Logo

Description automatically generated

**Secure Configuration:**

**Reducing the risk of cyberattacks**

|  |  |  |  |
| --- | --- | --- | --- |
| **Andrea Colon-De Feria**  **Florida State University** [**ACC19K@fsu.edu**](mailto:ACC19K@fsu.edu) | **Michael Dunne Florida State University** [**MRD23@fsu.edu**](mailto:Mrd23@fsu.edu) | J**onah McKitty Florida State University**  [**JAM19R@fsu.edu**](mailto:jam19r@fsu.edu) | **James Flannery Florida State University** [**JEF02d@fsu.edu**](mailto:JEF02d@fsu.edu) |
| **R.J. Johns**  **Florida State University**  **RDJ18**[**@fsu.edu**](mailto:FSUID@my.fsu.edu) | | **Frank Quintana  Florida State University** [**FJQ21@fsu.edu**](mailto:FJQ21@fsu.edu) | |

# **Abstract**

*The goal of this project is to show how organizations can effectively identify system misconfigurations and vulnerabilities in the environment and proactively address them before they are exploited. Network misconfiguration is a systemic problem across organizations of all sizes to include default configurations, improper privileges, insecure communications, lack of segmentation, and unpatched systems. Data breaches and network intrusions continue to make headlines, costing organizations millions of dollars. Threat reports are generated each year by industry leaders highlighting the root causes of these breaches and overall cybersecurity trends to help organizations mitigate the potential threats. However, the threat actors continue to evolve, and new vulnerabilities are identified daily resulting in continuing security incidents. By identifying a repeatable and manageable framework for proactive threat management, organizations can drastically reduce the likelihood of a cyber-attack.*

*Many tools exist, either host or network based, that can help facilitate the necessary monitoring to identify potential misconfigurations or vulnerabilities. Numerous tools that have a cost associated with them also have open-source alternatives. Whether it is a large enterprise network or a small business network, remedial efforts must be prioritized based on risk while working within the confines of security budgets.*

*Upon analysis of the tools and procedures, we will demonstrate how organizations can identify misconfigurations and demonstrate the ramifications of said misconfigurations to minimize the risk and impact of a cyber-attack in an ever-changing and fast-paced technological environment. Leveraging a defense-in-depth strategy focusing on the highest risk areas, providing valuable data through automation, and performing periodic monitoring and validation of security controls are paramount.*

Keywords: Misconfiguration, vulnerabilities, data breach, cybersecurity, threat management

# **Introduction**

We live in a world that depends increasingly on technology in every facet of our lives. Such dependencies and integrations make a target-rich environment for cybercriminals, script kiddies, and nation-states. The increasing complexity of software applications and the enormous number of features offered by software components detract from systems being adequately secured (Dass & Namin, 2021). It was estimated in 2019 that a cyberattack on businesses would occur every 14 seconds (Morgan, 2017). This can be directly attributed to misconfiguration in many ways.

Network misconfiguration is a systemic problem across organizations of all sizes including default configurations, improper privileges, insecure communications, lack of segmentation, and unpatched systems. Threat reports are generated each year by industry leaders highlighting the root causes of these breaches and overall cybersecurity trends to help organizations mitigate the potential threats. However, the threat actors continue to evolve, and new vulnerabilities are identified daily resulting in continuing security incidents. According to the National Institute of Standards and Technology, over 12,000 vulnerabilities were identified in 2022 (NIST, n.d.). This paper will highlight some of the key vulnerabilities and misconfigurations that leave organizations susceptible to cyberattacks and the tools available to proactively identify them.

The Cybersecurity & Infrastructure Security Agency defines cybersecurity governance as, “a comprehensive cybersecurity strategy that integrates with organizational operations and prevents the interruption of activities due to cyber threats or attacks” (Cybersecurity and Infrastructure Security Agency, n.d.). Establishing a governance program is the most pragmatic way of addressing vulnerabilities and misconfigurations. Industry frameworks such as those published by the National Institute of Standards and Technology and the International Organization for Standardization exist to help facilitate this.

# **Literature Review**

The cloud environment leveraged for this research paper is comprised of virtual machines. 60-65% of virtual machines that are in production are less secure than physical machines because of misuse and or inconsistencies in traditional security measures (Aalam, Kumar, & Gour, 2021). Virtual machines allow you to run multiple operating systems on a single physical server with resource optimization and the ability to streamline IT infrastructure. Securing these virtual machines is important as exploitation of vulnerabilities can be directly on the hypervisor itself, allow traversal from virtual machine to virtual machine, or allow unauthorized access to virtual data stores.

The National Institute of Standards and Technology highlights the need for security in virtualized infrastructure. It is critical to leverage virtual machines to support vital business processes, but with security levels equivalent to traditional physical devices. Key configurations such as network segmentation and traffic control are part of the hardening process. The virtual network configuration is a critical element in their protection through a combination of host-level and network-level measures (NIST, 2016).

**Access Control**

Within confidentiality, availability, and integrity, failure to implement proper access controls negatively impacts the confidentiality of systems. Access control should have granular capabilities at the permission assignment level and at the object level (i.e., a single virtual machine or a larger grouping of virtual machines). Access control should be able to specify and deny permission to some specific objects within a virtual machine group based on sensitivity (NIST, 2018). The hosts of virtual machines should also ensure that user accounts, both privileged and regular, are connected to the main directory infrastructure of the entire organization. In doing this, authentication methods such as Kerberos can be used. This would also ensure that security rules are enforced and changes to the user’s accounts can be made centrally (NIST, 2016).

