Securing segmented networks: Vulnerability detection methods and cybersecurity strategies

Vitalii Vlasenko[1,*,†], Halina Lastivka[1,†], Mykola Shalaiev[1,†], Dinara Ospanova[2,†] and Andrii Samila[1,†]

[1]Yuriy Fedkovych Chernivtsi National University, Kotsyubynsky Str., 2, Chernivtsi, 58002, Ukraine
[2]Kazakh Humanitarian Juridical Innovative University, Mengilik Str.,11, Semey, 070000, Kazakhstan

Abstract

The paper presents an approach to protecting segmented networks using the example of a created architecture of a learning environment for cybersecurity students, where practical skills can be honed. The stages of network design are considered, taking into account the principles of isolation, zoning, and access restrictions, as well as methods for identifying vulnerabilities and analyzing typical threats. In the process of building the environment, Proxmox and OPNsense technologies were used to ensure the implementation of a virtualized and flexible network infrastructure. An approach to creating a protection system and conducting re-testing to confirm the effectiveness of the implemented measures is described. The proposed solution helps to increase network resilience and has practical value for educational and research purposes.

Keywords

cybersecurity, network segmentation, vulnerabilities, training environment, Proxmox, OPNsense, security testing

1. Introduction

In today's conditions of increasing cyberattacks and the sophistication of attackers' methods, ensuring the protection of network infrastructure is a priority task for organizations and educational institutions. One effective way to increase the level of security is through network segmentation—dividing the overall infrastructure into isolated zones with limited access between them. This approach helps reduce the attack surface, localize security incidents, and limit their impact on other parts of the system.

As part of this work, a segmented network architecture was developed, which is used as a learning environment for students studying cybersecurity. This environment allows modeling of typical network scenarios, investigation of vulnerabilities, study of attack methods, and mastery of modern protection approaches. The article considers key aspects of designing such an architecture, identifying and analyzing vulnerabilities, implementing protective measures, and testing their effectiveness.

The relevance of the topic is due to the need for practically oriented approaches to studying network security, as well as the importance of a systems vision when building secure information environments.

2. Designing a virtualized segmented network for an educational environment

The presented architecture demonstrates an example of implementing a distributed segmented network based on the Proxmox virtualization platform [1]. This model provides high flexibility in managing

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

*Corresponding author.
†These authors contributed equally.
v.vlasenko@chnu.edu.ua (V. Vlasenko); g.lastivka@chnu.edu.ua (H. Lastivka); shalaiev.mykola@chnu.edu.ua (M. Shalaiev); d.ospanova@gmail.com (D. Ospanova); a.samila@chnu.edu.ua (A. Samila)
0000-0002-9085-5787 (V. Vlasenko); 0000-0003-3639-3507 (H. Lastivka); 0009-0006-3801-3511 (M. Shalaiev); 0000-0002-6131-4113 (D. Ospanova); 0000-0001-8279-9116 (A. Samila)

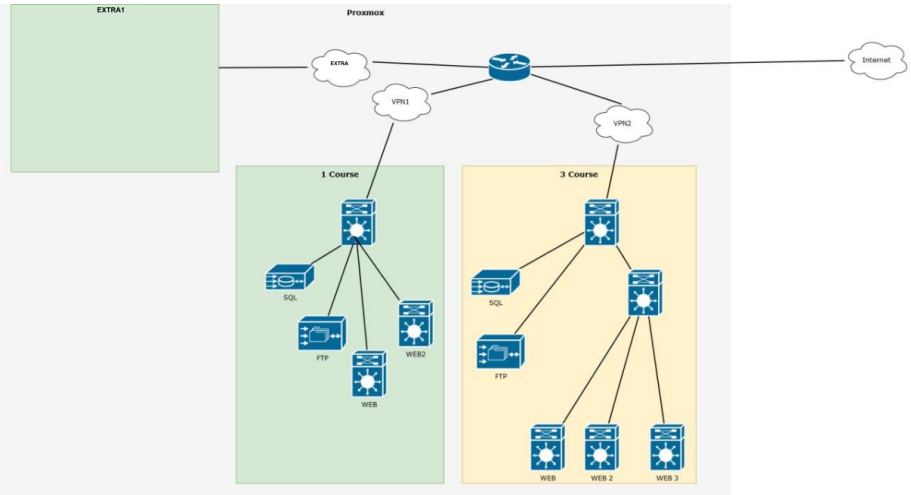

Figure 1: Scheme of the developed architecture of distributed networks.

computing resources, allows scaling the learning environment and implementing modern approaches to ensuring information security [2].

