Network Scanning & Vulnerability Assessment with Report Generation

Thesis · May 2014

CITATIONS
9

READS
43,211

1 author:

Nikita Jhala
Nirma University
1 PUBLICATION **9** CITATIONS

SEE PROFILE

Network Scanning & Vulnerability Assessment with Report Generation

By

Nikita Y Jhala

12MCEI12

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AHMEDABAD-382481

MAY 2014

Network Scanning & Vulnerability Assessment with Report Generation

Major Project

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Computer Science and Engineering

(Information & Network Security)

By

Nikita Y Jhala

(12MCEI12)

Guided By

Dr. Sanjay Garg

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AHMEDABAD-382481

MAY 2014

Certificate

This is to certify that the Major Project Report entitled "**Network Scanning & Vulnerability Assessment with Report Generation**" submitted by **Ms. Nikita Y Jhala (Roll No: 12MCEI12)**, towards the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering of Nirma University, Ahmedabad is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Dr. A.V. Ravi Kumar
External Guide,
Scientist SF,
Head (Computer Center),
IPR Gandhinagar.

Prof. Sharada Valiveti
Associate Professor,
Coordinator M.Tech - CSE(INS),
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Sanjay Garg
Internal Guide,
Professor and Head,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr K Kotecha
Director,
Institute of Technology,
Nirma University, Ahmedabad

Undertaking for Originality of the Work

I, **Nikita Y Jhala**, Roll. No. **12MCEI12**, give undertaking that the Major Project entitled "**Network Scanning & Vulnerability Assessment with Report Generation**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science & Engineering** of Nirma University, Ahmedabad, is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

_____

Signature of Student

Date:

Place:

Endorsed by

Dr. Sanjay Garg

(Signature of Guide)

Acknowledgments

The masters dissertation constitutes a stupendous task for an individual which requires the cooperation of many persons associated in research activities, directly or indirectly.
First of all, I take this privilege to express my heart-felt sense of gratitude and indebtedness to my external guide **Dr. Ravi A V Kumar**,Scientist SF, Head of Computer Center, Institute for Plasma Research, Gandhinagar. I would like to express that inspite of his most busy schedule in number of important assignments, he has remained prompt enough to provide his excellent and satisfactory comments vetting and honing my study to a significant extent.
I owe my gratitude to my internal guide, **Dr. Sanjay Garg**, Hon'ble Head of Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad, for his valuable comments, suggestions and access to his precious time.
I also acknowledge with deep gratitude the valuable help and special attention from all scientists of Institute for Plasma Research. From beginning to the end, they have been persistent source of guidance, valuable suggestion and encouragement.
It gives me immense pleasure in expressing thanks to **Prof. Sharada Valiveti**, PG INS - Coordinator, Computer Science Department, Institute of Technology, Nirma University, Ahmedabad for for an exceptional support and continual encouragement.
A special thank you is expressed wholeheartedly to **Dr K Kotecha**, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation he has extended throughout course of this work.
It gives me an immense pleasure to thank **Institute for Plasma Research, Ahmedabad** for providing basic infrastructure and healthy research environment. I would also thank all faculty members of **Computer Engineering Department, Nirma University, Ahmedabad** for their support towards the project work.
Throughout the preparation of the study my parents, Dr. Y C Zala & Mrs. Devyani Zala and my brother Vikrant Jhala, shared my concerns and anxieties. I can't adequately express my appreciation for this in words. I must thank them for giving me the environment to study, opportunities and potential to succeed. And also my I express my profound regards to my friends, for their consistent support and love .

-Nikita Y Jhala

12MCEI12

Abstract

Network scanning and vulnerability testing relies on tools and processes to scan the network and its devices for vulnerabilities.This aids in refining any organization's security policy due to identification of vulnerabilities, and guarantees that the security measures taken actually gives the protection that the organization expects and requires. Administrator needs to perform vulnerability scan periodically which helps them to uncover shortcomings of network security that can lead to device or information being compromised or destroyed by exploits.

Different implementations & tools of network scanning have distinctive proficiency and have different kinds of outputs. These outputs are typically heterogeneous which makes the further analysis a challenging task. In this dissertation, two basic open source scanners are considered NMAP & OpenVAS. We show how to incorporate this two scanners into a decently outlined GUI and give reliable information.

On the basis of impediments of NMAP and OpenVAS, another tool is developed which holds best of both devices alongside overcoming few drawbacks. Network scanner created under this dissertation performs scanning over the network identifying the active hosts and conjecture the OS of the remote hosts and installed programs into the remote hosts. Apart identifying the active hosts it could find open ports and list the services which are running in the host. Further vulnerabilities scanning is performed by comparing the information obtained from a network scan to a database of vulnerability signatures to produce a list of vulnerabilities that are presumably present in the network. Along with performing network scanning and vulnerability assessment, auto-scan mechanism is also added in new tool to test device when they are compromised. In this dissertation, features of new tool is explored. In other words, network mapping, vulnerabilities and configuration faults in network are shown in various formats. Also, an easy approach is defined to reduce the scan duration of vulnerability.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

As time passes, the world is becoming more connected due to internet and new networking technology. Due to open nature of Internet, security of network has hold attention. With the development of new technologies, organization is now moving its business functions to public network, and thus a huge amount of personal, commercial and organization's information are available on networking infrastructures worldwide. Thus a set of precautions are taken to ensure the data cannot be compromised or inaccessible to unauthorized person. Network access in unauthorized by an outside hacker or a disgruntled employee can intentionally harm or destruct exclusive information which adversely influences organization benefit, and upset the proficiency to contend in business. In this manner, Network security is happening to incredible essentialness due to intellectual property that could be gained through the web with some effort. Network security measures includes scanning and vulnerability analysis along with penetration testing.

Network scanning is fundamental for gathering information about the real state of computer systems or networks. It is a system for identification of active hosts on a network, either with the end goal of security assessment of network. Vulnerability Assessment is a systematic analysis of security status of Information systems. Both techniques are the most comprehensive service for auditing, penetration testing, reporting and patching for any organization's network.

1.1 Project profile

1.1.1 Problem statement

Identify internal and external threats by vulnerability assessment using network vulnerability scanner. Develop a web-based tool designed to detect weaknesses in computers, computer systems, networks.

The research at hand recognizes the importance of network security and specifically that of current vulnerability scanners. It is aimed principally at making a contribution towards enhancing vulnerability assessment process by combining tools and reducing administrative burden.

1.1.2 Objectives

- To produce a comprehensive view of all operating systems and services running and available on the network.
- Detect misconfigured devices in network such as misconfigured web server, firewall etc.
- To detect critical vulnerabilities such as vulnerable web servers in the network.

Tools & technology:

Tools & technology used: PHP, MySql, NMAP, OpenVAS

Testing Environment: IPR network

1.2 Motivation

A "computer system" is significantly more than hardware and software. It incorporates the policies and procedures of organization under which that hardware/software is utilized. Security holes can emerge from numerous ranges. When attacker breaks into a computing system, he takes advantage of lapses in procedures, technology, or management (or some combination of those factors), allowing unauthorized access or actions. The precise failure of the controls is termed a vulnerability or security flaw. And mistreatment of that failure to violate the security policy is termed exploiting the vulnerability.

Thus,a mechanism is required which can fulfill following objectives:

- Protection of network devices.
- Reduce the vulnerability of applications and end-systems originating from the network.
- Protect information throughout transmission over the network.

This mechanism is called "Network Security" which takes measures to reduce the susceptibility of a network to threats. To ensure network security,numerous open-source as well as commercial products are available.

1.2.0.1 Need of network security

The purpose of Network Security in an organization will be more clear by identifying the reasons for any Corporate Networks being vulnerable:-

- Complexity: More imperfections and unintended access points in vast, complex networks.
- Familiarity: Utilizing regular, well-known codes, software, operating systems, and/or hardware builds the likelihood an attacker has or can discover the knowledge and tools to exploit the flaw.
- Connectivity: More physical connections, privileges, ports, protocols, and services increment vulnerability.
- Password management flaws: The computer user uses weak passwords that could be uncovered by brute force. The users store the password on the computer where a program can access it. Users reuses same passwords between many programs and websites.
- Fundamental operating system design flaws: The operating system designer chooses to enforce sub-optimal policies on user/program management. For example operating systems with policies such as default permit grant every program and every user full access to the entire computer. This operating system flaw allows viruses and malware to execute commands on behalf of the administrator.

- Internet Website Browsing: Some internet websites may have harmful spywares that are installed automatically on the computer when visited. This spyware collects personal information and send them to third party.
- Software bugs: The programmer attaches an exploitable bug in a software program. The software bug may open backdoor from computer system and allow an attacker to misuse an application.
- Unchecked user input

The survey [11], conducted by Kaspersky's own Global Emergency Response Team, highlighted returning Malware as a common complaint shared by many customers. Kaspersky's team found that while it's anti-virus software can remove viruses and malware effectively, it managed to reinfect the machines by exploiting common network vulnerabilities. The greatest slip-up is to overlook network share access rights answerable for

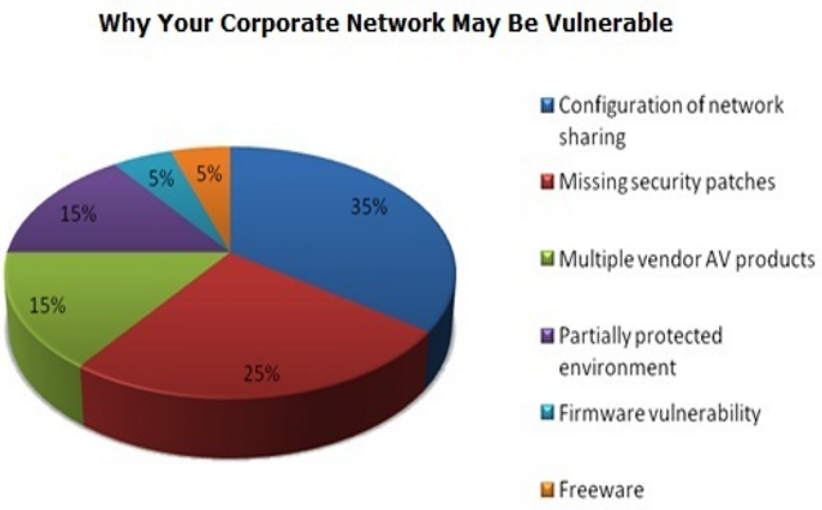


Figure 1.1: Kaspersky's survey

35% of incidents. In such a case there may be open sharing with access rights configured as "full access" to everyone on an network device such as internal file server e.g., a shared public document workspace where all documents are stored.

A network with just a single missing patch might be put at genuine danger. Also this is a typical issue seen for the most part in little to medium organizations with end-users numbering less than 500. These organizations either do not have enough expertise or ignores patching completely. As such, this mistake is answerable for 25% of occurrences.

Utilization of different vendor security solutions (15% of occurrences) may prompt a circumstance where it is tricky to alleviate malware ambushes. This may happen if one of the vendors does not react quick enough to attacks. Postpones in reactions may raced to days, weeks or even months. Throughout this time the result of an alternate vendor might locate and uproot vulnerability, yet just in its part of the network and attack can happen from the unprotected side. A partially protected environment (15% of incidents) is where an security solution is installed on part of the network, leaving different assets unprotected.

Firmware vulnerability (5% of incidents) may be misused by attackers if security administrator neglect to to monitor hardware devices, such as routers, firewalls and other network machines, to check whether they need fixing.

What's more an alternate generally rare slip-up (likewise 5% of incidents) is to accept that product downloaded from the Web is dependably splendidly sound programming.

Thus, network scanner tools can lessen the weakness of End-Systems to threats from external and internal entities by displaying list of vulnerabilities. But, using single tool cannot give accurate status of end-system which is explained further in literature survey.Thus, a combination of such tools can enhance the vulnerability report of network.

1.3 Scope of the work

The scope of this dissertation is better understood by the following requirements of organization. My goal is fulfill these requirements and give well-designed GUI and consistent data structure results.

Goal :

- **Check device configuration**
- **Vulnerability assessment of network**. The VA can be done internally and externally.
- **Autoscan**

Features of end-product :

1. Port Scanning and identification of the services
2. Vulnerabilities scanning

3. Exploiting services for known vulnerabilities
4. Password Cracking/Brute force
5. Provision to add remote servers in the software
6. Log Generation for reviewing and Generating Final report
7. Complete documentation of the software developed.

1.4 Organization of thesis

Following this introduction,Chapter 2 presents background knowledge of domain and overview of papers referred. It includes literature survey of previous work to date in the domains of network scanning,vulnerability assessment that is relevant to the work presented in the remainder of the thesis.

Chapter 3 proposes an approach to be followed based on issues and conclusion found in literature survey. It describes project plan, implementation approach and testing methods.

Chapter 4 give details about architecture and usage of tool and developed.

Chapter 5 presents some test cases and their results. It gives proof of how this tool can resolve issues discussed in Chapter 2.

Chapter 6 concludes thesis by discussing limitation of this tool and what future enhancement can be achieved.

Chapter 2

Literature Survey

Connections with different networks, for example, open internet give helpful channels through which attacker can bargain internal end-systems. Moreover, inner network clients can deliberately or unknowingly undermine the network and its end-systems through their movements. If there is possibility that one of the internal device on the network is compromised, it can turn into a risk to whatever is left of the network. Thus the internet as well as intranet provide convenient channels through which attacker (external/internal) can compromise end-systems So, Network security plays an essential role in an organization.

2.1 Network security

Network security counters both external and internal threats with a full suite of security shields to deliver dangers to the network. These protections incorporate the following:

- Physical and environmental protections to ensure network devices.
- Technical controls inside the network infrastructure to decrease its vulnerability to security threats.
- Controls applied within life-cycle courses of action to utmost the vulnerability of the network infrastructure to security threats.
- Information security operations to detect, react to, and recover from security incidents.

Network security controls threats from outside networks basically through protections conveyed at outer network interfaces. Inside the network security perimeter, protections

that are intended to detect, react to, and recover from attacks control threats from insiders and give in-depth defense against outer dangers.

Network security is based on specific principles and concepts that are related to asset protection. First of all, lets get familiar with common terms and their definitions related to asset protection:-

Asset : *An asset is anything of worth to an organization*[1]. By knowing which assets are needed to be protected, what is their value, location and exposure, an effective time, effort, and money can be spend in securing those assets.

Vulnerability : *Vulnerability might be seen as a flaw or weakness in the application which allows an attacker to cause undesirable operations or gain unauthorized access*[1]. Vicinity of vulnerability represents a risk to the user of the application as it may lead to sensitive information. Example: Buffer Overflow.

Threat : *It is any potential danger to assets*[1]. Example:Virus

Risk : *A risk is the probability that a specific threat using a particular attack will misuse a specific vulnerability of a system that brings about an undesirable consequence*[1].

Attack : *A set of actions that attempts to violate the security policies of a system*[1]. Example: Brute Force

Exploit : *A sequence of command or data chunk whose aim is to take benefit of a flaw or vulnerability in an application*[1].

Note:If a vulnerability exists but there is no threat toward that vulnerability, than technically there is no risk.

At the point when planning/evaluating/auditing network security, a network administrator must be aware of the following:

- The threats (or possible attacks) which could trade off security
- The associated risk factor of the threats (that is, how relevant those threats are for a particular system)
- The expense to actualize the correct security countermeasures for a threat
- An expense versus profit dissection to figure out if it is advantageous to execute the security countermeasures

Now, lets get familiar with concepts related to Network Security in this thesis:

1. Network scanning
2. Vulnerability assessment
3. Penetration testing

2.1.1 Network scanning

Network scanning or enumeration is a computer program used to retrieve usernames, hostnames, shares and services of networked computers. Network scanning, which can likewise be said as Network Security Scanner, is a complete networking utilities bundle that incorporates an extensive variety of tools for network monitoring, network security auditing, vulnerability auditing and more.
Fundamentally it comprises of six modules:

IP scan :

IP scanner tool used to test whether a specific host is reachable over a network[2]. It is furthermore used to individual test the network interface card of the device, or for speed test. The work of ping is done by sending ICMP - echo request packets to the target and listening for ICMP - echo response. The round trip time is measured by ping, it moreover records any packet lost and prints when finished a measurable rundown of the echo response packets retrieved, the minimum, mean, max and in some versions the standard deviation of the round trip time.

