Original Research Article

ENHANCING THE DESIGN OF A SECURED CAMPUS NETWORK USING DEMILITARIZED ZONE AND HONEYPOT AT UEW- KUMASI CAMPUS

ABSTRACT

The increasing complexity of information systems, as well as the rapid development of new vulnerabilities and exploits, the security of campus networks needs to be hardened to minimize or eradicate security flaws.

Aim: To discover the vulnerabilities and enhance the creation and deployment of secured campus network.

Place and Duration of study: University of Education, Winneba – Kumasi campus**.**

Methodology: The integration of De-Militarized zone and Honeypot techniques was used to beef up the security of the campus network against vulnerabilities and exploits. Penetration testing was used in the assessment of the University of Education's network infrastructure, and to demonstrate attacks and intrusion into the network infrastructure.

Results: Two firewall DMZ architecture techniques protect sensitive resources of the campus network by sanctioning the inflow and outflow of traffic, determining which segment allow and disallow traffic, whiles the Honeypot techniques were configured to keep the attention of attackers diverted from the main network, the full strength of an attack, until the administrators are prepared to put the effective counter in place. The fusion of DMZ and, Honeypot provide the System Administrators to effectively management the security of the campus networks.

Conclusion: Honeypots are used to detect vulnerabilities based on the attacker's behaviour and, data collected by honeypots can be used to enhance other security technologies. The fusion of DMZ and Honeypot into the security models of the campus network made it more robust.

Keywords: *Campus Network, Attacks, Threats, Vulnerability, Honeypot, De-Militarized zone, Penetration test*

INTRODUCTION

Almost every tertiary institution is using information technology as a leading strategy but not as a tool alone, for the best network infrastructure and implementation. The university's increased use of information technology necessitated a solid technical infrastructure and network architecture to ensure optimum performance and efficiency. According to [1], a university network is a significant instrument for communication, and collaborative studies, both of which

are essential for fostering a sturdy learning culture, and efficaciously assisting the academic requirement.

Ghana's University of Education, Winneba is one of the best tertiary institutions in Ghana. The university has four campuses situated in four towns but two regions. All the major resources (servers) for internet connectivity are located at the main campus. The evolution of Networking and the Internet have given way to a rise in threats to information and networks. The threats and attacks cause damage and theft to the network system. Due to the obvious benefits derived from such technology, countless applications have become more pervasive on the internet.
Cos of the vulnerability, which can be induced by inadequate software and hardware settings, poor network architecture, inherent technology weakness, or end users' carelessness, assaults were indeed persistent.

These networks consist of routers, switches, and firewalls [2].
Many services may be enabled by default on a router.
Most of these services are redundant, and an attacker could use them to obtain intelligence or exploit a victim.
Routing and firewall operations should be carefully managed and audited to mitigate network downtime, improve security, and prevent attacks, hackers, and network threats, as well as aid the analysis of alleged security lapses.
Due to the pseudonymous nature of cyber, the news headlines on the local news channel used every day complaint about this same current computer security threats from virtually uncertainties.
Cybercrime is on the upsurge, with phishing scams, spyware, identity theft, and internet scavengers targeting innocent victims. As a direct result of targeted attacks, we have noticed overtures by hackers to change the status quo of computer system information.

Though all campus networks are designed and secured, most attackers have learned about these techniques and succeeded in invading the network system to damage or steal vital information.
The ever-increasing population of students and staff contributes to the vulnerability of the network system.
However, given the sensitive nature of the data and resources available on campus networks, it is beneficial to improve the architecture and implementation of a secured campus network to preclude intrusion and unauthorized access to information and resources.

This can be enhanced by the configuration of hybrid Demilitarized zone (DMZ) and honeypot techniques to beef up the security of the campus network. The functionality of DMZ and Honeypot have the tendency to make the campus networks strong and confident.

2.0 Literature Review

2.1 Overview of Campus Network

[1] cited [3], defined campus network as connectedness of network systems in a contained environment, such as a university or organization premises.
The link-up or interconnection of various Local Area Networks (LANs) within the university community or corporate environment, is referred to as campus network.
Campus networks can connect a wide range of structures, including office buildings, university libraries, faculty and departmental buildings, and residential halls. The location of buildings on the campus will greatly influence the kind of network connecting devices and network transmission media to be used.
Campus networks are designed to provide the users in the university community to have easy access, distribution, and control of information and data.

The hierarchical architecture model reduce the complexity by breaking down the network into three major parts: access network, distribution network (convergence / aggregation network), and core network (backbone network), all of which are simpler, smaller, and easier to manage [1].

2.1.1 Secured campus Network

[4], proposed a secured campus network that could mitigate the security weakness in a campus network.

The proposed design involves the configuration of VLAN, VPN, and implementing a firewall for internal and external security – DMZ.

VLANs divide a network logically, generating new access points that efficaciously alienate data packets from the network segments, whereas improving the network's throughput, accessibility, and confidentiality.

Campus VPN offer a complete tunnel VPN service, which is a cryptographic logical link to the network from off-campus.

On a secured network, a firewall screened and blocks or allow network activity, both inbound and outbound. It blocks unauthorized access to incoming traffic and influences specific outgoing traffic. In the outgoing direction, all protocols and ports that may entail a potential threat are obstructed.

It is of great importance that many studies including dissertation and thesis writing are set in a well-defined concept. The importance of defining the concept is to put the study in the appropriate perspective, thereby actively engaging readers to enhance their understanding and interest. It is in this regard that the study is set to focus on the campus network and its security models.

The security of a campus network needs not to be compromised since it hosts different categories of users, according to researchers at the University of Bath and Northampton (Bath) They claim that all information, software, and hardware need to be protected from intruders, attackers, and hackers.

