ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2485

On the Development of a Threat Driven Model for Campus Network

Otasowie Owolafe[2]; Aderonke F. Thompson[1]; Adewale Oronti[2]; Olaniyi A. Ayeni[2];
Oladimeji O. Abereowo[2]; Yetunde Ogunlola[2]; and Boniface K. Alese[2]
[1]VTT Technical Research Centre of Finland;
[2]Cyber Security Department, Federal University of Technology, Akure, Nigeria.
Corresponding Author: Otasowie Owolafe

Abstract:- Technology as the foundation of almost every aspect of our lives has come to stay and moving with the trend is now the order of the day. Educational institutions are not left out in the advancement struggle. The use of these technologies in educational institutes comes with its attendant evil including but not limited to ransomware attack, denial of service attack, phishing attack, malware attack and the likes. This research therefore, aims to model the different attack types common to campus network. The traffic used for modelling the attack was collected from universities in the western part of Nigeria and the STRIDE and DREAD models were employed. The analysis showed that DoS (fail to auth to VPN to lock out user accounts) had the highest risk score (43) while DoS (complex search queries, CPU exhaustion) had the lowest score (26).

Keywords:- *Campus Network, STRIDE, DREAD, Cyber Attack, Data Breaches, Security Risk.*

I. INTRODUCTION

In an era where technology is the foundation of almost every aspect of our lives, ensuring the security of networks is paramount. In the field of information security, the continuous tussle that exist between good and bad has not stopped. There are always chances that information will be stolen so far it is valuable and adversaries have interested in it. Irrespective of the security measures taken, security loopholes and vulnerabilities that the adversaries can exploit are inevitably present. This is especially true for campus networks, which serve as the lifeblood of academic institutions, facilitating communication, collaboration, and access to vast repositories of information. Teaching, research, academic administration, and general management activities are all part of the campus network. In addition, it includes off-campus data communications, electronic bulletin boards, video conferencing, internet, and remote education services.

Students, faculty, and staff rely on this digital infrastructure for everything from accessing learning materials to collaborating on groundbreaking projects. However, as the importance of these networks grows, so do the threats they face. Cyber-attacks, data breaches, and network intrusions pose significant risks to the integrity, confidentiality, and availability of campus resources. Owing to certain features of campus networks, such as sharing, openness, and interconnectivity, campus network security must handle a wide range of possible threats and contend with the possibility of internal and external network attacks. These security risks attack can lead to many negative impacts which may have serious consequences.

This work will delve into research specific to campus networks. This includes studies on the types of threats most commonly targeting educational institutions, the vulnerabilities present in campus network configurations, and the impact of successful attacks on academic operations.

To address these challenges, the development of a robust threat and risk assessment model tailored specifically for campus networks is imperative. This model will provide a comprehensive framework for identifying, analyzing, and mitigating potential threats and vulnerabilities, thereby enhancing the overall security posture of the network. By understanding the unique characteristics and requirements of campus environments, this model can offer desired solutions that balance security measures with the need for accessibility and usability.

Despite these advancements, significant challenges remain in the development and implementation of a comprehensive threat and risk assessment model for campus networks. Issues such as budget constraints, resource limitations, and the rapidly evolving nature of cyber threats necessitate a flexible and adaptive approach. Moreover, the inherent complexity of campus environments, characterized by diverse user populations, decentralized administration, and heterogeneous infrastructure, adds another layer of complexity to the task at hand. While the development of a threat and risk assessment model for campus networks presents numerous challenges, it also offers significant opportunities to enhance the security and resilience of these critical infrastructures. By leveraging the collective insights of existing research and embracing emerging technologies and methodologies, we can pave the way for a safer and more secure digital campus environment.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2485

II. RELATED WORKS

A considerable body of research has been devoted to the development of threat and risk assessment models for various types of networks, ranging from corporate infrastructures to critical national systems. While these models offer valuable insights into the principles and methodologies of risk management, they often lack the specificity required to address the unique challenges posed by campus environments. However, several studies have emerged that focus specifically on campus network security, laying the groundwork for the development of a dedicated assessment model.

One notable study by Smith et al. (2018) conducted a comprehensive analysis of the security risks facing university networks, highlighting the importance of proactive risk management strategies. By examining common threats such as malware, phishing attacks, and insider threats, the study provided valuable insights into the vulnerabilities inherent in campus infrastructures. Similarly, Jones and Lee (2020) explored the efficacy of various security controls in mitigating the risks associated with student-owned devices connected to campus networks. Their findings underscored the need for a multifaceted approach that combines technical controls with user education and awareness.

Ismaila et al. (2018) offers a valuable exploration of the security challenges faced by campus networks. In their work titled “Campus Network Security: Threats, Analysis and Strategies”, they highlight the importance of considering both internal and external threats, emphasizing the need to safeguard against not only sophisticated cyberattacks but also physical security breaches and human error.

Liu et al. (2017) present a compelling argument for a multi-layered approach to securing campus networks. The research acknowledged the limitations of relying on a single security measure and advocate for a comprehensive strategy that addresses vulnerabilities at various levels. The researcher further explored the need for robust system security measures, such as keeping software up-to-date and implementing user access controls. They recognize the importance of securing applications as well, suggesting measures like vulnerability patching and user authentication protocols.

