ADDIS ABABA UNIVERSITY SCHOOL OF GRADUATES STUDIES DEPARTMENT OF INFORMATION SCIENCE

Network Security Assessment, Risk Analysis and Mitigation Techniques: The Case of Hawassa University Enterprise LAN

A thesis submitted to School of Graduate Studies of Addis Ababa University in partial fulfillment of the Requirement for the Degree of Master of Science in Information Science

By

ALIAZAR MERDEKIOS KEBA

October, 2017

Addis Ababa, Ethiopia

Acknowledgment

First and above all, I praise the almighty God for providing me this opportunity granting me the capability to proceed successfully in all the ups and downs. This thesis appears in its current form due to the assistance and guidance of several people. I would therefore like to offer my sincere thanks to all of them.

Dr. Workshet L, my esteemed Advisor, my cordial thanks for giving me the freedom to do my thesis in this area, for your warm encouragement, thoughtful guidance, critical comments, and correction of the thesis. I would like to thank you especially for friendly assistance with various problems all the time.

My deepest gratitude goes to Ato, Yoseph Debele & Ato Tamerat Chane for the trust, for your insightful discussion, offering valuable advice and materials, for your support during the whole period of the study, and especially for your patience and guidance during the writing process.

I greatly appreciate my good friend [Tsega, Abi, Paul, Mess, Ashu, Samiwara] who stand beside me, your excellent assistance and supports for me during my study was enjoyable and helpful. I will never forget the time that we were together and discussed about many issues. I warmly thank and appreciate my parents and my mother, sisters, and brother, brother-in-lows and nephews for their support in all aspects of my life. I thank you guys from the bottom of my heart!

Abstract

Today we live in a connected world. Communication is a key requirement for all systems and businesses. Increased integration of services and systems requires a compulsive need to establish fast and reliable communication that is as widespread as the organization and its business dealings. Information systems need to reach out to users, vendors, customers and partners (irrespective of their location); everything is connected to nearly everything else. All this brings us to the issue that looking at any system as something that is inside one box or in one enclosed space is not enough to gain assurance about its security.

Any major Ethiopian institution has a substantial number of computer systems on its campus, often in the scale of thousands. Hawassa University (HU) is one of the few Universities in the Country; who established a very well LAN infrastructure connecting thousands of nodes for the provision of Unified communication services (intranet/internet services) in its campuses located in and out of the city. Recently most of the campuses are interconnected with 10 GB fiber Optic cable backbone.

Due to several security risks enterprises running small-to-large sized businesses face daunting tasks that just a few years ago were not existent; the complexities of the business world have created new risks. Several methodologies, Security Assessment tools and techniques are designed to detect and report on security holes within software applications, allowing organizations to take corrective actions before devastating attacks occur. The common trend in several organizations related to the computer security is investing a tremendous amount of money for purchasing and deploying of security appliances, virus and spy ware protections and other actions sightlessly, without making detail requirement analysis on a specific scenario of a corporate services and business process applications. However, in most cases security assessment for its services and applications has overlooked so far. This research tried to carry out the detail security assessments over HU LAN Active devices, services and applications, the associated risks and put forward appropriate counter measures to fix the holes.

Table of Contents

List of Figures

List of Tables

Chapter One

1.1. Background of the Study and Rationale of Domain

In modern information era companies, organizations, schools and other corporations build and manage a more complex and sophisticated enterprise networks infrastructures for the sake of facilitating and enhancing their business. Mainly schools/universities are running a full-size enterprises network infrastructure to process, store and transfer information which significantly help them to achieve their goal they stand for like learning teaching, research, community work and other internal business inside the system. [30] However, most of common users who are using a network infrastructure don't have a detailed know how of how the network system works and how information streams all the way through the system. The users just enjoy the functions of the network, the ability to post messages to social media sites, make phone calls, search for information on the Internet, listen to music, and download and use countless apps and resources to their computers, tablets and phones without caring about how it works or how their favorite device connects to the network.

In recent years the advancement of the communication technology is rapidly increasing and the necessity of using network infrastructure is becoming vital to organizations and individuals to cope with the current changing environment of this highly competitive digital world. Alongside the benefit of networks systems for both individuals and organizations, the safety of the system and privacy of information is challenged by overwhelming flooding threats of hackers which use the vulnerabilities to exploit the systems we use.

Vulnerabilities could exist in numerous areas in our environments, including our architectural design, business processes, deployed software, and system configurations [10] and the attackers use different exploits as a vehicle to cause damage to the target system.
The vulnerability assessment process carefully identifies, prioritizes (ranking of risks) and quantifies all the vulnerabilities in a non-invasive manner. [5] Security vulnerabilities, such as weak configurations, un-patched systems, and botched architectures, continue to plague organizations. Enterprises like universities need people who can find these flaws in a

professional manner to help eradicate them from our infrastructures. [9] Hawassa University(HU) as educational institute already implemented enterprise LAN and it sooner or later need someone to assess its LAN infrastructure to identify and correct flaws formed due to several reasons.

Hawassa University (HU) is one first generation university in Ethiopia which located in SNNP region capital Hawassa town. [13] At the time of establishment of Hawassa University in April 2000, there was no Internet connection to speak of, except for few dial-up connections at some offices. After the establishment of the ICT Center in late 2000 with some 20 computers at its disposal, a shared dial-up Internet connection was introduced which, for the first time, started to serve the University staff to get access to the Internet (WWW and EMAIL). [13]

In the year 2003, the Ministry of Education (MoE) has sponsored the establishment of campus-wide networks at the Awassa College of Agriculture, Wondogenet College of Forestry and Dilla College of Teachers Education and Health Sciences (DCTEHS). Soon after the deployment of the network, a broadband Internet connection was introduced.

In the year 2008, a campus-wide network was established at the main campus. Moreover, the three campuses at Hawassa City, i.e. the Main Campus, the College of Health Sciences and the College of Agriculture, were interconnected via fiber-optic cables and these campuses were connected to the Internet through two gateways (at the Main Campus and the Awassa College of Agriculture).

The university subscribed a broadband fiber connection with bandwidth of 80Mb from Ethio Telecom which currently connected to main campus data center and serves as major back bone. Recently all three campuses except Wondo Genet Forestry campus are interconnected with 10 GB fiber Optic cable backbone in a star fashion *(Figure 1.1).* For the provision of Unified Communication services (various Internet/Intranet services), somewhat hierarchically designed network connecting almost all the buildings has been established. Over 5000 network nodes have already joined the LAN. HU LAN infrastructure is powered on different vendor products like CISCO, HP, Dell, ZTE, Polycom, Aruba, and others.

At present all the four campuses are having cabled LAN and Wi-Fi connections covers a couple of areas of the Campus's premises including offices, Libraries, Staff Residents, Student Dormitory, Teaching hotels, Cafeterias etc. The university still did not using VPN connection to the campuses but uses direct fiber link only between the three campuses. In all campuses there are VLANs based on their geographic location and applications running in the VLANs. There are 30 VLANs in main campus with IP arrangement of 172.22.0.0/16 and about 25 VLANs in the other two campuses (Agri and Health) having about 20 VLANs with IP range of 10.148.0.0/16. Deployment of extensive Wireless services in key locations had been carried out. The University LAN has highly resilience feature that avoids a single point of failure and provides continuous (24/7) services for the community. Some of the core Services and business process applications available in the University over the LAN are:

- ✓ Intranet
- ✓ Web Caching and Content Filtration (Proxy): for filtering contents via Squid/Squid Guard Proxy based on Agreed Internet Acceptable Use Policy and caching frequently accessed pages.
- ✓ HU e-mail service and HU official Website: dynamic and extensive information on academic and Administration wings (i.e. colleges, departments, services, etc.)
- ✓ DHCP server: for automatic IP address assignment of nodes on the network.
- ✓ Domain Name Service (DNS):for names to IP address resolution
- ✓ Backup Service: a server to back up - a disk-based storage system
- ✓ Student Information System (SIS)
- ✓ Human Resource System(HRS)
- ✓ Library Information Management System(LIMS)/ Koha
- ✓ E-learning, BSC, IBX finance systems and etc

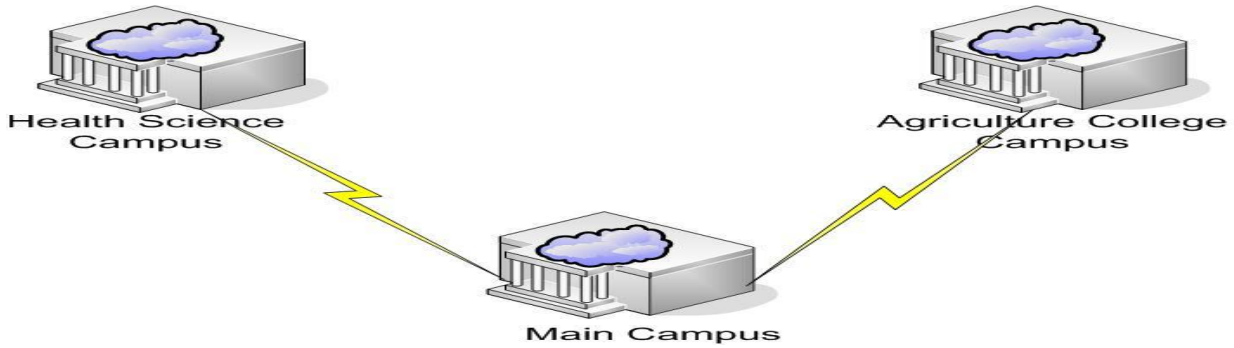


Figure1.1. *HU campuses Fiber connection*

The University ICT Development Center put high effort to upgrade the established LAN infrastructure and services to meet current industry standard. A lot of money has been invested to leverage and enhance the full power of existing infrastructure. Recently in HU a couple of new services and major business process applications pointed out above and many other LAN services have been developed on a production network. However, only few measures have been taking place to secure the services and applications from the inside and outside attacks. Some of the measures that has [been taken so far include; deploying hardware and software based Firewalls for content filtering and caching, i.e. Cisco Adaptive Security Appliance (ASA) is deployed at the edge of HU LAN, proxy (squid and squid guard) is placed in the inside network. Though the aforementioned actions had been taken without making detail analysis of the service's vulnerability that will encounter because of threats, it has been playing a great role in securing the services and applications.

The architecture of HU network has internal, external and demilitarized zone (DMZ) links, in the inside and DMZ networks, numerous services and business process applications are deployed on Linux/Unix and Windows platforms. The most sensitive services and applications that required to be secured such as HU official website, Mail server, HRMS and others are placed in DMZ network; in which any external and internal user has access within specified privilege. The rest of the services and applications are placed in the inside network.

In this research by following several methods and methodologies using various tools and techniques; the vulnerabilities are identified, classified (as high, medium and low risk vulnerability), make risk analysis and put forward mitigation measures to patch the holes. .

Although assessment identifies both technical and non-technical weaknesses (e.g. procedural deficiencies), the basically assessment is focused on an in-depth analysis of technical vulnerabilities. The following Logical design shows the placement and arrangement of network core devices and service servers of HU's network infrastructure.

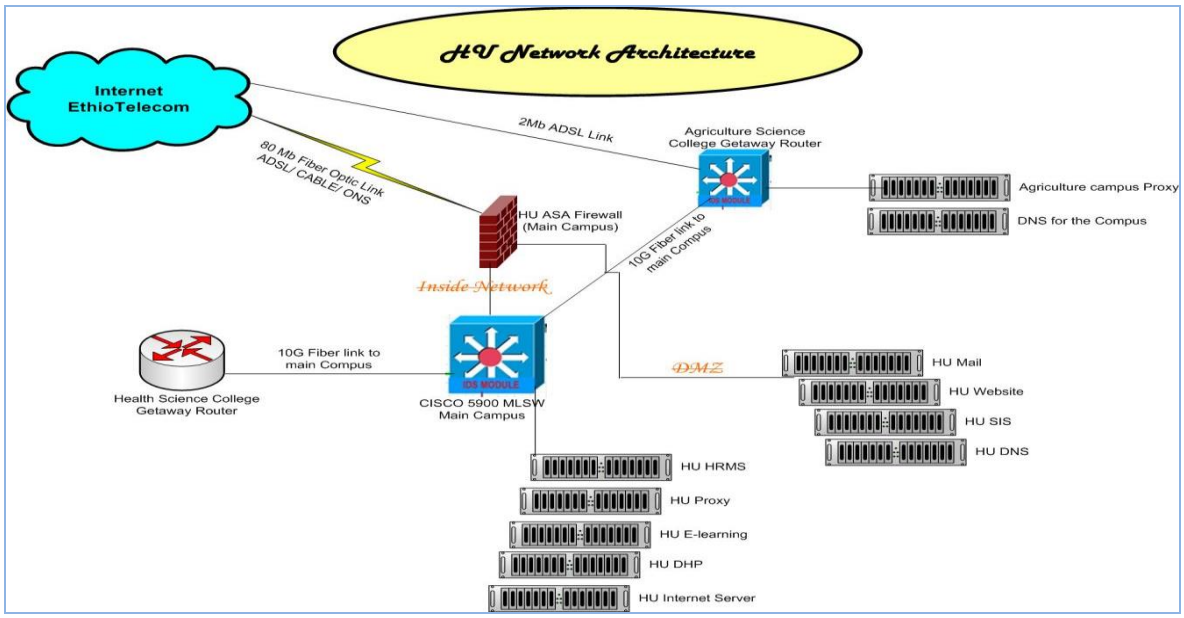


Figure 1.2. HU Network Topology Architecture

1.2. Statement of the Problem

In the present day, due to several security risks enterprises running small-to-large sized businesses face daunting tasks that just a few years ago were not existent; the complexities of the business world have created new risks. According to the study conducted by Kaspersky ***[15]*** during the second quarter of the year 2012, a total of **31 687 277** vulnerable programs and files were detected on the computers of Kaspersky Security Network users. From this study "System Access", "Denial of Services (DoS)", "Exposure of sensitive information", "Security bypass, Cross site scripting (XSS)" and "Manipulation of data" were the top six vulnerabilities detected on the systems.

The common trend in several organizations including HU related to the computer security is investing a lot of money for purchasing of security appliances, virus and spyware protections and other actions sightlessly, without making detail requirement analysis on a specific scenario of a given organization services and applications.

Hawassa University is one of the few universities in the country which established a very huge

LAN infrastructure, services and business process applications. However, due to lack of awareness and related issues vulnerability assessment and risk analysis part of the services are given less attention i.e. security assessment has never been done so far.[13]

The primary vulnerabilities on services and applications over the LAN are typically plagued by one or all of three weaknesses: such as Administrative security, Technical security and Physical security. [7]

Unauthorized discovery and mapping of systems and services; entering or accessing systems to which one does not have authority to access usually involves running a hack, script, or tool that exploits a known vulnerability of the system; disabling or corrupting LAN systems with the intent of denying services to intended users(this kinds of attack may crash the system or slowing down to the point that it is unusable); Malicious software's that can be inserted into a host to damage a system, corrupt a system, replicate itself; or deny services or access to LAN systems and other threats are the potential classes of attacks that use the aforementioned weaknesses over the HU LAN.

The risks that will encounter HU LAN systems related to the vulnerabilities will be compromising the availabilities, integrity and confidentiality of information in the University, i.e. it includes:

- If proper security measures are not incorporated into HU LAN systems, data breaches may occur through the use of external devices, such as laptops, mobile phones, or personal digital assistants (PDAs).
- If levels of access to the applications and services are not commensurate with information security parameters (such as passwords), there is a risk of unauthorized modification of data, or outright loss of data.
- If HU does not establish security standards and practices and implement them with information security software, HU employees themselves may unwittingly expose the University to compliance violations.

1.3. Objective of the study

1.3.1. General Objective

The general goal of this research is investigating and discovering vulnerabilities and the associated risks, and designing a possible counter measure for the identified vulnerabilities over HU LAN services and Applications accessed in and out of campuses.

1.3.2. Specific Objectives

The following specific objectives were sought to be achieved:

- ✓ Identify vulnerabilities over selected core HU LAN Active devices, services and business process applications based on OSI seven layers
- ✓ To find out and analyze the technical and administrative security issues or flaws exists in HU enterprise LAN
- ✓ Only selected controlled exploitation on available vulnerabilities were carried out
- ✓ Finally appropriate defense mechanisms with suitable counter measures are recommended to improve security stance of organizational and personnel at HU LAN and forward recommendations for further study.

1.4. Research Methodology

This research followed the method to perform security assessment after reviewing each of the open source testing methodologies and accepted standards for information security. As they provide useful insights in to testing from various different perspectives, we developed our own customized testing methodology to conduct security assessment on services and applications and provide a complete picture of risk assessment process.

The methodology prevents common vulnerabilities, or steps, from being overlooked and gives clients the confidence that we look at all aspects of their application/network during the assessment phase. *[23]* Whilst we understand that new techniques do appear, and some approaches might be different amongst testers, they should form the basis of all assessments.

The research approach first identified the questions that need to be answered; hence, various procedures and a set of execution steps had been carried out by giving answer for the following questions:

- ✓ Which Data Center Active devices, Services and Application have to be tested? (i.e. Security assessment type)
- ✓ What kind of sampling techniques ought to be used for the test?
- ✓ What kinds of tools and attack techniques should be used?(i.e. Assessment techniques)
- ✓ How devices and services should be tested and the procedures should be applied before, during and after the test?
- ✓ What security metrics can be used to evaluate the security vulnerability and risks posed by the identified risks? How to interpret and correlate the final analysis results?

The following section of the approach will answer each of the aforementioned lists of questions respectively:

1.4.1. Sampling Techniques Used

To answer the above bulleted questions in the Research Methodology section which is the research approach first identified and the core network devices listed in the after mentioned questions which are basically affect the security posture in any enterprise network infrastructure, we purposively selected and categorized the core devices to assess as follows:

- Network devices Security: We mainly focus on the likes of "Access Switch Security Assessment", "Router Security Assessment" and "Firewall security Assessment"
- Host Security: For the hosts in the network we may focus on "Web server Security Assessment", "Mail Server security Assessment", "DNS Server security Assessment", and "DHCP server security Assessment"
- Application and Data base security: Web Application and Data Base Security Assessment

So far HU LAN infrastructure is powered on by few vendor equipments at each layer and also different platforms (Windows, Linux/Unix, Networking device's IOSs) are installed on the systems.

Active devices which are part of this research, deployed on the production network are:

- ✓ Layer 2 Switches (Cisco2960 and Cisco3500)
- ✓ Layer 3/Multilayer Layer switches (Two Cisco6509, Three Cisco6513)
- ✓ Firewall (Two Cisco ASA 5510)
- ✓ More than three servers for different services and business process applications

Among the available sampling techniques, this research followed stratified sampling which is a variant on simple random and systematic methods and is used when there are a number of distinct subgroups, within each of which it is required that there is full representation.