Host scanning :

It is the ability of scanning over the network and recognize the live hosts and conjecture the OS of the remote host with installed programs into the remote hosts is called Host Discovery[2].

Port scanner :

It is a piece of software intended to search a network for open ports[2]. This is for the most part utilized by administrators for checking the security of their networks. In TCP/IP protocol stack, host and host services are alluded in this system utilizing two parts: an address and a port number. The unique and usable port numbers that are accessible are 65536. Just constrained extent of numbers are utilized by most administrations; when the service becomes critical enough these numbers will be inevitably gotten assigned by the IANA.

Nslookup :

Nslookup is a computer program used in Windows and UNIX to inquire Domain Name System (DNS) servers to find DNS details, including IP addresses of a particular computer, MX records for a domain and the NS servers of a domain. The "name server lookup" is the representation of nslookup[2]

Traceroute :

To retrieve the route taken by packets across an IP network in computer network the tool used is Traceroute[2]. Around an given host to gather data about network infrastructure and IP ranges , analyzers uses traceroute. It gives data about network architecture by mapping out the path taken by packets. For network troubleshooting frequently utilized tool is traceroute. To identify the path taken on the network to reach a particular destination it allows the user showing a list of routers traversed. This aides in routing problems or firewalls that may blocks access to a site. It gives list of routers traversed which recognizes the path undertaken the network to reach a specific destination which it permits the user. This aides in routing problems or firewalls that may blocks access.

Vulnerability Auditing :

For scanning vulnerable hosts, each known vulnerable script will attempt to exploit the targeted service. The fundamental point to test a host for defenseless scripts and endeavors including Operating framework, administration, firewall, Remote Procedure Call and remote organization vulnerabilities. The fundamental point is to test a host for vulnerable scripts and exploits for OS, service, firewall, Remote Procedure Call and remote administration vulnerabilities.

Anyway this module is not further illustrated here as it is covered in next concept.

2.1.2 Vulnerability assessment

Vulnerability assessment return information concerning potential security chances that permit IT staff to view the network the way a potential hacker may, unmistakably seeing the potential roads denial of service attacks or gaining information through packet sniffing. Vulnerability scanners often prioritize the weaknesses they discover, assigning different values to represent the potential damage a hacker could cause within a network by exploiting a specific weakness. This allows network administrators to prioritize repair work by indicating which nodes present the greatest security risks.
Here following concepts of vulnerability assessment is discussed:

- Where vulnerability can be found i.e. area of vulnerabilities?
- What are the type of vulnerabilities found?
- How this vulnerability is categorized i.e. vulnerability domains?
- Types of tools to perform vulnerability assessment
- Limitations of vulnerability assessment

2.1.2.1 Areas of vulnerabilities

At the point when evaluating an organization's or platform's risk, there are area ranges of vulnerability [4]. These area are described here. Security mechanisms are the methods and technologies that might be conveyed inside every area to accomplish the security policy objectives. The security polices will control the level of protection and security mechanisms implemented within each area.

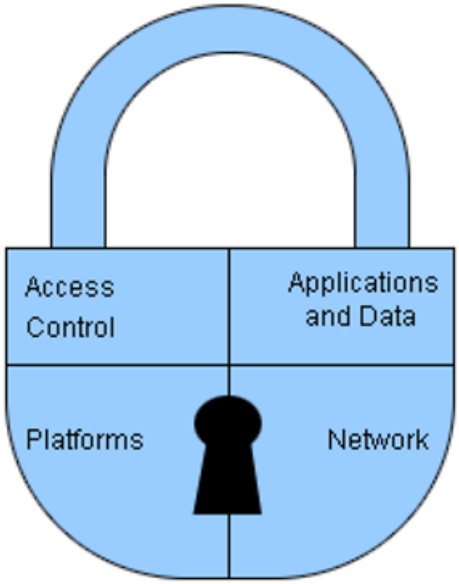


Figure 2.1: Areas of vulnerability

Access Control : *Access control is the procedure by which users are recognized and allowed privileges to information, resources and systems.*[4] Controlling how privileges are conceded and how resources are accessed is discriminating to ensuring private and confidential information from unauthorized users. The access control mechanism ought to record and timestamp all communications and transactions with the goal that they might be examined for security breaches and misuse.

Application and Data Protection : It includes tending to security concerns connected with the operating system, the application programs and the data. The objective is to empower better application and data availability, decrease exposure to data loss and to keep up integrity of the applications and data information.

Platforms Protection ; Platform protection is revolved around tending to physical attacks on the client hardware. The dangers incorporate hardware tampering, theft, or destruction, and data tampering, disclosure, or destruction.

Network Protection-Selected area for this dissertation : Network-based protection is implemented to address both **attacks attempted across a network** as well as **attacks against the networking protocols**. Network-based protection is executed to address both **attacks attempted over a network** and **attacks against the networking protocols**. Network-based attacks attempt to compro-

mise a system through flaws in the internet protocol standard. These attacks are ordinarily used to get access to systems, applications and data. These attacks can additionally be utilized to cause a "denial of service" failure that might avert users for accessing network assets. The network attack is typically the entrance point for the following level of attack on the client and/or network.

2.1.2.2 Vulnerability types

Normally, there are four types[5] of Vulnerability:

- Hardware vulnerability- It includes vulnerability cause by physical devices-adding, removing, flooding, Traffic interrupting, physical attacks etc.
- Software vulnerability- It include software based vulnerability generated by software Deletion, modification under this logic bombs, trapdoor, Trojan horse, information leaks and Virus are come.
- Data vulnerability-It includes data security by using confidentiality i.e. unauthorized disclosure of a data. For more valuable data communication in the system it is important to predict data from loss or from hacking by hacking. So, mostly we use encryption mechanism for secure data transmission. Data vulnerability consists of data loss, unauthorized access, or data hack by hackers.
- Web-based vulnerability- Web applications are the most common way to make services and data available on the Internet. Unluckily, with the greater number and complexity of these applications, there are increase in the number and complexity of vulnerabilities

2.1.2.3 Vulnerability domains

Every vulnerability is mapped to a vulnerability category:[6]. This includes vulnerabilities, potential vulnerabilities and information gathered checks. There is a one-to-one association between a vulnerability and a vulnerability category. When a vulnerability matches multiple categories [7], the service determines which category is the best match and assigns the vulnerability to that category.

BACK DOORS AND TROJAN HORSES	BRUTE FORCE ATTACK	CGI	DATABASE	DNS AND BIND
E-COMMERCE	FILE TRANSFER PROTOCOL	FINGER	FIREWALL	GENERAL REMOTE SERVICES
HARDWARE	INFORMATION (NIS, YP, WHOIS)	INFORMATION GATHERING	MAIL SERVICES	NEWS SERVER
NFS	PROXY	RPC	SMB / NETBIOS	SMTP AND MAIL SERVER
SNMP	TCP/IP	WEB SERVER	WINDOWS	X-WINDOW

Figure 2.2: Vulnerability Domains

2.1.2.4 Types of vulnerability assessment scanner

There are two types of VA scanners [3]:

Active Scanners :

Active scanners send probes to the network's nodes, inspecting the responses they get to evaluate whether a particular node represents a feeble point inside the network. A network administrator can additionally utilize an active scanner to recreate a attack on the network, revealing shortcomings a potential hacker might spot, or examine a node following an attack to determine how a hacker breached broke security. Active scanners can make a move to self-rulingly resolve security issues, for example, obstructing a possibly perilous IP address.

Passive Scanners :

Passive scanners distinguish the active operating systems, applications and ports all around a network, monitoring activity to focus the network's vulnerabilities. Be that as it may, while passive scanners can give data about shortcomings, they can't make a move to resolution security issues. These scanners can check the current software and patch versions on networked devices, showing which devices are using software that exhibits a potential entryway for hackers or trojan attacks, and reference this data against open databases containing lists of current patches. A network administrator can set passive scanners to run constantly or to work at specified interim.

2.1.2.5 Limitations of VA

There are few limitation[8] of vulnerability assessment process which is discussed over here.

While vulnerability scanners can aids network security tasks, they can't supplant the expertise of trained staff. Scanners are equipped for returning false-positives, demonstrating

a shortcoming where none exists, and false-negatives, in which the scanner disregards a security risk. Qualified personnel need to precisely check the information their scanners come back to discover incorrect results.

The second issue zone is authentication. Actually when they are properly configured, they recognize vulnerabilities for which signatures are defined. While anonymous (unauthenticated) filtering can provide for some benefit, failure to leverage authenticated scanning drastically diminishes scanner viability.

A third key issue is the scanner's failure to work with custom applications. CVE-based, known vulnerabilities are simply a little subset of general assault surfaces. Security checks may exist for the most well known applications and operating systems facilitated inside network, yet shouldn't something be said in regards to the custom applications that have developed in-house or outsourced to outsiders? There are no CVEs for custom applications.

Next issue is most vulnerability scanning tools can distinguish purposes of shortcoming, however they can't suspect complex attack plans. While vulnerability scanners ordinarily recognize and cover issues that might be used as the initial point of entry, they are restricted in recognizing the complex avenues an attacker could take to compromise your network.

Finally, vulnerability scanning also takes up a considerable amount of bandwidth, potentially slowing the network's performance.

2.1.2.6 Comparison between network scanning, vulnerability assessment and penetration testing

Network Scanning comprises the network utilities. It doesn't actually represent hole in network but the consequence of vulnerability or attack.

A vulnerability assessment is the methodology of identifying and quantifying vulnerabilities in network. It is an in-depth assessment of network posture, demonstrating shortcomings and giving the suitable mitigation techniques needed to either take out those shortcomings or lessen them to an adequate level of risk. To do this, most vulnerability assessments take after these general steps[12]:

1. Cataloging resources and assets in network

2. Assigning quantifiable worth and vitality to the resources

3. Identifying the vulnerabilities or potential dangers to every resource

4. Mitigating or wiping out the most genuine vulnerabilities for the most valuable resources

Then again, *a penetration testing simulates the actions of an external and/or internal attacker that expects to break the security of the organization.* Using numerous tools and techniques, the penetration tester attempts to exploit critical systems and get access to delicate information. Depending upon the degree, a pen test can stretch past the network to incorporate social engineering attacks or physical security tests.

The fundamental difference in approach between a vulnerability assessment and penetration test. A vulnerability assessment addresses the inquiry: "What are our weaknesses and how do we fix them?" A penetration test basically addresses the inquiries: "Can someone break-in and what can they attain?".

A vulnerability assessment attempts to enhance security act and create a more develop, incorporated security program, in as much as a pen test is just a depiction of security program's adequacy. In light of its approach, a vulnerability assessment is going to yield altogether more regard for most attempts than a pen test.

2.2 Related work

There are various tools available in market today. This tools are widely used as they are open source and give best results.

- Network mapping with **NMAP**
- Vulnerability assessment with **OpenVAS**

In this section, only overview of this tool and shortcums of this tools are discussed so as to get better idea why a new tool needs to developed. Features and usage of this tools are discussed in next chapter.

2.2.1 Network Mapper-NMAP

NMAP ("Network Mapper") is a free & open source utility for network discovery and security auditing. [13] Many systems and network administrators moreover feel that it significant for errands, for example, network inventory, managing service upgrade schedules, and monitoring host or service uptime. NMAP utilizes raw IP packets as a part of novel approaches to figure out what hosts are accessible on the network, what services (application name and version) those hosts offered, what operating systems (and OS versions) they are running, what kind of packet filters/firewalls are being used, and many different aspects. It was planned to rapidly scan large networks, however works fine against single hosts. NMAP runs on all major computer operating systems. Notwithstanding the excellent charge line NMAP executable, the NMAP suite incorporates a propelled GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping). Overview of NMAP is given in figure 2.3.

Advantages of NMAP:

- Unlimited IP scanning.
- Easy to setup and use.
- Fast Scans

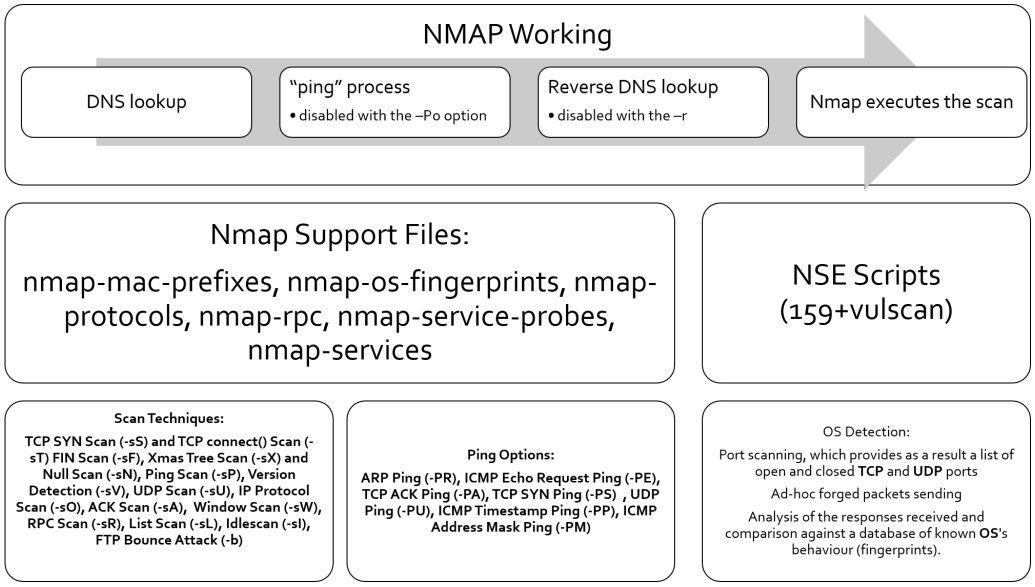


Figure 2.3: Overview of NMAP

Disadvantage of NMAP:

In the already 'saturated' market of vulnerability scanners, NMAP probably won't be receiving the necessary development attention needed.

2.2.2 OpenVAS

the Open Vulnerability Assessment System (OpenVAS) is a skeleton of several tools as and services offering a far reaching and influential vulnerability scanning and vulnerability management solution.[16] This security scanner is went hand in hand with a day by day overhauled feed of Network Vulnerability Tests (Nvts), in excess of 30,000 in aggregate (as of April 2013). OpenVAS is a "remote scanner" because of the fact that it doesn't have to be introduced on a target for it to test. Instead, it could be installed and configured on one and only device and test many hosts. OpenVAS is client-server architecture over SSL.

The architecture[15] in figure 4.4 is explained below:

- OpenVAS scanner: At the center of the architecture is the OpenVAS scanner which executes the Network Vulnerability Tests (NVTs). The NVTs are updated regularly with the NVT feeds.

