GROUP 8

Dec 03, 2023

BINARY STREAM – CYBERSECURITY ASSESSMENT

ISMAIL MAHAMED 125052191
JASKARAN SOHAL 150343218
RAYYAN KHAN 155534209
EASTON SOARES 108851213

Table of Contents

Executive Summary

Our examination revealed significant vulnerabilities, particularly in the SSH brute force logins with default credentials on core network machines, notably at the IP address 192.168.9.129. To mitigate this, we recommend changing all default credentials to strong, unique passwords, implementing an account lockout policy, and using multi-factor authentication.

Further analysis highlighted risks associated with the active directory (AD) system. We observed lax management of user account controls and permissions. Our response includes enforcing the principle of least privilege, stringent monitoring of account activities, regular audits, and enhancing user education on security best practices. In terms of network threats, multiple potential vulnerabilities were identified. These include risks from insider threats, inadequate segmentation and access controls, DNS tunneling, exposure of Docker Machine in the DMZ, firewall rule weaknesses, VPN server vulnerabilities, core router compromises, and risks associated with external connections. To counter these, we propose robust firewall rules, effective segmentation, encrypted VPN connections, stringent access controls, and regular security audits.

Physical assets, such as routers, workstations, and server racks, are also at risk. Physical security measures like access control, environmental monitoring, secure housing of critical hardware, and the use of tamper-evident seals are crucial. Our strategic recommendations include secure configuration management, network access control deployment, enhanced intrusion detection systems, establishing a disaster recovery site, hardware lifecycle management, physical intrusion detection systems, and secure disposal of hardware.

Controls proposed include information flow enforcement, ensuring least privilege access, comprehensive security awareness training, regular audit reviews, establishing an incident response capability, controlled maintenance, limiting physical access, vulnerability scanning, and integrated security information and event management systems. In conclusion, while our network infrastructure serves necessary functionality, we must be vigilant in protecting against threats that could exploit inherent vulnerabilities of network connections and devices. Our focus on cybersecurity measures and physical security of assets provides a comprehensive defense against all potential threats, ensuring the integrity and availability of our network infrastructure.

