Analysis And Audit of Campus Network

A Project Report

Submitted to the APJ Abdul Kalam Technological University

in partial fulfillment of requirements for the award of degree

Bachelor of Technology

in

Information Technology

by

Gowri Arunsha(TRV19IT029)

Sanjay J Prakash(TRV19IT048)

Suryanarayan Menon A(TRV19IT055)

Vinayak Naveen(TRV19IT058)

DEPARTMENT OF INFORMATION TECHNOLOGY

GOVERNMENT ENGINEERING COLLEGE, BARTON HILL,

THIRUVANANTHAPURAM-695035

KERALA

May 2023

DEPARTMENT OF INFORMATION TECHNOLOGY

GOVERNMENT ENGINEERING COLLEGE, BARTON HILL,

THIRUVANANTHAPURAM-695035

2022 - 23

CERTIFICATE

This is to certify that the report entitled **Analysis And Audit of Campus Network** submitted by **Gowri Arunsha** (TRV19IT029), **Sanjay J Prakash** (TRV19IT048), **Suryanarayan Menon A** (TRV19IT055) & **Vinayak Naveen** (TRV19IT058) to the APJ Abdul Kalam Technological University in partial fulfillment of the B.Tech. degree in Information Technology is a bonafide record of the project work carried out by them under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Prof. Josna V R,
(Project Guide),
Assistant Professor,
Department of Information Technology,
Government Engineering College,
Barton Hill, Trivandrum.

Dr. Haripriya A.P.,
(Project Coordinator),
Associate Professor,
Department of Information Technology,
Government Engineering College,
Barton Hill, Trivandrum.

Prof. Manju R.,
(Project Coordinator),
Associate Professor,
Department of Information Technology,
Government Engineering College,
Barton Hill, Trivandrum.

Dr. Vijayanand K. S.,

Professor and Head,
Department of Information Technology,
Government Engineering College,
Barton Hill, Trivandrum.

DECLARATION

We hereby declare that the project report **Analysis And Audit of Campus Network**, submitted for partial fulfillment of the requirements for the award of degree of Bachelor of Technology of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by us under supervision of **Prof. Josna V R**.

This submission represents our ideas in our own words and where ideas or words of others have been included, we have adequately and accurately cited and referenced the original sources.

We also declare that we have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in my submission. We understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Gowri Arunsha
Sanjay J Prakash
Suryanarayan Menon A
Vinayak Naveen

Trivandrum
29th May, 2023

Abstract

An analysis and audit of a campus network involves evaluating the network infrastructure, devices, and configurations to ensure that it is performing optimally and securely. This can involve checking the hardware and software components of the network, evaluating network performance and capacity, and identifying any vulnerabilities or potential issues that may need to be addressed. It can also include reviewing the network's security measures, such as firewalls, access controls, and intrusion detection systems, to ensure that the network is protected against cyber threats. The goal of an analysis and audit of a campus network is to identify any weaknesses or potential issues and to make recommendations for improving the network's performance and security.

There are many tools available for performing the above two processes. As a initial auditory measure, we conducted a preliminary review on the currently existing infrastructure and have constructed detailed network diagrams reflecting the current network infrastructure and have performed vulnerability analysis in order to determine the issues to be tackled. During the campus network security audit, we scanned our network using Nmap, an open source Linux command-line tool. The tool we used to set up security measures in our college network is pfSense, an Open Source firewall programme as it is cost effective and customizable to the college's need. In order to leverage additional features, a pfSense package, pfBlockerNG was installed. The Snort software provided by pfSense was used to construct an Intrusion Detection System(IDS). For analysis of the features implemented, the reports and alerts generated by pfSense was used.

Acknowledgement

We take this opportunity to express our deepest sense of gratitude and sincere thanks to everyone who helped us to complete this work successfully.We express our sincere thanks to **Dr. Vijayanand K.S**, Head of Department, Information Technology, Government Engineering College, Barton Hill, for providing us with all the necessary facilities and support.

We like to express our sincere gratitude to **Dr. Haripriya A.P.** and **Prof. Manju R.**, Department of Information Technology, Government Engineering College, Barton Hill,Trivandrum for their support and co-operation.

We would like to place on record our sincere gratitude to our project guide **Prof. Josna V R**, Assistant Professor, Information Technology, Government Engineering College, Barton Hill, for the guidance and mentorship throughout this work.

Finally we thank our family, and friends who contributed to the successful fulfilment of this project work.

Gowri Arunsha

Sanjay J Prakash

Suryanarayan Menon A

Vinayak Naveen

Contents

List of Figures

Chapter 1

Introduction

The inception of the current network infrastructure in use by Government Engineering College, Barton Hill, Thiruvananthapuram dates back to almost a decade. As the years have gone by, there has been a severe lack of sufficient augmentations and changes to the network architecture, which has led to several inherent issues. Lack of network segregation, lack of access controlling firewall and lack of Intrusion Detection System are just a few of the possible ones currently being faced. It is clear that the current network infrastructure is in need of modernization to conform with current standards of computing and data security.

As its stands, the college's archaic network setup cannot support the growing number of devices and requirements as time goes on. Lack of proper structure has led to numerous security vulnerabilities as well as inefficient traffic routing throughout the network. With this project we aim to update the college's network infrastructure to produce a computing benefit as well as an economic benefit in terms of reduction in spending required for upkeep of existing systems. Our methodology began with a thorough examination of the current network infrastructure, rigorous documentation of the network topology, and identification of any possible vulnerabilities. We used the GNS3 simulator to help in our study, allowing us to create extensive network diagrams that correctly replicated the campus network. Building on this basis, we reinforced our security measures by undertaking network analysis with Kali Linux's powerful Nmap tool. This allowed us to detect open and vulnerable ports, giving us a complete picture

of the network's security posture. We used pfSense, an open-source firewalling tool, that offers a wide range of packages that can enhance its capabilities and improve its functionality. For the campus's network's need, pfBlockerNG has been identified as a suitable package that provides extensive alias table functionality and customized lists through which access control measures were implemented. The system also includes an Intrusion Detection System(IDS) using Snort package in pfSense. The IDS system ensures no suspicious activity goes unmonitored. This helps identify and alert to possible security breaches.

We used an iterative method throughout the network security project, rigorously improving our procedures to assure correctness and efficacy. As we learned more about the network architecture, we updated the network diagrams created using the GNS3 simulator. Several exploits and vulnerabilities were identified during the network investigation phase using Nmap, which were quickly revealed and accompanied by recommended fixes to reduce the risks. We have evaluated pfSense and its packages in a virtual environment before deploying them in the real environment to confirm their performance and compatibility. The favourable findings acquired throughout the testing phase in internal labs gave confidence in the solution's scalability and dependability. All of these stages, as well as the outcomes, have been thoroughly described in this report.

Chapter 2

Literature Review

Yamasaki et al. [1] discusses that conventional VLANs, which are based on the IEEE802.1Q standard, have been widely used in campus-wide Wi-Fi systems to separate access networks from other campus networks and for access control. However, these VLANs have some limitations, including the shortage of VLAN IDs and the high cost of network management. To address these limitations, they have proposed the use of VLANs based on OpenFlow, which enables the easy configuration and management of virtual networks. OpenFlow VLANs allow for the addition of access management functions (AMF), which include databases of virtual group IDs and check functions for the source and destination addresses of packets. AMF can also perform a range of functions, including authentication, reporting, DHCP, access management, and communication. By using OpenFlow VLANs with AMF, it is possible to efficiently manage access and improve the overall performance of a campus-wide Wi-Fi system. Evaluation results of the proposed system showed that the times for authentication and pings were about 10ms longer than the basic OpenFlow controller, but were still considered practical. Overall, the use of OpenFlow in campus networks can enable more flexible and simplified management of VLANs and improve access control.

Xue et al. [2] discusses how Quality of Service(QoS) is an important consideration in campus networks, as it helps to avoid network congestion and maintain normal operation of the network. There are several different service models that can be

deployed to achieve this goal, including the best effort service model, the centralized service model, and the differentiated service model. To implement QoS in a campus network, there are several basic technologies that can be used, including flow classification, flow supervision, flow shaping, congestion management, and congestion avoidance. These technologies work together to ensure that the network is able to handle the demands placed on it and deliver high-quality service to users. This study focused on the use of the differentiated service model to deploy QoS technology in a university network. In this study, the researchers classified the flow at the network layer according to the Differentiated Services Code Point (DSCP) value of the data packet and at the data link layer according to the 802.1p value of the data frame. They then used the srtcm algorithm to supervise and reshape the flow and the PQ + WFQ queue scheduling algorithm to manage network congestion. Finally, they configured the red method to avoid congestion. The results of the study showed that the deployment of QoS technology in the university network led to significant improvements in network parameters such as packet loss rate, jitter, and delay. The network operation efficiency was greatly improved compared to before the transformation, and key network services were given priority.

Patel et al. [3] discusses about pfSense, which is a popular open source firewall and router platform that is based on a customised distribution of FreeBSD. One of the benefits of using pfSense is that it is cost effective and offers stability, making it a good choice for implementing a Unified Threat Management (UTM) system. In the study conducted to evaluate the effectiveness of pfSense in a virtual environment, the researchers used a method called ”whitebox testing” to analyse the system logs generated by pfSense. This method involves examining the internal components of the system to identify any vulnerabilities or weaknesses. To test the security of the pfSense system, the researchers used a number of tools and scripts, including traceroute, tcptraceroute, and the NSE Firewalk script. These tools were used to simulate various types of network attacks and assess the ability of pfSense to detect and disable them. The results of the study showed that the components of the pfSense system worked well together in detecting and disabling network attacks. Overall, the research suggests that pfSense is a reliable and effective platform for implementing UTM and improving the

security of a network.

SenthilKumar et al. [4] discussed the firewall functionality, scheduling features, and routing capabilities of pfSense.The firewall system is located between the concealed network and the Internet which enforces the security access rule by controlling the links to be established between the two or more networks. In every network traffic should pass through the firewall, which allows only acceptable traffic flows. The main purpose of this firewall system is to manage network access to or from a secured network. Some difficulty with the process of firewall system is due to malfunction, it might be terrible to other fewer secured systems on the internal network. They discussed two approaches for implementation. In the first approach by the author, firewall access rule routing and scheduling using the pfSense scheme is employed. The access rules are network security rules that can be set by the network authority to allow traffic to respective web servers. Their proposed system initially realizes the available information and services. The evaluation is done with the help of scheduling in the time interval. While comparing with the existing approach the range can be calculated with the 95% of latency. In the second approach, experiment evaluation showed that the proposed method has the capability of perceiving a movement percentage of new attacks. It explains that the system detection can be developed by using Similarity Index Algorithm. The Similarity Index Algorithm analyzes the inward packets recognized using malignant packet detection and decides to precede packets through the gateway. The result demonstrates the gateway operation can be turned on by investigating each packet.

Easha et al. [5] addresses issue that poor coverage areas for mobile networks are common on many campuses, and as a result, the ability of the wireless network to supplement Internet access for mobile devices in these areas becomes increasingly important. To provide a better wireless service, it is important to understand WLAN traffic patterns, network handovers between access points, and inter-network handovers between WiFi and mobile networks. To achieve this understanding and optimize the placement of networking equipment, researchers have focused on wireless measurements as a way to identify locations on campus where the current WiFi

network requires improvement. By collecting and analyzing these measurements, it is possible to recommend performance improvements based on AP performance testing, taking into account cabling length limitations and physical and aesthetic placement restrictions. Overall, the use of wireless measurements and analysis can help to improve the coverage and performance of WiFi networks on campus.

Tang et al. [6] analyzed the network for overall user behavior. The overall network traffic, load characteristics, and traffic throughput characteristics from a user point of view were also taken into consideration. During this analysis, they used Rivet to create interactive visualizations quickly for exploring the data. By using an interactive visualization to explore the data, they were able to spot unexpected trends, such as the division of users into sub-communities and the lease times being too short. Results are only valid for this local-area wireless network, but similar environments may exhibit similar behavior and trends. User association patterns in such large-scale systems had not been well investigated, which is crucial for performance enhancement and intelligent system management.The analysis can be broken down into sub-committees, each with its unique behavior regarding how much users move, when users are active (daily, weekly, and throughout the trace), and how much traffic the users generate. They found that although web-surfing and session applications such as ssh and telnet are the most popular applications overall, different users do use different sets of applications at different times and connect to different numbers of hosts. When incoming traffic dominates outgoing overall traffic, the opposite tends to be true during periods of peak throughput, implying that significant asymmetry in network capacity could be undesirable for the users. The asymmetric links would likely be unacceptable in this type of wireless network, and that optimizing packet processing is just as important as optimizing overall throughput.