- OpenVAS manager: It gives the combination of vulnerability scanning and vulner-

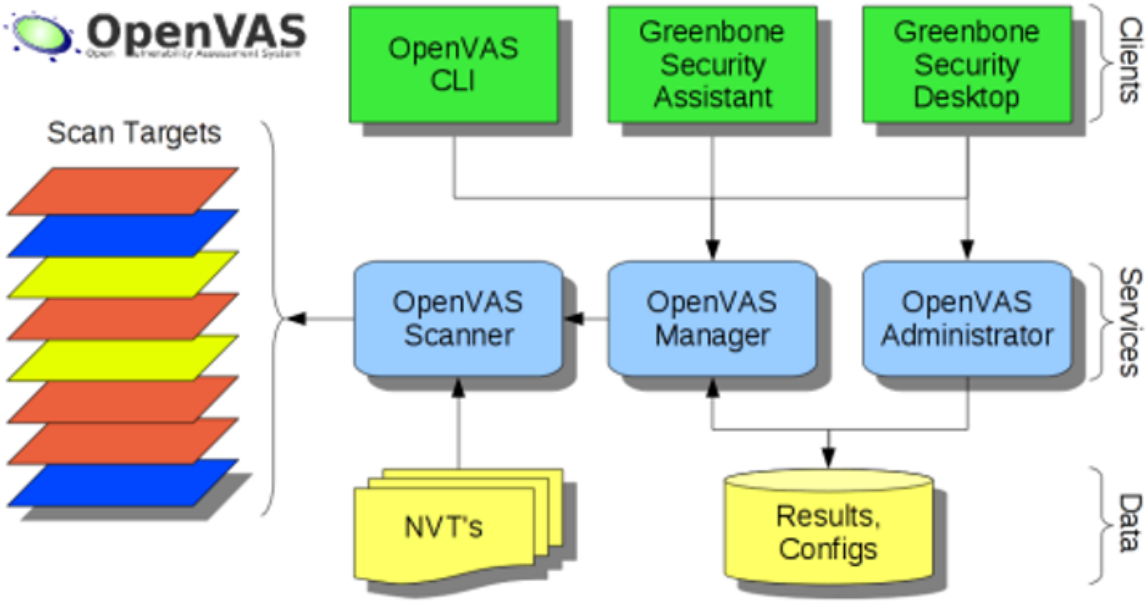


Figure 2.4: Architecture of OpenVAS

ability management. The administrator makes it conceivable to actualize various clients for consistent behaviour. It likewise controls a SQL database for central storage.

- Greenbone security assistant: GSA gives a browser based interface to the application.
- Greenbone security desktop: GSD gives a desktop client.
- OpenVAS CLI: It gives command line interface.
- OpenVAS Administrator: It is a full service daemon whose task is user management and feed management.

2.2.2.1 Working of OpenVAS

Most high-level network traffic, for example, websites, email, and so forth reach a server by means of a high-level protocol that is transmitted by a TCP stream. To keep assorted streams from intruding with each other, a computer partitions its physical connection to the network into thousands of logical paths, called ports. Every computer or device has many ports, all of which could possibly have services (i.e: a server for a particular protocol) listening on them. OpenVAS works by testing each one port on a computer,

figuring out what service it is running, and after that testing this service to verify there are no vulnerabilities in it that could be utilized by a hacker to attack.

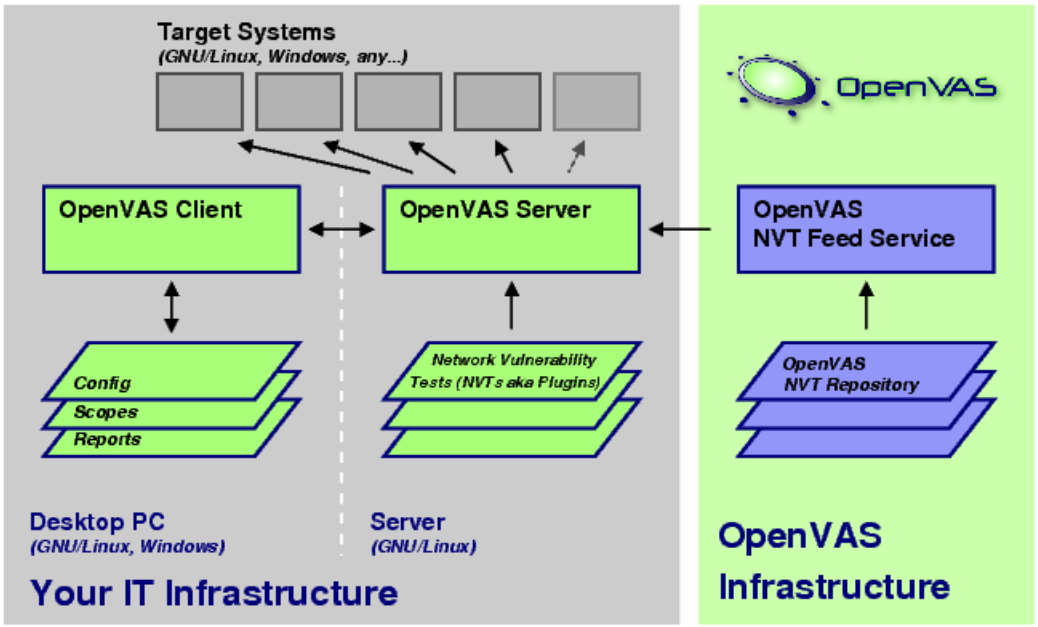


Figure 2.5: Working of OpenVAS

As shown in Figure 2.5[17], This testing is done by comparison with the available vulnerability tests i.e Network Vulnerability tests. In other words, NVT is defined as test schedules that check for vicinity of a vulnerability on a targets. OpenVAS coordinates the execution of huge numbers of such tests to numerous targets and gathers the results.

Advantages of OpenVAS:

- Free for unlimited IPs.
- Good community support
- Can produce audit reports.
- Keeps history of scans.
- Used and backed by consultants that work directly for the US Government. Used by German government

Disadvantage of OpenVAS:

OpenVAS is very complex to install and configure.

2.2.3 Comparison of tools

HackerTarget.com [18] performed a comparison test between various scannig tools i.e. Nessus, OpenVAS, Nexpose and NMAP. Key points of how testing was conducted is given below:

1. OpenVAS v5 was tested with the full and fast scan profile (ports were all TCP ports and top 100 UDP ports).
2. Nessus v5 was propelled utilizing the external network scan profile (additionally tested with internal network scan but results were same).
3. The Nexpose scanner was executed with the full review profile.
4. No tweaking of default scan profiles was embraced.
5. Tests were focused on an external network service, so no credentials were used.
6. This devices were inspected on a example set of exploitable and misconfigured services on the Metasploitable framework.

These are the amounts of vulnerabilities effectively uncovered and appraised by every vulnerability scanner, from the example set of exploitable services.

Nessus	OpenVAS	Nexpose	Nmap
7	7	7	6

Figure 2.6: Comparison results: Number of vulnerabilities found in each tool

7 out of 15 security holes identified

Security Issue	Nessus	OpenVAS	Nexpose	Nmap
FTP 21 Anonymous FTP Access	✓	✓	✓	✓
FTP 21 VsFTPd Smiley Face Backdoor	✓	✓		
FTP 2121 ProFTPD Vulnerabilities		✓		
SSH 22 Weak Host Keys	✓	🔍	✓	
PHP-CGI Query String Parameter Injection	✓	✓	✓	✓
CIFS Null Sessions	✓	✓	✓	✓
INGRESLOCK 1524 known backdoor drops to root shell				
NFS 2049 /* exported and writable	🔍	✓	🔍	
MYSQL 3306 weak auth (root with no password)	✓	✓	✓	✓
RMI REGISTRY 1099 Insecure Default Config				
DISTCCd 3632 distributed compiler				
POSTGRESQL 5432 weak auth (postgresql)				
VNC 5900 weak auth (password)			✓	
IRC 6667 Unreal IRCd Backdoor				✓
Tomcat 8180 weak auth (tomcat/tomcat)	✓		✓	✓

Figure 2.7: Detailed result from hackertarget.com

2.3 Conclusion of literature survey

Vulnerability assessment is an essential security control that ought to be implemented by any organization longing to secure their IT infrastructure.
Based on study till now, following issues of both tools are as follows:

Vulnerability Assessment : NMAP provides very less NSE scripts and vulscan results has large number of false positives.

Complexity to install/configure : OpenVAS is very complex to install and configure.

Report Generation : Custom report cant be generated by this tools

Scan Duration : OpenVAS intensive vulnerability scans takes time

Most organizations ought to begin with a vulnerability assessment, and according to the best of their capabilities select a "white box" pen test in the event that they are sure about their enhanced security posture.
The results of comparison of different tools show significant variation in discovered security vulnerabilities. In vulnerability assessment, its important to check the results for correctness (false positives) and to search for vulnerabilities that were missed (false negatives).

Thus, prescribed methodology to vulnerability examining is to:

- Tune the vulnerability scan profiles to suit your necessities
- Perform point by point examination of the results
- Run optional instruments (NMAP, an optional vulnerability checking result and/ or particular apparatuses). The utilization of numerous tools will give a more stupendous level of scope and support in affirming uncovered vulnerabilities.

Chapter 3

The Proposed Solution and Approach Methodology

3.1 Issues in existing system with proposed solution

Based on the literature survey, a list of issues which are going to be addressed in thesis are discussed in this section.Every scanner conveys a devoted set of information about the target hosts. To get a fairly finish picture of targets for more precise analysis, it requires the combo of results from both devices. This way each of the issue can be resolved.

Sr.No.	Issues		Solutions
	NMAP	OpenVAS	
1	**Vulnerability Assessment**		
	Less NSE scripts available and vulscan results has large number of False Positives	None (NVT feed available which can be update regularly)	Integrate NMAP and OpenVAS.
2	**Complexity to install/configure**		
	None	Very complex	WEB BASED GUI. No installation / configuration required at client side.
3	**Report Generation**		
	Only pdf	Custom Reports can't be generated	Create various other formats for output.
4	**Scan Duration**		
	None (Very Fast)	Intensive vulnerability scans takes time	Integrate NMAP and OpenVAS.

Table 3.1: Issues with proposed solution

Based on solutions suggested in 3.1, a new architecture is designed which is discussed in next section.

3.1.1 Generic architecture

To attain an deliberation from both scanners, following challenges are recognized for the implementation of the integrated scanner platform:

- The platform must be able to control the actions of both scanner (NMAP and OpenVAS).
- The platform must provide an option to scan with either with one of the scanner or the integration of both

Considering above points and proposed solutions, a design for new tool is given in 3.1. Figure 3.1 shows a rough overview of the architecture used for our proposed integrated

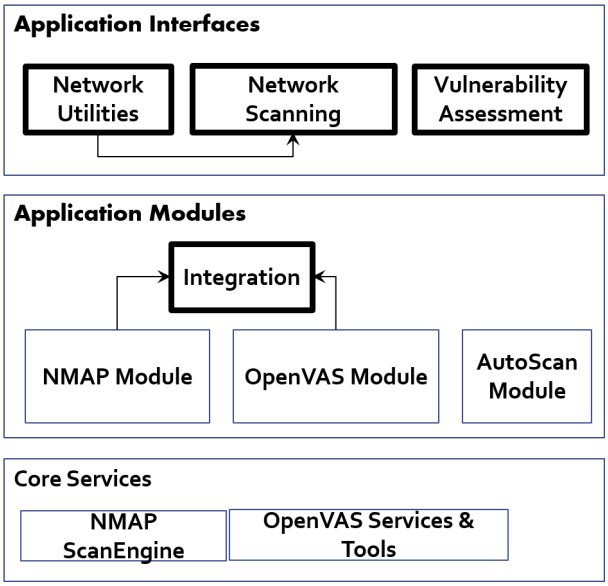


Figure 3.1: Generic architecture of Network Scanner

network scanning platform.

Layer 2 contains client interfaces.

Layer 1 contains various modules which accept requests, processes it, call core services and give response in pretty way.

Layer 0 comprises of core services which is used to do actual work.

3.2 Implementation method

Different types of network devices requires distinctive sorts of scanning & testing. The sort of scan ought to be weighed against the worth of the data on the target host and the need for connectivity to a given service. Proposed methodology has five steps:

- Defining the scope
- Perform vulnerability assessment using NMAP and OpenVAS both
- Reporting and delivering results
- Performing the penetration test to show usage of tool.

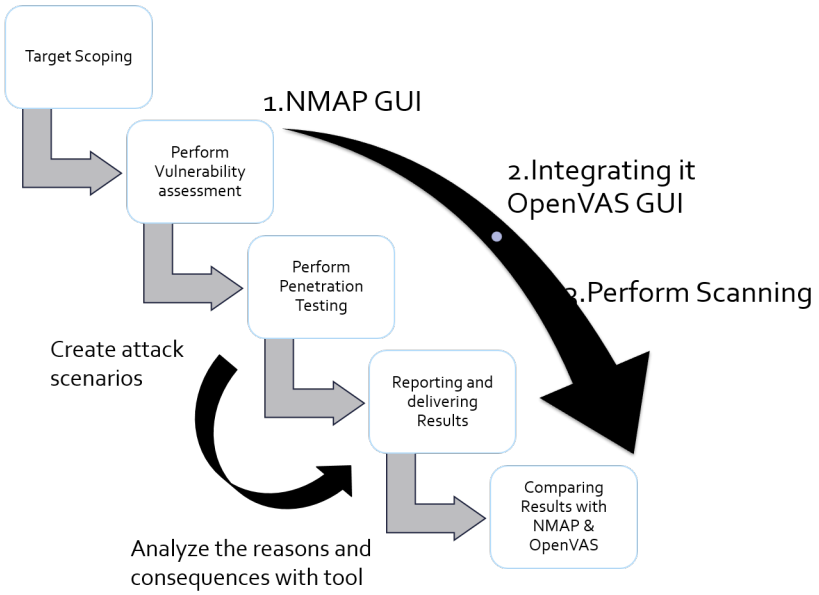


Figure 3.2: Steps of implementation

3.2.1 Target scoping

This step begins with preliminary study about network. It incorporates deciding the degree of testing (extent), what will be tested, from where it will be tested, and by whom[14].

Extent of testing : Targeted vs Full-Scale Testing

Network administrator must pick whether to target specific devices, for instance,

the firewall or to run a full-scale test of the entire network. Most ideal course is to do both to focus the level of exposure the public infrastructure, and the security of singular targets.

Targeted or Perimeter Testing includes:

- Routers and switches
- DNS server, web server,main server, file server and other application server
- Firewalls, both internal and external
- Related network perimeter security systems(IDS)

Testing arena :Local vs Remote Testing

Next,administrator must choose whether the testing will be performed from a remote area over the Internet or on location by means of the local network. This decision is dictated to a large degree by the targets that are selected for testing and by the current security implementations.

Testing authority :In-House vs. Outsourced Testing

Finally, executive must choose whether to use in-house assets to perform the testing or to contract outside experts. However the purpose of this dissertation is to develop tool for administrator, hence In-house testing.

