6-14-2024

Business Network Security and Risk Assessment

ehsan sheybani
USF, eosheybani@gmail.com

Giti Javidi
University of South Florida, javidi@usf.edu

BUSINESS NETWORK SECURITY AND RISK ASSESSMENT

TREO Paper

Ehsan Sheybani, University of South Florida, Tampa, FL, USA, sheybani@usf.edu

Giti Javidi, University of South Florida, Tampa, FL, USA, javidi@usf.edu

Abstract

In our increasingly interconnected global context, computer networks play a pivotal role in collecting and transmitting data across diverse applications such as environmental monitoring, industrial automation, healthcare, and smart city development. The growing significance of computer networks accentuates the need to address the complex challenges related to security, privacy, and forensics. This article explores the nuanced landscape of computer network security, striking a delicate balance between preserving data privacy and maximizing utility. Emphasis is placed on the emerging field of computer network forensics, with a specific focus on the assessment of network risks. In light of this, the article is recommended as essential reading, serving as a foundation for understanding computer network vulnerability and risk assessment in conjunction with other related articles. This research contributes to the discourse on securing computer networks, crucial for their sustained functionality in our interconnected world.

Keywords: Computer Networks; Risk; Security; Vulnerability.

1 Introduction

The increasing dependence on computer networks for communication and data exchange has elevated their attractiveness as prime targets for cyber attackers (Süzen, 2020). Within these networks, critical devices such as routers, switches, firewalls, and servers are particularly susceptible to malicious activities (Sebastian, & Hahn, 2017). Facing a spectrum of vulnerabilities, including malware infections, denial-of-service (DoS) attacks, and hacking attempts (Oser, Engelmann, Lüders, & Kargl, 2023), (Daud, Bakar, & Hasan, 2014), these network components demand focused attention for risk identification and mitigation. This article aims to provide a comprehensive understanding of the methodologies employed to identify risk sources associated with network devices, emphasizing key parameters influencing this risk. Additionally, it introduces a structured methodology for assigning a risk score to a network, rooted in the identification of these pivotal parameters. The primary contribution lies in the recognition and classification of features affecting the security of computer and/or IoT networks, establishing correlations that render them susceptible to security threats or attacks (Daud, Bakar, & Hasan, 2014). The article explores parameters, sources of risk, risk and vulnerability assessment tools, limitations of these tools, the integration of AI/ML in risk assessment, and challenges associated with AI/ML approaches to risk assessment. The focus is on examining the complex landscape of network forensics, particularly concerning the evaluation of network risks to provide insights into the vulnerabilities and risk assessment methods. This research is an attempt to fill the research gap, namely the need for a comprehensive exploration of the interplay between data privacy, network security, and utility maximization within computer networks, particularly focusing on the emerging field of network forensics and risk assessment. As such, here are the research questions addressed by this work:

How can the delicate balance between data privacy preservation and utility maximization be achieved within computer networks?

What are the emerging challenges and opportunities in the field of computer network forensics?

What methodologies and techniques can be employed for the assessment of network risks in the context of evolving cyber threats?
How do factors such as network topology, data encryption, and intrusion detection systems impact the overall security posture of computer networks?
What are the implications of network vulnerability and risk assessment for ensuring the sustained functionality of computer networks in our interconnected world?

1.1 Sources of risk for network devices

The following are the primary sources of risk associated with network devices:
Software Vulnerabilities: Network devices run on software, and any software can have vulnerabilities that attackers can exploit. A vulnerability is a weakness in the software that an attacker can use to gain unauthorized access or control of the device.
Misconfiguration: Misconfiguration occurs when network devices are not set up correctly, leading to security holes that attackers can exploit. Misconfiguration can also result in poor performance or even network downtime.
Insider Threats: Insider threats refer to the risk of an attack or data breach by an employee or someone with authorized access to the network. Insider threats can be intentional, such as a disgruntled employee seeking revenge, or unintentional, such as an employee accidentally exposing sensitive information.
Social Engineering: Social engineering is a technique used by attackers to manipulate people into divulging sensitive information or performing actions that compromise network security. Social engineering attacks can take many forms, including phishing, pretexting, and baiting.
Physical Threats: Physical threats refer to the risk of damage or theft of network devices. An attacker can gain physical access to a device and tamper with it, steal it, or destroy it (Chalvatzis, Karras and Papademetriou, 2019).

1.2 Parameters affecting risk

The following parameters have the most significant impact on the risk associated with network devices:
Network Complexity: The complexity of a network is a crucial factor in its risk management. A complex network is more challenging to manage and secure than a simple network, making it more vulnerable to attacks.
Access Control: Access control refers to the process of granting or denying access to network resources. Weak access control mechanisms can lead to unauthorized access, increasing the risk of attacks.
Patch Management: Patch management is the process of applying updates to software and devices to address security vulnerabilities. Poor patch management practices can leave network devices vulnerable to known exploits.
Security Monitoring: Security monitoring involves the continuous monitoring of network devices to detect and respond to security incidents. Inadequate security monitoring can delay detection and response to attacks, increasing the risk of damage.
Employee Training: Employee training refers to the process of educating employees on network security best practices and procedures. A lack of employee training can lead to unintentional security breaches, increasing the risk of attacks (Chalvatzis, Karras and Papademetriou, 2019).