Chapter 3

System Development

3.1 Proposed System

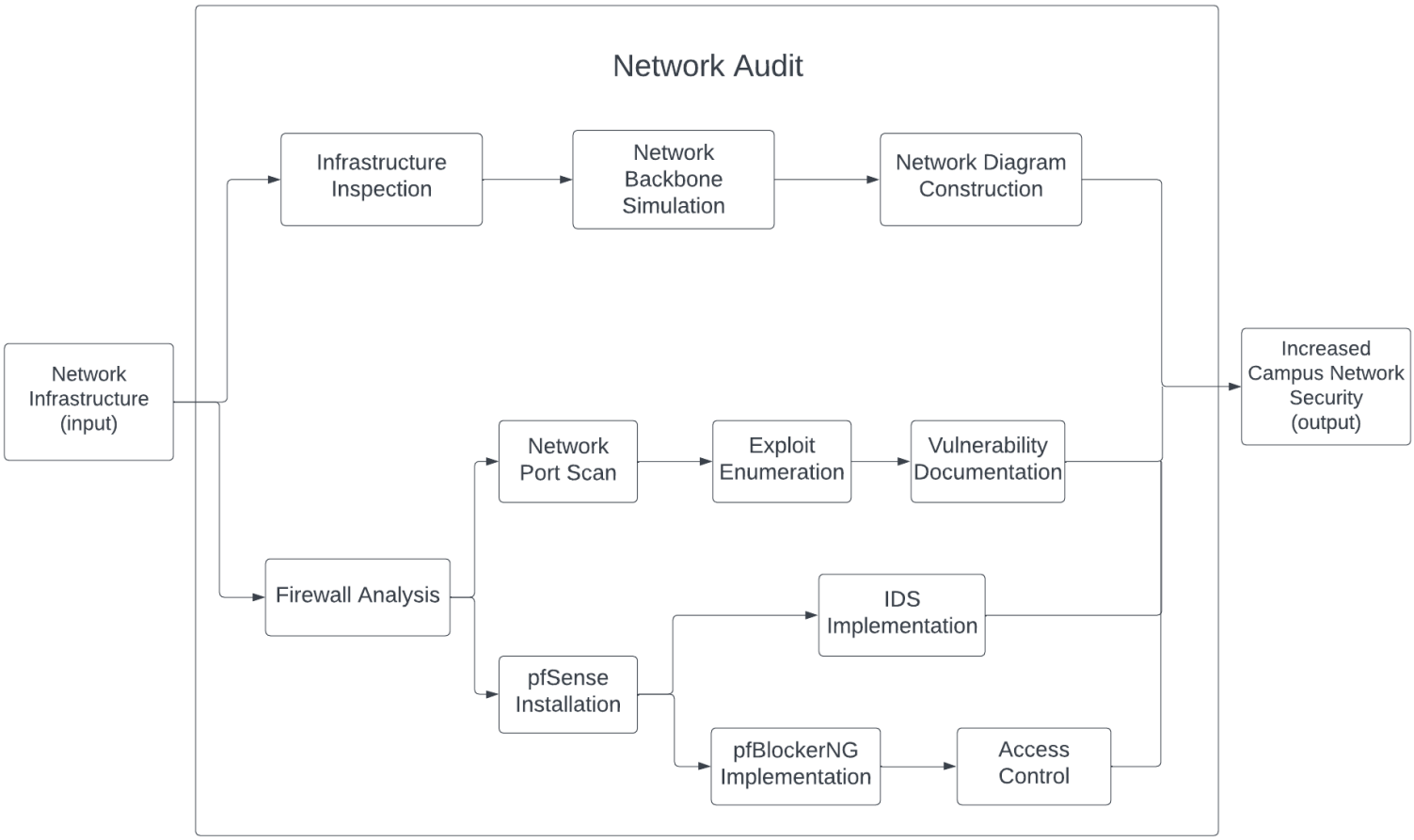


Figure 3.1: Project Block Diagram

3.1.1 Network Infrastructure (Input)

Network infrastructure on a college campus refers to the interconnected equipment and technology that enable communication and data transmission. It consists of the network backbone that connects buildings and facilities, wired and wireless infrastructure for device connection, network security measures, critical services like as email and file storage, internet connectivity, and network management tools. The network infrastructure enables students, professors, staff, and administration to communicate, collaborate, and access resources throughout campus.

3.1.2 Infrastructure Inspection

In order to improve network security, it was critical to inspect the network infrastructure around the college campus. This complete evaluation includes a thorough examination of numerous components such as routers, switches, firewalls, access points, and cabling infrastructure. Through this inspection we performed an exhaustive trace of each access point, its source and pathways taken by switch cables. It also entailed inspecting the physical security of these devices, such as making sure they are securely installed and not accessible to unauthorised personnel. In addition, checking the network architecture entailed determining the appropriateness of network segmentation, analysing traffic patterns, and finding any vulnerabilities or misconfigurations that may jeopardise the campus network's security. Through this we were able to detect flaws, plan necessary repair steps, and protect the network against possible security threats.

3.1.3 Network Backbone Simulation

Simulating the network backbone in a block diagram style proved an excellent method for visualising and comprehending a college campus's network infrastructure. The block diagram depicted the network components, their interconnections, and data flow at a high level. The network backbone is comprised of routers and switches responsible for routing and forwarding traffic throughout campus. Various network segments representing various locations or departments inside the college were connected to

the backbone. By modelling the network in this manner, it became simpler to detect possible bottlenecks, single points of failure, and security vulnerabilities, allowing for improved network security planning and decision-making.

3.1.4 Network Diagram Construction

As our team walked throughout campus, we mapped out the access points and their sources to create a network diagram. We detected the locations of the access points and tracked their connections to the appropriate network switches or routers. Each access point was depicted on the diagram as a node, along with its unique identity. The graphic also showed the linkages between the access points and the network architecture, as well as the physical channels that data was transported via. We obtained a thorough grasp of the campus network's wireless coverage and connection by graphically depicting the access points and their sources in the network diagram. This data would be important for planning network security improvements, optimising network performance, and guaranteeing proper campus coverage.

3.1.5 Firewall Analysis

We uncovered multiple vulnerabilities and recognised obsolete firmware as a major risk after analysing the firewall. However, given the expensive expense of replacing the firewall (15 lakh INR), we chose an alternate method. Instead of purchasing a new firewall, we chose to investigate the use of open source software to fix firewall vulnerabilities and upgrade the firmware. This method provided various benefits, including cost-effectiveness by avoiding costly proprietary licences. Furthermore, open source software allowed us to tailor the firewall setup to our individual requirements. Furthermore, open source software's active developer community assured regular upgrades and security patches. We achieved our aim of improving network security at a low cost by utilising open source technologies.

3.1.6 Network Port Scan

We used Nmap on Kali Linux to do a network port scan on ten subnets in the college network. Nmap, a sophisticated open-source tool, enabled us to inspect the target subnets in detail and detect any exposed or possibly susceptible ports. We started the port scan by entering the IP ranges of the subnets in the Nmap command, which probed each host inside the subnets for open ports and accompanying services. The results gave us significant information about the network's security posture, such as potential vulnerabilities or misconfigurations that attackers may exploit. This scan assisted us in prioritising security measures and addressing the open ports discovered, resulting in a more robust and secure network environment for the college campus.

3.1.7 Exploit Enumeration

Following a thorough port scan using Nmap that revealed open ports and vulnerable protocols, our next step was to identify potential exploits related with these discoveries. We used a variety of venues to collect useful data while keeping the individual context and vulnerability information in mind. We found known vulnerabilities associated with the reported open ports and protocols by cross-referencing the port scan results with vulnerability databases such as the NVD and CVE. This allowed us to uncover particular vulnerabilities that attackers may use to hack the system. Furthermore, we dug deep into security forums, mailing lists, and exploit databases, where we gleaned vital information about reported or found exploits in the security community. The goal of this enumeration was to analyse the security risks associated with the found vulnerabilities and prioritise remedial actions to improve the college campus's overall network security posture.

3.1.8 Vulnerability Documentation

To record the vulnerabilities we uncovered, we used standard documentation procedures. We made every effort to give clear and straightforward information on each vulnerability, such as its name, description, and possible impact on the network. We also documented which systems or software versions were impacted. We

outlined in simple terms how attackers may exploit these vulnerabilities and gave basic remedial instructions. Our literature contained directions on how to apply patches, update software, configure security settings, and contact IT help. We kept a simple vulnerability journal to keep track of our findings and progress. We were able to improve the security of our college campus network by implementing these documenting practises, which allowed us to prioritise and resolve the detected vulnerabilities.

3.1.9 pfSense Installation

We chose to install pfSense, an open-source firewalling programme, as part of our college campus network security initiative. We took advantage of the benefits of an economical and configurable network security solution by selecting pfSense. pfSense installation entailed either a dedicated hardware device or a virtual machine with the pfSense software. We followed the pfSense community's installation instructions, which walked us through the process of creating network interfaces, defining firewall rules, and applying security measures. We acquired control over traffic filtering, network segmentation, and VPN capabilities after installing pfSense. We were able to increase our network security defences while keeping expenses under control thanks to this open-source firewalling solution.

3.1.10 pfBlockerNG Implementation

In order to improve website blacklisting capabilities, we resorted to pfBlockerNG, a useful pfSense package known for its remarkable extended alias table functionality. This feature provides powerful features designed primarily for efficiently blacklisting websites. We can easily import and maintain a wide range of blacklists using pfBlockerNG, including those linked with dangerous domains and phishing sites. What distinguishes pfBlockerNG is its ability to generate customised lists that meet our specific needs. We keep granular control over our blacklisting approach by utilising this functionality, allowing us to ban whole domains, individual IP addresses, or even regions and nations. pfBlockerNG's upgraded alias table capability enables us to proactively protect our college campus network by effectively and efficiently restricting

access to websites that pose potential risks or threats.

3.1.11 Access Control

We were able to effectively deploy access control measures by combining pfBlockerNG's blacklisting capability with pfSense, an open-source firewalling application. This strategy enables us to improve network security while remaining within our resource constraints. We imported and managed a comprehensive library of known malicious domains, phishing sites, and unpleasant websites using pfBlockerNG's blacklists, ensuring that our access control methods were up to date with the current threats. We were able to be proactive in reducing developing dangers thanks to regular updates to these blacklists. We were able to adjust our access control rules to our unique needs by using pfBlockerNG's expanded alias table capability, which allowed us to ban access to whole domains, certain IP addresses, or even regions and countries. This degree of granularity enabled us to impose stringent security measures while maintaining network performance. The incorporation of pfBlockerNG's blacklisting functionality into our network infrastructure enabled us to proactively prevent access to potentially harmful websites, strengthening our defences against cyber threats and fostering a secure digital environment for our college community. We produced a cost-effective and efficient solution that considerably reinforced the network security of our college campus by efficiently using pfSense as our open-source firewalling technology and applying access control mechanisms with pfBlockerNG.

3.1.12 IDS Implementation

We opted to use the Snort software within pfSense to construct an Intrusion Detection System (IDS). This decision enabled us to improve the security of our network by continually monitoring and identifying any intrusions and harmful actions. We obtained real-time visibility into network traffic and received notifications anytime Snort recognised possible risks or malicious activity by implementing it. The Snort programme supplied us with a number of capabilities, like as packet sniffing, protocol analysis, and signature-based detection, which enabled us to identify and respond to many forms of network-based assaults. We increased the resiliency of our network

against attacks and dramatically improved our incident response capabilities by integrating Snort into pfSense. Snort enables us to take proactive security steps by identifying and alerting us to possible security breaches.

3.2 Technologies Used

The following technologies were used throughout our project from ideation to implementation stages:

3.2.1 Graphical Network Simulator-3 (GNS3)

To develop virtualized network environments for testing and analysis, we used GNS3 as a network simulator. GNS3 enabled us to build and install complicated network topologies, duplicate our college campus network, and test various security measures in a controlled environment. We were able to imitate network devices, simulate traffic flows, and evaluate the performance and efficacy of our suggested security solutions using GNS3. Before deploying changes in the live network, we were able to evaluate our network security designs, fine-tune configurations, and obtain useful insights into possible vulnerabilities. The usage of GNS3 as a network simulator substantially aided the success of our project by allowing for rigorous testing, improving our understanding of network security, and allowing us to construct a strong and secure network architecture.

3.2.2 pfSense - Free and open source firewall

As an open-source solution, pfSense supplied us with several capabilities and customization possibilities to strengthen our network security. We used the strength of pfSense as an open-source firewall tool and extended its capabilities by integrating the pfBlockerNG package for managing multiple blacklists and Snort as an intrusion detection system. We used the pfBlockerNG programme to create curated blacklists customised to our unique needs, preventing access to known dangerous websites and material. This proactive strategy assisted us in mitigating possible security issues and strengthening the resilience of our network. Furthermore, we effortlessly incorporated

Snort as an IDS package into pfSense, allowing for real-time monitoring and detection of suspicious activity. Snort's strong intrusion detection capabilities, which are based on signature-based analysis, enabled us to quickly identify and respond to many forms of network-based attacks. We constructed a complete security architecture that enabled proactive threat prevention, real-time monitoring, and quick reaction capabilities by integrating the benefits of pfSense, pfBlockerNG, and Snort. This integration dramatically increased the security of our network, guaranteeing a safe and secure environment for our college campus.

3.2.3 NMap - Network Mapper

Nmap was used as a strong tool for port scanning. We were able to scan the network using Nmap and detect open ports on various devices and systems. We acquired vital insights into the network's weaknesses by doing Nmap scans, which helped us identify potential entry points for attackers. Nmap's vast variety of scanning techniques and advanced capabilities enabled us to execute comprehensive scans on several subnets, allowing us to identify possible security flaws throughout the campus network. We may prioritise security measures, resolve open ports, and boost the network's defences by exploiting Nmap's port scanning capabilities. Nmap was critical to our network security approach, allowing us to proactively discover and remediate vulnerabilities.

3.2.4 Kali Linux toolset

We used the Kali Linux toolbox extensively in our college campus network security project, including the sophisticated Metasploit framework. As a specialised penetration testing platform, Kali Linux supplied us with a complete set of tools and resources to evaluate the security of our network architecture. As part of the Kali Linux toolbox, Metasploit provided a large choice of exploits, payloads, and auxiliary modules, allowing us to mimic real-world assaults and detect possible weaknesses in our network. We used Metasploit to conduct controlled penetration tests to analyse the efficiency of our network defences and the resilience of our system against common attack vectors. This enabled us to proactively detect and solve security weaknesses, ensuring that suitable security measures to secure our college were implemented.

