Original Research Article

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

ABSTRACT

With the advent of the increasing complexity of information systems and 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 design and implementation of a 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 network infrastructure of the University of Education, Winneba, and to demonstrate attacks and intrusion into the network infrastructure.

Results: Two firewall DMZ architecture techniques protect sensitive resources of the campus network, whiles the Honeypot techniques were configured **to** keep the attention of hackers diverted from the main network, averting the full force of an attack, until the administrators are ready to put the appropriate counter-action in place.

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. Increased use of Information technologies in the university requires a robust technical infrastructure and adequate network architecture to ensure optimum performance and efficiency. According to [1], a university campus network is an important

instrument for communication and facilitating collaborative research which are key factors to build a strong knowledge culture and efficiently support the academic mission.

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. Many critical applications have become more prevalent on the internet, due to the benefits derived from such technology.

The threats and attacks are persistent due to the vulnerability, which can arise from misconfigured software or hardware, poor network design, inherent technology weakness, and end users' carelessness.

These networks consist of routers, switches, and firewalls [2].

A router may have many services enabled by default.

Most such services are unnecessary and may be used by an attacker to gather information or for exploitation.

Careful management and diligent audit of routers and firewall operations will reduce network downtime, improve security and prevent attacks, hackers, network threats decrease and aid in the analysis of suspected security breaches.

Almost every day, the local news station's top stories are about the latest computer security threats from virtually unknowns, due to the anonymous nature of the Internet.

Cybercrime is on the increase targeting unsuspecting people via phishing frauds, spyware, identity theft, and Internet predators. We have seen attempts by hackers to compromise computer systems information as a direct result of focused attacks.

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 contributes to the vulnerability of the network system.

There is a need to enhance the design and implementation of a secured campus network.

This can be enhanced by the configuration of the Demilitarized zone (DMZ) and honeypot techniques to beef up the security of the campus network.

2.0 Literature Review

2.1 Overview of Campus Network

[1] cited Standford and Marsha (2006) in defining campus Networks as the interconnection of networks in a limited geographical area such as a university campus or organization campus.

Campus networks can be described as the link-up or interconnection of various Local Area Networks (LAN) within the university community or corporate campus.

Campus network may link a variety of buildings together, ranging from office buildings, university library faculty and departmental buildings as well as halls of residence. 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.

According to [1], the Hierarchical architecture model simplifies the design through the methodology of breaking the network in three main components that are *access network*, *distribution network* (convergence/aggregation network) and *core network* (backbone network) which

simplify, make it smaller and more manageable.

2.1.1 Secured campus Network

Bin Ali, Hossain & Parvez (2015), 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 configuration logically divides a network, creating multiple broadcast domains, that effectively allow traffic from the broadcast domains to remain isolated while increasing the network's bandwidth, availability, and security.

Campus VPN will provide a full tunnel VPN service that is an encrypted connection to the network from off-campus, this is to enable access to file-sharing/shared drives and certain applications that require a Campus IP address.

A firewall monitors and block or allow network traffic, both incoming and outgoing, on a private network. It affects certain outbound traffic and prevents unauthorized inbound traffic. All protocols and ports that can pose security risks are blocked in the outgoing direction.

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.

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.

According to Varsha (2017), Campus Networks can be made secure by using some security mechanisms. For providing better security to campus network security mechanisms like ARP inspection, DHCP snooping, Port Security, Private VLAN, Time based ACLs authentication of routing protocol and firewalls. Every security mechanism has its own functionality and feature.

Time-based ACL's provide access to the network during a certain period. Port security enables an administrator to configure individual switch ports to allow only a specified number of sources [1].

Tavares (2011) cited Bin Ali, Rahman and Hossain (2013) who purposed "Network Architecture with Security mechanism for Campus Networks". 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 captures packets in real-time, processes them, and can respond to threats, but works on copies of data traffic to

detect suspicious activity by using signatures. In the process of detecting malicious traffic, an IDS allows some malicious traffic to pass before the IDS can respond to protect the network. An IDS often requires assistance from other networking devices, such as routers and firewalls, to respond to an attack [3].

According to Network Security Using Cisco IOS IPS book (chapter 6: page 437), An IPS works inline in the data stream to provide protection from malicious attacks in real-time. IPS does not allow packets to enter the trusted side of the network. IPS runs a deeper analysis, which helps it to identify, stop, and block attacks that would normally pass through a traditional firewall device. When a packet comes in through an interface on an IPS, that packet is not sent to the outbound or trusted interface until the packet has been determined to be clean. The IDS and IPS work together to achieve optimum results.