Historically, administrators granted permissions to limited internal users based on their role. However, with the rise of networking and distributed computing, more sophisticated access control mechanisms are now required. This has been exacerbated by remote access over the Internet and self-service access models further exposing systems to external threats. Traditional access control models usually assume that the data owner, system owner, and users are in the same domain. However, data owners now store their data on external domains of service providers who have access, along with data owner administrators, and public users. Thus, confidentiality of data can be a critical issue in the cloud server environment (Namasudra & Roy, 2018).

One could think of access control as a digital bouncer, where a determination is made about who is allowed into specific areas within a virtual space. The defining and enforcing rules of access control dictate which users or systems can access certain resources or perform actions. The principle of least privilege emphasizes restricting access rights for users to the bare minimum necessary to complete the duties of their job. The zero-trust model is a security model that by default trusts no device or user and authenticates every transaction. The CISA Zero Trust Maturity Model v1.0 refers to NIST SP 800-207’s definition of zero trust as “a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.” By using this approach, a company minimizes the potential impact of security breaches by limiting exposure to critical resources.

The use of passwords as a security practice is deeply ingrained within the evolution of computing. As computing power has grown and interconnected systems are more prevalent, the need for more robust password practices has become more evident. The simple password schemes of the early days of computing can no longer be relied on. Passwords created under stricter composition requirements, to include blacklists and longer password lengths, are more resistant to automated cracking (Kelley et al., 2012).

Passwords are susceptible to many attacks including brute force, password spraying, and dictionary attacks. Users’ password strength perceptions and the actual strength of the password often do not align. The added stress posed by managing numerous strong, unique passwords leads to the use of weak and memorable passwords and the reuse of passwords across multiple accounts. This makes it easy for attackers to breach several accounts using one leaked password (Zimmermann, Marky, & Renaud, 2023). This was demonstrated in the cloud research environment with the same username and password being shared by all teams to access their virtual machines.

Effective password management and authentication revolves around implementing different strategies to create and maintain secure passwords. Should there be a higher security need, password-based authentication may not be sufficient. Authentication is the actual process of verifying the identity of users or systems attempting to access virtual machines and their applications. There are several authentication methods such as Kerberos, certificate-based, biometric, and multi-factor. With a method such as multi-factor authentication, an extra security layer is added by requiring multiple forms of verification types to include something you know, something you are, or something you have. These extra layers of security checks aid in making unauthorized access more challenging and protecting against distinct types of cyber threats.

Some of the most common cloud threats are information disclosure, replay attacks, spoofing identity, account hijacking, and the elevation of privilege. Enhanced authentication techniques are the first barrier of defense against various attacks that prevent unauthorized access to applications, data, services, and resources. Multi-factor authentication in cloud applications increases security and productivity, reduces the risk of compromised passwords, improves regulatory compliance, and enables enterprise mobility (Mostafa et al., 2023).

**Misconfiguration**

Virtual machines have become an integral part of modern-day organizations, with a unique set of security and access requirements. Unfortunately, when those security and access requirements are not properly configured, security incidents can occur. Security incidents and vulnerabilities are often caused by human errors, such as faulty input validation, missing firewall rules, faulty authentication, or buffer overflows that are exploited to disrupt services. For example, in early 2015, over 40,000 MongoDB instances were publicly accessible from the Internet, without authentication and authorization, and, in turn, allowed anyone to retrieve the stored data. Redis similarly had hundreds of thousands of systems unprotected due to misconfiguration. Misconfigurations can also lead to other vulnerabilities (Dietrich et al., 2018).

A vulnerability can be defined as a “weakness, a flaw or a hole of an information system, that can be exploited by one or more threats to harm the confidentiality, integrity, or availability of a system” (Spanos & Angelis, 2015). As the definition suggests, vulnerabilities can be found anywhere in an information system. A recent survey of 221 system operators indicated that approximately 77% acknowledged that they had misconfigured a system and 31% indicated at least one misconfiguration led to a security incident (Dietrich et al., 2018). Some of the misconfigurations included weak or default passwords, delayed or missing updates, and faulty assignment of permissions. Over 75% of the survey respondents also indicated the misconfiguration was due to a lack of knowledge and experience.

When virtual machines are first introduced to a system, they are configured with specific rules or parameters like filters for network packets or stateful firewalls (Jarraya, 2015). These rules change based on a user’s role in a system, and the parameters are determined after a careful assessment of the role and what websites, settings, and network information it should have access to. Misconfiguration happens when there are rules in a virtual machine that are not defined or are incorrectly defined, which leaves the machine vulnerable. Misconfiguration can happen at various stages. Configurations may have been overlooked when the machine was being deployed. More commonly though, misconfigurations happen during virtual machine migrations, which is when a virtual machine is moved from one host to another while it is still live (Le, 2020). Virtual machine migration requires reconfiguration of the rules and parameters, whether it is ensuring they are the exact same as before or defining and changing pre-existing ones (Jarraya, 2015).

**Patching**

A recent data breach at Equifax was attributed to an underlying vulnerability that had a patch available for months, but was never applied (Dietrich et al., 2018). Not applying security patches immediately upon release can be attributed to a variety of reasons. Testing may be needed before applying the patch. There may be technical debt that requires multiple iterations of patches or upgrades to apply recent patches. Additionally, there may be availability and functionality requirements that hinder applying a patch. In some instances, if a system is not known to those responsible, then it may slip through the cracks for patching.

In the SECNET environment, another scenario exists that is common across organizations. The software running on some of the virtual machines reached the end of support. This means that the manufacturer no longer provides support, including security patches. The only way to adequately address vulnerabilities is to upgrade. While a vulnerability may not exist in the present, a vulnerability could be identified at any time with limited means of addressing it. Lifecycle planning is critical to ensure that enough time is scheduled to move off systems before they reach support ends.

