



# Campus Network and Systems Security Assessment Using Penetration Testing: The Case of the University of Education Winneba, Kumasi

Christian Adu-Boahene<sup>1</sup>, Solomon Nii Nikoi<sup>1\*</sup> and Alberta Nsiah-Konadu<sup>2</sup>

<sup>1</sup>University of Education, Winneba, Kumasi Campus, P.O.Box 1277, Kumasi, Ghana.

<sup>2</sup>University of Education, Winneba, Mampong Campus, P.O.Box 40, Mampong, Ghana.

## Authors' contributions

*This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.*

## Article Information

DOI: 10.9734/AJRCOS/2021/v12i130273

### Editor(s):

(1) Prof. G. Sudheer, GVP College of Engineering for Women, India.

### Reviewers:

(1) K. Prathapchandran, Nehru Arts and Science College, India.

(2) Gudipudi Dayanandam, Government College For Men, India.

Complete Peer review History: <https://www.sdiarticle4.com/review-history/73420>

Original Research Article

Received 07 July 2021

Accepted 17 September 2021

Published 24 September 2021

## ABSTRACT

Network intruders are becoming more sophisticated in their approach, resulting in many difficulties in preventing them. They exploit both well-configured systems and vulnerable systems.

**Aims:** To examine the performance of a campus network against attacks on the network systems.

**Place and Duration of Study:** University of Education, Winneba- Kumasi campus.

**Methodology:** Penetration testing was adopted to investigate the vulnerabilities that may occur in a university network.

This helps to test for vulnerabilities on the network system that may expose the system to exploits.

**Results:** The test revealed that system-based attacks might be propelled by malignant pariahs on the Internet and noxious insiders straightforwardly associated with inward systems. The perpetrators can exploit vulnerabilities in network foundations and frameworks, for example, servers (web servers, software servers, file and mail servers, etc.), routers, and firewalls.

**Conclusion:** This work presents a way to deal with evaluating the security stance of a college utilizing penetration testing that meddles negligibly with the flow of traffic and activities on the network infrastructure. attack Insurance against network-based attacks is mind-boggling and, in the offer, to relieving one framework normally gives a stage that can be utilized to dispatch more attacks.

*Keywords: Attacks; vulnerabilities; penetration test; exploit; network infrastructure; security; servers.*

## 1. INTRODUCTION

There are various dangers to data frameworks and systems foundations today, which undermine the unwavering quality of data frameworks in our colleges. Data systems are mostly exposed to regular menaces including that of malware on computers, interruption in a permitted user's access to a system's network also known as Denial of service (DoS), spams, and computer hackers. The networks as well as the data systems of the university have been experiencing consistent threats from a variety of sources which include frequent ambush from computer hackers who are within the network as well as those outside the network, computer-assisted fraud.

Appiah et al. [1] stated in their experiment that the configuration of a university system network is very tedious because the information system used can be complex than those used in a commercial organization. This is because many of the users of the university network which includes the entire student body, faculties, departments, and the staff members of the university tend to be on their own. Despite how complex a university information system could be, it has to also make room for availability easy access to its clients including the students and the staff members.

Campus systems networks are always prone to various forms of attacks which includes physical attacks on various components of the network, attacks from electronic and social engineering mechanisms, where various users with dubious means will get their hands on restricted and private data on the network when they are in the network like getting access to the university's database systems. This study examines the performance of a campus network against attacks on the network systems. These system-based attacks might be propelled by malignant pariahs on the Internet and noxious insiders straightforwardly associated with inward systems. The perpetrators can exploit vulnerabilities in network foundations and frameworks, for example, servers (web servers, software servers, file and mail servers, etc.), routers, and firewalls. Insurance against network-based attacks is mind-boggling and, in the offer, relieving one framework normally gives a stage that can be utilized to dispatch more attacks.

Systems and Network administrators owe it an obligation to keep the frameworks and systems

secure from both inside and outer dangers and attacks. In a campus network, there is consistently the chance of somebody outside or inside trying to break into the system foundation by looking for vulnerabilities in the system. A campus network has a large category of users, for example, permanent workers like the academic staff, administrative staff, the entire student's body, and temporarily members of the university like the national service personnel, temporarily staff members, visitors, and guests who come to the university, that are given genuine access to specific assets on the system or to play out certain obligations in the frameworks, furthermore, could cause a wide range of issues for the system manager. An administrator(s) of the system or the frameworks ought to have full power over the system and frameworks. The Administrator is relied upon to know precisely what gadgets, frameworks, and administrations are continuously moving on the system, the shortcoming on the system, and alleviate them with the most recent updates. By and by, the system and frameworks directors frequently battle with discovering vulnerabilities, programming updates that can be utilized to alleviate vulnerabilities.

Security evaluation is exceptionally key in deciding the degree of bargain feasible for basic hosts in a system. This kind of evaluation can be executed utilizing penetration testing by effectively examining a system and examining abuses that bargain frameworks.

Penetration testing can be exceptionally successful in finding shortcomings in a system, yet is work serious and tedious, and can upset framework tasks. This work presents a way to deal with evaluating the security stance of a college organization utilizing penetration testing that meddles negligibly with network activities and requires no extra framework traffic other than that used to execute ordinary host weakness filters.

This approach mostly used in securing the campus network is by strengthening the security of the systems at their initial configuration and monitor the limitation of the systems and network during their operations. A campus network is susceptible to attacks and threats from both authorized users and nonauthorized users both outside and inside of the network, hence the need to test the potency of the network at a higher frequency. Security is not properly used in

the protection of information and other valuables at the University of Education Winneba (Kumasi Campus).

The management of information systems and networks at the UEW Kumasi campus is configured to strengthen the security of the network and systems. Moreover, this methodology in securing the college system and data frameworks might be incapable of countering system-based attacks. When a problem is detected by monitoring devices, the Administrators of the network react by fixing the problem. These methods of ensuring the frameworks and system may not be adequate, since it may place the attacker always ahead of the system and network managers. This may result in permanent damages like data theft, disruption, reputation damage, Denial of service, and many more. The act of testing for vulnerabilities in networks periodically without waiting for an attack could be the proactive way of protecting systems and networks of the university environment.

## **2. LITERATURE REVIEW**

With the advent of vulnerabilities and threats that may exist in information systems, there is the need for Information system security, which can also be termed as INFOSEC.

“Information security is a wide subject which is a subset in the field of Information Technology (IT) that centers around securing PCs, systems, and their clients” [2]. The assurance of data and data frameworks from unapproved get to, use, divulgence, disturbance, adjustment, or demolition, to give classification, uprightness, and accessibility can be term as Information framework security.

According to [1], Data security assurance might be accomplished by going through certain measures to ensure the safety and availability of information.

Confidentiality is the protection of information by restricting access to unauthorized users. It also involves restricting access to certain content reserved for some groups of users. The universities and all tertiary institutions are mandated to restrict access to students' private information. The various faculties and departments are restricted to certain information about the students. For instance, faculty is privy to students' academic records, the finance department is privy to the financial records of the

students and restricted in viewing the academic records of the student. Integrity assures the accessed information is not being altered and represents its purpose. “Integrity can in like manner be lost accidentally, for instance, when a PC power surge ruins an archive or someone affirmed to reveal an improvement unexpectedly eradicates a record or enters a wrong information” [3].