The network is logically divided into three separate segments, each of which performs a separate functional role. The first of these is the EXTRA segment, which is represented by the isolated EXTRA1 environment. It is connected to the Proxmox virtualization server and has its own secure VPN connection (VPN1), which allows it to communicate with the internal network without direct access to other segments. The EXTRA segment can act as a service environment — for example, contain backup systems, centralized monitoring, or external access services [3].

The second segment is the learning environment for first-year students — the "1 Course" segment. Its structure includes virtual servers, including a SQL server for storing and processing databases, an FTP server for file exchange, and two web servers (WEB and WEB2) used for testing and hosting web applications. All these nodes are interconnected via a local network switch or router, which also provides network connectivity via a VPN1 tunnel. The segment operates in isolation, which avoids unwanted influence on other parts of the network and a secure environment for conducting practical exercises [2].

The third segment is intended for third-year students and is designated as "3 Course". It implements a more complex infrastructure, including a separate SQL server, FTP server, and three web servers (WEB, WEB2, WEB3), each of which can be configured for a separate software environment or a specific educational task. This segment is connected to the central router via a separate VPN tunnel (VPN2), which allows not only to provide isolation from other environments, but also to apply its own rules for filtering and auditing traffic [3].

At the center of the general network is a router that acts as the main connection node. It provides access to the Internet for all segments, processes VPN connections (VPN1 and VPN2), and manages routing between network components. In addition, it can act as a firewall that controls access to external resources and protects against unauthorized connections [4].

The overall architecture provides high isolation between segments, which is important from a security point of view. The first and third year learning environments operate autonomously, without direct access to each other. Each VPN tunnel can be configured with its own access policies, which further enhances security [9]. By using Proxmox as a virtualization platform, administrators can quickly scale the environment, add new servers, or rebuild segments without significant technical overhead [1].

Thus, this architecture not only allows for efficient resource allocation between user groups, but also creates a solid foundation for building a practical environment with an emphasis on security and access control. This is especially important for educational institutions and laboratories where participants work with systems that simulate real-world network structures and threats [1].

3. Methods for detecting vulnerabilities in segmented network infrastructure

After developing and implementing the segmented network architecture, the next step is to assess it from a security perspective. Vulnerability testing allows to identify weaknesses in the settings of network services, software, and also to verify the effectiveness of the applied protection measures. Conducting such tests is critical to preventing potential attacks, information leaks, and violations of the integrity of the educational environment [5].

Within a segmented network, testing is carried out taking into account the division into separate functional zones. Each segment is analyzed independently, which allows us to focus on specific vulnerabilities inherent in a particular environment. This approach helps reduce the load on other parts of the network during scanning, but also to better localize the source of problems in case of detection of potential threats [6].

During testing, the main attention is paid to the most vulnerable services, such as web servers, FTP servers, and SQL databases. For example, web servers are tested for typical OWASP Top 10 vulnerabilities: SQL injection, cross—site scripting (XSS), weak authentication, dangerous configurations, or data leaks via HTTP headers. FTP servers are tested for anonymous access, weak encryption, or open ports. SQL servers are analyzed for incorrect permissions, injection vulnerabilities, and dangerous API requests [7].

The most popular open source and commercial tools are used during testing. These include:

- Nmap is a multi—purpose network scanning tool. It allows us to identify open ports, available services, operating systems, and key vulnerabilities. In the context of a segmented network, Nmap helps build a map of accessible nodes within a specific segment [8].
- Nessus is a commercial vulnerability scanner that provides detailed information about detected threats, categorizes them by risk level, and suggests remediation methods. Nessus is widely used to analyze internal servers—such as FTP or SQL—with a focus on known CVE vulnerabilities [5].
- OpenVAS is a free alternative to Nessus that also performs deep system auditing for vulnerabilities. It can be integrated into automated scan scripts or used manually during scheduled audits [6].
- CrackMapExec (CME) is a powerful security assessment tool for Windows/Active Directory environments. It can verify credentials, execute commands on remote hosts, detect configuration errors, open SMB layers, and other potential attack vectors. CME is particularly effective for examining interactions between nodes within a segment or when simulating the movement of an attacker within a network [6].
- Burp Suite is a tool for testing the security of web applications. Its main strength lies in the ability to intercept, analyze, and modify HTTP requests and responses. Burp Suite is particularly useful for detecting logic errors, XSS attacks, CSRF vulnerabilities, and testing authentication mechanisms [2].
- The Metasploit Framework is a powerful vulnerability exploitation framework that allows to simulate attacks based on the vulnerabilities found. In an educational environment, it is used to demonstrate practical exploitation scenarios, simulate intrusions, and test the effectiveness of attack detection tools [2].