**Segmentation**

The purpose of network access controls is to keep those machines and the data stored within them safe. Network access controls are implemented through devices on the network such as a firewall that is often the first line of defense against malicious actors trying to gain access to information or resources in a network. A misconfigured firewall could allow attackers to bypass the intended security controls. As an example, a valid rule intended to deny traffic could be ineffective based on the order of processing rules where a higher rule has been set to allow all traffic. In such a case, the rules the firewall is enforcing are not what the user intended (Alicea & Alsmadi, 2021).

Beyond unintentional misconfiguration, there exists the vulnerability of intentional lack of system segmentation. The historical concept of segmentation was primarily focused on separating trusted networks from untrusted networks. This did include external networks, but also limited segmentation internally for more sensitive systems. However, more recently, the concept of zero-trust segmentation which is to keep a business in a trust no one or anything mindset, takes into consideration that most breaches occur because otherwise immaterial systems do not have the appropriate security controls in place, and they are exploited to gain a foothold in the environment and attackers move to other areas of the network fairly easily based on privilege escalation and compromising legitimate accounts. The idea of a solid defensible perimeter is an illusion in today’s global, mobile, remote, and cloud-based IT landscape where the attack surface is never static, never localized, and never impregnable. Perimeter-based security is built on the implicit requirement that there is some way to filter users, network traffic, and transactions into trusted and untrusted buckets. The rise in breaches from insider threats, hijacked credentials, compromised devices, and phishing attacks has proven that model to no longer be sufficient. The perimeter is strong, but if someone can penetrate, the inner network is unprotected. The zero-trust security strategy, supported by a variety of implementation frameworks, has become a necessary reality for a growing number of enterprises (Campbell, 2020).

**Insecure Communications**

Connections between system networks continue to grow with the expansion of communication capabilities across the globe, redundant/backup connections, and new carriers. Unfortunately, the more interconnected they become, the less secure they are. This is because different networks usually have distinct security policies, control structures, and infrastructure vulnerabilities. As such, this may introduce opportunities for attackers to intercept communications between networks. Once data is intercepted, attackers may breach the security of data packets that are being transmitted and potentially leverage that information to further exploit systems in the environment (Das et al., 2020).

Secure communication protocols are being widely used instead of plain text communication protocols like HTTP to protect the data being transmitted, including attackers who attempt hide their malicious activity from the network security administration. The trend of encrypted traffic in the network has increased in the last decade due to security concerns. Encryption has provided a lot of benefits for the user ensuring data confidentiality (Zain ul Abideen, Saleem, & Ejaz, 2019). However, in some cases, applications and servers have limitations on what communication protocols they support. Some settings may be hardcoded into applications, or some applications or servers may be older and rely on deprecated and insecure protocols. In other cases, data may not be classified as sensitive enough to require encryption but instead rely on the data traversing a private network. This exposes the confidentiality of the data being transmitted if someone were to gain unauthorized access to that traffic on the network.

# **Computing Environment**

**Network Topology**

The cloud environment used for this research was a flat network, consisting of a pfsense firewall/router, Hyper-V, Linux, Windows, and Palo Alto virtual machines/appliances. The most common ports include 80 (http), 135 (msrpc), 443 (https), 445 (SMB), 3389 (RDP), 22 (SSH), and 2179 (Hyper-V RDP). Due to the flat nature of the network (see Figure 1), it would be simple for an attacker to laterally move across the network. A simple scan of the network using Zenmap was able to identify all hosts residing on the network and the respective open ports associated with each host. While separate subnets were configured on the various Palo Alto virtual interfaces, no hosts existed on those networks and any vulnerability identified on the accessible management interface would be identified on all interfaces.

A screen shot of a computer

Description automatically generated

Figure 1

There are five phases of penetrating a network. The first phase from an attacker’s standpoint is to gather data about the network. The network information for all nodes, DNS, gateway, firewall interface addresses, and network ranges was posted in an online forum. This was helpful in configuring labs, but also allowed for quick visibility into how an attacker might develop an attack strategy. The second phase from an attacker’s standpoint is scanning the network to identify potential targets. During a port scan of the environment using Zenmap, no restrictions were in place to limit network visibility. This allows an attacker to reach phase three, which is assessing the environment for vulnerabilities. Currently, Windows Server 2012/R2 and FreeBSD 11.2 are running in the environment. These operating systems reached end of support in 2023 and 2019 respectively and are inherently vulnerable as regular security updates are no longer available. Additionally, the Palo Altos are running pan-os version 9.1.9, which is end of life March 2024 and has 33 published vulnerabilities according to cvedetails.com to include remote command injection and denial of service.

To prevent phase two and three, implementing virtual local area networks (VLANs) would isolate each host when appropriate access control lists (ACLs) are implemented. ACLs can be applied either on the Hyper-V machines themselves, on the virtual machines, or on the router/firewall. In such a scenario, there would be no need for inter-machine communication and any traffic would be dropped using a zero-trust model. Only the necessary traffic would be allowed, which would be limited based on necessary ports to the domain controller, DNS server, and traffic destined for the internet. In the current environment, remote desktop protocol (RDP) and secure shell (SSH) are allowed from any location, allowing an attacker to attempt to authenticate to any machine. The Windows machines in the cloud environment do not have the local firewall enabled and do not enforce strong password controls. Minimum password length is set to zero characters, password complexity is disabled, and account lockout is not configured for Windows machines. Linux machines also do not have PASS\_MIN\_LEN configured in the login definitions and password complexity is not configured, allowing simple passwords that could be easily guessed. The Palo Alto firewalls enforce a minimum of eight characters but do not enforce password complexity. This would allow an attacker to easily brute force their way into a machine.

While Linux machines do have syslog enabled for logging and Palo Altos have audit logging turned on, Windows machines do not have audit logging enabled either locally or via group policy. Therefore, any potential malicious activity could go unnoticed. For the limited logging enabled, there is no centralized log aggregation utility to flag events of interest. The lack of logging increases the importance of intrusion detection tools that might otherwise be able to detect activity that is not being logged locally on a machine.

