WEB SECURITY VULNERABILITY ANALYSIS OF ETHIOPIAN GOVERNMENT OFFICES

BY

TILAHUN EJIGU (ID 7658/12)

A Thesis Submitted to

The Department of Computer Science for the Partial Fulfillment of the Requirements for the

Degree of Master of Science in Computer Science

ADMAS UNIVERSITY

January 2020

Addis Ababa

Statement of Declaration

I, am under signed, declare that this thesis entitled: **Web Security Vulnerability Analysis of Government Offices** I have undertaken the research proposal work independently with the guidance and support of the research advisor **Dr. Asrat M.** This research has not been submitted for any degree or diploma program in this or any other institutions and that all sources of materials used for the thesis has been duly acknowledged.

Declared by

Name: Tilahun Ejigu Belay

Signature: _____

Department: Computer science

Date _____

Certificate

This is to certify that the thesis report is prepared by Tilahun Ejigu, entitled ***"Web Security Vulnerability Analysis of Ethiopian Government Offices"*** and submitted in partial fulfillment of the requirements for the Degree of Masters of Science/MSc in Computer Science complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Name of Candidate: **Tilahun Ejigu** Signature: _____Date: _____.

Name of Advisor: **Dr. Asrat M.**: _____Date: _____.

Signature of Board of Examiner`s:

External examiner: _____Signature: _____Date: _____.

Internal examiner: _____Signature: _____Date: _____.

Dean, SGS: _____ Signature: _____Date: _____.

Acknowledgements

I am happy to offer my thanks to all who support and rendered their significant offer assistance for the fruitful finish of the research and I would like to extend my deepest gratitude to information network security agency (INSA), for its cooperation in providing to permit in which black box testing of governmental website. I am grateful to my advisor **Dr. Asrat M.** for his direction and consolation in this work. I want to express my gratefulness and on account of all my associates and relatives who purposely or accidentally have helped what's more, supported me all through my work to accomplished .

Tilahun Ejigu

ABSTRACT

This research focused on detailed analysis of Ethiopian governmental office server side and client side ***"Web Security Vulnerability Analysis of Ethiopian Government Offices"***. The purpose of this assessment is to discover weak links (vulnerabilities) and provide recommendations and guidelines to vulnerable entities found in its web application. however, choose to qualitatively assess impact and probability explicitly. ***For each term has been assign high, medium, or low*** vulnerability. A simple matrix is developed to estimate overall exposure. Vulnerability analysis is a series of activities undertaken to identify the weaknesses and holes to exploit security vulnerabilities. It helps to confirm the effectiveness of the security measures that have been analyzed. The methodology of vulnerability analysis includes three phases: test preparation, conducting test and test result analysis. Each of them involves a series of further steps and tasks. This report further illustrates how to apply this methodology to conduct ***vulnerability analysis on ten (10) sample governmental office web applications***, finally the result of the research shows all the possible number of Vulnerabilities rate and system weakness perspective attack of governmental office network asset vulnerability analysis finding results of both approaches based on ***vulnerability impact rate or risk level and system technology weakness or attack perspective*** by using black box testing.

Keywords: Vulnerability Analysis, Security Testing, Vulnerability Assessment, Penetration Testing, Web Application Penetration Testing.

Table of Contents

List of Acronyms

INSA:	Information Network Security Agency
METEC:	Metals and Engineering Corporation
MINT:	Minister of Innovation and Technology
ZAP:	Zed Attack Proxy
OWASP:	Open Web Application Security Project
VA:	Vulnerability Analysis
AUC:	African Union Commission
OSSTMM:	Open Source Security and Testing Methodology Manual
ISECOM:	Institute for Security and Open Methodologies
SANS:	System Admin, Audit, Network and Security
OS:	Operating system
FISMA:	Federal Information Security Management Act
ISAAF:	Information Systems Security Assessment Framework
NIST:	national institute of standards and technology
OISSG:	Open Information Systems Security Group
PTES:	the Penetration Testing Execution Standard
OISSG:	Open Information Systems Security Group
DNS:	Domain Name System
CVE:	common vulnerability Exposures
HTTP:	Hyper Text Transfer Protocol
DSL:	Digital subscriber line
SQL:	Structured Query Language
IT:	information technology
ICT:	Information and Communication Technology.
XSS:	Cross-site Scripting
SSL:	Secure Sockets Layer
TLS:	Transfer Layer Security
CMS:	content management system
CIA:	Confidentiality, Integrity and Availability
PHP:	Personal Home Page
XML:	extensible Markup Language
URL:	Uniform Resource Locator
APTEH:	Application Penetration Testing and Ethical Hacking
ECA:	Africa Economic Commission for Africa

List of Figures

List of Tables

CHAPTER ONE

INTRODUCTION

Network security is a growing field of concern for Ethiopian governmental offices and agencies. Information technology Security can protect a network by testing the network for potential threats, and continuous defense against malicious attacks. Network threats in today's age, are forever changing. Hackers with malicious intent are continually attempting to infiltrate networks to steal information cyber security now in the world dynamic change.

The significant of security analysis today's connected device pose challenge for cyber security professional uses computer network to access and store information its needs understand more security challenges and security analysis.in Ethiopian most governmental office From the security point of view a hardware system like PC, software and network infrastructure Weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) because the researcher have been observed from INSA'S annual auditing and evaluation report from 20 governmental office auditing serve 15 of governmental office vulnerable in case of weak information system.so they should be implementing effective cyber security measurement particularity challenge today because there are more device than people and attackers are becoming more innovation and connected internet that is the era of internet of things, so after vulnerability analysis the research has been done to understand and recommended the best practices, standard and bench marks of vulnerability tools. In Vulnerability Assessment and Penetration Testing Methodology Overview including the main steps of vulnerability analysis those are. Discovery: The penetrator performs information discovery via a wide range of techniques, Enumeration: the specific networks and systems are identified through discovery, Vulnerability Identification: The vulnerability identification step is

a very important phase in penetration testing. This allows the user to determine the weaknesses of the target system and where to launch the attacks. And Exploitation and launching of attacks: After the vulnerabilities are identified on the target system **[1]**.Vulnerability assessment tools generally work by attempting to automate scan a "footprint" analysis to determine what network services and software programs. In Information System Security Framework and Vulnerability Assessment for Ethiopian governmental office using Kali Linux has been used for penetration testing tools like OWASP Zed Attack Proxy (ZAP) for vulnerability scanning in security weaknesses **[2];** however after evaluating this research has been recommend the best counter measure to the existing vulnerability considering internal and external system.

The reason why to use vulnerability assessment tools, e.g., network scanners, host scanners, database scanners, web application scanners, is that to be effective, the tool needs to have a detailed knowledge of the targets it has been scan. A network scanner needs to know how to perform and interpret a network footprint analysis that involves first discovering all active nodes on the network, then scanning them to enumerate all of the available net- work services.

In Demystifying the Audit Process for Security Officers Sanjay There are many reasons to conduct an information security audit including: estimation of organizational preparedness, identification of vulnerable areas, benchmarking against standards and practices **[3].**

Basic knowledge

Vulnerability Analysis (VA) is the process of scanning the system or software or a network to find out the flaws and weakness in that. This also includes series of systematic measures used to review and prioritize security vulnerabilities in a network or communication system/ or any application service. Vulnerability Assessment helps businesses in the determination of security posture of the environment and the level of exposure to threats. The process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately and Network security is composed of hardware and software components designed to protect the data and information being processed on the network.

1.1 Vulnerability analysis Benchmark

In this research has been Reviewed vulnerability assessment tools currently available Understand the steps to take when benchmarking multiple items and determine acceptable measures when benchmarking vulnerability assessment tools Analyzing these domains has been provide a comprehensive understanding of how to conduct a successful benchmark of vulnerability assessment scanners against Cyber-Physical Systems .cyber security is a critical concern in society today. Key Result of my research indicate that both tools together can provide a comprehensive assessment of the vulnerabilities in network infrastructure and scientific instruments.in this vulnerability analysis Benchmarking the research has been follow some steps like Selecting and Scanning tool installation, scanning configuration, Scanning execution, Vulnerability report inspection and Vulnerability handling:

1.1.1 Penetration Testing

The art of exploiting weaknesses and vulnerabilities in networks, web applications, or people. This is different than just performing a vulnerability scan against web security. A penetration test takes the perspective of an outside intruder or an internal individual with malicious intent. This may not always involve technology. **There different types of penetration testing services.**

- **External Network Penetration Testing.** The network attack where access might be gained through internet-connected servers or network equipment by individuals outside of your organization who lack appropriate rights or credentials.
- **Internal Network Penetration Testing.** The companies mitigate risk due to internal threats against their corporate network. While external testing investigates avenues that remote hackers might use to enter networks, internal testing looks at ways employees or insiders might lead to a breach either through neglect, malice, or the accidental download of an application.
- **Application Penetration Testing.** Threats and vulnerabilities posed by the many internet-based applications in use throughout your enterprise. Conveniently accessed from any location worldwide and just as easily breached, web applications offer significant points of access.
- **Wireless Penetration Testing.** the advanced expertise in a range of wireless technologies, offering ethical hacking services to investigate and identify potential access points where hackers could enter your internal network
- **Social Engineering Penetration Testing.** This survey employees to see how well they understand your organization's information security policies and practices.