Network Configuration

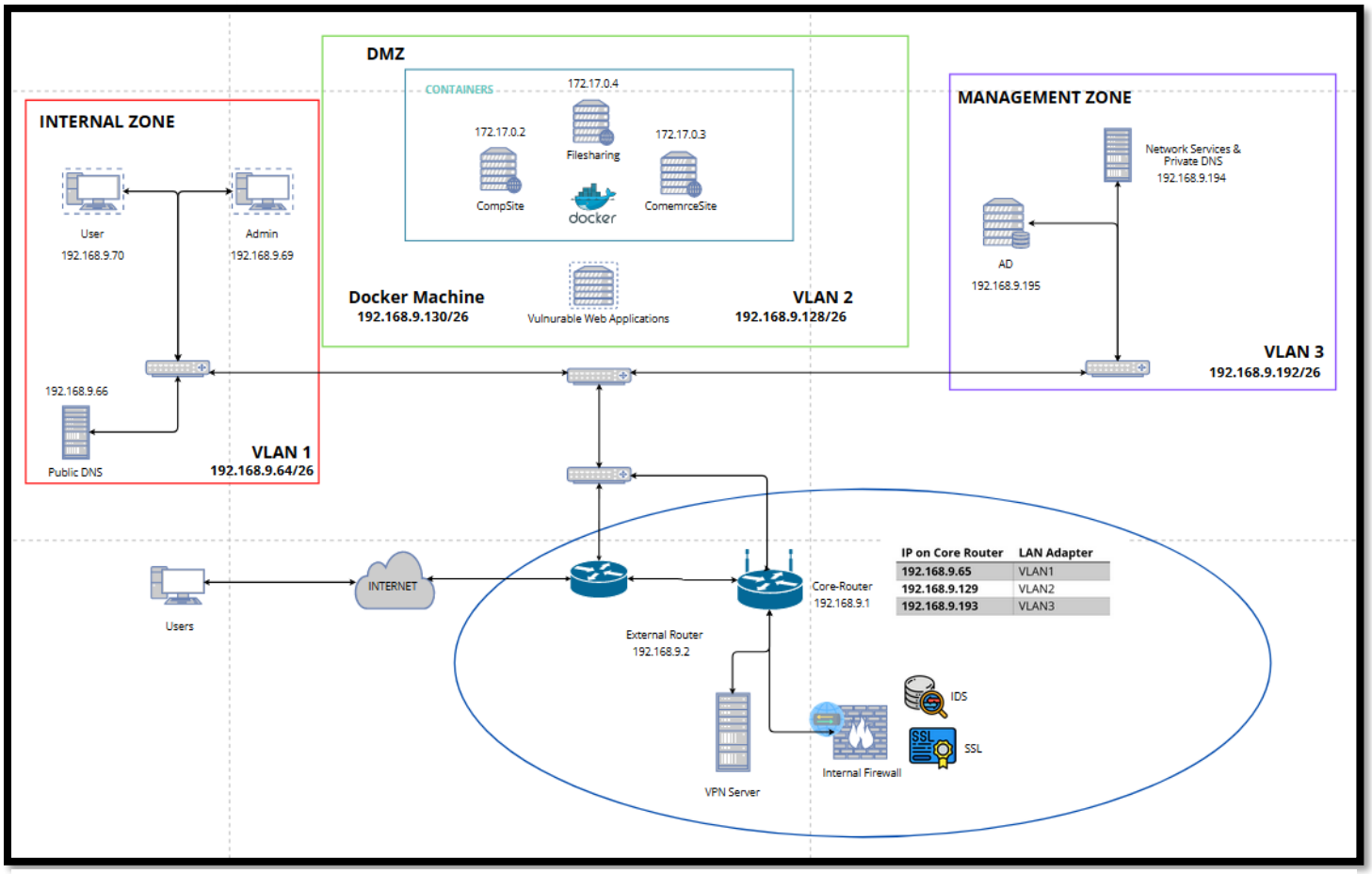
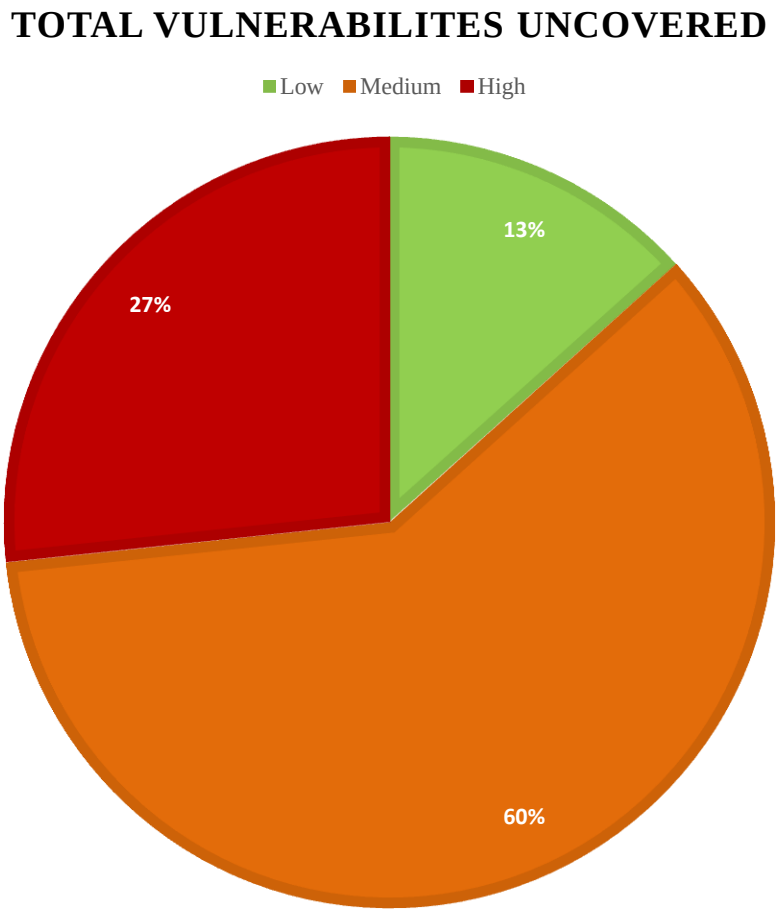