The research by Chen et al. (2013) adopting the Case of Seven Universities offers a valuable case study approach to understanding campus network security vulnerabilities. By focusing on seven specific universities, their work provides insights into the real-world challenges faced by educational institutions. By analysing the security posture of multiple universities, Chen et al. (2013) were able to identify common vulnerabilities, such as weak password policies and unpatched software. Their findings serve as a cautionary tale and highlight the need for ongoing vigilance in maintaining campus network security.

The research of Jianhua (2023) delves into the application of Markov models for analyzing security and privacy concerns within smart campuses. While Du Jianhua's (2023) focus is primarily on network security, the underlying concept of using a probabilistic model to assess risk can be extended to student privacy protection as well. By analyzing user behavior and data access patterns, we might be able to identify situations where student privacy is at risk.

The research by Wu et al. (2020) focuses on the practical steps involved in building and implementing a security defense system for a university campus network. By examining Wu et al.'s work (2020), it discusses valuable insights into the real-world process of translating security best practices into a functional system.

The research by Li et al. (2020), provide a comprehensive analysis of the evolving landscape of campus network security threats and corresponding protective measures. By examining the evolving nature of threats and the corresponding protective measures outlined by Li et al. (2020), ensures the threat and risk assessment model remains relevant and addresses the most current security concerns faced by campus networks.

Building upon these foundational works, recent advancements in cybersecurity technologies and methodologies have paved the way for more sophisticated threat and risk assessment models designed specifically for campus networks. For example, the use of machine learning algorithms for anomaly detection has shown promising results in identifying suspicious behaviour and potential security breaches that has enabled institutions to stay abreast of emerging threats and vulnerabilities, enhancing their ability to proactively defend against attacks.

III. METHODOLOGY

Network security can be enhanced through threat modelling, which involves identifying targets, identifying vulnerabilities, and implementing countermeasures to either stop or lessen the impact of cyberattacks on the system. Threat modelling entails describing the resources of an organisation, figuring out the purpose of each application in the overall scheme of things, and then creating a security profile for each application. The next step in the modelling process is to identify and rank probable dangers. Once these are done, damaging occurrences and their fixes are recorded. For a campus network, a threat-driven model entails locating possible risks and creating countermeasures through security control design. This is a high-level layout.

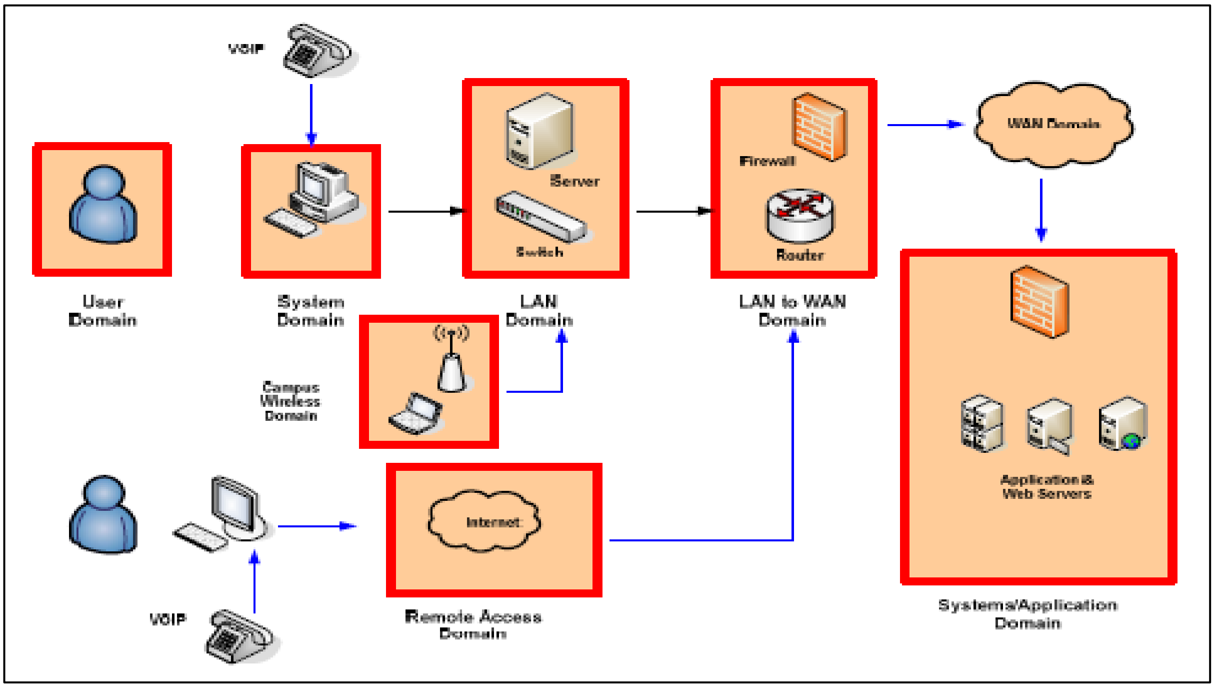

Fig 1: Campus Network Domain

❖ *Threats*

- Unauthorized Access: Hackers, students, or staff attempting to gain unauthorized access to the network.
- Malware and Ransomware: Malicious software spread through phishing, infected devices, or exploited vulnerabilities.
- Denial of Service (DoS/DDoS): Overwhelming the network with traffic, causing disruptions and outages.
- Data Breaches: Unauthorized access or exfiltration of sensitive data, such as student records or research.
- Insider Threats: Authorized users misusing their access or intentionally causing harm.
- Physical Security: Unauthorized access to network devices, servers, or data centers.
- Social Engineering: Phishing, pretexting, or baiting attacks targeting students and staff.
- Bring Your Own Device (BYOD): Unsecured personal devices connecting to the network.
- Outdated Software and Vulnerabilities: Exploitation of unpatched software or known vulnerabilities.
- Natural Disasters and Power Outages: Disruptions due to environmental factors.