1.2 Statement of the problem

Today's state-of-the-art ***network security*** the reasons why because now a day cyber space becoming wide via the world and connected device however Ethiopia also weak cyber technology implementation compare with other country according to INSA's auditing report and new challenges arise alongside growth, and increasing technological exposure. Based on the 2013 Economic Report on Africa Economic Commission for Africa (ECA) and the African Union Commission (AUC), Africa is facing several Internet-related challenges in relation to security risk, intellectual property infringement and protection of personal data. Cybercriminals target people inside and outside their national boundaries and most African governments have neither the technical, nor the financial capacity to target and monitor electronic exchanges deemed sensitive for national security.in addition The European Commission's Digital Single Market Strategy and the advisory Scientific Advice Mechanism recognize cyber security as a core policy priority. The EU Cyber Security Strategy provides a policy framework for EU initiatives. But in Ethiopia government's doesn't exit nether policy or auditing service .In addition Vulnerability analysis use to computers, networks or applications for known weaknesses. In plain words, these scanners are used to discover the weaknesses of a given system. They are utilized in the identification and detection of vulnerabilities arising from within a network-based asset such as a firewall, router, web server, application server. Because security vulnerability analysis use are numerous, industry frameworks and best practice guidance typically include vulnerability assessments in their list of suggested measures Simply, a governmental organization cannot fully understand the security flaws, overall risk, and assets that are vulnerable to cyber security breaches. To stay understand and to counter surprise attacks, a thorough vulnerability analysis help to fix the unattended security issues. The research was interested because cyber space is wide in the world and connected with

devices so that this thesis discovers vulnerabilities before attack Ethiopia government's office network infrastructure and the problem describes about the degree of risk and attack vulnerability of governmental office asst. Most businesses are connected to the Internet and have implemented measures (policies, systems) to protect themselves from unauthorized access. *Generally this research statements of problem were* understand about.

- Security analysis and its vulnerability in case of web security assessment pinpoints and prioritizes security defects in server and client side.
- Understand about security analysis and address vulnerability impact rate or risk level and system technology weakness or attack perspective.
- vulnerability is utilized by an unauthorized individual to access government network resources, can be compromised, so address vulnerabilities before they can be utilized and aware vulnerability levels of our country network asset or web.
- Identify higher-risk vulnerabilities resulting from lower-risk vulnerabilities exploited in a particular way.

I have been challenged Penetration testing that is a security exercise where a cyber-security asked attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a web system's defenses which attackers could take advantage and ***enhance cyber security knowledge***.

1.3 Objectives

1.4.1 General objective

The main objective of this thesis to understand the governmental office web security analysis used different vulnerability scanner tools discover the security weakness within impact rate and put possible recommendation and countermeasures.

1.4.1 Specific objectives

- Understanding deferent network security scanning tools.
- Measure Ethiopian governmental offices web security.
- Understand Data gathering (reconnaissance) methodology in cyber security.
- Identify vulnerability of system in governmental website.
- Evaluate to the information technology use its web security.
- Analysis the status of the system how much it is secure.
- Decision of the vulnerability analysis finding in the web.
- Determine web vulnerability risk level High-Risk, Medium-Risk, or Low-Risk.

1.4 Methodology

In this research has been used dynamic technique of vulnerability analysis strategy because there differ standard in differ serve now mainly the research has been selected *Information Systems Security Assessment Framework (ISAAF),* The Open Source Security and Testing Methodology Manual (OSSTMM). And Application Penetration Testing and Ethical Hacking (APTEH) published by (System Admin, Audit, Network and Security) SANS Security company is the another methodology that we use through our documentation to do everything step by step follow like Reconnaissance, Network mapping, vulnerability identification and final reporting and recommendation [4].

1.5 Scope and limitation

1.5.1 Scope

The vulnerability scanning service covers all network infrastructures in the given internet address ranges from which responses were detected. For each machine detected, the services and characteristics of the machine are analyzed.

- Perform vulnerability scan to search for known vulnerabilities. Information regarding known vulnerabilities can be obtained from the vendors' security announcements.
- Discovered vulnerabilities External Vulnerability and Internal Vulnerability in network.
- To identify the gaps in the existing defense and finally recommended cyber security mitigation.
- Focused on federal governmental network infrastructure asset use black box test.

1.5.2 Limitation

The result of the research would be more comprehensive if it covers the entire governmental network infrastructure in Ethiopia. However, due to data limitation and time constraints the student researcher has forced to focus on main of federal governmental web and network infrastructure asset in addition ***coved-19 pandemic affected to internal or white box testing to communicate organization of system administrator***.

1.6 Contributions of the research

Vulnerability analysis is a method used to discover known vulnerabilities of computing systems available on a network. It helps to detect specific weak spots in application software or the operating system (OS), which could be used to crash the system or compromise it for undesired purposes. Classifies system hole in computers, networks and communications equipment and

predicts and recommend the effectiveness of countermeasures. The most Vulnerability analysis significances are.

- Identifying vulnerabilities and misconfigurations.
- Testing security controls and Identifying lack of security.
- Improves security policies and procedures develop cost-effective methods for implementing information security policies and procedures.
- Discover vulnerability, impact and recommend mitigation.
- Avoid vulnerability issues that the systems and Provide an appropriate level of security.
- Show Ethiopian governmental network system vulnerability levels.

The result of the research would be more comprehensive if it covers the entire governmental office network in Ethiopia. However, due to access limitation and time constraints, it is delimited to some sample governmental office in Addis Ababa the major information security resources and facilities and the office of IT staffs are sited. These staffs can provide the necessary information about the research better than other staffs who work at in office.

The finding is really the meat of the report. They were understood what the entire test was for. We were finding the vulnerability by different technique and methodology to rise out the weakness of the system different governmental network infrastructure .each finding should include the best practice vulnerability mitigation recommendation. The Expected outcome of this work is to identify the vulnerability of the network infrastructure and verify the implementation and performance of security systems. The audit determines whether the security systems safeguard assets and maintain the confidentiality, integrity and availability of information.

1.7 Organization of the rest of the report

In this research has been discovered a numbers of vulnerabilities in the organization's network asset that could potentially lead to the analysis sensitive information and financial losses and affect the organization's business reputation and organization with a report containing the list of vulnerabilities, mentioning their risk level (low, medium or high) and defining *impacts and counter measures recommendation* to reduce risks. Network vulnerability analysis is usually followed by penetration testing. There's no use in conducting penetration testing *before* the discovered vulnerabilities are patched, as the goal of penetration testing is not just trying to get into the network but also examining the network environment '*with a new set of eyes'* after the improvements are made. Vulnerabilities can be identified through vulnerability analysis however in this research has been applied different Testing technique include the following:

- Information Security test and evaluation (ST&E) procedures
- Use Penetration testing techniques
- Use automated vulnerability scanning tools.
- Analysis and Report the final result.

CHAPTER TWO

LITERATURE REVIEW

In This section is a review of all relevant research that impinges on my thesis. It is the work done by others that relates to what the research has been demonstrated with the current work. This is also where the literature related to methods that the research has been used in my current work should be introduced. This literature review is organized by first described the concepts related to vulnerability analysis and penetration testing that used different testing tools and methodologies are also reviewed. The vulnerability analysis focused on different government offices web applications and network device is reviewed to indicate the type of vulnerability and their impacts.

2.1 Network Security

Network and computer security is critical to the cyber activity health of every organization. Over the past few years, Internet-enabled business, or e-business, has drastically improved efficiency and revenue growth. E-business applications such as bank, supply-chain management, and remote access allow companies to streamline processes, lower operating costs, and increase customer satisfaction. However, as networks enable more and more applications and are available to more and more users, they become ever more vulnerable to a wider range of security threats. To combat those threats and ensure that governmental organization is not compromised, security technology must play a major role in today's networks. To protect governmental organization network assets: One of the primary goals of computer and network security vulnerability analysis is the information show that organization’s computers and networks security status. [17]

2.2 Network Vulnerability

In this paper review a network vulnerability analysis and a weakness of system or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach. Nonphysical network vulnerabilities these applications are consist of different network devices and computers and it is very important to protect these applications and devices from malicious hackers so that chances to exploit the vulnerabilities may reduce. [18] [5].

2.2.1 Vulnerability assessment (vulnerability analysis)

Vulnerability analysis is the process of identification of threats and weaknesses in IT security, however to solve the statement of the problem the research has been used Several Methods have been proposed but each has its own strengths and weaknesses. In this paper the researcher have been examine some of the popular methods. Several tools based on behavior modeling, fault trees, test & failure models provide host based analysis by checking logs, versions of system software and by monitoring performance metrics [19] [**8**].

