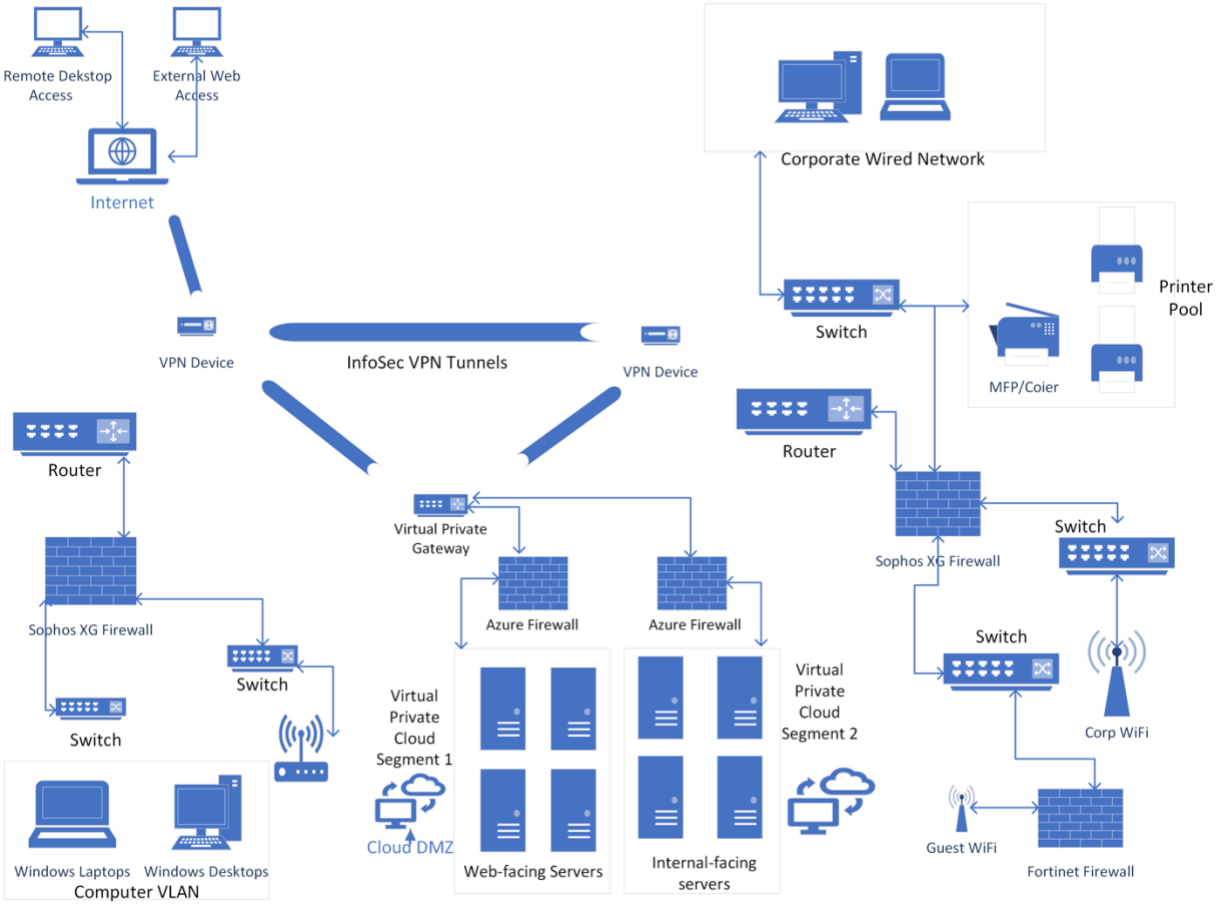
File transfer protocol, which uses port 20 and 21 is an outdated protocol. Port 21 being open in Company B's network leaves the company open to anonymous authentication, cross-site scripting, brute-forcing passwords, and directory traversal attacks. (Ibeakanma, 2022) Since it is simple to run a port scan using tools, like nmap, the likelihood of this vulnerability being exploited is high. The impact to the company if the vulnerability is exploited is very high, as anyone could sign in using anonymous authentication.