The study is set to focus on the campus network and its security models. The importance of defining the concept is to put the study in the appropriate perspective, thereby actively engaging readers. It is in this regard that the study will be based on a well-defined concept.

Address Resolution Protocol (ARP) inspection, Dynamic Host Configuration Protocol (DHCP) snooping, Port security (PortSec), Private Virtual Local Area Network (VLAN), Time-based Access Control Lists (ACLs) encryption of routing protocol, and firewalls are all examples of campus network cryptographic protocols. Each security service has its own set of capabilities and features.

Time – based ACLs allow network access for a set number of times. Administrator can configure port security on individual switchports to allow only certain range of resources [1].

[1]cited [4], proposed "Network architecture with security mechanism for campus networks" as the ultimate goal. Network architecture and security are very important in deploying a university campus network. The above-mentioned security mechanism can be enhanced by deploying IDS and IPS, DMZ, IPSEC, and Honeypot that will make the security more robust.

An IDS encapsulates packets in real-time, workflow them, and can react appropriately, but it uses credentials to detect suspicious transactions on copies of data traffic. An Intrusion Detection system permits some nefarious traffic to pass prior to actual responding to secure the network in the detection process of malicious activity. In order to react to an invasion, an IDS frequently needs help from other

networking devices like routers and firewalls [5].

According to Network Security Using Cisco IOS IPS book (chapter 6: page 437), An IPS protects against malicious actors in live time working concurrently inside the ciphertext.

Packets are disallowed to access the reliable edge of the network cos of IPS. IPS performs a more thorough assessment, allowing it to detect, stop, and restrict threats that otherwise transmit through a perimeter firewall. Whenever a packet enters into one of the IPS interfaces, it is not let into the outgoing or trusted interface until it is ascertained to be safe. The IDS and IPS work together to achieve optimum results.

Security management of campus network is not just the responsibility of only few technicians; it must be incorporated into the action plan of college and university administration as well as the collaboration of the entire college and university's faculty, staff and students [5].

2.1.2 Router and Firewall Security Policy

Routers connect two or more local networks within an entity, as well as corporate route. The data transfer that the inside routers forward between networks may be subject to restrictions typically, the router will forward traffic across multiple networks known as "autonomous systems". The traffic between such varied networks make up the internet is directed by core network routers.

A firewall is a rapid technology roadblock that protects communication networks or host from unauthorized or unwarranted connectivity. It can defend a network against intrusions by inspecting all datagrams of the conversation trying to pass via system and denying those that do not comply with the security standards.

The concept of a security function against a network intrusion which is a protection mechanism. In the firmware region of the router, the security engine provides security protocols such as packet filtering, authentication, access control, vulnerability analysis, and audit trail [6]. At layer 2,3,4, and 7, routers and firewalls support a wide range of network services.

Almost every type of network traffic conceivable is carried by campus networks. Faculty and staff computer systems are consistent with those reported in any workplace, but in higher education, they are only the cherry on top of the ice. Students use same connectivity that connect temperature sensor and research equipment to connect game consoles, smart assistants, cameras, and smart microwaves.

A one-size-fits-all network would be impractical given the level of diversity. Running subnetworks for all those applications, however, would be prohibitively expensive. Subnetting is a trick that networking and security experts have up their sleeves.

Administrators can use this strategy to create logical networks that run on the same physical infrastructure as one another. Even though a student's laptop and scanning electron microscope are both connected to the same switch, they are logically separate. Depending on the needs and priorities of the campus, segmentation allow each device to operate under its own security policies, and provide a different level of service [7] .

2.1.3 The Use of Network Admission Control to Automate Traffic Assignment

Switches and firewalls are the most common devices used by colleges and universities ti deploy network segmentation. At the network's edge, switches provide access to individual devices before consolidating traffic from higher-level switches.

Administrators can create Virtual Local Area Networks (VLANs) to isolate devices from one another using modern switches. On a switch, administrators might define four VLANs for faculty/staff, students, guest, and infrastructure for example.

According to [7], when a switch, network admission control (NAC) technology integrates it to ascertain where it should be placed. Once a device is connected to a VLAN, it can only communicate with other devices on the same VLAN.
VLAN trunking technique is used by network administrators to transmit the same network across campus switches. This means that infrastructure, and students' devices can communicate, but on communication between devices on different VLANs is permitted, even if they are connected to the same switch.

2.2 Security Issues in a campus Network
Vulnerability, threats, and attacks are three terms commonly used when addressing network security. Vulnerability is a flaw that exist in all networks and devices. Routers, switches, desktops, servers, and even security devices fall into this category [2].
There are three primary vulnerabilities or weaknesses, according to [2], which are :

a) Deficiencies in technology:

   computer and network technologies

   have inherent security flaws.

   TCP/IP flaws, operating system

   flaws, and network equipment

   flaws are all examples.

b) Weakness in the configuration

c) Flaws in the security policy.

There are numerous types of network attacks and security threats, as well as network attack methodologies and classifications.
Any method, process, or means used to maliciously attempt to compromise network security is referred to as a network attack. An individual will attack a corporate network for the following reasons: stealing data, altering stored data, stealing software, stealing hardware, and abusing user accounts and privileges are all examples of data theft. Running code to destroy the system, damaging or corrupting data, and preventing a legitimate authorized user from accessing network services and resourcing, among other things.
Passive communication monitoring, active network attacks, close-in attacks, insider exploitation, and threats through the service provider are all possible attack types [8].
Passive attack, Active attack, Distributed attack, Insider attack, Close-in attack, Phishing attack, Hijack attack, Spoofing attack, Password attack, and ARP spoofing attack are just a few examples of network attacks.