2.2.2 Vulnerability Analysis Framework

In this paper state the methodologies developed for network security analysis the dynamics of network services and complexity of network connectivity can be represented with the traditional state machine approach. In fact all attacks or faults in a system cause the network to evolve along sequence of network states before they finally bring the network system to its strength. The vulnerability analysis architecture requires identification of a set of global measurement that could be associated with various faults Network components Network Services [19].

2.2.3 Vulnerability Analysis Methodology

The vulnerability analysis methodology provides the evaluator with explicit guidance on addressing to my research problem statement vulnerabilities analysis of Ethiopian Governmental

network asset. The current work to improve the comprehensiveness of the Vulnerability analysis in Black box network vulnerability testing metrics is characteristic parameters that represent attacks or faults. The research has been used these vulnerability metrics in our analysis approach to quantify the impact of the attacks and faults on a network service. [19] [**9**] [4].

2.2.4 Vulnerability scanning:

In this current work the research has been used deferent ***kali Linux*** vulnerability scanner tools it consists in discovering known security holes, flaws, software or techniques that take Black box network vulnerability testing. Most of vulnerability scanners rely on a local database that contains all the information required to check a system for security holes in services and ports, anomalies in packet construction, and potential paths to exploitable programs or scripts. When vulnerabilities are discovered, countermeasures should be applied in the system so as to solve the problem [20] [**12**] [**6**].

2.3 Scanning Tools

There are number of free network scanner tools in different scanning methods that have different strength and weaknesses, in this reconnaissance phase which are Identify active hosts and open ports, but some scanners provide additional information, such as target operating system, about the scanned hosts. However, activities like operating system fingerprinting are not foolproof, because system administrators can configure their firewalls to block certain ports and types of traffic and configure their systems to respond in nonstandard [21] [**10**] [**11**].

2.4 Steps of Penetration Test

In this research has been set a goal, after that the research has been reconnaissance the information on the system on which has been going to perform test. The research has been run the discovery by scanning the port and vulnerability assessment, analysis has been be performed on the basis of gathered information. A report has been be complied finally as evidence which includes vulnerability analysis and remedies on all the collected vulnerabilities and including the following steps of penetration testing.

A. ***Network Reconnaissance***: It refers to collect as much information as we can about target in prior to perform an attack.

B. ***Service Discovery***: It refers to identification of all the open as well as close ports and even for the known vulnerabilities on the target machine.

C. **Vulnerability Identification**: It can be identified and gained system level or even network level. From normal access hacker can even proceed with privilege escalation.

D. **Vulnerability report:** The concept of vulnerability analysis report is show a critical process that should be followed in any organizations as a way to weakness identify, assess and respond to new vulnerabilities before those vulnerabilities threat/attack [**22**]

2.5 Mapping the Application

The first step in the vulnerability analysis process of attacking an application is gathering and examining some key information about it to gain a better understanding of what you are up against. The mapping exercise begins by enumerating the application's content and functionality in order to understand what the application does and how it behaves. Much of this functionality is easy to

identify. This has been enabled you to identify the key attack surface that the application exposes and find exploitable vulnerabilities. [23] [**14**].

2.6 Threats in cyber security

Today our society, economy, and critical infrastructures day to day activity have become largely dependent on computer networks and information technology solutions. Cyber-attacks become more attractive and potentially more disastrous as our dependence on information technology increases. It is because cyber-attacks are cheaper, convenient and less risky than physical attacks. Cyber criminals only require a few expenses beyond a computer and an Internet connection. They are unconstrained by geography and distance. They are difficult to identity and prosecute due to anonymous nature of the Internet. Given that attacks against information technology systems are very attractive, it is expected that the number and sophistication of cyber-attacks has been keep growing however to solve this problem the current work recommended the best vulnerability analysis methodology and vulnerability report [24].

2.7.1 Exploiting existing vulnerabilities

- **Hardware** is the most privileged entity and has the most ability to manipulate a computing system. That potential to give attackers considerable flexibility and power to launch malicious security attacks if the hardware is compromised.
- **Network infrastructure and protocol vulnerabilities** The early network protocol was developed to support entirely different environment we have today in a much smaller scale and often does not work properly in many situations it is used today. Weaknesses in network protocols are complicated when both system administrators and users have limited knowledge of the networking infrastructure, so it is to need vulnerability analysis.

2.7.2 Cyber attacks.

Cyber Attacks are actions taken to harm a system or disrupt normal operations by exploiting vulnerabilities using various techniques and tools. Attackers launch attacks to achieve goals either for personal satisfaction or recompense. The measurement of the effort to be expended by an attacker, expressed in terms of their expertise, resources and motivation is called attack cost. Attack actors are people who are a threat to the digital world. They could be hackers, criminals, or even governments; however my current work statement of the problem covered to response cyber-attack before damage, Common cyber-attack types are:

- Physical attacks: This sort of attack tampers with hardware components. Due to the unattended and distributed nature of the Internets of thing.
- Reconnaissance attacks: unauthorized discovery and mapping of systems, services, or vulnerabilities.
- Denial-of-service: This kind of attack is an attempt to make a machine or network resource unavailable to its intended users.
- Access attacks: unauthorized persons gain access to networks or devices to which they have no right to access.
- Attacks on privacy: Privacy protection in Internet of things has become increasingly challenging due to large volumes of information easily available
- Cyber-crimes: The Internet and smart objects are used to exploit users and data for materialistic gain, such as intellectual property theft, identity theft, brand theft, and fraud
- Destructive attacks: Space is used to create large-scale disruption and destruction of life and property. Examples of destructive attacks are terrorism and revenge attacks [**25**].

2.7 Reporting

During Upon completion of vulnerability analysis, a report should be generated that identifies system, network, and organizational vulnerabilities and discovered vulnerabilities analysis, this deliverable is especially useful for summarizing of findings to manage, detailing findings and description of impact, recommendations, and tracking progress during the remediation process using necessary information of target:

Security testing results can be used in the following ways:

- As a reference point for corrective action
- In defining mitigation activities to address identified vulnerabilities
- As a benchmark for tracking an organization's progress in meeting security requirements
- To assess the implementation status of system security requirements To conduct cost/benefit analysis for improvements
- To system security to enhance other life cycle activities, such as risk assessments.

The report format can vary based on the standard type to meet reporting requirements the research has been used best practice format, such as those of Federal Information Security Management Act (FISMA). Security testing results should be documented. Because a report may have multiple audiences, ensure that all are appropriately addressed. Reports that has been remain within the organization can be tailored for the appropriate audiences, such as program management, information management, security engineers, configuration management, or technical staff. Internal reports should include test methodology, test results, analysis [26].

2.8 Review of Related work

In this research has been used external testing that refers to attacks on the organization's network asset perimeter using procedures performed from outside the organization's network infrastructures and web application. [4].

In The Approach of Auditing Network Security By Anantha Sayana discovers the basic vulnerabilities associated with a network can be describe in area Availability that control to ensure availability and reliability of a network infrastructure [5] .In Jai Narayan Vulnerability Assessment and Penetration Testing is a step by step process. Vulnerability assessment is scanning the system or software or a network to find out the weakness and loophole in the system that. Boundary condition vulnerability, Input validation vulnerability, Authentication Vulnerabilities, Configuration Weakness Vulnerabilities, and Exception Handling Vulnerabilities [**6**].In Kirandeep Kaur Penetration testing is a method of evaluating the security of a machine. Services are evaluated to identify weakness, vulnerabilities and the absence of patches, Identifying the security holes, firewall configuration and Wireless points. It includes internal penetration testing External Penetration testing [**7**].

Penetration Testing and Vulnerability analysis plays a vital for every kind of computer application. In computer networks and communications, our information use to travel out of computers so presence of vulnerabilities may compromise our whole networks to exploited [**8**] .in the Security Testing Methodologies Industry-wise, a number of security testing methodologies that aim to ensure that the penetration testing industry following a strict approach when performing assessments. By adopting these methodologies, it prevents common vulnerabilities, or steps, from being overlooked and gives clients the confidence that all aspects of the proposed target are tested during the assessment phase [**9**]

2.8.1 Summary of related work

Table 1: Summary of related work

author	**approach**	**tools**	**vulnerabilities identified**	**countermeasures**
Jai Narayan [**10**]	the process of vulnerability scanning	Nmap	Best security scanner and to find host discovery.	Closed unnecessary ports, miss configured firewalls.
SheetalBairwa, Bhawna Mewara [**11**]	Based on client server architecture that test is run on the server side.	Nessus	various vulnerabilities present in the remote host	patched the hole
Haftom Gebreziagbher [**12**]	Open source package	Kali Linux	Scanning and exploit	Patched the weakness
Anantha Sayana [**13**]	network architecture	Meltigo	Network architecture and sub domain	Monitoring external network
Nagendran K [**14**]	Web Application Penetration Testing	Nikto, W3af and Acunetix	Scanning security vulnerabilities	Report the vulnerability And block hole
Arul Louise Jennifer [**15**]	Discover vulnerabilities in web application.	UniScan	Web weaknesses scanners	Report the vulnerability And block
Shreya Goswami [**16**]	web applications scanner	Vega, Netsparker and Grabber	web applications scanner	Identify system hole and block

CHAPTER THREE

3.1 RESEARCH DESIGN AND METHODOLOGY

The first phase of the research was formulating the research problem the problem was initiated by personal interest to conduct a research on the area of Ethical hacking vulnerability analysis.