Company B Impact, Risk & Likelihood

As to the impact, risk, and likelihood of the Distributed Ruby Remote Code Execution Vulnerabilities. These are addressed in the vulnerability report for Company B. The impact of these vulnerabilities being exploited is critical. If threat actors can exploit the vulnerability, they will be able to execute commands on the application server, compromising its availability to the medical professionals that depend on the software for patient care and records. The likelihood of the attack occurring is high since it is an attack that can be carried out without the need for social engineering or special authentication (Company B Vulnerability Report and Cybersecurity Tools). The risk is high, as it could result in loss of confidentiality integrity and availability to the extent that it has a severe adverse effect on the company's assets (sensitive data).

The impact of the PostgreSQL server admin being reachable form the internet is critical. If someone were to exploit the vulnerability it would result in root-level compromise of the server. This server being compromised could be catastrophic to operations. The risk is high. If someone accesses the SQL server admin, they would be able to view, modify, and exfiltrate sensitive data. The likelihood of the attack occurring is high since it is an attack that can be carried out without the need for social engineering or special authentication (Company B Vulnerability Report and Cybersecurity Tools).

C.


Remote Dekstop Access
External Web Access
Internet
VPN Device
InfoSec VPN Tunnels
VPN Device
Corporate Wired Network
Switch
Printer Pool
MFP/Coier
Router
Router
Sophos XG Firewall
Switch
Switch
Switch
Virtual Private Gateway
Azure Firewall
Azure Firewall
Sophos XG Firewall
Switch
Corp WiFi
Virtual Private Cloud Segment 1
Cloud DMZ
Web-facing Servers
Internal-facing servers
Virtual Private Cloud Segment 2
Guest WiFi
Fortinet Firewall
Windows Laptops
Windows Desktops
Computer VLAN

D.

OSI Layer and TCP/IP Layer for each component:

Device	OSI Layer	TCP/IP Layer
Firewall	Layer 4 – Transport Layer	Layer 3 – Transport Layer
Router	Layer 3 – Network Layer	Layer 2 – Internet Layer
Servers	Layer 7 – Application Layer	Layer 4 – Application Layer
Switches	Layer 2 – Data Link Layer	Layer 1 – Network Access Layer
Cabling	Layer 1 – Physical Layer	Layer 1 – Network Access Layer
VPN	Layer 3 – Network Layer	Layer 2 – Internet Layer
Laptops and Workstations	Layer 7 – Application Layer	Layer 4 – Application Layer

E.

The decision-making process for the planning of the merged network involved a few things. First, with a working budget of only $50,000 for the first year, cost was a consideration for every component. It was also necessary to eliminate vulnerabilities as much as possible as well as make the new network easy to maintain.

Physical Network Components

There were many end-of-life hardware components and some outdated operating systems being used at both original companies that needed replaced or upgraded. While a few things were moved around, much of the original physical infrastructure was retained. An infosec VPN virtual infrastructure was implemented to facilitate site-to-site connectivity, remote-to site connectivity and to access the DMZ and internal servers.

Deleted Physical Hardware

The Cisco 7600 border router and the 4 Cisco 3750 switches that provided the bulk of the infrastructure for Company A were end-of-life devices that were no longer supported by the company. This left the devices and the network open to a vulnerability being exploited. Of the 5

servers that Company A had, 3 were end of life and no longer supported, creating vulnerabilities. Since servers were going need to be accessed by both companies anyway, it made more sense to move these servers into the cloud with the servers from Company B rather than replacing them.

Company B was using an IPS router as the border router. While research shows that this was not out of date, the router was not sufficient for the new company's needs. The decision was made to replace it with the same router being sourced for Company A for ease of programming. All retired Windows operating systems were replaced with Windows 11 Pro licenses.

Retained Physical Hardware

As discussed earlier, much of the infrastructure was sufficient to meet the security and networking needs of the merged company. Retaining hardware that meets the minimum security and business needs of the company allowed us to use more of the budget for replacing EOL equipment and provisioning the cloud resources needed to make the merged company operable and secure. The cable plants from both networks didn't need modified or replaced because other than removing a few servers, moving the guest WI-FI, and adding VPN capability, the original networks remained the same and at their original site. The three HPE Aruba 2930F 48GPoE switches from Company B were retained. They are still within their service life and have the capabilities needed to fulfill the business and security needs of the merged company. The 2 Meraki M28 Access points from Company A's original infrastructure, as they are still supported by the manufacturer and meet the security and business needs of the company. All 150 physical workstations as well of the laptops were retained along with all non-retired operating systems.