Chapter 4

Implementation

4.1 Initial Inspection

We used a methodical strategy to improve network security in our project. The first stage entailed evaluating the current network architecture in order to obtain a thorough grasp of how all of the components interrelated. To map all the settings and connections of switches, routers, firewalls, and other networking equipment, we meticulously inspected them. This first evaluation allowed us to identify possible points of vulnerability and areas that needed to be investigated further. It was during this initial inspection that we recognized the outdated firmware used by the SOPHOS XG 210 module that was being used at the time. After discussions with department staff, we were told that the existing plan was to replace this module with a new one which would incur a cost of 15 Lakh INR to the college. It was during these discussions that the idea of using open source software in place of an expensive proprietary licensed model came up. We decided on ideating with pfSense, a firewall/router computer software distribution based on FreeBSD.

We chose to graphically describe the network backbone and its capabilities in a block diagram manner to acquire a better understanding of it. We were able to visualise the network topology, simulate traffic flows, and test various security measures in a controlled environment by virtually reproducing the network architecture. This model takes into account the utilisation of pfSense in place of the outdated SOPHOS XG 210 module.

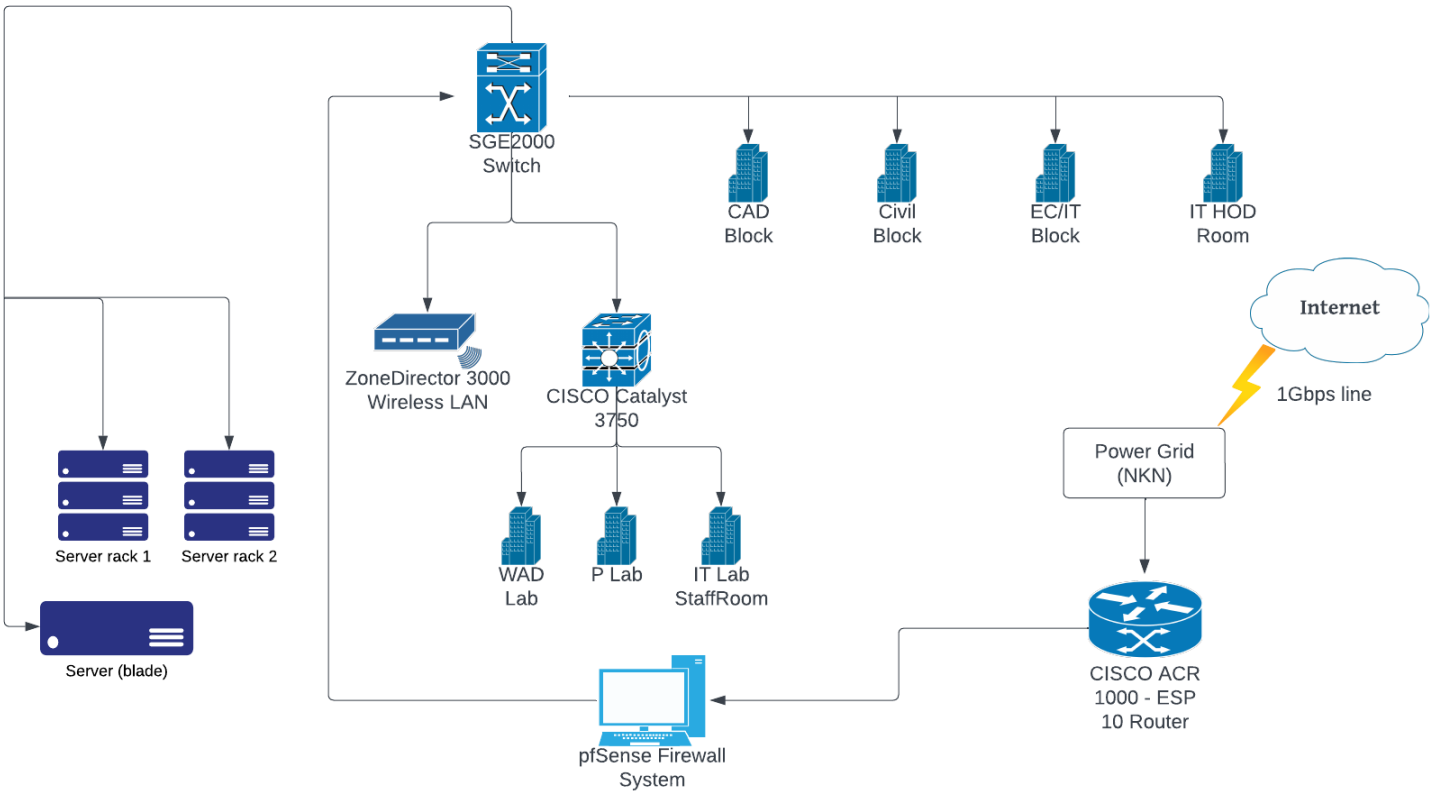


Figure 4.1: Network Architecture Block Diagram

Following this, we made the strategic choice to map the whole network architecture and access points using GNS3 simulations in order to comprehensively examine the network security of the college campus and detect potential weaknesses. We were able to develop virtual representations of the network, recreating its structure and components within a simulated environment, thanks to our method. We were able to analyse the network structure, identify access points, and spot any existing issues by doing so.

To complete this assignment, our team conducted a thorough walkthrough of the college campus, precisely recording the position and features of each access point. We investigated numerous sorts of access points, such as Wi-Fi routers, switches, and Ethernet ports. We also paid particular attention to any visible flaws, such as misconfigurations, obsolete firmware, or physical vulnerabilities, that might jeopardise network security. We have enumerated on the results of this inspection in the next chapter.

4.2 Network Penetration Testing

We used the Kali Linux toolbox to conduct vulnerability assessments and discover possible network weaknesses as part of our overall network security upgrade project for the college campus. Our initial goal was to map the network topology and identify any open or vulnerable ports using Nmap, a robust network scanning tool. We ran extensive port scans across the college campus network using Nmap, allowing us to identify services and apps operating on various servers. We learned a lot about the network's vulnerability and potential attack vectors by looking at the open ports.

We detected a vulnerability linked with the RPCbind service during the scanning procedure. RPCbind is a frequently used network service that supports remote procedure calls (RPC). We concluded that the vulnerability might possibly be exploited to conduct a Denial of Service (DoS) attack through in-depth research and subsequent study. We used Metasploit, a well-known penetration testing platform, to investigate this vulnerability further and analyse its possible effect. On this note, the rpcbomb module in the Metasploit framework was used to precisely target the discovered vulnerability in RPCbind. This module enabled us to simulate and analyse the possible effect of a vulnerability-based assault. Furthermore, we discovered several devices in the network using insecure administrator credentials, which could be easily overtaken by an attacker who could cause Denial of Service (DOS) attacks. There were also IPs in the network running HTTP services with outdated SSL certificates. These observations are shown in the next chapter

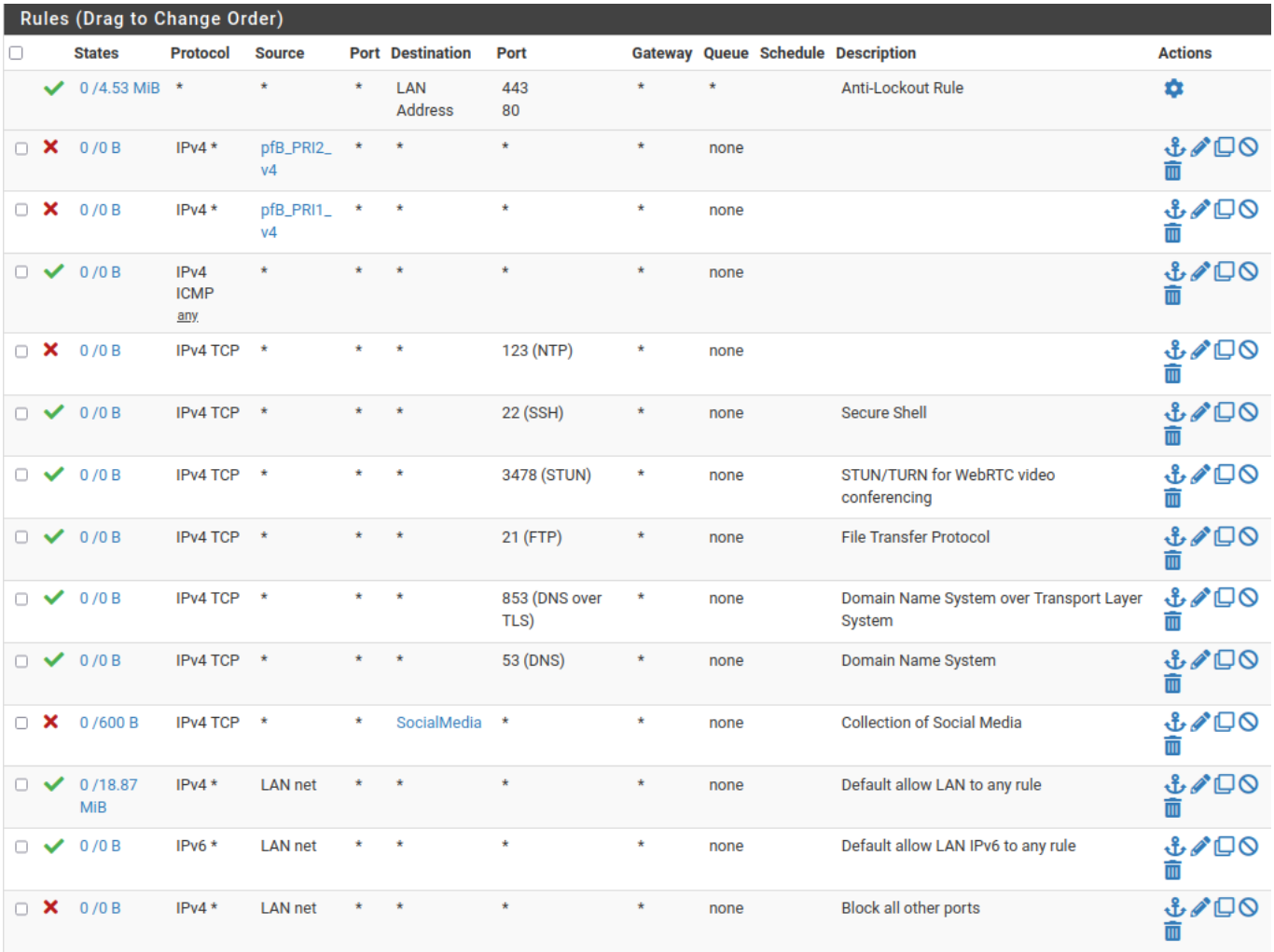
4.3 pfSense Implementation

We began by assessing the security demands of our campus network, reviewing our current firewall infrastructure, identifying its shortcomings, and establishing the specifications for the new solution. After the evaluation, we developed a detailed plan for the pfSense implementation. This plan outlined our specific goals, objectives, and the deployment schedule. After an initial testing phase with running pfSense on a virtual machine environment, we proceeded with the installation of the pfSense software onto dedicated hardware which involved downloading the pfSense image,

creating installation media, and booting the system from the installation media and configured the network interfaces during the installation process to ensure connectivity. Once pfSense was successfully installed we began configuring it through the web based pfSense administration interface.

We built a thorough set of rules to regulate inbound and outgoing traffic with an emphasis on safeguarding LAN connections. This included setting up open rules for protocols like SSH to enable safe remote network access, allowing authorised users to connect to network equipment remotely. We also established STUN/TURN rules to facilitate real-time communication apps and FTP for secure file transfers between services and devices running on the network.

Additionally, designed DNS/TLS traffic rules to support appropriate name resolution and secure DNS communication, guaranteeing that domain requests and answers are encrypted and secured. Furthermore, we implemented HTTP/HTTPS firewall rules to allow online browsing while maintaining the safe transfer of website content. We created particular rules to prohibit connections to social media networks in order to achieve a balance between network utilisation and security. This was done by using the alias feature to create an alias called SocialMedia that contained Fully Qualified Domain Names (FQDNs) for websites like Facebook, Instagram, WhatsApp and Youtube. Finally, we also included two rules using aliases for primary and secondary pfBlockerNG blocklists PR1 and PR2 which we have discussed in the next section. The cumulative rule table is shown in Figure 4.2. Thes strategy aims to boost productivity while lowering possible security threats related with social media use on the college network.