In this case, information needs to be secured to avoid alteration and loss, when this is assured then the integrity of the system is assured. Availability is the ready accessibility of information by authorized users for modification and update. Any factor that will hinder information access by an authorized user should be eliminated. Access to information by an authorized user must also be within a timeframe to check security bottlenecks.

Data security examination can be characterized as the way toward deciding how successfully an element being evaluated meets explicit security plan” [4].

The explicit study to learn about the susceptibilities and risks that exist in an information system is termed as Information Security Assessment. This survey can be carried with the aid of certain tools like Testing, Interview, and Examination. Testing is the process of utilizing at least one assessing object under indicated conditions to take a gander at veritable and foreseen results. The meeting is the conduction of conversations with people or target bunches inside an association to accomplish explanation or distinguish the region of proof. Assessment is the way toward watching, investigating, looking into, breaking down, checking, or considering not less than one evaluation equipment to enhance understanding, and achieve elucidation, or proof. Evaluation outcomes are utilized to aid the affirmation of security control possibility after some time [1]. Asset accessibility is for the most part a constraining variable in a way of repeating the security evaluations. This is because Information security examination requires a set of equipment like time, staff, and computer programs. The data security evaluation procedure is supposed to accompany at least one of the following procedures: planning, execution, and post-execution. The planning point is the stage of collecting information that is needed in assessing execution. In this stage data is accumulated on the resources for being surveyed, the dangers of enthusiasm against the advantages, and the

security controls to be utilized to alleviate those dangers. The data assembled is utilized to build up the planning approach. A security evaluation ought to be intended to address objectives and targets, scope, necessities, group jobs and obligations, confinements, achievement factors, suspicions, assets, course of events, and expectations [4]. The execution stage is utilized to recognize weaknesses and approve them when suitable. It tends to ascertain exercises intended for the proposed kind of evaluation strategy and procedure. As indicated by [4], express activities for this stage differentiate by assessment, interminable flexibility of this stage assessors will have perceived structure, mastermind, and legitimate strategy weaknesses.

The post-Execution stage includes the way toward investigating distinguished weaknesses to decide underlying drivers, build up suggestions, and build up the last report.

“Penetration test gives an indebt point of view on current security stance of an association's IT framework” [1]. A penetration test can be referred to as a way of analyzing the security of a PC's framework through a remotely associated system, for example, the Internet and to recognize weaknesses in the framework and system while endeavouring real attack strategies by computer hackers [5]. Penetration testing is a viable security evaluation strategy and the most ideal approach to survey the security status of some random data framework.

According to Appiah [2], The demonstration of surveying all the IT foundation segments including working frameworks, correspondence medium, designed gadgets, applications, physical security, and human brain research utilizing comparable or indistinguishable techniques to that of an attacker yet performed by the approved and qualified IT experts is termed as penetration testing.

In a campus network, the Penetration tester could run the test as a member of the network system and outside the network through the internet.

Testing from within, or as a member of the Local Area Network will help to discover how vulnerable the system could be if the attacker is within the network as an authorized or unauthorized user. Testing from outside via the internet also helps to discover the vulnerability of

the system if the attacker launches an attack from any location.

When the core function and purpose are established about an Attacker and Penetration tester then the difference between the two can be ascertained. The goal and consent given to the analyzer by an official administration draw out the distinction between Penetration analyzer and attacker according to [6] discoveries. The goal of a penetration analyzer is to misuse security shortcomings in a data framework or system foundation, decide the attainability of an attack, the business sway, and report discoveries to the official administration [1].

Interestingly an attacker will misuse security shortcomings to access data or upset service.

A penetration analyzer has consent from the official administration to misuse security shortcomings while an attacker doesn't. Penetration testing must be performed with the consent and consciousness of the official administration. Whereas, the attacker does not seek permission from anyone but goes ahead to exploit the vulnerability of the information system to launch attacks.

The objective of an Ethical hacker is to distinguish weaknesses and fix them before they are abused. The methodology is more extensive in scope than penetration testing. At the end of the day, penetration testing is a subset of white hat hacking methods [7]. Penetration analyzer performs digital security evaluation on explicit IT framework while moral hacking survey all frameworks security blemishes utilizing many hacking approaches. As indicated by an article distributed by [7], the white-hat hacker needs to have wide information in programming and equipment procedures, while penetration testing needs to have information and abilities in the particular territory being tried. According to [8], vulnerability scans are designed to identify known weaknesses in your frameworks and report possible presentations. Penetration tests are expected to abuse shortcomings in the design of your IT network and decide how much a malicious attacker can increase unapproved access to your benefits. A susceptibility check is normally computerized, while a penetration test is a manual test performed by security proficient.

White box testing gives the penetration analyzers data about the objective system before they start their work. As cited by [2], White box examination is a penetration examination process where the

analyzer has some previous information on the system being tried including the system geography or the IP addresses of the system to be evaluated. "The penetration testing team has the most extensive knowledge possible about the system to be tested". The white box examination is also referred to as the Full knowledge Examination process.

The data is usually learned before the testing includes details of IP addresses; protocols used with the source codes as well the network infrastructure schematics and even passwords. White-box penetration testing gives an extensive evaluation of either inside or outer susceptibilities, settling on it the most ideal in making decisions for count examination [9]. However, a close relationship exists between white-box penetration testers and executive management/developers, the tester could even be part of the organization. This relationship gives the tester access to a high level of system knowledge. Though access to information is good, it may affect the tester's behaviour, since his operation is based on knowledge not readily available to hackers.

Black Box Testing, as indicated by Infosec organization is the kind of penetration test where the analyzer has no earlier inward information on the focused-on system or framework simply like a normal programmer. This suggests the revelation of penetration evaluation relies upon incredible examination of at present running activities and structures inside the target framework. As confirmed by [1], this approach can also be referred to as Remote penetration testing or External testing.

Discovery testing permits the penetration analyzer to recognize shaky areas dependent on what a white hat hacker is well on the way to target [10]. In any case, that can leave a few spots of the foundation untested. A discovery entrance analyzer must be OK with mechanized inspecting instruments and methods of reasoning for manual invasion testing. The compelled data provided for the passage analyzer makes disclosure penetration tests the quickest to run since the term of the undertaking by and large depends upon the analyzer's ability to discover and experience weaknesses in the target's outward-standing up to organizations. "This sort of testing is the most practical, yet additionally requires a lot of time and has the best potential to neglect a weakness that exists inside the interior piece of system or application" [11].

Similarly, [3] concurred that the white box testing is progressively far-reaching, as both inner and outer vulnerabilities are assessed from an "in the background" perspective that isn't accessible to run-of-the-mill attackers. Whiles discovery testing is the most practical, however, has the best potential to disregard helplessness that exists inside the inward piece of system or application. The White box and Black box testing approaches have their quality and shortcoming. In settling on a choice of directing a penetration test, there is no correct choice about white box or discovery testing. The situation decides the decision of approach.

In the long run, the most significant thing is the methodology which carries the best advantage to the association considering the evaluation of the association and its organogram. Gray Box Testing is the blend or intertwining or coordination of both white box and discovery penetration testing. This offers space to provide food for the exes of the two methodologies. The reason for Gray Box pen testing is to give an inexorably connected and powerful assessment of a framework's security than a revelation evaluation [11]. Black box examination can also reproduce as an attacker that has just entered the border and has some type of inward access to the system, and this assists with making an increasingly effective and smoothed out methodology.