# **Description of Methods**

A variety of vulnerability management tools exist in the marketplace, including Tenable, Qualys, Rapid7, and Acunetix. These tools are robust in their capabilities, but along with the capabilities comes a large price tag. Part of the basic functionality of these tools is scanning for open ports. Zenmap is an equivalent port scanning tool that is available for free. Zenmap was able to provide a blueprint of the cloud network, identifying open ports as well as operating systems and versions in some instances. This allowed for additional reconnaissance. Once the port scan was run, it was identified that port 443 (https) was open on 192.168.72.254. Manual review took place in a web browser to try to connect over port 443 and provided access to the administrative web interface for the firewall/router (see Figure 2). This further confirmed the type of device that it was from the web interface. Knowing this type of information, an attacker could then use other free tools such as Metasploit (see Figure 3) to then further attempt to identify vulnerabilities and exploit them. This demonstrated the impact of lack of segmentation in the environment. Administrative interfaces should only be accessible from trusted and limited network ranges. Also, a simple query online for default credentials revealed that the device had default credentials enabled and allowed unauthorized access to the system (see Figure 4).

A screenshot of a computer

Description automatically generated

Figure 2

A screenshot of a computer

Description automatically generated

Figure 3

A screenshot of a computer

Description automatically generated

Figure 4

While port 80 was a common port identified above, performing a packet capture using another free tool, Wireshark, did identify several instances of clear text credentials (see Figure 5). A search for SNMP traffic revealed version 2 running in the environment, which transmits community strings in the clear. After capturing the community string, an attempt to connect to the host via SNMP revealed that the community string could be leveraged to modify configurations through the write access granted. Additionally, using Metasploit, it was discovered that additional vulnerabilities existed for exploitation to include default public community strings and SNMP enumeration. This demonstrated the impact of misconfiguration. SNMP version 3 is a secure version that does not use clear text community strings and should be implemented. Additionally, default community strings should be changed to prevent information leakage.

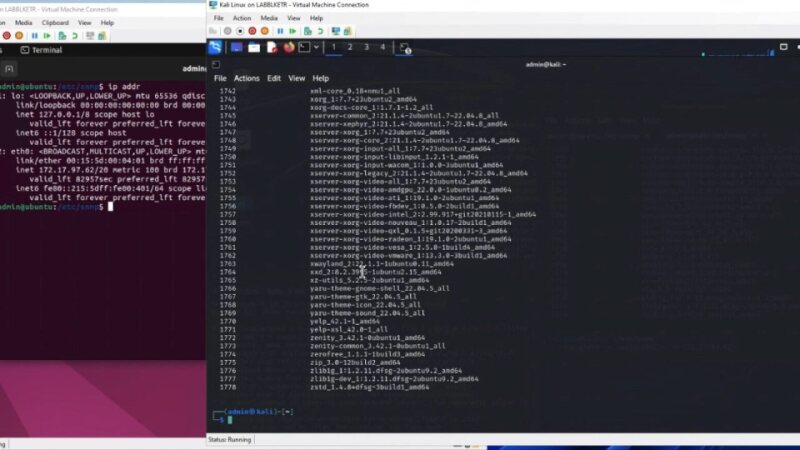
[](https://fsu-my.sharepoint.com/:v:/g/personal/acc19k_fsu_edu/EV5CXy-zceJErLWLMYLEhU0BEppuXHWEH_LLqG7saECsDQ?e=dabeBb&nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJTdHJlYW1XZWJBcHAiLCJyZWZlcnJhbFZpZXciOiJTaGFyZURpYWxvZy1MaW5rIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXcifX0%3D)

Figure 5

Wireshark can be leveraged to find a plethora of insecurely transmitted information such as passwords, usernames, billing information, emails, etc. Using Wireshark to capture network traffic in the cloud environment, a search for insecure HTTP traffic uncovered an online order being placed containing name, contact information, and billing information (see Figure 6). This information was captured and navigation to a common merchant website indicated that the information captured could be used to make fraudulent purchases unbeknownst to the owner. Not only does this demonstrate poor security hygiene, but it is also a clear violation of payment card industry regulations. As noted above, insecure communications are common, but leveraging HTTPS to encrypt the transmission would prevent an attacker from gaining unauthorized access to sensitive or personal information.

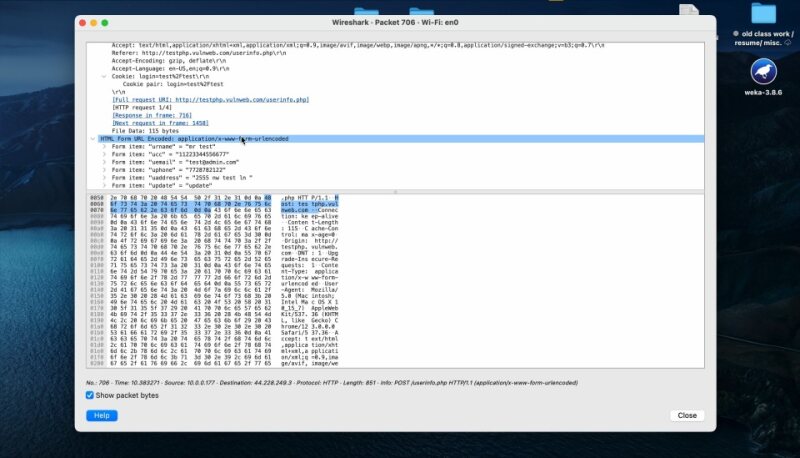
[](https://fsu-my.sharepoint.com/:v:/g/personal/acc19k_fsu_edu/ERQ9kSmRbKFKney-uUNv3MsBiQbraGDeWCu3d0hHEGbZ-g?e=z3gCRm&nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJTdHJlYW1XZWJBcHAiLCJyZWZlcnJhbFZpZXciOiJTaGFyZURpYWxvZy1MaW5rIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXcifX0%3D)

Figure 6

As noted above, Linux machines in the cloud environment did not enforce password strong password parameters. As such, to demonstrate the weakness, a new user was created (admin) with a simple and common default password (admin). Leveraging John the Ripper, the MD5 hash was able to be cracked in less than a minute (see Figure 7). This demonstrates the consequences of poor access control and why a strong password policy is required to prevent unauthorized access to systems.