Anything that has the potential to harm a computer system is classified as security threat, viruses, trojan horses, back doors, and outright hacker attacks are just few examples of potential threats.
Internal or external security threats exist. Internal security threats include Denial of Service (DoS), which brings all external services, such as web, email, and FTP, to a halt, rendering them unusable; network user attack, which affects the firewall's internal segmentation, which can help contain the damage; and web virus, which infests the system reading email and spread throughout the organization. Email with viruses is an external threat, as is a webserver attack threat, which could give an attacker access to other internal network systems; and a network virus, which can enter through unprotected ports.

2.3 The analysis of the current situation of Campus Network Security
Aside from the virus's regular appearance, campus network must contend with three major security threats.
The firewall's drawback include: many campuses only have a layer barrier-firewall installed, but this firewall has numerous limitations. The firewall is a

passive defense device, and the campus network has a number of obvious flaws, such as these firewall limitations.

Honeypot technique is a type of active defense that can help the campus network avoid being attacked [9].

Internal attack: according to relevant material's statistics, insider attacks account for more than 80% of campus network attacks, with computer universality, curious or motivated student eavesdrop on someone else's code and other important information [10]. Malicious attacks on the school management system are harmed by this mischief.

Hacker attack: The internet is a network that connects two gateways. Many campuses have "heavy technology, light safety, light management" tendencies as a result of safety concerns and capital constraints, and campus network builders often overlook security issues and only setup one firewall. Cos of these flaws, hackers can use the campus internet connections to create an inverse school network, causing serious damage to the system and data [9].

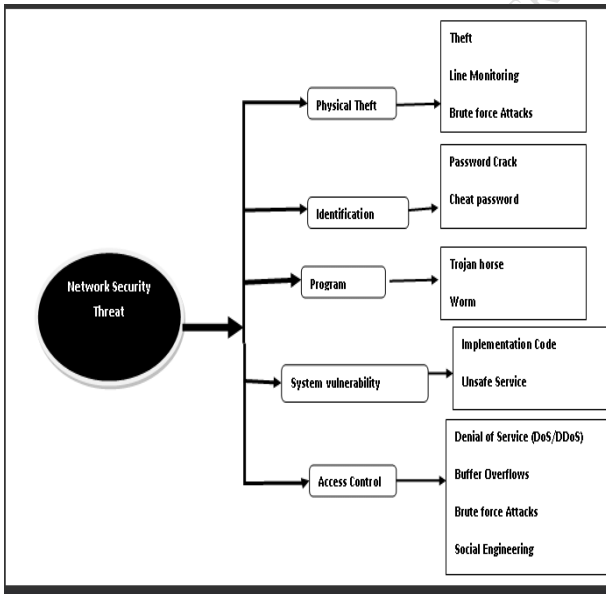

Figure1 Network Security Threats

The above figure 1 is the graphical representation of the classification of network security threats and their main target operation.

As cited by [11], the type of media to be used between buildings, outside cable specification, rights-of-way, avoidance of natural barriers, underground or aerial cabling requirements, line of sight for interbuilding wireless transmissions, and security issues are all issues that are associated with campus network.

As cited by [11], if a cable is open in a campus network, it can be tapped or cut. Since many internal resources are available as corporate user.

Quite some assaults on the network begins within the firewall. This also signifies an attacker infiltrate a node on an organization's connectivity, to access the entire internal network conveniently, as a result of poor network security configuration.

2.2 Some current Security Solutions to campus network threats

According to [11], firewall technique, Virtual Local Area Network (VLAN). Strong encryption, multiple server-side operating systems, and so on, can be adopted to mitigate poor network security in the campus network.

In campus networks the use of virtual private network (VPN) technology helped in configuring each node's VPN client to encrypt network traffic between a computer and a VPN concentrator on the campus network.

However, on most campuses VPN is already present.

More so, VPN can assist a member of campus computer to connect securely. Since WLAN (Wireless Local Area Network) reduces the workload of the network cabling, it is an integral component of the campus network. Thus it must be monitored, managed well, and centralized configuration.

Formulation of systems and specifications for network security must be strengthened. "Any user, user group, or department wants to establish its local area network or to establish connectivity to external data communications networks must assign a member of that user group or department to coordinate with Network Services and obtain approval" as quoted by [11]. Within

the campus network, colleges and administrative units can create sub-domains. These sub-domains must incorporate manifold

As cited by [11], at least two of the operating systems with different kernel architectures should be set inside the server central core in the pipeline, enabling all traffic to pass through it, and task analysis should be performed separately on both systems. Again, all redundant ports must continually be disabled on the server.

Additionally, to safeguard all conceivable virus admittance from the internet, network virus protection instruments must be effective and regularly updated. For online virus detection, virus cleanup, and virus tracking. An anti-virus application should be installed. Intrusion detectors must be installed at campus network perimeter to detect infested computers and mean traffic entering or exiting the campus network [11].

To detect infected computers attempting to scan or join nonexistent hosts, a network honeypot should be placed on an idle network section [10]

2.4 The Use of DMZ and Honeypot to enhance Network Security

This study advocates the hybrid of honeypots and DMZ as effective security model tools to enhance the mitigation of issues in network security.

A DMZ is a typical or logical subnet that divides an internal Local Area Network (LAN) from other insecure networks, most commonly the internet [12].

This segment of the campus network houses the webserver. The idea is to logically separate hosts in the DMZ section from outside network segment.

The DMZ configuration gives complete control over network traffic flowing from the internet to the webserver, as well as traffic flowing from other network segments [13].

The webserver listens on Transmission Control Protocol (TCP) port 8080 instead of 80, and the webserver's listening socket must not be altered; instead, the Destination Network Address Translation (DNAT) rule's Port Address Translation (PAT) functionality is used to alter the target port of IP packet traversing through the firewall. To allow HTTP traffic from the internet to reach the webserver in the DMZ , an cess rule is created.