A number of Security Controls must be put in place which include:

- Network Segmentation: Divide the network into secure zones, limiting lateral movement.
- Firewalls and Access Control Lists (ACLs): Restrict incoming and outgoing traffic based on rules and policies.
- Intrusion Detection and Prevention Systems (IDPS): Monitor and block suspicious traffic.
- Encryption: Protect data in transit and at rest with SSL/TLS, IPsec, and disk encryption.
- Strong Authentication and Authorization: Multi-factor authentication, secure passwords, and role-based access control.
- Regular Vulnerability Management: Patching, software updates, and vulnerability scanning.
- Network Monitoring and Incident Response: Continuously monitoring of the network and responding to incidents.
- Security Awareness Training: Educate students and staff on security best practices and threats.
- Physical Security Measures: Access controls, surveillance, and secure data center and network device storage.
- Disaster Recovery and Business Continuity Planning: Regular backups, redundancy, and contingency planning.

❖ *Threat Model Process.*

A. Identifying the Assets

In threat modelling process, the initial stage is the identification of the University Network Assets. A University Network Asset is any valuable component that is owned by the University that attackers are interested in. Major components include, but are not restricted to, the network, host, application, key research data, and student identities.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2485

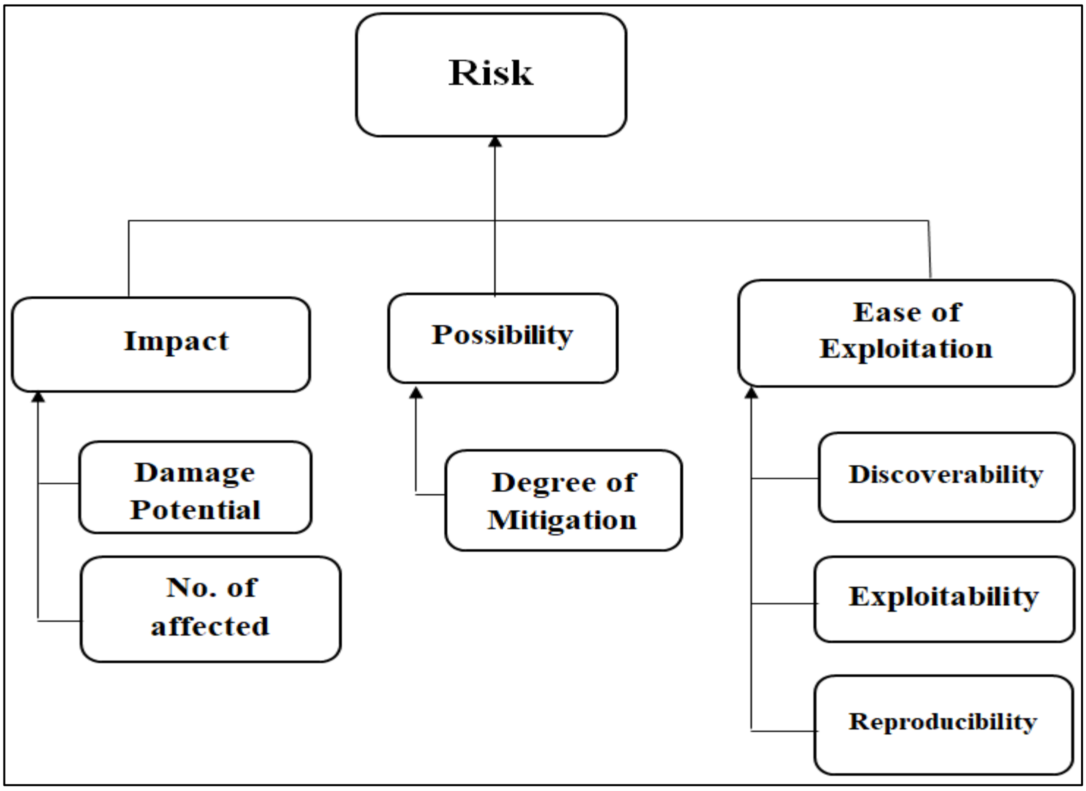

Fig 2: Threat Model Process

The first thing to identify in the threat process model on campus network is the inherent risk. The impact of the risk if exploited, the possibility of the risk happening and the ease of exploitation.

B. Decompose of Network

Finding vulnerabilities in a network's deployment configuration, architecture, or implementation is the main purpose of this phase. The Campus Network's components are dissected to provide a thorough grasp of the concepts, including Application Architecture, Deployment/ Infrastructure, and Component. The campus network's Threat Driven Model will then be created. The networks' Potential Entry Points (E), Protected Resources (P), Data Flows across system components (D), and Trust Boundaries (T) will thereafter be used to identify this model.