Security management of campus network is not only the duty of few technicians but needs to be integrated into the agenda of college and university management and the cooperation of staff and students of the whole college and university [4].

2.1.2 Router and Firewall Security Policy

Routers forward traffic between two or more local networks within an organization or enterprise routes. Interior routers may impose certain restrictions on the traffic they forward between networks. Most at times, the router forward traffics between different networks called different "autonomous system". Backbone routers direct the traffic between the different networks make up the Internet.

A firewall is a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts. It can protect a network from external attacks by examining all packets of a message attempting to pass through the network and rejecting the packets that do not meet the security policy.

Security policy is the definition of security function against a network intrusion. The security engine provides security functions of packet filtering, an authentication, an access control, intrusion analysis and audit trail in the kernel region of the router. [5]. Routers and Firewall supports a large number of network services at layers: 2, 3, 4 and 7.

Campus networks carry almost every type of network traffic imaginable. Faculty and staff computers are similar to the devices in any workplace, but they are just the tip of the iceberg in higher education. Students connect video game consoles, smart assistants, cameras and even smart microwaves to the same networks that connect temperature sensors and research equipment.

Given that degree of diversity***, a one-size-fits-all network is impractical.*** Yet it would be too expensive to run completely separate networks for each of those applications. Fortunately, networking and security professionals have a trick up their sleeves: *network segmentation*.

This strategy lets administrators define separate logical networks that run on the same physical infrastructure. A student's laptop and a scanning electron microscope might be connected to the same switch, but they are logically separated from each other. Segmentation ***allows each device to operate under distinct security policies*** and have a different quality of service, depending on campus needs and priorities. [6]

2.1.3 The Use of Network Admission Control to Automate Traffic Assignment

Colleges and universities typically implement network segmentation using two types of devices: switches and firewalls. Switches reside at the edge of the network, providing access for individual devices and then aggregating traffic from other switches at higher levels

in the network. Modern switches let administrators define virtual local area networks that separate devices from each other. For example, administrators might define four VLANs on a switch corresponding to networks earmarked for faculty/staff, students, guests, and infrastructure. [6]

According to Chapple, when a new device connects to the switch, network admission control (NAC) technology ***interrogates the device to determine proper placement*** Once the switch connects a device to a VLAN, that device can directly contact only other devices on the same VLAN.

Network engineers typically carry the same network across switches on campus using ***VLAN trunking technology***. This means that infrastructure devices can connect to each other and student devices can connect to each other, but no communication is permitted between devices on different VLANs, even if they are connected to the same switch.

2.2 Security Issues in a campus Network

When discussing network security, three common terms used are Vulnerability, threats and attacks. Vulnerability is the weakness that is inherent in every network and device. This includes routers, switches, desktops, servers and even security devices [2].

According to [2], there are three primary vulnerabilities or weaknesses and they are:

a. *Technology weakness*: computer and network technologies have intrinsic security weaknesses. These include TCP/IP weakness, operating system weakness, and network equipment weakness.
b. Configuration weakness
c. Security policy weakness.

There is a wide range of network attacks and security threats, network attack methodologies, and categorizations of network attacks.

Network attack can be defined as any method, process or means used to maliciously attempt to compromise network security. The following are reasons why an individual will attack a corporate network: *Stealing data, Modifying stored data, Stealing software, Stealing hardware, illegally using user account and privileges, Running codes to destroy system, Running code to damage or corrupt data, performing actions that prevent legitimate authorized user from accessing network services and resources, and more.*

Classes of attack would possibly add passive observance of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service supplier [7].

Some of the network attacks are Passive Attack, Active Attack, Distributed Attack, Insider Attack, Close-in Attack, Phishing Attack, Hijack attack, Spoof attack, Buffer overflow, Exploit attack, Password attack, and ARP spoofing attack.

Security threat refers to anything that has the potential to cause serious harm to a computer system. Threats may include viruses, Trojan, back doors to outright attacks from hackers.

A security threat may be internal or external. Internal security threat could be Denial of Service (DoS), usually, it affects the whole external services like web, email, and FTP down, making it unusable; Network user attack threat affect the internal segmentation of the firewall, which can help contain the damage; web virus infects the system reading email and consequently spread to the entire organization.