In this section has been also describe any experiments you may have run, it has been also discuss any testing methodologies and how these would be actually applied in research and discusses the strategies and the methodology of conducting vulnerability analysis. The methodology of vulnerability analysis includes three phases: testing preparation, information gathering, vulnerability analysis, and vulnerability report.

The research methodologies evaluated on four Ethiopian governmental office network securities. The vulnerability test on the same targets aims to provide testing security how to conduct the methodologies and to evaluate the effectiveness of the research. Since the research statement of the problem was already described detail at the chapter one problem statement section, the remaining methodologies used in this research has been be described below.

3.2 Vulnerability analysis standard and procedure

Standards for vulnerability analysis aimed to provide a basic outline and definition of the vulnerability analysis. Also to give an outline of the steps used for it, there are many standards to follow vulnerability analysis, so choosing one of them should be based on the goal of having the test. Currently various standards Technical vulnerability analysis using could be followed, such as:

- ISAAF (Information Systems Security Assessment Framework)
- OSSTMM (Open-Source Security Testing Methodology Manual)
- NIST SP 800-115(national institute of standards and technology)
- PTES (the Penetration Testing Execution Standard)
- OISSG (Open Information Systems Security Group)
- OWASP testing guide
- Manual testing
- SANS resource
- Web application security testing tools

In this my current work the research has been used the best methodology ISAAF (Information Systems Security Assessment Framework) standard which aimed to help the administrator to evaluate my application, system and network controls. The methodology solved the question, how it should be vulnerability analysis and what are the step/procedures to be followed. The main approach includes three phases and nine steps.

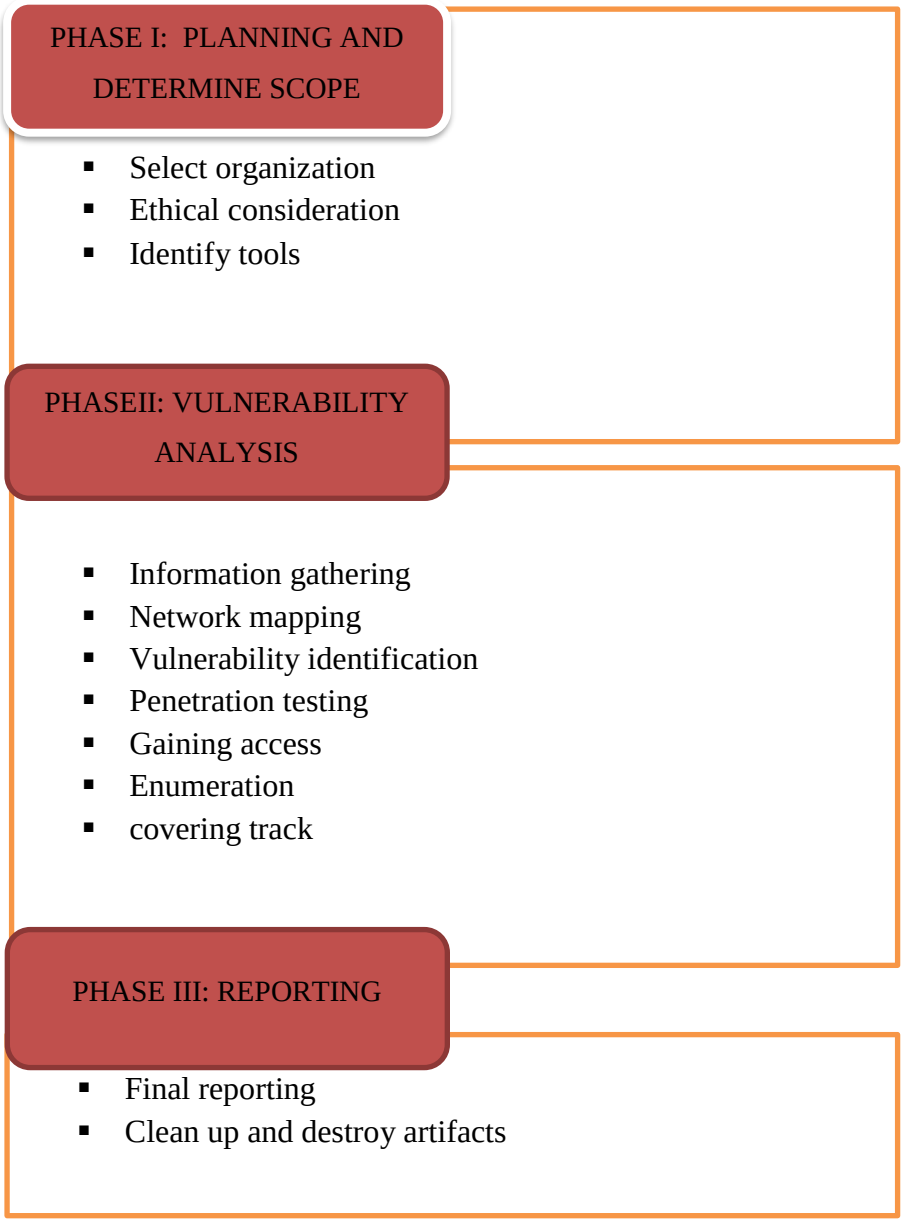

Figure 1: The Phases of Penetration Testing (ISSAF) Standard

3.2.1 Black box testing

Also known as a 'blind' test, this is one where the pen-tester is given no background information besides the name of the target company and an external test, the ethical hacker goes up against the company's external-facing technology, such as their website and external network servers. In some cases, the hacker may not even be allowed to enter the company's building. This can mean conducting the attack from a remote location or carrying out the test from a truck .however, in this research have been used this types of testing ***because coved-19 pandemic affected to internal or white box testing to communicate organization of system administrator***.

This testing approach focuses on the input that goes into the application software, and the output that is produced. The testing involve does not cover the inside details such as code, server logic, and development method that Test is performed from a user's point-of-view and not of the designer's.

3.3 Data type and source of data

The data for this research was gathered through the use of primary and secondary data sources. The primary data source involved through the use from electronic search Site: www.google.com,manually automated and vulnerability scanner tools generating result such as port scanners, ping tools, host vulnerability scanners, and network mappers.

3.4 General approach

The research methodology design Based on the objective of the research, the types of approach that use qualitative type of research approach, because the result of the vulnerability analysis

should be explained briefly the observational and document analysis that Appling different network security penetration testing activity.

3.5 Data collection

In This research requires selecting existing methodologies that are necessary for black box system vulnerability testing and used qualitative research methodology observational and document analysis Appling different network security penetration testing tools. Some Common data collection methods for in this research listed below.

- Search engine queries to gather information about the personnel, systems, or technologies of the client system.
- Domain name searches, WHOIS lookups, and reverse DNS to get subdomains.
- The Social Engineering to find out positions, technologies, email addresses
- Reconnaissance Internet foot-printing looking for email addresses, social accounts.
- open source Kali Linux penetration testing tools
- Data from related existing surveys and reports.

3.6 Target selection

Identification of Target When approaching a organization it is important to understand research concerned that in which organization To conduct. In this section research is necessary first to select specific sector in Ethiopia government offices so that it is possible take some Governmental sector and make vulnerability analysis by using vulnerability analysis benchmark. In addition to that, the sector should be one of the high assets values of the countries who have websites that can be accessed remotely and which are vulnerable. The sectors might be classified as financial sector, industry sector and infrastructure sector etc.

3.7 Tool Selection

Vulnerability testing can be executed by both manually and automatically. Now, the next task that we are going to do is, selecting automated web vulnerability scanner which helps to detect available vulnerabilities from the tested system. There are different both commercial and open source web vulnerable scanners that allows to detect vulnerabilities. Here the research has been used both of them and the commercial scanners have trial version. So by taking this trial as an advantage, the research has been done to test the selected system automatically. The tools that the research has been done to use for the testing are mainly categorize in to three:

- Online Web application testing tools
- Kali Linux preinstalled penetration-testing programs.
- Custom scripts for security testing

3.8 Sampling design

The research has been tried to describe something about Ethiopia governmental office web security in the first chapter. Though, here we are going to describe Ethiopia network security in some details. **From *http://www.ethiopia.gov.et/*** information in Ethiopia there are more than 70 federal government websites, both in federal and regional level. But, ***I have been discuses with INSA's auditing and evaluation director Mr desalegn W/geworgis the research sample focused on federal web security***, ***about 10 governmental websites*** are tested and their result is expressed in terms of table and chart. Here the research has been used the non-probability sampling technique to select the working websites. On this research has been worked the total number of sample size was 70 Governmental websites.