Repurposed Physical Hardware

A few items were repurposed to improve some level of uniformity between the two physical networks. The Fortinet 800D Firewall that was at the edge of Company A's network was moved to serve as a firewall between Company B's main network and its guest network. The second Sophos XG Firewall from company B was moved to Company A's network edge so that both networks would have the same firewall. This increases ease of administration and increases security as the same settings can be used for each. The legacy Windows workstations and the legacy Windows laptops were upgraded to run Windows 11 Pro.

Added Physical Hardware

A few hardware components were sourced to replace outdated hardware and physical hardware to implement InfoSec VPN was added to each physical network. For the border router,

the Cisco Catalyst 9200L Border Router was selected. Budget really came into play for this selection. We had to select a model that had the capability to run the network segments at each location and the ability to route the VPN connections. Two of these were purchased, one for each location. VPN hardware was placed at the edge of each network to provide the secure site-to-site, remote-to-site, and site-to-cloud connections. 2 HPE Aruba 2930F 48GPoE switches were purchased to replace two of the removed Cisco switches. The other two were no longer needed due to moving the DMZ from Company A to the cloud.

Cloud Network Components

Since Company A was running physical servers that were mostly end of life and Company B had a virtual server farm, including legacy machines, I made the decision to house the merged company's servers in the cloud using Azure services. This was the most efficient decision, and it is also cost effective. The cloud network has two segments, each with its own firewall. One segment houses the DMZ for internet-facing servers and the other houses internal servers only accessibly via the company's site-to-cloud VPN. This way anyone at the company or connecting remotely will have access, but it is isolated from the internet, otherwise. One important thing that changed with the merged network is that all unused ports were closed and processes using insecure ports were moved to secure ports. Since the company's server needs are likely to change as the merger solidifies it doesn't make sense to invest a lot of money on hardware that may not be needed after a year.

Deleted Cloud Network Components

The virtualized server from Company B was removed the servers moved to the new Azure cloud network.

Added Cloud Network Components

A virtual network was created on Azure Cloud Services running two network segments. One for the DMZ and one for the internal servers.

DMZ Virtual Network Segment

An Azure Firewall was placed at the endpoint of the DMZ network segment. By using different firewall for each segment, an additional layer of security is added to the network segments. The firewall was a relatively expensive compared to the other Azure services commissioned, but given the business requirements of the merged company, having a data breach

or other unauthorized access would have an extremely negative financial effect. An Azure virtual private gateway was placed at the edge of the network segment to provide secure site-to-cloud connections. The Azure services placed in the DMZ cloud network segment are an Azure VM application server, an Azure Files instance to replace the FTP/Web server, an Ubuntu Linux FTP Server for incoming EDI running on Azure virtual server, three instances of Microsoft Entra Domain Services, a Ruby on Rails Azure Server, an Azure Database for PostgreSQL, Azure Database for MariaDB, 2 Instances of NGINX As a Service and a SSL/TLS Linux Server running on an Azure virtual server. Each service was selected to serve the same purpose as the server it is replacing. When selecting the service level, needed computation bandwidth was balanced with budget to make selections that fit the budget and met the minimum needs of the business needs and security needs.

Internal Virtual Network Segment

The virtual network segments providing services for the internal corporate network is also protected by its own Azure Firewall. The firewall was relatively expensive compared to the other Azure services commissioned, but given the business requirements of the merged company, having a data breach or other unauthorized access would have an extremely negative financial effect. A virtual private gateway was placed at the network edge to provide secure site-to-cloud InfoSec VPN connections. The virtual services placed on this network are an Azure SharePoint virtual server, three Azure exchange servers, two Azure Cloud file servers, three instances of Elastic on Azure and 4 Azure virtual servers running RDP. Two exchange servers replace legacy virtual servers, and one replaces a physical exchange server.

F.

Zero Trust Access Control

Zero Trust is a newer concept in network security where, by default, no person or device is trusted, so each person and device must be authenticated and authorized before being granted access to network assets.

The merged network topology implements zero trust access control throughout. Identity and Access management is provided by Duo and Microsoft Entra. The new network is set up to require identity to be verified across physical and cloud networks and only allows users to access

resources they have permission to authorize and only the permissions necessary are granted to each person.

Defense in Depth

Defense in depth is achieved by layering security controls to protect against various threats.