A stratified sample is constructed by classifying LAN equipments based on the characteristics they have, i.e. Classification of Network equipments had been taken based on the OSI layer they are working (Layer 2, 3, 4 and 7 equipments). The selection of elements is then made separately from within each stratum;

- ⇨ For layer two switches, since their configuration is almost identical (i.e. only location and management IP is different), therefore only three switches (one from each model) are selected for the test.
- ⇨ For layer three Switches (Routers), one from Cisco 6506 and from Cisco 6509 model had been tested
- ⇨ Since both existing Firewalls have the same configuration (only their IP address is different) one of these had been taken

Finally, as it is clearly indicated on the scope of this research, among the available services and applications over the HU LAN, for those which are given high priority by considering their higher impact of the vulnerability if an attacker is able to compromise. Therefore, services and applications like: DNS and Proxy servers, Web Server, Mail server, DHCP server, Student Information System (SIS) are included in our test plan.

1.5. Scope and Limitation of the study

During this research there have been restrictions to undertake the study. Black Box testing method is mainly used because the university ICT development office responsible for managing the network infrastructure don't have enough formally documented resources to provide us the required technical documents (Security Policy, Core devices Configuration files, etc) to analyze. So far, vulnerabilities on services and applications over the LAN are typically plagued by one or all of the areas of weaknesses: (i.e. Administrative, Technical and Physical security) and performing security testing in all devises, services and applications at university enterprise network infrastructure would be time taking (even more than a year or two) and also requires investment of huge amount of money. However, this research focused on all security issues on few core HU LAN systems in main campus data center and services

distributed in side main campus LAN infrastructure, i.e. sensitive LAN device, services and applications are selected based on the impact they have if they are compromised. The assessment process will identify mainly technical weakness and environmental (Physical, administrative) weaknesses in a network.

1.6. Significance of the Study

A university LAN system services are one of the backbone to realize mission and vision of the University; these systems support decision making, such as program planning, resource allocation, product and service selection, etc. Therefore, ensuring availability, maintaining integrity, protecting University's confidential information not to be hacked should be given high attention. The main significances of this research include:

- ✓ All the systems should maintain the expected performance, be secured, easy for administration and support to achieve the goal of core business processes (i.e. teaching learning and research and extension processes) of HU under Ministry of Education Government of Ethiopia.
- ✓ The IT professional like System and Network Administrators will be aware of that how much vulnerable the LAN system is, and prepare the available counter measures
- ✓ The university will make ensure the security of services and network and may look towards adopting appropriate measures against threats posed to their systems
- ✓ The proposed mitigation techniques will help to correct improper configurations and incorrect deployment of devices and services, Patch holes in the servers, etc.
- ✓ Organizations, Business process owners (i.e. policy developers, University Registrar, Property administration, Human Resource Managers etc.) and individuals who has direct or indirect relation or access to HU resources including Government, the university community (students, Instructors, researchers, Administration staffs) will be benefited.

  Apart from this, the research finding can be an input for other same institutions that have the same infrastructure with HU and also aid as a reference for future researchers in the domain in future endeavors.

2. Chapter Two

2.1. Review of Literature

This chapter provides a review of relevant literatures in the areas of vulnerability assessment, exploitation, various methodologies, risk analysis and counter measures.

Vulnerabilities could exist in numerous areas in our environments, including our architectural design, business processes, deployed software, and system configurations [33]. Security assessments (Vulnerability assessments) are focused on finding vulnerabilities [7]; using the available flaws on the LAN, threats can cause harm to the target organization and whenever there is any vulnerability that a given threat can attack LAN systems will be compromised and have great risks. The attackers use different exploits as a vehicle to cause damage to the target system.
Vulnerability assessment is a process for assessing the internal and external security controls by identifying the threats that pose serious exposure to the organizations assets [3]. The vulnerability assessment process carefully identifies and quantifies all the vulnerabilities in a non-invasive manner.

2.2. Vulnerability Assessment Records

According to Kaspersky Security Network study in 2012 second quarter [22], Kaspersky Lab products detected and neutralized over 1 billion threats, a total of 89.5 million URLs serving malicious code were detected and a total of 14,900 files from malicious programs targeting Android were detected. Apart from this, in the third quarter of the same year, [22] Kaspersky Lab products detected and neutralize 1,347,231,738 threats, 28% of all mobile devices attacked run Android OS version 2.3.6 which is released in September 2011, 56% of exploits blocked in third quarter were using Java vulnerabilities, and a total of 91.9 million URLs serving malicious code were detected, a 3% increase compared to second quarter of 2012.
The number of browser-based attacks in 2011 increased from 580,371,937 to 946,393,693, i.e.

the number of web-based attacks in 2011 is 1.63 times the total for 2010. [16]

Vulnerability Statistics for 2011, by SecurityLab.ru issued an annual report that provides statistics on vulnerabilities published in 2011[17]. The total number of vulnerabilities described in 2011 is 4733. By January 1 vendors were able to fix only 58% of vulnerabilities and publish workarounds for 7%. This means that more than a one third of the vulnerabilities remained exploitable for cyber criminals.

This report reveals that almost a quarter of vulnerabilities (24.2%) allowed hackers to compromise a system by executing arbitrary code on the victim`s computer, 21% led to CrossSite Scripting, about 15% could trigger denial of service. 13% of the detected flaws could be used for sensitive information disclosure. Finally, 12% allowed unauthorized data manipulation. 77% of all the vulnerabilities detected in 2011 could be exploited remotely, 15% - over the local network and 8% required local access. The report also includes Vulnerabilities sorted by the type of software's.

Website security is a moving target; new attacks techniques are frequently disclosed; new website launches are common; new Web technologies are made available every day. New application code is released constantly. Enterprises need timely information about how they can best defend their websites, gain visibility into their vulnerability lifecycle, measure the performance of their security programs, and determine how they compare to their industry peers.

Establishing these metrics is crucial towards improving enterprise security [12].

White Hat Security Web Site Statistics Report (summer 2012)[8], key findings in 2011: Vulnerability classes Cross-Site Scripting, Information Leakage, and Content Spoofing take the top three spots as they represent 50%, 14%, and 9% of the total population respectively. Also noticeable on the list are Cross-Site Request Forgery, Insufficient Authorization, and SQL Injection all at 4%.

Most Targeted Operating Systems in 2011; Microsoft operating systems are by far the most targeted, followed by Cisco IOS and Apple Mac OS X. Google Android made its entry in the top this year. [8] It will be interesting to observe its evolution in the next year as the number of Android smart phones and tablets increases at fast rate and it is expected to generate more and

more interest from security researchers and hackers. The same applies for Apple iOS, which already has a good number of vulnerabilities.

2.3. Vulnerability Testing Methodologies

A module-based approach such as the Open Source Security Testing Methodology Manual (OSSTMM) is advisable for grouping individual test steps since this allows the steps involved in a penetration test to be categorized thematically. [4] This gives the test a clear framework and also allows the tester to devise a suitable penetration test by selecting or excluding certain modules.

2.3.1. Open Source Security Testing Methodologies

There have been various open source methodologies introduced to address security assessment need using these assessment methodologies, one can easily pass the time-critical and challenging task of assessing the system security depending on its size and complexity. Some of these methodologies focus on the technical aspect of security testing, while others focus on managerial criteria, and very few address both sides. [19]

The most common and well-known open source security assessment methodologies to provide extended views of assessing the network and application security are: [18]

I. Open Source Security Testing Methodology Manual (**OSSTMM**)
II. Information Systems Security Assessment Framework (**ISSAF**)
III. Open Web Application Security Project (**OWASP**)
IV. United states National Institute of Standards and Technology(**NIST**) Special Publication 800-115: Technical Guide to Information Security Testing and Assessment
V. Back Track Testing Methodology(**BTTM**)

I. Key Features of Open Source Security testing Methodologies

The overall **OSSTMM** testing procedures focus on [18]:

- ✓ What has to be tested,
- ✓ How it should be tested,
- ✓ What tactics should be applied before, during and after the test, and

- ✓ how to interpret and correlate the final results;

II. **ISSAF methodology** is designed to evaluate the network, system and application controls, i.e. the layers of a penetration test can be applied to the following targets: Networks, Hosts, Applications, and Databases.

The approach comprises the following three phases:

- ✓ Planning and preparation
- ✓ Assessment
- ✓ Reporting, Clean-up and Destroy Artifacts

III. **OWASP methodology** focus is on Web Application Testing which includes the following: Gets quite deep into techniques and tools, Information gathering, Business logic testing, authentication testing, Session management testing, Data validation testing, Denial of service testing, Web service testing, and AJAX testing, [18]

According to OWASP, the top ten (10) attack vectors are:

- ✓ Cross site Scripting (XSS) and Cross Site Request Forgery(XSRF)
- ✓ Injection Flaws (including SQL injection)
- ✓ Malicious File Execution
- ✓ Insecure Direct object Reference
- ✓ Information Leakage and Improper Error Handling
- ✓ Broken Authentication and session Management
- ✓ Insecure Cryptographic Storage
- ✓ Insecure Communications
- ✓ Failure to Restrict URL Access

IV. **NIST** has released a document called ***"Technical Guide to information Security testing and assessment"*** that covers network penetration testing methodologies at a high level. It covers: Planning for tests, Conducting detail Analysis and dealing with validation of discovered issues.

V. **Back Track Testing Methodology** [14] is composed of a number of steps that should be followed in a process at the initial, medial, and final stages of testing in order to accomplish a successful assessment. These include: Target Scoping, Information Gathering, Target Discovery, Enumerating Target, Vulnerability Mapping, Social Engineering, Target

Exploitation, Privilege Escalation, Maintaining Access, and Documentation and Reporting. There are many security testing methodologies which claim to be perfect in finding all security issues, but choosing the best one still requires a careful selection process under which one can determine the accountability, cost, and effectiveness of the assessment at optimum level. Thus, determining the right assessment strategy depends on several factors, including the technical details provided about the target environment, resource availability, security tester knowledge, business objectives, and regulatory concerns[19].

The ISSAF Penetration testing methodology is designed to evaluate the network, system and application controls. [19] The approach includes following three phases: Planning and Preparation, Assessment, Reporting, Clean-up and Destroy Artifacts.

There are a number of other vulnerability "scoring" systems managed by both commercial and non-commercial organizations. They each have their merits, but they differ by what they measure. For example, CERT/CC produces a numeric score ranging from 0 to 180 but considers such factors as whether the Internet infrastructure is at risk and what sort of preconditions are required to exploit the vulnerability. [5]

The SANS vulnerability analysis scale considers whether the weakness is found in default configurations or client or server systems**.** Microsoft's proprietary scoring system tries to reflect the difficulty of exploitation and d the overall impact of the vulnerability**.** While useful, these scoring systems provide a one-size-fits-all approach by assuming that the impact for vulnerability is constant for every individual and organization.

Common Vulnerability Scoring System (**CVSS**) which was designed to provide the end user with an overall composite score representing the severity and risk of a vulnerability. The score is derived from metrics and formulas. [21]

When the **base metrics** are assigned values, the base equation calculates a score ranging from 0 to 10, and creates a vector. The vector facilitates the "open" nature of the framework. The base and **temporal metrics** are specified by vulnerability bulletin analysts, security product vendors, or application vendors because they typically have better information about the characteristics of vulnerability than do users. [5]

The **environmental metrics**, however, are specified by users because they are best able to assess the potential impact of vulnerability within their own environments.
Many organizations are using CVSS, and each are finding value in different ways: Vulnerability Bulletin Providers, Software Application Vendors, User Organizations and Vulnerability Scanning and Management, Security (Risk) Management, Researchers. [5]

There are several ways of manipulating or damaging IT systems and of preparing an attack on IT systems, such as Network-based attacks, social engineering, Circumvention of physical security measures.

2.4. Reconnaissance

After the test has been thoroughly scoped and any required planning is finished, the test begins with the reconnaissance phase (information gathering). [2] By using different tools and techniques (such as non-technical (documentation) and technical like *nslookup, whois, maltego, etc.)*
According to German Federal Office for Information Security**,** Modules for the penetration test procedures have been divided in to two classes accordingly, **I modules** for reconnaissance and **E modules** for penetration attempts.
In Reconnaissance phase (module I) the following tasks will be executed: Analysis of Published Data, Basic Network Information, Stealthy Port Scans, Noisy Port Scans, Application Identification, System Identification, Router Identification, Firewall Identification, Vulnerability Research, and Application Interface Identification

In module II Active Intrusion Attempts (E modules) the following tasks will be executed: Verification of Actual Vulnerabilities, Router vulnerability Testing, Test of Trust Relationships Between Systems, Testing the Firewall From Both Sides, Intercepting Passwords, Password Cracking, Test of Susceptibility to Denial of Service Attacks. [2] Each module includes a brief description, the expected results, the requirements, the testing steps to be performed, and the associated risks.

The ***DNSstuff*** Toolbox tools and other information gathering tools (Nslookup, dig) can help to gather information names and IP address of the hosts on the LAN. [35]

Maltego is an open source intelligence and forensics application, Over 50 different kinds of transforms, such as: DNS, IP address to org name(netblock),Org name to person's name(whois), Person's name to PGP key (public key servers), PGP key to person's name (who signed the key?), Person's name to phone numbers (phone lookup) and others can be performed. *[36]*

2.5. Vulnerability Scanning

The overarching goal of the scanning phase is to learn more about the target environment and find openings by directly interacting with the target systems˙ According to studies scan types such as Network sweeping, Network tracing, port scanning, OS fingerprinting, version scanning and vulnerability scanning performed on this phase of penetration testing.

TCPdump is a free open source sniffer that is quite flexible and fast. It supports variety of filters, with a powerful language for specifying individual filter types. *[38]*

Scapy is a fantastic and flexible environment for creating and interacting with packets. It's incredibly full featured, allowing users to forge packets, sniff them, and read them from a pcap-style packet capture file, edit packets, and interact with networked targets in real-time or via scripts.

Nmap is primarily a port scanner, showing which TCP and UDP ports are open on a target system. It also provides numerous other features, including ping sweeps, operating system fingerprinting, trace routing and much more. *[39]*

Nessus is Comprehensive Security and Compliance Auditing with Automatic Monitoring. *[40]*

- ✓ Agent less auditing of configurations, patches, and web applications
- ✓ 55,000+ vulnerability and configuration checks (plugins) – new plugins updated daily
- ✓ Scans networks, systems, data, and applications
- ✓ Post-scan analysis and monitoring tools

The **Samurai Web Testing Framework (SamuraiWTF**) is a live Linux environment that has been pre-configured to function as a web pen-testing environment. The CD contains the best of the open source and free tools that focus on testing and attacking websites. *[41]*

SamuraiWTF has Over 100 tools, extensions, and scripts, included: w3af, BeEF, Burp Suite, Grendel-Scan, DirBuster, Maltego CE, Nikto, WebScarab, Rat Proxy, nmap. [42]

Joomscan - OWASP Joomla Security Scanner detects file inclusion, sql injection, and command execution vulnerabilities of a target Joomla Web site. [43]

Nikto is an Open Source web server scanner which performs comprehensive tests against web servers for multiple items, including over 6500 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. [44]

2.6. Vulnerability Exploitation

OSI was built to allow different Layers to work without the knowledge of each other. Lower Levels affect higher Levels. I.e. if one layer at lower layer is attacked, the whole communications are compromised without the other layers being aware of the problem. When it comes to networking, layer 2 can be a very weak link; if one of protocols working at Layer 2 (like, DHCP, CDP, VTP, STP, ARP etc.) is attacked the availability of the whole LAN might be completely compromised.

Ettercap is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis. [45]

Wireshark is a free and open-sourcepacket analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. [46]

W3af(**W**eb **A**pplication **A**ttack and **A**udit **F**ramework)is an open-source web application security scanner. The project provides a vulnerability scanner and exploitation tool for Web applications. It provides information about security vulnerabilities and aids in penetration

testing efforts. [47]

Metasploit World's most used penetration testing software. The Metasploit Project is a computer security project which provides information about security vulnerabilities and aids in penetration testing and IDS signature development. [48]

SQLmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections. [49]

2.7. Computer Network Security Assessment and Related works in Ethiopia

In recent years as money governmental and private organizations especially educational institutes investing and building ICT infrastructure to assist business process and benefit from the unlimited resources from Internet.[11]

Banking systems, Educational Initiations, and other private and governmental organizations in Ethiopia are employing ICT development programs and focuses on deploying network-based services to meet the current international standard.[27]

The public sector and the education sector have begun to benefit from WoredaNet and the ICT strategy though the accomplishment is not to the perceived standard. The national e-education initiative with implementation strategy of ICT use in education and the subsequent action plans, for example, has come up because of the WoredaNet program." The use of Computer and internet in Ethiopia is very much limited though there is a clear policy direction from the government and policy makers. [29] Awareness creation and preparation to use computer and the internet for learning and other business seems promising. The promise founded itself on the launching of WoredaNet, an e-government communication and the ICT strategy, which are the major enablers for the fast development of ICT use in the country today. [29]

But how far the government and organizations in Ethiopia strive to incorporate ICT (Computer and Internet) infrastructure to their system, the issue of the information security and its related systems (network devices, servers and likes) overlooked. [6] In Ethiopia, currently cyber security policy and standards are inexistent. Information security law, ethics and relevant legislation and regulation concerning the management of information in an organization is not yet developed. [33] And additionally there is no established information security policy and a management body responsible for ensuring information security in the healthcare system implemented in the hospitals. [33] The result also shows that from the asked vulnerabilities, staffs‟ training awareness and education was the top ranked issue, malicious software's taking the least." Furthermore, The security culture posture and practice of information security and its tools in Banking system in Ethiopia, and they discovered that the practice of managing information security and culture of network security assessment in enterprise LAN hosting organizations, the likes of Banking system and even ISP's is insufficient. [30]

As it is mentioned in background of the study. Hawassa University is also hosting a large LAN infrastructure which has a significant number of users and it deployed a number of sensitive services accessed from in and out of the university LAN.
To protect information and its related systems, tools such as well organized network security assessment, policy, awareness, training and education, and technologies are of vital importance.[6]

Therefore, after thorough analysis of literatures in culture and practice of network security assessment and information security in Ethiopia, there is strong conviction in a research based approach to address network and information security challenges. Moreover we are aspired to find out what are the culture and practices in network security and the threats it poses to information and network services in HU at large.

3. CHAPTER THREE

3.1. Research Methodology: Security Testing Types

To evaluate the security controls by identifying the threats that pose serious exposure to the organizations assets, the two most general approaches that are widely accepted by the industry are **Black-Box** and **White–Box testing**. Black box testing is generally used when the tester has limited knowledge of the system under test or when access to source code is not available [4]; I.e. security assessment could be performed over the network and will not be aware of any internal technologies deployed by the concerning organization and also it would spend extra time on Recon and Mapping.

The white-box approach is also referred to as crystal box testing, in which the tester should be aware of all the internal and underlying technologies used by the target environment; i.e. virtually all access to the host server provided and often includes source code and configuration files review. The time and cost required to find and resolve the security vulnerabilities is comparably less than the black-box approach. [12]

However, threats in real world could be from Black hat or White hat hackers on the corporate network infrastructure, and hence the combination of both types of penetration testing types provides a powerful insight for security assessment viewpoints. Because of the feature it comprises it's referred to as **Grey-Box testing**, i.e. It lies between black box and white box testing, a set of advantages posed by both approaches are the key benefit in devising and practicing a gray-box approach. Therefore, this research is carried out with grey-box testing.