C. Identify the Threats

The threat would be discovered in the third stage. While there are several models for identifying threats, the STRIDE Model—which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege is the one that this study focuses on using to identify risks. This approach will assist in identifying issue areas and estimating the level of risk in each. The threat type's definition, matching security attribute, and default controls are all included in the STRIDE model.

D. Documented Threats and Countermeasures

At this step, a list of the most significant risks to the host, application layer, and network will be identified, along with a description of the necessary countermeasures for each threat. In order to do threat modelling, the Network Administrator/System Administrator will find this section useful in understanding and classifying threats.

E. Rating Identified Threats

The rating of the dangers that have been detected is the final step, and the DREAD model will be applied in this task. After threat modelling is finished, this step will be carried out. Prior to that, risk assessment and analysis were carried out (using equation 1). This is done in an effort to rank the risks connected to particular dangers. DREAD serves as a categorization framework for comparing, quantifying, and ranking the level of risk associated with each threat that has undergone assessment. Five categories are identified by DREAD as having the most influence on determining potential threat.

The DREAD formula is shown as:

$$\text{RISK\_ASSESMENT} = \frac{(\text{DAMAGE} + \text{REPRODUCIBILITY} + \text{EXPLOITABILITY} + \text{AFFECTED USERS} + \text{DISCOVERABILITY})}{5} \quad (1)$$

IV. ANALYSIS AND RESULT

➢ *IBR Campus Threat Modelling*

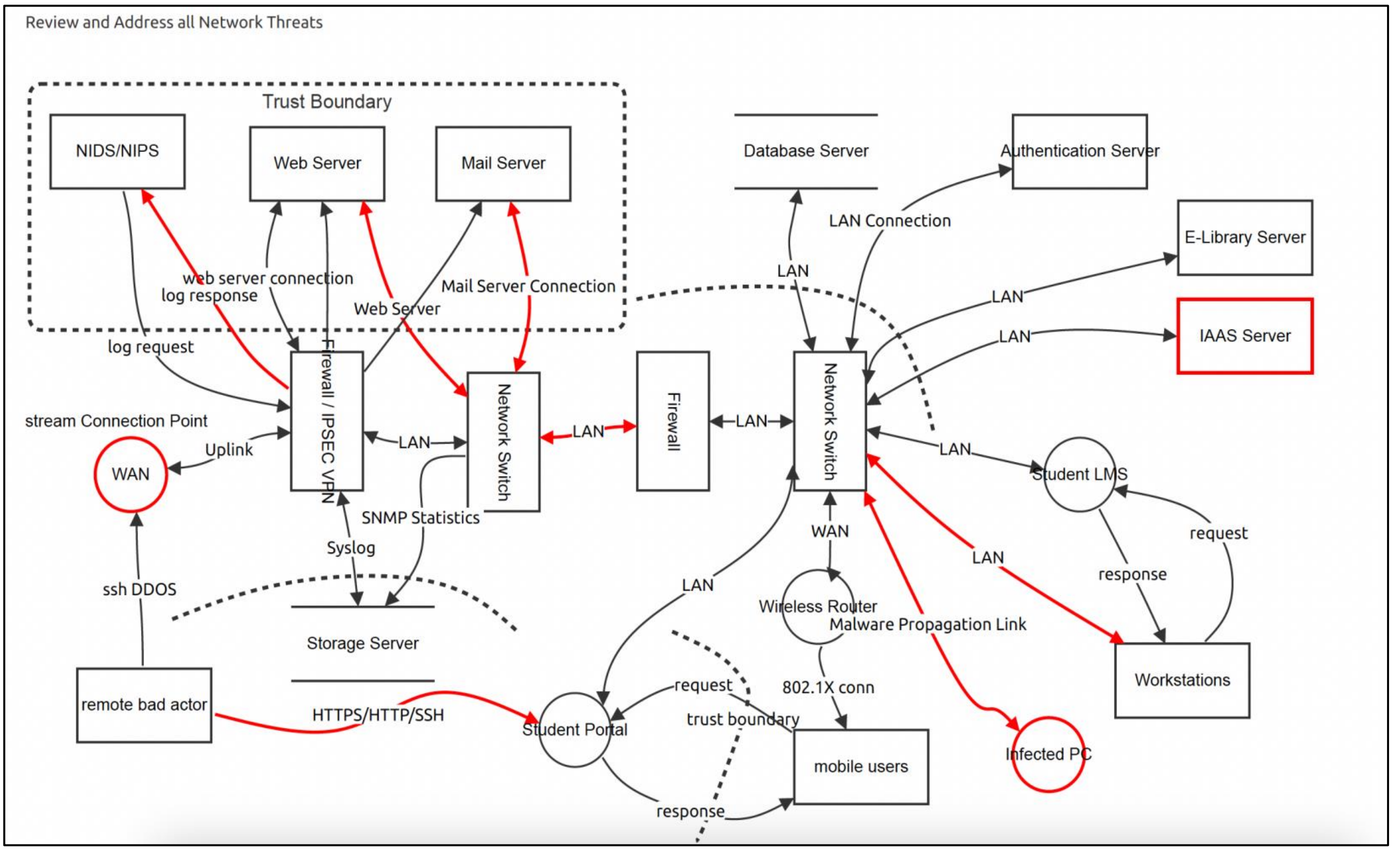

Fig 3: Campus Threat Modelling

Table 1 WAN (Process) Packet Input and Output Point on the Network

S/N	Title	Type	Priority	Status	Description	Mitigations
11	Generic privilege Elevation	Elevation of privilege	High	Mitigated	An Attacker can use to change roles if authorisation is tampered with	Block attackers JWT access to change roles
49	Bandwidth Depletion	Repudiation	Medium	Open	Flood Attack and Amplifcation Attack	Deploy Team Cyrmu ACL at Ingress Interface
53	Blackhole	Spoofng	Medium	Mitigated	Drop packets by sending false routes reply messages to requests	Blackhole all bad bgp routes