Our network contains multiple layers of protection both at network edge and throughout the network. VPN connections only allow authorized users to connect and encrypt data so that it is secure in transit. Firewalls at the network edges and between network segments filter and analyze traffic to protect the network and its assets against malicious actors. An intrusion detection system is implemented to alert to any intrusion. Network segmentation is implemented to prevent a bad actor who does gain access to the network from moving from web facing assets to internal assets. Zero Trust access control is implemented to protect movement of bad actors within network segments.

G. Regulatory Compliance Requirements

Two regulatory compliance requirements that are relevant to the newly merged company are the PCI Data Security Standard and General Data Protection Regulation.

PCI DSS

PCI-DSS, or PCI Data Security Standard "applies to any company who store, process and/or transmit cardholder data (PCI)." Since the merged company provides bank cards to customers and accepts card payment for services, they must follow PCI-DSS. According to the page 8 of the PCI DSS v4.0 Quick reference manual, PCI-DSS requires companies to build and maintain secure network systems, protect account data, maintain a vulnerability management program, implement strong access control measures, regularly monitor, and test networks and maintain an information security policy. The proposed network topology for the new network meets these requirements. The network topology was designed securely, and continuity of hardware, software and cloud elements was implemented to make maintenance as simple as possible to ensure maintenance is kept up. The new company stores all data securely with the help of OneTrust for data privacy and Lifecyle management and Code42 for data security. data in

transit is sent through an encrypted VPN. Access control measures are implemented via Duo and Microsoft Entra. Access is only granted for necessary functions. The company works with Arctic Wolf to maintain a vulnerability management program, monitor the network and perform periodic penetration testing. An information security policy has been established for the merged company's network.

GDPR

There is a law that governs any data collection, use and storage in the European Union, called GDPR, or General Data Protection Regulation. It is relevant to the merged company because the company operates internationally. According to the Intersoft Consulting website (gdpr-info.eu), the GDPR operates on six principles of data privacy. Data must be processed lawfully, fairly and in a transparent manner; collected for a specified explicit and legitimate purpose and only processed for that purpose; adequate, relevant and limited to what is necessary in relation to the purpose; accurate and up-to-date; kept for only as long as needed; and processed in a way that ensures security as personal data. The merged network includes the necessary security to ensure all data collected remains secure. Data in the network is secured by firewalls, network segmentation, encryption, and identity access management. The company contracts with a company called OneTrust to ensure that the company's data processing and lifecycle management is in compliance with GDPR.

H. Emerging Threats for Merged Network

During a transition such as a company merger, the company can be more susceptible to security threats. There are changes in the physical network, virtual assets are being moved around, and personnel are being combined.

Social Engineering

One threat that could emerge for the merged company is social engineering. Since social engineering uses tricking people as its main vector, a time when personnel form two companies are being merged is a time when it could be easier for a bad actor to trick an employee into verbally disclosing sensitive information such as passwords or clicking on a link containing malware. If a bad actor gains access to network assets through social engineering, it could

compromise the merger, compromise data security, and erode public trust. To manage this risk the company should implement user education and implement information disclosure policies. All employees should be made aware of phishing and vishing tactics and trained not to click on any email links. Training should include warning signs to look for to see if an email may be from a malicious actor. A bad actor could also use vishing to take advantage of the fact that employees from one company may not be familiar with those of the other. It is important to implement a policy that information is not to be disclosed over the phone. Any access to information or other assets needs to go through proper authentication and authorization channels.

Ransomware

Currently, one of the most prevalent cybersecurity attack methods is ransomware. When conducting a ransomware attack, a malicious actor, gains access to the network and encrypts data, then demands the company pay a ransom in exchange for the decryption key. The impact of a ransomware attack on the merged company would be critical. Since they provide financial services, and medical software, the company not being able to complete essential business functions could be financially costly and erode public trust. The merged topology implements many controls to mitigate this risk. The merged network is equipped with an intrusion detection system, firewalls, a virtual private network, strong identity access management protocols. The company contracts with Arctic Wolf for log monitoring and has a security policy that implements a strong password policy, multi-factor authentication and phishing awareness training.

I.

Cost-benefit Analysis – For itemized cost of new hardware and cloud solutions, please see exhibit A.

The restrictive budget available to design the merged network necessitated making calculated choices for each component. For each physical and cloud asset, it was necessary to balance security and performance.

Since the merged company handles person, medical and financial data, security of that data had to be the top priority in the budget. Since that is the case, security infrastructure items such as firewalls, VPN devices, segmentation and redundancy were given more funding to ensure that the company's data would be secure at rest, in transit and in the hands of personnel.