3.2.2 Vulnerability assessment

Vulnerability assessment work is divided into two parts. First is vulnerability discovery by finding or tracking vulnerability present in the given system. Second is eliminating or avoiding this vulnerability from system which is the role of user (network administrator). Vulnerability assessment process follows following steps:

1. Discover the Network i.e Reconnaissance
2. Enumerate the devices (target hosts) on the network
3. Determine the services on the devices (target hosts)
4. Detect and verify known vulnerabilities found for each target host.
5. Report on vulnerabilities

Also vulnerability assessment practices are as follows:

- Manual scan
- Performing scans at a regular interval such ad daily, weekly, monthly or yearly.
- Perform emergency scans when under attack

Based on the architecture, we define here the requirement of tool that is to be developed

3.2.2.1 Functional requirement

Each functional requirement is categorized into four modules which are as follows:

1. Network Utilities: It includes tools to reconnaissance i.e. to discover the network
   - i Ping
   - ii Traceroute
   - iii whoIS lookup
   - iv Nslookup
   - v DNS enumeration
2. Network scanning using NMAP
   - i Show open and filtered ports of each host that are scanned in last 7 days, or from saved report and cron job. Thus identifying if there is configuration change in device.
   - ii Nmap Scan on target using different scanning profiles.
   - iii Select NSE scripts to perform configuration and vulnerability checks.
   - iv Profile editor to create new profiles or edit existing ones.
   - v Downloading / Saving in server option.
   - vi Loading the saved report/ loading the report run by cron.
   - vii Visualization of output in different formats:
     - 2D graph
     - 3D View

- Tabular data
- PDF Report

3. Vulnerability Scanning with OpenVAS

   i Dashboard which gives following information:

   - Overview
     - Current Status (New, Running, Stopped, Paused) of tasks
     - Total count of vulnerabilities(High, Medium,low) of each scan
     - Total count of vulnerabilities(High, Medium,low) of each task
     - Resources overview i.e count of tasks, target groups, scan configurations etc.
     - Top Vulnerability detected till the current time.
     - Top tasks with high vulnerability detected till the current time.
   - OpenVAS scanner details
   - Scan Configuration List
   - Target List

   ii OpenVAS tasks

   - Listing all tasks
   - Start, Pause, Resume and Stop tasks
   - Create Targets option
   - Create Tasks option
   - Create tasks witch takes NMAP output as its input so as to reduce the scan time

   iii Reports

   - Different formats of reports are creating by adding different details. This details are:
   - Scan start time, stop time and target list for the task
   - Overview of vulnerabilities found in task (count of high, medium, low, logs and false positive)

- List of ports founds in each host with its threat (High, Medium, Low, Log)
- Provide Category count of threats found in each category

4. Auto scan

   i Create group of IPs.

   ii Select what kind of scan to be performed (NMAP or OpenVAS or both) and accordingly provide NMAP profile and OpenVAS scan configuration.

   iii Give priority (when to scan) to this group i.e daily, weekly, monthly, yearly or at particular time.

   iv Provide Editing/ Deleting group option

   v In the case of attack detected by snort, perform vulnerability scan and send report to admin

3.2.2.2 Non-functional requirement:

1. Open Source: The tool must be low cost solution with possibilities to modify in future.

2. Portability: A vulnerability scanning engine must be capable of scanning multiple OS platforms (as organization uses a mix of Windows, Linux, Unix, MacOS, etc.)

3. Accuracy: Results must be accurate as it directly impacts the decision made by administrator related to network security.

3.2.3 Delivering reports

After completing the vulnerability assessment, administrator needs to analyze all information derived from the testing procedure. The ability to generate reports in different formats is important in summarizing and presenting information.
The tool lists and prioritize vulnerabilities by categorizing risks (based on CVSS factor) as low, medium or high and prescribe repairs for that issues. It may also give additional information, for instance, Internet links, for discovering extra data or obtaining patches to repair vulnerabilities. The final report may include the following parts:

- Graphical representation: 2D graphs and 3D representation of scan output along with raw scanner output.

- Vulnerability reports: A detailed report of the discoveries about each device's vulnerabilities, which categorizes and prioritizes risks, and makes suggestions about repairs, with some additional information.

Different types of reports are already mentioned in functional requirements.

3.2.4 Testing

Testing is performed within network itself. Testing includes:-

- Port Scanning and identification of the services using NMAP: The first task of scanner is to discover what's on the network, and what it's running, and what OSes were running on each system. It attempts to determine which applications and services are running on these systems, and their configurations.

- Vulnerabilities scanning using OpenVAS: Perform vulnerability scan using both tools individually as well as by integrating them. The vulnerability scanner relies on a database provided by OpenVAS that holds all the information needed to check a system for vulnerabilities.

- Detect change in configuration: The scanner perform daily scan on critical devices. It should provide alert if there is any change in result due to configuration change. Because it may or may not be an authorized modification in configuration of device.

3.3 Project plan

Based on implementation steps and requirements of tool, whole development was divided into phases shown in figure 3.3. Phase 1 includes the basic study of project. Phase 2

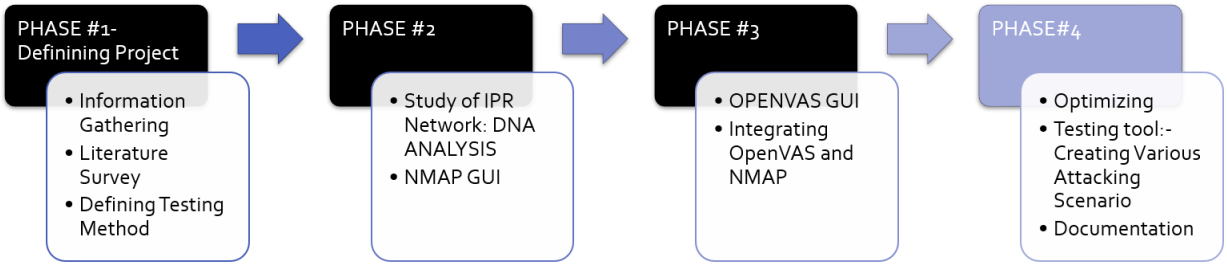


Figure 3.3: Development Phases

includes studying internal network, performing network scanning and developing NMAP module. Phase 3 comprises of development of OpenVAS module and defined a mechanism for integration of both modules. Phase 4 includes development of auto-scan module. It also comprises various attack tests based on vulnerability found. But this tests are out of scope of this dissertation. This tests are conducted only for understanding purpose.

Chapter 4

Design and Development

Network Scanner is web based portal for NMAP and OpenVAS. It offers best of both tools. It resolves many issues found in this two tools.

This chapter contains detailed architecture of Network Scanner. It explain core services (NMAP and OpenVAS) and how it is used in this tool.

4.1 Architecture of Network Scanner

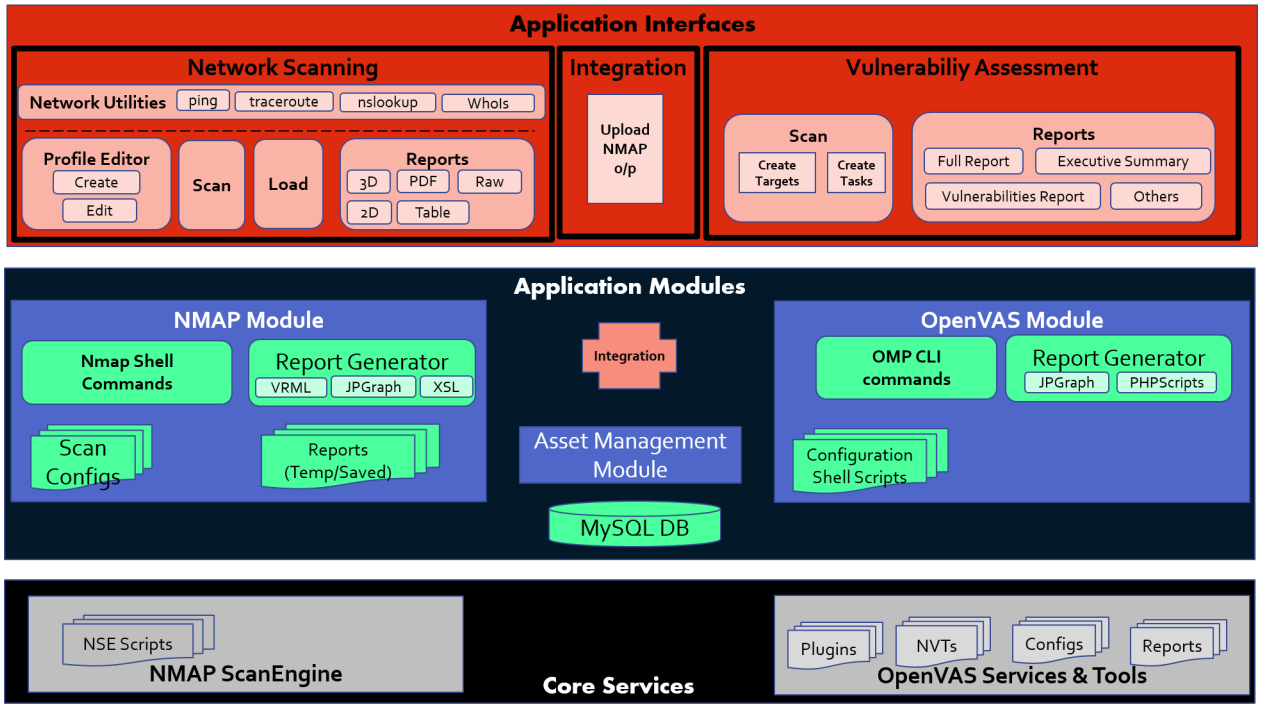


Figure 4.1: Detailed architecture of Network Scanner

4.2 Layer 0:Core services

Figure 4.2: Layer 0:Core services

At core this tool uses NMAP and OpenVAS.

4.2.1 NMAP scan engine

The basic overview about NMAP is already covered in previous chapters. Here, working and usage of NMAP is explained.

4.2.1.1 NMAP working

- NMAP scan is based on TCP/IP protocols. It queries target hosts and the reactions are deciphered into helpful security data.
- All of the eminent data that NMAP uncovers is identified with these transmission between NMAP and the remote hosts.
- 15 different scanning methods within NMAP
- More than 20 options to use when scanning
- Output of NMAP can be saves in four different ways i.e pdf, 2D graph, raw output and tabular output.
- There are timing variable and packet delay settings that can be tweaked and altered.
- NMAP is based on four protocols: IP, TCP, UDP, ICMP

NMAP support files[13]:

In addition to the NMAP executable, there are six support files that provide NMAP with additional information during a scan:

nmap-mac-prefixes: Correlate and display manufacturer names in the NMAP output.

nmap-os-fingerprints: Collection of OS unique responses.

nmap-protocols: Relegate a known name to any protocol that may be found throughout the output. In the event that IP protocol no. 8 reacts to an output, the nmap-conventions record is refered: IP number 8 insinuates Exterior Gateway Protocol (EGP), and NMAP will show that Exterior Gateway Protocol was dynamic on the host.

nmap-rpc: shows and correlates the project name based around the nmap-rpc data.

nmap-services probes: Find the type of application running on a system (httpd, mysqld, ftp etc, than the particular application name (Microsoft IIS, Apache httpd, etc.), its version number, and occasionally some additional application information.

There are timing variable and packet delay settings that can be tweaked and altered.

NMAP is focused around four protocols: IP, TCP, UDP, ICMP

4.2.1.2 NMAP usage

1. **NMAP Ping**:
   Before NMAP will scan a device, it checks to be sure the device is really on the network. NMAP has a plethora of pings from which to pick. Here's the entire list:

   ARP Ping (-PR) :

   The ARP ping sends an Address Resolution Protocol packet to a device on a local subnet. Because this isn't an IP frame, this ping can't be used to identify devices across IP subnets.

   ICMP Echo Request Ping (-PE) :

   This ping is a "real" ping, because ICMP echo request is sent and looks for an ICMP echo reply. Since most smart firewalls are blocking ICMP, this option isn't very useful to other protected networks.

   TCP ACK Ping (-PA) :

   When the default NMAP ping works, it's because the TCP ACK ping got a response. The ACK ping sends a random TCP ACK on port 80 to another device, and the out-of-order ACK usually prompts a response.

TCP SYN Ping (-PS) :

The TCP SYN ping performs the same function as NMAPs TCP SYN scan, but only uses a single port. Port 80 is used by default, but any port can be specified to assist with those hard-to-ping devices.

UDP Ping (-PU) :

Don't forget about UDP! With this ping type, you want to choose a port that isn't open, because a closed UDP port will usually reply with an ICMP port unreachable message. Of course, a protected network is probably filtering ICMP, so use this ping with the understanding that it may not always be the best choice.

ICMP Timestamp Ping (-PP) :

The ICMP timestamp ping uses the "get timestamp" function of ICMP. This function is useful, but it still relies on ICMP to get the message from one side to another. Avoid this ping across filtered links.

ICMP Address Mask Ping (-PM) :

The ICMP address mask ping is an unusual ICMP function, and most devices don't give up critical information such as subnet masks. Again, the limitations of an ICMP-based ping still apply.

Some of these pings may be more appropriate than others, depending on what user is trying to identify on the remote device. For example, if your NMAP scan is focused on identifying UDP ports it may be more appropriate to ping the remote device with a UDP ping.

Other NMAP pings might be useful in rare circumstances. For example, the ICMP address mask ping is an unusual method to use as an NMAP ping, but it can be relatively useful for identifying older systems that may respond to this antiquated ICMP method.

2. **NMAP Scan Techniques**:

After NMAP ping procedure, the scanning process of NMAP can begin. When run as privileged user, the default NMAP scan is the TCP SYN scan, and when operating as a non-privileged user the default NMAP is the TCP connect() scan. Other techniques are shown in figure 4.3[13]

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

Figure 4.3: NMAP scan techniques

3. **NMAP vulnerability scan**:

   It can be done using NMAP Scripting Engine which automates networking tasks.It is a modular system to enhance Nmap which uses Lua to run scripts. This scripts are executed conditionally, can access basic scan data and are able to do exploiting.

   Another approach is using vulscan.:

   A module named "Vulscan" improves NMAP to a vulnerability scanner. To determine potential defects as per the identified product, the NMAP option -sV is used which enables version detection per service. The output is than looked up in an offline vulnerability databases.

   - Installation: Download the binary file and install them into the folder of NMAP installation
   - Usage:To start a basic vulnerability filter, user need to run the following minimal command:

     nmap -sV –script = vulscan www.example.com [–script-args "vulscandb = db-name"]
   - Databases used: cve,exploitdb,openvas,ovsdb, scipvuldb, securityfocus, securitytracker, xforce
   - Disadvantage: Large no. of false positive

4.2.2 OpenVAS

The architecture of OpenVAS has already been discussed before.

4.2.2.1 OpenVAS architecture

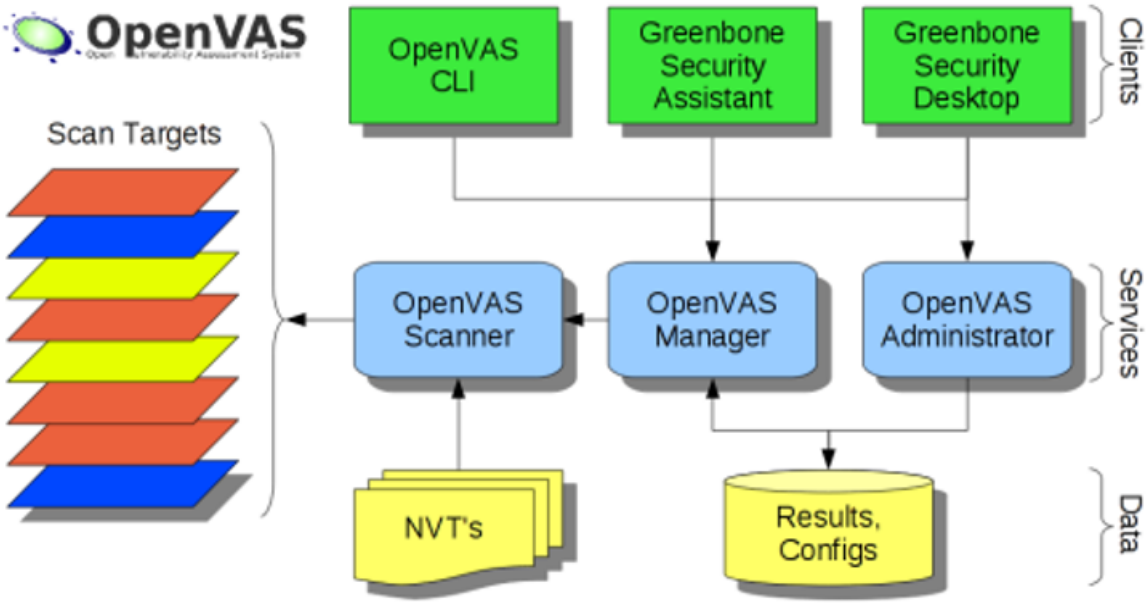


Figure 4.4: Architecture of OpenVAS

The protocols implemented in OpenVAS:

- OTP: OpenVAS Transfer Protocol
- OMP: OpenVAS Management Protocol
- OAP: OpenVAS Administrative Protocol

Overview of features:

OpenVAS Scanner :OpenVAS Scanner can scan many hosts concurrently. It uses OpenVAS Transfer Protocol which always has SSL support.