The external threats are Email with viruses; webserver attack threat could grant the attacker access to other internal systems of the network; and Network

virus, which could enter through unprotected ports and compromise the whole network.

2.2 The analysis of the current situation of Campus Network Security

Apart from the common occurrence of the virus, the campus network has to face three major security hidden dangers.

The limitation of the firewall: Many campuses only install a layer barrier-firewall, but there are many limitations in the firewall. The firewall is passive defense equipment, and the campus network has many obvious shortcomings as these limitations in the firewall used in the campus network. Honeypot technology has active defense characteristics and can help the campus network avoid being attacked [8].

***Internal attack*:** According to relevant materials statistics, the percent of campus network attacks by inside is more than eighty percent (80%). With computer universalness, some students' computer level is already beyond school network management personnel's imagination, and these students affected by curiosity or motives eavesdrop someone else's code and other important information [9]. This mischief damage even malicious attacks school management system.

Hacker attacks: The internet is a connection from one gateway to another gateway. Due to the safety consciousness and capital reasons, many campuses exist the "heavy technology, light safety, light management" tendencies, and the builders of the campus network do not pay much attention to the security problems, and often set up one firewall. These weaknesses provide an opportunity for hackers and make them an inverse school network through the campus internet connection, and cause serious damages to the system and data [8].

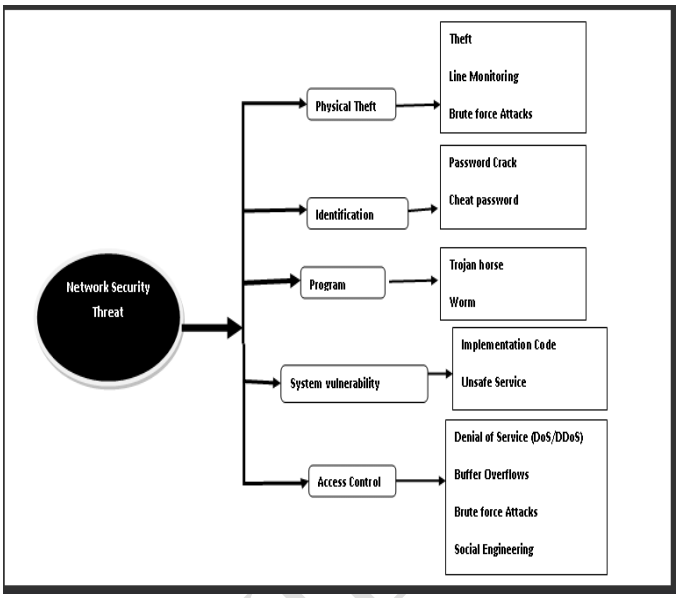

Figure1 Network Security Threats

2.3 The Use of DMZ and Honeypot to enhance Network Security

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

DMZ is a physical or logical subnet that separates an internal local area network (LAN) from other untrusted networks, usually the internet [10]. This segment of the campus network houses the webserver. The idea is to logically separate the hosts in the DMZ segment from other hosts outside that segment of the network.

The DMZ configuration, provide full control over network traffic from the Internet to the web server, as well as traffic from other network segments to the web server [11].

The web server listens on TCP port 8080 instead of 80 and the listening socket of your web server must not be

changed, the use of Port Address Translation (PAT) feature of the DNAT rule is used to modify the destination port of IP packets passing the firewall.

An Access rule is created to allows HTTP traffic from the Internet to the web server residing in the DMZ

2.4 Campus Security using Honeypots

Honeypots are closely monitored decoys that are employed in a network to study the trail of hackers and to alert network administrators of a possible intrusion.

Honeypots can be classified based on their deployment and based on their level of involvement. Based on deployment, honeypots may be classified as production honeypots and research honeypots. Based on design criteria, honeypots can be classified as pure honeypots, high-interaction honeypots and low-interaction honeypots.

Production Honeypots: capture only limited information, and are used primarily by companies or corporations; Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security.

Research Honeypots are run to gather information about the motives and tactics of the Blackhat community targeting different networks. These honeypots are used to research the threats organizations face and to learn how to better protect them against those threats. Research honeypots are used to capture extensive information and are used primarily by research, military, or government organizations [12].