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /4.53 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✗	0 /0 B	IPv4 *	pfB_PRI2_v4	*	*	*	*	none			
✗	0 /0 B	IPv4 *	pfB_PRI1_v4	*	*	*	*	none			
✓	0 /0 B	IPv4 ICMP any	*	*	*	*	*	none			
✗	0 /0 B	IPv4 TCP	*	*	*	123 (NTP)	*	none			
✓	0 /0 B	IPv4 TCP	*	*	*	22 (SSH)	*	none		Secure Shell	
✓	0 /0 B	IPv4 TCP	*	*	*	3478 (STUN)	*	none		STUN/TURN for WebRTC video conferencing	
✓	0 /0 B	IPv4 TCP	*	*	*	21 (FTP)	*	none		File Transfer Protocol	
✓	0 /0 B	IPv4 TCP	*	*	*	853 (DNS over TLS)	*	none		Domain Name System over Transport Layer System	
✓	0 /0 B	IPv4 TCP	*	*	*	53 (DNS)	*	none		Domain Name System	
✗	0 /600 B	IPv4 TCP	*	*	SocialMedia	*	*	none		Collection of Social Media	
✓	0 /18.87 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	
✗	0 /0 B	IPv4 *	LAN net	*	*	*	*	none		Block all other ports	

Figure 4.2: pfSense Firewall Rules

4.4 pfBlockerNG Implementation

To improve the security of the campus network, pfBlockerNG was integrated into pfSense to give advanced filtering features. The sophisticated software pfBlockerNG allows traffic to be blocked depending on many criteria such as IP addresses, domains, countries, and more. In the general settings, we determined the update frequency for the blocklists and configured the logging option. Then we configured the IP Blocklist settings, giving us the choice of selecting from a variety of publically available blocklists or creating custom blocklists specifically tailored to the needs of the campus network. Furthermore, DNSBL (DNS Blocklist) settings in pfBlockerNG were customised to prevent DNS resolution for undesirable or malicious domains. To further strengthen the network's security, blocklists such as StevenBlack's porn blocklist,

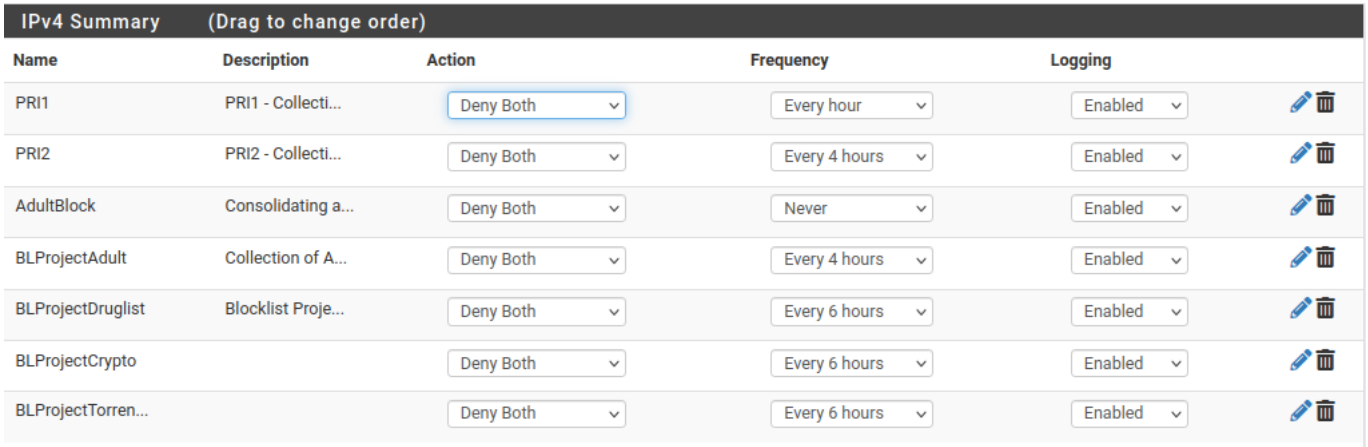


Figure 4.3: pfBlockerNG Blacklists

EasyList's Adblock list, BlockList project's list of adult sites, drug vendors/adverts, torrent domains, crypto vendors/providers were manually added. Thorough testing was done to verify pfBlockerNG's effectiveness. We accessed known blocked domains, performed vulnerability scans, and made attempts to access blocked IP addresses, to ensure appropriate blocking actions were taking place and unwanted or malicious traffic was effectively filtered. Throughout the implementation process, we documented the configuration steps and captured relevant screenshots or examples. A summary of the blocklists implemented with pfBockerNG along with their source is shown in Figure 4.4 and Figure 4.5.

NAME	SOURCE	DESCRIPTION
PR1	Talos Intelligence SPAMHAUS Project Feodo Tracker SSL Blacklist CINS Army Firehol Project	Collection of Feeds from the most reputable blocklist providers. (Primary tier)
PR2	AlienVault	Collection of Feeds from Secondary Tier providers
ADULTBLOCK	StevenBlack	StevenBlack's Porn blocklist
ADS_BASIC	StevenBlack	StevenBlack's basic Ad-blocklist
EASYLIST	EasyList	Privacy and AdBlock

Figure 4.4: Blocklist Groups

NAME	SOURCE	DESCRIPTION
BLPROJECTADULT	Blocklist Project	Blocklist Project's list of adult sites
BLPROJECTDRUGLIST	Blocklist Project	Blocklist Project's list of possible drug vendors/adverts
BLPROJECTTORRENTBLOCK	Blocklist Project	BLProject's list of torrent domains for illegal downloads
BLPROJECTCRYPTO	Blocklist Project	BLProject's list of crypto vendors/providers

Figure 4.5: Blocklist Groups

4.5 IDS Implementation

We understood the significance of having a strong intrusion detection system to monitor and safeguard our network from any security risks.After doing some research and evaluating different options, we opted to use Snort IDS due to its reputation as a strong and dependable open-source solution. For the installation, within in the pfSense web interface we navigated to the Packet Manager and searched for Snort, then installed the package onto our pfSense firewall. After the installation, we proceeded with the configuration of Snort and enabled the appropriate rule sets to detect different types of network intrusions and attacks. These rule sets address a variety of known threats and vulnerabilities. We also set Snort to log all detected events, including alerts and packet captures, for later study. To validate the effectiveness of Snort IDS, we performed an ICMP flood attack and monitored Snort's response to verify its detection capabilities. With the successful implementation of Snort IDS in pfSense, our campus network gained an additional layer of security.

Chapter 5

Results and Discussion

5.1 College Network Diagram

We started mapping our college network by taking a complete inventory of our network devices, which included switches, routers, access points, and endpoints and identified the physical location of these devices and other relevant information. We then created a network diagram to illustrate the general layout of our college network. We used gns3 software to visually represent the network devices and their interconnections. This diagram provided a clear understanding of the network topology.

5.1.1 Main Block Network

From the main switch, SGE2000, three connections lead to different areas within the main building: the ITHoD room, the office and the library. A direct connection extends from SGE2000 to the ITHoD room, this connection provides network connectivity for the devices within the ITHoD room, the classrooms from the second floor to the fifth floor and the staff rooms in these floors. Another connection from the SGE2000 switch reaches the office area. This connection provides network access to office devices such as desktop computers, printers, and other networked resources, as well as to the principal's room and the CA room. A connection extends from the CA room to the Girl's hostel, 2001, 200B1 rooms. Lastly, a connection extends from the SGE2000 switch to the library. This connection enables network connectivity to the devices in the library, ground floor classrooms and the IT staff room.

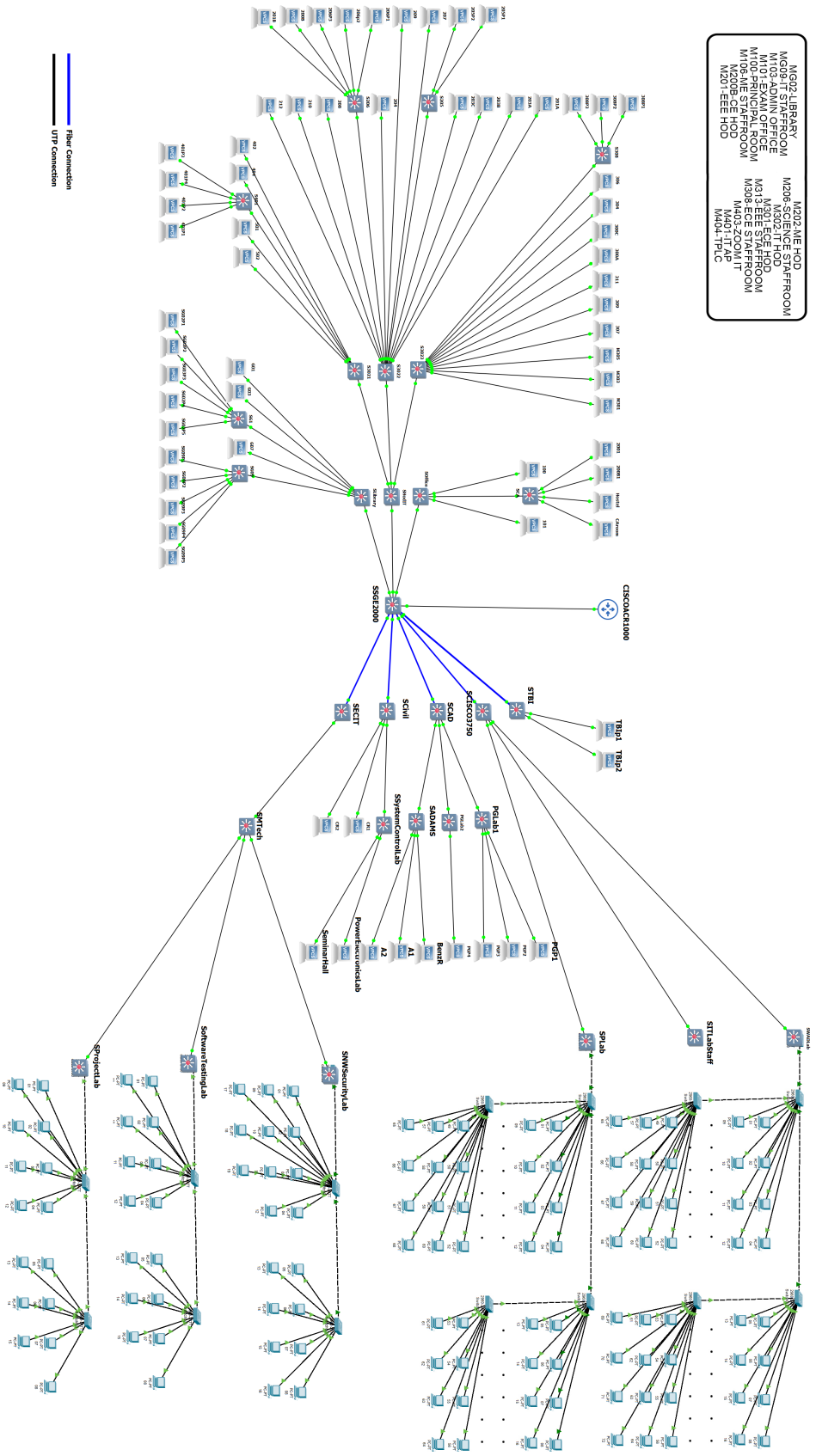


Figure 5.1: College Network Simulated in GNS3

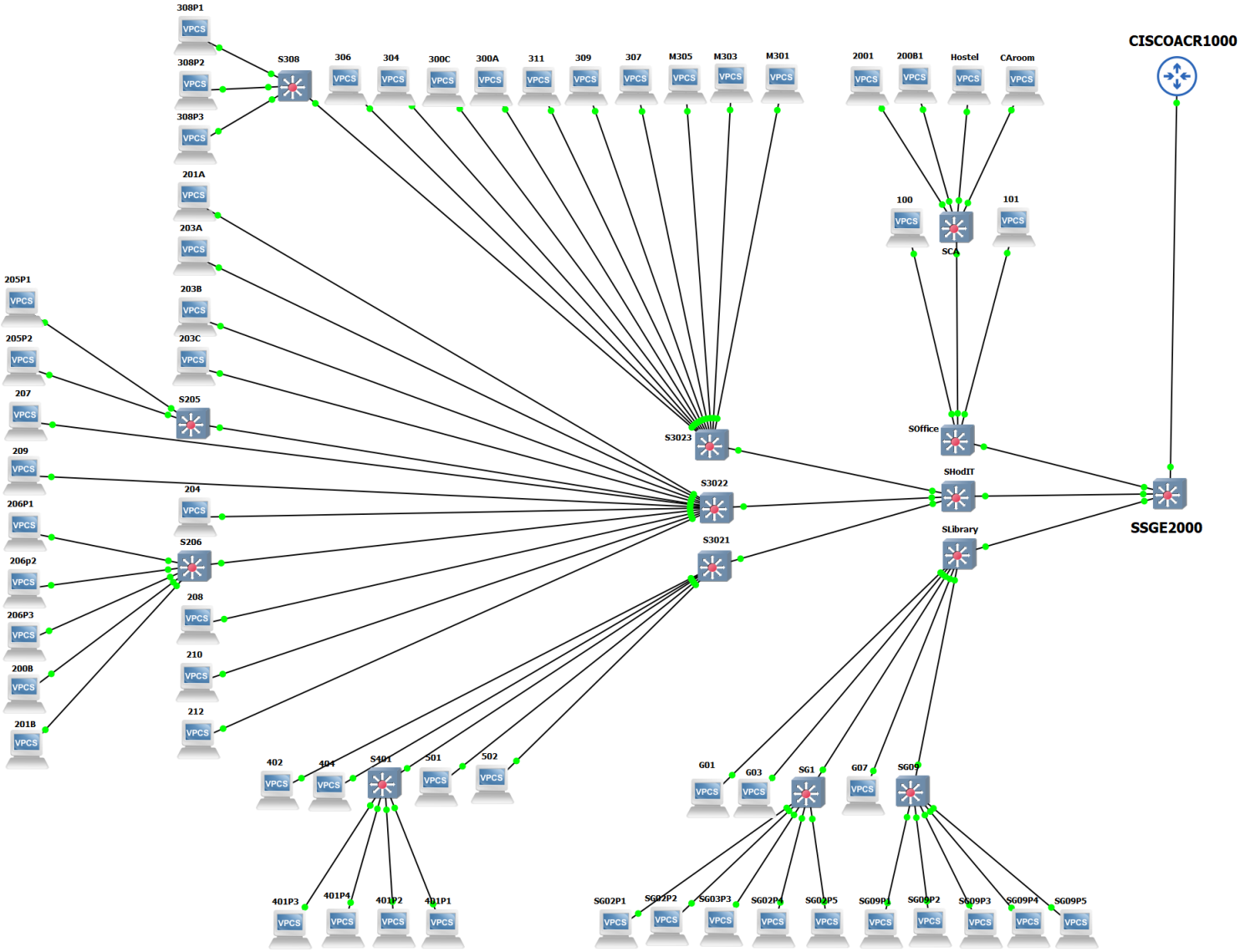


Figure 5.2: Main Block Network Simulated in GNS3

5.1.2 EC-IT Block Network

From the main switch, SGE2000, a connection leads to a CISCO3750 swicth and from there it branches to the WAD Lab, Programming Lab and the IT Lab staff room. In both the WAD lab and Programming lab, there are four switches from which connections to the computers in the lab are made. Another connection from the main switch, SGE2000, reaches the Mtech Staff room, from where it extends to the Network Security Lab, Software Testing Lab and the Project Lab. There are two switches in each of these labs that offer network connectivity to all of the computers there.