Figure 1: Network Topology

Critical Threats

➢ Applications & Services



High	Medium	Low
4	9	2

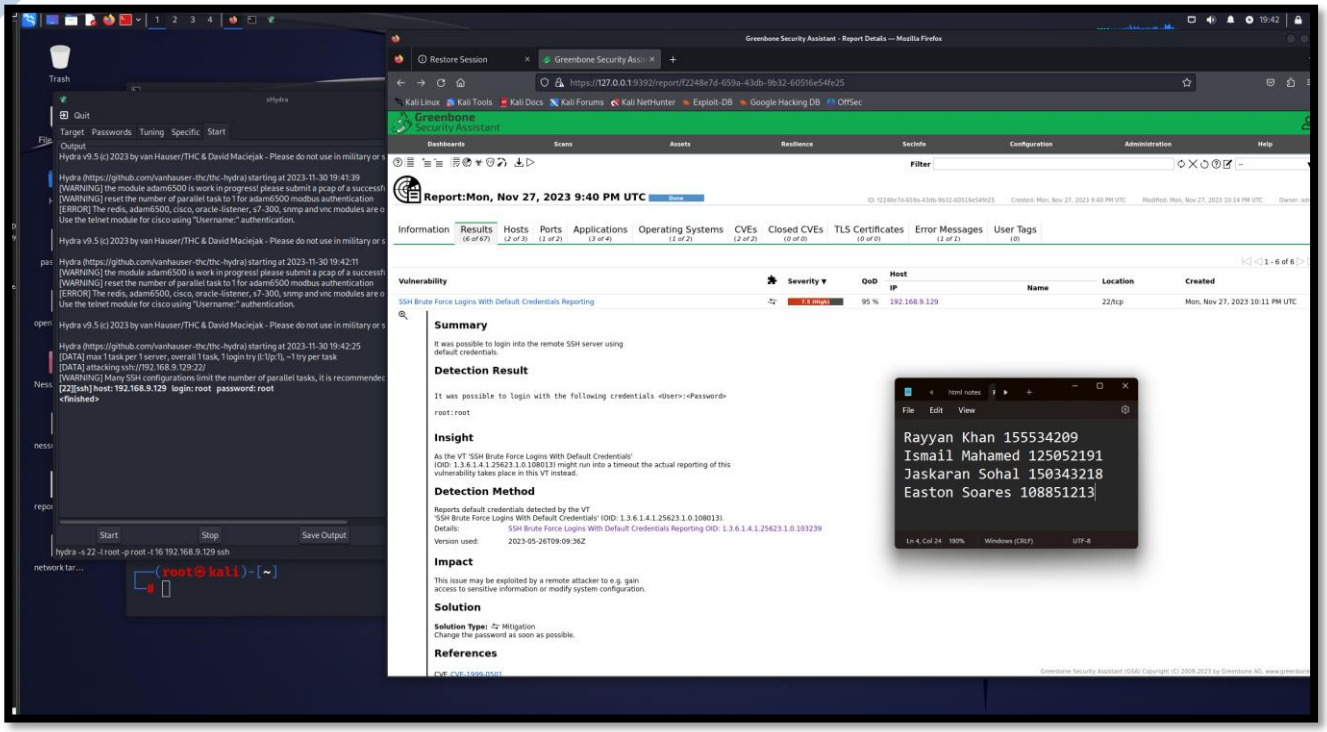


Figure 2: SSH Brute Force Login to VLAN Segment

Brute-Force Example

We identified a significant vulnerability regarding SSH brute force logins with default credentials on one of our core machines, specifically at the IP address 192.168.9.129 within the VLAN 2 segment of our network. This machine, which acts as a core router, is critical to our network's infrastructure. To assess the threat, we performed a series of penetration tests, simulating an external attacker's attempt to gain unauthorized access.

Our testing revealed that this machine was susceptible to SSH brute force attacks, primarily due to the usage of default credentials, which are often easily guessable or available in public databases of default usernames and passwords. We simulated login attempts using a combination of common usernames and passwords, and our attempts were alarmingly successful, indicating a severe security flaw.

To address this, we immediately recommended changing all default credentials to strong, unique passwords, and implementing an account lockout policy to deter brute force attacks. Moreover, we suggested the use of multi-factor authentication (MFA) for an additional layer of security.

Application and Service Threats

Regarding the broader network, we recognized that one of the biggest attack vectors was the active directory (AD) system, which, if compromised, could allow for lateral movement across user accounts. This vulnerability is particularly concerning as it can enable attackers to move stealthily within the network, escalate privileges, and gain access to sensitive information or critical systems.