OpenVAS Manager : OpenVAS manager depends on OpenVAS Management Protocol (OMP) to perform its job such as scheduling tasks, managing concurrent tasks, stop, pause and resume of scan tasks, false positive management and notes management for scan results etc. It uses SQL Database (SQLite) for storing configurations and

scan results. It provides reports format plugin framework with various plugins for: XML, HTML, LateX, etc. OMP always have SSL support.

OpenVAS Administrator :OpenVAS Administrator uses SSl supports OpenVAS Administration Protocol (OAP). It is responsible for user management, feed synchronization and feed status view.

OpenVAS CLI : OpenVAS CLI is command-line client for OMP. It runs on linux, windows etc.

4.3 Layer1:Application module

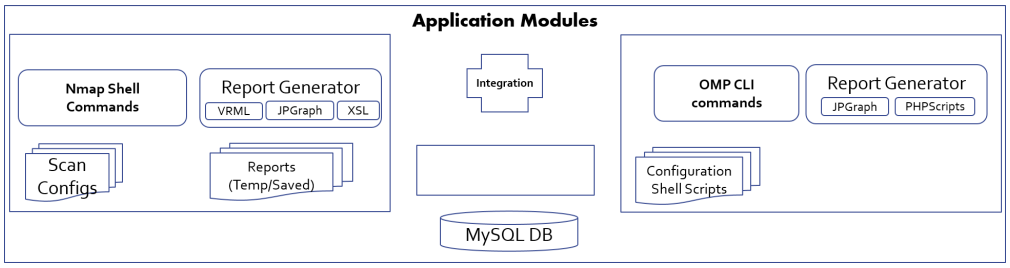


Figure 4.5: Layer 1:Application module

4.3.1 NMAP module

NMAP is developed which can fulfill all the functional requirement.It performs following functions:

Host Discovery :

The scanner checks availability of target hosts. For each host, the scanner checks whether the host is connected to the network, whether it has been closed down and whether it restricts all Internet connections. The service pings each one target host utilizing ICMP, TCP, and UDP probe packets. The TCP and UDP probes are sent to default ports for common services on each host, such as DNS, TELNET, SMTP, HTTP and SNMP. In the event that these probes trigger no less than one reaction from the host, the host is viewed as "alive". The sorts of probes sent and the list of ports checked throughout host discovery are configurable through extra options. if the host is not "alive" then the scan process won't proceed. User may decide to output dead hosts through scan options, however that alternative may build scan

time and is not proposed for Class C or bigger networks.

After host discovery, these steps are taken rapidly: port scanning, operating system detection, service discovery and discover vulnerabilities in host when the vulnerability-check feature is enabled.

Port Scanning :

The scanner discovers all open TCP/ UDP ports on scanned hosts. Scan options are available to make choice of TCP and UDP ports to be checked.

OS Detection :

The scanner endeavors to distinguish the operating system installed on target hosts. This is accomplished through TCP/IP stack fingerprinting, OS fingerprinting on redirected ports.

Service Discovery :

At the point when a TCP or UDP port is accounted for as open, the scanner utilizes a few discovery methods to distinguish which service is running on the port, and affirms the kind of service running to acquire the most faultless information.

Vulnerability Assessment :

Using the information gathered about each target host in the previous scanning steps, the scanner begins vulnerability assessment. The scanner scans for all vulnerabilities in the vulnerability database or a selected list of vulnerabilities, based on the user's scan settings. The service runs vulnerability tests that are applicable to each target host based on the information gathered for the host.

Report Generation :

- Raw scanner output.
- Graphical representation: 2D graphs and 3D representation of scan output
- PDF & tabular format

4.3.2 OpenVAS module

This module depends on OMP CLI of OpenVAS to perform its functions..

4.3.2.1 OMP CLI

OpenVAS Command-Line Interface (openvas-cli) package is used to perform vulnerability scanning.

For most of the common tasks, omp binary provides commands. Using -iX switch with XML requests gives full capabilities of the XML based OpenVAS Management Protocol.

Example: Let uname and password OpenVAS be "uname" and "upass". The initial command to interact with OpenVAS Manager listening on port 9390 on xxx.xxx.xxx.xxx is: **omp -u uname -w password -h xxx.xxx.xxx.xxx -p 9390 iX '<help/>'**.

Scanning host using OMP

1. Choose which tests to perform

2. Choose scan configuration:

   Scan configuration will tell OpenVAS which plugins and options to use. By dafault, Various configurations can be seen using following command:

   ```
   omp -u uname -w password -h xxx.xxx.xxx.xxx -p 9390 iX  '<get_configs/>'
   ```

   Lets select the configuration named "Full and fast" (ID: daba56c8-73ec-11df-a475-002264764cea)to perform scan.

3. Add target host

   Set up the target host having IP address yyy.yyy.yyy.yyy on which scan is performed. Available targets are listed using following command:

   ```
   omp -u uname -w upass -h xxx.xxx.xxx.xxx -p 9390 iX  '<get_targets/>'
   ```

   Adding a target to scan requires a name and the IP address of the target:

   ```
   omp -u uname -w upass -h xxx.xxx.xxx.xxx -p 9390 iX
   '<create_target><name>Target Name</name>
   <hosts>yyy.yyy.yyy.yyy</hosts>
   </create_target>'
   ```

4. Start the task for scanning process

   Finally, command for starting the scan:

```
omp -u uname -w upass -h xxx.xxx.xxx.xxx -p 9390 iX
'<start_task task_id="254b3305-e85a-46eg-97b2-5fb1d2e9695a"/>'
```

   This task can additionally be paused or stopped before it is done using following commands:

```
omp -u uname -w upass -h xxx.xxx.xxx.xxx -p 9390 iX
'<stop_task task_id="254b3305-e85a-46eg-97b2-5fb1d2e9695a"/>'
```

```
omp -u uname -w upass -h xxx.xxx.xxx.xxx -p 9390 iX
'<pause_task task_id "254b3305-e85a-46eg-97b2-5fb1d2e9695a"/>'
```

   The command to get status of the different tasks is:

```
omp -u uname -w upass -h xxx.xxx.xxx.xxx -p 9390  -G
```

5. Get the reports for a task:

   - Get the report's ID:

     After each one scan, a report is produced. The command for listing IDs of those reports is:

```
omp -u uname -w upass -h xxx.xxx.xxx.xxx -p 9390 iX
'<get_tasks details="1"/>'
```

     To avoid listing all the tasks, an alternate choice is to get the IDs of the distinctive reports produced for a given task, knowing the task's ID:

```
omp -u uname -w upass -h xxx.xxx.xxx.xxx -p 9390 iX
'<get_tasks task_id="254b3305-e85a-46eg-97b2-5fb1d2e9695a" details="1"/>'
```

   - Get the report's format

     Various formats are available like XML, PDF, Latex and NBE. TO get the report in particular format, Id of format is to be retrieved.

     The command to list out the IDs of various formats is:

```
omp -u uname -w upass -h xxx.xxx.xxx.xxx -p 9390 iX
'<get_report_formats/>'

omp -u uname -w upass -h xxx.xxx.xxx.xxx -p 9390 iX
'<get_reports report_id="57d8to01-531a-4qy6-42ag-5e861d8284ar"
format_id="c402cc3e-b531-11e1-9163-406186ea4fc5"/>'
```

6. Understanding return status codes

   Return codes of OMP are very much alike to the HTTP response codes.

Status Code	Status Message
2xx	Command successful (received, understood and accepted)
200	Ok
201	Ok, resource created
202	Ok, request submitted
4xx	Command could not be executed due to an error made by the client
400	Syntax error
401	Authenticate first
403	Access to resource forbidden
404	Resource missing
409	Resource busy
5xx	Command failed due to an error in the manager
500	Internal error
503	Service unavailable / Service temporarily down

Figure 4.6: OMP Status Code

4.3.2.2 Integrating OpenVAS & NMAP

1. Provide information to identify the target host

2. Create new scan configuration with NMAP output

```
 omp --config-file="auth.xml" -iX
"<create_config><copy>daba56c8-73ec-11df-a475-002264764cea</copy>
<name>new config</name></create_config>"
```

```
 omp --config-file="auth.xml" -iX
"<modify_config config_id='"$config_id"'>
<preference>
<nvt oid='1.3.6.1.4.1.25623.1.0.14259'>
<name>NMAP (NASL wrapper)</name>
</nvt>
<name>File containing grepable results :</name>
<type>file</type>
<value> NMAP Output</value>
</preference>
</modify_config>"
```

3. Create a task using this scan configuration.

4. Start the scanning process.

4.4 Layer 2:Application interface

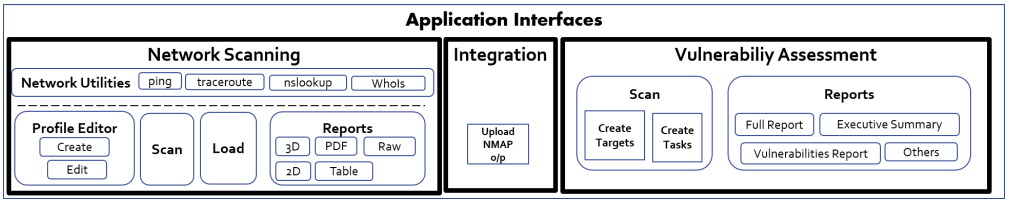


Figure 4.7: Layer 2:Application interface

To implement various task as as discussed above, following are the features of interfaces provided to user.

1. Network utilities

   - Ping
   - Traceroute
   - WhoIs Lookup
   - Browser Profiling

2. NMAP GUI

- Scanning network
- Visualization of report 3D, 2D, PDF, Tabular
- Saving and loading reports
- Creating/Editing scan Profile
- NSE vulnerability scan

3. OpenVAS GUI

- Creating tasks
- Adding targets
- Creating and adding scan profiles
- Different report format- Executive Summary, Full Summary etc.

4. Group GUI

- Create group of IPs
- Assign scan profile to group
- Assign priority to group Daily, Weekly, Monthly, Yearly, Scheduled
- Add scan job to cronTab

4.5 How issues are resolved?

Until now the various features, functions and working of Network Scanner is explained. This tool can address all the issues discussed in table 3.1. Following table shows what actual solution is provided to each issue.

Sr.No.	Issues		Solutions
	NMAP	OPENVAS	
1	**Vulnerability Assessment**		
	Less NSE scripts available and vulscan results has large number of False Positives	None (NVT feed available which can be update regularly)	Integrate NMAP and OpenVAS. Allows user to access either/ both services.
2	**Complexity to install/configure**		
	None	Very complex	WEB BASED GUI. No installation / configuration required at client side.
3	**Report Generation**		
	Only pdf	Custom Reports cant be generated	Network Scanner NMAP module provides following reports: Raw, 3D, 2D, Table, PDF. Also Saving and Loading options are available. Network Scanner OpenVAS module gives custom report like Executive Summary,Full Summary, Vulnerability Report, Host details, Category Count
4	**Scan Duration**		
	None (Very Fast)	Intensive vulnerability scans takes time	Use NMAP NASL Wrapper, Upload NMAP grepable output of target in port scanner family (NMAP NASL).

Table 4.1: Issues with solutions provided

Chapter 5

Results and Discussions

The purpose of this testing is to utilize this application, by performing network scanning and detecting potential vulnerabilities within network. Concurrently, while network scanner is scanning the target for vulnerabilities, the Intrusion Detection System (IDS) will be monitoring all inbound and outbound network traffic through a LAN network connection. The IDS on the installed on server shall attempt to detect these scans is another application called SNORT with customized detection rules. The Intrusion Detection System (IDS)searches for signatures of attacks, which are particular prototypes that typically demonstrate suspicious or malignant intent.
SNORT is an open source network intrusion prevention and detection system utilizing a rule driven language, to recognize and respond to attacks.
This tests includes:

1. Vulnerability assessment process
2. Utilization of tool: Whether this tool provides all main functionality or not?
3. Checking configuration of device: NMAP scripts and vulnerability scan from OpenVAS gives output if there is fault in configuration of device.
4. Vulnerability Scan: At the end,using both tool, vulnerability scan process is shown.
5. At the end, comparison is made between OpenVAS and Network Scanner.

5.1 Test Case 1: Vulnerability assessment process

Aim: We consider here each step of vulnerability assessment and explain how it can be accomplished by Network Scanner.

5.1.1 Reconnaissance

Discovering the network is called reconnaissance. The tool developed is installed on Kali Linux and is already connected to all devices through LAN connection. But for this first step , machine is given public IP to see what information is available to external world. This information is gathered using network utilities tools as explained below.

1. **Ping Utility**

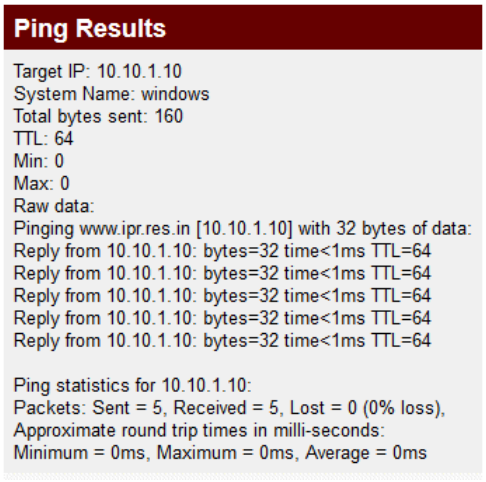


Figure 5.1: Ping output

2. **Traceroute**

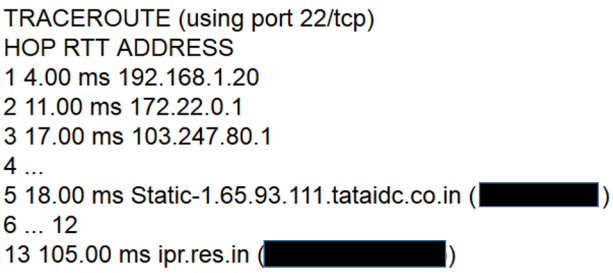


Figure 5.2: Traceroute output

3. **whoIs Lookup**

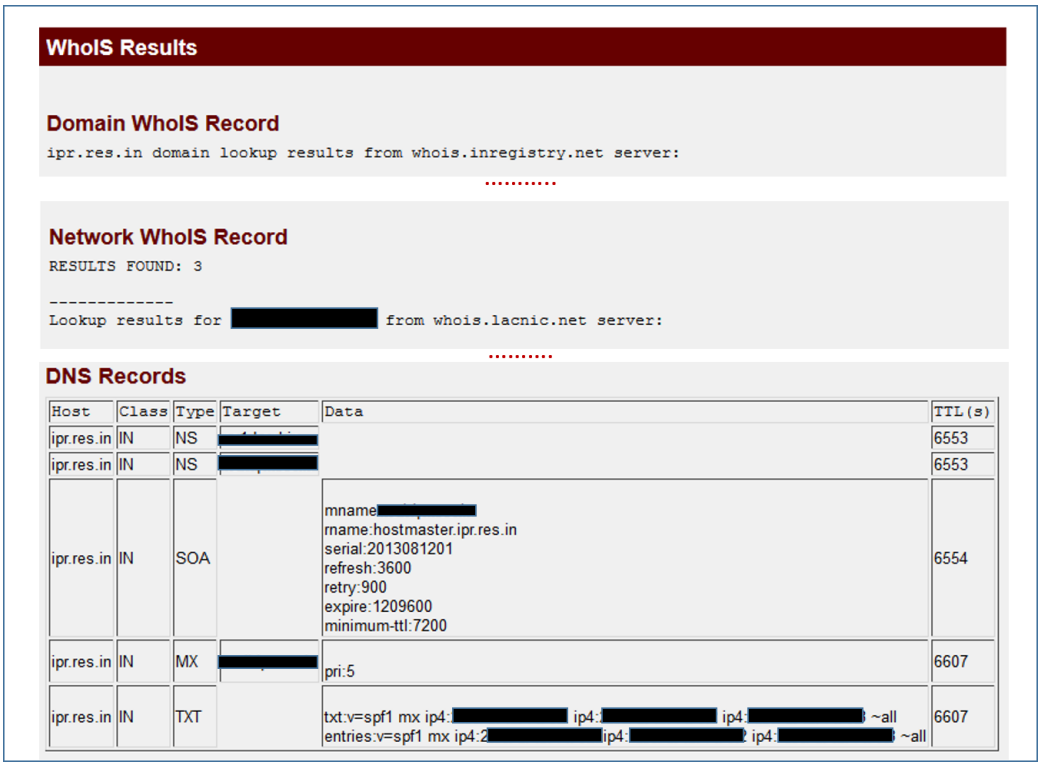


Figure 5.3: Partial output of whoIs Lookup

4. **DNS enumeration**:

Various tools[14] are grouped together to get Domain Name System (DNS) information. This tools were executed from external host. Domain name of IPR i.e. "ipr.res.in" is considered here.