Table 2 Firewall / IPSEC VPN (Actor) provide access for only legitimate remote login and block all others

S/N	Title	Type	Priority	Status	Description	Mitigations
9	VPN IPSEC	Spoofing	High	Mitigated	attacker can steal authentication credentials and use for impersonate	IPSEC with strong cipher encrypts user logins during access so that packet spoofing is prevented

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2485

Table 3 NIDS / NIPS (ACTOR) Network Intrusion Detection System / Network Intrusion Prevention System

S/N	Title	Type	Priority	Status	Description	Mitigations
23	STRIDE NIDS/NIPS Threat	Repudiation	High	Mitigated	To detect and prevent unauthorised network access	Prevent unauthorised access and privilege modification Send alert messages during intrusion.
24	IDS Threat	Repudiation	High	Mitigated	Detection Intrusion Prevent	Intrusion into the ACL

Table 4 Network Switch (Actor) Layer 3 Network Access

S/N	Title	Type	Priority	Status	Description	Mitigations
25	Layer 3 STRIDE Threat	Spoofing	High	Mitigated	Provide layer 3 routes for packet switching	Protect against lateral movement and breakdown broadcast domain

Table 5 Wireless Router (Process)

S/N	Title	Type	Priority	Status	Description	Mitigations
25	Router STRIDE Threat	Spoofing	High	Mitigated	Monitor Wireless Network Access	Block all wireless attacks using ACL

Table 6 Mail Server (Actor) Campus Mail Service

S/N	Title	Type	Priorit y	Status	Description	Mitigations
33	Mail STRIDE threat	Spoofing	High	Mitigated	Mail Service for Communication (IMAPs, POP3s, HTTPs)	Identity theft prevention by using on IMAPs, POP3s, HTTPs. Establishing of DMARC, SPF, DKIM records to preventing spam attacks.

Table 7 Firewall (Actor) Prevent unauthorised access

S/N	Title	Type	Priority	Status	Description	Mitigations
0	New STRIDE threat	Spoofing	High	Mitigated	Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
27	STRIDE threat FW	Repudiation	High	Mitigated	Provide information about log manipulation	Prevent log manipulation by redirecting logs for processing to external device

Table 8 Network Switch (Actor) Packet routing

S/N	Title	Type	Priorit y	Status	Description	Mitigations
18	Generic STRIDE threat	Spoofing	High	Mitigated	Stop inter-vlan routing	Use Micro-Segmentation to breakdown Vlans

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2485

Table 9 Workstations (Actor)

S/N	Title	Type	Priority	Status	Description	Mitigations
20	PC STRIDE Mitigation	Spoofing	High	Mitigated	An attacker locks a legitimate user out of their account by performing many failed authentication attempts.	Prevent any PC without uptodate antivirus from accessing LMS

Table 10 Syslog (Data Flow) Audit logs for Forensic

S/N	Title	Type	Priority	Status	Description	Mitigations
12	Tampering Threat	Tampering	High	Mitigated	Prevent syslog deleting and modification from attackers	Access level of read only for non-privilege

Table 11 SNMP Statistics (Data Flow) Send SNMP statistics to Syslog server

S/N	Title	Type	Priority	Status	Description	Mitigations
13	Tampering of Syslog	Tampering	High	Mitigated	Send generated syslog to designated syslog for audit trail	prevent change of syslog access

Table 12 Malware Propagation Link (Data Flow) Malware Propagation Link

S/N	Title	Type	Priority	Status	Description	Mitigations
16	Malware ID	Information disclosure	High	Open	Information Disclosure	Prevent Lateral Data Movement

Table 13 LAN (Data Flow) UDP Flood

S/N	Title	Type	Priority	Status	Description	Mitigations
39	UDP Flood STRIDE threat	Denial of service	High	Mitigated	UDP flood attacks may also fill the bandwidth of connections located around the victim system.	Limit number connection

Table 14 LAN (Data Flow)

S/N	Title	Type	Priority	Status	Description	Mitigations
40	ICMP Flood Attack	Denial of service	High	Mitigated	An ICMP flood attack is initiated when the zombies send a huge number of ICMP_ECHO_REPLY packets (“ping”) to the victim system.	Drop all ICMP_ECHO_REPLY

Table 15 Request (Data Flow)

S/N	Title	Type	Priority	Status	Description	Mitigations
21	LMS STRIDE request	Information disclosure	High	Mitigated	service request	Use https for web traffic request and drop all other non-https traffic

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2485

Table 16 LAN (Data Flow)

S/N	Title	Type	Priorit y	Status	Description	Mitigations
38	UDP Flood attack	Denial of service	High	Open	UDP flood attacks may also fill the bandwidth of connections located around the victim system.	Limit number of connections per second

Table 17 LAN (Data Flow)