A screenshot of a computer program

Description automatically generated

Figure 7

Also as noted above, no logging is configured on the Windows machines in the environment and syslog is on but stored locally with no monitoring for Linux and Palo Alto machines. This increases the importance of having network-based security tools to detect potential malicious activity. An intrusion detection capability exists within the Security Onion platform deployed in the cloud environment to monitor network traffic. During the previously mentioned activities of port scanning, various rules were triggered within the SGUIL interface for monitoring OSSEC and Suricata (see Figure 8). This included the detection of NMAP scans, suspicious inbound traffic, and operating system probe detection. The intrusion detection logs included the rule that was triggered along with the source and destination, allowing for an investigation into the events and acting if deemed necessary. The above demonstrated activities could potentially be identified to alert security personal that malicious activity is taking place and respond.

A screenshot of a computer

Description automatically generated

Figure 8

When accessing remote or local hosts, the network protocol that an organization chooses to implement is incredibly important. Communications back and forth between hosts carry with them a lot of data, most of which is sensitive and if not secured properly, can be accessed, and utilized maliciously. Input data such as credentials or network information can all be visible depending on the way that a machine is configured to send commands to a remote host. Telnet is a prime example. Telnet is an antiquated protocol that passes information in clear text and allows users to access remote systems. While revolutionary for its time, all data that is sent or received using telnet can be viewed by unauthorized users using modern tools to sniff traffic on the network. Using Wireshark to capture network traffic in the cloud environment, a search for “telnet” identified several telnet sessions occurring within the network (see Figure 9). Additionally, when the telnet traffic stream was pieced together, there was a wealth of information revealed such as IP information, port information, username, and password. This is another example of the consequences of insecure communications.

While the credentials revealed in the packet capture were being used to issue commands to a network device, a further exploration of the network was attempted using the same credentials to determine if that account was provisioned access to other machines. An attempt to log onto a Windows machine on the network was successful. While the session established was secure on the Windows machine, the damage was already done by leveraging insecure telnet on another device. This was a clear demonstration of poor access controls, using the same credentials on separate and distinct system types and provisioning that access with potentially unnecessary local administrator privileges. Administrator accounts should be unique to each device, using different usernames and passwords, to prevent lateral movement once one machine is compromised.

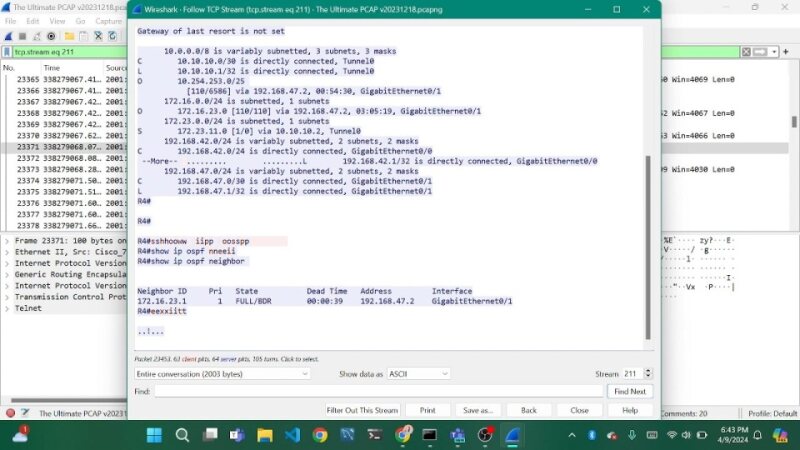
[](https://fsu-my.sharepoint.com/:v:/g/personal/acc19k_fsu_edu/Eei2_KzJ4bBIg64A0LIsQ2QBcFruAy60RJ_x8j4oOoyikQ?e=cCWZr3&nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJTdHJlYW1XZWJBcHAiLCJyZWZlcnJhbFZpZXciOiJTaGFyZURpYWxvZy1MaW5rIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXcifX0%3D)

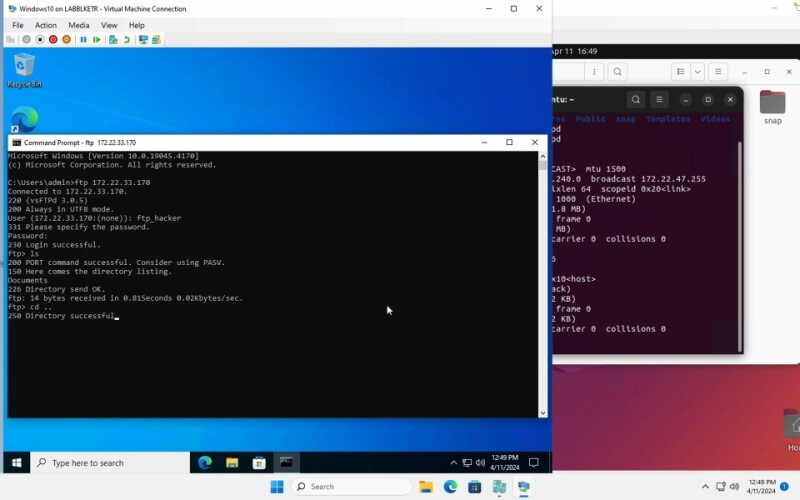
Figure 9

In another example of insecure communications, when Wireshark was filtered for the FTP protocol, the pcap file revealed clear text authentication credentials and source and destination information (see Figure 10). Having credentials that grant unauthorized access to a system can have a multitude of implications. This includes accessing sensitive files within the system, downloading them, or even uploading malicious files to render the system inoperable as was demonstrated through simulation (see Figure 11).