Our review of the AD system uncovered that user account controls and permissions were not being managed as strictly as they should be. To mitigate this risk, we enforced the principle of least privilege, ensuring that user accounts only had access to resources essential for their roles. We also implemented more stringent monitoring of account activities to detect any unusual patterns that could indicate a compromise, such as multiple login failures or unexpected access to high-value resources.

Moreover, we proposed regular audits of user accounts and privileges, ensuring that any unnecessary accounts are disabled and that permissions are always up-to-date with current job roles. We also stressed the importance of user education, making sure that all users are aware of security best practices, such as not reusing passwords across different services and recognizing phishing attempts. By identifying these potential threats and taking immediate action to address them, we enhanced the security posture of our network and reduced the risk of successful attacks on our applications and services.

➢ Networks

In analyzing the network diagram we've worked on, we can identify several potential threats specific to network connections and the infrastructure itself. These threats can compromise not just individual systems but the entire network if not addressed promptly and effectively.

MANAGEMENT ZONE

Network Services
Private DNS
Active Directory

DEMILITARIZED ZONE

Docker containers (hosting web servers for the workplace)
Docker machine (for hosting web servers within a Docker container)

INTERNAL ZONE

User
Admin
Remote User

Internal Zone and VLAN 1 (192.168.9.64/26):

1. **Insider Threats**: With multiple users and an admin within this zone, there is a risk of insider threats. Any malicious or compromised internal actor can exploit the trust and access granted to perform unauthorized activities.

2. **Segmentation and Access Controls**: The VLAN setup must be properly configured to prevent unauthorized cross-VLAN communication. If VLAN 1 is not adequately segregated from VLANs 2 and 3, attackers could potentially pivot from one VLAN to another after compromising an initial target.

3. **Public DNS Security**: The Public DNS is a critical service and a prime target for attackers. DNS tunneling could be used to exfiltrate data from our internal network to an external server.

DMZ and VLAN 2 (192.168.9.128/26):

1. **Exposure of Docker Machine (192.168.9.130/26)**: The Docker Machine in the DMZ hosts vulnerable web applications. It's crucial that these applications are isolated from the rest of the network. Any compromise here could lead to a broader network breach.

2. **Firewall Rules and Perimeter Security**: The DMZ is typically more exposed to external threats due to its nature. Our firewall rules must be robust and regularly updated to ensure only necessary ports and protocols are open.

3. **VPN Server Security**: The VPN server provides external access to our network. Any vulnerabilities here could be exploited to gain unauthorized internal access. Ensuring that VPN connections are encrypted and authenticated is critical.

Management Zone and VLAN 3 (192.168.9.192/26):

1. **Access to Network Services and Private DNS (192.168.9.194)**: The management zone contains sensitive network services and private DNS. This zone should have stringent access controls to prevent unauthorized access from both internal and external actors.

2. **Active Directory (AD) Security (192.168.9.195)**: AD is a repository for all user accounts and credentials within our network. Compromising AD would allow attackers to move laterally across the network, escalate privileges, and access restricted data.

Core Router and VLAN Interfaces:

1. **Core Router Vulnerabilities**: The core router (192.168.9.65, .129, .193) is the backbone of our network, connecting all VLANs. If compromised, an attacker could redirect traffic, cause denial of service, or breach the network's security perimeter.

2. **Lateral Movement Risks**: The ability for an attacker to move laterally between VLAN interfaces on the core router could lead to a complete network takeover. Ensuring ACLs (Access Control Lists) are in place and effective is essential.

External Connections and the Firewall:

1. **External Router (192.168.9.2)**: As the gateway to the internet, this router must be secured against attacks. It should have the necessary configurations to prevent DDoS attacks, IP spoofing, and other common threats.

2. **IDS and SSL Inspection**: The IDS must be properly configured to detect and alert on suspicious activities. SSL inspection should be in place to check encrypted traffic, but with the necessary privacy considerations.

Overall Network Design Concerns:

1. **Single Points of Failure**: Our network must be designed to avoid single points of failure. Redundant pathways and failovers should be considered, especially for critical network components like the core router.

2. **Compliance with Security Standards**: We must ensure our network design complies with relevant security standards and frameworks to mitigate risks associated with non-compliance.

3. **Regular Security Audits**: Continuous monitoring and regular audits are crucial. Network configurations and firewall rules should be reviewed to ensure they still align with our security policies.