- **dnsenum:** The dnsenum tool can be used to find out information about the complete list of IP addresses and the corresponding hostnames stored in the targeted DNS server. It works by utilizing a DNS zone transfer. It has additional approaches, which can get extra names and sub-domains utilizing the Google search engine, find out sub-domain names by brute forcing the names from the text file, Carry out Whois queries on C-class domain network ranges and calculate its network ranges, carry out reverse lookup on network ranges, and use threads to do different queries. Name Servers:

  ---

  dnsserver.ipr.res.in 43200 IN A 192.168.204.2

dnsserver.ipr.res.in 43200 IN A 192.168.205.2

dnsserver.ipr.res.in 43200 IN A 202.41.112.178

dnsserver.ipr.res.in 43200 IN A 192.168.202.217

Mail (MX) Servers:

---

mail.ipr.res.in 43200 IN A 192.168.200.60

mail1.ipr.res.in 43200 IN A 202.41.112.201

Brute forcing with dns.txt:

---

admin.ipr.res.in 43200 IN A 192.168.201.81

adserver.ipr.res.in 43200 IN A 192.168.201.84

adserver.ipr.res.in 43200 IN A 202.41.113.51

backup.ipr.res.in 43200 IN CNAME

backupnews.ipr.res.in 43200 IN A 202.41.114.25

beta.ipr.res.in 43200 IN A 202.41.112.118

dns.ipr.res.in 43200 IN A 202.41.112.252

jobs.ipr.res.in 43200 IN A 192.168.205.87

mail.ipr.res.in 43200 IN A 192.168.200.60

mail1.ipr.res.in 43200 IN A 202.41.112.201

news.ipr.res.in 43200 IN CNAME

backupnews.ipr.res.in 43200 IN A 202.41.114.25

nms.ipr.res.in 43200 IN CNAME

ds1.ipr.res.in 43200 IN A 192.168.201.200

ns2.ipr.res.in 43200 IN A 192.168.201.5

nsa.ipr.res.in 43200 IN A 192.168.200.100

nss.ipr.res.in 43200 IN A 192.168.203.185

webmail.ipr.res.in 43200 IN CNAME

bambino.ipr.res.in 43200 IN A 192.168.201.100

webserver.ipr.res.in 43200 IN A 192.168.202.115

ipr.res.in class C netranges:

202.41.112.0/24

202.41.113.0/24

202.41.114.0/24

- **dnsmap:** The dnsmap tool uses an approach similar to that of dnswalk and dnsenum to find out subdomains. It comes with a built-in wordlist for brute forcing, and it can also use a user-supplied wordlist.

  [+] searching (sub)domains for ipr.res.in using built-in wordlist

  admin.ipr.res.in

  IP address #1: 192.168.201.81

  [+] warning: internal IP address disclosed

  backup.ipr.res.in

  IP address #1: 202.41.114.25

  beta.ipr.res.in

  IP address #1: 202.41.112.118

  cc.ipr.res.in

  IP address #1: 192.168.201.200

  [+] warning: internal IP address disclosed

  jupiter.ipr.res.in

  IP address #1: 202.41.113.45

  mail.ipr.res.in

  IP address #1: 192.168.200.60

  [+] warning: internal IP address disclosed

  mercury.ipr.res.in

  IP address #1: 202.41.113.19

  news.ipr.res.in

  IP address #1: 202.41.114.25

ns2.ipr.res.in

IP address #1: 192.168.201.5

[+] warning: internal IP address disclosed

proxy.ipr.res.in

IP address #1: 202.41.112.3

IP address #2: 192.168.201.3

[+] warning: internal IP address disclosed

webmail.ipr.res.in

IP address #1: 192.168.201.100

[+] warning: internal IP address disclosed

[+] 11 (sub)domains and 12 IP address(es) found

[+] 6 internal IP address(es) disclosed

[+] completion time: 5 second(s)

- **dnsrecon:** This tool is written in Ruby language and has similar features to all of the previous tools. ./dnsrecon.py -d ipr.res.in

  [*] Performing General Enumeration of Domain: ipr.res.in

  [-] DNSSEC is not configured for ipr.res.in

  [*] SOA dnsserver.ipr.res.in 192.168.202.217

  [*] SOA dnsserver.ipr.res.in 192.168.204.2

  [*] SOA dnsserver.ipr.res.in 192.168.205.2

  [*] SOA dnsserver.ipr.res.in 202.41.112.178

  [*] NS dnsserver.ipr.res.in 192.168.204.2

  [*] NS dnsserver.ipr.res.in 192.168.205.2

  [*] NS dnsserver.ipr.res.in 202.41.112.178

  [*] NS dnsserver.ipr.res.in 192.168.202.217

  [*] MX mail.ipr.res.in 192.168.200.60

  [*] MX mail1.ipr.res.in 202.41.112.201

  [*] Enumerating SRV Records

  [-] No SRV Records Found for ipr.res.in

  [*] 0 Records Found

- **fierce:** The purpose of this tool is similar to that of the previous ones, but it has an advantage that allows you to find out other IP addresses used by the domain you want to check, and it can scan the domain simultaneously using threads.

  DNS Servers for ipr.res.in:

  dnsserver.ipr.res.in

  192.168.202.76 ravikumar.ipr.res.in

  202.41.115.73 govind.ipr.res.in

  192.168.201.155 arvind.ipr.res.in

  192.168.201.209 shailendra1.ipr.res.in

  ....

  ....

  Subnets found (may want to probe here using nmap or unicornscan):

  172.25.10.0-255 : 1 hostnames found.

  192.168.200.0-255 : 18 hostnames found.

  192.168.201.0-255 : 255 hostnames found.

  192.168.202.0-255 : 253 hostnames found.

  192.168.203.0-255 : 252 hostnames found.

  192.168.204.0-255 : 61 hostnames found.

  192.168.205.0-255 : 103 hostnames found.

  202.41.112.0-255 : 193 hostnames found.

  202.41.113.0-255 : 135 hostnames found.

  202.41.114.0-255 : 26 hostnames found.

  202.41.115.0-255 : 22 hostnames found.

5.1.2 Enumerate the devices on the network

Once the network information is retrieved, a simple NMAP scan can tell whether host is up or down.

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-13 01:15 India
Standard Time
Nmap scan report for ipr.res.in (                )
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 2.01 seconds
```

Figure 5.4: Output of regular NMAP scan

5.1.3 Determine the ports and services on the devices

```
Nmap scan report for ipr.res.in (                )
Host is up (0.25s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
```

Figure 5.5: Output of regular NMAP scan

Using NMAP we can also identify the services running on target. Various NMAP options are mentioned in Appendix A.

5.1.4 Detect and report vulnerabilities

Vulnerabilities can be detected using both NMAP and OpenVAS which are explained in later test cases. A sample OpenVAS report is shown in Appendix B. Also various other formats are shown later in this chapter.

5.2 Test Case 2: NMAP module

Aim: Show the utilization of NMAP module and how it performs vulnerability scanning. This test simulates an attacker PC trying to scan a target PC over a network. The Network Scanner's NMAP module will run on the Attacker PC with an connection.The NMAP software executes various port and ping scans against the Target PC and displays

the results locally. The SNORT IDS is installed in a server which is connected to same LAN network.

The SNORT IDS will listen to and capture inbound/outbound network traffic that it acquires from its LAN connection to the Host PC's physical Ethernet adapter.

The SNORT IDS will utilize both predefined and user-defined rules to detect and report any intrusion attempt made by the Attacker PC. The SNORT IDS will log any intrusion attempt (e.g. port scans) made by the Attacker PC into a local MySQL database for later viewing.

5.2.1 Description of test environment

The test environment includes two PC's running Linux , and a switch with snmp enabled. One of the PC is where tool is installed and targets are another PC and switch. Both PCs and switch, both are active and are in same LAN network.

5.2.2 Test plan

Phase 1: A basic demo program is to be implemented to verify that Network Scanner's NMAP module are working properly.

Phase 2: Identify the vulnerability on Attacker's PC.

5.2.2.1 Phase 1

Various features of NMAP module are as follows:

1. **Host discovery** : nmap -n -sn <target-range>

```
# Nmap 6.40 scan initiated Mon May 12 16:21:14 2014 as:
/usr/bin/nmap -n -sn -oA temp/NmapReport_1399891874 --
stylesheet ../nmap.xsl 10.10.2.0/24
Nmap scan report for [redacted]
Host is up (0.0025s latency).
.....
.....
# Nmap done at Mon May 12 16:21:16 2014 -- 256 IP addresses (15
hosts up) scanned in 2.21 seconds
```

Figure 5.6: NMAP - host discovery

2. **Port scanning and service discovery** : nmap -p1-65535 -sV <target-range>

Host: [redacted]

Port	Protocol	State	Service
80	tcp	open(syn-ack)	http
3389	tcp	open(syn-ack)	ms-wbt-server

Host: [redacted]

Port	Protocol	State	Service
22	tcp	open(syn-ack)	ssh
80	tcp	open(syn-ack)	http
111	tcp	open(syn-ack)	rpcbind
3306	tcp	open(syn-ack)	mysql

Host: [redacted]

Port	Protocol	State	Service
80	tcp	open(syn-ack)	http
3389	tcp	open(syn-ack)	ms-wbt-server

Figure 5.7: NMAP - port scanning and service discovery

3. **OS detection**: nmap -O <target-range> [This requires root privileges. So instead we use nmap -T4 -A [target-range] which does port scanning, service discovery as well OS detection.]

Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Uptime guess: 109.828 days (since Thu Jan 23 03:58:05 2014)

Figure 5.8: NMAP - OS detection

4. **Different formats of reports**:

   (a) **Raw output**: Raw output means what NMAP returns on promt.

```
Nmap scan report for cctrainee5.ipr.res.in (10.10.2.55)
Host is up (0.017s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql

# Nmap done at Mon May 12 16:55:02 2014 -- 1 IP address (1 host
up) scanned in 0.53 seconds
```

Figure 5.9: NMAP - Raw output

(b) **3D View**: Each host is placed sequentially, starting next to the little square representing the subnet. Placing the mouse over this square gives information about the subnet. Each host is symbolized by a cylinder. The height of the cylinder gives numerical information about the host, typically the number of open ports.

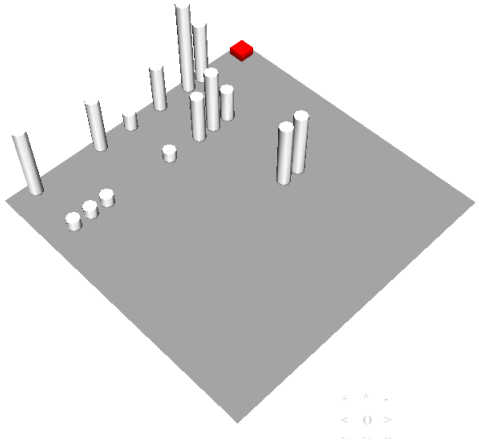


Figure 5.10: NMAP - 3D view

(c) **2D Graph**: Each bar refers to individual host. Green bar refers to open ports. Red bar refers to closed ports. And blue bar refers to filtered ports.

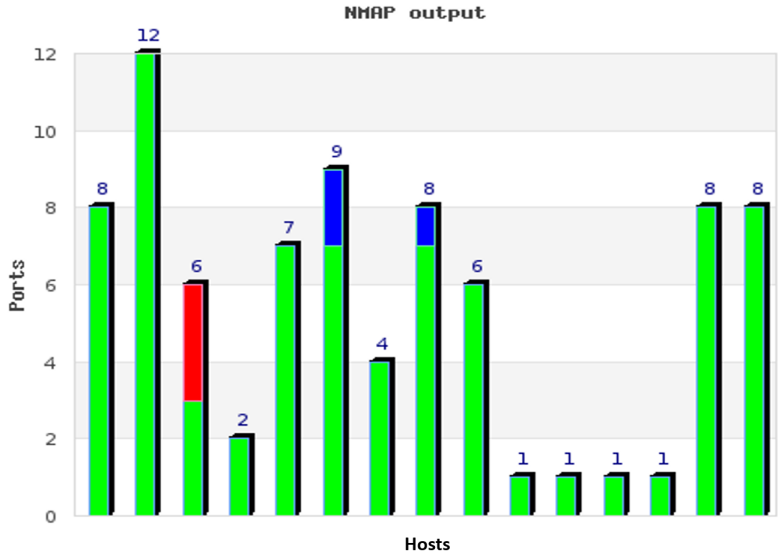


Figure 5.11: NMAP - 2D graph

(d) **Tabular output**

Hosts up: 1 / Hosts down: 0 / Hosts total: 1
Host: [redacted]

Port	Protocol	State	Service	Version
80	tcp	open(syn-ack)	http	(Apache httpd)
3306	tcp	open(syn-ack)	mysql	(MySQL)

Figure 5.12: NMAP - Tabular Format

(e) **PDF format**

Nmap Scan Report - Scanned at Mon May 12 16:55:02 2014

Scan Summary | **cctrainee5.ipr.res.in (10.10.2.55)**

Scan Summary

Nmap 6.40 was initiated at Mon May 12 16:55:02 2014 with these arguments:
/usr/bin/nmap -oA temp/NmapReport_1399893901 --stylesheet ../nmap.xsl 10.10.2.55

Verbosity: 0; Debug level 0

Nmap done at Mon May 12 16:55:02 2014; 1 IP address (1 host up) scanned in 0.53 seconds

10.10.2.55 / cctrainee5.ipr.res.in

Address

- 10.10.2.55 (ipv4)

Hostnames

- cctrainee5.ipr.res.in (PTR)

Ports

The 998 ports scanned but not shown below are in state: **closed**

- 998 ports replied with: **conn-refused**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack			
3306	tcp	open	mysql	syn-ack			

Figure 5.13: NMAP - PDF Format

In phase 1, along with showing how NMAP module can be utilized, it is also shown that how misconfigured device can be identified. Consider a target PC where mis configured Apache Service is running.

1. **Vulnerability assessment using NSE scripts**

   (a) Initially regular scan is performed on target i.e. nmap <target>

```
Nmap scan report for cctrainee5.ipr.res.in (10.10.2.55)
Host is up (0.017s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql

# Nmap done at Mon May 12 16:55:02 2014 -- 1 IP address (1 host
up) scanned in 0.53 seconds
```

Figure 5.14: VA for http service - Regular scan

   (b) Than, nmap scan with service discovery is done i.e. nmap -sV [target]. In the output,it can be seen that target runs "http" service on port 80.

```
# Nmap 6.40 scan initiated Mon May 12 16:53:51 2014 as:
/usr/bin/nmap -sV -Pn -oA temp/NmapReport_1399893831 --
stylesheet ../nmap.xsl 10.10.2.55
Nmap scan report for cctrainee5.ipr.res.in (10.10.2.55)
Host is up (0.015s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.2.23 ((Fedora))
3306/tcp open  mysql   MySQL (unauthorized)

Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Mon May 12 16:53:59 2014 -- 1 IP address (1 host
up) scanned in 7.67 seconds
```

Figure 5.15: VA for http service - Service discovery

   (c) There are two ways to perform nmap scan with NSE scripts.

      i. nmap -T4 -A -v -sC <target>: This will include scripts which comes under default category.