A screenshot of a computer

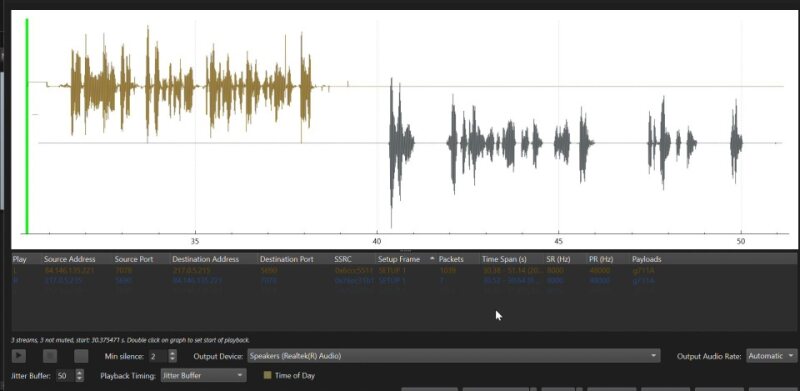
Description automatically generated

Figure 10

[](https://fsu-my.sharepoint.com/:v:/g/personal/jam19r_fsu_edu/Ectx2wZG-PxGoJ8XKJBjPQ8BJVFwLLZDOhSJF5Hf5KK8ZA?e=MXMkNg&nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJTdHJlYW1XZWJBcHAiLCJyZWZlcnJhbFZpZXciOiJTaGFyZURpYWxvZy1MaW5rIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXcifX0%3D)Figure 11

Proper configuration of an FTP server can help mitigate and prevent this type of activity. FTP can be configured to leverage SSH (SFTP) or SSL (FTPS) to encrypt both credentials and the data being transmitted. The FTP Server should also be configured to isolate each user's session to their respective home directory. The file system permissions should be properly configured to restrict access to sensitive files and directories. The implementation of a chroot jail for each FTP user, which restricts their access to a specific directory subtree would also be helpful in securing the server.

Wireshark was used to further analyze the pcap file extracted from the cloud environment to assess VOIP traffic. This showed that SIP packets on the network were not employing industry best practices by implementing encryption for voice traffic. Without encryption, sensitive information, including call content, authentication credentials, and session details, becomes susceptible to interception. By employing encryption protocols, organizations can mitigate this risk and maintain the privacy of their communications. Due to its absence, SIP traffic was easily accessed and analyzed in the environment (see Figure 12). Unencrypted SIP traffic from the pcap file was able to be played back to hear the contents of the call. In this example, the call was in Swedish, but the use of readily available free translation tools easily shows a roughly translated transcription excerpt of the call contents (see Figure 13). This content can easily be used by an attacker to socially engineer a phishing campaign, including the name of the developer and the name of the internal application.

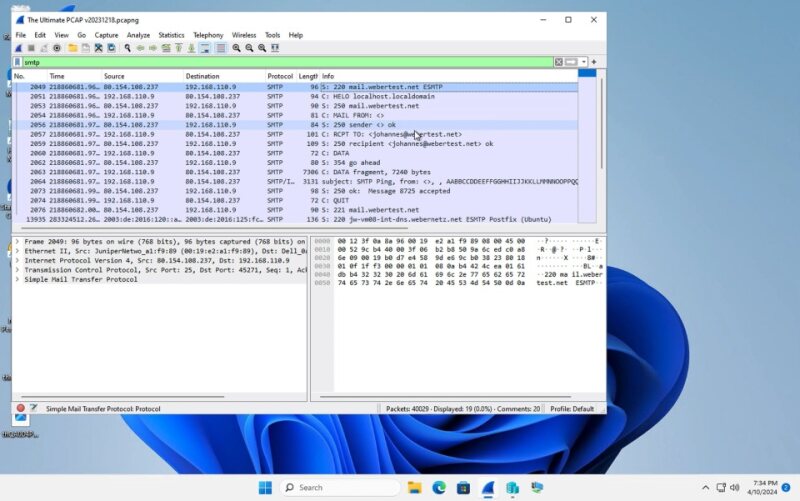
[](https://fsu-my.sharepoint.com/:v:/g/personal/fjq21_fsu_edu/EdMaa8N-eOpNsrV9OVoVuoABIXItsNkNBT97ejZ1rqGx8g?nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJPbmVEcml2ZUZvckJ1c2luZXNzIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXciLCJyZWZlcnJhbFZpZXciOiJNeUZpbGVzTGlua0NvcHkifX0&e=QJNObJ)Figure 12