2 Vulnerability Scanning

Vulnerability scanning is the process of identifying potential security vulnerabilities in a network, system, or application In the ever-evolving landscape of cybersecurity, vulnerability scanning stands as a critical defense mechanism against potential threats lurking within digital ecosystems. This proactive approach involves the systematic exploration of computer systems, networks, and applications to identify vulnerabilities that could be exploited by malicious actors. Vulnerability scanning not only serves as an initial line of defense but also provides organizations with valuable insights into their digital infrastructure's weaknesses. By shining a light on these vulnerabilities, organizations can take targeted measures to fortify their defenses and enhance their overall security posture. In an era where digital

assets are constantly under siege, vulnerability scanning emerges as an indispensable practice to safeguard sensitive information and maintain the integrity of digital operations [19].
In an interconnected world teeming with sophisticated cyber threats, the importance of vulnerability scanning cannot be overstated. As organizations increasingly rely on digital technologies to streamline operations, deliver services, and store sensitive data, they also become more susceptible to cyberattacks. Vulnerability scanning acts as a proactive shield, enabling organizations to identify and rectify potential weak points before malicious actors capitalize on them. By regularly assessing systems and applications for vulnerabilities, organizations can effectively reduce the attack surface, thwart potential breaches, and adhere to regulatory compliance standards. In this dynamic cybersecurity landscape, vulnerability scanning empowers organizations to stay one step ahead of cyber threats and maintain the trust of their stakeholders. There are several methods for vulnerability scanning, including:
Network Scanning: Involves using automated tools to scan a network for vulnerabilities. The tools scan open ports, network services, and protocols to identify potential vulnerabilities.
Host-based Scanning: Involves scanning individual devices, such as servers, desktops, or laptops, to identify vulnerabilities in the operating system, installed applications, and system configurations.
Application Scanning: Involves scanning web applications and databases to identify potential vulnerabilities. The tools simulate attacks and analyze the application's response to identify vulnerabilities, such as SQL injection or cross-site scripting.
Manual Testing: Involves testing the network, system, or application manually to identify vulnerabilities. Manual testing requires expertise and may be time-consuming, but it can provide a more comprehensive assessment of the security posture.
Cloud-Based Scanning: Involves scanning cloud-based infrastructure and applications for vulnerabilities. The tools are designed to scan the cloud environment, including virtual machines, storage, and databases.
Passive Scanning: Passive scanning involves monitoring network traffic to identify potential vulnerabilities. Passive scanning does not generate traffic, making it less intrusive and suitable for environments with strict security requirements.
Organizations should perform regular vulnerability scanning to identify potential threats and vulnerabilities and take appropriate measures to mitigate them (Chalvatzis, Karras and Papademetriou, 2019), (Süzen, 2020), (Wang, Bai, Li, Chen, & Chen, 2020).

References

Chalvatzis, I., D. A. Karras and R. C. Papademetriou, (2019). "Evaluation of Security Vulnerability Scanners for Small and Medium Enterprises Business Networks Resilience towards Risk Assessment," *2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, Dalian, China, 2019, pp. 52-58, doi: 10.1109/ICAICA.2019.8873438.

Daud, N. I., Bakar, K. A. A., & Hasan, M. S. M. (2014, August). "A case study on web application vulnerability scanning tools," In *2014 Science and Information Conference* (pp. 595-600).

Mazhar, T., Irfan, H. M., Khan, S., Haq, I., Ullah, I., Iqbal, M., & Hamam, H. (2023). "Analysis of Cyber Security Attacks and Its Solutions for the Smart Grid Using Machine Learning and Blockchain Methods," *Future Internet*, *15*(2), 83.

Oser, P., Engelmann, F., Lüders, S., & Kargl, F. (2023, April). "Evaluating the Future Device Security Risk Indicator for Hundreds of IoT Devices," In *Security and Trust Management: 18th International Workshop, STM 2022, Copenhagen, Denmark, September 29, 2022, Proceedings* (pp. 52-70). Cham: Springer International Publishing.

Sebastian, D. J., & Hahn, A. (2017, September). "Exploring emerging cybersecurity risks from network-connected DER devices," In *2017 North American Power Symposium (NAPS)* (pp. 1-6).

Süzen, A. A. (2020). "A Risk-Assessment of Cyber Attacks and Defence Strategies in Industry 4.0 Ecosystem*," International Journal of Computer Network & Information Security*, 12(1).

Wang, Y., Bai, Y., Li, L., Chen, X., & Chen, A. (2020, June). "Design of network vulnerability scanning system based on NVTs," In *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)* (pp. 1774-1777).