Analysis and Audit of Campus Network

Gowri Arunsha [1] Sanjay J Prakash [1] Suryanarayan Menon A [1]
Vinayak Naveen [1] Josna V R [2]

Abstract

An analysis and audit of a campus network involves evaluating the network infrastructure, devices, and configurations to ensure optimal performance and security. This includes checking hardware and software components, evaluating network capacity and performance, and identifying vulnerabilities. Security measures such as firewalls, access controls, and intrusion detection systems are reviewed. Network diagrams are created to visualize the infrastructure, and vulnerability analysis is performed. Tools like Nmap are used for network scanning, while pfSense, an open-source firewall program, is implemented for security measures with the addition of pfBlockerNG for advanced features. The goal is to identify weaknesses, address issues, and provide recommendations for enhancing network performance and security.

Introduction

The current network infrastructure at Government Engineering College, Barton Hill, Thiruvananthapuram is outdated and lacking in necessary security measures, leading to vulnerabilities and inefficiencies. To address these issues, a project was undertaken to modernize the network infrastructure and enhance computing and data security. The project involved examining the existing network, documenting its topology, and identifying vulnerabilities. Tools like GNS3, Kali Linux's Nmap, and pfSense were used for network analysis, detecting open ports, implementing access control measures, and deploying an Intrusion Detection System (IDS). An iterative approach was followed, continually improving procedures and addressing vulnerabilities. The solutions were thoroughly tested in a virtual environment before deployment, ensuring scalability and dependability. The entire process and outcomes are also detailed in a report.

Objectives

The present study investigates the following objectives:

- **Objective 1:** Inspect, analyze and provide a better, more flexible understanding about the college's current network infrastructure.
- **Objective 2:** Network vulnerability assessment, exploit enumeration, their reporting to authorities, and provision of solutions for the same.

Methodology and Implementation

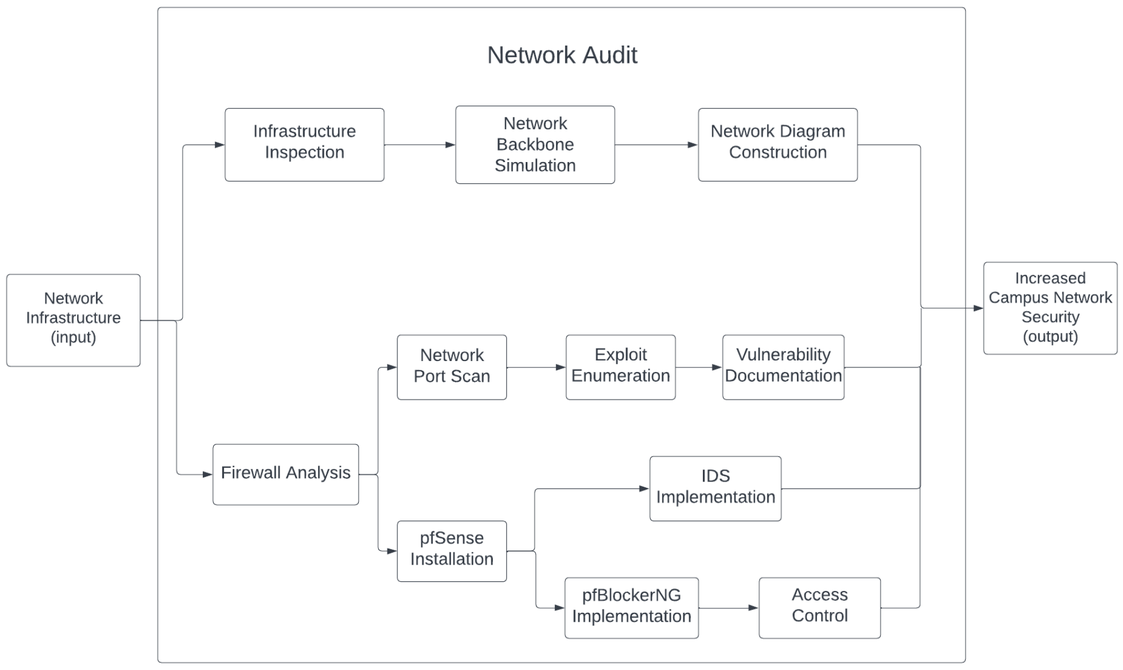

Figure 1. Project Flow Chart

We did a detailed investigation of the college network throughout the project to get a complete grasp of its infrastructure. This entailed walking across campus, detecting entry points, and recording any problems or weaknesses. We built sophisticated simulations using technologies like GNS3 to aid with analysis and planning. These simulations gave us a realistic image of the network, allowing us to discover possible flaws and create appropriate security solutions.

In order to improve network security, we performed a full firewall assessment. The existing firewall was discovered to have multiple vulnerabilities and obsolete firmware. We chose an alternative approach rather than investing a significant amount of money (15 lakh INR) in new firewall infrastructure. We implemented pfSense, an affordable and open-source firewall technology, which proved to be instrumental in addressing our security concerns.

By deploying pfSense, we were able to significantly reduce our exposure to potential threats. Additionally, we integrated supplementary programs like pfBlockerNG, which enabled us to enhance our access control capabilities by blocking specific domains. This strategic decision not only resulted in substantial cost savings but also provided us with a flexible and robust security solution. The adoption of pfSense and its associated programs allowed us to achieve a higher level of network security while ensuring the efficient allocation of our resources. By leveraging these technologies, we successfully mitigated security risks and established a more resilient network infrastructure.