### 3. METHODOLOGY

This work is to investigate the susceptibilities that may exist in a university network infrastructure and how system administrators can utilize penetration testing to reveal and confirm these vulnerabilities. The work also focuses on determining the degree of security of system-based attacks with the perspective of improving data frameworks' security. Penetration testing was adopted to investigate the vulnerabilities that may occur in a university network.

According to [12], "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".

Penetration testing is a re-enacted digital attack against your PC framework to check for exploitable weaknesses [13]. The most important component of the penetration test is the vulnerability assessment. There are three distinct methodologies for leading penetration tests. The

researcher or tester must comprehend the test condition, and embrace a proper way to deal with testing.

Penetration testing on the university campus environment was performed by utilizing the grey box testing method. This method is brought about to help reduce the probability of harm to the college's system framework [14]. The University of Education, Winneba (UEW) with a primary focus on the Kumasi campus situated at Tanoso in the Kwadaso Municipal Assembly was chosen condition for leading the evaluation and entrance testing.

University of Education, Winneba is known to be the largest public university in Ghana with four specialized campuses within two geographical regions (Central and Ashanti), delivering Programmes mainly in Education as a result of its core mandate, in addition to Arts, Linguistics, Business, Sciences, and Technology. Each campus is known for a specialized stream of Programmes. The Ajumako campus is known for Linguistics, Asante Mampong campus is known for Agricultural Science, Kumasi campus is known for vocational and technology and Winneba serves as the hub of all the Education Programmes as well as certain Programmes from the other campuses. The Winneba campus is even subdivided into three: North, Central, and South campus all within the Winneba traditional area. All the campuses are on the same web server which is located on the Winneba campus. Intranet1 is the type of network used to link all the campuses on the same platform.

This strategy is chosen as perfect for leading penetration test in a college situation not just on the grounds that it empowers the analyzer to plan out his activities, and follow a precise methodology yet, in addition, improves the repeatability of the test. Each phase of the test and its coordination is prepared before the genuine test is led. Consequently, the test has been directed in a creation domain, planning was basic to forestall any unplanned results. This approach, apparatuses, and procedures were utilized for scholastic framework or system to find and recognize the conceivable outcomes of misusing the vulnerabilities of the framework.

### 3.1 Initiation

This is the place regulatory and planning exercises are done. Here the destinations of the test, scope, lawful limitation, approvals, and

planning for the task are delineated and figured. Above all, specific issues like degree, consent and endorsement, following and capacity, announcing, and safeguards should be thought of.

The penetration tester (researcher) obtained permission from the ICT Directorate of the University of Education, Winneba – Kumasi campus to obtain approval before the test was conducted on the campus network. The researcher (tester) was constantly tracked and gather information in addition to the point-by-point data of host and weaknesses found all through the stages in a database. This database contains each datum expected to reach determinations about the test to be performed. The researcher was circumspect in the presentation of the test reports. Certain touchy subtleties and found passwords in the outcome were avoided by the overall population. Any movement that has the capability of harming or interfering with the administrations on the creation plan was limited or deliberately run during the off-top time. Any disavowal of administration attacks was done on the ends of the week and on occasions and during the lockdown period. This is mindfully done to forestall any interference on the college's system foundation.

### 3.2 Setting Up and Selection of Gadgets

At this phase of planning the analyzer (specialist) chose the penetration testing apparatuses and methods were utilized which was be perfect for the particular condition and upgraded the precision of the test. This is the stage where a decision is made to consider whether to use open source and free instruments or make use of enterprise and paid devices. The analyzer perseveringly chose fitting apparatuses and methods for the specific condition. The proposed apparatuses utilized are Nmap, Nessus, OpenVAS, and Metasploit systems.

### 3.3 Intelligence Gathering (Reconnaissance)

Knowledge gathering extended from uninvolved data gathering, dynamic data social affairs to

target examining the framework and system [1]. It is imperative to comprehend the objective system or frameworks before the genuine test. With the accomplishment of observation, both inactive and dynamic surveillance methods were

utilized. In performing a loof surveillance different sorts of searches, for example, Web nearness, Network count, Domain Name System (DNS) - based observation was led, to find data identified with the University of Education, Winneba including the college's frameworks, representative data, physical area and business action without interfacing with them legitimately to the system.

In directing dynamic observation Nmap was broadly utilized during this phase for organizing the study, port checking, working framework, and administration identification. Nmap came pre-introduced on Kali alongside other valuable devices.

### 3.3.1 Network mapping step

The main purpose of this stage is to delve more into the system and study every potential threat to focus on where an attacker is about to strike; as it were, forthright at which a powerless objective framework, port, and administration have been distinguished. Planning and profiling movement will frequently envelop some level of system examining to decide the attributes of any firewall and interruption identification advancements utilized on the objective system Nmap's, ICMP ping-clear was utilized to recognize live host in the system fragment. At the point when all the IP locations and system fragments are recognized, port filtering alongside OS and administration fingerprinting was completed against a live host. The insight assembled during this stage was utilized as an info boundary for the following stage. Data, for example, plan run, have IP addresses, introduced working frameworks and open ports distinguished was gathered and archived to give away from of the system.

## 3.4 Vulnerability Discovery Phase

This Phase is made of two major activities:

- Scanning and Identifying vulnerabilities in the network
- Research and Susceptibility Assessment

### 3.4.1 Susceptibility Scanning and Identification

The scanning and identification of the weakness stage were done utilizing two separate system susceptibility scanners; Nessus and OpenVAS. The two scanners were designed so that they could distinguish vulnerabilities that exist because of setup defects. To empower the

analyzer to find vulnerabilities from both interior and outer hub of the college's system, the susceptibility filter was directed from both the inward area and a remote area outside to the system. To upgrade the nature of vulnerability check and to maintain a strategic distance from any unintended outcome of the examining on the system foundation, it is significant for the analyzer to move toward the filtering with an all-around planned out advance.

These fundamental advances were followed to do the sweep:

- i. Study and extension the system engineering and parts for evaluation
- ii. Decide the limit of investigation
- iii. Identify resources and timetable errands
- iv. Impact examination for dynamic outputs which incorporates evaluation of administrations or workers check-in online creation
- v. Plan for personal time and possibility if pertinent
- vi. Define the sweep strategy to decide the degree of output required – data gathering, strategy checking, port filtering, secret key investigation, attacks incitement, and so on.
- vii. Scan the objective system and hosts dependent on the characterized check strategy
- viii. Gather the sweeping outcome and examine for safety escape clauses

### 3.4.2 Experimentation and Vulnerability Assessment

Most data were gathered about the defenselessness from the web and different weakness databases which is made up of the National Vulnerability Databases (NVD), and a need rundown of all susceptibilities found is archived. Data assembled from the helplessness examining and Identification stage, the analyzer (analyst) continued to do additionally explore on the found vulnerabilities. Fig. 1 below the report from the vulnerability scan:

## 3.5 Exploitation

In this stage, all the perceived shortcoming was examined to affirm if those weaknesses were exploitable or they were assuredly not. It may not be possible to abuse all risks perceived as weaknesses, in this way, just weaknesses that have straightforwardly available undertakings,

was personally handled using Metasploit Framework. The undertakings were done from two rule territories centers; the inward region inside the University's framework and a far-off region outside the UEW structure.