2.5 Campus Security using Honeypots

Honeypot is a decoy that are closely monitored, and used in a network to track down hackers, and alert network administrators of a possible new threat. Honeypots are classified based on where they are placed, and how they are involved.

Honeypots are classified as production honeypot or research honeypots based on their implementation. Honeypots are categorized as pure honeypots, high-interaction honeypots, or low-interaction honeypots depending on the design metrics.

production honeypots are placed inside the server farm with other application servers by an initiative to enhance their overall state of security. They capture only limited information and are primarily used by enterprises or corporate entities.

Honeypots are used to gather information about the Black hat community's motivation and tactics when they target different networks. These honeypots are used to gain more knowledge about the threats organizations face, and how to mitigate them.

Research honeypot are used mainly by military, government units or researchers, to collect extensive data [14].

Honeypot technology, according to [15], is a very efficient instrument to use. Honeypot configuration discovers, analyze, records the invader behavior, and take defensive strategy. When integrated with the current state of the campus network security, the initiation of honeypot technique as an active defense in network security, is increasingly playing important role in the protection of campus network security [10]. The honeypot

technology provides enhanced network safeguards for the campus.

High-interaction honeypots replicate the activities of real systems that host a variety of services, allowing an attacker to waste time with a large number of services. Honeynet is a perfect example.

Low-interaction honeypots only replicate the services that threat actors recurrently request . An example is *Honeyd*.

Honeypots are cost-effective way to improve an organization's security infrastructure. It is effective tool for network forensics and intrusion detection, though it is not an outright panacea for security breaches. Honeypots are widely used by the research community to study network security issues such as internet worms, spam control, DoS attacks, and so on.

This technique is known as "bait and switch," and it allows the administrator to choose whether data should be sent to the server farm or to the honeypot network. This approach is used to detect worms in the campus network.

In cha campus network it plays the role of a firewall and an Intrusion Detection System (IDS) or an intrusion prevention system (IPS). The network is composed of the following devices and configurations:

(a) A DSL router, which connects the lab to the Internet via a DSL connection;

(b) A dual-homed software router/firewall (Pascal), acting as the gatekeeper between the network and the outside world;

(c) A regular switch connecting the DMZ (*Demilitarized Zone*) to the server cluster;

(d) A DMZ that contains publicly accessible servers (such as a Web server) and testing workstations (e.g., for monitoring network traffic, etc.);

(e) A 2nd router/firewall (Einstein) separating the DMZ from the server cluster;

(f) switch connecting the 2nd router/firewall with the back-end servers;

(g) A set of network security servers, including firewalls, VPN server, IAS (Microsoft's Internet Authentication Server), and Radius server;

(h) A testbed of computers, which are equipped with swappable disk units and are connected via a VLAN switch and routers.

Currently, the prototype network consists of two routed-Virtual LANs, which are useful for simulating several network configurations. The honeypots experiments were performed using the testbed machines in VLAN and Newton, which is the test machine in the network.

2.6 Methods of discovering Vulnerabilities

This presupposes there are vulnerabilities with the existing security models used or implemented in the campus network.

By discovering the vulnerabilities and exploits that exists within the computer network infrastructure, a penetration test can give Network and System Administrators a holistic view of the security posture [16].

To discover and verify vulnerabilities, the penetration test was used to establish the network's level of security against network-based assaults in order to improve information system security.

Running a penetration test requires the tester should be aware of the testing environment and use a structured approach to perform the test. This enables a deeper understanding of the system or network to be tested.

A penetration test can be conducted in three different approaches: white box, black box, and Grey box.

White-box test- the tester is provided with a thorough understanding of the target network or system's infrastructure. This testing could be viewed as genuine test or an attack by an insider with knowledge of the systems. A white-box penetration test's primary purpose is to supply information to the tester so that he can get insight into the system, and deploy the test based on his prior knowledge . for

example, in a white-box infrastructure penetration test, information such as network diagrams, and infrastructure details are provided , as well as the source code of the application and design information, among others, as is in the case of an application penetration test.

Black-box test: This testing can be viewed as a simulation of a real-world external attack. The tester is completely unaware of the target network system's infrastructure. Ethical hackers or testers must obtain information from public sources and examine everything from the ground up to uncover flaws. For black-box testing, the stages of mapping the network operating system fingerprinting, enumerating shares, and services are typical example. A black-box penetration test identifies system flaws that can be exploited from outside the network [17].

The integrated (Black-box and white-box) methodology gives valuable insight from both internal and external security perspectives. This testing can be thought of as a realistic simulation of an outside attack, hence Grey-box testing. The tester has no prior knowledge of the target network system's infrastructure. To find problems, ethical hackers or testers must get data from public sources, and investigate everything from the ground up. Processes like network mapping, operating system fingerprinting, and enumerating shares and services are common components of black-box testing. A black-box penetration test identifies system weakness that can be exploited from outside the system.

According to [18], Grey-box penetration testing was chosen since it aids in the elimination of any internal or external security flaws within the institution network infrastructure environment that an attacker could exploit. In terms of cost, it saves time for the penetration testers to unearth publicly available information.

3. METHODOLOGY

The method of investigation chosen by the researcher for the assessment of the campus network and systems is penetration testing.

The three penetration-testing methodologies can be compared in terms of speed, efficiency, and coverage. The most time consuming and extensive sort of penetration testing is white-box testing. Overall, black-box penetration testing is the quickest way to test for vulnerabilities. Although testers lack information needed to target, their attacks on the most high-value or potentially vulnerable targets, the limited information available to them raises the likelihood of vulnerabilities being overlooked and diminishes test efficacy [17].