```
Nmap scan report for cctrainee5.ipr.res.in (10.10.2.55)
Host is up (0.00031s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.2.23 ((Fedora))
| http-methods: OPTIONS GET HEAD POST TRACE
| Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-title: Test Page for the Apache HTTP Server on Fedora
3306/tcp open  mysql   MySQL (unauthorized)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
# Nmap done at Mon May 12 16:53:17 2014 -- 1 IP address (1 host up)
scanned in 8.74 seconds
```

Figure 5.16: VA for http service - Scanning with default scripts

ii. nmap -vvv –script = vuln and http* < target >: This will detect all scripts which comes under category of "vuln" and whose name begins with "http". Thus it executes all http scripts which comes uner vuln cateogry.

```
Nmap scan report for cctrainee5.ipr.res.in (10.10.2.55)
Host is up (0.0080s latency).
Scanned at 2014-05-12 16:50:46 IST for 80s
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
| http-enum:
|   /info.php: Possible information file
|_  /icons/: Potentially interesting folder w/ directory listing
|_http-fileupload-exploiter:
|_http-frontpage-login: false
|_http-iis-webdav-vuln: ERROR: This web server is not supported.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: VULNERABLE
|     Description:
|       Slowloris tries to keep many connections to the target
web server open and hold them open as long as possible.
|       It accomplishes this by opening connections to the
target web server and sending a partial request. By doing
|       so, it starves the http server's resources causing
Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|_      http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-trace: TRACE is enabled
| Headers:
| Date: Mon, 12 May 2014 11:14:10 GMT
| Server: Apache/2.2.23 (Fedora)
| Connection: close
| Transfer-Encoding: chunked
|_Content-Type: message/http
|_http-wordpress-enum: [Error] Wordpress installation was not
found. We couldn't find wp-login.php
3306/tcp open  mysql

Read data files from: /usr/bin/../share/nmap
# Nmap done at Mon May 12 16:52:06 2014 -- 1 IP address (1 host
up) scanned in 81.30 seconds
```

Figure 5.17: VA for http service - Scanning with vuln+http scripts

iii. nmap –script =http-methods.nse –script-args http-methods.retest=1 < target >:A scan can be performed with particular script to get more in-

formation about vulnerability. **Thus, above example not only show the vulnerability but also points to fault in configuration of http service.**

```
Nmap scan report for cctrainee5.ipr.res.in (10.10.2.55)
Host is up (0.0096s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
| http-methods: OPTIONS GET HEAD POST TRACE
| Potentially risky methods: TRACE
| See http://nmap.org/nsedoc/scripts/http-methods.html
| OPTIONS / -> HTTP/1.1 200 OK
|
| GET / -> HTTP/1.1 403 Forbidden
|
| HEAD / -> HTTP/1.1 403 Forbidden
|
| POST / -> HTTP/1.1 404 Not Found
|
|_TRACE / -> HTTP/1.1 200 OK
3306/tcp open  mysql

# Nmap done at Mon May 12 16:49:38 2014 -- 1 IP address (1 host
up) scanned in 0.76 seconds
```

Figure 5.18: VA for http service - Configuration fault

2. **Vulnerability assessment using vulscan.nse**: nmap -sV –script = vulscan [target]

```
# Nmap 6.40 scan initiated Mon May 12 17:03:06 2014 as: /usr/bin/nmap -sV --script vulscan/vulscan.nse
-oA temp/NmapReport_1399894386 --stylesheet ../nmap.xsl 10.10.2.55
Nmap scan report for cctrainee5.ipr.res.in (10.10.2.55)
Host is up (0.00038s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.2.23 ((Fedora))
| vulscan: scip VulDB - http://www.scip.ch/en/?vuldb:
| [9891] Apache HTTP Server 2.2.22 suEXEC Feature .htaccess information disclosure
| [4583] Apache httpd up to 2.2.21 Threaded MPM denial of service
| [4582] Apache httpd up to 2.2.21 protocol.c information disclosure
| [2393] Apache httpd up to 2.2.2 HTTP Header Handler Expect-Header cross site scripting
| [4527] Apache Struts up to 2.2.3.1 ExceptionDelegator Code Injection
| [4352] Apache httpd 2.2.x APR apr_fnmatch() denial of service
| [2452] Apache httpd up to 2.2.3 on Windows mod_alias Designfehler
| [2414] Apache httpd up to 2.2.3 mod_rewrite buffer overflow
|
| MITRE CVE - http://cve.mitre.org:
| [CVE-2013-1896] mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether
 .....
 .....
| [10783] PCCS-Mysql User/Password Exposure
|_