4. **Encryption of Data in Transit**: All sensitive data traveling across the network should be encrypted to prevent interception and ensure confidentiality.

In conclusion, while our network infrastructure serves the necessary functionality, we must be vigilant in protecting against threats that could exploit the inherent vulnerabilities of network connections and devices.

➢ Hardware and Physical Assets

Top Vulnerable Assets

Routers & Cabling

Desktop PCs, USB Ports

Physical Server Racks

Physical Assets:

1. **User and Admin Workstations (Internal Zone)**: Our workstations are critical for day-to-day operations. Physical threats include theft, unauthorized access, and damage due to environmental factors like water or fire. We should employ physical security measures such as locking devices, access control to the premises, and environmental monitoring systems.

2. **Public DNS Server (VLAN 1)**: Essential for resolving domain names, this server is a prime target for physical attacks that could disrupt network connectivity. Adequate cooling, power supply redundancy, and physical access controls are necessary to mitigate risks.

3. **Core Router (VLANs 1, 2, 3)**: This router is the backbone of our network, directing traffic between VLANs. Physical damage or tampering could cripple the entire network. We should place it in a secure location with limited access and employ hardware security modules (HSMs) for cryptographic operations.

4. **External Router and VPN Server**: The external router connects us to the internet, while the VPN server provides secure remote access. They are susceptible to physical tampering, which could lead to network breaches. They must be housed in secure, climate-controlled environments with uninterrupted power supplies (UPS).

5. **Docker Machine (DMZ)**: Hosting vulnerable web applications, this machine must be physically secure to prevent direct access or tampering that could lead to a network compromise. We need to ensure it's in a locked server room with access logged and monitored.

6. **Network Services and Private DNS (Management Zone)**: These servers manage network traffic and security policies. Physical threats include tampering and data theft. Secure racks, biometric access controls, and surveillance are recommended.

7. **Active Directory Server (Management Zone)**: AD is a repository for user credentials and policies. Physical access to this server could lead to a complete network compromise. We must secure it in a server room with multi-factor authentication access controls.

Potential Threats to Physical Assets:

1. **Environmental Threats**: Natural disasters, such as floods or earthquakes, could physically damage our network infrastructure. We must have disaster recovery plans and backups in place.

2. **Power Surges and Failures**: Sensitive network equipment could be damaged by power surges. Using surge protectors and having backup generators can mitigate this risk.

3. **Hardware Failure**: Regular wear and tear can lead to hardware failure. We need to have a maintenance schedule and spare parts for critical components.

4. **Physical Intrusion**: Unauthorized personnel gaining access to sensitive areas can tamper with or steal equipment. We need security personnel, surveillance cameras, and intrusion detection systems to prevent this.

5. **Tampering**: Deliberate tampering with network devices could lead to a breach. We need tamper-evident seals and logs of physical access to detect such activities.

6. **Theft**: Theft of equipment can result in loss of data and services. We should implement asset tracking and fast response procedures in case of theft.

7. **Interception**: Signals from unshielded cabling can be intercepted. We should use shielded cables and secure the physical infrastructure against eavesdropping.

By securing our physical assets against these threats, we can ensure the integrity and availability of our network infrastructure. It's crucial that we not only focus on cybersecurity measures but also on the physical security of our assets to provide a comprehensive defense against all potential threat

Strategic Recommendations

Recommendations:

1. **Secure Configuration Management**: It is crucial that all network devices are configured securely. We should implement a configuration management plan that includes regular reviews and audits to ensure that configurations are not only compliant with security policies but also adapted to evolving security threats and business needs.
2. **Network Access Control (NAC)**: We recommend deploying NAC to further enforce security policies for all devices attempting to access the network. This would allow us to prevent unauthorized devices from gaining network access and ensure that all devices comply with security policies before they are allowed on the network.
3. **Segmentation and Isolation**: Critical systems, especially those containing sensitive data, should be segmented from the rest of the network. We propose the use of physical or virtual segmentation to isolate these systems, which can limit the spread of potential attacks and reduce the risk of lateral movement by threat actors within our network.
4. **Disaster Recovery Site**: Establishing an offsite disaster recovery site is essential. This site should be equipped with necessary hardware and be ready to take over in case our main site becomes inoperative. Regular testing of the disaster recovery plan should be conducted to ensure it's capable of restoring operations within an acceptable time frame.
5. **Hardware Lifecycle Management**: We should adopt a hardware lifecycle management process to replace outdated and unsupported hardware. This will minimize the risk of failures and ensure that our network components remain within the support window for security updates and patches.