S/N	Title	Type	Priorit y	Status	Description	Mitigations
47	DDoS Smurf Attack	Tamperin g	High	Mitigated	DDoS Smurf attack is a type of an amplification attack where the attacker sends packets to a network amplifier, with the return address changed to the victim's IP address. The attacking packets are typically ICMP ECHO REQUESTs.	Limit number of ICMP ECHO Host can process

Table 18 web server connection (Data Flow) web server connection

S/N	Title	Type	Priorit y	Status	Description	Mitigations
34	Web Service STRIDE Threat	Denial of service	High	Mitigated	Port 443 DDOS attack prevention	Limit number

Table 19 LAN (Data Flow)

S/N	Title	Type	Priorit y	Status	Description	Mitigations
42	WEB DDoS	Denial of service	High	Open	Unavailability and inability to access a particular web site due to DDoS attacks	Drop all DDoS

Table 20 response (Data Flow)

S/N	Title	Type	Priority	Status	Description	Mitigations
22	LMS information response	Information disclosure	High	Mitigated	LMS response	Use https for web traffic response and drop all other non-https traffic

Table 21 LAN (Data Flow)

S/N	Title	Type	Priorit y	Status	Description	Mitigations
43	Protocol Exploit	Tamperin g	High	Mitigated	TCP SYN (Transfer Control Protocol Synchronize) protocol, and the other misusing the PUSH + ACK protocol	Limit DDoS TCP SYN attack before instructions get to zombies Run a good

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2485

Table 22WAN (Data Flow)

S/N	Title	Type	Priority	Status	Description	Mitigations
41	Signal Interference	Tampering	High	Mitigated	Signal Interference	Use Non-Overlapping frequency

Table 23 ssh DDOS (Data Flow) ssh bruteforce

S/N	Title	Type	Priority	Status	Description	Mitigations
2	ssh bruteforce	Information disclosure	High	Mitigated	various login attempt from bad actors	outright ban after 2 bad request
3	ssh bruteforce	Information disclosure	High	Mitigated	ban user for wrong trial	ban user layer 3 for 31 days

Table 24 Web Server (Data Flow) Web Server Layer 3 connection

S/N	Title	Type	Priority	Status	Description	Mitigations
35	New STRIDE threat	Denial of service	High	Open	Network Connection	Prevent DDOS using ACL

Table 25 log response (Data Flow) IPS/IDS response

S/N	Title	Type	Priority	Status	Description	Mitigations
4	IPS/IDS logs	Tampering	High	Open	provide information from all logs to core infrastructure and send alert messages to admin	block all bad request and alert admins

Table 26 log request (Data Flow) IPS/IDS request

S/N	Title	Type	Priority	Status	Description	Mitigations
5	IPS/IDS	Tampering	High	Mitigated	request all logs from core infrastructures for processing	provide information for processing

Table 27 LAN (Data Flow)

S/N	Title	Type	Priority	Status	Description	Mitigations
45	Malformed Packet Attacks	Tampering	High	Mitigated	Malformed packet attacks involve using the victim's processing resources to deliver IP packets that are improperly formatted to the target system, ultimately bringing it down. If the number of these attacks increases, the victim system may become overloaded and crash.	Limit number of IP packet a single host can send

Table 28 Mail Server Connection (Data Flow)

S/N	Title	Type	Priority	Status	Description	Mitigations
36	Mail Server	LAN Denial of service	High	Open	Lan Connection	Prevent DDOS using ACL

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2485

Table 29 Uplink (Data Flow)

S/N	Title	Type	Priority	Status	Description	Mitigations
50	DDoS	Denial of service	High	Mitigated	Actice Attack	drop all ICMP, UDP, and all detected smurf packets

Table 30 LAN (Data Flow)

S/N	Title	Type	Priority	Status	Description	Mitigations
52	SQL Injection	Tampering	High	Mitigated	SQL Injection attacks	Patching of DB regularly

Table 31 HTTPS/HTTP/SSH (Data Flow) bruteforce login attempts

S/N	Title	Type	Priority	Status	Description	Mitigations
1	HTTP, HTTPS, SSH Bruteforce Attack	Information disclosure	High	Open	remote user trying various login requests from	remote sites to take over server limit number of bad request
8	SSH Bruteforce	Denial of service	Medium	Mitigated	block unwanted access out-right	block and change default ssh port to new user defined

Table 32 Authentication Server (Actor)

S/N	Title	Type	Priority	Status	Description	Mitigations
51	Stealing of User Token	Spoofing	High	Mitigated	Stealing of User Credentials Prevent	User and Password credentials guessing

Table 33 E-Library Server (Actor)

S/N	Title	Type	Priority	Status	Description	Mitigations
48	SSH BruteForce	Spoofing	High	Mitigated	huge volume of attack traffic, which is known as a Bruteforce attack trying to guess access credentials	Limit SSH connection to Server

Table 34 IAAS Server (Actor) Infrastructure as a Server

S/N	Title	Type	Priority	Status	Description	Mitigations
37	IAAS STRIDE Threat	Spoofing	High	Open	Prevent illegitimate access	Prevent unauthorised container creation by restriction user privilege access

Table 35 Database Server (Store) Main Database server

S/N	Title	Type	Priority	Status	Description	Mitigations
32	Database STRIDE threat	Information disclosure	High	Mitigated	Prevent Information disclosure against Database	Block all IP not authorised to make connection