### 3.6 Phase of Reporting

This stage included documentation of the considerable number of exercises that were completed in all the past stages. The revealing stage happened in corresponding to different stages and toward the finish of the stage of the attack. Reports contain an assessment of the vulnerabilities situated as possible dangers and suggestions for alleviating the vulnerabilities and dangers. This reporting stage was done in such a manner to ensure the straightforwardness of the tests and the vulnerabilities they revealed.

When all is said in done, this last report gives a chance to comprehend the general security stance of the frameworks or system. Coming up next was remembered for the report

- Detail investigates both elevated level and low-level discoveries and clarifications of the means important to rehash the adventures
- Discoveries which are made up of both positive and bogus positive dangers
- Proposals

#### • Clean-Up

During experimentation, items, for example, strategies, tables, perspectives, or records are made available for the penetration experimentation method. For instance, a re-enacted account that is used in the beginning stage of the test must be re-established during the finishing stage of the test. The cleaning up express should be done totally and cautiously to re-establish the framework to its unique state. This expression ought to be checked and inspected to guarantee that penetration analyzers don't remiss or purposely leave an escape clause in the framework or system.

#### • Configuration and the Penetration Testing Setup

Two separate testing destinations were employed in empowering the analyzer to direct the testing process from both the internal network (a private network) and external hubs. The first destination was laid outside the college

condition explicitly in the specialists associated with web broadband. The second destination inside the college was situated in the desktop research of the University of Education, the main campus, which is located at Winneba.

#### • Set Up for External Testing

The external testing process for the outer penetration testing was done in the home of the analyzer with very fast and efficient internet connectivity. At the top of the line, a work station was set up to represent a virtual to host the machine to make a penetration testing condition. The red cap working framework that was introduced on the host was a Linux distribution name the Community Enterprise Operating Linux (CentOS).

Two different virtual machines were developed on the host using the Kernel-based Virtual Machine (KVM). KVM is a virtualization programming that permitted analyzers to introduce diverse working frameworks on isolated virtual machines as if it was performed on physical machines. The visitor OS was marked Kali 2020, and the host hostname was given Kali. Kali, an Ubuntu-put together appropriation was introduced for Chris. Allude to informative supplement for increasingly outer set-ups.

#### • Internal Testing Setting Up

The internal testing of the network (a private network) was performed at the computer Laboratory of the campus which was the analyzers focused condition. The analyzer used a very good and efficient personal computer as a setup for the virtual host machine to create a penetration testing condition on the network. The working systems, virtual machines, and testing devices did not any different aside from only the IP addresses used.

Four main instruments namely, Nmap, OpenVAS, and the Metasploit Frameworks were utilized in the entrance testing process. This process was effectively delineating the foundation courses of action which was needed by these instruments. The instruments were presented and used on the analyzers machine to achieve both the internal and external testing objectives. The Kali Linux was used in presenting these instruments. Metasploit Framework Community Edition was installed to replace the Metasploit Framework.



The open ports found on the target host

Port	State	Service	Product	Product Version	Risk Level
22	open	ssh	OpenSSH	5.3	HIGH
80	open	http	Apache httpd	2.2.15	HIGH
443	open	https	Apache httpd	2.2.15	HIGH
3306	open	mysql	MySQL	5.1.73	INFO

Details

**Risk description:**  
This is the list of ports that have been found open on the target hosts. Having unnecessary open ports may expose the target systems to inutile risks because those network services and applications may contain vulnerabilities.

**Recommendation:**  
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

**Fig. 1. Vulnerability scan report 1**

Another instrument that was largely in the penetration testing framework was the Metasploit Framework. This instrument was associated with the Kali Linux default foundation. Regardless, to use the latest version of the system, the installer was downloaded from the Metasploit official webpage. Supplement A shows steps used during the Metasploit game plan.

Nmap was pre-installed in Linux Kali and can be initiated in the Metasploit framework with both the Command Line (CLI) Interface and Graphic User Interface (GUI). As a result, no installation was required, which is needed in the configuration.

OpenVAS was introduced naturally on Kali; along these lines, no establishment was required; in any case, OpenVAS was should have been arranged.

NESSUS is first propelled, either through the Kali Applications menu or by running Nessus at the order line, the fundamental interface will open, giving you your workspace.

At first, the host's sheet will be vacant so you can either import a Nmap examine results document or, as this model shows, click in the sheet on the content "Snap here to include host(s) to scope".

The structure of the Metasploit was set up for penetration testing on the ground's assessment. As concentrated in a writing review, the Metasploit system contains numerous interfaces like msfgui, Msfconsole, msfcli, and so on. Msfconsole was utilized as an approach to get to the Metasploit system.

Armitage has GUI and CLI was used for the penetration testing on the campus network. This is a version of the Metasploit framework that enables the tester to use both the command line and graphical user interface to test the network.

#### 4. ANALYSIS AND DISCUSSION OF RESULTS

The analyzer's machine was associated with the objective system for performing outside infiltration testing using the web or the internet. The analyzer utilized the burrow apparatuses, similar to *google* and *whois* to question Domain Name Service (DNS) on UEW's space to assemble starter data about the University of Education, Winneba.

Figs 2 and 3 display the report from the whois question to the UEW's DNS

Fig. 4 unveiled the three live hosts of the University of Education, Winneba. The IP addresses discovered are 41.74.91.129, 41.74.91.141, and 41.74.91.153. The report from digging provides the analyst with the information needed on the DNS, web servers, IP addresses, and mail servers. The location of the IP addresses on the servers was uncovered using the DNS inquiry and Fig. 5 is a pictorial view of the hops used to reach the UEW site from its Kumasi campus. The analyzer continued to keenly figure the subnet cover of grounds plan utilizing the Nmap apparatus to examine the system utilizing an alternate subnet veil before downsizing the subnet to a progression of alive hosts. Fig. 6, Fig .7, and Fig. 8 disclosed the

Nmap query on the three live hosts respectively. The reports indicate the open ports on the live hosts. Nmap was utilized to distinguish what number of hosts dwell inside the system and their related IP addresses. Nmap -sV 41.74.91.153/32 utilized a subnet mask of 32. [root@kali ~]# Nmap -sV 41.74.91.153/32

### Whois Record for Uew.edu.gh





Domain Profile	
Registrar	Ghana Dot Com IANA ID: 1499 URL: - Whois Server: -
Registrar Status	ok
Dates	5,716 days old Created on 2005-12-19 Expires on 2025-12-30 Updated on 2019-12-10
Name Servers	
Tech Contact	-
IP Address	41.74.91.153 - -1 other site is hosted on this server
IP Location	 - Central - Winneba - University Of Education Winneba
ASN	 AS37263 UNIVEDU, GH (registered Sep 29, 2010)