In addition to the network mapping, we conducted comprehensive network penetration testing utilizing tools like Nmap and the Kali Linux tool suite. This testing allowed us to assess the network's resilience to potential attacks by performing thorough scans and identifying vulnerable areas. Through these tests, we successfully uncovered and exposed numerous vulnerabilities, enabling us to proactively address them. By reporting these vulnerabilities, we not only bolstered network security but also raised awareness among campus officials about the potential threats and the necessary actions to mitigate them effectively.

Results and discussion

We meticulously mapped our college network by conducting a comprehensive inventory of network devices, including switches, routers, access points, and endpoints. We identified their physical locations and relevant details, and created a visually descriptive network diagram using gns3 software. The diagram showcased the overall layout and topology of our college network. Starting from the main switch, SGE2000, connections were established to different areas within the main building, such as the ITHoD room, office, and library. Additionally, connections extended to various labs, staff rooms, hostels, and other blocks. Notably, the diagram highlighted the interconnections between switches and the specific devices they provided network access to, enhancing our understanding of the network's structure.

Problem	Description	Solution
11 devices running rpcbind protocol on port 135.	RPC enumeration possible to launch Remote Code Execution attacks, attacker could compromise information about active services.	Filter access to port 135 (currently open)
18 devices running msrpc protocol on port 111	Metasploit RPCbomb exploit tested and found working - attacker could escalate and cause Memory Leaks along with Denial of Service	Filter access to port 111 (currently open)
Cisco SG 300-28 network switch with insecure credentials	Attackers could access this and remotely shut it down easily/cause Denial of Service	Reset credentials and setup strong password

Figure 2. Table of vulnerabilities discovered using Nmap

During our network security audit, we discovered critical vulnerabilities that demand immediate attention. Machines running vulnerable protocols on specific ports pose risks of remote code execution and denial of service attacks. Insecure credentials on a switch and a wireless access point could lead to unauthorized access and network disruptions. Obsolete SSL certificates on certain IPs expose users to potential phishing attacks. Swift action is necessary to implement port filtering, secure credentials, and update SSL certificates to enhance network security.

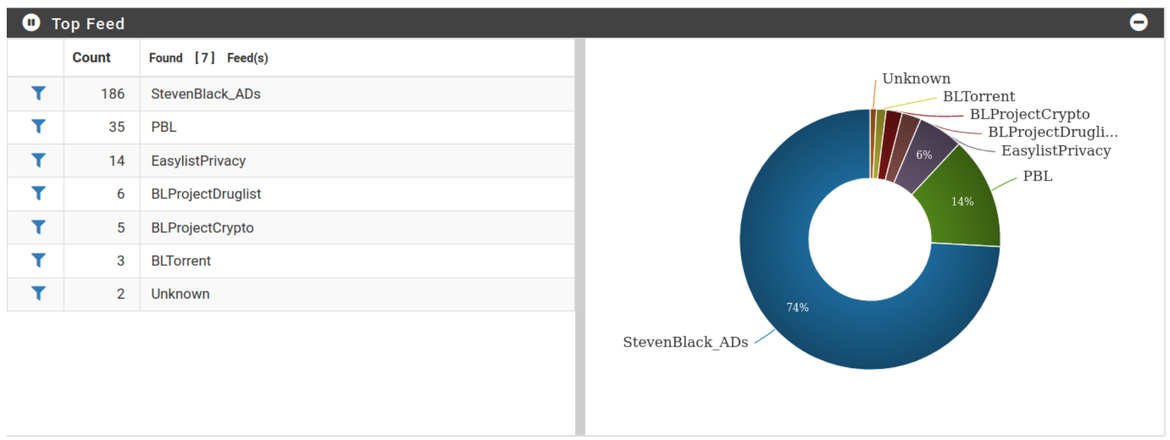

Figure 3. DNSBL Reports

Our implementation of pfBlockerNG, a website blocking solution, proved highly effective in enhancing network security. It successfully blacklisted specified URLs, adding an additional layer of protection to the college campus network. The generated reports in the form of pie charts provided valuable insights into the overall block frequency and distribution of blocked websites across different categories. These visual representations facilitated a clear understanding of the website blocking activities and provided valuable data-driven insights to further strengthen network security measures.

Conclusions

Our network security project at Government Engineering College Barton Hill successfully upgraded the existing network infrastructure by implementing pfSense, which improved network security, reduced costs, and increased operational efficiency. The deployment of pfSense, along with packages like pfBlockerNG, provided effective solutions for protecting the network and enhancing overall security posture. This project resulted in a safer environment for users, financial savings, and an upgraded network architecture with improved resilience and robust security measures.

References

[1] Easha, Farhana Binte Kamrul, Robert Abbas, and Matthew Daley, Campus Wi-Fi Coverage Mapping and Analysis, arXiv preprint arXiv:2004.01561 (2020).

[2] SenthilKumar, P., and M. Muthukumar, A study on firewall system, scheduling and routing using pfsense scheme, 2018 international conference on intelligent computing and communication for smart world (I2C2SW). IEEE, 2018.

[3] Diane Tang and Mary Baker, Analysis of a local-area wireless network, Association for Computing Machinery, New York, NY, USA, 1–10. https://doi.org/10.1145/345910.345912.

[4] Patel, Krupa C., and Priyanka Sharma, A Review paper on pfsense-an Open source firewall introducing with different capabilities customization, IJARIIE3 (2017): 2395-4396.

[1] Btech Undergraduate Student, Department of Information Technology, Government Engineering College, Barton Hill, Trivandrum

[2] Assistant Professor, Department of Information Technology, Government Engineering College, Barton Hill, Trivandrum