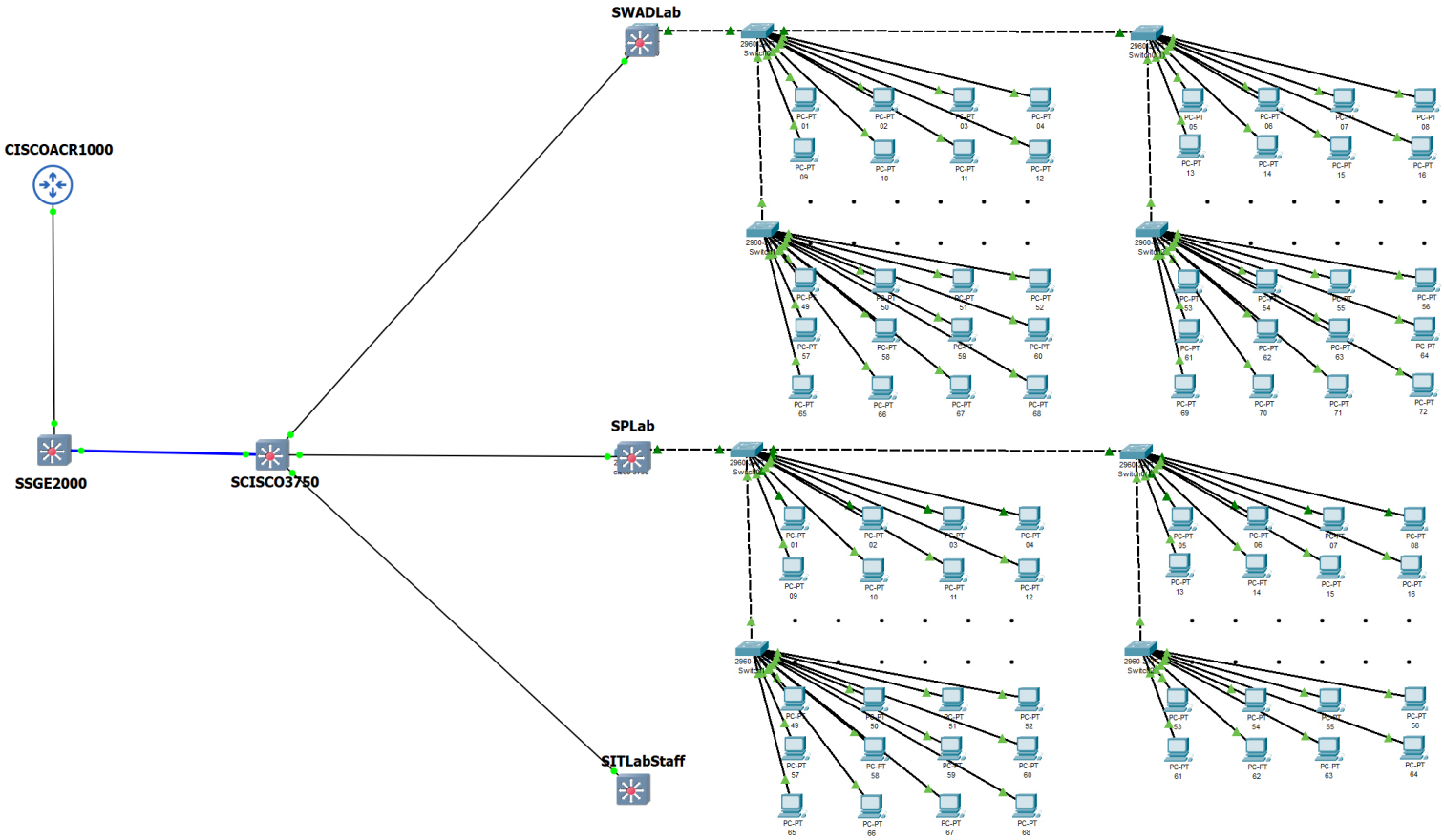


Figure 5.3: EC-IT Block Ground Floor Network Simulated in GNS3

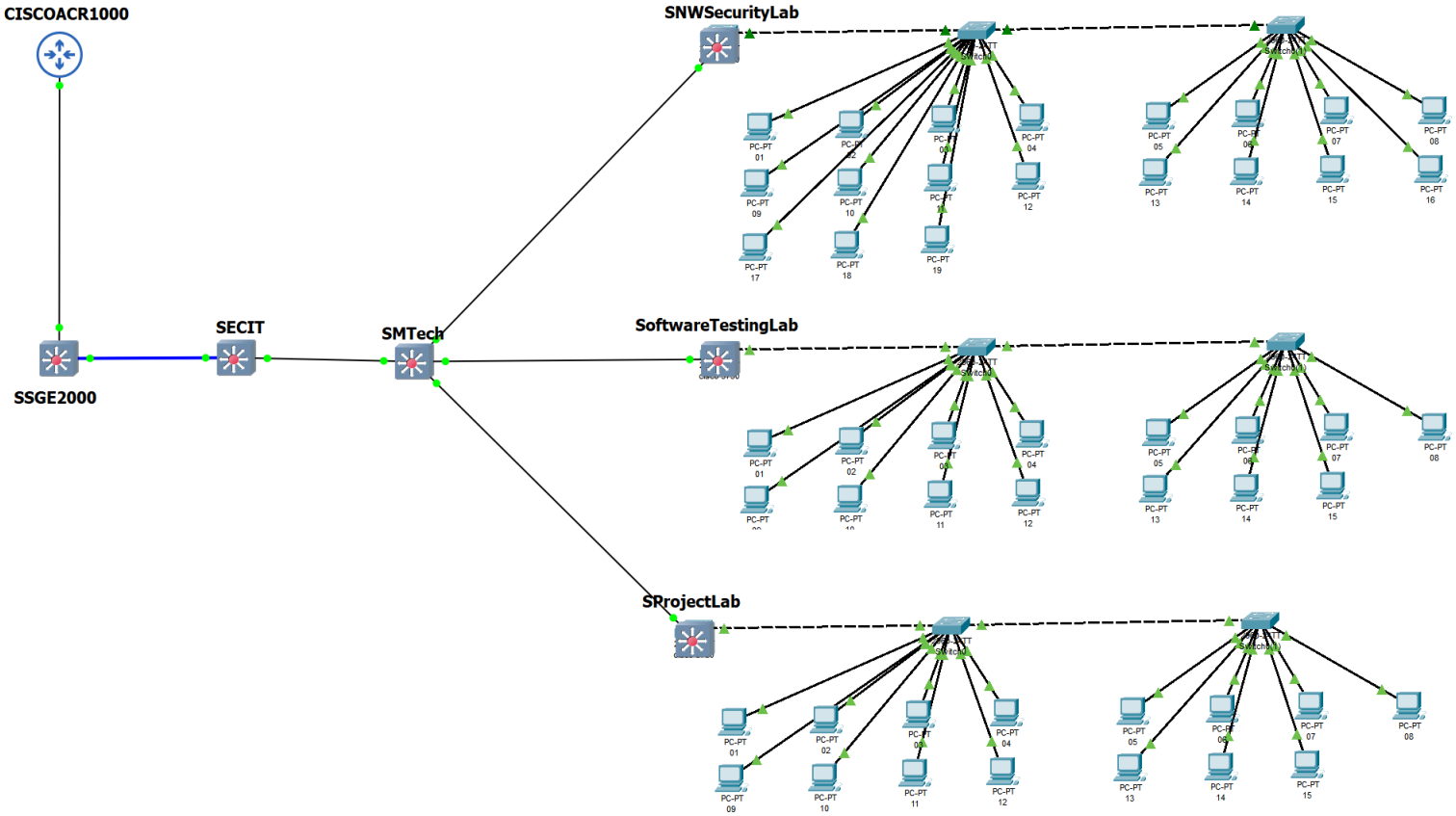


Figure 5.4: ECIT Block Top Floor Network Simulated in GNS3

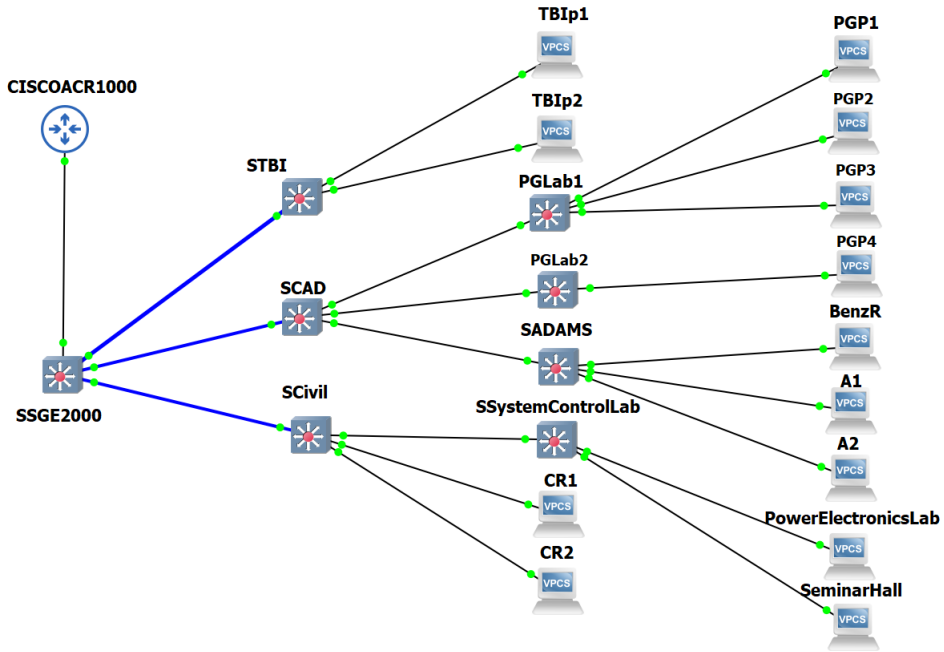


Figure 5.5: TBI, CAD, Civil Block Network Simulated in GNS3

5.1.3 TBI, CAD and Civil Block Network

From the main switch, SGE2000, connections lead to the switches in the three buildings: the TBI block, the Civil block and the CAD block. The switch in Civil Block leads the switch in System Control Lab which in turn extends connections to the Power Electronics Lab and the Seminar Hall. The CAD block switches branch to three switches in PGLab1, PGLab2 and ADAMS. The switch in TBI block provides connection to the two ports in TBI block.

5.2 Network Analysis Results

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 5.6: Table of vulnerabilities discovered using Nmap

During our network security audit, we detected 11 machines on the college campus network executing the rpcbind protocol on port 135. This discovery generated concerns since the rpcbind protocol is known to include flaws that might lead to Remote Code Execution (RCE) attacks. To combat this, we recommended filtering port access so that incoming packets are analysed to ensure that malicious packets are not broadcast.

Similarly, we detected 18 machines on the college campus network running the msrpc protocol on port 111. This discovery prompted serious concerns because the

Problem	Description	Solution
D-Link DAP-1360 wireless access point with insecure credentials	Attackers could access this and remotely shut it down easily/cause Denial of Service	Reset credentials and setup strong password
Outdated certificates	Certain IPs use outdated certificates - can lead to MitM, certificate spoof or phishing attacks.	Update SSL certificates regularly
3 printer devices with insecure credentials	Attackers could remotely disconnect or perform Denial of Service on these devices	Reset credentials and setup strong password

Figure 5.7: Table of vulnerabilities discovered using Nmap

msrpc protocol is known to contain vulnerabilities that might be used for malevolent reasons. We did testing with the Metasploit framework and especially the rpcbomb exploit to assess the possible impact of these vulnerabilities. This test validated the exploit's success, emphasising the danger of a prospective attacker exploiting this vulnerability to cause memory leaks and conduct Denial of Service (DoS) attacks against the vulnerable devices. Again, we have recommended filtering port access to port 111.