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2485

Table 36 mobile users (Actor)

S/N	Title	Type	Priority	Status	Description	Mitigations
17	Generic STRIDE threat	Spoofing	High	Mitigated	prevent inter-vlan routing	Prevent lateral movement using micro-segmentation

Table 37 Storage Server (Store) log storage for forensic/ audit trail

S/N	Title	Type	Priority	Status	Description	Mitigations
6	log protection	Tampering	High	Mitigated	prevent unauthorised log tampering	prevent unauthorised access to the log server
7	log entry deletion and tampering	Tampering	High	Mitigated	prevent information tampering	prevent information tampering by using ACL

Table 38 Student LMS (Process)

S/N	Title	Type	Priority	Status	Description	Mitigations
19	STRIDE DDOS threat	Denial of service	High	Mitigated	Stop DDOS towards LMS server Block	Use ACL and IP tables for Unauthorised Access

Table 39 Student Portal (Process)

S/N	Title	Type	Priority	Status	Description	Mitigations
31	WEB STRIDE threat.	Denial of service	High	Mitigated	Prevent DDOS attack on port 443	Prevent port Knocking on port 443 and block DDOS against https connection

Table 40 Infected PC (Process)

S/N	Title	Type	Priority	Status	Description	Mitigations
14	generic spoofing attack	Spoofing High	Mitigated malware PMitigated malware PC Prevent spoofing attack	Mitigated	malware PC	Prevent spoofing attack
15	Information disclosure	Information disclosure	High	Open	To extract data from network in a promiscuous mode	Prevent information disclosure

A robust and flexible campus network that addresses the growing need for cyber security challenges can be built by taking into account the goal of the research project, which is to develop an adaptive model to handle various security patterns. This will allow an institution to prioritise planning for cyber threats and to allocate a sufficient amount of resources to safeguard an academic network. An overview of architectural threat analysis on a typical three-layered campus network was made possible by this thorough data analysis of the potential risks that were found during the data collection and analysis process. The study makes it possible to place its findings in the context of earlier research and offers a foundation for enhancing network architecture threat analysis techniques. Our evaluation provides a replication package1 for conducting the search, filtering, and data evaluation, which is freely accessible, along with the lists of search results.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2485

➢ *The Threat Modeling Problem*

Traditional Threat modeling requires brainstorming virtually or physically with experts from the Engineering, Architecture, and Security teams. Using Data Flow Diagrams (Figure 3), the complete solution is illustrated component by component, and one of the several available Threat modeling techniques is applied (STRIDE). The result of this process is a list of probable threats and mitigations.

To create the threat model the following were emphasized: from information gathering, the following actors were considered:

- **The end user --** typical use case: https web browsing Note: though end users may generally have full control over their device, they may not know the underlining problems their workstations can cause until the system CPU usage start rising. In some cases, some are not aware at all.
- **The WAN -** this is usually the exit point out of the network where the entire campus exchange internet bound activities. The device is mostly statically configured to exchange internet request through the upstream provider which is the ISP. The ISP regulate the amount of traffic in and out of the Network in according to what the institution subscribed to.
- **The campus Data Center -** This is the heart-beat of the campus network which is often the command-control center with various network switches serving as access equipment for end-user connection. Other devices which are mainly servers that contains hosted services for both internal and external academic purposes. Remote user device wanting to connect to the campus servers are enforced to use IPSEC-VPN service for high-level secure connection.

Analysis of various threats found are as follows:

Table 41 Assets, Data and Services to be Protected?

1	Web and Mail Servers in DMZ.
2	Database Servers that contain staff and students' credentials, result and other data!
3	Authentication Servers inside the LAN contains user auth details.
4	NIDS/NIPS smart host in DMZ, keep spam/AV/ACL filters updated.
5	in LAN but exposed to Internet, very confidential docs but under close monitoring!
6	IAAS server in DMZ, hosting VMs and Linux Containers and the other test VMs for the Data Center web developers.
7	Wireless APs.
8	E-Library Server
9	2 VPN gateways in DMZ.
10	Cisco Router as ISP WAN gateway
11	Network Switches for LAN (all with various micro-segmentation)
12	Hundreds of wireless APs across campus, all connected to a switch which goes to the internal LAN-connected firewalls.

Table 42 Adversaries and Their Objectives, Skills, Resources, and Risk Tolerances.

	Type/Name	Notes
1	Random worms.	Not out to get us specifically, but might be using new exploits and carrying destructive payloads.
2	Random hackers looking for anything to break into using new exploits.	Not out to get us specifically, mostly script kiddies.
3	Hackers trying to get the CC numbers from our student portal databases.	Bad for us, active profiling and probing, highly skilled, motivated by money, many attempts but the server active ACL blocked all.
4	Hackers trying to get into the LAN through the VPN but they couldn't.	Our site specifically targeted, active profiling and probing, low-to-high skills.
5	Hackers doing DoS attacks for extortion or fun.	Web servers specifically targeted, probably script kiddies, but possibly business adversaries too.
6	Retired employees trying to get remote VPN access, get old mail, or cause problems.	Most probably just want their old e-mail.
7	Current employees trying to get around security, which they find annoying.	Very low skilled, poor skilled users doing stupid things, almost never truly malicious.
8	Hackers hired to steal a copy of student result in order to change CGPA.	Very bad for us, highly skilled, paid, motivated, specific target worth a lot of money, long-term and stealthy effort from them, this will continue forever but administrators must continue to upgrade
9	Random viruses on the workstations of the	Not targeted for us specifically, just "normal" viruses.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2485

	webmasters and admins.	
10	Floods, tornados, power issues, earthquakes and other natural disasters.	Not targeted for us specifically (well, at least probably not).