3.2. Research Method

A Quantitative or Qualitative (or both as required) approach is taken in this research by starting with a review of existing information security and information security assessment theory and practice. Each of the open source security testing methodologies has good features and limitations; hence, adapting any single methodology does not necessarily provide a complete picture of the risk assessment process.

In this research the method used is to perform security assessment after reviewing each of the

open source testing methodologies and accepted standards for information security as they provide useful insights in to testing from various different perspectives, we developed our own customized testing methodology to conduct security assessment on services and applications and provide a complete picture of risk assessment process.

The research approach first identified the questions that need to be answered; hence, various procedures and a set of execution steps had been carried out by giving answer for the following questions:

- ✓ Which Data Center Active devices, Services and Application have to be tested? (i.e. Security assessment type)
- ✓ What kind of sampling techniques ought to be used for the test?
- ✓ What kinds of attack techniques should be tested?(Assessment techniques)
- ✓ Which tools should be used for the test?
- ✓ How it should be tested? And what tactics /procedures/ should be applied before, during and after the test?
- ✓ What security metrics can be used to evaluate the security vulnerability?
- ✓ How Risk analysis can be performed?
- ✓ How to interpret and correlate the final results?

The following section of the approach will answer each of the aforementioned lists of questions respectively:

3.2.1. Security Assessment type

- ✓ **Network Security**: puts its main focuses on intermediate network access devices. It assesses device model and OS, configuration details, ports, and protocols allowed on the designated ports. Access Switch Security Assessment, Router Security Assessment and Firewall security Assessment are the main types of assessment conducted in this study.
- ✓ **Host Security**: Hosts are any devices such as Server machines and Workstation computers involved in the LAN, which are basically hosts services accessed through the network. In this study we will focus on HU Web server Security Assessment, HU Mail Server security Assessment, DNS Server security Assessment and DHCP server security Assessment.

- ✓ **Application and Data base security**: It focuses on application vulnerability which resides in the selected LAN. Web Applications running on HU LAN and their respective Database Security Assessment are the main target on this point.

3.2.2. Sampling Techniques Used

HU LAN infrastructure is powered on by few vendor equipments at each layer and also different platforms (Windows, Linux/Unix, Networking device's IOSs) are installed on the systems.

Active intermediate network devices and applications which are part of this research, deployed on the production network are:

- ✓ Layer 2 Switches (Cisco2960 and Cisco3560)
- ✓ Layer 3/Multilayer Layer switches (Two Cisco6509, Three Cisco6513)
- ✓ Firewall (Two Cisco ASA 5510)
- ✓ More than five servers for different services and business process applications
- ✓ Others

Among the available sampling techniques, this research followed stratified Sampling which is a variant on simple random and systematic methods and is used when there are a number of distinct subgroups, within each of which it is required that there is full representation. A stratified sample is constructed by classifying LAN equipments based on the characteristics they have, i.e. Classification of Network equipments had been taken based on the OSI layer they are working (Layer 2, 3, 4 and 7 equipments). The selection of elements is then made separately from within each stratum;

For layer two switches, since their configuration is almost identical (i.e. only location and management IP is different), hence only three switches (one from each model) are selected for the test. But in the case of layer three Switches (Routers), one from Cisco 6506 and from Cisco 6509 model had been tested and Both existing Firewalls installed in HU LAN have the same configuration (only their IP address is different) one of these had been taken for the assessment. Finally, as it is clearly indicated on the scope of this research, among the available services and applications over the LAN, for those which are given high priority by considering the high impact of the vulnerability if an attacker is able to compromise. Therefore, services and applications like: DNS and Proxy servers, Web Server, Mail server, DHCP server, SMIS are included in the test.

3.2.3. Assessment Techniques

In this section we defined the attacks used for the corresponding devices and services in the network. This selected attacks in the respecting areas critically defines the security posture of the network devices and services because if this attacks were exploited by an attacker, it will have great impact on the confidentiality, integrity and availability of information and reputation of the organization.

We planned to assess the network security weakness in Access Switched to collect possible information by using techniques like MAC Attacks, ARP Spoofing/ARP poisoning and Remote login protocols to identify security loop holes in access switched like CAM table overflow and MAC address spoofing and protocol malfunctioning. When we came to router and firewall network devices assessment technique is performed to find out there is mis-configuration of devices and Remote login protocol issues. Meanwhile, the host security posture of HU services and application which are running in the LAN like DHCP, DNS and other Web Servers are assessed using Rouge DHCP Server attack, DHCP starvation, DoS overflow and DNS cache poisoning attack techniques to indentify vulnerabilities in the host systems.

Its common in security assessment to look in to Mail server security posture and it is important to analyze the applications running on the LAN and the Database type and structure used for the respective services to scrutinize the security posture of the services. When assessing the applications and Database of services we managed to identify the vulnerabilities by the likes of Cross Site Scripting (XXS), Injection Flaws (SQL injections) and Cross Site Request forgery (CSRF)(an attack targets a victims browser).

Thus the above mentioned types of threats and the required responses to those threats, and the assessment method helps to prevent the attacks and closes the gaps for hackers to access the network.

3.2.4. Tools Used for the Assessment

The following tools were used to assess the network devices and services based on the behavior the tools have and the areas they are needed. There are different types of scanners each with different goals [32]. A port scanner is scanning the ports of the network and tries to find out what ports, services and operating system the target are running. Application scanners assess a specific application running on the network. Vulnerability scanners contain all the functionality of the above described scanners and try to give a complete picture of the vulnerabilities in the network.

- Fping
- Hping
- Nslookup
- Whois
- Maltego
- WireShark
- dsniff
- Netcat
- Nmap or Vega
- TCP Dump
- Nessus
- w3af
- Metasploit
- SQLmap
- Linux/Kali Linux
- Linux/Ubuntu
- Google-FU
- Windows

For this research the scanners were chosen on the basis that they should be able to scan different platforms and applications common in computer networks. The scanners should also be either world leading in number of users, award winning or developed by a world leading company. Then, we have discovered that there are other scanners on the market that are probably just as good as the ones chosen but the lack of time restricted the number of scanners were selected.

3.2.5. Security Testing Procedures

Using various kinds of tools and techniques a set of execution steps will be carried out. This stage of the methodology answers the question, how it should be tested and what are the procedures to be followed. The approach includes the following four phases:

1. Phases -I: Planning and Determine Scope
2. Phase -II: Vulnerability Assessment and Identification
3. Phase -III: Security Risk Analysis and Countermeasures
4. Phase –IV: Reporting, Clean-up and Destroy Artifacts

3.3. Planning and Determining Scope

This phase comprises the steps to exchange initial information, plan and prepare for the test. It will provide basis for this research. The activities like Identification of contact individuals, Agree to specific test cases and escalation, Opening meeting to confirm the scope, approach and methodology paths had been accomplished during this phase.

3.4. Vulnerability Assessment and Identification

In this phase a layered approach shall be followed. The following layers are envisaged:

3.4.1. Reconnaissance

Information Gathering**:** find all the information about the target (devices, application and services) using both technical (like DNS/WHOIS) and non-technical (search engines, news groups, mailing lists, observations, documentations etc.) methods.

3.4.2. Network Mapping

When all possible information about the target has been acquired, a more technical approach is taken to 'footprint' the network and resources. A set of tools and applications can be used in this stage to aid the discovery of technical information about the hosts and networks involved in the test.

- Find live hosts
- Port and service scanning
- Perimeter network mapping (router, firewalls)
- Identifying critical services/Service fingerprinting
- Operating System fingerprinting

3.4.3. Vulnerability Identification

- Exploitable weak points will be detected; several activities will be carried out.
- Perform vulnerability scan to search for known vulnerabilities. Information regarding known vulnerabilities can be obtained from the vendors' security announcements, or from public databases such as Security Focus, CVE or CERT advisories.
- Identify vulnerable services and applications
- Perform false positive and false negative verification (e.g. by correlating vulnerabilities with each other and with previously acquired information)

3.4.4. Enumerating Discovered Vulnerabilities

- ↗ Obtain password (plaintext or encrypted) by using sniffing or other techniques
- ↗ Sniff management or user traffic and analyze it

3.5. Security Risk Analysis and Countermeasures

3.5.1. Security Metrics

To manage security issues, the risk and impacts must be measured and should be analyzed. The need for metrics is important for assessing the current security status, to develop operational best practices and also for guiding future security research. Apart from this, Metrics gives a way to prioritize threats and vulnerabilities and the risks they pose to enterprise information assets based on a quantitative or qualitative measures. In this research as vulnerability test metrics used three ways to evaluate risks, i.e. quantitatively, qualitatively or combining the two methods.

The following Questions need to be answered to facilitate decision making on the metrics to be used in this research.

- ✓ Which model is used to determine the urgency and priority of response to vulnerabilities that would convey vulnerability severity in HU LAN systems?
- ✓ Why this model is selected?
- ✓ How does this model work?
- ✓ What security metrics can be used to evaluate the security vulnerabilities?

To determine the urgency and priority of response to vulnerabilities, this research uses the **Common Vulnerability Scoring System (CVSS) model** which is an open framework that addresses this issue. *[14]*

The reasons why this CVSS model is selected are, it is an open framework and it was designed to provide the end user with an overall composite score representing the severity and risk of a vulnerability.

Common Vulnerability Scoring System (CVSS) offers the following benefits:

- ❖ Standardized Vulnerability Scores
- ❖ Open Framework
- ❖ Prioritized Risk

The score is derived from metrics and formulas. When the base metrics are assigned values, the base equation calculates a score ranging from 0 to 10, and creates a vector. The

metrics are in three distinct categories that can be quantitatively or qualitatively measured.

- **Base metrics:** contain qualities that are intrinsic to any given vulnerability that do not change over time or in different environments. [14]
- **Temporal metrics:** contain vulnerability characteristics which evolve over the lifetime of vulnerability [14]
- **Environmental metrics:** contain those vulnerability characteristics which are tied to an implementation in a specific user's environment. [14]

3.6. Metrics Parameters

3.6.1. Base Metrics

According to CVSS there are about seven base metrics which represent the most fundamental features of vulnerability ***[14]***

1. **Access Vector (AV)-** measures whether the vulnerability is exploitable **locally** or **remotely**
2. **Access Complexity(AC)-** measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system(**high or low**)
3. **Authentication(A)-** measures whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability **(required or not required)**
4. **Confidentiality Impact(CI)-** measures the impact on confidentiality of a successful exploit of the vulnerability on the target system**(none, partial, or complete)**
5. **Availability Impact(AI)-** measures the impact on availability of a successful exploit of the vulnerability on the target system**(none, partial or complete)**
6. **Integrity Impact(II)-** measures the impact on integrity of a successful exploit of the vulnerability on the target system**(none, partial or complete)**
7. **Impact Bias(IB)-** allows a score to convey greater weighting to one of three impact metrics over the other two

3.6.2. The Temporal Metrics: which represent the time dependent features of the vulnerability are:

1. **Exploitability (E)** measures how complex the process is to exploit the vulnerability in the target system. The possible values are: **unproven**, **proof of concept**, **functional**, or **high**.
2. **Remediation level (RL)** measures the level of an available solution. (**Official fix**, **temporary fix**, **workaround**, or **unavailable**)
3. **Report confidence (RC)** measures the degree of confidence in the existence of the vulnerability and the credibility of its report. (**unconfirmed, uncorroborated, or confirmed)**

3.6.3. The Environmental Metrics: represent the implementation and environment specific features of the vulnerability.

1. **Collateral damage potential (CDP)** measures the potential for a loss of physical equipment, property damage or loss of life or limb. (**none, low, medium, or high**)
2. **Target distribution (TD)** measures the relative size of the field of target systems susceptible to the vulnerability. (**none, low, medium, or high**)

3.7. Metrics Scoring Equations

Scoring equations and algorithms for the base, temporal and environmental metric groups are described below. Equations for evaluating the Base, Temporal, and Environmental metric groups to calculate a score between **0 and 10** for each of the metric groups to measure risk level.

3.7.1. Base Equation

The base equation is the foundation of CVSS scoring. It is:

BaseScore= round_to_1_decimal((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))

Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))

Exploitability= 20* AccessVector*AccessComplexity*Authentication

f(impact)= 0 if Impact=0, 1.176 otherwise

AccessVector = case AccessVector of requires

local access: 0.395

adjacent network accessible: 0.646

network accessible: 1.0

AccessComplexity = case AccessComplexity of

high: 0.35

medium: 0.61

low: 0.71

Authentication = case Authentication of

requires multiple instancesof authentication: 0.45

requires single instance ofauthentication: 0.56

requires no authentication: 0.704

ConfImpact = case ConfidentialityImpact of

none: 0.0

partial: 0.275

complete: 0.660

IntegImpact = case IntegrityImpact of

none: 0.0

partial: 0.275

complete: 0.660

AvailImpact = case AvailabilityImpact of

none: 0.0

partial: 0.275

complete: 0.660

Table3.1: Base Equation "adapted or taken from [14]"

3.7.2. Temporal Equation

It will combine the temporal metrics with the base score to produce a temporal score ranging from 0 to 10. Further, the temporal score will produce a temporal score no higher than the base score, and no less than 33% lower than the base score. The temporal equation is:

TemporalScore= round_to_1_decimal(BaseScore*Exploitability
*RemediationLevel*ReportConfidence)

Exploitability = case Exploitability of

unproven: 0.85

proof-of-concept: 0.9

functional: 0.95

high: 1.00

not defined: 1.00

RemediationLevel = case RemediationLevel of

official-fix: 0.87

temporary-fix: 0.90

workaround: 0.95

unavailable: 1.00

not defined: 1.00

ReportConfidence= case ReportConfidence of

unconfirmed: 0.90

	uncorroborated:	0.95			
	confirmed:	1.00	and	not defined:	1.00

Table3.2: "adapted or taken from [14]".

3.7.3. Environmental Equation

It will combine the environmental metrics with the temporal score to produce an environmental score ranging from 0 to 10. Further, this equation will produce a score no higher than the temporal score. The environmental equation is:

EnvironmentalScore = round_to_1_decimal((AdjustedTemporal)+
(10-AdjustedTemporal)*CollateralDamagePotential)*
TargetDistribution)

AdjustedTemporal = TemporalScore recomputed with the BaseScore's Impact sub-equation replaced with the AdjustedImpact equation

AdjustedImpact= min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq) *(1-AvailImpact*AvailReq)))

CollateralDamagePotential = case CollateralDamagePotential of

none:	0
low:	0.1
low-medium:	0.3
medium-high:	0.4
high:	0.5
not defined:	0

TargetDistribution =case TargetDistributionof

none:	0
low:	0.25

	medium:	0.75
	high:	1.00
	not defined:	1.00
ConfReq = case ConfReq of		
	low:	0.5
	medium:	1.0
	high:	1.51
	not defined:	1.0
IntegReq = case IntegReq of		
	low:	0.5
	medium:	1.0
	high:	1.51
	not defined:	1.0
AvailReq = case AvailReq of		
	low:	0.5
	medium:	1.0
	high:	1.51 and not defined: 1.0

Table3.3: "adapted or taken from [14]".

3.8. Qualitative and Quantitative Risk Analysis

Quantitative or qualitative (or both) risk Analysis is conducted based on the security risk decision variables which include the following aspects:

- ⇨ Severity of the impact Value of the asset
- ⇨ Likelihood that a vulnerability will be exploited
- ⇨ Severity of the impact

Each of the security risk decision variables (e.g., threat frequency, vulnerability impact, and safeguard effectiveness) may be determined through a complex computation

(quantitative analysis) or through subjective judgment (qualitative analysis).

The impact which describes how HU community would be affected based on the threat outcomes like:

- ✓ Disclosure of a critical asset
- ✓ Modification of a critical asset
- ✓ Loss/ destruction of a critical asset
- ✓ Interruption of a critical asset

3.9. Vulnerability Impact and Assessing Damage Metrics

The impact vectors in the Base group indicate the damage of the risk. These impact vectors are limited to immediate consequences of exploitations on *confidentiality, integrity, and availability* (CIA metrics) of data and services.

The higher the Environmental metrics and exploitation impacts on goals are, the higher the damage is. If even one aspect of the damage is High, the risk ultimately is high impact, and thus, we take the worst case scenario (pessimistic) as such:

Let *d1, d2, ….,dn* be the values of damage metrics

Damage = Max (d1, d2,…,dn)

3.9.1. Qualitative Analysis

Qualitative security risk equation variables are not expressed in terms of monetary values, but as an ordered category of monetary loss such as “Critical,” “High,” “Medium,” and “Low. Qualitative assignments can be used to represent quantitative measure of security properties.

- ⇨ Low means no vulnerabilities found;
- ⇨ Medium, b/n one and five found; and
- ⇨ High, more than five found (completely compromise availability, Confidentiality or Integrity)

3.9.2. Quantitative Analysis

It is an approach that relies on specific formulas and calculations to determine the value of the security risk decision variables.

There are two classic quantitative security risk analysis formulas:

- ⇨ Annual loss expectancy
- ⇨ Single loss expectancy

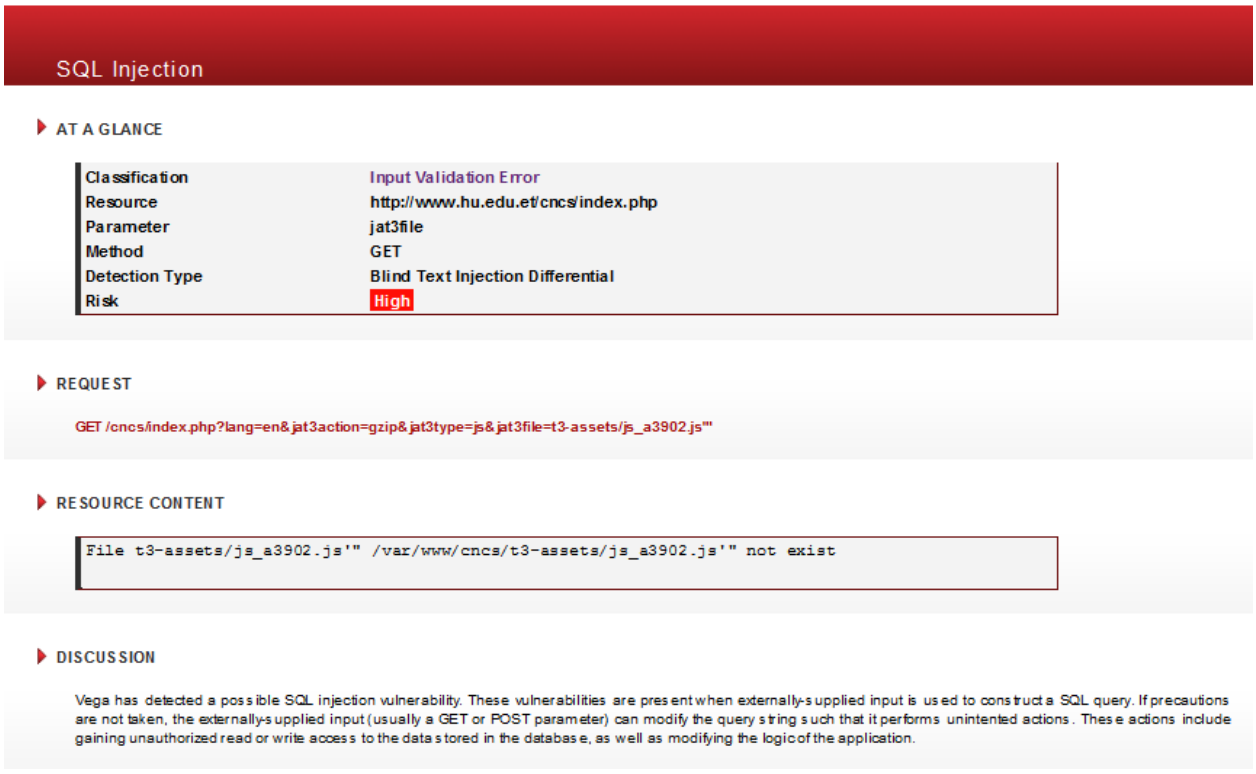
*Annual loss Expectancy (ALE) = Single loss Expectancy * Annual Rate of Occurrence*

*Single loss Expectancy = Asset Value * Exposure Factor*

From the above formulas in table 3.1, 3.2, and 3.3 quantifying the risk in terms of money is performed.