However, Gray-box testing sacrifices a little speed in favour of better efficiency and coverage as compared to the black-box testing. Compared to black-box penetration testing, this test delivers a more targeted and efficient examination of a network's security.

A gray-box testing approach was used to execute a penetration test on a campus network. To reduce the risk of harm to the campus network system, the proposed approach was used.

The network infrastructure was examined at the University of Education, Winneba – Kumasi campus, where the evaluation and penetration testing were conducted. The decision was based on the tester's experience with the institution, and its IT and network systems as well as the prospect of acquiring permission and network access because the tester is an employee of the institution.

The penetration test was carried out from two major test sites chosen to allow the analyst to mimic an attack from both within the university's network and from a remote point outside of the university's network.

Learning and understanding what penetration test is, how penetration methodology may be followed, and which tools and techniques can be utilized are all part of conducting the penetration test on the campus network. In deploying the penetration test against the UEW network, a proposed four-phased penetration testing technique based on the methodology designed by the US National Institute of Standards and Technology (NIST) was used.

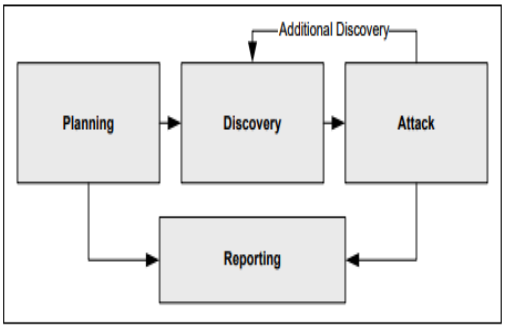

Figure 2: Four-Stage Penetration Testing Methodology

This method graphically displayed in figure 2, addresses penetration testing from a project management standpoint, in which the entire test is considered as a single project with associated tasks spanning the planning, execution, and reporting stages.

Stage1: The Planning Phase

The planning stage is crucial to a successful penetration test. During this phase, no actual testing takes place. Four primary actions were carried out during this phase: *Initiation, Tool selection and setup, and Intelligence gathering*.

Initiation: The test objectives, scope, legal restrictions, authorizations, and assignment scheduling are determined and formulated.

Selection and setting up of tools: The analyst chose Linux kali, which is developed specifically for offensive system security. Kali offers all penetration testing tools, and the approaches to be employed, include the Network services test, client-side test, and wireless security test, all of which are suited for the university environment and would improve the test's accuracy.

Intelligence gathering: passive and active reconnaissance strategies were used in order to be successful at the intelligence gathering. Various type of searches, such as web presence, Network enumeration, and Domain Name System (DNS) – based reconnaissance was used to unearth the information about the university's systems, employees, physical location, and business activity, without connecting directly to the network. Nmap was heavily utilized for network survey, port scanning, operating system, and service enumeration during active reconnaissance. Nmap, alongside other essential utilities are pre-installed in Linux Kali.

Stage 2: The Discovery Phase

There are two sub-stages (Vulnerability Identification and Vulnerability Assessment) in this phase.

Vulnerability Identification is the data collection process, which includes data collection and scanning. To identify possible victims, network ports and services are identified. Other techniques are utilized to obtain information on the targeted network in addition to port and service identification.

Vulnerability assessment is seen as an important part of the penetration testing. The information gathering during the vulnerability scanning and identification stage can be used to conduct additional investigation into the vulnerabilities detected. Information regarding the vulnerability would be gathered from the internet and other vulnerability databases, such as the National Vulnerability Databases (NVD), and a priority list of all detected vulnerabilities would be documented.

Stage 3: Attacked Phase (Exploitation)

All identified vulnerabilities were reviewed to see if they could be exploited or not. The Metasploit framework was used to exploit vulnerabilities that were

publicly available for exploits. The exploits were carried out from an internal location within the university's network and a remote location outside the network of the university community.

Stage 4; Reporting Phase

It was prepared a list of all the actions that were completed in each of the previous phases. The reporting phase happened concurrently with other stages and at the conclusion of the attack phase. This reporting phase was done to reflect the actual discovery of the tests and the vulnerabilities it identified.

Before the proctored exams, each stage of the test and its logistics are arranged. This method was chosen as the best for conducting penetration tests in a university setting because it not only allows the tester to plan out his activities and follow a logical approach, but it also improves the test's repeatability. As a result, the test is being carried out in a live environment. Careful planning was required to avoid any unforeseen consequences .

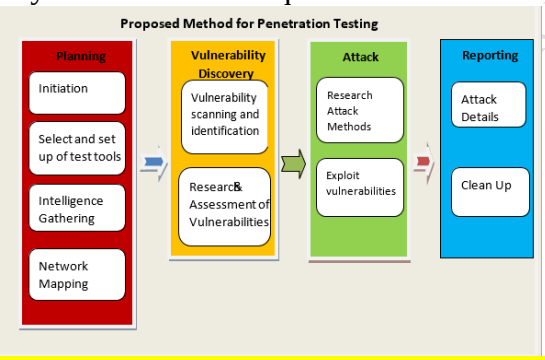

Figure 3 Proposed Methodology for Penetration Testing

The method employed for the testing, as well as the many phases that occur during penetration testing are graphically presented in figure 3 above. To uncover and determine the possibility of exploiting the vulnerabilities, the same methodology, tools, and techniques might be applied for other academic systems or networks.