Within the college campus network, we discovered a Cisco SG 300-28 network switch with unsecured credentials. This revelation raised serious concerns since it exposed the switch to unauthorised access, allowing an attacker to remotely shut it down and generate a Denial of Service (DoS) problem. In addition, we discovered a vulnerable D-Link DAP 1360 wireless access point on the college campus network. This same trend was also seen with three printer devices being used in the network. This finding highlighted serious concerns since it exposed the devices to unauthorised access, potentially allowing an attacker to compromise the device and impair wireless network communication. We also found IP addresses providing HTTP services were utilising obsolete SSL certificates. This generated worries about the security

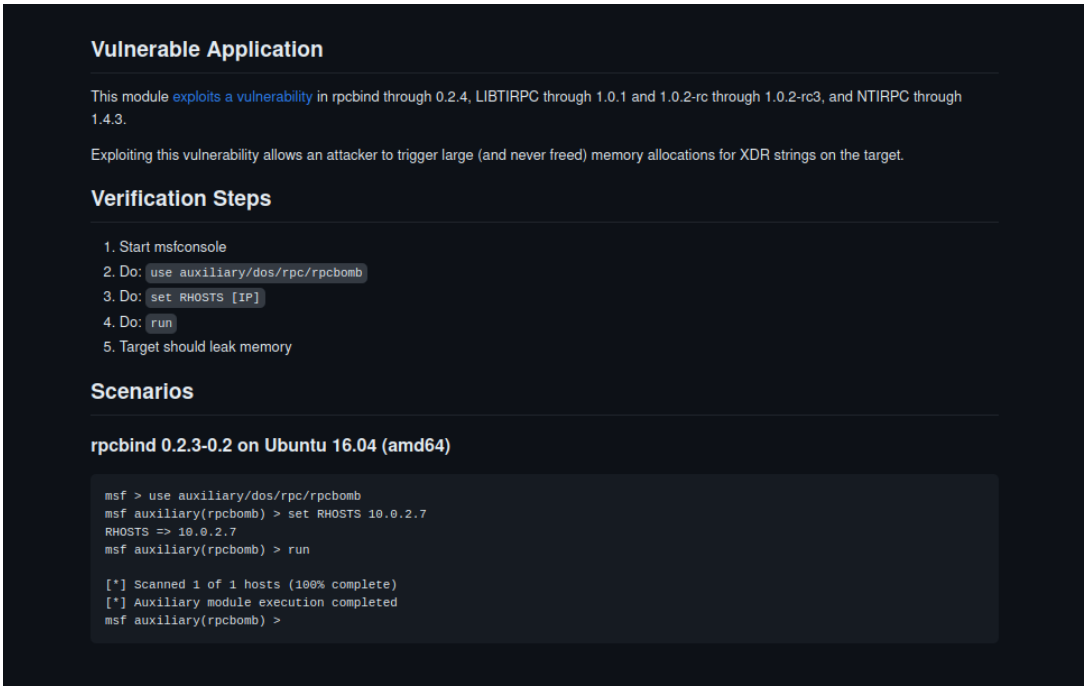


Figure 5.8: Metasploit documentation for msrpc exploit

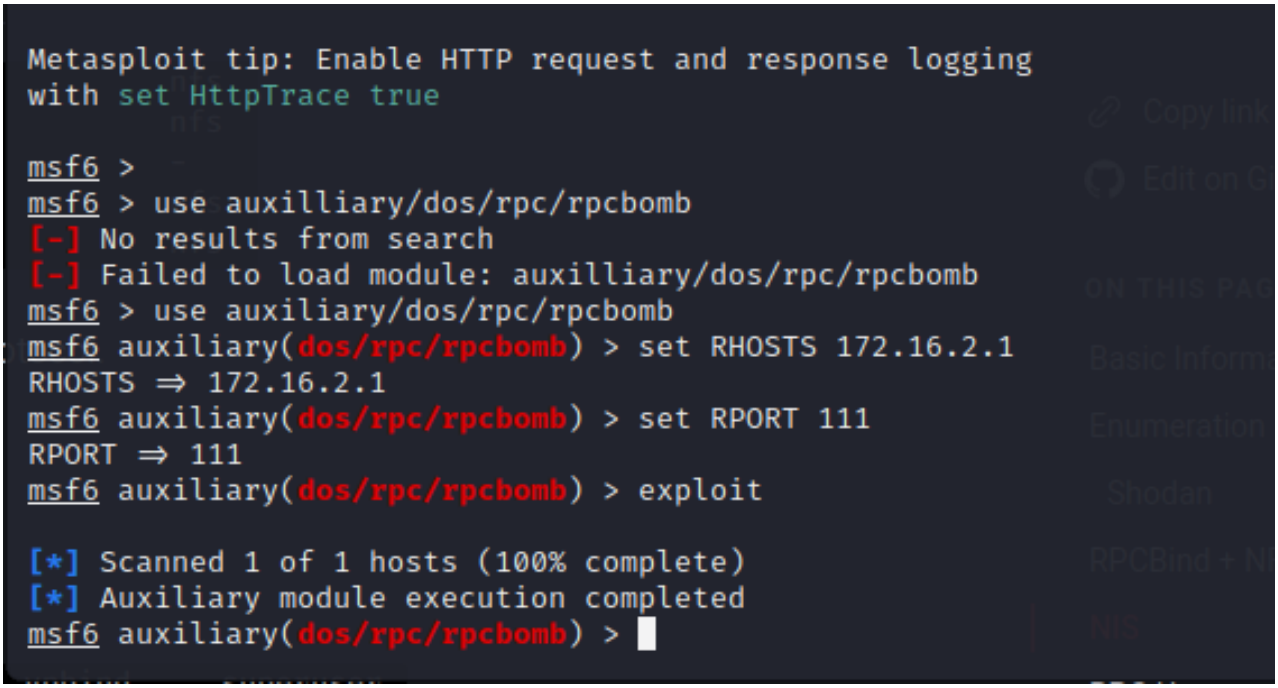


Figure 5.9: Successful RPCBomb attack on port 111

of communications over these connections, possibly exposing users to Man-in-the-Middle (MitM) and phishing attacks. These vulnerabilities were disclosed, and it was advised that the credentials used to access be quickly secured.