Graphical user interface, text, application

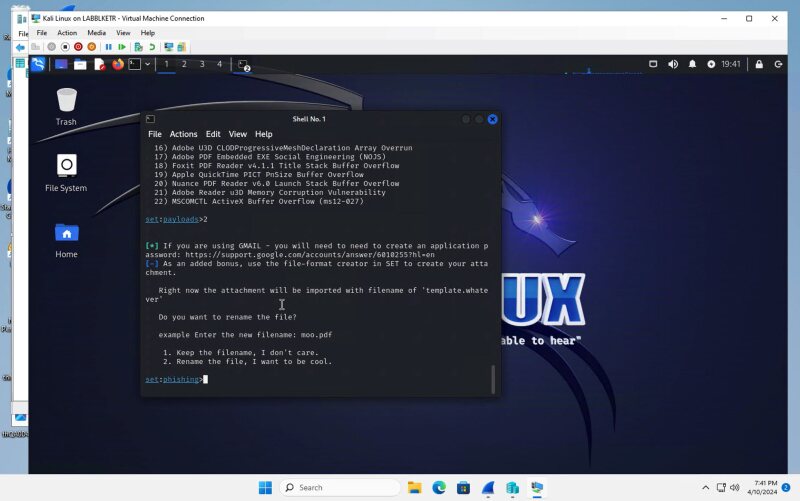
Description automatically generated

Figure 13

Lastly, the analysis of the PCAP capture filtered for SMTP (Simple Mail Transfer Protocol) traffic using Wireshark shed light on significant insights into the email communication taking place within the network (see Figure 14). By dissecting the SMTP traffic, crucial details such as email senders, recipients, email subjects, and associated IP addresses were unveiled. The absence of encryption in the network traffic facilitates this level of transparency, laying bare potentially sensitive information to prying eyes. Unfortunately, this wealth of information can be leveraged for malicious purposes, including email spoofing, spamming, or email phishing attacks aimed at further extracting confidential data. With access to such detailed information about email exchanges, malicious actors can craft deceptive emails, mimicking legitimate correspondence to trick unsuspecting recipients into divulging sensitive information or executing malicious files. This underscores the critical importance of implementing robust encryption protocols and security measures to safeguard email communications and protect against the exploitation of sensitive information for nefarious purposes.

[](https://fsu-my.sharepoint.com/:v:/g/personal/rdj18_fsu_edu/EUfEkR_wz0JKrY0txA-wu8wB2XNiSlKYZG1daTymZmbQAw?nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJPbmVEcml2ZUZvckJ1c2luZXNzIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXciLCJyZWZlcnJhbFZpZXciOiJNeUZpbGVzTGlua0NvcHkifX0&e=UujoBi)Figure 14

The utilization of Kali Linux Social Engineering tools (see Figure 15) exemplifies a sophisticated approach to exploiting vulnerabilities in digital communication systems. With these tools, attackers can spoof email addresses, creating a facade of legitimacy to perpetrate targeted phishing attacks. By impersonating trusted entities or individuals, such as reputable organizations or colleagues, the attackers aim to deceive recipients into divulging sensitive information or unwittingly granting access to critical systems or services. This method not only undermines the trustworthiness of electronic communication but also poses significant risks to personal and organizational security. Through the manipulation of email headers and content, coupled with social engineering tactics, malicious actors can exploit human psychology and technical weaknesses to achieve their nefarious objectives. Consequently, awareness of these tactics and implementation of encryption are imperative to mitigate the threat posed by such sophisticated cyberattacks.

Figure 15[](https://fsu-my.sharepoint.com/:v:/g/personal/rdj18_fsu_edu/EeWrFI1O_29Pkhj9ugAP7-YBxOk6lvj6dbJmF06hoMcSJQ?nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJPbmVEcml2ZUZvckJ1c2luZXNzIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXciLCJyZWZlcnJhbFZpZXciOiJNeUZpbGVzTGlua0NvcHkifX0&e=9R3KIa)

# **Conclusion**

In conclusion, this project has provided a comprehensive exploration of the critical issue of system misconfigurations and vulnerabilities within organizational environments. The overarching goal has been to demonstrate how organizations can effectively identify and address these vulnerabilities proactively, thereby reducing the likelihood of cyber-attacks. Throughout this research, it has become evident that network misconfigurations represent a significant systemic challenge across organizations of all sizes, leading to various vulnerabilities that are often exploited by cyber adversaries. The consequences of such vulnerabilities, including data breaches and network intrusions, underscore the urgency for organizations to adopt proactive measures in securing their systems.

A key finding of this study is the availability of numerous tools, both commercial and open source, that can aid organizations in identifying potential misconfigurations or vulnerabilities. By leveraging these tools effectively, organizations can gain valuable insights into their security posture and take preemptive actions to mitigate risks. Moreover, discussion on access control mechanisms and authentication methods has highlighted the importance of implementing robust security measures to protect against unauthorized access. Proper access control, authentication, and password management are essential components of a comprehensive cybersecurity strategy, safeguarding the confidentiality, availability, and integrity of systems and data. Furthermore, the analysis has shed light on the root causes of security incidents and vulnerabilities, often stemming from human errors such as misconfigurations. This emphasizes a critical need for knowledge and experience in addressing these issues effectively. In our assessment and testing, we emphasize effective identification and proactive resolution of system misconfigurations and vulnerabilities. Network misconfigurations pose risks such as default settings, improper privileges, and unpatched systems. While threat reports guide mitigation efforts, evolving threat actors and daily vulnerabilities drive modern cybersecurity operational demands. Host and network-based tools, including cost-effective open-source alternatives, aid in identifying such vulnerabilities. Additionally, implementing network segmentation provides a mechanism to limit the exposure of systems that may have been inadvertently misconfigured.

By using freely available security tools, we demonstrated how organizations can identify misconfigurations or insecure implementations in an environment and demonstrate their ramifications. While the tools identified herein were able to replicate typical misconfigurations, various industry and vendor security benchmarks exist that can help prevent these misconfigurations. Leveraging a strategy that defines benchmarks to harden systems before they are deployed, maintaining consistent system hygiene practices, and performing proactive monitoring and validation of security controls through security tools will enable organizations to properly secure their environments proactively and subsequently identify where gaps may exist. By analyzing tools and procedures, we demonstrate the impact of misconfigurations and minimizing risk in our controlled testing environment. Human error remains a continuous risk, so implementing tools to detect misconfigurations or even if misconfigurations are missed, having tools to identify potential probes or exploitation of vulnerabilities are key.