High-interaction honeypots imitate the activities of the real systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste his time. An example is Honeynet.

Low-interaction honeypots simulate only the services frequently requested by attackers. An example is *Honeyd*.

The use of honeypots provides a cost-effective solution to increase the security posture of an organization. Even though it is not an absolute panacea for security breaches, it is useful as a tool for network forensics and intrusion detection. Nowadays, the research community to study issues in network security, such as Internet worms, spam control, DoS attacks, etc., is also extensively using them.

This technique is usually called "bait and switch", and allows choosing what is supposed to reach the production network or the honeypots 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.

3.5 Methods of discovering Vulnerabilities

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

A penetration test can provide Network and system Administrators with a realistic assessment of security posture by identifying the vulnerabilities and exploits that exist within the computer network infrastructure [13]

To discover and verify vulnerabilities, the penetration test was used to determine the level of security of the network against network-based attacks with the view of improving information systems security.

Running a penetration test requires the tester to understand the test environment, and adopt a formal approach to testing. 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 complete knowledge regarding the target network or system infrastructure. This testing can be considered as a real test or attack by an insider who might be in possession of knowledge of the system. The main goal of a white-box penetration test is to provide information to the tester so that he can gain insight into the system, and deploy the test based on preconceived knowledge. For instance, in a white-box infrastructure penetration test, information about network diagrams and infrastructure details, and many more are provided and the source code of the application is provided along with the design information, etc. are provided in the case of an application penetration test.

Black-box test: This testing can be considered as a real test of a real-world attack by an outsider. The tester has no prior information regarding the target network system infrastructure. Ethical hackers or testers need to gather their information from public sources to find the loopholes on their own, testing everything from scratch. The steps of mapping the network, operating system fingerprinting, enumerating shares, and services are typical for black-box testing. A black-box penetration test determines the vulnerabilities in a system that are exploitable from outside the network [14].

The combined (Black -box and White-box) approach that provides a powerful insight for internal and external security viewpoints. This combination is known as **Grey-Box** testing. The key benefit of this approach is a set of advantages posed by both approaches mentioned above. Grey box penetration testing helps to eliminate any internal or external security issues lying at the institution's infrastructure environment that an attacker can exploit. According to Melmeg (2007), Grey box penetration testing is a preferred method because it helps to eliminate any internal or external security issues within the institution’s network infrastructure environment that an attacker can exploit. In terms of cost, it saves time for the penetration testers to uncover information that is publicly available [15].

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. White-box testing is the slowest and most comprehensive form of penetration testing. In all, ***black-box penetration testing*** is the fastest type of penetration test. The limited information available to the testers increases the probability that vulnerabilities will be overlooked and decreases the efficiency of the test since testers do not have the information necessary to target their attacks on the

most high-value or likely vulnerable targets [14].
However, Gray-box testing makes a slight tradeoff in speed compared to black-box testing in exchange for increased efficiency and coverage. The test provides a more focused and efficient assessment of a network's security than black-box penetration testing.

In a campus network, the penetration test was conducted using the grey box testing approach. The proposed approach is adopted to minimize the possibility of damage to the campus network system.

The selected environment for conducting the assessment and penetration testing is the University of Education, Winneba-Kumasi campus, where the network infrastructure was tested. This choice was a result of the tester's familiarity with the institution and its IT and network system and also the possibility of obtaining permission and access to the network since the tester is a staff of the university.

The penetration test was conducted from two main test sites selected to enable the tester to simulate an attack from a location within the University of Education, Winneba Kumasi campus' network, and a remote location outside of the university's network.
Performing the penetration test on the campus network involves learning and understanding what penetration test was, how penetration methodology could be followed, which tools and techniques could be used. A proposed four-phased penetration testing *methodology* which is based on the methodology designed by the National Institute of Standards and Technology (NIST) of the United States would be followed to conduct the test against the UEW network.