Fig. 2. Report from Whois search for UEW IP

IP Location	 Ghana Winneba University Of Education Winneba
ASN	 AS37263 UNIVEDU, GH (registered Sep 29, 2010)
Whois Server	whois.afrinic.net
IP Address	41.74.91.153

```

% The AFRINIC whois database is subject to the following terms of Use. See
https://afrinic.net/whois/terms

% No abuse contact registered for 41.74.80.0 - 41.74.95.255

inetnum:      41.74.80.0 - 41.74.95.255
netname:      UEW-20100413
descr:        University of Education, Winneba
country:      GH
org:          ORG-UW1-AFRINIC
admin-c:      IY1-AFRINIC
admin-c:      EKK1-AFRINIC
tech-c:       EKK1-AFRINIC
tech-c:       RA43-AFRINIC
status:       ALLOCATED PA
notify:        cahinson@uew.edu.gh
notify:        registrar@uew.edu.gh
notify:        vc@uew.edu.gh
notify:        ragyare@uew.edu.gh
mnt-by:       AFRINIC-HM-MNT
mnt-lower:    UEW-MNT
mnt-domains:  UEW-MNT
changed:      hostmaster@afrinic.net 20100413
changed:      hostmaster@afrinic.net 20111013
    
```

Fig. 3. Report from Whois search for UEW IP continued

```

;<<> DiG 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 <<> +additional www.uew.edu.gh. @ns1.uew.edu.gh.
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 28802
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.uew.edu.gh.                IN      A

;; ANSWER SECTION:
www.uew.edu.gh.                10800  IN      CNAME   studldap.uew.edu.gh.
studldap.uew.edu.gh.          10800  IN      A       41.74.91.153

;; AUTHORITY SECTION:
uew.edu.gh.                    10800  IN      NS      ns2.uew.edu.gh.
uew.edu.gh.                    10800  IN      NS      ns1.uew.edu.gh.

;; ADDITIONAL SECTION:
ns1.uew.edu.gh.                10800  IN      A       41.74.91.129
ns2.uew.edu.gh.                10800  IN      A       41.74.91.141

;; Query time: 255 msec
;; SERVER: 41.74.91.129#53(41.74.91.129)
;; WHEN: Wed Sep 8 13:46:40 2021
;; MSG SIZE rcvd: 139
    
```

Fig. 4. UEW digging report from External source

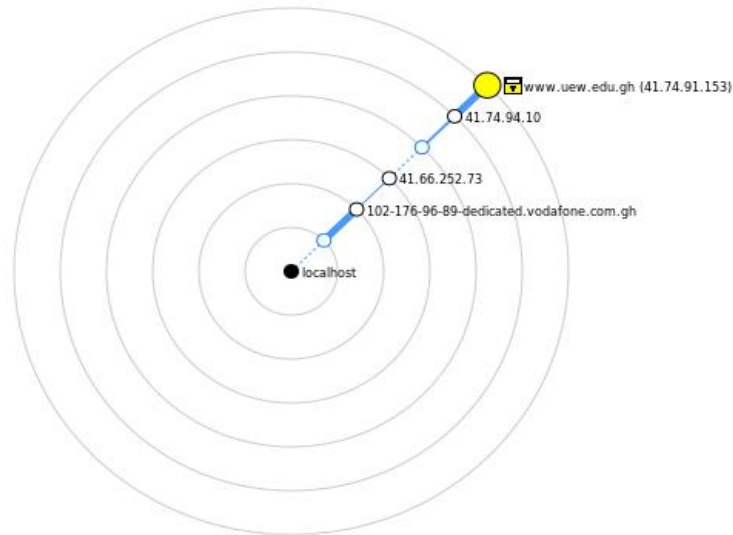


Fig. 5. Fish view of UEW Nmap from Internal

```
(root@kali)~# nmap ns1.uew.edu.gh
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-08 07:13 CDT
Nmap scan report for ns1.uew.edu.gh (41.74.91.129)
Host is up (0.066s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
111/tcp   open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 25.74 seconds
```

Fig. 6. Nmap Scan Report for 41.74.91.129

```
Nmap scan report for ns2.uew.edu.gh (41.74.91.141)
Host is up (0.0088s latency).
rDNS record for 41.74.91.141: www1.uew.edu.gh
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
111/tcp   open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 13.96 seconds
```

Fig. 7. Nmap scan Report for 41.74.91.141

```
# nmap www.uew.edu.gh
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-08 07:16 CDT
Nmap scan report for www.uew.edu.gh (41.74.91.153)
Host is up (0.054s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 30.43 seconds
```

Fig. 8. Nmap scan Report for 41.74.91.153

```
(root@kali)~# nmap -sV 41.74.91.153
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-08 07:38 CDT
Nmap scan report for 41.74.91.153
Host is up (0.0095s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.15
443/tcp   open  ssl/http Apache httpd 2.2.15 ((CentOS))
3306/tcp  open  mysql    MySQL 5.1.73
Service Info: Host: uew.edu.gh

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.43 seconds
```

**Fig. 9. Nmap Scan report for 41.74.91.153**

```
(root@kali)~# nmap -sV 41.74.91.141
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-20 07:57 CDT
Nmap scan report for ns2.uew.edu.gh (41.74.91.141)
Host is up (3.7s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
53/tcp    open  domain   ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)
111/tcp   open  rpcbind  2-4 (RPC #100000)
514/tcp   filtered shell
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:6

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.19 seconds
```

**Fig. 10. Nmap scan Report for 41.74.91.141**

```
(root@kali)~# nmap -sV 41.74.91.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-08 07:40 CDT
Nmap scan report for ns1.uew.edu.gh (41.74.91.129)
Host is up (0.083s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
53/tcp    open  domain   ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)
111/tcp   open  rpcbind  2-4 (RPC #100000)
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:6

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.58 seconds
```

**Fig. 11. Nmap scan Report for 41.74.91.129**

Fig. 9 displays the number of ports scan, service, and software versions on the target host 41.74.91.153. This clearly shown that 1000ports were scanned, 996 filtered ports and 4 open ports were discovered. The opened ports discovered are 22, 80,443, and 3306. The status of open and filtered ports was discussed after collating all the scan reports.

The other host IP addresses detected after digging the campus network of UEW were 41.74.91.141 and 41.74.91.129. Nmap scan was run on them too as shown by the figures above:

```
[root@kali ~]# nmap -sV 41.74.91.141
```

Figs. 9, 10, and 11 show that 3 live has to react to ICMP parcels were recognized. The 3 live has were filtered and recorded. ICMP ping clear output led from outside the system may not generally yield any noteworthy data in insight gathering because not all associations ordinarily permit ICMP opposing their hosts and systems. Devices used in filtering the ports procedure were utilized with various conventions like TCP or UDP to beat ICMP's wastefulness. The discovery of OS and administration unique finger impression Nmap was utilized.

The results of the ACK filtering testing against the three hosts found in the objective system are

shown in Table 1 below. The results showed some default ports on the host network that were not filtered. In the cause of the process, the traffic catching procedure was done by TCP dump. The scanning proposed there was a firewall running on the network since the host on all the 3 live hosts returns the RST flag. The TCP ACK scan process could not detect which ports were closed or open in the network. In view of this, the TCP SYN scan and the TCP FIN scan were utilized against the host. Between the TCP and UDP scans, the UDP scan was found out to be consuming a lot of time as compared to the TCP scans. However, regardless of a moderate UDP examination, it helped UDP examination, it helped in confirming and understanding the objective system. The Nmap orders executed while gathering insight are recorded underneath:

Nmap switches - sS is for SYN examine, - sU for UDP check, - T4 indicated the filtering mode as Aggressive, - p as port range, - A for administration identification and standard snatching, and - oX for the yield record.