3.9 Data analysis

Data analysis believed necessary discover potential vulnerabilities on the network through the use of automated tools & scripts and through manual analysis reports and collecting of raw data, classification and tabulation was done by the researcher to make it ready for the analysis. All collected data was organized and processed separately for each item in a way appropriate to answer the questions in the problem statement. This discovers by using statistical tool like charts, and verbal descriptions were used to present the data.

Generally in case of the complicated and lengthy processes, vulnerability analysis is required to mention every step to make sure that analysis all the information in all the phase of testing. Along with the methodology, the research has been discovered about the systems and tools, scanning results, vulnerability analysis, details of my findings, etc.

CHAPTER FOUR

DETAIL VULNERABILITY ANAYSIS FINDINGS

Multiple security weaknesses were discovered during the vulnerability analysis Ethiopian governmental web applications and that vulnerability also listed as in hosts vulnerabilities based on Likelihood and Impact. Under this section the security audit finding on the application are listed in the tables below. The vulnerabilities are discovered from testing and using the methodologies explained above chapter. For this research has been selected ***as a sample 10 governmental office website from around 70 website in the portal http://www.ethiopia.gov.et/.***

In the previous research part a simplified view was given on methods how the research had been executed and procedures are clearly defined. It could be seen that some of these procedures have overlap; from this overlap the general vulnerability analysis and testing methods that the research has been 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, in this section of the research, 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 in this research sample *governmental office website listed below in table.*

Table 2: sample governmental office website listed

Target No	Name of mister office	URL name
1.	Ministry of Health	http://www.moh.gov.et/ejcc
2.	Ethiopian Institute of Agricultural Research	http://www.eiar.gov.et/
3.	Ethiopian Ministry Of Revenues	http://www.mor.gov.et/
4.	Federal Ethics and Anti-Corruption Commission	http://www.feac.gov.et/
5.	Ethiopian Public Health Institute	https://www.ephi.gov.et/
6.	Prime Minister office	https://pmo.gov.et/
7.	Federal Cooperative Agency	http://fca.gov.et/
8.	Ethiopian management institute	http://www.emi.gov.et/
9.	Ethiopia's Investment Commission	https://www.investethiopia.gov.et/
10.	Ethiopian Government Electronic Services Portal	https://evisa.gov.et

4.2 Application security

Application security is defined the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.

Application security describes security measures at the application level that aim to prevent data or information within the app from being stolen or hijacked used specific hole of system. It encompasses the security considerations that happen during application development, design, configuration, and use technology but it also involves systems and approaches to protect apps after they get deployed or hosted. Application security may include hardware, software, and procedures that identify or minimize security vulnerabilities. A router that prevents anyone from viewing a computer's IP address from the Internet is a form of hardware application security.

***Why application security is important*?** The reason for this is because hackers are going after apps with their attacks more today than in the past. Application security testing can reveal weaknesses at the application level, helping to prevent these attacks.

There are Different types of application security features today include.

- Authentication
- Authorization
- Encryption
- Application security testing
- Logging privilege

4.3 Reconnaissance

In this section shows experiment, that network reconnaissance gathering information about a network, such as the network structure, applications and services, and vulnerabilities. All the information about the targets (devices, application, network and services) using both technical (***use kali Linux operating system)*** and nontechnical (observations and documentations) methods carried out. The following table summarizes show both technical and non-technical methods: From the vulnerability analysis testing of network infrastructure and basic network information, the application systems which includes the technology used is obtained. The governmental website or target listed in this chapter above in the table three, in this reconnaissance phase does not include each targets name and URL for purposed of governmental office security privacy based on rule of engagement agree with INSA if necessary demo and screenshot evidence open for advisor and examiner in which except published, so the research has been seen when you ask any practical evidence any time.

Table 3: remote code execution vulnerability

No.	1 (target one)
Vulnerability Name	Drupal 8.6.4 remote code execution vulnerability exists
Vulnerability Description	Vulnerability has been discovered in the Drupal core module, which could allow for remote code execution. The remote code execution vulnerability exists due to a lack of proper data sanitization in some fields, which could result in a website being completely compromised.
Risk Level	**High**
Impact	An attacker who is able to execute such a flaw is usually able to execute commands with the privileges of the programming language or the web server.

Table 4:bootstrap@3.2.0 vulnerabilities

No.	1.2
Vulnerability Name	bootstrap@3.2.0 vulnerabilities Cross-site Scripting (XSS)
Vulnerability Description	A cross-site scripting attack occurs when the attacker tricks a legitimate web-based application or site to accept a request as originating from a trusted source.
Risk Level	**High**
Impact	The following environments are susceptible to an XSS attack: ▪ Web servers ▪ Application servers and Web application environments

Table 5: Apache HTTP Server < 2.4.8 Multiple Vulnerabilities.

No.	1.3
Vulnerability Name	Apache HTTP Server < 2.4.8 Multiple Vulnerabilities
Vulnerability Description	A denial-of-service vulnerability in the mod_log_config module that can be triggered due to insufficient user-input sanitation when logging a cookie with an unassigned value .
Risk Level	**High**
Impact	An attacker can A denial-of-service vulnerability.

Table 6: Unrestricted File Upload vulnerability

No.	1.4
Vulnerability Name	Unrestricted File Upload
Vulnerability Description	Although file uploading restriction is applied. (i.e. the upload page is only allows to upload photo extension files such as JPEG,JPG,PNG,BMP,GIF and PDF), it failed to check the content file as it is only checks the file extensions, so that it is possible to bypass this restriction. Using upload malicious file to the server.
Risk Level	**High**
Impact	A malicious user can :- ✓ Upload a file using malicious path or name which overwrites critical file or personal data that other user's access.

Table 7: Brute force attacks in admin page

No.	1.5 (the origin IP)
Vulnerability Name	Brute force attacks in admin page
Vulnerability Description	It occurs when a bad actor attempts a large amount of combinations on a target. These attacks frequently involve multiple attempts on account passwords with the hopes that one of them has been be valid. It's a bit like trying all of the possible combinations on a padlock
Risk Level	High
Impact	Uses previously-known password-username pairs, trying them against multiple websites. Exploits the fact that many users have the same username and password across different systems

Table 8: apache http server 2.2.2 vulnerabilities outdate

No.	**2 (target two)**
Vulnerability Name	apache http server 2.2.2 vulnerabilities outdate
Vulnerability Description	Errors exist in the bundled expat library that may allow an attacker to crash the server when a buffer is over- read when parsing an XML document. (CVE-2009-3720 and CVE-2009-3560)
Risk Level	**Medium**
Impact	The remote web server may be affected by several issues Successful exploitation allows malicious users to cause a denial of service.

Table 9: Joomla! Core 2.5.x Security Bypass (2.5.0 - 2.5.24)

No.	2.1
Vulnerability Name	Joomla! Core 2.5.x Security Bypass (2.5.0 - 2.5.24)
Vulnerability Description	Joomla! Core is prone to security bypass vulnerability. Exploiting this issue may allow attackers to perform otherwise restricted actions and subsequently bypass intended access restrictions via vectors involving authentication.
Risk Level	**Medium**
Impact	allow remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via the HTTP User-Agent header

Table 10: Privilege Escalation

No.	2.2
Vulnerability Name	**Privilege Escalation**
Vulnerability Description	Privilege escalation means a user receives privileges they are not entitled to. These privileges can be used to delete files, view private information.
Risk Level	**High**
Impact	Accessing the database as the administrator can do such as Employee and user's data can be access delete and update using the query.

Table 11: Vulnerability NamePHP 5.5.x < 5.5.21 Multiple Vulnerabilities

No.	2.3
Vulnerability Name	PHP 5.5.x < 5.5.21 version Multiple Vulnerabilities
Vulnerability Description	The remote web server uses PHP version that is affected by multiple vulnerabilities in the system.
Risk Level	**High**
Impact	A remote attacker, using a specially crafted PHP file, can exploit this vulnerability to disclose memory contents, cause a denial of service, or possibly execute code.

Table 12: Apache Http Server 2.4.18 Bypass Restriction Vulnerability.

No.	3 (Target three)
Vulnerability Name	Apache Http Server 2.4.18 Bypass Restriction Vulnerability.
Vulnerability Description	The Apache HTTP Server 2.4.18 through 2.4.20 which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation.
Risk Level	**Medium**
Impact	The vulnerability allows a remote attacker to bypass security restrictions on the target system.

Table 13:bootstrap@3.2.0 Cross-site Scripting (XSS)

No.	3.1
Vulnerability Name	bootstrap@3.2.0 Cross-site Scripting (XSS)
Vulnerability Description	Bootstrap is a popular front-end framework Affected versions of this package are vulnerable to Cross-site Scripting (XSS)
Risk Level	**Medium**
Impact	vulnerable to Cross-site Scripting (XSS)

Table 14: Unrestricted File Upload

No.	3.2
Vulnerability Name	Unrestricted File Upload
Vulnerability Description	Is vulnerable to Unrestricted File Upload. The upload page shows only warning messages but it accepts unhallowed file extensions when click submitting button. Then attacker have been upload malicious file to the server
Risk Level	**High**
Impact	Access to internal data and server information and control the whole server.