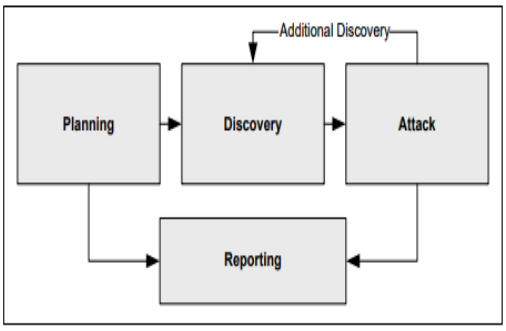

Figure 2: Four-Stage Penetration Testing Methodology

This method approaches penetration testing from a project management perspective, whereby the whole test is viewed as one project with related activities starting from planning, initiation of the test, to the completion and reporting stage.
The planning phase sets the groundwork for a successful penetration test. No actual testing occurs in this phase.
The discovery phase of penetration testing includes the actual testing and covers information gathering and scanning. Network port and service identification is conducted to identify potential targets. In addition to port and service identification, other techniques are used to gather information on the targeted network:
Vulnerability assessment is the view as a vital component of penetration testing. Each stage of the test and its logistics are planned ahead before the actual test is conducted. This method is selected as ideal for conducting penetration test in a university environment not only because it enables the tester plan out his actions, and follow a methodical approach but also enhances the repeatability of the test. Since the test is being conducted in a production environment, planning was critical to prevent any unintended consequence.
The above figure 3.1, graphically presents the methodology used for the testing, the different phases that occur during the penetration testing. The same methodology, tools, and techniques could be used for other academic systems or networks with the intention of discovering

and determining the possibilities of exploiting the vulnerabilities.

4. ANALYSIS AND DISCUSSION OF RESULTS

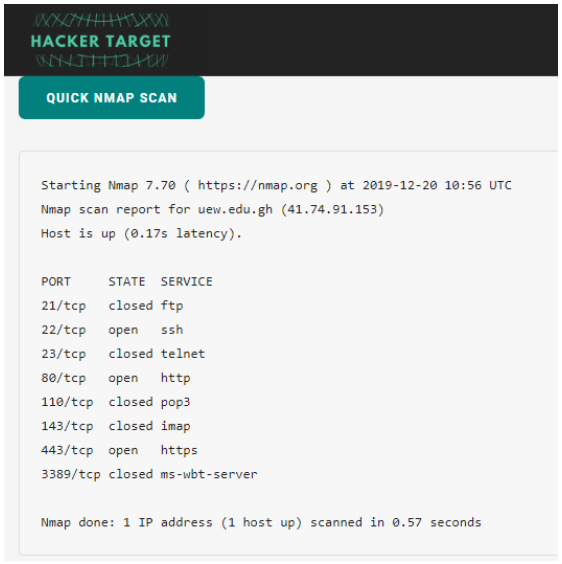

Figure 3 NMAP Report on Port Scan

In figure 3, 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. The port 22 uses the SSH for remote login. The port 80 is for world wide web (http) connection.

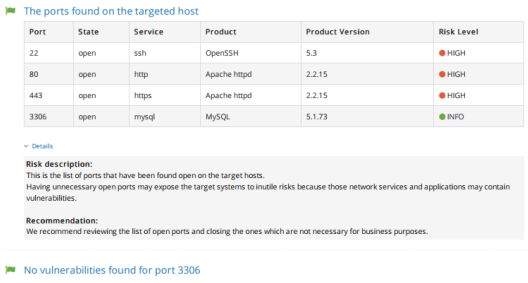

Figure 4 Ports found on the target host (UEW)

The above figure 4, displays the state of the ports and their risk levels. It is evident from the scan that port 22,80, and 443 have a high risk of vulnerability due to the fact that 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.

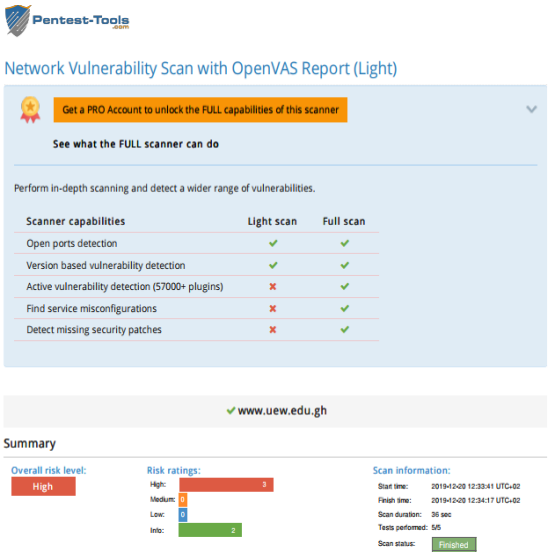

Figure 5 Network Vulnerability scan report for UEW

Figure 5, presents evidence from the port scan analysis affirming the vulnerability of the UEW campus network and susceptible to attacks.