Additionally, fingerprint techniques were used to gather information on operating systems, services, and versions of each targeted host. When an open port is found in the target host, services and operating system (OS) running are identified. Currently, most application misuses were composed focusing on OS and administrations. Knowledge Gathering on OS, administrations, and variant data could help tight down the rundown of expected shortcomings and vulnerabilities. Affirmatively, using fingerprinting strategies was useful in finding important pieces of information on potential weaknesses and adventures inside the objective system framework.

Nmap was used to dissecting the bundles got when SYN parcels are provided in the open and close ports. The banner grabbing technique was used to identify services using the sV flag of Nmap. This banner was utilized to snatch significant from every application on all have, all the yields were sent out into independent content documents. These outcomes are introduced in Table 1 below:

**Table 1. Information gathered from an External point**

Host Address	Open Ports	Services	Operating System
41.74.91.129	22	Ssh	OpenSSH 5.3
	53	Domain	RedHat Enterprise Linux 6
	111	Rpcbind	RPC#100000 2.4
41.74.91.141	22	Ssh	OpenSSH 5.3
	53	Domain	RedHat Enterprise Linux 6
	111	Rpcbind	RPC#100000 2.4
41.74.91.153	22	Ssh	OpenSSH 5.3
	80	http	Apache httpd 2.2.15
	443	Ssl /http	Apache httpd 2.2.15 (CentOS)
	3306	Mysql	Mysql 5.1.73

**Table 2. Information Gathered from Internal Scan**

Host	Open Ports	Services	Operating System
41.74.91.129	22	Ssh	RedHat Enterprise Linux 6
	53	Domain	Linux 6
	111	rpcbind	
41.74.91.141	22	Ssh	RedHat Enterprise Linux 6
	53	Domain	Linux 6
	111	rpcbind	
41.74.91.153	22	ssh	CentOS
	80	http	
	443	http/ssl	
	3306	Mysql	

The analyzer's PC with Linux Kali and all the pen test instruments introduced on it as talked about before. This PC was associated straightforwardly with the college's system in the PC lab through a divider plate associated with a 24-port unmanaged switch. Nmap was utilized as the principle beginning data acquisition device.

When the machine was associated with the system, the packet fence interface was started to enter username and secret phrases give you access to the web. A Dynamic Host Configuration Protocol (DHCP) server consequently allocated an IP of 10.20.0.155 a short time later. Nmap support was propelled in a comparative arrangement, and switches/alternatives were utilized to lead the underlying output as was done on the outer system examine and the consequence of the sweeps was spare into a database.

4096 hosts were found on the inward system fragment when the underlying output with Nmap was led on the interior system portion.

Table 2 shows the consequence of the underlying output of the inside system.

The host finding in the data-gathering stage was utilized to supplement the examining and powerlessness evaluation method applied to the hosts. Robotized scanners and manual strategies are utilized to check and distinguish vulnerabilities. All the more along these lines, the computerized and manual checking procedures ought to be utilized for a bit of extensive information about the potential vulnerabilities that may have influenced the framework or system. Manual methods require more opportunity to finish the powerlessness check and because of time limitations, the mechanized scanners were utilized. In the offer to upgrade the exactness of the defenselessness check, two diverse powerlessness scanners were utilized to test the hosts found.

OpenVAS and Nessus were chosen to decide the vulnerabilities present in these basic frameworks. These two scanners were utilized to recognize the OS and administrations running in the objective hosts, which has and benefits were defenseless. Table 3 below reveals the hazard factors and their comparing Common Vulnerability Scoring System (CVSS) Base Score rage. These hazard factors were seller explicit so any Severity marked 'Basic' on

Nessus might not have a similar degree of seriousness utilizing some different scanners. Consequently, chance components ought to be thought of as rules as it just mirrors the CVSS base score.

The OpenVAS organization was used to perform the vulnerability scan. This scan was conducted against the internal and external network segments.

Vulnerability scan result for 41.74.91.129 According to the OpenVAS documentation and Nessus documentation, all vulnerabilities recognized were marked as being False positive, Log, Low, Medium, and High relying on the CVSS base score as shown in Tables 4, 5, 6, and 7 show the separated outcomes for OpenVAS based on the open ports on the three live hosts, whiles Tables 8 and 9 indicate that of Nessus. Dangers marks as Log and False Positive were excluded from the table.

The home transmission release was utilized for surveying the defenselessness against the objective hosts of the grounds network. The output was executed against the hosts on the 41.74.91.129/32 system section and a similar scan configuration was utilized to check for susceptibilities on the 41.74.80.0/20 system portion. The output report incorporates the outline, depiction, arrangement, hazard factor, a reference identified with the distinguished susceptibilities.

Reports from OpenVAS and, Nessus showed that hosts on Campus networks were susceptible to information disclosure, spoofing, buffer overflow, remote code execution, the elevation of privilege, and Denial of services. The vulnerabilities identified were studied to verify whether they were exploitable or not.

To upgrade the abuse and post-misuse stages, the examination was increased. Robotized weakness evaluation apparatuses were noisy yet couldn't show the real security stance of the general framework or system. There could be conceivable bogus positives and bogus negatives. The OpenVAS and Nessus gave a decent pattern to examine the security of frameworks and system foundations. They additionally assisted with recognizing unpatched applications and security settings that are out of consistency.

In any case, robotized scanners should be a bit of any Network and System head's device compartment or passageway analyzer's toolbox.

These scanners are an asset for IT security at whatever point structured fittingly and without any problem. The two scanners used in the scanning of the network were the Nessus scanner and the OpenVAS scanner.

Nearly, the two scanners ought to be on basic criteria(s) or pattern to choose which scanner was proficient and successful. Thusly, to defeat this problem, a concise examination among Nessus and OpenVAS was performed.

**Table 3. Risk factors based on CVSS based scores**

Risk Factor	Base Score of CVSSv3	Base Score of CVSS v2	Frequency
High	8.5	8.5	20
Medium	6.9	6.9	11
Low	0.0	0.1	8
Info	0		0

**Table 4. OpenVAS Susceptibility Scanning from the External Point (Target host 41.74.91.153)**

Target Port	Critical	High	Medium	Low
22	0	3	5	0
80	0	7	3	0
443	0	7	3	0
3306	0	0	0	2

**Table 5. OpenVAS Susceptibility Scanning from the External Point (Target host 41.74.91.129)**

Target Port	Critical	High	Medium	Low
22	0	5	5	0
53	0	0	0	2
111	0	0	0	1

**Table 6. OpenVAS Susceptibility Scanning from the External Point (Target host 41.74.91.141)**

Target Port	Critical	High	Medium	Low
22	0	5	5	0
53	0	0	0	2
111	0	0	0	1

**Table 7. OpenVAS Susceptibility Scanning Reports from the Internal point**

Target Hosts	Critical	High	Medium	Low
41.74.91.129	1	2	6	5
41.74.91.141	1	2	5	3
41.74.91.153	1	8	9	5