Table 15: Joomla! CMS versions 3.2.0 through 3.4.1

No.	3.3
Vulnerability Name	Joomla! CMS versions 3.2.0 through 3.4.1
Vulnerability Description	Joomla! Core is prone to security bypass vulnerability. Exploiting this issue may allow Lack of CSRF checks potentially enabled uploading malicious code.
Risk Level	**Medium**
Impact	Allows remote attackers to have unspecified impact via unknown vectors.

Table 16: Apache (win32) 2.4.9 Multiple Vulnerabilities

No.	4 (target four)
Vulnerability Name	Apache (win32) 2.4.9 Multiple Vulnerabilities
Vulnerability Description	In Apache HTTP Server up to 2.4. 9 (Web Server). This affects some unknown processing of the component mod status. The manipulation with an unknown input leads to a memory corruption vulnerability (Heap-Based)
Risk Level	**Medium**
Impact	The vulnerability allows a remote attacker to perform denial of service attack.

Table 17: PHP 5.5.x < 5.5.21 Multiple Vulnerabilities

No.	4.1
Vulnerability Name	PHP 5.5.x < 5.5.21 Multiple Vulnerabilities
Vulnerability Description	The remote web server uses a version of PHP that is affected by multiple vulnerabilities.
Risk Level	**High**
Impact	A remote attacker, using a specially crafted PHP file, can exploit this vulnerability to disclose memory contents, cause a denial of service, or possibly execute code.

Table 18: Joomla! 1.7.0 < 3.8.8 Multiple Vulnerabilities

No.	4.2
Vulnerability Name	Joomla! 1.7.0 < 3.8.8 Multiple Vulnerabilities
Vulnerability Description	According to its self-reported version, the instance of Joomla! Running on the remote web server is 1.7.0 affected by multiple vulnerabilities. Missing token checks in the image actions of common templates causes CSRF vulnerabilities.
Risk Level	High
Impact	Incorrect Access Control in the SQL field type of common fields allows access for non-super-admin users.

Table 19:jquery@1.12.4 vulnerabilities (cross-site scripting attack)

No.	5 (target five)
Vulnerability Name	jquery@1.12.4 vulnerabilities(cross-site scripting attack)
Vulnerability Description	A cross-site scripting attack occurs when the attacker tricks a legitimate web-based application or site to accept a request as originating from a trusted source The attacker injects code that appears safe, but is then rewritten and modified by the browser, while parsing the markup.
Risk Level	**High**
Impact	The following environments are susceptible to an XSS attack: ✓ Web servers ✓ Application servers and Web application environments

Table 20: SSL medium strength cipher suites supported (sweet32) vulnerability

No.	5.1
Vulnerability Name	SSL medium strength cipher suites supported (sweet32) vulnerability
Vulnerability Description	The remote host supports the use of SSL ciphers that offer medium strength encryption. The vulnerability by plugin 42873 SSL Medium Strength Cipher Suites Supported (SWEET32) is an attack on 64-bit block ciphers in TLS or SSL ciphers that offer medium strength encryption, which regard as those with key lengths at least 56 bits and less than 112 bits.
Risk Level	**Medium**
Impact	Limit the length of TLS sessions with a 64-bit cipher, which could be done with TLS renegotiation or closing and starting a new connection.

Table 21: joomla 3.6 5 PHPMailer remote code execution vulnerability

No.	5.2
Vulnerability Name	joomla 3.6 5 PHPMailer remote code execution vulnerability
Vulnerability Description	Joomla 3.6.5 Core suffers from remote code execution vulnerability. And versions. Exploit automated. It is possible to specify a list of sites.
Risk Level	**High**
Impact	Remote Code Execution in third-party PHPMailer library

Table 22: jquery 1.2 vulnerabilities Cross-site scripting

No.	6 (target six)
Vulnerability Name	*jquery 1.2 vulnerabilities Cross-site scripting*
Vulnerability Description	The vulnerability exists due to insufficient sanitization of user-supplied data in the regex operation in "jQuery.html Prefilter
Risk Level	**Low**
Impact	The disclosed vulnerability allows a remote attacker to perform cross-site scripting (XSS) attacks.

Table 23:bootstrap@4.1.3 Cross-site Scripting (XSS)

No.	6 .1
Vulnerability Name	bootstrap@4.1.3 Cross-site Scripting (XSS)
Target	https://pmo.gov.et/
Vulnerability Description	A cross-site scripting attack occurs when the attacker tricks a legitimate web-based application or site to accept a request as originating from a trusted source.
Risk Level	**Low**
Impact	The following environments are susceptible to an XSS attack: ✓ Web servers ✓ Application servers ✓ Web application environments

Table 24: brute force router login page

No.	6 .2 (origin IP)
Vulnerability Name	brute force router login page
Vulnerability Description	A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered.
Risk Level	**High**
Impact	Gaining privilege to access admin page Uses previously-known password-username pairs, trying them against multiple websites. username and password across different systems

Table 25: PRTG network monitor default password

No.	6 .3
Vulnerability Name	PRTG network monitor default password
Vulnerability Description	Default Credential vulnerability is a type of vulnerability that is most commonly found to affect the devices like modems, routers, digital cameras, and other devices having some pre-set (default) administrative credentials to access all configuration settings.
Risk Level	**High**
Impact	Gaining privilege to access admin page Uses previously-known password-username pairs, trying them against multiple websites. Exploits the fact that many users have the same username and password across different systems

Table 26: Open port 135,139,445 and 49155

No.	7 (target seven):
Vulnerability Name	Open port 135,139,445 and 49155
Vulnerability Description	An open port is an attack surface. The daemon that is listing on a port could be vulnerable to a buffer overflow, or another remotely exploitable vulnerability.
Risk Level	**High**
Impact	Exploiting vulnerabilities in services and applications running on open ports.

Table 27: PHP 5.5.x < 5.5.21 Multiple Vulnerabilities

No.	7.1
Vulnerability Name	PHP 5.5.x < 5.5.21 Multiple Vulnerabilities
Vulnerability Description	The remote web server uses a version of PHP that is affected by multiple vulnerabilities.
Risk Level	**High**
Impact	A remote attacker, using a specially crafted PHP file, can exploit this vulnerability to disclose memory contents, cause a denial of service, or possibly execute code. (CVE-2014-9427)

Table 28: brute force attack DSL router via 197.156.101.225

No.	7.2
Vulnerability Name	brute force attack DSL router via 197.156.101.225
Vulnerability Description	A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered.
Risk Level	**High**
Impact	To Gaining privilege to access admin page Uses previously-known password-username pairs, trying them against multiple websites. Exploits the fact that many users have the same username and password across different systems

Table 29: Registration page Unrestricted File Upload

No.	8 (target eight)
Vulnerability Name	Registration page Unrestricted File Upload
Vulnerability Description	Although file uploading restriction is applied. (i.e. the upload page is only allows to upload photo extension files such as JPEG,JPG,PNG,BMP,GIF and PDF), it failed to check the content file as it is only checks the file extensions, so that it is possible to bypass this restriction.
Risk Level	**High**
Impact	A malicious user can:-Upload a file using malicious path or name which overwrites critical file or personal data that other user's access.

Table 30: Joomla! 1.5 Vulnerabilities cross-site scripting

No.	8.1
Vulnerability Name	Joomla! 1.5 Vulnerabilities cross-site scripting
Vulnerability Description	According to its self-reported version, the instance of Joomla! Running on the remote web server is 1.5.0 affected by multiple vulnerabilities.
Risk Level	High
Impact	Incorrect Access Control in the SQL field type of common fields allows access for non-super-admin users.

Table 31: sql database phpmyadmin page password brute force

No.	8.2
Vulnerability Name	sql database phpmyadmin page password brute force
Vulnerability Description	Password privilege A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered.
Risk Level	**High**
Impact	To Gaining privilege to access phpmyadmin page Uses previously-known password-username pairs, trying them against multiple websites. Exploits the fact that many users have the same username and password across different systems

Table 32: brute force attack DSL router

No.	8.3
Vulnerability Name	brute force attack DSL router
Vulnerability Description	A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered.
Risk Level	**High**
Impact	To Gaining privilege to access DSL admin page Uses previously-known password-username pairs, trying them against multiple websites. Exploits the fact that many users have the same username and password across different systems

Table 33:Joomla! 3.6 outdate Multiple Vulnerabilities

No.	9(target nine):
Vulnerability Name	Joomla! 3.6 outdate Multiple Vulnerabilities
Vulnerability Description	According to its self-reported version, the instance of Joomla! Running on the remote web server is 1.6.0 affected by multiple vulnerabilities. Missing token checks in the image actions of common templates causes CSRF vulnerabilities.
Risk Level	High
Impact	The SQL field type of common fields allows access.