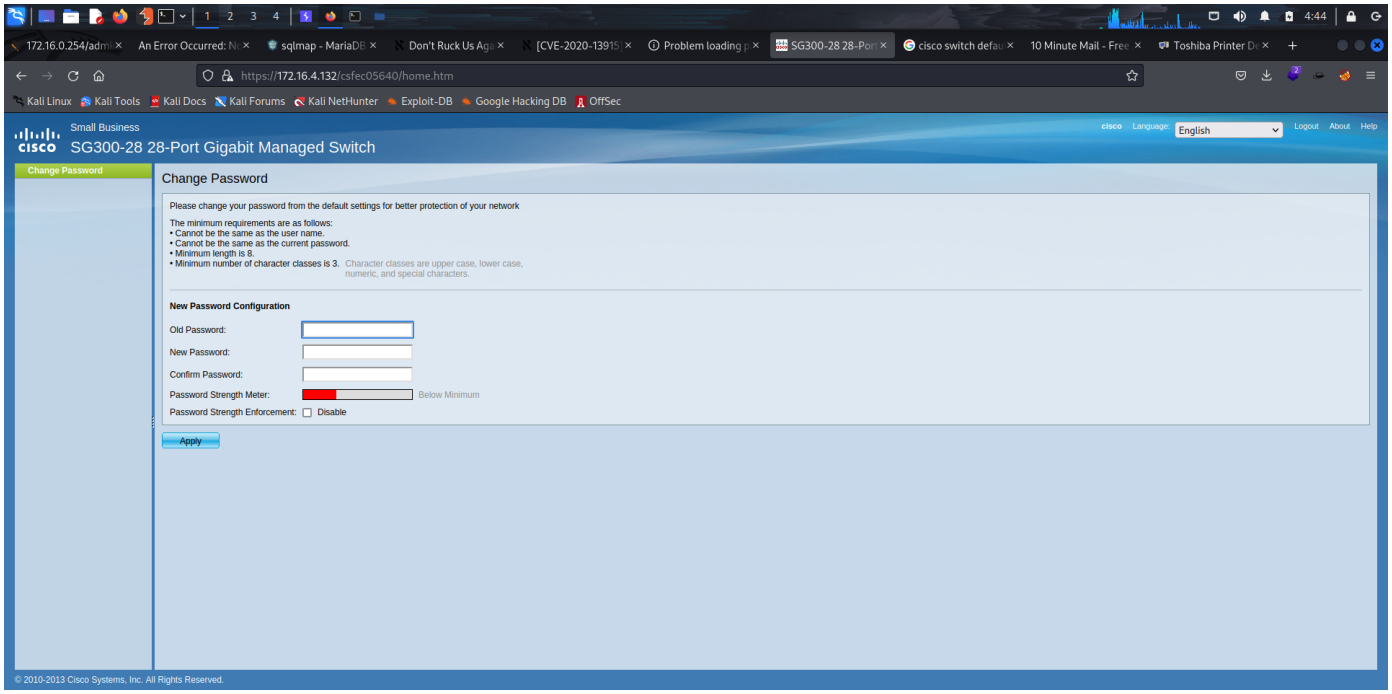


Figure 5.10: Cisco SG 300-28 Switch Admin Console

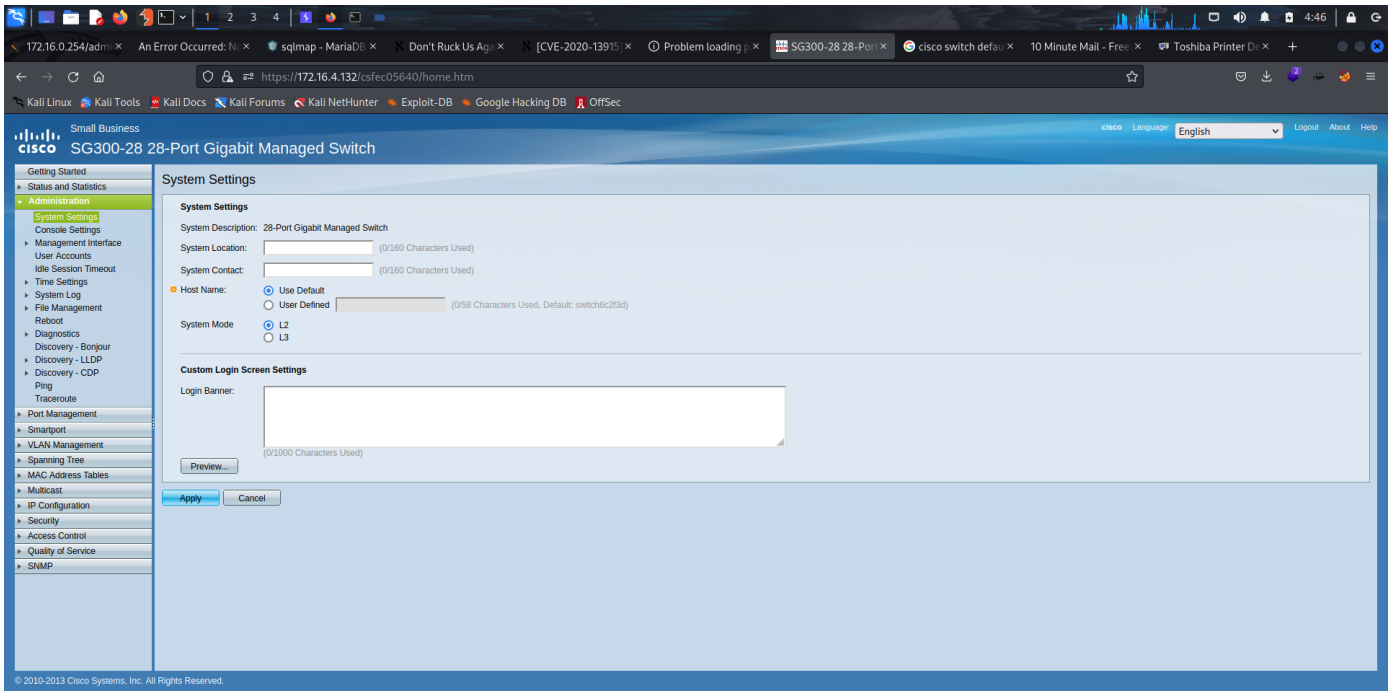


Figure 5.11: Cisco SG 300-28 Switch Admin Console

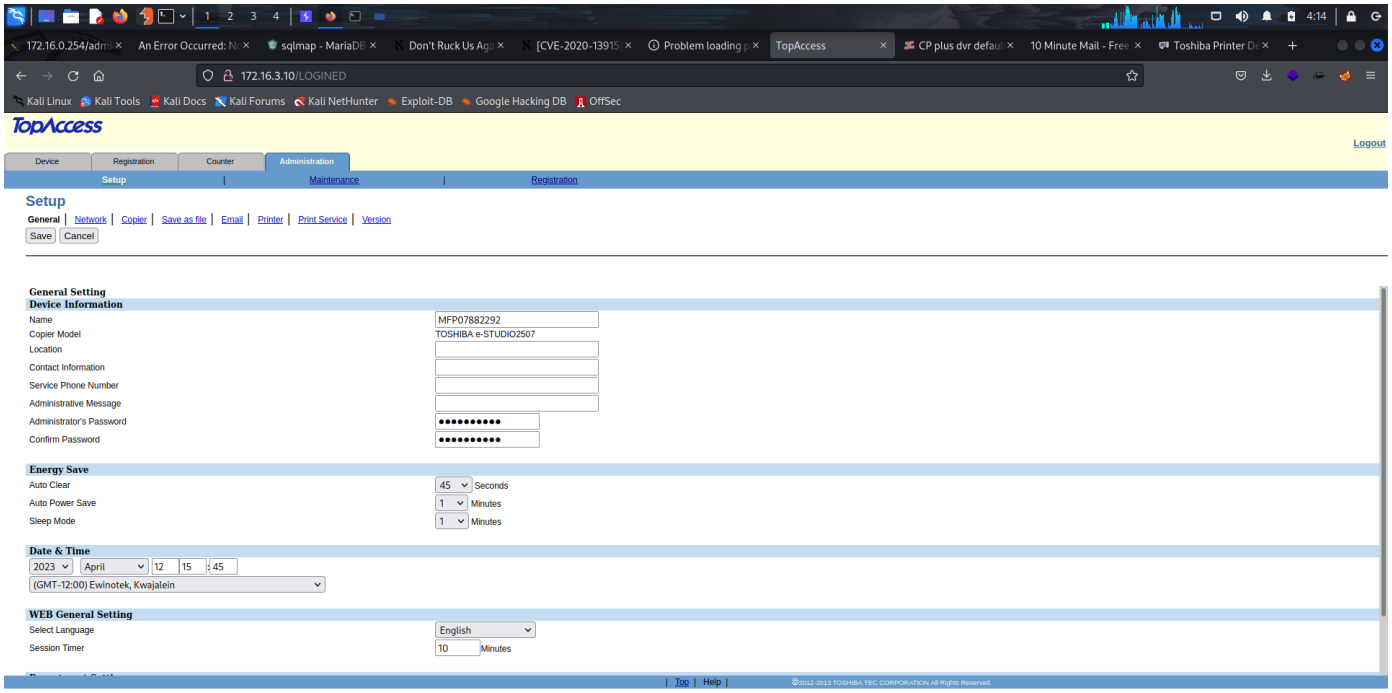


Figure 5.12: Insecure login for Toshiba TopAccess E2507 printer

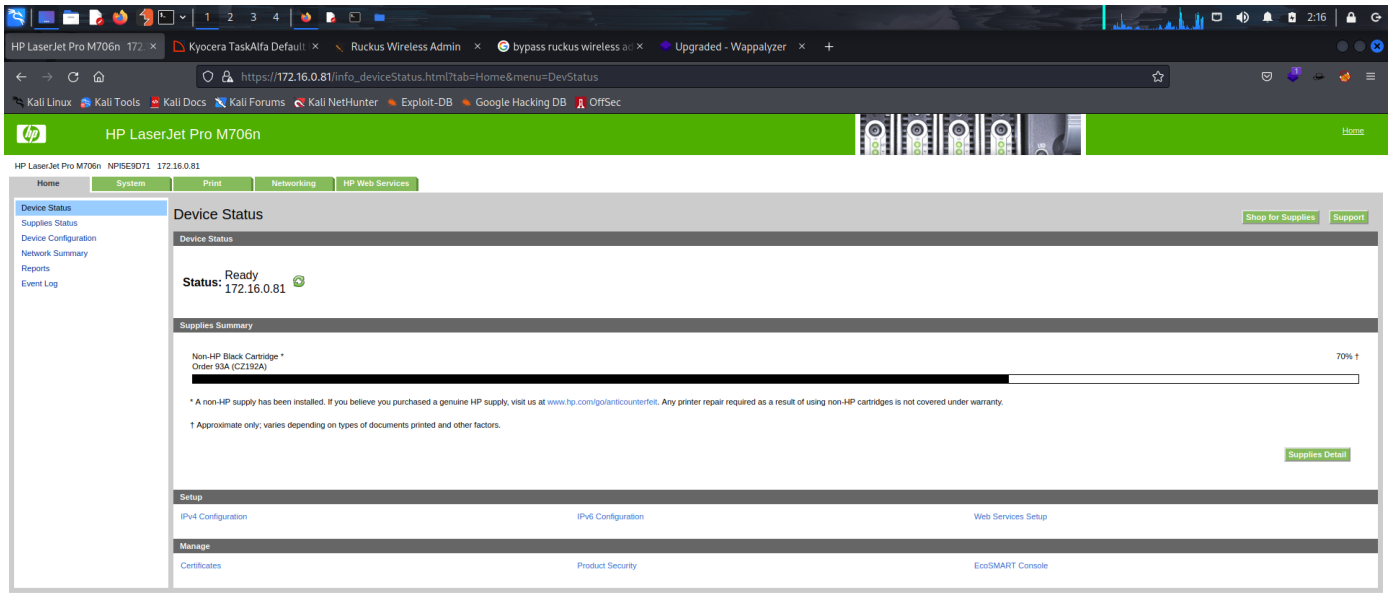


Figure 5.13: Insecure login for HP LaserJet Pro M706n printer

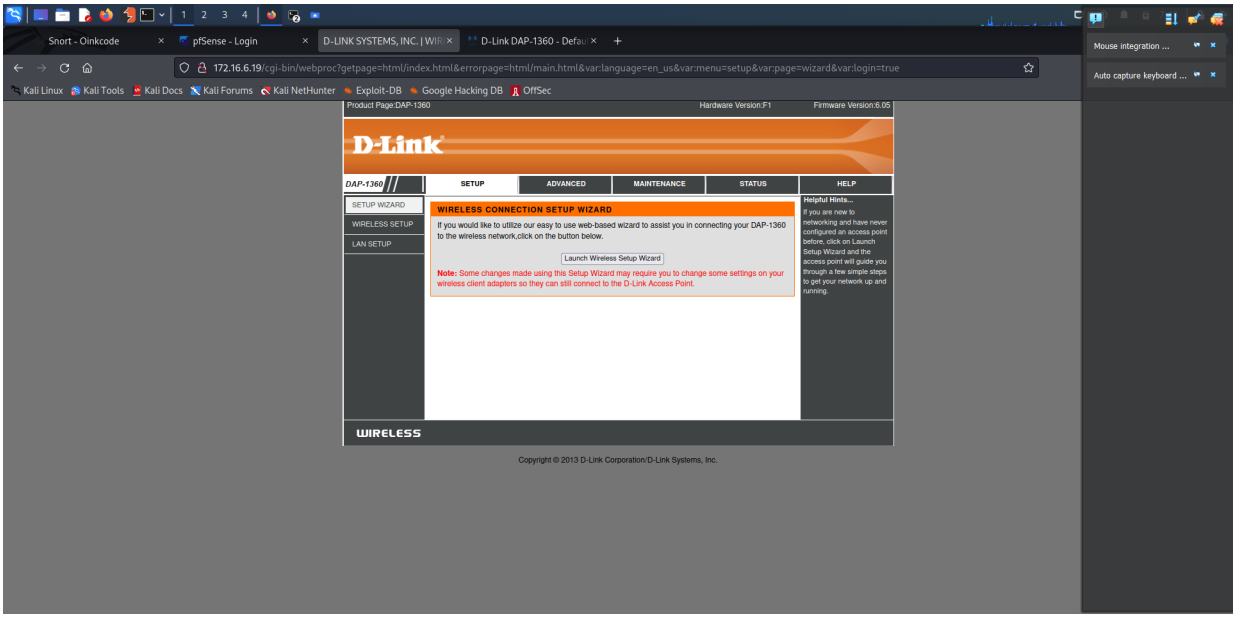


Figure 5.14: D-Link DAP-1360 WAP Admin Console

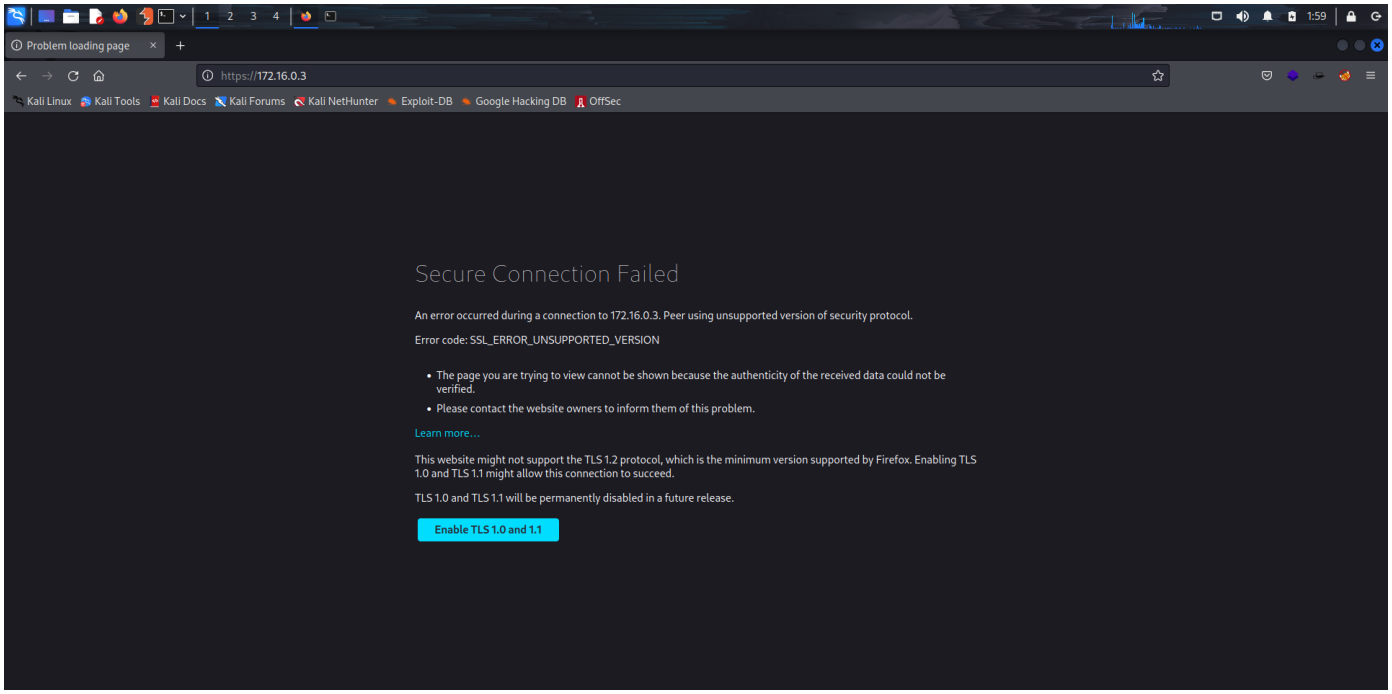


Figure 5.15: Insecure http page with outdated certificates

5.3 pfSense Results

We discovered that pfBlockerNG, our selected website blocking solution, was quite successful in its functioning. It effectively blacklisted the specified URLs, adding another layer of protection to the college campus network. It created extensive reports in the form of pie charts to visualise the outcomes of the blocking action. These reports provided a simple summary of website blocking information, offering useful insights into general block frequency and block report distribution across different categories. The report's first pie chart presented the overall block frequency, displaying

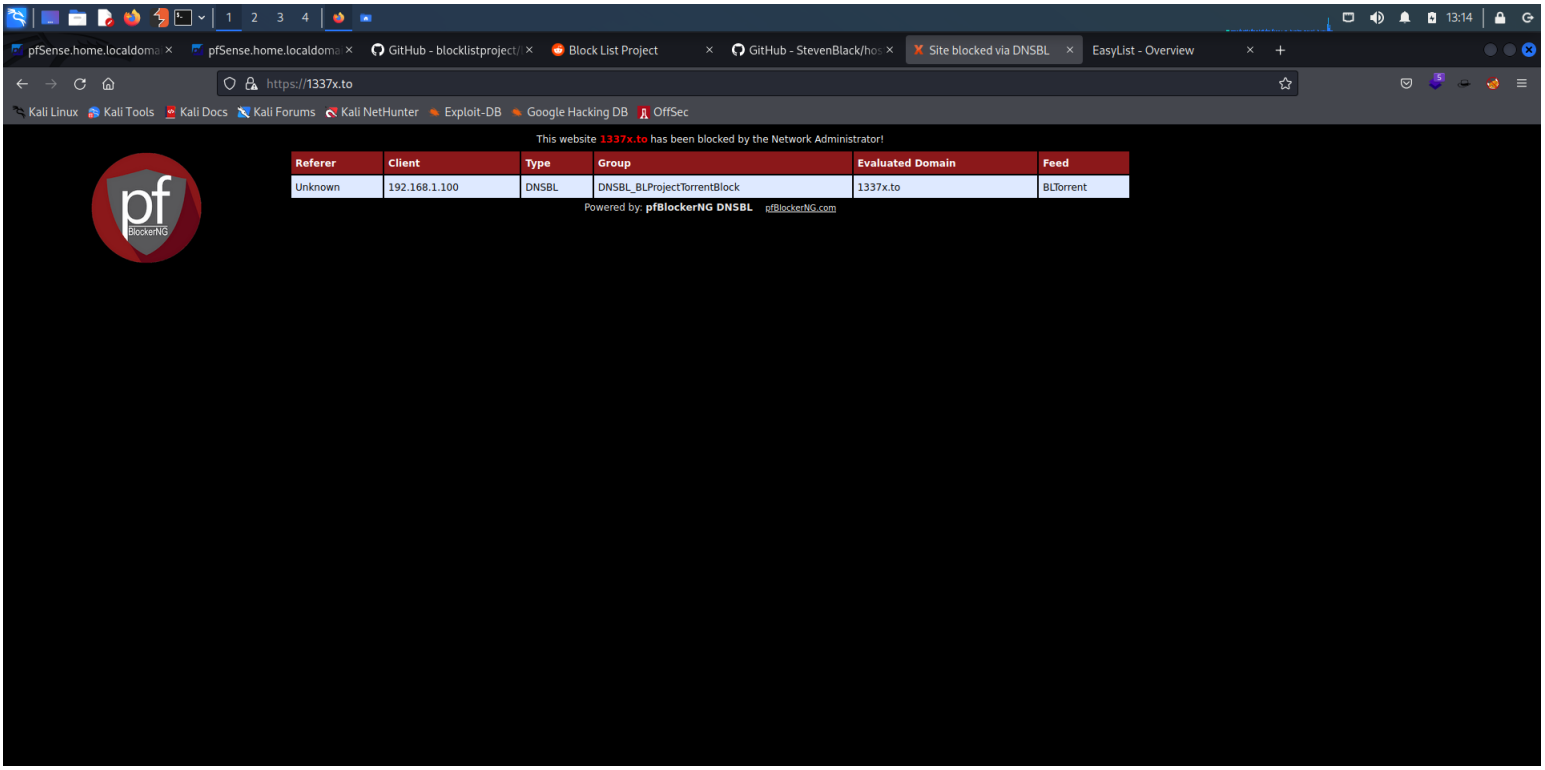


Figure 5.16: Alert shown as pfBlockerNG blocks a blacklisted domain

the percentage of blocked website requests in comparison to the total number of requests. This visual depiction enabled us to evaluate the efficacy of the website blocking methods and acquire an insight of the extent to which undesired or possibly hazardous content was blocked from entering the network.