3.10. Counter Measures

The mitigation model has been designed to tackle threats and security holes found by the study. All possible Counter measures are proposed alongside the proposed model to safe guard the University LAN from attackers for each of the discovered vulnerabilities and possibly exploit it. For example the HU web server has scanned by Vega scanner and we have found SQL Injection vulnerability with high risk of exploited by an attacker and Vega have given us the possible discussion, the impact it will cause to harm the service and the counter measure with the remediation to mitigate it.



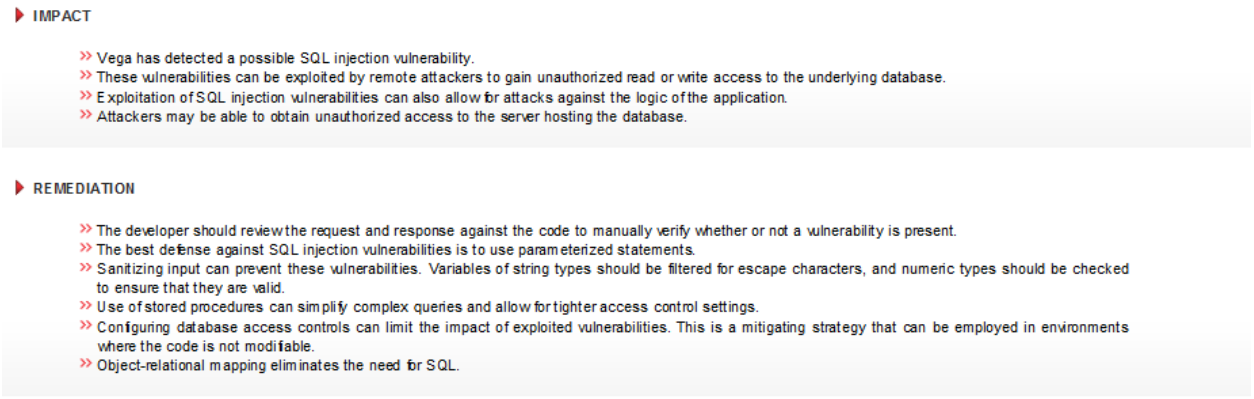


Figure 3.1 Vega scan result of HU web server with URL www.hu.edu.et

3.11. Reporting, Clean-up and Destroy Artifacts

I. Verbal Reporting

During the course of this research work when a critical issue was identified, it was supposed to be reported immediately to ensure that the University network and system administrators are aware of it. At this point criticality of issue has been discussed and countermeasure to safeguard against this issue has been provided.

II. Final Reporting

After the completion of all test cases defined in scope of this research work, a written report describing the detailed results of the tests and reviews has been prepared with recommendations for improvement.

III. Clean-up and Destroy Artifacts

All information that is created and/or stored on the tested systems has been removed from these systems. If this is for some reason not possible from a remote system, all these files (with their location) should be mentioned in the technical report so that HU technical staff will be able to remove these after the report has been received.

4. Chapter Four

4.1.Vulnerability Assessment Detection and Findings

4.1.1. Overview

Principally, the core objectives of this study and the security assessment and identifying vulnerabilities are to ensure the integrity, confidentiality and availability of data/information for the intended users using the LAN. Several controls actions, countermeasures are implemented to mitigate the flaws and to achieve the projected objectives of the assessment. There are common ways to measure and monitor the design and effectiveness of controls and countermeasures is through an information security assessment.

In the previous section a simplified view was given on methods how the research had been executed and procedures are clearly listed. It could be seen that some of these procedures have overlap; from this overlap the general vulnerability detection methods that will be discussed in this section were formulated. This section might not show all the possible detection methods and collected data. The methods that are shown in this section might also not be directly applicable and are left as future work. Therefore, based on the aforementioned methods, in this section of the research, data collection and analysis phase is explained.

After completing the steps to exchange initial information, planning and preparing for the test, defining the scope and limitations, preparing the necessary tools, defining rules of engagement and other groundwork had been executed.

4.2. Reconnaissance

Reconnaissance is defined as Information Gathering: all the information about the targets (devices, application and services) using both technical (like DNS/WHOIS) and non-technical (observations and documentations) methods carried out. *[14]* The following table summarizes both technical and non-technical methods:

From the Analysis of network documentation, observation the LAN infrastructure and basic network information, the information about HU LAN systems which includes the technology used is obtained:

Requirements:	IP address/IP range or domain/server names
Test Steps:	1st - Referring LAN documentation and observation 2nd - Query public databases (whois, Ripe, Arin) 3rd - Query domain and name of the University using Maltego 4th - Query name servers, with a zone transfer attempt (dig) 5th - Ping scan of the IP range, neighboring IP addresses and common host names
Tools used:	Whois, Maltego, DNS lookup, Ping, dig and Fping
Expected Result:	Domain names of HU: dnssrv.hu.edu.et, n1.hu.edu.et and n2.hu.edu.et IP address ranges ... 10.0.0.0/13 and 172.22.1.0-172.22.190.0/24 Host names found on the LAN : `websnssrv.hu.edu.et on 172.22.18.57 and websrv.hu.edu.et on 172.21.4.52` Description of server functions: see the output Figure 4.1 below ISP information: HU's registered Public IP from EthTelecom of 197.154.209.0/30

Table 4.1: Reconnaissance Procedure, Tools used and Results found on HU LAN

Using the above tools we perform reconnaissance to get HU's network information. It helps us to find out the likes of Domain name, IP ranges and host names as listed on the above table, which helped us to determine our attack scope and plan to next tasks to the assessment. Based on the recon process carried out on the HU LAN we obtained the detailed information about hosts and their corresponding description and IP address to go to the next level on our study.

```
adminsrv.hu.edu.et.     10800 IN    A       172.22.18.56
App.hu.edu.et.          10800 IN    A       172.22.130.44
avsrv.hu.edu.et.  10800 IN    A       172.22.18.73
bsc.hu.edu.et.          10800 IN    CNAME avsrv.hu.edu.et.
cs.hu.edu.et.           10800 IN    A       172.22.18.46
dlib.hu.edu.et.         10800 IN    A       172.22.18.78
dnssrv.hu.edu.et.10800 IN    A       172.22.18.54
egranary.hu.edu.et.     10800 IN    CNAME egranarysrv.hu.edu.et
elemail.hu.edu.et.      10800 IN    A       172.22.18.31
filesrv.hu.edu.et.      10800 IN    A       172.22.18.25
GSSO.hu.edu.et.         10800 IN    CNAME App.hu.edu.et.
lis.hu.edu.et.          10800 IN    A       172.22.18.49
localhost.hu.edu.et.    10800 IN    A       127.0.0.1
mail.hu.edu.et.         10800 IN    CNAME mailsrv.hu.edu.et.
mailrelay.hu.edu.et.    10800 IN    A       172.21.4.50
mailsrv.hu.edu.et.      10800 IN    A       172.22.2.254
```

Figure 4.1: dig sample output on recon process

4.3. Network Mapping

After reconnaissance process successfully done, we needed to map the network structure of HU and it is key for us to find and investigate on live hosts, services running on the hosts and open and closed port numbers.

The mapping process will be carried out using the following check lists and all possible information about the target has been acquired:

1. Find live hosts
2. Port and service scanning
3. Perimeter network mapping (router, firewalls)
4. Identifying critical services/Service fingerprinting
5. Operating System fingerprinting

4.3.1. Find Live hosts

Purpose: Live hosts in the HU's target LAN had been acquired
Requirements: IP address/IP range or domain/server names
Test Steps: Ping scan of the IP range, neighboring IP addresses and common host names
Tools used: Nmap, Dig, Ping and Fping
Result: Using t **'Ping scan of IP range'** tool we discovered all live host at the time and their matching services. As the result all live hosts are identified.

Table 4.2: Live scan Procedure, Tools used and Results

4.3.2. Port and service scanning:

Port scan ran on all identified devices in order to identify which services each device offers, and with which operating system

Requirements:	Knowledge of basic network information
Test Steps:	Perform a basic port scan procedures using the selected tools.
Tools used:	Nmap, Dig and Tcpdump
Sample result found from Nmap tool scan on HU mail server	Information on the services offered by the devices with respect to the operating system running and the ports on the services associated with protocols. Sample output of the port and service scanning test on HU mail server **# nmap -oNNmapMail -O -sV -n _sT 172.22.2.254**

	# Nmap 6.01 scan initiated Sun June 21 12:52:12 2014 as: nmap -oNNmapMail -O -sV -n –sT 192.168.5.20 Nmap scan report for 172.22.2.254 Host is up (0.00026s latency). Not shown: 986 closed ports **PORT STATE SERVICE VERSION** 22/tcpopen sshOpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0) 25/tcp open smtpPostfix smtpd 53/tcp open domain ISC BIND 9.7.0-P1 80/tcpopen http Zimbra http config 110/tcpopen pop3 ZimbraCollabration Suite pop3d 143/tcpopen imap-proxy nginximap proxy 465/tcpopen ssl/smtpPostfix smtpd 587/tcpopen smtpPostfix smtpd 993/tcpopen ssl/imap-proxy nginximap proxy 995/tcpopen ssl/pop3 ZimbraCollabration Suite pop3d 5222/tcpopen jabber Zimbra 6 jabberd 5269/tcpopen jabber Zimbra 6 jabberd 7025/tcpopen lmtpZimbralmtpd 7777/tcpopen socks5 (No authentication; connection failed) **Device type: general purpose** Running: Linux 2.6.X OS CPE: cpe:/o:linux:kernel:2.6 OS details: Linux 2.6.19 - 2.6.35 Network Distance: 2 hops **Service Info**: Hosts: mail.hu.edu.et, mail.hu.edu.et; OS: Linux; CPE: cpe:/o:linux:kernel OS and Service detection performed. # Nmap done at Sun June 21 12:52:54 2014 -- 1 IP address (1 host up) scanned in 43.09 seconds

Table 4.3: Ports and service scan Procedure, Tools used and Results

4.3.3. Perimeter Network Mapping (Router)

To identify the posture of Routers and Firewalls used by HU, their functionality within the network as well as the IOS used, the manufacturer & the router model, it is important to make stealthy or covert queries.

Requirements:	• Knowledge of basic network information and most importantly results from port scans and system identification are required.
Test Steps:	• Trace routes using a "traceroute" command using command prompt on windows or Fping on Linux system and analyze the routed IP packets from the scan result.
Tools used:	Nmap, traceroute and Fping
Expected Result:	• On the regard of Routers: - The IP address and function of the routers in the network, IOS, manufacturers and router model • Identify the Firewall's: - Type/form (packet filter, dual or single-homed, application gateway etc.) - Model (manufacturer, version, configuration access etc.) - Configuration (Open ports, open protocols, etc.)

Table 4.4: Perimeter network mapping scan Procedure, Tools used and Results

4.3.4. Perimeter Network Mapping (Firewall)

Requirements:	Knowledge of basic network information and Results from port scans
Test Steps:	Banner lookup of the Firewall components Direct port scan of the Firewalls Trace routes using a "traceroute" command
Tools used:	Nmap traceroute and Fping
Result:	IP address and\or DNS names of the HU's Firewall components (firewall hosts, application gateway, etc.) Firewall IOS and IP address of other components of the Firewall configuration (internal and external routers) Model and patch level of the Firewall software

Table 4.5: Perimeter network mapping scan Procedure (FW)

4.3.5. Identifying Critical Services

On this assessment the services hosed at HU network that can be accessed over the internet identified.

Requirements:	Results from port scans and system identification
Test Steps:	Evaluate the result of a port scan Identify publicly available internet application/services such as SIS, HU official website, HU-Mail service
` Tools used:	´ Nmap and Vega/Nessus
Result:	Identification of server services offered on mail and web server of HU are HTTP, SMTP, POP, IMAP and etc. Identification of applications offered found according to the scan is SMIS

Table 4.6: Critical Services scan Procedure

4.3.6. Operating System Fingerprinting

Information about the Operating system, the patch level status and the system's hardware are obtained.

Requirements:	Knowledge of basic network information
Test Steps:	Perform a port with system detection\IP packet analysis Analyze banner information of the target device
Tools used:	Nmap and Vega/Nessus
Result:	Information about the Operating system Information about the patch level status Information about the Hardware

Table 4.7: OS Fingerprinting scan Procedure

The following table summarizes the result of network mapping, such as target's IP address, name, Operating system type, how it is discovered and listening ports etc. are included. The following table briefly depicts the detailed results found on the above steps to map the HU LAN structure. For the purpose of the HU's LAN information security target system the actual IP addresses are altered and instead we prefer to use the class IP address 192.168.x.x format.

Target IP Address	Target Name	Target OS	How Discovered	Listening Ports	Remarks
192.168.1.0 /24	**L2 Switch**	**Cisco 3560/296 0/2950 12.1(22)**	Non-technical (Documentation) Ping Fping Nmap Maltego W3af	23/tcp 80/tcp	All live switches on the LAN Management IP address of the switch Function of the switch in the network& IOS, manufacturers &switch model is identified
192.168.3.1 192.168.3.3	**Firewall/AS A**	**Cisco ASA-55x0 V 8.0(4)**	Non-technical (Documentation) traceroute Fping nmap	All ports are filtered	live Firewalls are identified IP address of the Firewalls Function of the Firewalls in the network IOS, manufacturers and Firewalls model
192.168.3.2 192.168.3.4	**Router/DH CP server**	**Cisco IOS 12.1(27)**	Non-technical (Documentation) nmap traceroute Fping	23/tcp 80/tcp	All live Routers are identified IP address of the routers Function of the routers in the network IOS, manufacturers and router model
192.168.5.1 0	**www.hu.ed u.et**	Linux 2.6.X	Fping nslookup nmap	53/tcp 80/tcp 443/tcp	Identification and Information about the Operating system Information about the patch level status

					Information about the Hardware Information on the services offered by the devices Information about the ports on the services
192.168.5.20	**mail.hu.edu.et**	Linux 2.6.X	Fping nslookup Nmap	22/tcp 25/tcp 53/tcp 80/tcp 110/tcp 143/tcp 465/tcp 587/tcp 993/tcp 995/tcp 5222/tcp 5269/tcp 7025/tcp 7777/tcp	Identification and Information about the Operating system Information about the patch level status Information about the Hardware Identification of server services offered (HTTP, SMTP, POP, IMAP etc.) Information about the ports on the services
192.168.5.30	**ns.hu.edu.et**	Linux 2.6.X	Fping nslookup nmap	22/tcp 53/tcp 80/tcp 8080/tcp	Information about the Operating system Information about the patch level status Information about the Hardware

Table 4.8: Network mapping summary

Based on the above table result, we realize that HU LAN uses two DNS server and all the service which are only accessed are primarily using the internal DNS server and those services which are going out into Internet uses DNS serves hosted at EthioTelecom. The following figure shows the mapping of HU LAN network structure regarding name serves and services.

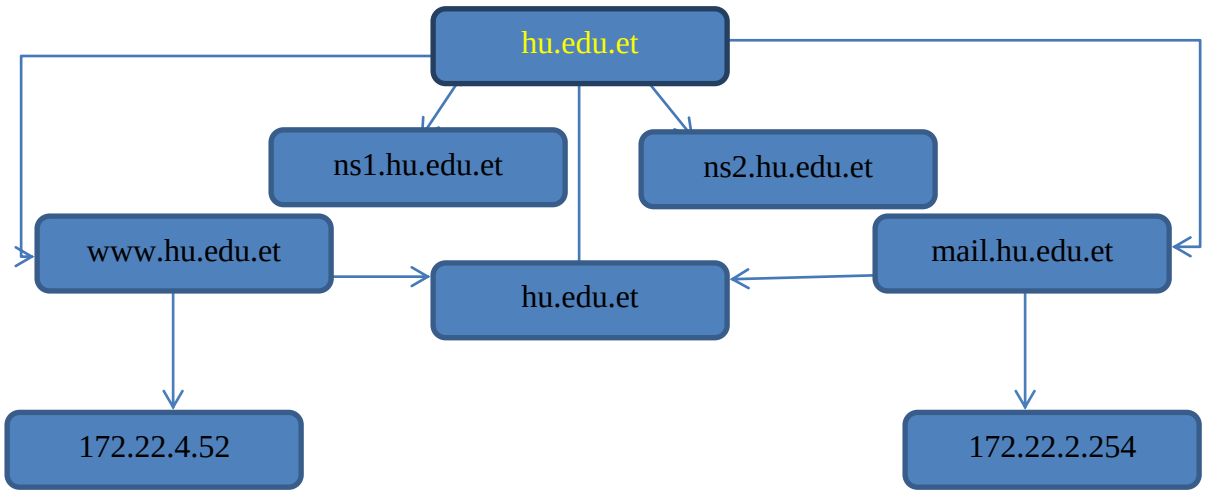


Figure 4.2. Network mapping summary

4.4. Vulnerability Identification

In this section of the study exploitable weak points have been detected;

- ✓ Perform vulnerability scan to search for known vulnerabilities on Switches, Routers and Firewalls
- ✓ Identify vulnerable services and applications.
- ✓ Perform false positive and false negative verification (e.g. by correlating vulnerabilities with each other and with previously acquired information)

4.4.1. Identify Vulnerabilities on Network Active Devices

The identified **Layer 2Switches, Routers and Firewalls** are examined for Vulnerabilities and for ways in which they can be manipulated.

Requirements:

- ✓ Results from Switches, Routers and Firewall identification
- ✓ Information on the firewall components used and network access to a point behind the firewall.