6. **Enhanced Intrusion Detection Systems (IDS)**: The current IDS should be upgraded to include more advanced heuristic and behavioral-based detection capabilities. This would enable us to detect and respond to unknown threats and zero-day exploits that traditional signature-based IDS might miss.
7. **Physical Intrusion Detection Systems**: In addition to CCTV surveillance, we suggest installing advanced physical intrusion detection systems such as motion sensors and alarm systems to protect against unauthorized physical access.
8. **Fire Protection Systems**: Given the electrical nature of network equipment, fire poses a significant risk. We recommend installing comprehensive fire detection and suppression systems in all areas housing critical network infrastructure.
9. **Climate Control for Hardware**: Sensitive hardware requires a controlled environment to operate optimally. We should ensure that all our hardware is stored in conditions with regulated temperature and humidity.
10. **Secure Wireless Networks**: If wireless networks are used, we recommend implementing robust security protocols such as WPA3 and regular scanning for unauthorized access points. We should also consider the use of wireless intrusion prevention systems.
11. **Redundant Internet Connectivity**: To maintain business operations, we recommend setting up redundant internet connections with automatic failover. This will help prevent a single point of failure and ensure continuous internet access.
12. **Vendor Security Management**: We need to manage the security risks associated with third-party vendors. This includes conducting regular security assessments of vendors and ensuring that they adhere to our security requirements.
13. **Security Information and Event Management (SIEM) Integration**: Our SIEM system should be integrated with all network hardware to provide centralized logging and correlation of security events, which can speed up the detection of and response to incidents.
14. **Power Supply Security**: We advise the use of UPS systems and redundant power supplies for all critical hardware to protect against power fluctuations and outages.
15. **Data Center Physical Security**: For any on-premise data centers, we should enforce strict physical security protocols, including mantraps, security guards, and biometric access controls.
16. **Mobile Device Management (MDM)**: With the prevalence of mobile devices accessing our network, an MDM solution should be implemented to manage and secure these devices effectively.
17. **Secure Disposal of Hardware**: As we upgrade our hardware, secure disposal methods must be put in place to prevent data recovery from old devices.

Controls

Access Control (AC):

AC-4 Information Flow Enforcement: Enforce approved authorizations for controlling the flow of information within the network, particularly between different zones (e.g., Internal, DMZ, Management).
AC-6 Least Privilege: Ensure that users have only the access necessary to perform their duties. This might involve restricting admin access to only those who need it.

Awareness and Training (AT):

AT-2 Security Awareness Training: Provide training for all users, including administrators and managers, regarding cybersecurity threats and best practices.

Audit and Accountability (AU):

AU-6 Audit Review, Analysis, and Reporting: Regularly review and analyze audit logs to detect unauthorized or malicious activity.

Incident Response (IR):

IR-4 Incident Handling: Establish an incident response capability to handle incidents that include execution of a response plan and post-event analysis.

Maintenance (MA):

MA-2 Controlled Maintenance: Perform maintenance on the network infrastructure with proper oversight and ensure maintenance tools are appropriately protected.

Physical and Environmental Protection (PE):

PE-2 Physical Access Authorizations: Limit physical access to the network infrastructure, especially in sensitive areas like the management zone.

Risk Assessment (RA):

RA-5 Vulnerability Scanning: Perform regular vulnerability scanning of exposed services, particularly those in the DMZ and the Docker machine.

Conclusion

After a thorough cybersecurity assessment by our group, we have identified key vulnerabilities and proposed comprehensive measures to enhance our network's security. These include strengthening passwords, enforcing least privilege access, improving user account management in the active directory, enhancing network security through robust firewall rules and segmentation, and bolstering physical security for critical hardware.

Our strategic approach involves deploying advanced security solutions such as network access controls, intrusion detection systems, and comprehensive security training for all users. We also emphasize the importance of regular audits, incident response planning, and secure hardware disposal.

In summary, our findings underscore the urgent need for a holistic and proactive approach to cybersecurity, encompassing both digital and physical defenses. By implementing these strategies, we can significantly fortify our network against a wide range of threats, safeguarding our critical data and infrastructure.