The second pie chart displayed block reports by category, illustrating the many kinds of websites that were prohibited. We were able to determine the exact sorts of content that were commonly restricted as a result of this breakdown, such as social media, pornographic content, or harmful websites. We were able to fine-tune our

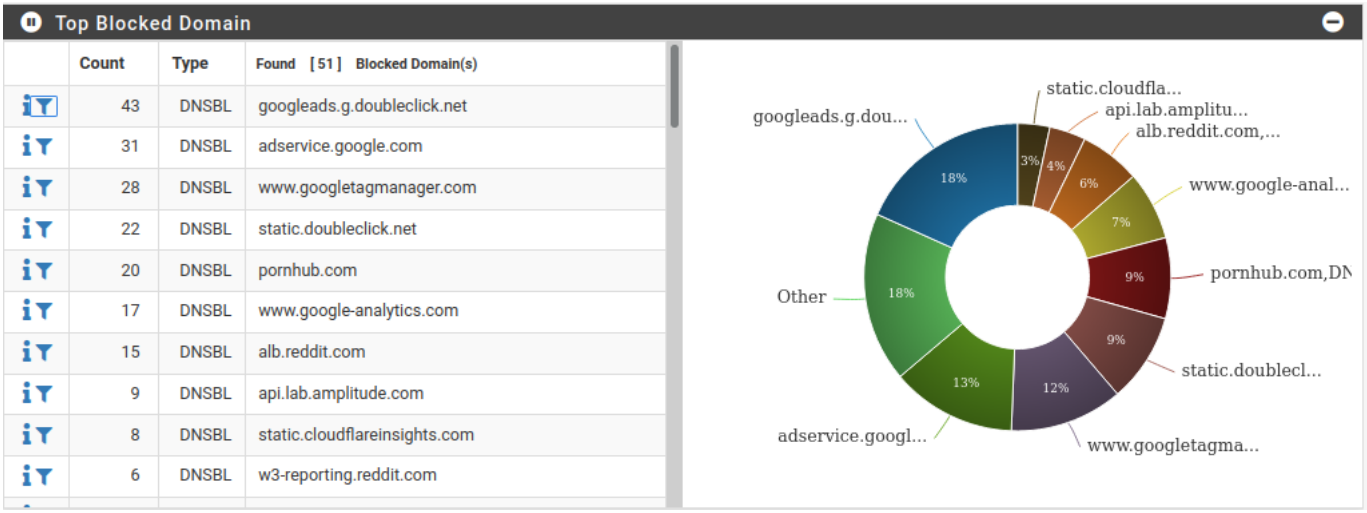


Figure 5.17: DNSBL Reports

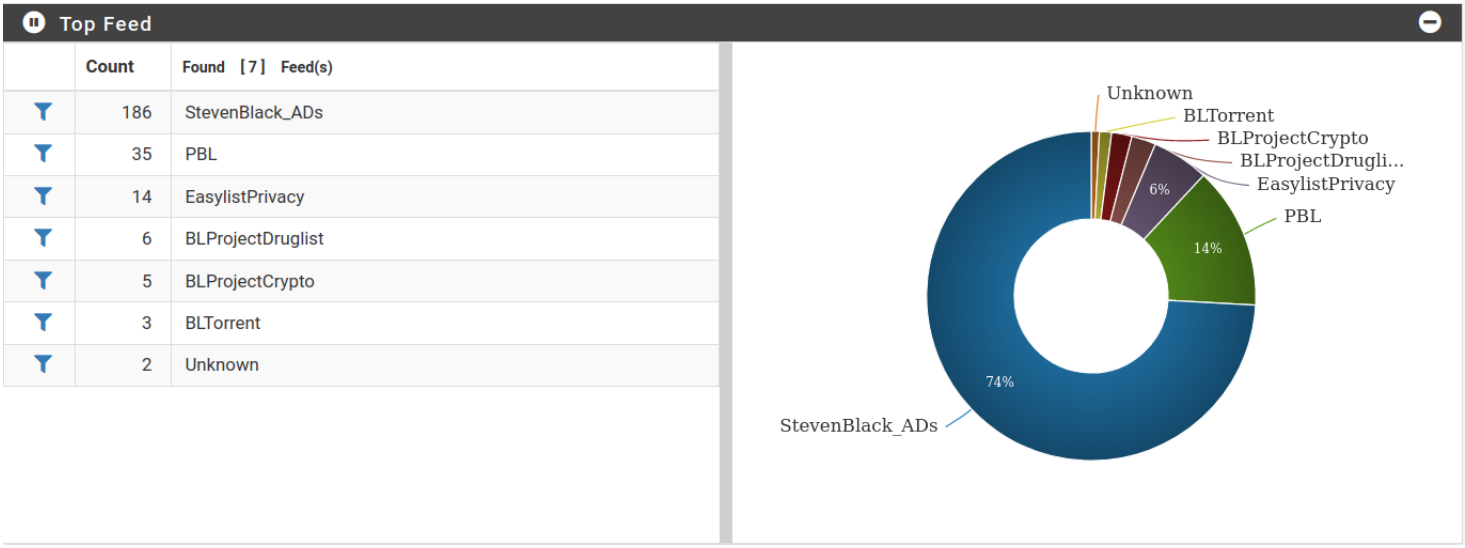


Figure 5.18: DNSBL Reports

website filtering strategies and prioritise the categories that posed the greatest security threats by analysing this data.

The use of pie charts gave a clear and simple picture of the website blocking activity, making the findings easier to grasp and disseminate to key parties. These visual representations enabled us to illustrate the success of pfBlockerNG in blocking websites while also providing significant information into the kind and frequency of banned material. We improved our awareness of website blocking activities and got significant data-driven insights to augment network security measures even further by harnessing the power of visual reporting.

We used the Snort software in pfSense to improve network monitoring and detect

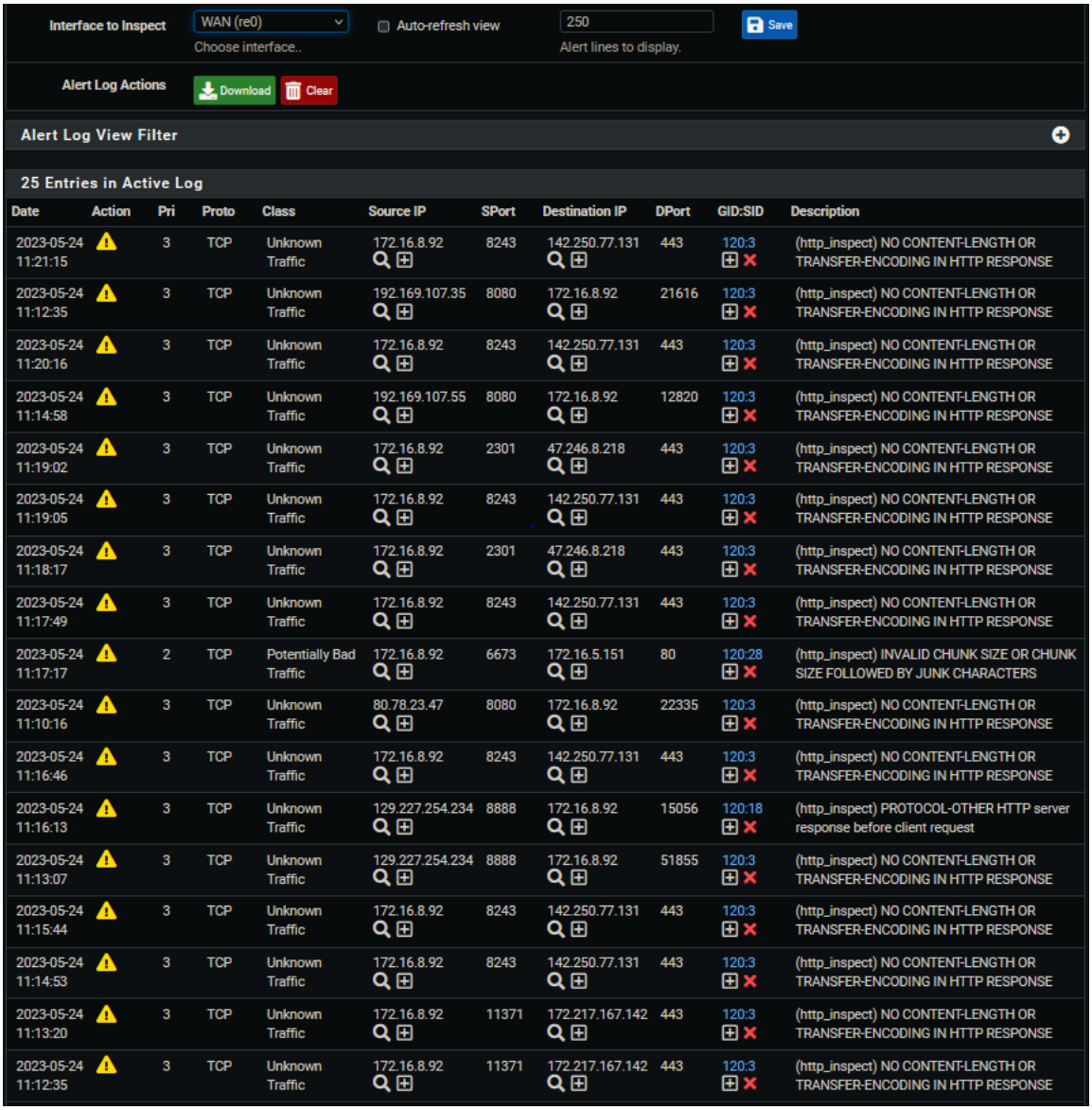


Figure 5.19: IDS alerts

suspicious inbound network activity. We executed a simulation as part of our testing by sending an ICMP HELLO flood to a test network running pfSense. The goal of this test was to evaluate Snort's capacity to detect and report harmful network behaviour. The study not only offered a thorough analysis of the ICMP HELLO flood test, but it also showed Snort's usefulness as an intrusion detection system. Its capacity to detect and report on unusual network activity was critical in maintaining the network's security posture and mitigating possible threats.

Chapter 6

Future Scope

There are various areas for future upgrades and developments based on the network security project's successes. Implementing VLAN (Virtual Local Area Network) technology to further segregate network traffic and increase network performance and security is one critical feature. VLANs can give improved isolation and control over network resources by logically splitting the network into independent virtual networks. Furthermore, further configuration and rule optimisation should be investigated to increase pfSense moderation. This involves fine-tuning firewall rules, putting in intrusion detection and prevention systems, and upgrading and patching the pfSense platform on a regular basis to meet emerging security vulnerabilities.

Furthermore, there is plenty of space to improve network vulnerability analysis skills. To do this, powerful network scanning and penetration testing techniques may be used to discover and mitigate possible security issues. To guarantee continuing protection against emerging threats, vulnerability assessments and security audits should be performed on a regular basis. Furthermore, developing a comprehensive incident response strategy and performing frequent security awareness training for network users will aid in the development of a proactive security and event management culture.

We can continue to enhance its network security posture and respond to growing security issues by concentrating on these future scopes. To properly defend the college campus network and its precious assets, network security must be seen as an ongoing process that involves continual monitoring, modification, and adaptability.

Chapter 7

Conclusion

Our network security project carried out at Government Engineering College Barton Hill, Thiruvananthapuram, has effectively addressed the requirement for modernization and upgrading of the existing network infrastructure. Through meticulous evaluation and analysis, we identified critical flaws such as the lack of network segmentation and absence of an access-limiting firewall. By implementing pfSense, we established robust security measures to manage traffic, enforce access restrictions, and minimize threats, resulting in improved network security, reduced costs, and increased operational efficiency. With the deployment of pfSense, accompanied by packages like pfBlockerNG and Snort, we provided effective solutions for protecting the network against external threats, creating a safer environment for network users, and enhancing the overall security posture and resilience of the college's network.

Furthermore, the considerable financial gain achieved might be used to assess the project's performance. The choice to use pfSense instead of pricey proprietary firewall systems resulted in significant cost savings, with the initial estimate of 15 lakh INR for new firewall firmware being reduced to a mere 1 lakh INR for a dedicated pfSense server. Finally, the network security project not only upgraded the network infrastructure but also improved the college's overall security posture. The project has effectively developed a resilient network architecture that corresponds with industry standards and enables the smooth operation of vital services by resolving identified vulnerabilities and installing robust security solutions.

References

[1] Y. Yamasaki, Y. Miyamoto, J. Yamato, H. Goto and H. Sone, *Flexible Access Management System for Campus VLAN Based on OpenFlow*, 2011 IEEE/IPSJ International Symposium on Applications and the Internet, 2011, pp. 347-351, doi: 10.1109/SAINT.2011.66.

[2] J. Xue, Y. Wu, J. Tao and Y. Zhang, *Research on Campus Network Based on QoS Technology*, 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP), 2020, pp. 418-423, doi: 10.1109/ICICSP50920.2020.9232073.

[3] Patel, Krupa C., and Priyanka Sharma, *A Review paper on pfsense-an Open source firewall introducing with different capabilities & customization*, IJARIIE 3 (2017): 2395-4396.

[4] 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.

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

[6] 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.

turnitin

Similarity Report ID: oid:8268:36419112

PAPER NAME

Analysis_and_Audit_of_Campus_Network-4.pdf

WORD COUNT	CHARACTER COUNT
8583 Words	**49206 Characters**
PAGE COUNT	FILE SIZE
49 Pages	**5.2MB**
SUBMISSION DATE	REPORT DATE
May 29, 2023 2:01 PM GMT+5:30	**May 29, 2023 2:02 PM GMT+5:30**

11% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 10% Internet database
- 0% Publications database
- 8% Submitted Works database

Excluded from Similarity Report

- Crossref database
- Crossref Posted Content database
- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less then 10 words)