Test Steps:

- ✓ Attempt to find vulnerabilities on Layer 2 switches over the LAN(majorly focusing on the attacks compromising the availability)
- ✓ Run a vulnerability scanner on the Router/firewall system hosts(firewall hosts) from inside
- ✓ Attempt to hack and log in to the Router /Firewall using standard passwords.
- ✓ Identify and validate Router/Firewall ACLs

Tools used:

- ✓ fping
- ✓ nmap
- ✓ traceroute
- ✓ Macof
- ✓ Gobbler
- ✓ Ettercap
- ✓ Wireshark and
- ✓ Nessus

Result:

- ✓ Layer 2 switches vulnerabilities
- ✓ Firewall and Router vulnerabilities
- ✓ Verification of the identified vulnerabilities of the type of firewall in use
- ✓ Exhaustive list of the systems that can be reached behind the firewall

4.4.1.1. Layer 2 switches Vulnerabilities

1. MAC Attacks

a) CAM table flooding

Using "macof" tool that can flood a switched LAN with random MAC addresses so as to make full the CAM tables of the switches, in doing this, the hacking computer can easily capture frames that are not addressed to it. And also the availability will be highly affected. The syntax for this attack is:

Macof -i eth0 -s 192.168.10.66 –d 192.168.1.8

Randomly generated MAC addresses using Macof on the switch

56:2d:ce:5:3a:d1 46:d4:7c:4:cb:d 192.168.10.66.32706 > 192.168.1.8.11631: S 2027166896:2027166896(0) win 512

52:8d:95:3d:39:9d b7:f7:ed:69:12:6e 192.168.10.66.15163 > 192.168.1.8.14802: S 98038451:98038451(0) win 512

4e:fc:cb:30:30:be a9:72:5a:f:9e:7e 192.168.10.66.50551 > 192.168.1.8.1388: S 639407978:639407978(0) win 512

c2:fc:64:3c:41:4f a1:4b:6d:29:d8:15 192.168.10.66.19899 > 192.168.1.8.53957: S 1838444805:1838444805(0) win 512

e3:12:1d:11:5c:b7 86:e2:23:2c:c2:a3 192.168.10.66.25804 > 192.168.1.8.9263: S 1376686869:1376686869(0) win 512

6d:85:fb:3b:c8:c6 cb:cb:fa:51:a4:fc 192.168.10.66.32922 > 192.168.1.8.5714: S 206356110:206356110(0) win 512

73:2:f:52:de:4c 9a:a7:b8:4:f9:99 192.168.10.66.21066 > 192.168.1.8.27097: S 1150980233:1150980233(0) win 512

45:43:d5:75:32:4a 9c:93:ad:d:d5:86 192.168.10.66.40184 > 192.168.1.8.32739: S 431975925:431975925(0) win 512

ed:49:53:6d:5f:96 e5:f9:d6:6a:c:9c 192.168.10.66.47758 > 192.168.1.8.51679: S 16698049:16698049(0) win 512

c7:17:e2:78:85:e9 ef:87:ac:70:43:91 192.168.10.66.32727 > 192.168.1.8.50038: S 1780012256:1780012256(0) win 512

b5:77:a0:18:4b:eb 8b:d5:c7:18:9f:62 192.168.10.66.54565 > 192.168.1.8.50038: S 1420892512:1420892512(0) win 512

3f:42:6a:4b:5b:f b7:40:5f:54:a2:2a 192.168.10.66.3903 > 192.168.1.8.7371: S 123233346:123233346(0) win 512

28:ff:1:34:56:d0 39:3f:52:23:b8:6d 192.168.10.66.6711 > 192.168.1.8.11851: S 1169433596:1169433596(0) win 512

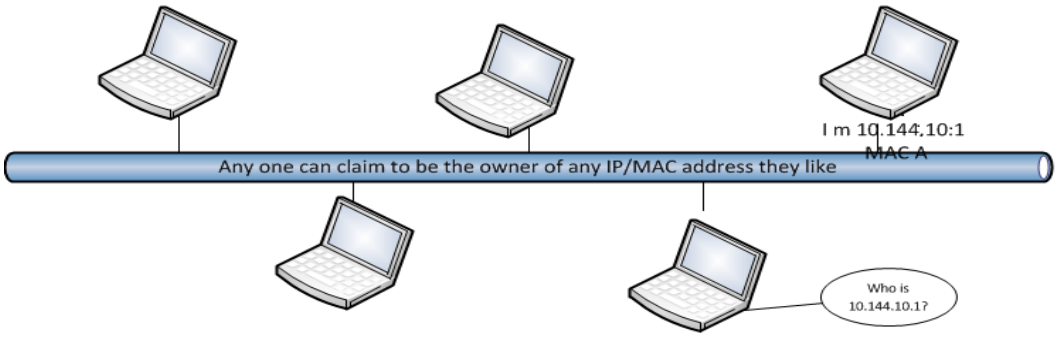
86:a0:4a:77:4b:e2 15:7b:e:41:a9:17 192.168.10.66.9667 > 192.168.1.8.31516: S 519195920:519195920(0) win 512

b) MAC Spoofing

MAC spoofing attacks occur when an attacker alters the MAC address of their host to match another known MAC address of a target host. In this test the attacker machine alters its MAC address by gateways MAC address and hence the computers connected to LAN in the same broadcast domain will consider the attackers machine as a gateway, all the frames which is aimed to be forwarded to the gateway is coming to the attacking machine; i.e. Since the switch changes the MAC address table, the target host does not receive any traffic until it sends traffic.

2. ARP Attack

ARP Spoofing/Poisoning



An ARP Spoofing attack is the egression of unsolicited ARP messages. These ARP messages contain the IP address of a network resource, such as the default gateway, or a DNS server, and replaces the MAC address for the corresponding network resource with its own MAC address, any traffic destined for the legitimate resource is sent through the attacking system. Using "***ettercap***" *spoofing tool,* we chose to ARP poison only on few windows machines in one broadcast domain; target machine IP address 192.168.10.230 and the router (gateway) 192.168.10.1.

On the Windows machine, with the help of ***Wireshark,*** we can compare the ARP traffic before and after the poisoning:

Before the poisoning

Before being able to communicate together, the router and the Windows machine send an ARP broadcast to find the MAC address of the other.

IP address Physical Address Type

***192.168.10.100-00-0c-07-ac-0a dynamic**

***192.168.10.3 00-0a-42-45-b4-0a dynamic After Poisoning**

The router ARP broadcast request is answered by the Windows machine similarly than in the previous capture.

The difference between the two steps comes from the fact that there is no request coming from Windows (192.168.10.230) to find the MAC address associated to the router (192.168.10.1) because the poisoner continuously sends ARP packets telling the Windows machine that 192.168.10.1is associated to his own MAC address (**bc-30-5b-c5-eb-f4**) instead of the router MAC address (**00-00-0c-07-ac-0a**).

IP address Physical Address Type

***192.168.10.1 bc-30-5b-c5-eb-f4 dynamic**

***192.168.10.3 00-0a-42-45-b4-0a dynamic**

Therefore, the ARP table of the router and the Windows machine are poisoned: The Linux machine is now "in the middle".

***Note:* In this test result the actual IP address is not disclosed to keep the confidentiality of the LAN Infrastructure**

4.4.1.2. Firewall Vulnerabilities

Tool used: Nessus/Vega

. **Vulnerability:** SSL Self-Signed Certificate

Synopsis: The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

. **Vulnerability**: SSL Certificate Signed using Weak Hashing Algorithm

Synopsis : The SSL certificate has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate that has been signed using a cryptographically

weak hashing algorithm - MD2, MD4, or MD5. These signature algorithms are known to be vulnerable to collision attacks. In theory, a determined attacker may be able to leverage this weakness to generate another certificate with the same digital signature, which could allow him to masquerade as the affected service.

. Other Vulnerabilities found on the HU Firewall

Tool Used: Nessus

The following list of vulnerabilities found in the HU Firewall, their risk factor is medium

OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Ciphersuite Disabled Cipher

SSL / TLS Renegotiation DoS

SSL Certificate Cannot Be Trusted

SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

SSL RC4 Cipher Suites Supported

Unencrypted Telnet Server

4.4.1.3. Router Vulnerabilities

Tool used: Nessus and Vega

1. **Vulnerability:** Unencrypted Telnet Server

Synopsis

The remote Telnet server transmits traffic in clear text

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information.

Use of SSH is preferred nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

4.4.2. Identified vulnerabilities on Hosts

Requirements: Information on the services used and the results of the port scans

Test Steps: Scan the services offered for potential vulnerabilities

Tools used:

- ✓ Nmap
- ✓ Wireshark
- ✓ Nessus
- ✓ Ettercap
- ✓ JoomScan
- ✓ W3af
- ✓ Ettercap
- ✓ Metasploit and
- ✓ Metasploit

Result:

- ✓ Using different vulnerability scanners, all the possible available vulnerabilities had been identified
- ✓ List of potential vulnerabilities on the services(e.g. DHCP server, DNS server web servers, mail server)

Note: *Only Vulnerabilities which has* ***medium*** *and* ***high Risk*** *factors are considered*

4.4.2.1. DHCP Server Vulnerabilities: Usually there are two different classes of potential security problems related to DHCP servers. The first one is Rogue DHCP Server Attack, and if an attacker plants this rogue DHCP server in to the production network, it is possible that the devices in the LAN could respond to client requests and supply them with spurious configuration information. This could be used to make clients unusable on the network. The second one is Unauthorized DHCP Clients or DHCP Starvation Attacks. If an attacker plants this attack, a client cloud be set up that masquerades as a legitimate DHCP client and thereby obtain configuration information intended for that client. This cloud then used to compromise the network later on.

The normal operation of DHCP enabled network is as follows:

DHCP Discovery (Broadcast) x (Size of Scope)

DHCP Offer (Unicast) x (Size of DHCPScope)

DHCP Request (Broadcast) x (Size of Scope)

DHCP Ack (Unicast) x (Size of Scope)

1. **DHCP Starvation Attacks using "Gobbler"**:A tool used to to audit DHCP networks

Description

Gobbler/DHCPx looks at the entire DHCP scope and tries to lease all of the DHCP addresses available in the DHCP scope;

Note: this is a Denial of Service /DoS/ attack using DHCP leases. Therefore, the attack isn't tested over the LAN. However, the configuration of the switches shows that it's vulnerable to this attack.

2. **Rogue DHCP Server Attack**

Description

A malicious user disguises itself as a DHCP server and responds to DHCP requests with a bogus IP address. These attackers are known as "man-in-the-middle" attacks. This attack is tested by inserting Rogue DHCP server; the configuration of the DHCP server is vulnerable to this attack.

4.4.2.2. DNS Server Vulnerability

DNS continues to be a favorable target for hackers. The ubiquity of BIND as DNS server software around the world, and the possibility as a hacker can expect should be he/she succeed in tacking over a server or simply use DNS implementation to reorient a traffic, are some of the things which make DNS a source of security issues. *[36]*

1. **Scanning (Port, Service and Operating System Fingerprinting)**

The following **Nmap** port and service scanning and Operating system fingerprinting output is discovered on DNS server:

Scanning 192.168.10.10

Initiating **SYN Stealth Scan** at 23:42

Discovered open port 22/tcp on 192.168.10.10

Discovered open port 53/tcp on 192.168.10.10

Discovered open port 8080/tcp on 192.168.10.10

Discovered open port 80/tcp on 192.168.10.10

Scanning 4 services on 192.168.10.10

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcpopen sshOpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)

ssh-hostkey: 1024 df:18:e2:ed:42:5c:9d:51:79:bd:08:f2:16:cc:66:3b (DSA)

2048 57:2a: fb: 06:b5:73: ab: c0:c1:d4:60:16:9f:d8:4f:f8 (RSA)

256 78:94:d1: fc: 7f:b7:a2:23: fc: b5:7d: 78:00:00:f9:ed (ECDSA)

53/tcpopen domain ISC BIND 9.8.1-P1bind.version: 9.8.1-P1

80/tcpopen http Apache httpd 2.2.22 ((Ubuntu))

Http-methods: GET HEAD POST OPTIONS

8080/tcpopen http-proxy Squid http proxy

Http-open-proxy: Potentially OPEN proxy.

Methods supported: GET HEAD

MAC Address: 00:26:55: FF: 25:48 (Hewlett-Packard Company)

Device type: general purpose

Running: Linux 2.6.X|3.X

OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3

OS details: Linux 2.6.32 - 3.6

2. **Vulnerability Test on DNS server**

DNS Cache poisoning and **DoS overflow** vulnerability Exploitation had been carried out on the DNS server. However, the server was not vulnerable to DNS poisoning and HU's DNS server is only vulnerable to any DoS attacks including DoS over flow.

Vulnerability: DoS over flow

Remote attackers cause a denial of service (memory consumption) via a crafted regular expression.

***Note:** In this test result the actual IP address is not disclosed to keep the confidentiality of the LAN Infrastructure*

4.4.2.3. Web Server Vulnerabilities

1. **Vulnerability:** PHP expose_php Information Disclosure

Tool used: Nessus and Vega

Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information

Description

2. The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.

3. Vulnerability: SVN user disclosure vulnerability

Tool used: W3af

Description

A .svn/entries file was found within the web root. This file is created by the popular *Subversion* version control system and it contains a list of files and directories under version control. The entries file is one of several Subversion metadata files created within ".svn/" subdirectories in the working directory (the local directory where files are checked out by a developer). It is common for these metadata directories to be copied up into the web root by developers.

The .svn/entries file is a serious information leak, as it can give attackers information about hidden files and directories within the web root.

4. Vulnerability: Full path disclosure vulnerability

Tool used: W3af

Description

Full Path Disclosure (FPD) vulnerabilities enable the attacker to see the path to the webroot/file. e.g.: /home/omg/htdocs/file/. Certain vulnerabilities, such as using the load_file() (within a SQL Injection) query to view the page source, require the attacker to have the full path to the file they wish to view.

5. Vulnerability: Cross-Site Request Forgery(CSRF)

Tool used : W3af and Vega

Description:

CSRF is an attack that tricks the victim into loading a page that contains a malicious request. An attacker can access functionality in a target web application via the victim's already authenticated browser. Targets include web applications like social media, in browser email clients, online banking, and web interfaces for network devices.

The following few scripts are vulnerable to a trivial form of XSRF

http://www.hu.edu.et/media/system/js/

http://www.hu.edu.et/images/stories/

http://www.hu.edu.et/components/com_docman/includes/

http://www.hu.edu.et/images/

http://www.hu.edu.et/xmlrpc/

----------*Output omitted*

6. **Web scanning**

Tool Used: joomscan

Vulnerability: Generic: htaccess.txt has not been renamed

Description:

htaccess.txt has not been renamed. Versions Affected: Any|/htaccess.txt|Generic defenses implemented in .htaccess are not available, so exploiting is more likely to succeed.

7. **Web Scanning**

Tool used: joomscan

Vulnerability: core plugin: TinyMCETinyBrowseraddon multiple vulnerabilities

Description: These vulnerabilities came due to missing the core plugins of joomla

4.4.2.4. Mail Server Vulnerabilities

Tool used: Vega and Nessus

1. **Vulnerability:** SSL Certificate Cannot Be Trusted

   Synopsis

   The SSL certificate for this service cannot be trusted.

   Description

   The server's X.509 certificate does not have a signature from a known public certificate authority.

   If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could establish a man-in-the- middle attack against the remote host.

2. **Vulnerability**: SSL Weak Cipher Suites Supported

   Synopsis

   The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

During the test using ettercap sniffing tool, while the user is accessing *http://mail.hu.edu.et*

user name: XYZ

password : abcd

it was possible to sniff the uncrypted user name and password

3. **Vulnerability:** Cross-Site Request Forgery(CSRF)

   Tool used : W3af

   Description: See the CSRF description above

   The following scripts are vulnerable to a trivial form of XSRF:

   http://mail.hu.edu.et/zimbra/css/skin.css

   http://mail.hu.edu.et/zimbra/

   http://mail.hu.edu.et/zimbra/css/common,login,zhtml.css

   http://mail.hu.edu.et/

   The following scripts allow an attacker to send POST data as query string data (this makes XSRF easier to exploit):

   The URL: http://mail.hu.edu.et/zimbra/ is vulnerable to cross-site request forgery. It allows the attacker to exchange the method from POST to GET when send in data to the server.

   The URL: http://mail.hu.edu.et/zimbra/css/skin.css is vulnerable to cross-site request forgery.

   The URL: http://mail.hu.edu.et/zimbra/ is vulnerable to cross-site request forgery.

   The URL: http://mail.hu.edu.et/zimbra/css/common,login,zhtml.css is vulnerable to cross-site request forgery.

   The URL: http://mail.hu.edu.et/ is vulnerable to cross-site request forgery

   .**Other Vulnerabilities found on the Mail server**

   Tool Used: Vega and Nessus

   The following list of vulnerabilities found in the HU Mail server, their risk factor is medium

   - ✓ SSL Anonymous Cipher suites supported

- ✓ DNS server zone transfer Information disclosure(AXFR)
- ✓ SSL medium strength cipher suites supported
- ✓ SSL version 2(V2) protocol detected
- ✓ SSL RC4 cipher suites supported

4.4.2.5. Vulnerabilities on Web Application and Databases

The interfaces which have been identified and can be accessed on internet, particularly those between self-developed systems are examined for potential vulnerabilities. This can involve DMZ services, which can access applications in HU network via an interface (e.g. accessing the system with online transactions) and applications within the institute network.

Requirements: Information on the applications and services used and the results of the port scans

Test Steps: Scan the services offered for potential vulnerabilities

Tools used:

- ✓ nmap
- ✓ Nessus
- ✓ JoomScan
- ✓ W3af
- ✓ Ettercap
- ✓ Metasploit and
- ✓ Metasploit
- ✓ SQLma

Result: Using different vulnerability scanners, all the possible available vulnerabilities had been identified.

Note: *Only Vulnerabilities which has* ***medium*** *and* ***high Risk*** *factors are considered*

SIS Server Vulnerabilities

1. **Vulnerability:** Clickjacking

   Tool Used: W3af

   Synopsis: Possible clickjacking attack

   Description

   The whole target has no protection (X-frame option header) against Clickjacking attack. Clickjacking, also known as UI-Redress attack, misleads the victim by overlaying multiple frames and making some frames invisible. Thus the victim is displayed with one webpage but his/her action is actually on another webpage that is selected by the attackers.

2. **Vulnerability**: PHP expose_php Information Disclosure

   Tool used: Nessus and Vega

   Synopsis

   The configuration of PHP on the remote host allows disclosure of sensitive information.

   Description

   The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.

3. **Vulnerability**: SSL Version 2 (v2) Protocol Detection

   Synopsis

   The remote service encrypts traffic using a protocol with known weaknesses.

   Description

   The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

4. **Vulnerability:** SSL / TLS Renegotiation DoS

   Synopsis

   The remote service allows repeated renegotiation of TLS / SSL connections.

   Description

   The remote service encrypts traffic using TLS / SSL and permits clients to renegotiate connections. The computational requirements for renegotiating a connection are asymmetrical between the client and the server, with the server performing several times more work. Since the remote host does not appear to limit the number of renegotiations for a single TLS / SSL connection, this permits a client to open several simultaneous connections and repeatedly renegotiate them, possibly leading to a denial of service condition

5. **Vulnerability:** .svn/entries Disclosed via Web Server

   Synopsis

   The remote web server discloses information due to a configuration weakness.

Description

The web server on the remote host allows read access to '.svn/entries' files. This exposes all file names in your svn module on your website. This flaw can also be used to download the source code of the scripts (PHP, JSP, etc...) hosted on the remote server.