Table 43 Main Threat Discovered

Description of Threat	Risk Score	Damage	Discoverability	Exploitability	Stealthiness	Repeatability
DoS: SYN flooding, Smurf, other low-level attacks.	39	0	10	10	3	10
DoS: complex search queries, CPU exhaustion.	26	0	5	5	3	5
DoS/Tamper: somehow diddle the data in the SQL Servers.	37	7	3	3	5	5
DoS: upload GBs of data to take up all free space.	35	0	5	10	3	10
DoS: fail to auth to VPN to lock out user accounts.	43	0	10	10	5	10
DoS: fail to auth to wireless to lock out user accounts.	41	0	8	10	5	10
Auth: guess username and password to VPN.	35	5	5	5	5	5
Auth: guess username and password to wireless.	35	5	5	5	5	5
Auth: guess username and password to authentication server.	35	5	5	5	5	5
Auth: highjack live web sessions.	35	5	5	5	5	5
Auth: trick VPN/AP into using a less secure auth protocol.	35	5	5	5	5	5
Auth: spoof hacker's source IP/MAC address to bypass firewall.	35	5	5	5	5	5
Auth: sniff credentials in transit over network.	35	5	5	5	5	5
Auth: crack sniffed credential data, like password hashes.	35	5	5	5	5	5
Auth: bypass requirement to authenticate at all on IIS app.	35	5	5	5	5	5
Auth: use malware on users' computers to steal passwords.	35	5	5	5	5	5
Elevation: trick web apps into executing commands.	35	5	5	5	5	5
Elevation: buffer overflow exploits to IIS apps.	35	5	5	5	5	5
Elevation: buffer overflow exploits	35	5	5	5	5	5
Disclosure: cross site scripting (XSS) attacks to Web applications.	35	5	5	5	5	5
Disclosure: SQL injection attacks to web apps.	35	5	5	5	5	5
Disclosure: directory browsing and travesal on web.	35	5	5	5	5	5
Disclosure: crack SSL encryption on sniffed HTTPS packets.	35	5	5	5	5	5
Disclosure: crack IPSec on sniffed VPN packets.	35	5	5	5	5	5

Disclosure: extract keys from Web/VPN servers.	35	5	5	5	5	5
Disclosure: extract credit card data from Databse Servers in DMZ.	35	5	5	5	5	5
Disclosure: extract password hashes from Auth in DMZ.	35	5	5	5	5	5
Tamper: corrupt transaction data in SQL Servers.	35	5	5	5	5	5
Tamper: capture and replay packets for a transaction.	35	5	5	5	5	5
Malware: upload and execute binaries or scripts.	35	5	5	5	5	5
Malware: trick servers into downloading and running EXEs.	35	5	5	5	5	5
Malware: disable anti-virus scanner without detection.	35	5	5	5	5	5
Malware: open listening backdoor port without detection.	35	5	5	5	5	5
Malware: execute existing binaries with arbitrary arguments.	35	5	5	5	5	5
Stealth: edit log data.	35	5	5	5	5	5
Stealth: evade IDS signatures.	35	5	5	5	5	5
Stealth: modify files without detection.	35	5	5	5	5	5
SE: trick workstations into changing a password.	35	5	5	5	5	5
SE: trick admins into installing fake patches/updates.	35	5	5	5	5	5
SE: trick admins to changing the firewall rules.	35	5	5	5	5	5

V. CONCLUSION

In conclusion, the evolving attack surface and new vulnerabilities developing daily make it inefficient to perform Threat modeling frequently during a release but Network Administrators and Web Developers must continue to stay updated.

ACKNOWLEDGMENT

The authors wish to appreciate the Director and Staff of the Computer Resource Center, Federal University of Technology, Akure for their support during the data collection process and also, TETFUND IBR (TETF/DR & D/CE/UNI/AKURE/IBR/2022/VOL.II) for supporting the research.

REFERENCES

[1]. Chen, M., Wang, J., Mao, J., & Li, J. (2013). Assessing the Security of Campus Networks: The Case of Seven Universities. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7795939/
[2]. Du, J. (2023). Exploring the path of network security and student privacy protection in smart campus based on Markov model.
[3]. Ismaila, R., Hassan, R. A., & Awang, A. M. (2018). Campus Network Security: Threats, Analysis and Strategies.
[4]. Jones, D. W., & Lee, J. (2020). The Efficacy of Security Controls in Mitigating Risks Associated with Student-Owned Devices on Campus Networks.
[5]. Li, S., Liu, Y., & Wang, H. (2020). Research on the Development Trend and Protective Measures of Campus Network Security in Colleges and Universities.
[6]. Liu, Y., Jing, L., & Wang, Y. (2017). Research on Campus Network Security Problem and Protection Strategy.
[7]. Smith, A., Hancock, P., & Southgate, V. (2018). A Risk Management Framework for University Networks.
[8]. Wu, X., Liu, Z., & Wang, H. (2020). The Construction and Implementation of the Security Defense System of University Campus Network.