4. ANALYSIS AND DISCUSSION OF RESULTS

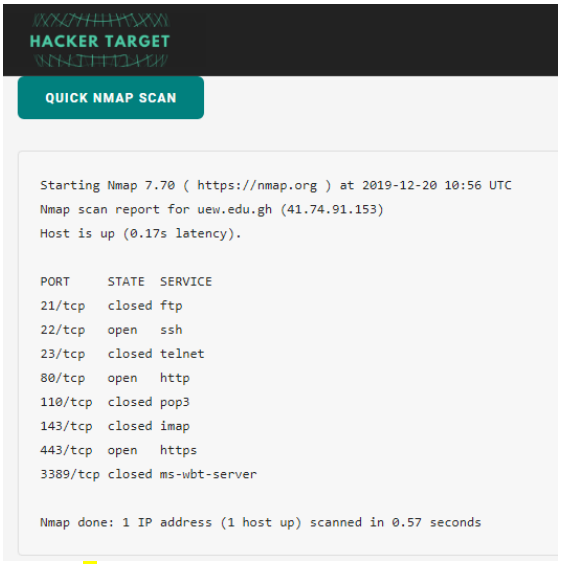

Figure 4 NMAP Report on Port Scan

In figure 4, it can be seen that some ports are closed and others are opened. The opened ports are 22, 80, and 443. These ports are opened to provide specific services like ssh, and HTTP. Port 22 uses SSH for remote login. Port 80 is for the world wide web (HTTP) connection.

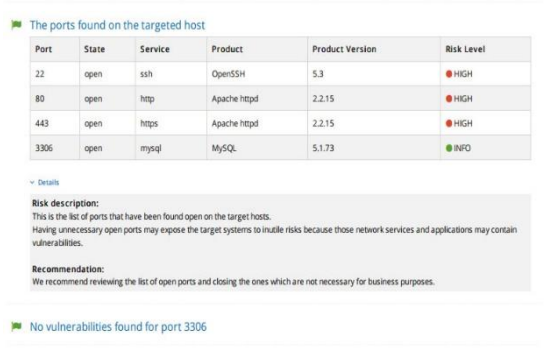

Figure 5 Ports found on the target host (UEW)

The above figure 5, displays the state of the ports and their risk levels. It is evident from the scan that ports 22,80, and 443 have a high risk of vulnerability since their ports were open. When ports are opened it may expose the target system to the risk of attacks. Most especially when these ports may contain network services and applications that may be dangerous in the

hand of a vicious person. However, no vulnerability was found on port 3306.

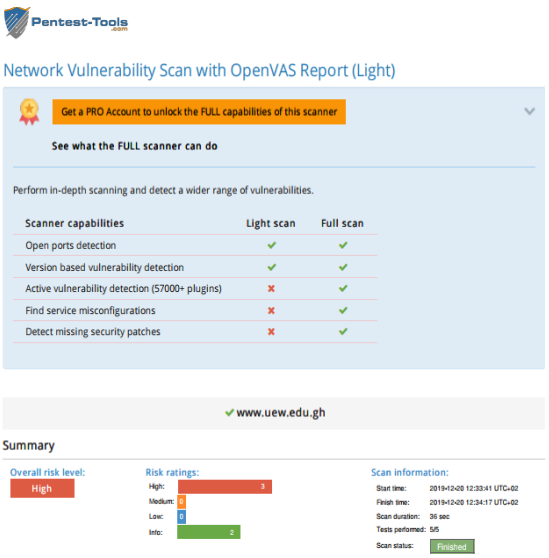

Figure 6 Network Vulnerability scan report for UEW

Figure 6, presents evidence from the port scan analysis affirming the vulnerability of the UEW campus network and susceptibility to attacks.

Table 1 Open Ports found

Port	State	Service	Product	Risk Level
22	Open	Ssh	openSSH	High
80	Open	http	Apache httpd	High
443	Open	https	Apache httpd	High
3306	Open	Mysql	MYSQL	Low

Table 1 is a display of open ports and their services and risk level. This is the tabular representation of figure 5.

4.2 Findings

4.2.1 Security of the Campus Network

The penetration tests conducted on the campus network of UEW indicate that the security of the network is not all that secure against vulnerabilities such as attacks and risks.

Ports are the first doors knocked on by attackers. If found open, they can become a real threat if the services you are running on them are not properly hardened from a network, operating system, and software application point of view. Every network port is potentially risky and no port is natively secured.

SSH and port 22 can be simple targets if passwords are weak. When the credentials include default or easily guessed user names and passwords. Port 22, the designated Secure Shell port that provides access to remote shells on physical server hardware, is susceptible [19].

HTTP traffic uses TCP port 8080, 8088, and 8888, according to [19]. The servers connected to these ports are mostly outdated machines that have been left unmanaged and unsecured for years, accumulating escalating vulnerabilities.

By default, SSH listens on port 22, which implies that if an attacker discovers port 22 open, he can use it to connect the host system [20].

In both tests, it was realized in figure 4 and figure 5 indicate that there were four ports opened and susceptible to attacks, thus may be vulnerable. Eventually, this assessment of the UEW network has exposed the security challenges concealed in the network.

The above findings show the need to enhance the campus network of UEW in other to make the security of network service, applications, and other resources more robust.

4.3 The design of secured campus network using DMZ and Honeypot

The campus network will have two firewalls with a demilitarized zone demarcated in between the two firewalls. Within the demilitarized zone, the webserver, and the honeypot device will be stationed there. On the other side of one firewall is the actual Local area Network and on the other side of the next firewall is the gateway router.

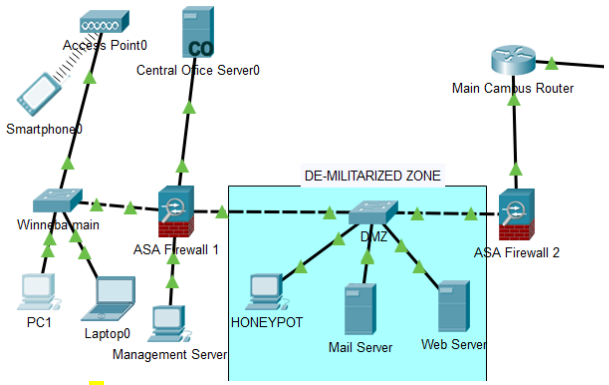

Figure 7 Enhanced Campus Network Design

Figure 7 is the design of the enhanced secured campus network proposed to mitigate the vulnerabilities and attacks.