Table 34:bootstrap@3.2.0 Cross-site Scripting (XSS)

No.	9.1
Vulnerability Name	bootstrap@3.2.0 Cross-site Scripting (XSS)
Vulnerability Description	Bootstrap is a popular front-end framework for faster and easier web development. Affected versions of this package are vulnerable to Cross-site Scripting (XSS)
Risk Level	**Medium**
Impact	vulnerable to Cross-site Scripting (XSS)

Table 35: brute force attack Ooma telo device

No.	9.2
Vulnerability Name	brute force attack Ooma telo device
Vulnerability Description	A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered.
Risk Level	**High**
Impact	To Gaining privilege to access Ooma telo admin page Uses previously-known password-username pairs, trying them against multiple websites. Exploits the fact that many users have the same username and password across different systems

Table 36: Bootstrap 3.3.5 (framework vulnerability)

No.	10(target ten) :
Vulnerability Name	Bootstrap 3.3.5 (framework vulnerability)
Vulnerability Description	Affected versions of this package are vulnerable to Cross-Site Scripting (XSS) attacks via the data-target attribute.
Risk Level	**Medium**
Impact	E-visa prone to XSS.

Table 37: Unrestricted File Upload

No.	10.1
Vulnerability Name	Unrestricted File Upload
Vulnerability Description	Although file uploading restriction is applied. (i.e. the upload page is only allows to upload photo extension files such as JPEG,JPG,PNG,BMP,GIF and PDF), it failed to check the content file as it is only checks the file extensions.
Risk Level	**High**
Impact	A malicious user can: Upload a file using malicious path or name which overwrites critical file or personal data that other user's access.

Table 38: User validation in registration form

No.	10.2
Vulnerability Name	User validation in registration form
Vulnerability Description	In registration form not validates or incorrectly validates input that can accept any characters in input field.
Risk Level	**Medium**
Impact	E-visa prone to integer denial of service vulnerabilities

Table 39: TLS version 1.0 protocol detection

No.	**10.3**
Vulnerability Name	TLS version 1.0 protocol detection
Vulnerability Description	TLS 1.0 is vulnerable to man-in-the-middle attacks, risking the integrity and authentication of data sent between a website and a browser.
Risk Level	**Medium**
Impact	The remote service encrypts traffic using an older version of TLS.

Table 40: Brute force attacks in ZTE DSL router admin page

No.	10.4
Vulnerability Name	Brute force attacks in ZTE DSL router admin page
Vulnerability Description	Attempts a large amount of combinations on a target to involve multiple attempts on account passwords with the hopes that one of them has been be valid.
Risk Level	**High**
Impact	Uses previously-known password-username pairs, trying them against multiple websites.

4.4 Risk Calculation

Throughout the document, each risk calculated has been listed in a table under this section as a finding and categorized as a **High-Risk**, **Medium-Risk**, or **Low-Risk**. Based one Common ***Vulnerabilities and Exposures (CVE***) system provides a reference-method for publicly known information-security vulnerabilities and exposures) that is a catalog of known security threats according to the CVE website and Chief information officer (CIO) reports directly to the chief executive officer analysis. The research has been used the following Risk calculation formula to calculate the risks.

Risk= Likelihood*impact

This means that the total amount of risk exposure is the probability of an unfortunate event occurring, multiplied by the potential impact or damage incurred by the event. If you put a value on the impact, then you can value the risk and in a simple way compare one risk factor to another.

High risk: - these findings identify conditions that could directly result in the compromise of the web application. These include getting access to the website by resetting user accounts of different user levels i.e. normal user up to administrator user level. This has been allowed an attacker to perform tasks on administrator user level.

Medium risk: - these findings identify conditions that do not immediately or directly result in the compromise but do provide a capability to gain control on the web application. These includes the session cookie does not expires after the users click on log out. These has been allowed attackers to login and perform tasks using the cookie once they steal it from legitimate user.

Low risk: - these findings identify conditions that provide information that could be used in combination with other information to gain insight into how to compromise the web application. These include vulnerabilities like information disclosure and displaying server banners.

4.5 Summary and Vulnerabilities analysis finding

The discovered of vulnerabilities analysis had been classified in two based on vulnerability impact rate or risk level and system technology weakness or attack vulnerable that covers compromise Confidentiality, Integrity and Availability (CIA) on services and applications over the website. The following chart shows the number of Vulnerabilities rate and system weakness

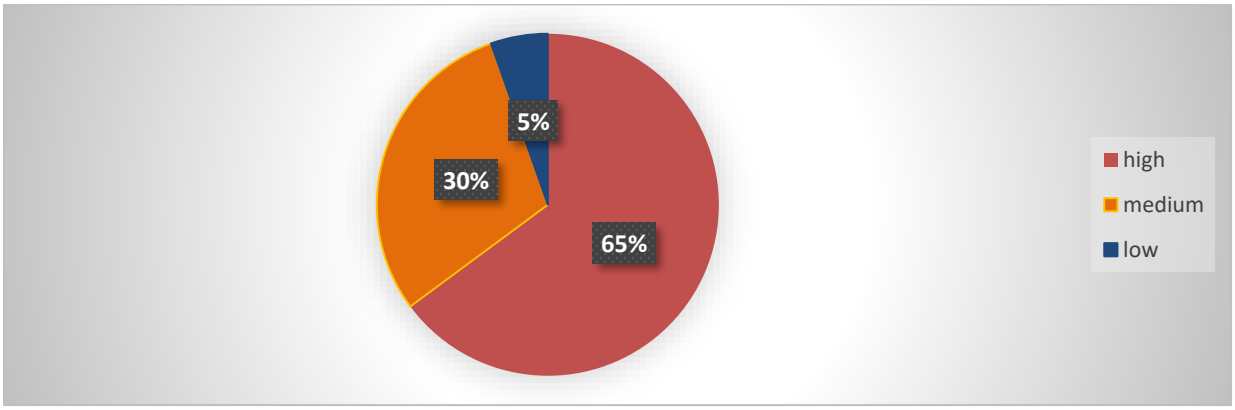

Figure 2: impact rate or risk level

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

Table 41: risk level analysis

No	Risk level	Number of vulnerability	Percentage
1	High impact vulnerabilities	24	65%
2	Medium impact vulnerabilities	11	30%
3	Low impact vulnerabilities	2	5%

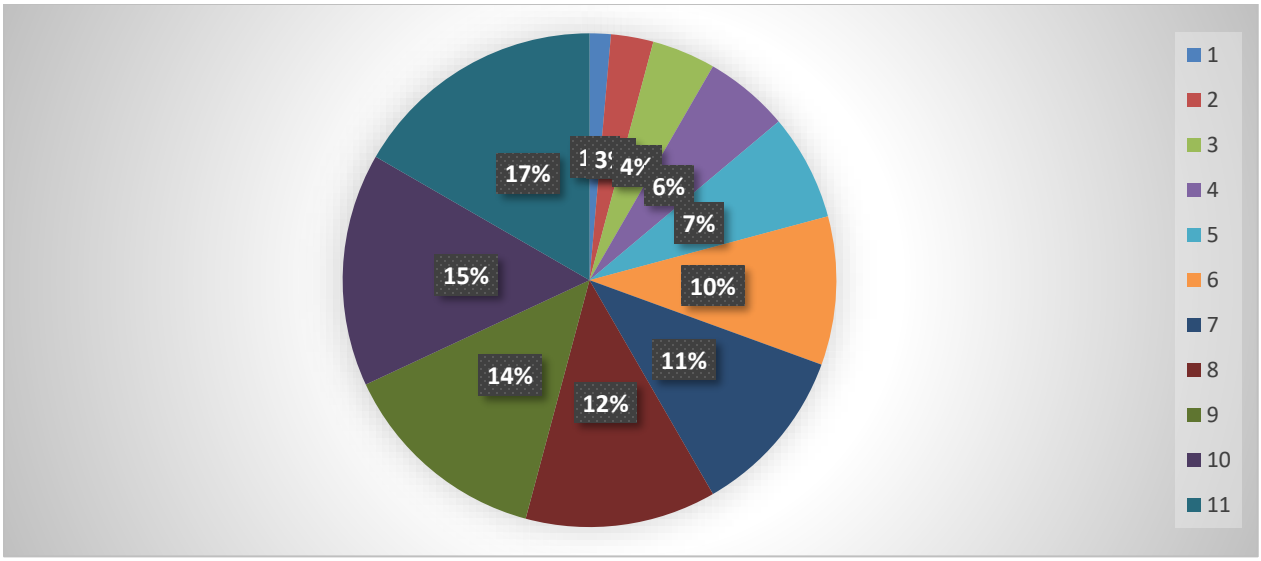

Figure 3: website vulnerability based on system technology weakness

The system technology weakness or attack vulnerable (web technology and attack perspective rate) discovered on the services and applications are described as follows.