In summary, the proactive identification and mitigation of system misconfigurations and vulnerabilities are essential steps in mitigating the risk of cyber-attacks and safeguarding organizational assets. The insights provided in this project underscore the ongoing and multifaceted nature of cybersecurity challenges faced by organizations. Only through diligence and a commitment to cybersecurity best practices can organizations ensure the protection of their systems and data in an increasingly interconnected and digitized world.

# **References**

Aalam, Z., Kumar, V., & Gour, S. (2021). A review paper on hypervisor and virtual machine security. *Journal of*

*Physics: Conference Series*, *1950*(1), 12027-. <https://doi.org/10.1088/1742-6596/1950/1/012027>

Alicea, M., & Alsmadi, I. (2021). Misconfiguration in firewalls and network access controls: Literature review. *Future Internet*, *13*(11), 283-. <https://doi.org/10.3390/fi13110283>

Campbell, M. (2020). Beyond Zero Trust: Trust Is a Vulnerability. *Computer (Long Beach, Calif.)*, *53*(10), 110–113. <https://doi.org/10.1109/MC.2020.3011081>

Cox, O. & Kanji, H. (2022, Nov. 10). Building Effective Cybersecurity Governance. *Harvard Law school Forum on Corporate Governance.* <https://corpgov.law.harvard.edu/2022/11/10/building-effective-cybersecurity-governance/>

CVSS severity distribution over time. (n.d.). National Vulnerability Database. <https://nvd.nist.gov/general/visualizations/vulnerability->visualizations/cvss-severity-distribution-over-time

Cybersecurity and Infrastructure Security Agency (n.d.). “Cybersecurity Governance.” [https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance#:~:text=Cybersecurity%20governance%20is%20a %20comprehensive,to%20cyber%20threats%20or%20attacks](https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance#:~:text=Cybersecurity%20governance%20is%20a%20%20comprehensive,to%20cyber%20threats%20or%20attacks)

Das, P., Shuvro, R. A., Rahnamay-Naeini, M., Povinelli, K., Ghani, N., & Hayat, M. M. (2020). A Theory for Optimizing Insecure Internetwork Connections. *IEEE Systems Journal*, *14*(4), 4842–4853. <https://doi.org/10.1109/JSYST.2020.2977291>

Dass, S., & Namin, A. S. (2021). Reinforcement learning for generating secure configurations. *Electronics (Basel)*, *10*(19), 2392-. <https://doi.org/10.3390/electronics10192392>

Dietrich, C., Krombholz, K., Borgolte, K., & Fiebig, T. (2018). Investigating system operators’ perspective on security misconfigurations. *PROCEEDINGS OF THE 2018 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (CCS’18)*, 1272–1289. <https://doi.org/10.1145/3243734.3243794>

ISO/IEC (2015). Information technology — Governance of IT for the organization. *38500:2015*. <https://www.iso.org/standard/62816.html>

Jarraya, Y., Eghtesadi, A., Sadri, S., Debbabi, M., Pourzandi, M. (2015). Verification of firewall reconfiguration for virtual machine migrations in the cloud, *Computer Networks*. *Volume 93, Part 3, 2015. Pages 480-491.* <https://doi.org/10.1016/j.comnet.2015.10.008>

Kaspersky (2023, Jan. 11). *Miscommunications in IT security led to cybersecurity incidents in 62% of companies* [Press Release].<https://www.kaspersky.com/about/press-releases/2023_miscommunications-in-it-security-lead-to-cybersecurity-incidents-in-62-of-companies>

Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., & Lopez, J. (2012). Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. *2012 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP)*, 523–537. <https://doi.org/10.1109/SP.2012.38>

Le, T. (2020). A Survey of Live Virtual Machine Migration Techniques. *Computer Science Review. Volume, 38.* [*https://doi.org/10.1016/j.cosrev.2020.100304*](https://doi.org/10.1016/j.cosrev.2020.100304)

Morgan, S. (2017). Global ransomware damage costs are predicted to hit $11.5 billion by 2019. *Cybercrime Magazine*. <https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/>

Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. *Applied Sciences*, *13*(19), 10871-. <https://doi.org/10.3390/app131910871>

Namasudra, S., & Roy, P. (2018). PpBAC: Popularity Based Access Control Model for Cloud Computing. *Journal of Organizational and End User Computing*, *30*(4), 14–31. <https://doi.org/10.4018/JOEUC.2018100102>

National Institute of Standards and Technology (2016). *Extending Network Security into Virtualized Infrastructure*.

Information Technology Laboratory. <https://csrc.nist.gov/files/pubs/shared/itlb/itlbul2016-06.pdf>

National Institute of Standards and Technology (2023). *NIST Risk Management Framework (RMF).* Information Technology Laboratory. <https://csrc.nist.gov/Projects/risk-management>

National Institute of Standards and Technology (2018). *Security Recommendations for Server-based Hypervisor*

*Platforms*. Information Technology Laboratory. <https://doi.org/10.6028/NIST.SP.800-125Ar1>

Spanos, G., & Angelis, L. (2015). Impact Metrics of Security Vulnerabilities: Analysis and Weighing. *Information Security Journal: A Global Perspective, 24*(1–3), 57–71. <https://doi.org/10.1080/19393555.2015.1051675>

Zain ul Abideen, M., Saleem, S., & Ejaz, M. (2019). VPN Traffic Detection in SSL-Protected Channel. *Security and Communication Networks*, *2019*, 1–17. <https://doi.org/10.1155/2019/7924690>

Zimmermann, V., Marky, K., & Renaud, K. (2023). Hybrid password meters for more secure passwords - a comprehensive study of password meters including nudges and password information. *Behaviour & Information Technology*, *42*(6), 700–743. <https://doi.org/10.1080/0144929X.2022.2042384>