6. **Other Vulnerabilities found on the SIS server**

Tool Used: Nessus and Vega

The following list of vulnerabilities found in the SIS server, their risk factor is medium

- ✓ SSL Anonymous Cipher suites supported
- ✓ SSL certificate cannot be trusted
- ✓ SSL self-signed certificate
- ✓ SSL medium strength cipher suites supported
- ✓ SSL weak cipher suites supported
- ✓ SSL RC4 cipher suites supported
- ✓ Web Server Uses Plain Text Authentication Forms
- ✓ Web Server Uses Basic Authentication Without HTTPS

4.5. False Positive and False Negative Verification

The primary requirement for a Vulnerability Assessment solution is accurate testing. Ease of use and clear reports are important, but if accuracy isn't there then little else matters.

Poor accuracy in Vulnerability Assessment produces two kinds of testing error.

- ✓ Overlooking vulnerability (a false negative) leaves a security flaw we don't know about.
- ✓ Reporting vulnerability as present when in fact none exists (false positive) sends we looking for something that can't be found.

Performing false positive and false negative verification is one of the sub procedures in this study, obviously we don't want either. As per the verification made on only few of the vulnerabilities detected in the previous section, the following are the verification outcomes

While we are attempting to attack SIS server using a tool called "*W3af"* it reports that the server is vulnerable to Blind SQL Injection.[43]

When running the Exploit feature from *W3af* it says, vulnerability exploited ….Done.

It was also tried to test the vulnerability with **SQLmap,** however the parameter is reported not injectable (it had been tried different approaches, level, etc.). Hence, it is expected to encounter false positives of this type while using *W3af.* [43]

4.6. Enumerating Discovered Vulnerabilities

- ✓ Obtain password (plaintext or encrypted) by sniffing or other techniques
- ✓ Sniffing management or user traffic over the LAN and analyze it

4.6.1. Obtain password (plaintext or encrypted) by sniffing

Password sniffing is a technique for gathering passwords that involves monitoring traffic on a network to pull out information.

There are many techniques that can be used to acquire someone's password without their permission. Some common techniques include:

- ✓Simply observing someone while they type their password, known as *"shoulder surfing*".
- ✓Tricking someone into telling you their password, known as "*social engineering*".
- ✓Stealing usernames and passwords from insecure systems
- ✓Guessing a password by trying out many possibilities from dictionaries and password lists, known as a "brute-force attack"
- ✓Guessing a password based on personal information you know, such as a birth date, pet's name, etc.
- ✓Installing software or hardware devices known as "keyloggers" to capture the input from the keyboard.
- ✓Monitoring network traffic to someone else's computer, known as "sniffing". Passwords sent in plain-text (no SSL or other encryption) can be discovered in this way.

In this study sniffing passwords, by using different tools and techniques on some of the services and network equipments had been carried out over the LAN. And it is observed that any time when a password is sent across a network, it is vulnerable to sniffing, Administrators use remote logging by sending the passwords to the systems. In most of the systems particularly all the network devices remote login and HU mail server's email address and passwords are sending over the network are disclosed in plaintext. Hence, sniffing of these usernames/passwords was easy task for the sniffer (particularly when the hacker is placed his hacking machine on the same broadcast domain). For example, it is common to sniff and catch user name and password of Firewalls, Routers and Switches over the network using a tool called "*Wireshark"*.

And also, when the user is trying to log into HU email service, since the service does not offer a secure login (i.e. A secure URL for a service starts with "https://"); however, HU's mail service is using only "*http*" and hence sniffing unencrypted account name (account_name@target_domain_name) and password using various tools (like *"Ettercap"*) was possible. [45]

4.6.2. Sniffing Management or User Traffic and Analysis

In the previous task, Sniffing the unencrypted user name and password had been carried out, then stealing the configuration files of the Firewalls, Routers and Switches was successfully executed, apart from this pivoting to all available network equipment had been carried out. Every Configuration file was sniffed and analyzed, some flaws (vulnerabilities) observed on the configuration files are listed below:

- ⇨ VLAN 1(default VLAN) in every switch over the LAN works as management VLAN
  - VLAN1 is a native VLAN which doesn't need VLAN tagging protocol, and hence it is vulnerable for VLAN hopping attack
- ⇨ Telnet protocol is used for remote login
  - Unencrypted or clear text of username and password are passing to devices over the LAN
- ⇨ SSH protocol for remote login is not supported by any of the active devices
  - The IOS needs to be upgraded to the latest version so as to support SSH as a default remote login protocol
- ⇨ The Router is also used as DHCP server on the LAN. However, because of the flaws it was having availability could be compromised highly
  - Since the DHCP server was not configured to limit the number of IP addresses to lease for the client machines by one interface, DHCP starvation attacks was successfully executed. Therefore, limiting the number of IP address request by client machines will not be able to lease more IP address than MAC addresses allowed on the port.
- ⇨ Limiting the number of IP addresses on a switch port is also used to mitigate MAC attack (CAM table Flooding)

- DHCP snooping untrusted clients is not configured, it was possible to introduce Rogue DHCP Server Attack on the LAN and compromise the availability of the services

⇨ Pivoting from one Switch to the routers or to Firewall (or vice versa)is allowed by the ***Access control list policy***, this might be very risky or will have high negative impact for the LAN to compromise integrity, confidentiality and availability of the services over LAN.

⇨ Cisco discovery protocol (CDP) is enabled on all the Networking equipments

- CDP shares information such as router model, software version, IP address and other information to the neighboring device, and hence an attacker could get all information about the network equipments. Therefore, CDP should be disabled in every switch/Router/Firewall configuration.

⇨ SSL protocol used by the Firewall is self-signed(i.e. when using a self-signed certificate, there is no chain of trust), A real certificate is safer than self-signed.

⇨ Since the mail server was using the default protocol (http://mail.hu.edu.et) sniffing the user account and password was executed, then any individual users information was disclosed

- *http* request ought to be redirected to https*(http + SSL)* to mitigate this flaw.

5. Chapter Five

5.1. Security Risk Analysis and Proposed Mitigation Countermeasures

5.1.1. Security Risk Analysis

HU has been striving to invest a multi million dollars to build the LAN infrastructure, purchase equipments, install and configure these equipments for the provision of different intranet and internet services over the LAN. However, so far security assessment and risk analysis was given less attention; paying no/less attention to this enormous issue could have an immense risk on the University services and business processes. In this section classification and quantitative risk analysis of vulnerabilities discussed. Apart from that the respective counter measures are proposed to mitigate the treats on each type of network device category and services running HU LAN infrastructure.

5.1.2. Quantitative and Qualitative Risk Analysis

Quantitative or qualitative (or both) risk analyses are conducted based on the security risk decision variables which include: Severity of the impact value of the asset and likelihood that vulnerability will be exploited.

5.1.2.1. Qualitative Risk Analysis

Qualitative security risk equation variables are not expressed in terms of monetary values, but as an ordered category of monetary loss such as “Critical,” “High,” “Medium,” and “Low. Qualitative assignments can be used to represent quantitative measure of security properties.

- ✓ Low means no vulnerabilities found;
- ✓ Medium, between one and five found; and
- ✓ High, more than five found,

5.1.2.2. Quantitative Risk Analysis

Quantifying the risk in terms of money is performed based on the two classic quantitative risk analysis formulas each service and application’s vulnerabilities they have.

- ✓ Annual loss expectancy
- ✓ Single loss expectancy

Annual loss Expectancy (ALE) *= Single loss Expectancy * Annual Rate of Occurrence*

Single loss Expectancy *= Asset Value * Exposure Factor*

Where, ***Asset value(AV)*** *refers to Implementation(configuration) value in terms of money and* ***Exposure factor(EF)*** *refers potential percentage of loss to a specific service/application if a specific threat is realized*

Since the scope of this study is focusing only on technical weakness (i.e. configuration or technology weakness) of HU LAN services and Applications, the quantitative risk analysis is done for the vulnerabilities which have a complete impact on availability over the LAN services.

5.2. Network Devices Security Risk Analysis and Counter Measures

Despite the risk /impact/ of service detection over the LAN is very low or none, acquiring all the basic information about a corporate network would be carried out prior to the other phases of attacking/exploitations. Therefore, HU should devise some mechanism for service detection countermeasures, such as:

- ⇨ Deny all unwanted traffic at network borders.
- ⇨ Keeping limited visibility to the open Internet is primary.
- ⇨ Use of PortSentry is the second-best method of protection;
    - PortSentry listens to unused ports on a system and detects connection requests on these supposedly quiet ports

5.2.1. Layer 2 Switch Vulnerability Risk Analysis

In a corporate LAN if layer two is hacked, communications are compromised without the other layers being aware of the problem. Figure 5.1 Shows that If L2 Switch's vulnerability is exploited the whole LAN service availability is compromised)

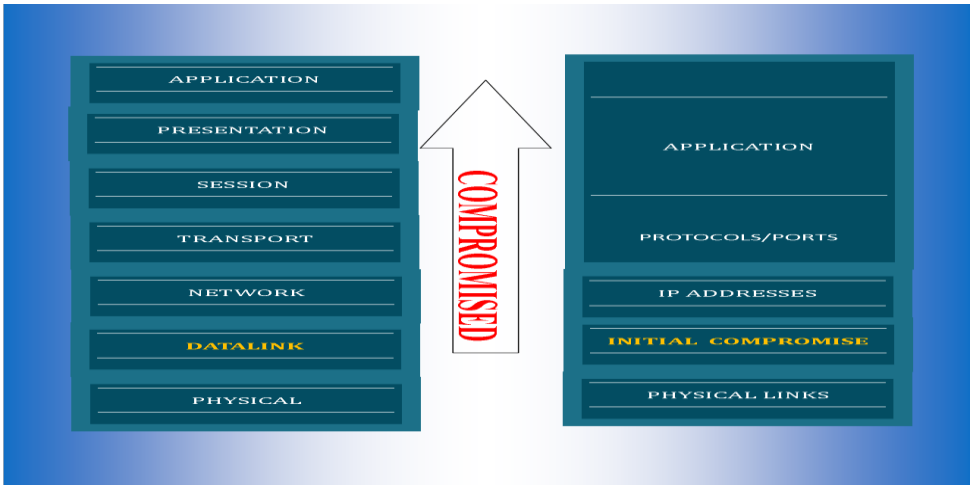


Figure 5.1. Layer 2 Vulnerability Impact

During the vulnerability identification, the following list of vulnerabilities obtained on Layer 2 (L2) switches and the risk factor is under *high* category, because if *CAM table flooding, MAC spoofing and ARP spoofing/poisoning* attacks techniques are executed the availability is absolutely compromised until it is recognized and solved.

The following vulnerabilities are recognized and observed on HU's Layer 2 Cisco Switches:

- ✓ VLAN 1(default VLAN) in every switch over the LAN works as management VLAN
  - VLAN1 is a native VLAN which doesn't need VLAN tagging protocol, and hence it is vulnerable for VLAN hopping attack
- ✓ Telnet protocol is used for remote login
  - Unencrypted or clear text of username and password are passing to devices over HU LAN
- ✓ SSH protocol for remote login is not supported by any of the active devices
  - The IOS needs to be upgraded to the latest version so as to support SSH as a default remote login protocol

Exploiting these attacks on the Layer 2 switches severely affect the availability of the service I.e. Exposure factor is 100 %(1). Asset Value (average configuration value in the current market) for a single L2 switch in terms money ≈ 3000.00ETB and currently an estimated number of Over 120 L2 switches are already joined the production network

⇨ Which implies that, Sub-Asset Value ≈ 9,500.00ETB * 155 ≈1472500.00ETB

HU is paying for the service provider (Ethio Telecom):

Per day = 6088.675ETB

Per month= 182660.25

Per year = 2,191,923.00ETB

If one of vulnerabilities could be exploited once in a month the total Asset value will be:

Asset Value= 360000.00ETB + 6088.675ETB = 1478588.675ETB

Single loss Expectancy = Asset Value * Exposure Factor

Therefore, single loss Expectancy=1478588.675ETB *1

≈**1478588.675ETB** ----------1

⇨Annual loss Expectancy of the exploit:

Annual loss Expectancy (ALE) = Single loss Expectancy * Annual Rate of Occurrence

≈ 1478588.675ETB * 12

≈**17,743,064.1ETB**----------2

Note: the loss can vary as per the frequency of the attacks (it may be less or more)

5.2.2. Counter Measures for discovered Vulnerabilities on L2 Switches

- ✓ Limiting the number of MAC addresses on a specific port of a switch can be a solution for this kind of attacks; the following configuration on a switch access interfaces a solution for mitigating this attack

  Switch#conf t

  Switch(config)#int range fa0/1 – 24

  Switch(config-if)#switchportportsecurity max 2 /* this command will restrict the number of MAC addresses to 2*/
- ✓ Use the port security feature to mitigate MAC spoofing attacks. Port security provides the capability to specify the MAC address of the system connected to a particular port. This also provides the ability to specify an action to take if a port security violation occurs. Particularly for all servers and Active devices connected to the switch, it's better to use sticky nature.

  Switch(config-if)#switchportportsecurityviolation restrict

  Switch(config-if)#switchportportsecuritymac address sticky
- ✓ Isolating production servers and Active devices from users VLAN (in another broadcast domain)

- ✓ Mitigation of ARP Poisoning can be performed on the Cisco IOS with DAI (DYNAMIC ARP INSPECTION) which is relying on *DHCP Snooping*.

  Enable DAI

  iparp inspection vlan<Vlan ID>

  Enable DHCP snooping

```
switch(config)# ipdhcp snooping
!Enable DHCP Snooping!
switch(config)# ipdhcp snooping vlanvlan_id {, vlan_id}
!Enable DHCP Snooping for specific VLANs!
switch(config-if)# ipdhcp snooping trust
!Configure an interface as trusted for DHCP Snooping purposes!
switch(config-if)# ipdhcp snooping limit rate rate
!Set rate limit for DHCP Snooping!
```

- ✓ Management VLAN should be changed from the default VLAN1 to another VLAN
- ✓ Secured Remote Login protocol should be changed from telnet to secured remote login protocol (SSH)
- ✓ Upgrading IOS of the switches should be performed

5.2.3. Routers and Firewalls Vulnerability Risk Analysis

HU's two Routers and two Firewalls are working at the core layer of the LAN, they are using Hot stand by Routing protocol (HSRP) (one is active and the other is standby), the routers are responsible for inter VLAN routing and also give service as a DHCP server. The Firewall is a gate way device and also split the network in to three major sub networks (Internal, External and DMZ networks)

The vulnerabilities obtained on the deployment of these devices are as follows:

⇨ Unencrypted Telnet Server

Unencrypted or clear text of username and password are passing to devices over the LAN

Risk Factor: Low

CVSS Base Score: 2.6

CVSS Vector Score: CVSS2#AV:N/AC:H/Au: N/C:P/I:N/A:N [14]

⇨ DHCP Starvation Attacks

Risk Factor: High (availability of the service will be highly compromised)

⇨ Rogue DHCP server attack

Risk Factor: High (particularly availability could be compromised highly)

⇨ VLAN hopping Attack

VLAN 1(default VLAN) in every switch over the LAN works as management VLAN

⇨ VLAN1 is a native VLAN which doesn't need VLAN tagging protocol, and hence it is vulnerable for VLAN hopping attack

Risk Factor: Medium

⇨ SSH protocol for remote login is not supported by any of the active devices

⇨ The IOS needs to be upgraded to the latest version so as to support SSH as a default remote login protocol

Risk Factor: Medium

⇨ SSL Self-Signed Certificate

- Risk Factor: Medium
- CVSS Base Score:6.4
- CVSS Vector Score:CVSS2#AV:N/AC:L/Au: N/C:P/I:P/A:N

⇨ SSL Certificate Signed using Weak Hashing Algorithm

- Risk Factor: Medium
- CVSS Base Score: 4.0
- CVSS Vector Score:CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N
- CVSS Temporal Vector:CVSS2#E:F/RL:OF/RC:C
- CVSS Temporal Score:3.3

⇨ Other Vulnerabilities with almost the same risk factor as the above SSL Self-signed Certificate:

- OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Cipher suite Disabled Cipher
- SSL / TLS Renegotiation DoS
- SSL Certificate Cannot Be Trusted
- SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
- SSL RC4 Cipher Suites Supported

Among the above listed vulnerabilities most of them exploitation's impact is medium, however they are capable of revealing the configuration file of the devices (there is nothing

safer more than disclosing the configuration files of network devices for the attackers).The higher the exploitation impacts on goals are, the higher the damage is. If even one aspect of the damage is High, the risk ultimately is high impact, and thus, we take the worst case scenario (pessimistic) as such:

Let *d1, d2…dn* be the values of damage metrics

Damage ≈ Max (d1, d2… dn)

Once the username and passwords are sniffed every configuration file is disclosed for the attackers, Exploiting this attack on the Routers/Firewalls severely affect the availability and confidentiality of the service. Which implies that Exposure factor are 100 %.

Let us say an asset Value (average configuration value in the current market) for a single core layer Router in terms money ≈ 12,000.00ETB and Asset Value (average configuration value in the current market) for a single Firewall in terms money ≈ 18,000.00ETB.

- ⇨ For two routers ≈ 2 * 12,000.00=24,000.00ETB
- ⇨ For two Firewalls ≈ 2 * 18,000.00ETB
- ⇨ Internet service Per day ≈ 6088.675ETB

If this vulnerability could be exploited once in a month the total Asset value will be:

Asset Value= 24000.00ETB + 6088.675ETB ≈ 30088.67ETB

Single loss Expectancy = Asset Value * Exposure Factor

= 30088.67ETB * 1≈ **30,088.67ETB**

Annual loss Expectancy (ALE) = Single loss Expectancy * Annual Rate of Occurrence

=30088.67ETB * 12 ≈**361,064.04ETB (for Routers Exploitation)**

With the same token for the Firewalls**:**

Single Loss Expectancy≈ **42,088.675 ETB**

The Annual loss Expectancy≈ **505,064.10 ETB**

The loss might be more than this (i.e. since the configuration of the Router/Firewall is a little bit complex the problem might not fixed within a day) and the down time may also seize the day to day activities of the University community.

Note: *The aforesaid attacks perhaps occur at the same time and the severity of exploitation will be in many folds than quantified above.*

5.2.4. Counter Measures for discovered Vulnerabilities on Router and Firewall

1. Secured Remote Login protocol should be changed from telnet to secured remote login protocol (SSH) (i.e. Disable telnet service and use SSH instead)
2. Attacker uses a new MAC address to request a new DHCP lease, therefore restrict the **z**

   Switch(config-if)# switchportportsecurity max 2

   Switch(config-if)# switchportportsecurity violation restrict

   The attacking machine will not be able to lease more IP addresses than MAC addresses allowed on the port (i.e. in the example the attacker would get only two IP addresses from the DHCP server)
3. Countermeasures for DHCP Attacks, Rogue DHCP Server = DHCP Snooping
   By default all ports in the VLAN are Untrusted; i.e. When configured with DHCP Snooping, all ports in the VLAN will be "Untrusted" for DHCP replies. Therefore, Rogue DHCP servers can be mitigated by DHCP Snooping features
   DHCP Snooping Untrusted Client
   Interface Commands:

   noipdhcp snooping trust (Default) DHCP Snooping Trusted Server or Uplink
   Interface Commands:

   ipdhcp snooping trust
4. Management VLAN should be changed from the default VLAN1 to another VLAN
5. Secured Remote Login protocol should be changed from telnet to secured remote login protocol(SSH)
6. Upgrading IOS of the Routers and Firewalls should be performed
7. Upgrade to OpenSSL 0.9.8j or later.
8. Purchase or generate a proper certificate for this service.
9. Contact the vendor for specific patch information.
10. Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

5.3. Hosts Vulnerability Risk Analysis

5.3.1. DNS Server vulnerability Risk Analysis

When we carried out DNS Cache poisoning and DoS overflow vulnerability exploitation on HU DNS server. The server is vulnerable to any DoS attacks including DoS over flow. If this threat is not resolved, the remote attackers could cause a denial of service (memory consumption) via a crafted regular expression.