Table 42: Numbers of threat

Target No	threat	numbers of threats
1	contain management system (CMS)	6
2	bootstrap vulnerability	5
3	apache server vulnerability	3
4	file upload restriction vulnerability	3
5	Brute force attack vulnerability	4
7	jquery version vulnerability	2
8	TLS version vulnerability	2
9	network open port	1
10	SQL database vulnerability	1
11	user validation vulnerability	1
12	PHP version multiple vulnerability	2

- In this research generally as shown that above ***pie chart and table*** has been summarized all vulnerability analysis finding results of both approaches based on ***vulnerability impact rate or risk level and system technology weakness or attack perspective.***

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

In this Chapter, the conclusion and the recommendations for future works of this research is given The Chapter is organized in two sections. The conclusion of the research and the recommendations for future works are presented. Vulnerability analysis is a comprehensive method to identify the Penetration testing in a system. It offers benefits such as prevention of financial loss; compliance to industry regulators, customers and shareholders; preserving corporate image; proactive elimination of identified risks before damage. The research has been chosen black box penetration testing, depending on the specific objectives to be achieved. The security of a website vulnerability analysis adapting any pen-test methodology does not necessarily provide a complete picture of the vulnerability analysis process, which execute pen-test methodology.

The research had carried out by identifying:

- The sampling technique to be used
- The procedures that should be applied the test methodology and
- Active devices, services and applications have been tested.
- Vulnerability analysis techniques
- The kali Linux tools to be used for the tests.
- Security metrics to be used to perform risk analysis

Vulnerabilities are identified in this research shows that the network system and all devices 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

impacted was proposed only for the discovered vulnerabilities. Vulnerability analysis and scanning to search known vulnerabilities on Ethiopian governmental office hosts and web applications based on low, medium and high Risk factors are considered. All the available vulnerabilities had been identified and verified, these include in this research:

- Application and Database vulnerabilities
- Enumeration of Identified vulnerabilities
- Verification of the identified vulnerabilities
- Firewall and Router vulnerabilities
- Hosts vulnerabilities analysis.
- Vulnerability analysis can be an efficient and cost-effective strategy to protect the organization's systems against attacks; however vulnerability analysis should be follow a comprehensive methodology format to present the system test results via governmental office network asset. One of the most important parts of the test analysis phase is the preparation of remediation which includes all necessary corrective measures for the identified vulnerabilities.

5.2 Recommendations

The aim of this research is to have a vulnerability analysis web security and governmental ICT infrastructures 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 website for the vulnerabilities that could have enormous impact on governmental office network infrastructure. Finally in this research has been recommended like to put forward our strong remind to origination:

The governmental office network asset needs to have strong IT policy for:

- Upgrading IOSs of Networking devices on a regular basis
- Web Technology updating
- IT service management
- Logical Access Control
- Internet Acceptable use policy
- Use strong password policy
- Web Back end and front end security implement
- All the vulnerabilities reported by this research and reconfigure the affected application the soonest possible with the proposed consider the risk impact.

As summary of recommendation the vulnerability should be fixed as soon as possible especially the high vulnerability. And the application uses third party frameworks and libraries that should have to be updated and patched on the regular basis, but currently, the websites which has multiple types of vulnerabilities. In this research has been done only focused on the some governmental office website target network asset, the other office network infrastructure is needs to be vulnerability analysis for the future work.

References

[1] Ankita Gupta Anamika Saini, "Blue Eyes Technology," *International Journal of Engineering Research and General Science*, vol. 4, no. Issue 1, January-February, 2016 , p. 549, , 2016.

[2] Haftom Gebreziagbher, "Information System Security Framework and Vulnerability Assessment for Ethiopian Higher Educational," *International Journal of Information Technology*, vol. Volume 2, Issue 12, no. ISSN (2413-2950) –, pp. 16-17, December 31, 2018.

[3] Sanjay Goel1, "Managing Information Security: Demystifying the Audit Process for Security Officers," in *Managing Information Security: Demystifying the Audit Process for Security Officers*, Washington University at Albany, SUNY, 2002, p. 3.

[4] SURESH KUMAR, "Ethical Hacking and Penetration Testing Strategies," *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)*, vol. Volume 11 Issue 2 , no. ISSN: 0976-1353, p. 22, NOVEMBER 2014.

[5] By S. Anantha Sayana, "Approach to Auditing Network Security," *Information Systems Audit and Control Association*, vol. V OLUME 5, p. 2, 2003.

[6] b,*, BM Mehtre Jai Narayan Goela, "Vulnerability Assessment & Penetration Testing as a Cyber Defence," in *3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)* , School of Computer and Information Sciences, University of Hyderabad, Hyderabad 500046, India, Procedia Computer Science 57 (2015).

[7] Kirandeep Kaur Kavita, "ulnerability Assessment and Penetration Testing," *nternational Journal of Engineering Trends and Technology*, vol. Volume4, no. Issue3, 2013.

[8] Chandresh Parekh Nidhi Vora*1, "Vulnerability Assessment and Penetration Testing in Web," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. Volume 2, no. Issue 6 | , pp. 731-735, 2017 IJSRCSEIT.

[9] SensePost (Pty), "Security Assessment Methodologies," South, 1999/004700/07.

[10] Jai Narayan, "Vulnerability Assessment and Penetration Testing in Web," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 2, no. 6, p. 734, 2017.

[11] Sheetal Bairwa1, "VULNERABILITY SCANNERS: A PROACTIVE," *International Journal on Computational Sciences & Applications (IJCSA)* , vol. Vol.4, no. No.1, pp. 113-120, February 2014.

[12] Haftom Gebreziagbher, "Information System Security Framework and Vulnerability Assessment for Ethiopian Higher Educational," *International Journal of Information Technology*, vol. Volume 2, no. , Issue 12, p. 16, December 31, 2018.

[13] By S. Anantha Sayana, "Approach to Auditing Network Security," *I NFORMATION S YSTEMS C ONTROL J OURNAL*, vol. V OLUME 5, , 2003.

[14] Adithyan A, Chethana R, Camillus P, Bala Sri Varshini K B Nagendran K, "Web Application Penetration Testing," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 10, no. 2278-3075, p. 130, August 2019.

[15] R. Senthil Kumaran2 Arul Louise Jennifer.A1, "Development of Vulnerability Scanner," *International Research Journal of Engineering and Technology (IRJET)*, vol. 05, no. 07, p. 1280, July 2018.

[16] Shreya Goswami, "Web Application Vulnerabilities Scanners and Their Application," *https://indiancybersecuritysolutions.com/*, 24-08-2018.

[17] Rahul Pareek, "NETWORK SECURITY: AN APPROACH TOWARDS SECURE COMPUTING ," *Journal of Global Research in Computer Science* , vol. Volume 2, no. 2229-371x, July 2011.

[18] Nadeem Ahmad, "Analysis of Network Security Threats," *Electrical Engineering* , no. MEE10:76, pp. 26-32, Sep 2010.

[19] JayaPrakash, Ramkishore, Salim Hariri Guangzhi Qu, "A Framework for Network Vulnerability Analysis," p. 2.

[20] Quatre Camins, "http://www.salle.url.edu/GRSI 10 de 7 de 2009).," *New Challenges in Detection and Management of*, de 7 2009.

[21] Susan Wade, and John T. Michalski Cynthia K. Veitch, "Cyber Security Assessment Tools and Methodologies for the Evaluation of Secure Network," Digital Instrumentation & Control Branch Washington, DC 20555-000, Washington, Cyber Security Assessment Tools and Methodologies for

[22] Muhammad Zulkifl Hasan, Muhammad Taimoor Aamer Chughtai Muhammad Zunnurain Hussain, "Penetration Testing In System Administration," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 06, no. 06, p. 276, JUNE 2017.

[23] Inc. John Wiley & Sons, *The Web Application Hacker's Handbook*. Indianapolis: The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition, 2011.

[24] Surya Nepal Julian Jang-Jaccard, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences 80 (2014) 973–993*, p. 974, August 2013.

[25] Mohamed Abomhara and Geir M. Køien, "Cyber Security and the Internet of Things:Vulnerabilities, Threats, Intruders," *Department of Information and Communication Technology*, vol. Publication 22 May 2015, p. 75, 4 September 2014.

[26] NIST Special Publication 800-115, "Technical Guide to Information Security Testing," *Recommendations of the National*, no. MD 20899-8930 , p. 8, September 2008.

Appendix I: Interview Question

1. Why perform a vulnerability analysis?
2. What type of hosted environment do you require to security testing?
3. What type of test do you require?
4. What is the “target” of the vulnerability analysis applied?
5. What type of tools is used?
6. What is the primary purpose of vulnerability analysis?
7. What are the goals of conducting a vulnerability analysis exercise?
8. What are the three types of vulnerability analysis methodologies?
9. What is Black-Box Testing?
10. What is the advantage of vulnerability analysis for governmental office?