4. Evaluation of testing results and classification of identified vulnerabilities

After the completion of vulnerability scanning, penetration testing, and security assessments, the next crucial stage involves an in-depth analysis of the results obtained. This process is not limited to simply documenting the identified weaknesses; rather, it aims to evaluate their criticality, determine the potential impact on the organization's infrastructure and business processes, and establish a clear order of priority for remediation. A comprehensive and well-structured interpretation of testing outcomes

enables the creation of an effective cybersecurity enhancement strategy that is both technically and strategically justified [5].

During the analysis phase, all detected vulnerabilities are systematically classified according to their type, severity, location within the network infrastructure, and likelihood of exploitation. Common categories include software flaws such as SQL injection or Cross-Site Scripting (XSS), insecure configurations such as open ports or anonymous logins, weak authentication mechanisms, outdated software components, and the use of insecure protocols. The severity of each issue is typically determined using the Common Vulnerability Scoring System (CVSS v3.1), which assigns a numerical value from 0.0 (none) to 10.0 (critical) based on a set of technical and contextual factors. These include the attack vector (local, adjacent network, or remote), attack complexity, required privileges, necessity of user interaction, and the potential impact on the confidentiality, integrity, and availability of systems.

In some cases, additional assessment models such as the OWASP Risk Rating Methodology or the DREAD framework are used to complement CVSS scoring, especially when there is a need to incorporate a broader business impact perspective. This ensures that the remediation strategy is not solely based on technical metrics but also takes into account the operational, reputational, and financial consequences of a potential exploit [6].

The analysis process often reveals a wide range of issues with varying degrees of severity. For example, in the “1 Course” network segment, scanning revealed the possibility of anonymous access to an FTP server without authentication. This misconfiguration, which allows unauthorized users to view or modify files, is rated as a medium-severity vulnerability [8]. Another finding involved the use of an outdated Apache HTTP server version containing multiple publicly disclosed CVEs, including a remote code execution flaw [2]. Due to its high CVSS score, this issue was deemed critical and in need of immediate software updates. In the “3 Course” segment, a web application was found to lack adequate user input filtering, enabling the execution of XSS attacks that could result in the theft of user session tokens or the injection of malicious content. Additionally, the discovery of an active Telnet service transmitting data in cleartext presents a serious security risk, as it allows attackers to intercept credentials during transmission [2].

In the “EXTRA” segment, the use of weak SMB credentials was confirmed using the CrackMapExec tool, enabling unauthorized execution of commands on remote hosts and facilitating lateral movement within the network. Furthermore, in several environments, network segmentation flaws allowed hosts from one segment to scan and interact with systems in other supposedly isolated zones, undermining the principle of security boundaries [2].

All of these vulnerabilities are thoroughly documented with detailed descriptions, including technical evidence such as affected services, software versions, CVE identifiers, and proof-of-concept data. Each entry also contains a risk assessment based on CVSS scoring, the probability of exploitation, and the potential damage to the organization, followed by clear recommendations for remediation. These may include applying security patches, modifying configurations, enforcing stricter access control, or implementing additional protective measures [8].

- A description of the problem.
- Technical details (open port, service, version, CVE-identifier).
- A risk assessment (CVSS score, probability of exploitation, potential damage).
- Remediation recommendations (updates, configuration changes, additional protection).

Such a comprehensive evaluation process provides not only a clear understanding of the current security posture but also serves as the foundation for a targeted and prioritized remediation plan. By aligning technical severity scores with real-world business impact, organizations can ensure that their efforts are focused on addressing the most dangerous and exploitable vulnerabilities first, thereby significantly enhancing overall network resilience and reducing the risk of successful cyberattacks [3].

5. Network security strategy development and practical recommendations

After completing the stages of architecture analysis, penetration testing, and vulnerability identification, the next critical step is to implement effective and sustainable measures to enhance network security. The goal is not limited to addressing the vulnerabilities already discovered, but to create a comprehensive, forward-looking strategy aimed at preventing future attacks and ensuring long-term resilience [7].

A fundamental element of this strategy is the least privilege principle. Each user account, service, or process should have only the minimal rights necessary to perform its assigned tasks. By applying Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC), organizations can precisely define access levels, reducing the risk of lateral movement by attackers in case of account compromise [7].

Another cornerstone is network segmentation. A properly segmented network architecture should divide the infrastructure into distinct security zones — such as production, testing, administrative, and guest networks — with clearly defined boundaries enforced by firewalls or advanced routing rules. Micro-segmentation, achievable via Software-Defined Networking (SDN) solutions, can provide even finer isolation, allowing administrators to monitor and control inter-segment traffic with greater accuracy [3].