4.3.1 De-Militarized zone configuration

The most important DMZ access criterion is as follows: Web Server (in DMZ with IP 41.74.91.153) should have only HTTP and HTTPS access to the unsecured internet. The remainder of the traffic should be shut down. The DMZ web server should be able to connect to the SQL server on the internal network, but all other traffic should be banned.

STEP 1 – allow certain traffic to pass through the DMZ and into the network. All other traffic from the DMZ to the inside must be denied.

STEP 2 –allow only certain types of traffic to pass across the DMZ to the outside world.

STEP 3 –Block Everything else.

4.3.2 Setting up the Honeypot on Cisco platform

The researcher wrote a rule for the incoming access list, under which all attempts to get from the Internet to the telnet port of our devices fall. At the end of the rule, a unique label "HONEYPOT_UEW" is affixed. According to it, then we will look for triggers in the log.

```
IP access-list extended ACL-WAN-In
   … deny TCP any eq telnet log
         HONEYPOT_UEW …
```

It's crucial to pick the correct trap criteria.

Connection from the outside is on port 23 (telnet). In this case, the object group will be instantly filled with the IP addresses of bots from all over the Internet, and the memory allocated for access lists will simply end. To catch attempts to access any one of the devices port 22 (SSH) is used. This is an order of magnitude smaller than telnet.

A large number of bots climbs on port 7547, trying to connect using the CPE WAN Management protocol.

Another option that could be used to catch attempts to use the Smart Install Client, enabled on port 4786.

Again, a trap was mounted on port 80 by selecting an IP address outside the segment where the webserver is configured. The idea is that the search engine robots should not fall into it.

This is an example of a trap on an IP address [10.1.2.10].

```
IP access-list extended ACL-WAN-
In … deny TCP any host 10.1.2.10
   eq www log HONEYPOT_UEW2 …
```


4.4 RESULTS FROM IMPLEMENTATION

4.4.1 Log Analysis of the Honeypot Configuration

Logging on the router, must be enabled, then something like this gets into the log:

```
225435: Jan 20

09:45:17.826: %SEC-7-

IPACCESSLOGP: list acl-WAN-

In denied tcp
```

```
172.19.32.12(59472) ->

10.10.2.9(23), 1 packet

[HONEYPOT_UEW]
```

It was observed that from an external IP address [174.19.32.12] An attempt was made to contact the 23rd port of our IP address [10.10.2.9]. The label "HONEYPOT_UEW" in the line is also present. By the way, [174.19.32.12] is an attacker caught while writing running this study.

To analyze the log, Embedded Event Manager (EEM) - a tool for automating tasks and customizing software behavior built into Cisco IOS was used.

In the configuration mode of the router, an applet was created to analyze the log and, while in the logline of the "HONEYPOT_UEW" tag, cuts the attacker's IP address and adds this address to the Blacklist object group.

When the next line with the label

```
event manager applet honeypot
event syslog occurs 1 pattern
"HONEYPOT_UEW" action 100 regexp
"([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+)"
"$_syslog_msg" result IP_address
action 200 if $_regexp_result eq
"1" action 210 cli command
"enable" action 220 cli command
"conf t" action 230 cli command
"object-group network hosts-
BlackList" action 240 cli command
"h $IP_address" action 250 cli
command "end" action 260

syslog msg "IP address $IP_address

added to blacklist" action 270 end

action 300 cli command "exit"
```

"HONEYPOT_UEW" occurs in the log, an event; in the event handler itself, from the logline using the pattern "([0-9] + \. [0-9] + \. [0-9] + \. [0-9] +)", the attacker's IP address is cut out and assigned IP_address variable (action 100); if the address is successfully cut out, and no problems with parsing the string happened (action 200), then console commands are executed that add the IP address to the object group (action 210 - 250); A trap is written to the log (action 260).

4.4.2 Analysis of De-Militarized Zone Configuration

All traffic from the inside (VLAN 2) to the DMZ was blocked, but traffic from the DMZ to the inside was permitted.

However, specific traffic from the DMZ to Outside was allowed and all other traffic was blocked.

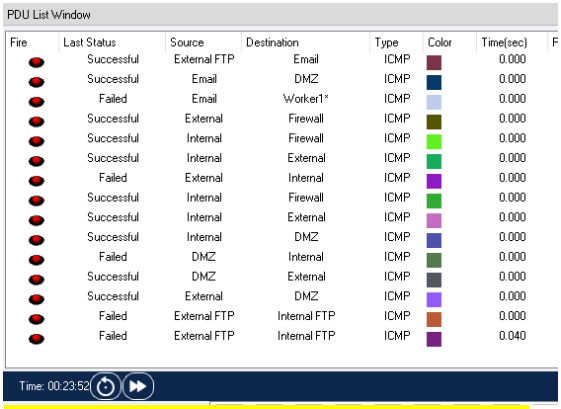

Figure 8 Simulation Result after DMZ Implementation

Figure 8 shows that traffic from the internal network to the DMZ was successful, but traffic from the DMZ to the internal network was unsuccessful. However, traffic from Internal to External network was successful but from External to Internal network failed. Again, traffic from Internal to DMZ was successful but vice versa failed. More so, traffic from DMZ to External and vice versa were successful.