Operating systems took up a large portion of the budget, but upgrading to current operating systems was necessary given that unsupported operating systems create many vulnerabilities that could be taken advantage of by a malicious actor.

Cost-benefit analysis was given much thought in making the decision to move the servers to a cloud network. We could have opted to place the servers at each site, but secure connections would still be necessary and the overhead for the hardware would have been greater than the amount allowed for the budget. Also, given the recent merger, it is very likely business needs will change going forward and the shared DMZ and internal server networks in the cloud provides flexibility to adapt in the future without great reinvestment.

The routers and switches selected were also carefully thought out. Cheaper components could have been sourced but they would not have met business needs, given the components, security settings and VPN capability needed by the merged company. More expensive options would have more features for future scalability but would not have allowed budget for other necessary changes and upgrades to the network.

Justification

While designing a merged network for the two companies with a budget of $50,000 had many possible solutions, this design is efficient and effective. In addition to staying within budget, the most important objective was security. Security is not just implementing hardware, software, and policies to maintain security but creating an infrastructure that facilitates following security protocol. After all, the weakest link in network security are the humans who interact with the network. Simplifying the merger and the technology used as much as possible mitigates the potential for human error.

Our design facilitates communication between locations and remote employees without sacrificing security. Placing server functionality in a cloud that is easily and securely accessible by both physical locations facilitates inter-operability while implementing sufficient security safeguards.

Addendum A

Physical Network Components	**Cost**	**Quantity**	**Base Cost**		**Total Cost**
VPN Device	126	1	126		126
VPN Device	126	1	126		126
Company A Laptop OS	200	14	2800		2800
Workstation Operating Systems	200	39	7800		7800
Cisco Catalyst 9200L Border Router 1/2	1590	2	3180		3180
HPE Aruba 2930F 48G PoE+ Switches	$1,715	2	$3,430		$3,430
Virtual Private Cloud Segment for DMZ		**Quantity**	**Base Cost**	**# Months**	**Total Cost**
Azure Virtual Network Segment	20	1	20	12	240
Virtual Private Gateway	26	1	26	12	312
Azure Virtual Firewall	287	1	287	12	3444
Application Server - Azure VM Server	35	1	35	12	420
Azure Files	120	1	120	12	1440
Virtual Ubuntu Linux FTP Server for incoming EDI	61	1	61	12	732
Virtual Servers running Microsoft Entra Domain Services	110	3	330	12	3960
Ruby on Rails Azure Server	60	1	60	12	720
Azure Database for Postgre SQL	60	1	60	12	720
Azure Database for MariaDB	60	1	60	12	720
NGINX As A Service - Replaces 3 Nginx virtual servers	219	1	219	12	2628
SSL/TLS Server on Linux Azure VM	83	1	83	12	996
Virtual Private Cloud Segment for Internal Network		**Quantity**	**Base Cost**	**# Months**	**Total Cost**
Azure Virtual Network Segment	20	1	20	12	240
Virtual Private Gateway	26	1	26	12	312
Azure Virtual Firewall	287	1	287	12	3444
Sharepoint Virtual Machine on Azure	20	1	20	12	240
Azure Exchange Server	48	1	48	12	576
Azure Exchange Server	48	2	96	12	1152
Azure Cloud File Server	48	1	48	12	576
Azure Cloud File Server	48	1	48	12	576
Elastic on Microsoft Azure	120	3	360	12	4320
Azure VM Server Running RDP	48	4	192	12	2304
			Total 1st year cost		**47534**

Works Cited

Mike. (2021, May 7). *What is an Open Telnet Vulnerability, what is the risk and how can you mitigate that risk? - Skyway West*. Skyway West. https://www.skywaywest.com/2021/01/what-is-an-open-telnet-vulnerability/#:~:text=Why%20is%20it%20a%20risk,connections%20and%20discover%20confidential%20information

Gain a shell remotely : Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities. (n.d.). https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.108010

Stefan. (2023, August 16). *Security monitoring of inactive accounts - Stefanini*. Stefanini. https://stefanini.com/en/insights/articles/security-monitoring-of-inactive-accounts#:~:text=These%20dormant%20accounts%20seem%20harmless,systems%20and%20extract%20valuable%20information

Ibeakanma, C. (2022, March 29). *The 8 most vulnerable ports to check when pentesting*. MUO. https://www.makeuseof.com/vulnerable-ports-check-when-pentesting/