Patch and update management must be an ongoing process. All servers, network devices, and software components should be continuously monitored for security updates, preferably through automated patch management systems. Given the risks associated with Common Vulnerabilities and Exposures (CVEs), rapid patching of internet-facing assets, such as web servers and databases, is essential to minimize the exploitation window. Vulnerability scanners like Nessus, OpenVAS, or Qualys can be integrated into routine maintenance cycles to identify outdated or misconfigured components [5].

Authentication hardening plays a pivotal role in securing access. Multi-Factor Authentication (MFA) should be mandated for all administrative accounts, VPN access points, and sensitive systems. Strong password policies, enforced rotation, limited session duration, and the deployment of anomaly-based login monitoring mechanisms further reduce the risk of unauthorized entry [7].

In segmented networks, clear zoning policies are mandatory. Test, training, and production environments must remain completely isolated, each governed by tailored access, monitoring, and control policies. Unauthorized creation of tunnels between these zones should be strictly prohibited, with any exceptions subject to real-time monitoring and audit logging.

For threat detection, deploying Intrusion Detection Systems (IDS) such as Suricata, Zeek (formerly Bro), or Snort is highly recommended. These tools can detect port scanning, exploit attempts, and the transfer of suspicious payloads. When integrated with centralized Security Information and Event Management (SIEM) platforms like the ELK Stack, Graylog, or Wazuh, organizations can achieve real-time correlation of security events and enable rapid incident response [3].

Access protocol security is another crucial consideration. Legacy, unencrypted protocols like Telnet and FTP should be entirely phased out in favor of secure alternatives — SSH, SFTP, or FTPS. Furthermore, remote administrative access should be restricted to a defined set of trusted IP addresses, enforced through IP whitelisting or Zero Trust Network Access (ZTNA) solutions.

Beyond technical controls, human factor mitigation is essential. Continuous security awareness training should be conducted for all staff or students interacting with the network. Education on cyber hygiene, phishing recognition, and social engineering prevention is critical to reducing the likelihood of successful human-targeted attacks. Regular phishing simulations and scenario-based training can significantly improve resilience.

In conclusion, effective network protection demands a multi-layered defense model:

- Technical isolation via segmentation and secure communication protocols.
- Strict access control through least privilege enforcement and authentication hardening.
- Continuous monitoring with IDS/IPS and SIEM integration.
- Vulnerability management through proactive patching and scanning.

- Human-centric security via awareness training and behavioral risk reduction.

Implementing these recommendations aligns with the principles outlined in NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and CIS Critical Security Controls, substantially increasing an organization's cyber resilience and reducing the probability of a successful compromise.

6. Validation of the effectiveness of security measures through re-testing

After implementing security measures, it is critical to retest the network to assess the effectiveness of the implemented solutions. This testing helps ensure that the vulnerabilities identified during the initial analysis have been successfully eliminated and potential attack vectors have been closed. In addition, retesting may reveal new weaknesses that may have appeared as a result of changes in the architecture or system updates [2]. Regular retesting is becoming an integral part of the network security management cycle. It allows us to maintain the relevance of protection measures in the face of the rapid development of cyber threats and changes in the technological environment. This approach helps not only to minimize risks, but also to increase the overall level of confidence in the security of the information infrastructure [6]. Thus, retesting and confirmation of protection are key stages in ensuring the reliability and resilience of segmented networks. They allow not only to close existing vulnerabilities, but also to establish constant control over security, which is especially important in the face of modern cyber threats that are constantly evolving and becoming more complex [2].

7. Conclusions

The paper considers the creation of a training segmented network environment and practical approaches to its protection. The most common vulnerabilities and methods of attacks on various network components are analyzed, and appropriate security measures are proposed. Repeated testing confirmed the effectiveness of the implemented solutions. The developed environment is used in the educational process, where cybersecurity students have the opportunity to hone practical skills in conditions close to real ones. The results emphasize the value of using segmentation as a training tool and its role in improving cybersecurity posture.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Proxmox ve administration guide, https://pve.proxmox.com/pve-docs/, 2025.

[2] W. Stallings, Network Security Essentials: Applications and Standards, Pearson, 2017.

[3] Cisco Systems, Network segmentation best practices, https://www.cisco.com/c/en/us/solutions/enterprise-networks/network-segmentation.html, 2021.

[4] Opnsense and proxmox integration best practices, https://forum.opnsense.org/index.php?topic=XXXX, 2025.

[5] K. Scarfone, W. Jansen, Guidelines on network security testing, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf, 2008.

[6] M. Whitman, H. Mattord, Principles of Information Security, Cengage Learning, 2018.

[7] D. Kim, M. Solomon, Fundamentals of Information Systems Security, Jones & Bartlett Learning, 2016.

[8] S. Northcutt, Network segmentation and microsegmentation for security, https://www.sans.org/white-papers/39827/, 2019.