Table 4.1 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

4.2 Findings

4.2.1 Security of the Campus Network

The penetration tests conducted on the campus network of UEW clearly 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.
Weak passwords can make SSH and port 22 easy targets. Port 22, the designated Secure Shell port that enables access to remote shells on physical server hardware is vulnerable where the credentials include default or easily guessed user names and password [16].
According to [16], HTTP traffic uses TCP ports 8080, 8088, and 8888. The servers attached to these ports are largely legacy boxes that have been left unmanaged and unprotected, gathering increasing vulnerabilities over time.

Usually, by default, ssh listen on port 22, which means if the attacker identifies port 22 open, then he can try attacks on port 22 in order to connect with the host machine [17].

In both tests it was realized in figure 4 and figure 5 clearly 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.

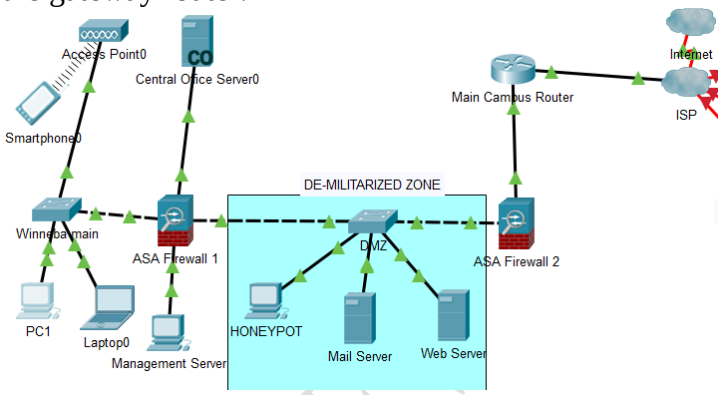

Figure 6 Enhanced Campus Network Design

Figure 6 is the design of the enhanced secured campus network proposed to mitigate the vulnerabilities and attacks.

4.3.1 De-Militarized zone configuration

The key requirement of DMZ access is enlisted below –
Web Server (in DMZ with IP 41.74.91.153) should have access to the unsecured Internet over HTTP and HTTPS protocols only. The rest of the traffic should be blocked.
DMZ Web Server should be able to reach SQL Server in inside network rest of traffic should be blocked.
STEP 1 –Allow specific traffic from the DMZ to the inside. Deny all other traffic from the DMZ to the inside.
STEP 2 –Allow specific traffic from the DMZ to the outside.
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 is important to choose the right criteria for traps.

The 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 device 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 analyzes the log and, while in the log line of the “HONEYPOT_UEW” tag, cuts the attacker's IP address and adds this address to the Blacklist object group.

```
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"
```

When the next line with the label "HONEYPOT_UEW" occurs in the log, an event; in the event handler itself, from the log line 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 DMZ were denied whiles specific traffic from the DMZ to the inside was allowed.
However, specific traffic from the DMZ to Outside was allowed and all other traffic was blocked.

The fusion of DMZ and Honeypot into the security models of the campus network made it more robust. This time around the system administrator is informed about any intrusion as well as provides information on the attacker to study him.

5. CONCLUSION

Assessment phase and four of such identified vulnerabilities were exploited during the Attack phase, as shown in section 4.3. This showed that the penetration testing has the potential of revealing the true state of security of the computer system or network infrastructure.

The aim of the DMZ to deny all traffic from inside (VLAN) to the DMZ, and only specific traffic from the DMZ to the network inside was allowed. The traffic from DMZ to the outside of the network would be allowed but all other traffic will be denied. The algorithm in section 4.3.1 and configuration in appendix 4 helped achieve that goal.
The main aim of the Honeypot is to divert the attention of the attacker or hacker from the main network, averting brutal force of attack. The configuration in section 4.3.2 helped achieved that purpose.

The fusion or integration of de-militarized zone and honeypot security strategies can help enhance the robustness of the campus network security.

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 dissertation work. This extension can empower the Network and System Administrators of small and medium scale organization 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 various security models.

There should be the need to periodically scan for vulnerability to mitigate it before the system get exploited by unauthorized user.

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

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

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

[5] 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.

[6] 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.

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

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

[9] 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.

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

[11] 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/.

[12] 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.

[13] 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.

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

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

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

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