Thus, DoS attack has its own risk factor. The risk Information depicted on below the table shows the impacts it poses on the target DNS server if exploited by the attacker.

Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service Overflow

Table5.1: DoS overflow risk information

CVSS Vector: AV: N /AC: L /Au: N/C:N/I:N/A:C

Risk Factor: medium

CVSS Base Score: 5.3

5.3.2. Counter Measures for discovered Vulnerabilities on HU DNS server

Denials of Service attacks have not gone away and are still used en mass to tie up services to make them unavailable. First of all to secure the DNS servers with recommended plugins (like updating BIND), and also only allow certain hosts to do DNS requests. However, it is impossible to stop this flood of traffic aimed at a site. Sometimes offensive counter measures like reflect the traffic back at the attackers is possible. Apart from the DoS overflow, DNS Cache poisoning vulnerability Exploitation had been carried out on the DNS server. However, the server was not vulnerable to DNS poisoning and HU's DNS server is only vulnerable to any DoS attacks including DoS over flow. It was good that it has been updated by the latest version of BIND.

5.3.3. Web Server Vulnerability Risk Analysis

The web server is vulnerable to:

- ⇨ PHP expose_php Information Disclosure
  - Risk Factor: Medium
  - CVSS Base Score: 5.0
  - CVSS Vector Score: CVSS2#AV:N/AC:L/Au: N/C:P/I:N/A:N
- ⇨ SVN user disclosure vulnerability
  - Risk Factor: Medium
  - CVSS Base Score: 5.0
  - CVSS Vector Score: CVSS2#AV:N/AC:L/Au: N/C:P/I:N/A:N
- ⇨ Full path disclosure vulnerability

  The risks regarding FPD may produce various outcomes. For example, if the web root is getting leaked, attackers may abuse the knowledge and use it in combination with file inclusion vulnerabilities to steal configuration files regarding the web application or the rest of the operating system
  - Risk Factors: Low to Medium (circumstantial)
  - Exploit Likeliness: Extremely High.
  - FPD vulnerabilities enable an attacker to know the path to the web root. This information can be used in order to launch further attacks.
- ⇨ Cross-Site Request Forgery(CSRF)
  - Risk Factor: High

- CVSS BaseScore: 5.1
- CVSS Vector: AV:N/AC:H/Au: N/C:P/I:P/A:P

⇨ htaccess.txt has not been renamed

- *htaccess.txt* has not been renamed. Versions Affected: Any|/htaccess.txt|Generic defenses implemented in .htaccess are not available, so exploiting is more likely to succeed.

⇨ core plugin: TinyMCETinyBrowseraddon multiple vulnerabilities

⇨ plain text password

5.3.4. Counter Measures for discovered Vulnerabilities on HU Web server

1. In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.
2. Remove .svnmetada subdirectories from web root, Ensure that .svn metadata directories are never present within the web root. The developer should use the "svn export" command prior to deploying their code onto the server, rather than "svn checkout" (the "export" command does not create any local .svn metadata directories).
3. Preventing an FPD injection without having an error handling / management system is as simple as disabling the display of error messages. This can be done in PHP's php.ini file, Apache's httpd.conf file, or via the PHP script itself:

   php.ini:

   ```
   display_errors = 'off'
   ```

   httpd.conf/apache2.conf:

   ```
   php_flagdisplay_errors  off
   ```

   PHP script:

   ```
   ini_set ('display_errors', false);
   ```

4. Various CSRF countermeasures available:
   - ✓ Requiring a secret, user-specific token in all form submissions and side-effect URLs prevents CSRF; the attacker's site cannot put the right token in its submissions
   - ✓ Requiring the client to provide authentication data in the same HTTP Request used to perform any operation with security implications
   - ✓ Limiting the lifetime of session cookies
   - ✓ Ensuring that there is no clientaccesspolicy.xml file granting unintended access to Silverlight controls

- ✓ Ensuring that there is no crossdomain.xml file granting unintended access to Flash movies

5. Upgrading the version of Joomla/installing the plugins/can resolve these vulnerabilities

5.3.5. Mail Server Vulnerability Risk Analysis

The following list of vulnerabilities discovered and risk is analyzed

- ⇨ SSL Certificate Cannot Be Trusted
  - Risk Factor: Medium
  - CVSS Base Score:6.4
  - CVSS Vector Score:CVSS2#AV:N/AC:L/Au: N/C:P/I:P/A:N
- ⇨ SSL Weak Cipher Suites Supported
  - Integrity, confidentiality and availability of the user can be compromised
  - Risk Factor: medium
  - CVSS Base Score:6.3
  - CVSS Vector Score: CVSS2#AV:N/AC:M/Au: N/C:P/I:P/A:P
- ⇨ Cross-Site Request Forgery(CSRF)
  - Risk Factor: Medium
  - CVSS Base Score: 5.1
  - CVSS Vector: AV:N/AC:H/Au: N/C:P/I:P/A:P

Other Vulnerabilities

- ⇨ SSL Anonymous Cipher suites supported
- ⇨ DNS server zone transfer Information disclosure(AXFR)
- ⇨ SSL medium strength cipher suites supported
- ⇨ SSL version 2(V2) protocol detected
- ⇨ SSL RC4 cipher suites supported

5.3.6. Counter Measures for discovered Vulnerabilities on HU mail server:

1. Purchase or generate a proper certificate for this service.
2. Reconfigure the affected application if possible to avoid use of weak ciphers.
2. Block any **http** request rather replace *https://mail.hu.edu.et*
3. See the mitigation proposed for CSRF vulnerability above.
4. Reconfigure the affected application if possible to avoid use of weak ciphers,
5. Limit DNS zone transfers to only the servers that need the information,

6. Reconfigure the affected application if possible to avoid use of medium strength ciphers,
7. Consult the application's documentation to disable SSL 2.0 and use SSL 3.0, TLS 1.0 or higher instead.

5.3.7. Web Application and Databases Security Risk Analysis and Counter Measures (SIS Server)

The following list of vulnerabilities identified, the risk is analyzed and counter measures are proposed to mitigate the vulnerabilities:

- ⇨ Clickjacking:
  - Risk Factor: Medium
  - CVSS Base Score:6.8
  - CVSS Vector Score: CVSS2#AV:N/AC:M/Au: N/C:P/I:P/A:P
  - CVSS Version 2 Metrics:
- ⇨ PHP expose_php Information Disclosure
  - Risk Factor: Medium
  - CVSS Base Score:5.0
  - CVSS Vector Score:CVSS2#AV:N/AC:L/ Au: N/C:P/I:N/A:N
- ⇨ SSL Version 2 (v2) Protocol Detection
  - Risk Factor: Medium
  - CVSS Base Score: 5.0
  - CVSS Vector Score: CVSS2#AV:N/AC:L/Au: N/C:P/I:N/A:N
- ⇨ SSL / TLS Renegotiation DoS
  - Risk Factor: Medium
  - CVSS Base Score: 4.3
  - CVSS Vector Score: CVSS2#AV:N/AC:M/Au: N/C:N/I:N/A:P
- ⇨ .svn/entries Disclosed via Web Server
  - Risk Factor: Medium
  - CVSS Base Score:5.0
  - CVSS Vector Score: CVSS2#AV:N/AC:L/Au: N/C:P/I:N/A:N

Other Vulnerabilities found on the SIS server

- ⇨ SSL Anonymous Cipher suites supported

- ⇨ SSL certificate cannot be trusted
- ⇨ SSL self-signed certificate
- ⇨ SSL medium strength cipher suites supported
- ⇨ SSL weak cipher suites supported
- ⇨ SSL RC4 cipher suites supported
- ⇨ Web Server Uses Plain Text Authentication Forms
- ⇨ Web Server Uses Basic Authentication Without HTTPS

5.3.8. Counter Measures for discovered Vulnerabilities on HU Web Application and Databases

1. The scary thing about a Clickjacking attack is there isn't any foolproof way of detecting when it is happening to web based applications. There are a few steps we can take to ensure clickjacking is stopped at the source
    - ⇨ Upgrade Flash Player
    - ⇨ Edit the Flash Settings(On Global Settings, Turn Flash Off at the Source)
    - ⇨ Block Scripts From the Browser
        - **Internet Explorer:** IE 8 and above have some safeguards in place that allow web developers to prevent unauthorized overlays on their web sites
        - **Firefox and NoScript:** Install the NoScript plug-in for Firefox. NoScript will prevent all Flash movies from playing whenever you visit a site
2. In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.
3. Consult the application's documentation to disable SSL 2.0 and use SSL 3.0, TLS 1.0 or higher instead.
4. Contact the vendor for specific patch information.
5. Configure permissions for the affected web server to deny access to the '.svn' directory.
6. Reconfigure the affected application if possible to avoid use of weak ciphers,
7. Purchase or generate a proper certificate for this service.
8. Reconfigure the affected application if possible to avoid use of medium strength ciphers
9. Reconfigure the affected application, if possible, to avoid use of RC4 ciphers
10. Make sure that every sensitive form transmits content over HTTPS

5.3.9. Summary and Discussion on Discovered Vulnerabilities found

The discovered vulnerabilities had been classified based on the capabilities they have to compromise Confidentiality, Integrity and Availability (CIA) on services and applications over the LAN. The following chart shows the **number** of Vulnerabilities discovered based on CIA with their impact (i.e. impacts such as **none, partial and complete**) respectively.

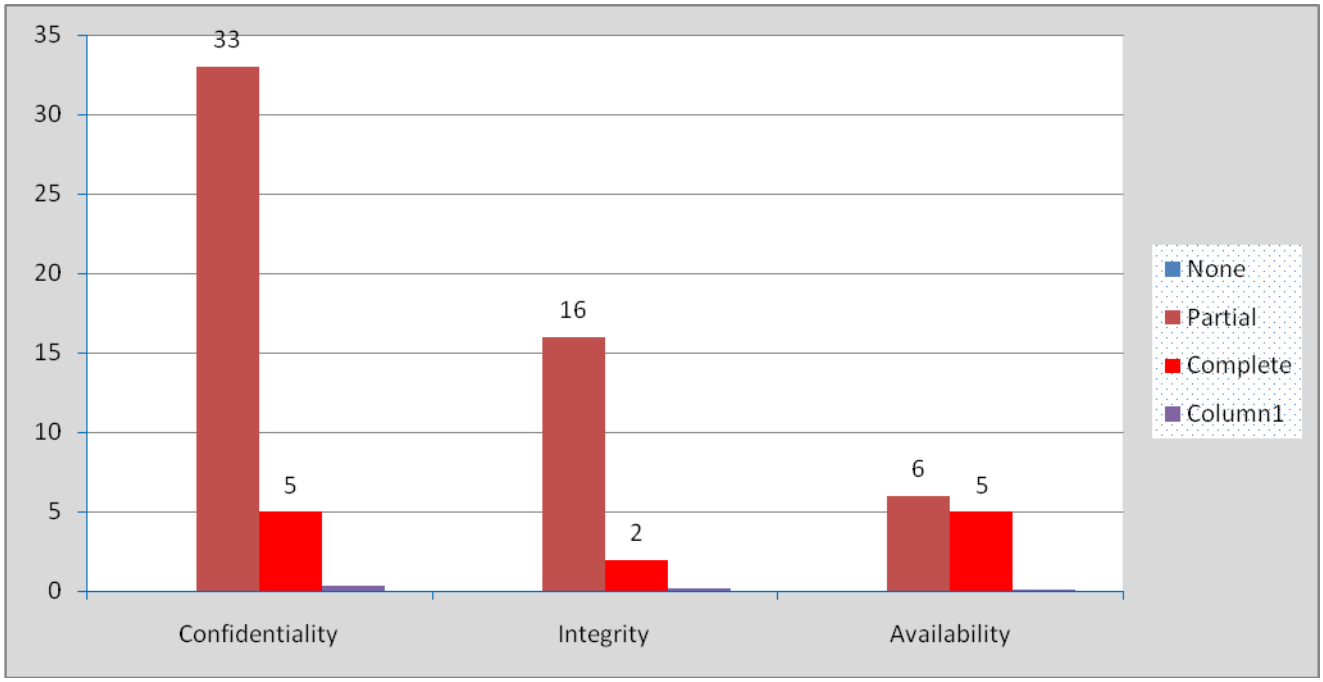


Figure 5.2: CIA based discovered Vulnerabilities

The impacts of Vulnerabilities (Low, Medium, and High) discovered on the services and applications are described as follows:

- ✓ High impact vulnerabilities = 17%
- ✓ Medium impact vulnerabilities 77.64%
- ✓ Low impact vulnerabilities 5.36%

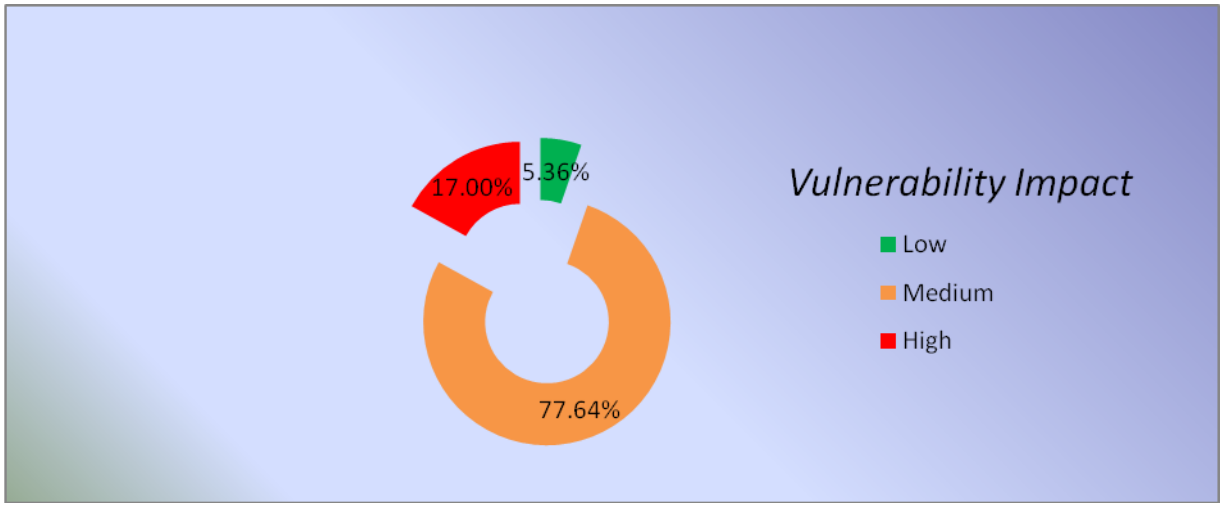


Figure 5.3: Vulnerabilities Impact percentage

So far the research found some other non-technical and administrative flaws which may lead the attackers to inspect the systems from different point because of the following reasons. HU network infrastructure is not centrally managed, each campus and schools already deployed different services on their locality and even it has no uniform IP address arrangement among the campuses. Each campus has its own IP address arrangement and additionally they have leased their own line from EthioTelecom but they also interconnected each other as a redundant link to go out to the internet. This situation opens up a great opportunity to the attacker to plot an attack from different point and simply risk the security of the services running in the campus.

Furthermore, we staged an attack on different HU LAN devices and services running in and out of the LAN based on Open Source Security Testing Methodology (OSSTMM) as shown on chapter four and we camp managed to find critical vulnerabilities and threats in HU LAN. Those identified loop holes on the network may cause unprecedented damage on the integrity and privacy of information of the individual user and the organization at large. The study mainly used the CVSS scoring of vulnerabilities to analyze and prioritize the Risks posed by the identified vulnerabilities if they are used by an attacker. Based on the threat level we proposed the right measures to be taken to mitigate the gap.

6. Chapter Six: Conclusions and Recommendations

In this Chapter, the conclusion and the recommendations for future works of this research is given. The Chapter is organized in three sections. Section 6.1 gives the conclusion of the study. The limitations faced on this research will be deeply discussed in section 6.2 and the recommendations for future works are presented in Section 6.3.

6.1. Conclusion

Ethiopian higher institution has a substantial number of computing utility (computers, phone, and other computing devices) which are regularly goes online in their campuses utilized by staff and students to benefit from unlimited resources from internet. Despite the increase in the utilization of internet over the year after year, the user and their providers have no concert knowledge of how far they are secure and will be secure they are in the realm of overwhelming abundance of resources and services they got over internet. Most of the University communities are still not fully exploring the power of computer and network resources, and these resources remain under-utilized or pose a serious risk because of the threats of virus and unavailability as well as luck of information integrity in an unsecured LAN infrastructure. Vulnerabilities are identified in this study shows that the network system and services running in the HU LAN have potentially exposed for attack and poses risk to the users and the system as well, if they are not properly mitigated.

In order to judge the security of a system accurately, adapting any single methodology does not necessarily provide a complete picture of the risk assessment process, hence, to execute different types of tests step-by-step the methodology of this study devised (merged) from the different a well known security assessment methodologies.

The study had carried out by identifying:

- ✓ Active devices, services and applications ought to be tested,
- ✓ The sampling technique to be used
- ✓ Security assessment techniques
- ✓ The tools to be used for the tests
- ✓ The procedures that should be applied during the test and
- ✓ Security metrics to be used to perform risk analysis and mitigation

The security assessment had been executed by grouping HU LAN systems in to *Host*

security, *Network security* and *Application and database security*. By using stratified Sampling technique. Samples from different LAN active devices had been carefully chosen and different tools and techniques applied for security assessment test.

The procedures of the research were clear and well defined like; planning and determining the scope, Vulnerability Assessment and Identification, Security Risk Analysis and Countermeasures, finally after the report is compiled Clean-up and Destroy Artifacts from the testing environment to clear the footprints to the target system.

As per the procedure followed, after the scope is determined, the reconnaissance phase had been carried out. The result of network mapping, such as target's IP address, name, and Operating system type, how it is discovered, listening ports etc. are summarized.

Vulnerability identification and verification had been carried out, i.e. vulnerability scanning to search known vulnerabilities on switches, Routers, Firewalls, hosts/services/ and applications; and also false positive and false negative verification were performed. The vulnerabilities with medium and high Risk factors are considered. All the available vulnerabilities had been identified and verified, these include:

- ✓ Layer 2 switches vulnerabilities
- ✓ Firewall and Router vulnerabilities
- ✓ Hosts/services/ vulnerabilities
- ✓ Application and Database vulnerabilities
- ✓ Enumeration of Identified vulnerabilities
- ✓ Verification of the identified vulnerabilities(i.e. few controlled Exploitation on the identified vulnerabilities carried out)

Apart from this, in the vulnerability identification phase all devices, services and applications mentioned on the scope of this research had been tested against a well-known vulnerability on common vulnerability data bases (CVE). However, executing risk analysis and mitigation technique was proposed only for the discovered vulnerabilities. Security risk impact is analyzed qualitatively and quantitatively (in terms of monetary values particularly for those which have immense impact on availability) and mitigation for all the discovered vulnerabilities forwarded.