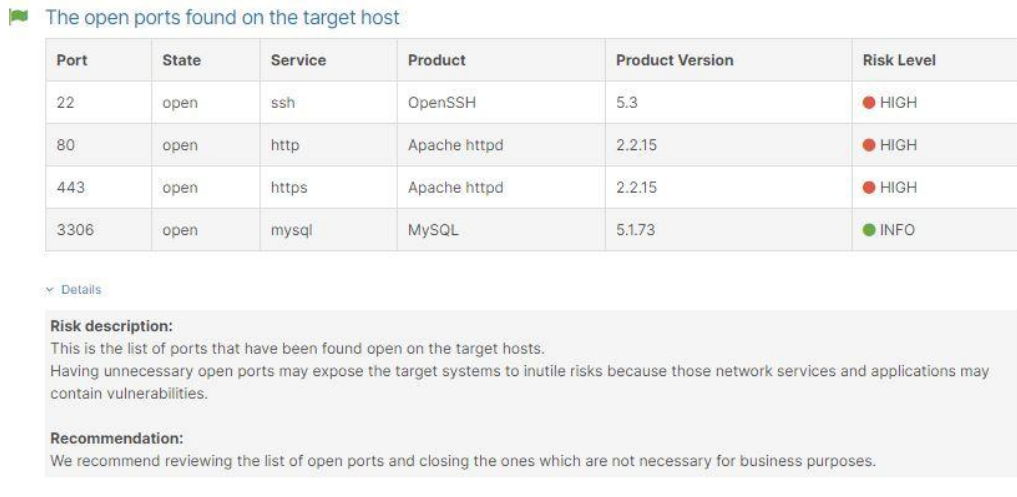
**Table 8. Nessus Susceptibility scans outcome from the External point**

Target Hosts	High	Medium	Low
41.74.91.129	3	5	7
41.74.91.141	4	7	8
41.74.91.153	5	7	9

**Table 9. Nessus Susceptibility Scan outcome from the internal point**

Target Hosts	High	Medium	Low
41.74.91. 129	2	7	5
41.74.91. 141	2	5	7
41.74.91. 153	5	6	10





**Fig. 12. Vulnerabilities found on UEW**

Source: OpenVAS scan

The report in Fig. 12 reveals that there is a high-risk level on open ports 22, 80, and 443. Port 3306 is without vulnerability risk because it is opened for information.

#### 4.1 Comparison of the CVEs results from Nessus and OpenVAS

This evaluation was executed to comprehend which scanner was more beneficial at perceiving more CVEs shortcomings than the other scanner.

OpenVAS and Nessus were refreshed with the most recent modules on a similar date, when the sweeps were executed, Nessus modules check was 61,828 and OpenVAS modules tally was 59,329. Nessus distinguished 905 CVEs susceptibilities out of each of the 3,152 susceptibilities while OpenVAS recognized 948 CVEs susceptibilities out of every one of the 2,925 vulnerabilities Nessus or OpenVAS or both. Table 10 below is the tabular representation of the outcomes.

Fig. 13 underneath showed all the CVE recorded shortcomings which both the Nessus and OpenVAS ordered during the extents.

Indisputably the number of weaknesses, and CVE recorded weaknesses found by every single scanner the effectiveness of the Nessus scanner and the OpenVAS were resolved. Table 8 displays realize the level of all CVEs weaknesses recognized by Nessus and OpenVAS. OpenVAS was progressively feasible and beneficial at discovering CVEs recorded

weaknesses, then Nessus. Along these lines, it was sheltered to suggest OpenVAS as a dependable and proficient defenselessness scanner. Be that as it may, Nessus had a bigger modules database, thorough announcing strategies with a broad pre-characterized sifted which made it an intriguing choice. Further examination could have given much better thought regarding the two scanners. Contingent on the time compels, Penetration analyzer or Network and System Administrator can perform Scanning and Vulnerability Assessment stage, utilizing either Nessus or OpenVAS or both. Utilizing the two scanners can give a superior image of the system or the frameworks.

#### 4.2 Internal Penetration Testing

##### 4.2.1 Exploiting Host on 41.74.91.129

Impelling the Metasploit Framework Msfconsole request was used to lunch the Metasploit framework in the Kali machine. Msfconsole was used to dispatch manhandles, load partner modules, search abuses, and perform enumeration against the goal set.

A search request was used to examine the undertaking. Both the Nessus and OpenVAS had featured MS15-030 undertaking, so 'ms15-030'keyword was used as an interest limit.

A command was utilized to stack the particular endeavour module and show alternatives order was utilized to list the module choices.

Using the request exploit the analyzer attempted to manhandle the host, 41.74.91.129.



This was not a powerful undertaking exactly as expected considering the way that a gathering affiliation was needed. In any case, if this was some web worker or database worker and crushing the worker was still be a Denial-of-Service condition. Along these lines, this was considered productive abuse.

The run order was utilized to execute misuse, to confirm that the attack was fruitful a PC was associated legitimately to a switch in the PC lab which is connected to the college system to check if the approved DHCP server will give an IP to the PC. The PC couldn't get a programmed IP address from the server, anyway, when the PC was designed with a static IP address of 41.74.91.129 and a ping test led against the 41.74.91.141 host, it was found that the host was alive. Although the DHCP server was alive it couldn't issue any longer IP address this implied the IP pool was depleted affirming that the assault was fruitful.

At the point when the objective frameworks were undermined, the specialist endeavours to

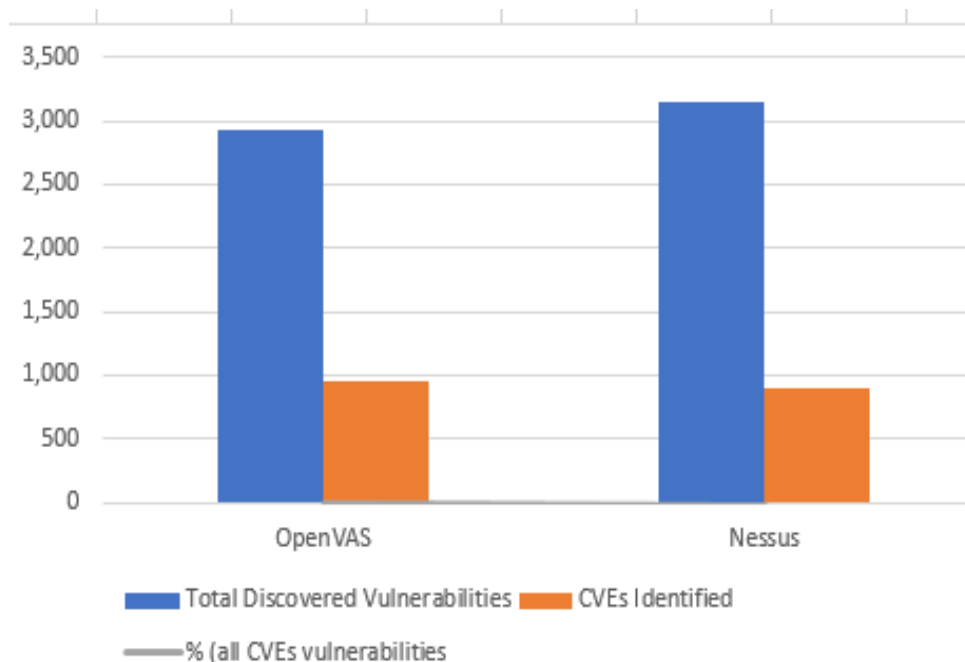
distinguish the framework's expected exposures and adventure the shortcoming, to discover how profound analyzer /assailant can get inside the framework or system. Contingent on the entrance test extension and analyzer's capacity post-abuse had boundless prospects.