The fusion of DMZ and Honeypot into the security models of the campus network made it more robust. This technique can be called DmzHoneypot. The DMZ discharges its operations to allow and, disallow certain traffic inflows and, outflows whiles the Honeypot intelligently gather information about the attacker or hacker as well as blacklisting the attacker IP address and quarantine it. This time around the system administrator is informed about any intrusion as well as provides information on the attacker to study him. The information gathered on the attacker can be used against him or her.

5. CONCLUSION

As state in section 4.3, four of the vulnerabilities discovered during the evaluation phase were exploited during the attack phase. This demonstrated that penetration testing has the ability to uncover the true state of a computer system's or network infrastructure's security.

All traffic from the inside (VLAN) to the DMZ is blocked, and only particular traffic from the DMZ to the network inside is permitted.
All traffic from the DMZ to the rest of the network will be permitted, but all other traffic will be blocked.
The algorithm in section 4.3.1 helped achieve that goal. The results after DMZ implementation in figure 8 above are evident of robust sanction of inflow and outflow of traffic.

The main goal of the Honeypot is to divert the attackers' focus away from the main network, avoiding the brutality of the attack. The configuration in section 4.3.2 helped achieve that purpose.

The combination or integration of Demilitarized zone and Honeypot security mechanisms can assist improve the security of campus networks.
The hybrid of DMZ and Honeypot toughens the campus network security as a result of their individual features that were merged. This technique can be described as Hybrid Honeypot.

6. FUTURE WORK

This work can be extended in different ways:
Work can be on automating the entire proposed penetration testing methodology to build a complete security testing solution as an extension of this paper. This extension can empower the Network and System Administrators of small and medium scale organizations to test and measure IT assets without any problems.

Work can be done on enhancing the design and implementation of a secure enterprise network using the integration of other security models.

An extensive study can be carried out on the effectiveness of honeypot as a security model in campus or enterprise networks.

The use of De-militarized zone with two firewalls can be assessed thoroughly for its implementation on any enterprise network.

However, in the future periodical scan for vulnerability can be automated, this is to intermittently alert system Administrators before the system gets exploited by an unauthorized user.

References

[1] Á. S. Tavares, "Network Architecture for University Campus Network," *College of Communication Engineering of Chongqing University*, pp. 7-25,79-93, 2011.

[2] S. Alabady, "Design and Implementation of a Network Security Model for Cooperative Network," *International Arab Journal of e-Technology*, pp. 27-36, 2009.

[3] H. R. Standford and L. Marsha, "Computer Networking," in *Computer Networking*, Pearson Education Asia, 2006.

[4] M. N. H. M. E. &. P. M. M. Bin Ali, "Design and Implementation of a Secure Campus Network," *International Journal of Emerging Technology and Advanced Engineering*, Vols. 370-374, 2015.

[5] N. Huang, "On Campus Network Security System of College and University," *JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE*, pp. 2-4, 2014.

[6] Y. Wu, J. Wu, K. Xu and M. Xu, "The design and implementation of router security subsystem based on IPSec," *: 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering. TENCOM '02. Proceedings.*, 2002.

[7] M. Chapple, "EdTech Focus on Higher Education," 22 November 2018. [Online]. Available: https://edtechmagazine.com/higher/article/2018/04/Segment-Your-Campus-Network-for-Stronger-Security.

[8] R. Udayakumar, K. Thooyamani and Khanaa, "Deploying site-to-site VPN connectivity: MPLS VsIPSec," *World Applied Sciences Journal*, pp. 6-10, 2014.

[9] Z. ChengXin, "Network Intrusion Prevention Theory and Practice[M].," *BeiJing: Mechanical Press*, 2006.

[10] S. y. r. w. Huang xin, "Study on Application of Honeypot in Campus Net Security," *Proceedings of the 2nd International Conference On Systems Engineering and Modeling (ICSEM-13)*, 2013.

[11] L. Kumari, S. Debbarma and R. Shyam, "Security Problems in Campus Network and Its Solutions," *International Journal of Advanced Engineering & Application*, 2011.

[12] Techtarget, "Definition - DMZ," 2019. [Online]. Available: https://searchsecurity.techtarget.com/definition/DMZ.

[13] C. Barracuda, "Barracuda NextGen Firewall X/ Documentation," 1 December 2018. [Online]. Available: https://campus.barracuda.com/product/nextgenfirewallx/doc/15893192/how-to-configure-a-dmz/.

[14] K. Rakshitha, A. M. Prajna, S. Roopashree and N. Poojit, "Campus Security using Honeypot," *International Conference on Advances in Computer and Electrical Engineering (ICACEE')*, pp. 24-41, 2012.

[15] S. y. r. w. Huang xin, "Study on Application of Honeypot in Campus Net Security," in *Proceedings of the 2nd International Conference On Systems Engineering and Modeling (ICSEM-13)*, Nanning Guangxi, 2013.

[16] S. Fashoto, G. Ogunleye and I. Adabara, "Evaluation of Network and Systems Security using Penetration Testing in a Simulation Environment," *GESJ: Computer Science and Telecommunication*, p. 27, 2018.

[17] H. Poston, "Penetration testing," 27 January 2019. [Online]. Available: https://resources.infosecinstitute.com/what-are-black-box-grey-box-and-white-box-penetration-testing/.

[18] A. Melmeg, "Penetration Testing," 2007. [Online]. Available: http://www.giac.org/cisspapers/197.pdf. [Accessed 30 September 2019].

[19] D. Geer, "Security - Network Security," 24 April 2017. [Online]. Available: https://www.csoonline.com/article/3191531/securing-risky-network-ports.html.

[20] R. Chandel, "Penetration Testing," 11 January 2020. [Online]. Available: https://www.hackingarticles.in/ssh-penetration-testing-port-22/.

[21] Cisco_Systems, Network Security Using Cisco IOS IPS, Cisco Press, 2006.