6.2. Limitations of the Study and Future work

As mentioned in the scope and limitation of the research, during this research I have face some very challenging obstacles that are hindered the progress of the study. Hawassa university today almost totally relying on ICT infrastructure to process and execute it business; however, it is investigated in the study that security has been overlooked by HU's IT professionals rather deploying some security devices on the system, they couldn't notice the matter how big it is, because either they couldn't comprehend the risks or it might not distress their system so far. Paying less attention for security might have devastating effect and overwhelm the whole system of the institute. This research finding gives special insights towards both the knowledge and applied domains for future researches and projects. Some of the limitations we have faced during the study are list below:

- The university concerned body is not even willing to provide the necessary information for this research because of the suspicion of if we might hurt or compromise their system in service. For example the ICT directorate office did not let us get the necessary documents for the study such as the university Security Policy, core devices configuration and the network logical diagram to analyze it based the standards and tools which may help us to study the posture of the infrastructure.
- The tools to run the research test bed require higher machines and even some of the tools are freely available. Because of this the study only limited on analyzing secondary data and international practices which might work on HU's LAN structure.
- Weaknesses on LAN services and applications can be from technical (misconfiguration or technology) or administrative (management or policy) or Physical. However, the scope of this research was limited only on technical flaws of the LAN systems and assessment on administrative policy issues need further work.
- Security assessment is an ongoing task and it needs more time to learn the process but less than six months of time was allotted for this research, and hence by allocating more time security assessment over the LAN services like; Wireless LAN and on all business process applications and databases ought to be executed. Additionally because of time limit the research only focuses on main campus network devices and services.
- Because of the risk of crashing a target system during a test, some particular attack vectors were off the table for a vulnerability testing. By referring to the publicly

available known exploits from well-known vulnerability databases like CERT, CVE and others, assessment should be done regularly.

- In this study we have only focused on main campus network, the other three campus network infrastructure is needs to be assessed. Different services like, e-learning, Library Information Management System and others are not even located in the university data cent rather they are situated on the perspective offices without considering the security risk.

6.3. Recommendations

The goal of this research is to have a secured ICT infrastructure is to defend information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. From this research point of view, misconfiguration of services and applications exposed the LAN for the vulnerabilities that could have enormous impact on HU LAN. Finally I would like to put forward our recommendation:

1. The University needs to have strong ICT policy for:
   - Information Technology governance
   - Security and Program Change management
   - Environmental and Physical access control
   - ICT service continuity
   - Logical Access Control
   - Internet Acceptable use policy
2. Upgrading IOSs of Networking devices on a regular basis
3. Consider all the vulnerabilities reported by this research and reconfigure the affected application the soonest possible with the proposed countermeasures
4. Unknown plugins are identified so it s better to look for plugins and patches from well-known vendors
5. Purchase or generate a proper certificate for all deployed services.
6. Regularly contact the vendor for specific patch information.
7. It is better to centrally manage resources and devices in the well designed and Data Center and all the university campuses to have and share same bandwidth with redundant lease line.

Reference

1. *ABDUL KADIR KHAN. (2012). "Use of Internet By Teachers And Research Scholars In Hawassa University", Department of Informatics Hawassa University, Hawassa, Ethiopia*
2. *Patrick Engebretson, (2011). "The Basics of hacking and penetration Testing: Ethical hacking and penetration Testing Made East", New York. Syngress Press.*
3. *Moazzam Khan. (2013). "Security Metric Based Network Risk Assessment". Georgia. Georgia Institute of Technology.*
4. *Security Innovation.Inc. "Security Testing Methodology. 2011. Attacking Software Applications to Uncover Vulnerabilities", Boston, Seattle.*
5. *Ali A., Dr. Mohd. R., Shish A. (2012). "Analysis of Penetration Testing and Vulnerability Assessments with New Professional Approach", India. Dept. of C.S.E/IT, Integral University.*
6. *Nakeva N. (2000-2002). "Methodologies to Perform a Self-Assessment", USA. SANS Institute.*
7. *IT Threat Evolution: Q2 2012, [Web], June, 2015. from http://www.securelist.com/en/analysis/204792239/IT_Threat_Evolution_Q2_2012*
8. *IT Threat Evolution: Q3 2012, [Web], June, 2015. from: http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012*
9. *Scarfone K., Murugiah S., Amanda C., Angela O. (2008). "Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology" Gaithersburg. 2008.*
10. *Positive Technologies. 2011 "POSITIVE RESEARCH: Vulnerability Statistics"*
11. *Mansour A. 2010. (2010). "Writing a Penetration Testing Report: GIAC (GPEN) Gold Certification". SANS Institute.*
12. *Jeremiah Grossman, (2012). "Whitehat Security Website Statistics Report". USA. WhiteHat Security.*
13. *Hawassa University official web site: http://www.hu.edu.et/*
14. *Peter Mell., Karen S., Sasha R. (June, 2007). "A Complete Guide to the Common*

Vulnerability Scoring System, Version 2.0, USA. National Institute of Standards and Technology".

15. *Kaspersky Security Bulletin. Statistics (2011), [Web}. June, 2015. from: http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011*
16. *White Security Web Site Statistics Report, (Summer 2012),[Web]. July, 2015. from:https://www.whitehatsec.com/assets/WPstats_summer12_12th.pdf*
17. *The Most Vulnerable Operating Systems and Applications in 2011, [Web]. from: http://www.gfi.com/blog/the-most-vulnerable-operating-systems-and-applications-in-2011/*
18. *PENETRATION TESTING METHODOLOGY.[Web], from:http://www.oissg.org/wiki/index.php?title=PENETRATION_TESTING_METHODOLOGY*
19. *Farkhod A, Feruza S. (2009). " Methodology for Penetration Testing", South Korea. Hannam University.*
20. *Berinato S. "A Few Good Information Security Metrics". (2005) [Web. from: http://www.csoonline.com/article/220462/a-few-good-information-security-metrics*
21. *BackTrack 4: Security with Penetration Testing Methodology: [Web], from:http://backtrack4-security-penetration-testing-methodology.html*
22. *Scott Berinato, (2005). " A Few Good Information Security Metrics"*
23. *Karen Scarfone, Murugiah Souppaya, Amanda Cody, and Angela Orebaugh, (2008). "A Complete Guide to the Common Vulnerability Scoring System Version 2.0". National Institute of Standards and Technology.*
24. *Kadry S.W. (2008). "Design and Implemetation of System and Network Security for an Enterprise with Worldwide Branches" Beirut, Lebanon. Hassan School of Engineering.*
25. *Salah A. Design and Implementation of a Network Security Model for Cooperative Network, Mosul, Iraq.*
26. *Rajasthan, India. V. S. Rathore, Jaipur, Santosh K. M. "A Novel Distributed Network for Ensuring Highly Secure Proposed Enterprise Network Integrated Firewall",*
27. *M. E. Kabay, Network World, Security metrics research, May 27, (2009). [Web]. from:http://www.networkworld.com/newsletters/2009/052509sec2.html*

28. *The Role of Information Communication Technology in Education: case of Eastern Mediterranean University Oluwatobi Bakare, Fisseha Mikre, Eastern Mediterranean University*
29. *Abiy Woretaw, (2012). "Information Security Culture In The Banking Sector In Ethiopia" Information Network Security Agency*
30. *C. Onwubiko, A. P. Lenaghan, L.Hebbes . (2009). " An Integrated Security Framework for Assisting in the Defense of Computer Network", Kingston, UK. Kingston University,*
31. *Salah Alabady (2009). "Design and Implementation of a Network Security Model for Cooperative Network" Computer Engineering Department, University of Mosul, Iraq,*
32. *Dessie Kiber (2011). " Analysis of the health information security management practices of healthcare organizations in Amhara region, Ethiopia the case of Felege Hiwot Regional Referal Hospital", Addis Ababa University*
33. *A Penetration Testing Model, German Federal Office for Information Security, Undated*
34. *DNSstuff Toolbox: [Web],August, 201.5 from:* http://www.dnsstuff.com/, *last accessed on July 28, 2015*
35. *Maltego for pen Testers: [Web], from:* http://www.paterva.com/maltego, *last accessed on July 6, 2015*
36. *SANS, Security 560.2, (2011) Network Penetration Testing and Ethical Hacking*
37. *TCPDUMP & LiBPCAP: [Web], Web:* http://www.tcpdump.org, **Release Date:** *May 20, 2015*
38. *Nmap Security Scanner: [Web], from:* http://www.nmap.org, *last accessed on June 3, 2015*
39. *Nessus Vulnerability Scanner: [Web], From:* http://www.nessus.org, *last accessed on June 5, 2015*
40. *Samurai Web Testing Framework: [Web], From: http://www.samurai-wtf.org/, last accessed on June 2, 2015*
41. *Assessing and Exploiting Web Applications with Samurai-WTF, 2012, Justin Searle (et.al)*
42. *OWASP Joomla Security Scanner: [Web], from:*http://sourceforge.net/projects/joomscan,*Last Updated: 2014-05-04*
43. *Nikto is an Open Source web server scanner: [Web], from :*http://cirt.net/nikto2, *last*

accessed on June 20, 2015

44. *Ettercap [Web], from:* http://ettercap.github.io/ettercap/ *last accessed on June 10, 2015*
45. *Wireshark [Web], From:*http://www.wireshark.org/, *last updated on June5 , 2015*
46. *W3af [Web], from:*http://w3af.org/ *,last accessed on June 10, 2015*
47. *Metasploit [Web], from:* http://www.metasploit.com, *last accessed on May,1, 2015*
48. *SQLmap [Web], from:* http://sqlmap.org/, *last accessed on June 13, 2015*
49. *Official website of the Department of Homeland Security, [Web], from: https://buildsecurityin.us-cert.gov/articles/tools/black-box-testing/black-box-security-testing-tools, last updated May 14, 2015*

Glossary

Terms	Explanation
Application	Web based business process applications/softwares/
Active Directory	A server is a common repository for information about objects that reside on the network, such as users and groups, computers and printers, and applications and files
AAA	AAA is the acronym for authentication, authorization, and accounting. A service that can be used for user access control; AAA will give control and better audit for username and password for administrators
Black-box test	A penetration test in which the tester has no prior information about the network he/she is testing.
CERT	Computer Emergency Response Team; a group of IT specialists who ward off attacks on IT systems.
CGI	Common Gateway Interface; program for processing data on a web server that has been transferred from a =>browser.
Cracker	A person who obtains unauthorized access to or manipulates other IT systems, often with unlawful intentions.
CVE	Common vulnerability Entry databases
CVSS	Common Vulnerability Scoring System
DDoS	Distributed => Denial-of-Service; a DoS attack in which the target system is attacked by means of simultaneous attacks on a number of distributed systems.
Denial-of-Service (DoS)	A cracker's attacking method in which it tries to impair the availability of an IT system by overloading it
DMZ	De-Militarized Zone; a decoupled, isolated partial network located logically between an insecure network and a network that has to be protected and normally contains servers or services such as web servers and e-mail servers that can be accessed externally.
DNS	Domain Name System
Domain Name System	A mechanism for turning computer names into =>IP addresses
DoS	Denial-of-Service
Firewall	Protection measure between two computers when one has a higher protection requirement
FTP	File Transfer Protocol; application layer protocol for the transfer of files
Grey Box Testing	Acombination of white-box testing and black-box testing. The aim of this testing is to search for the defects if any due to improper structure or improper usage of applications. Gray-box testing is also known as translucent testing
Hacker	A person with a technical interest in the functionality of hardware and software and therefore has the know-how necessary for circumventing security arrangements in hardware and software. Often no distinction is made between a hacker and a cracker in everyday language, while the distinction is normally upheld in specialist circles.
Host	Operator of a server.
HTTP	Hypertext Transfer Protocol; application layer protocol for presenting websites.

IP address	A number that consists of four blocks of numbers between 0 and 255 (written in decimals) and which can be used address a system on the internet or intranet
ISA server	A server used for web filtering
LAN	Local Area Network.
Linux	A free (=> Open Source) Unix compatible operating system.
Network Active Devices	Network devices like Router, Firewalls, Switches, Access points, Hubs, Bridges, etc.
Open Source	An initiative that promotes the free availability of software and the disclosure of the corresponding source codes
OSI reference model	Seven-layer model for demonstrating and standardizing communication between computer systems.
Packet filter	Security layers 1 to 3 of the =>OSI reference model.
Router	A network device that connects two or more networks
Security policy	A document that describes the security objectives of an organization in an abstract way
Services	Services provided over the LAN to make successful communication (i.e. services like Web Service, mail Service, DNS service, DHCP Service, Proxy Service Etc.)
SMTP	Simple Mail Transfer Protocol; an application layer protocol mainly used for transferring e-mails.
Sniffer	A tool for intercepting network traffic
Spoofing	The attacking method of a cracker who attempts to deceive systems or persons through technical manipulation (e.g. faking a false IP address, faking a false DNS address etc.)
TCP/IP	A network protocol used on the internet and in internal networks.
Tools	Softwares/ Scripts used Reconnaissance, Vulnerability scanning, identification, verification/Exploit the Vulnerabilities
Vulnerability scanner	Security software which allows systems to be checked for potential software vulnerability and security gaps.
WAN	Wide Area Network; an organization-wide network that spans several different sites
VPN	Virtual Private Network : a Private network over a public line
Web bug	An invisible part of a website which enables a system not visible to the user to intercept information on the user's system configuration (IP address, browser version etc.)
Web server	A computer that makes information available on the internet for retrieval
White-box test	A penetration test in which the tester has prior information on the network he/she is testing.

Appendices

A.1 Tools

The following table provides a list of security assessment tools that had been used in this study. Most of the tools listed are freeware. The list does not compare the functionality of the tools and does not claim to be exhaustive.

Name	Particularities	Platform	Source
Reconnaissance tools			
Ping	End to end connectivity	Unix/Linux, Windows	
fping	End to end connectivity	Unix/Linux,	
Nslookup	DNS lookup	Unix/Linux, Windows	http://www.dnsstuff.com
Whois	Implements a standard whois search	Unix/Linux, Windows	http://www.dnsstuff.com
dig	Perform zone transfers on Linux and Unix platforms	Unix/Linux,	http://www.dnsstuff.com
Maltego	Over 50 different kinds of transforms, such as: DNS IP address to org name(netblock) Org name to person's name(whois) Person's name to PGP key (public key servers) PGP key to person's name(who signed the key?) Person's name to phone numbers (phone lookup)	Unix/Linux, Windows	http://www.paterva.com/maltego
Google FU	Email and file match	All	http://www.google_fu.com
Port scanners			
Nmap	Port scanner with	Unix/Linux,	http://www.insecure/nmap

	extended functions such as stealth scans or system recognition	Windows	
Super Scan	Port scanner with an easy-to-operate user interface	Windows	http://www.computech.ch
Vulnerability scanners			
Nessus	Vulnerability scanner made up of client and server components	Unix/Linux, Windows	http://www.nessus.org
Joomscan	OWASP Joomla! Security Scanner	Unix/Linux, Windows	*http://sourceforge.net/projects/joomscan/*
SamuraiWTF	live linux environment that has been pre-configured to function as a web pen-testing environment	Windows, Unix/Linux	http://samurai.inguardians.com
w3af	**Web Application Attack and Audit Framework**	Windows, Unix/Linux	http://w3af.org/
Vega	An Open Source Web Application Security Platform Vulnerability scanner	Windows /Linux	https://www.subgraph.com/
LAN sniffers			
Dsniff	Dnisff contains a collection of programs that allow the interception of network traffic in switched networks	Unix/Linux	http://www.monkey.org
Ethereal /WIreshark/	A packet sniffer that can also interpret application layer information	Windows, Unix/Linux	http://www.ethereal.com
Tcpdump	Packet sniffer for OSI layers 1 to 4	Unix /Linux	http://www.tcpdump.org
Scapy	Packet crafting, manipulation, and analysis	Linux/Unix	SANS Security 560.2
Ettercap	Comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and	Linux/Unix	http://ettercap.github.io/ettercap/

	many other interesting tricks		
Cain	Password sniffing and cracking tool	Windows, Unix/Linux	http://www.oxid.it/cain.html
Attacking tools			
Hping	For testing firewall rules, many other options	Unix/Linux	http://www.hping.org
Macof	Flood network with random MAC addresses with macof tool	Unix/Linux	http://tournasdimitrios1.wordpress.com/
Gobbler	Exploiting Ethernet, Honeypot technology and DHCP	Windows, Unix/Linux	*http://gobbler.sourceforge.net/*
W3af	**Web Application Attack and Audit Framework**	Windows, Unix/Linux	http://w3af.org/
Metasploit	World's most used penetration testing software	Windows, Unix/Linux	*http://www.metasploit.com*
SQLmap	an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers	Unix/Linux	http://sqlmap.org/

A.2. Sample Output of Vulnerabilities

Sample out for HU web server using Vega Vulnerability scanner

AT A GLANCE

Classification	Input Validation Error
Resource	**http://www.hu.edu.et/cncs/index.php**
Parameter	**jat3file**
Method	**GET**
Detection Type	**Blind Text Injection Differential**
Risk	**High**

REQUEST

GET /cncs/index.php?lang=en&jat3action=gzip&jat3type=js&jat3file=t3-assets/js_a3902.js'"

RESOURCE CONTENT

```
File          t3-assets/js_a3902.js'"          /var/www/cncs/t3-
assets/js_a3902.js'" not exist
```

DISCUSSION

Vega has detected a possible SQL injection vulnerability. These vulnerabilities are present when externally-supplied input is used to construct a SQL query. If precautions are not taken, the externally-supplied input (usually a GET or POST parameter) can modify the query string such that it performs unintented actions. These actions include gaining unauthorized read or write access to the data stored in the database, as well as modifying the logic of the application.

IMPACT

- Vega has detected a possible SQL injection vulnerability.
- These vulnerabilities can be exploited by remote attackers to gain unauthorized read or write access to the underlying database.
- Exploitation of SQL injection vulnerabilities can also allow for attacks against the logic of the application.
- Attackers may be able to obtain unauthorized access to the server hosting the database.

REMEDIATION

- The developer should review the request and response against the code to manually verify whether or not a vulnerability is present.
- The best defense against SQL injection vulnerabilities is to use parameterized statements.
- Sanitizing input can prevent these vulnerabilities. Variables of string types should be filtered for escape characters, and numeric types should be checked to ensure that they are valid.
- Use of stored procedures can simplify complex queries and allow for tighter access control settings.
- Configuring database access controls can limit the impact of exploited vulnerabilities. This is a mitigating strategy that can be employed in environments where the code is not modifiable.
- Object-relational mapping eliminates the need for SQL.

REFERENCES

Some additional links with relevant information published by third-parties:

- SQL Injection (Wikipedia)
- mysql_real_escape_string() (PHP Manual)
- SQL Injection (Rails security guide)
- How To: Protect from SQL Injection in ASP.NET (MSDN)
- Dynamic SQL and SQL Injection (Raul Garcia's blog)
- SQL Injection Prevention Cheat Sheet (OWASP)