From the scientist's point of view, this progression filled in as a method for exhibiting what an assault can do and indicating the conceivable reactions when the system or framework is undermined.

In the system, has on 41.74.91.129, 41.74.91.153, and 41.74.91.141 were effectively undermined utilizing Metasploit structure dependent on the exploitable vulnerabilities the analyzer was not too fruitful abusing the host on 41.74.91.129. Anyway, key client accounts subtleties were found because of the assault on the host, with this data a genuine assault can utilize advanced secret phrase devices to break into the host.

**Table 10. Scanners Efficiency**

Scanners used	Plug-ins	Total Discovered Vulnerabilities	CVEs Identified	% (all CVEs vulnerabilities)
OpenVAS	59,329	2,925	948	51%
Nessus	61,828	3,152	905	49%



**Fig. 13. Comparison of Nessus and OpenVAS CVE**

## **5. CONCLUSIONS**

The outcome that was gotten after the experiment in this proposal indicated that infiltration tests had a worth whenever acted in an efficient and a laid down procedures and processes. Thus, if assessing the infiltration rate of a system is assigned to the Systems Administrator's as part of his obligation, which is not exclusively can such tests supplement the other errand executed to additionally fortify the system or framework yet it might help with finding a few vulnerabilities or escape clauses in the framework or system foundation. Penetration test ought not to be seen as a stress on the System Administrator but preventive measure.

The primary objective of this proposal planned is to check if the level of framework controls actualized by UEW System Administrators was sufficient to protect the college from external-based hacks or intrusion. Security control instruments actualized on the campus network's organized framework are insufficient, edge barriers and like was left unattended to. For example, the outcomes obtained using Nmap uncovered that practically all hosted ports checked were not sifted. The analyzer didn't experience any edge protection gadget when directing the assault from the outside or remote location, the system did not execute any firewalls on the borders of the system. On the off chance that to be sure there was, it might have been misarranged. Likewise, from the inside point inside the UEW network, the analyzer had the option to join the assaulting machine to the system and effectively get an IP address to direct the attack from the inner section secretly by the interruption location framework (IDS) on the system. This demonstrated that contraption may be a few mistakes in the planning procedure and the prioritization of the security identifying with the issues of the port was not completed. This prompts the request. In any case, oftentimes System and Network Administrators are expected to encounter these tests? what's more, this solicitation has not been answered yet by any demonstrated equation. The rehash of such a test ought to rely upon how routinely significant control is made to the system condition. The noteworthiness of importance may shift starting with one Network and System official then onto the accompanying. For example, including or erasing a client account data isn't a significant change yet including another worker or resuscitating the part or refreshing the Internetwork Operating System (IOS) of a switch

protected the entry testing. Thusly, invasion testing should be established true to the form of risk-related within a framework or structure, size, and nature of the affiliation.

Aftereffects of the weakness filter and the infiltration experiment likewise demonstrated that the UEW network foundation was defenseless against attacks including forswearing of administration (DoS attacks), the underlying driver of these recognized vulnerabilities was fundamentally unpatched programming and misconfiguration of gadgets on the system. Even though all the operating systems discovered were mostly fixed with the most recent fix the administrations and application of the projects were not fixed which makes the system helpless. For instance, the IDS gadget on the system didn't distinguish any of the systems evaluation and clear ping exercises completed by the analyzer during the test, this showed the gadget might not have been arranged appropriately to find clear pings.

The analyzer distinguished the intricate idea of a run of the mill college system and frameworks foundation, and the colossal number of clients relying upon the system foundation as a significant test as this doesn't bear the cost of the frameworks and system overseers the scope of time to direct a careful and successful infiltration test.

However, the finding of this proposal was limited to only the test reports of OpenVAS and Nessus, though other vulnerability scanners were used passively to authenticate our findings.

## **6. FUTURE WORK**

Any future researcher can look into the following line of work and consider the topics below in their research:

(a) Another project can be looking at how to automate the penetration testing system to come out with a more secured and robust security testing course of action as an increase of this hypothesis work. This development can serve as an aid to the Network and System Administrators to test and know the level of their ICT tools without any hindrances.

(b) Proposal research can be stretched out to expand the proficiency by additionally regarding human factor during a penetration examination. The focal point of this postulation was on finding and misusing susceptibilities identified with PC frameworks and systems found in this manner

human factor was not thought of. Be that as it may, workers inside the association might be the most fragile connection in security. Along these lines, this study can be stretched out by coordinating social designing instruments and procedures into the leaving entrance testing approach.

## CONSENT

The goal and consent given to the analyzer by an official administration draw out the distinction between penetration analyzer and attacker according to discoveries.

## ETHICAL APPROVAL

As per international standards or university standards written ethical approval has been collected and preserved by the authors.

## COMPETING INTERESTS

Authors have declared that no competing interests exist.

## REFERENCES

1. Appiah M, Chandrasekaran S. U.S. Patent No. 18,701,102. Washington, DC: U.S. Patent and Trademark Office; 2014.
2. Computer Science Degree Hub. FAQ – What is Information System Security, Retrieved from Computer Science Degree Hub; 2020. Available: <https://www.computersciencedegreehub.com/faq/what-is-information-systems-security/>
3. Bourgeois D, Bourgeois, DT. Chapter 6: Information System Security. In D. Bourgeois, DT Bourgeois. Information System for Business and Beyond (p. Chapter 6). Press Books; 2014.
4. Scarfone K, Souppaya M, Cody A, Orebaugh A. Technical guide to information security testing and assessment. NIST Special Publication, 2008;800(115):2-25.
5. Computer Tech Reviews. Definitions; 2020. Available: Computer Tech Reviews: <https://www.computertechreviews.com/definition/penetration-test/>
6. Northcutt S, Novak J. Network intrusion detection. Sams Publishing; 2002.
7. Hudson DA, Manning CD. Compositional attention networks for machine reasoning; 2018. arXiv preprint arXiv: 1803.03067.
8. Glover M. U.S Patent No. 6,763,466. Washington, DC: US. Patent and Trademark Office; 2004.
9. Conforti M, Pascale S, Robustelli G, Sdao F. Evaluation of prediction capability of the artificial neural networks for mapping landslide susceptibility in the Turbolo River catchment (northern Calabria, Italy). Caten, 2014;113:236-250.
10. Ernest MD, Notkin D. Dynamically discovering likely program invariants. University of Washington; 2000.
11. Claffy K, Clark D. The 10<sup>th</sup> workshop on active internet measurements (AIMS-10) report. ACM SIGCOMM Computer Communication Review. 2019;48(5): 4147.
12. Fashoto SG, Ogunleye GO, Adabara, I. Evaluation of Network & System security using Penetration testing in a simulation environment GESI: Computer Science and Telecommunication. 2018;17
13. Allen L, Heriyanto T, Ali S. Kali Linux- Assuring security by penetration testing. Packt Publishing Ltd.; 2014.
14. Acharya S, Pandya V. The bridge between Black Box and White Box Gray Box Testing Technique. International Journal of Electronics and Computer Science Engineering. 2012;170–120.

© 2021 Adu-Boahene et al.; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

### Peer-review history:

The peer review history for this paper can be accessed here:  
<https://www.sdiarticle4.com/review-history/73420>