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
# Nmap done at Mon May 12 17:03:22 2014 -- 1 IP address (1 host up) scanned in 15.72 seconds
```

Figure 5.19: VA for http service - Using vulscan2.0.nse

3. **Dashboard**: After an successful attack, attacker maintains the access by creating connection to random port of device. This dashboard shows the change in configuration of device.

5.2.2.2 Phase 2

Target for phase 2 is snmp enabled switch. As described above, various NMAP scans are performed on snmp and vulnerability is identified on the switch.

1. **Port scanning and service discovery**: The steps are followed same as above so combined output is shown below.

2. **Vulnerability assessment**:Here it is observed that switch is using version 1 switch. So using permutation of 5 letters and length 5, a community string list is created which performs the brute force attack on this switch. Thus, NMAP return the valid credentials i.e valid community string for this device.

Version Check	Starting Nmap 6.40 (http://nmap.org) at 2014-05-12 12:51 IST Nmap scan report for 10.10.2.60 Host is up (0.0019s latency). PORT STATE SERVICE VERSION 161/udp open snmp MAC Address: 28:C6:8E:BB:74:C7 (Netgear,) Service detection performed. Please report any incorrect results at http://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 5.22 seconds
SNMP BRTUE	Starting Nmap 6.40 (http://nmap.org) at 2014-05-12 12:51 IST Nmap scan report for 10.10.2.60 Host is up (0.0019s latency). PORT STATE SERVICE 161/udp open snmp | snmp-brute: |_ nirma - Valid credentials MAC Address: 28:C6:8E:BB:74:C7 (Netgear,) Nmap done: 1 IP address (1 host up) scanned in 134.46 seconds

Figure 5.20: VA for snmp service

5.3 Test Case 3: OpenVAS Module

Aim: Show the utilization of OpenVAS module of network scanner and how it takes less time compare to OpenVAS

OpenVAS is a standard tool for vulnerability scan. But as it had been discussed that OpenVAS scan takes really long time. This tests shows how by integrating it with NMAP can reduce its scan duration time.

5.3.1 Description of Test Environment

10 switches are selected in which this tests are performed. Then, 10 groups of switch are created where group 1 includes 1 switch, group 2 includes switch from group 1 and one more additional switch, group 3 includes switches from group 2 and one more additional switch and so on.

5.3.2 Test plan

Phase 1: A basic demo program is to be implemented to verify that both OpenVAS and Network Scanner are working properly.

Phase 2: Perform scanning of each group. It is to be noted that any group if first scanned with typical Full and Fast configuration and then with integration of both NMAP and OpenVAS. Scan duration is recorded.

5.3.2.1 Phase 1: Performing a vulnerability scan using simple OpenVAS module

First we perform vulnerability scan of one PC using OpenVAS. It gives results as follows:

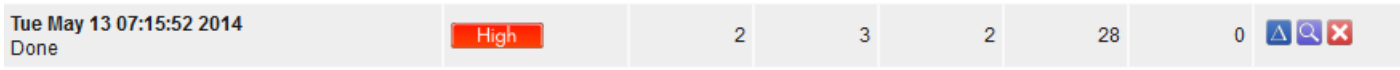


Figure 5.21: OpenVAS scan output

Than we perform vulnerability scan of same PC using OpenVAS:

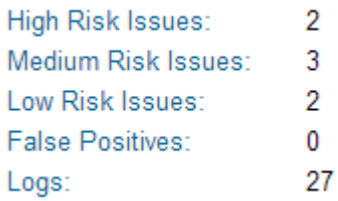


Figure 5.22: Network Scanner output

5.3.2.2 Phase 2: Performing a vulnerability scan for NMAP+OpenVAS

We scanned each group using both type of configuration. The scan duration for each group is shown in table 5.1.

Node	**Scan Duration with NMAP**	**Scan Duration without NMAP**	**Difference (in seconds)**
1	0:09:51	0:09:19	32
2	0:11:59	0:11:11	48
3	0:33:16	0:31:40	96
4	0:15:15	0:13:32	103
5	0:37:48	0:35:26	142
6	1:19:12	1:25:15	375
7	0:38:53	0:28:45	608
8	1:02:56	0:34:02	1735
9	1:06:47	0:35:11	1896
10	1:12:31	0:38:14	2074

Table 5.1: Scan duration of different group of nodes

This data is plotted on graph difference in scan duration Vs. No. of nodes.

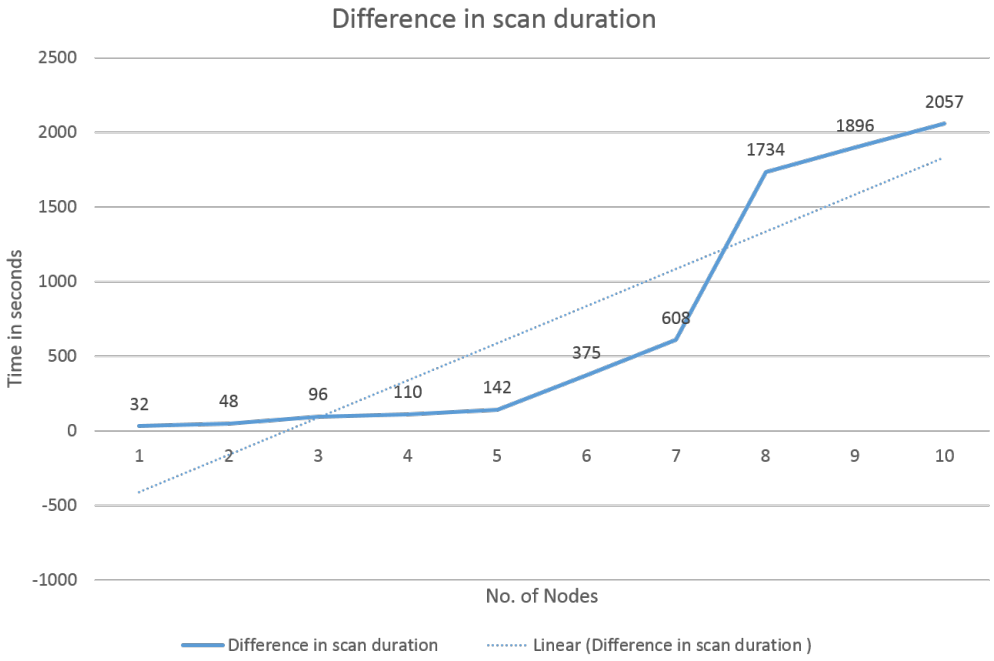


Figure 5.23: Scan duration Vs. No. of nodes

From the graph we can conclude that as we increase no. of host scan time reduces.

Chapter 6

Conclusion and Future Scope

Every day, vulnerabilities are found in commonly used software products. A network scanner developed in this project is an application which is used to scan the network and report any identified vulnerabilities.It is a web-based GUI which deals with two important aspect of network security:- network scanning and vulnerability assessment.
Network scanning includes identification of alive hosts in the network, which operating systems is installed on them, and what services are running on them. Throughout the vulnerability check a database of vulnerability signatures is contrasted with the data acquired from a network scan output to produce a list of vulnerabilities that are presumably present in the network. What's more to check whether the vulnerability might be abused or not,and on the off chance that it can what are conceivable systems, testing is carried out.
It performs functions of both NMAP and OpenVAS. It gives an administrator web-based GUI developed in PHP thus fulfilling portability and open-source requirement of project. The scanning can be done manually or a schedule can be fixed by administrator. The results are shown in different formats for better understanding of management authorities. This project was an excellent primer when implementing network security, but it was not without its challenges.
There are still limitation to this tool and the approach of vulnerability scanning.

Limitations of Network Scanner:

1. For 3D output, VRML plugin needs to be installed at client side.

2. **Authentication:** Network Scanner detect only vulnerabilities for which OpenVAS have signatures.

3. **Scanner's incapability to work with custom applications:** Signatures are only available for known vulnerabilities which are just a little subset of most general attack surfaces. Security checks exists for the well known operating systems and applications facilitated inside network, however shouldn't we think about the custom apps that have been developed in-house or outsourced to outsider, there are no CVEs for custom applications.

4. **Network scanner can't envision complex attack schemes:** While vulnerability scanners normally distinguish and reports about issues that could be used as the initial step of entrance, they are not able to distinguish the complex boulevards an attacker could take to compromise network.

5. While vulnerability scanners can facilitate network security tasks, they can't replace the expertise of trained personnel. Scanners are capable of returning false-positives, indicating a weakness where none exists, and false-negatives, in which the scanner overlooks a security risk. Qualified personnel need to carefully check the data their scanners return to detect erroneous results.

6. Vulnerability scanning also takes up a considerable amount of bandwidth, potentially slowing the network's performance.

The project's capabilities so far represent "the tip of the iceberg". Future projects have great potential for growth and expansion. One possible expansion is optimizing OpenVAS scanner to deal with time-wait condition on target's machine which sometimes slows down the operation on machine or in severe case crashes the machine. Another possible expansion of NMAP is to introduce more NSE scripts for vulnerability scanning. One more possible expansion is to integrate SNORT also with Network Scanner.

Appendix A

NMAP options

Usage	nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:	
Can pass hostnames, IP addresses, networks, etc. Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254	
-iL <inputfilename>	Input from list of hosts/networks
-iR <num hosts>	Choose random targets
--exclude <host1[,host2][,host3],...>	Exclude hosts/networks
--excludefile <exclude_file>	Exclude list from file

HOST DISCOVERY:	
-sL	List Scan - simply list targets to scan
-sP	Ping Scan - go no further than determining if host is online
-PN	Treat all hosts as online -- skip host discovery
-PS/PA/PU [portlist]	TCP SYN/ACK or UDP discovery to given ports
-PE/PP/PM	ICMP echo, timestamp, and netmask request discovery probes
-PO [protocol list]	IP Protocol Ping
-n/-R	Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>	Specify custom DNS servers
--system-dns	Use OS's DNS resolver

SCAN TECHNIQUES:	
-sS/sT/sA/sW/sM	TCP SYN/ Connect()/ ACK/ Window/ Maimon scans
-sU	UDP Scan
-sN/sF/sX	TCP Null, FIN, and Xmas scans
--scanflags <flags>	Customize TCP scan flags
-sI <zombie host[:probeport]>	Idle scan
-sO	IP protocol scan
-b <FTP relay host>	FTP bounce scan
--traceroute	Trace hop path to each host
--reason	Display the reason a port is in a particular state

PORT SPECIFICATION AND SCAN ORDER:	
-p <port ranges>: Only scan specified ports Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080	
-F	Fast mode - Scan fewer ports than the default scan
-r	Scan ports consecutively - don't randomize
--top-ports <number>	Scan <number> most common ports
--port-ratio <ratio>	Scan ports more common than <ratio>

SERVICE/VERSION DETECTION:	
-sV	Probe open ports to determine service/version info
--version-intensity <level>	Set from 0 (light) to 9 (try all probes)
--version-light	Limit to most likely probes (intensity 2)
--version-all	Try every single probe (intensity 9)
--version-trace	Show detailed version scan activity (for debugging)

SCRIPT SCAN:	
-sC	equivalent to --script=default
--script=<Lua scripts>	<Lua scripts> is a comma separated list of directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2,...]>	Provide arguments to scripts
--script-trace	Show all data sent and received
--script-updatedb	Update the script database.

OS DETECTION:	
-O	Enable OS detection
--osscan-limit	Limit OS detection to promising targets
--osscan-guess	Guess OS more aggressively

TIMING AND PERFORMANCE:	
Options which take <time> are in milliseconds, unless you append 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).	
-T[0-5]	Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>	Parallel host scan group sizes
--min-parallelism/max-parallelism <time>	Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>	Specifies probe round trip time.
--max-retries <tries>	Caps number of port scan probe retransmissions.
--host-timeout <time>	Give up on target after this long
--scan-delay/--max-scan-delay <time>	Adjust delay between probes
--min-rate <number>	Send packets no slower than <number> per second
--max-rate <number>	Send packets no faster than <number> per second

OUTPUT:	
-v	Increase verbosity level (use twice or more for greater effect)
-d[level]	Set or increase debugging level (Up to 9 is meaningful)
--open	Only show open (or possibly open) ports
--packet-trace	Show all packets sent and received
--iflist	Print host interfaces and routes (for debugging)

MISC:	
-6	Enable IPv6 scanning
-A	Enables OS detection and Version detection, Script scanning and Traceroute
--datadir <dirname>	Specify custom Nmap data file location
--send-eth/--send-ip	Send using raw ethernet frames or IP packets
--privileged	Assume that the user is fully privileged
--unprivileged	Assume the user lacks raw socket privileges
-V	Print version number
-h	Print this help summary page.

EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sP 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -PN -p 80

Appendix B

Sample OpenVAS Report

Executive Summary

This report is a high level summary of a OpenVAS scan job. The intended audience is for authorities, operational managers and support staff responsible for the target hosts or networks. The purpose of this document is to provide a list of total vulnerabilities found (low, medium, high) with its risk rating.

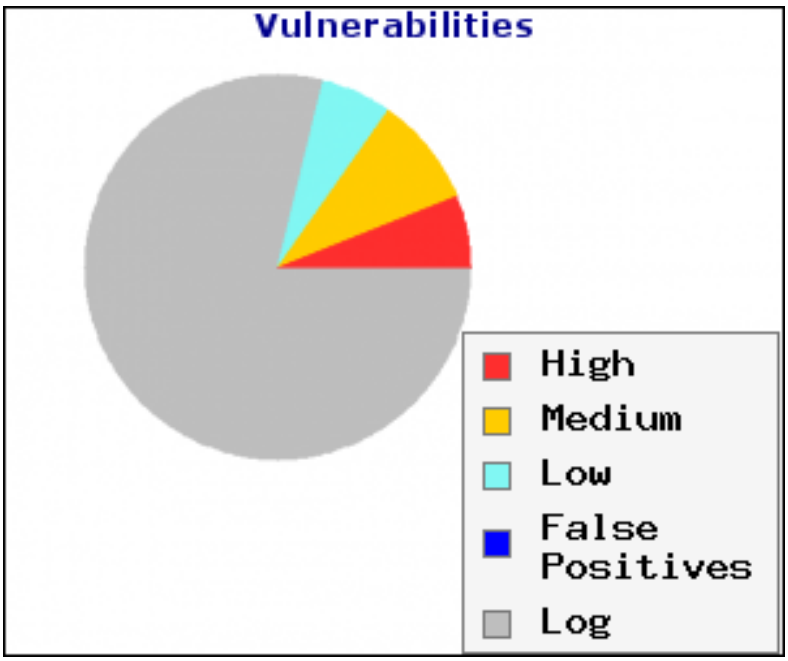
Task: 1node_pc

Scan Job Details

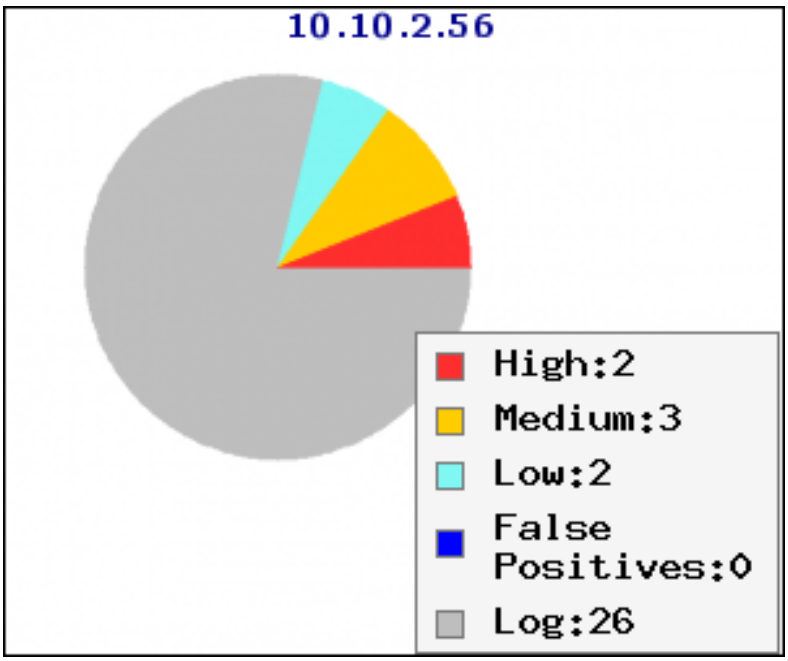
Start Time of Scan:	24/03/2014 11:54
End Time of Scan:	24/03/2014 12:03
Target Scanned:	....

Number of Issues Found: 33

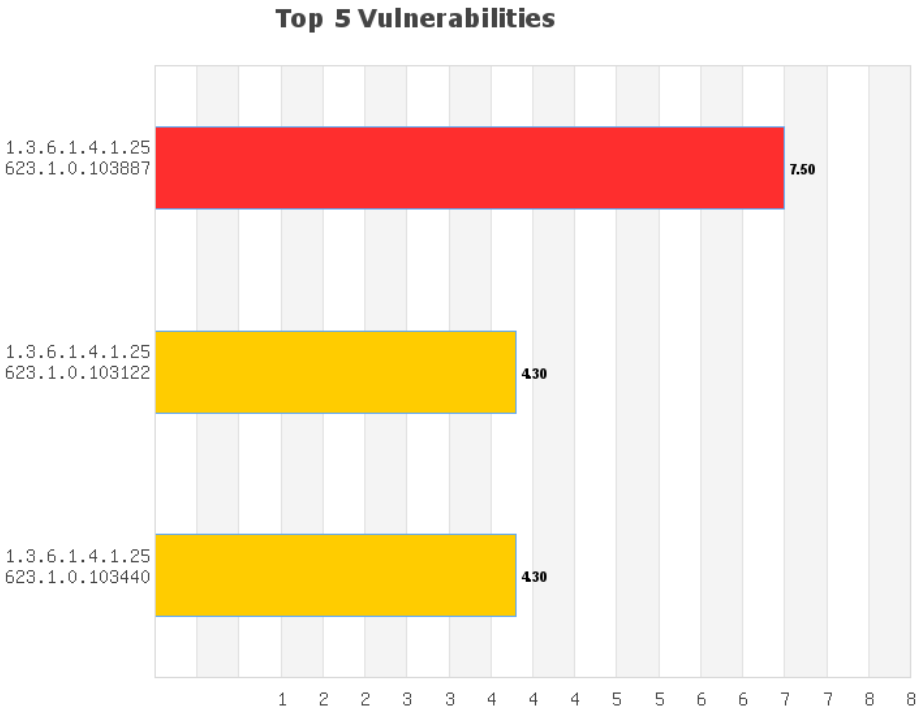
High Risk Issues:	2
Medium Risk Issues:	3
Low Risk Issues:	2
False Positives:	0
Logs:	26



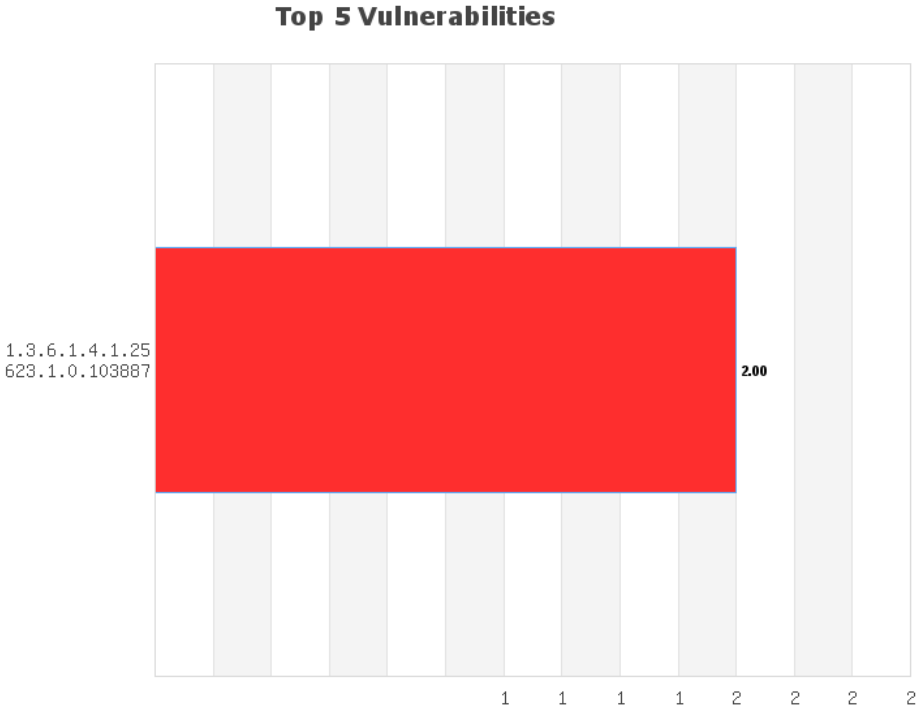
Vulnerabilities By IP



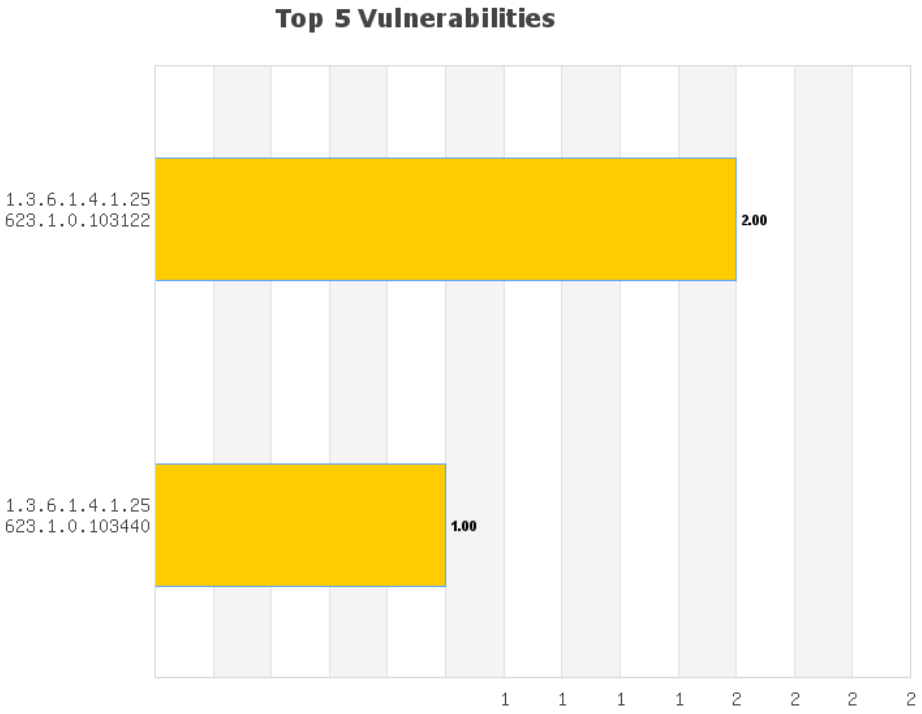
Top Vulnerabilities Detected



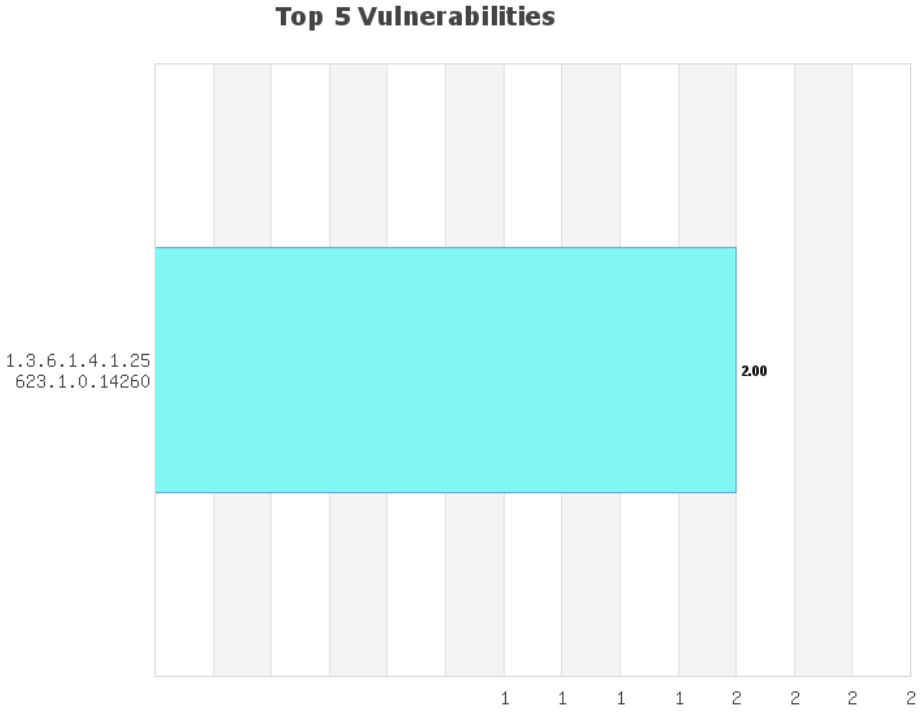
Top High Vulnerabilities Detected



Top Medium Vulnerabilities Detected



Top Low Vulnerabilities Detected



High Risk Vulnerabilities Detected

Host	Vulnerability	Severity Rating
10.10.2.56	Apache Web Server ETag Header Information Disclosure Weakness	4.3
10.10.2.56	Check for SSL Weak Ciphers	4.3

Medium Risk Vulnerabilities Detected

Host	Vulnerability	Severity Rating
10.10.2.56	Multiple IP Video/Camera Server Web Interface Default Admin Credentials	7.5

Low Risk Vulnerabilities Detected

Host	Vulnerability	Severity Rating
10.10.2.56	Nikto (NASL wrapper)	0

Logs

Host	Vulnerability	Severity Rating
10.10.2.56	CPE Inventory	0.0
10.10.2.56	Host Summary	0.0
10.10.2.56	OS fingerprinting	0.0
10.10.2.56	Checks for open udp ports	0.0
10.10.2.56	arachni (NASL wrapper)	0.0

Host	Vulnerability	Severity Rating
10.10.2.56	Traceroute	0.0
10.10.2.56	Checks for open tcp ports	0.0
10.10.2.56	HTTP Server type and version	0.0
10.10.2.56	DIRB (NASL wrapper)	0.0
10.10.2.56	Services	0.0
10.10.2.56	Directory Scanner	0.0
10.10.2.56	wapiti (NASL wrapper)	0.0
10.10.2.56	Apache Web Server Version Detection	0.0
10.10.2.56	Services	0.0
10.10.2.56	OpenVAS Manager Detection	0.0
10.10.2.56	SSL Certificate Expiry	0.0
10.10.2.56	Check for SSL Medium Ciphers	0.0
10.10.2.56	HTTP Server type and version	0.0
10.10.2.56	DIRB (NASL wrapper)	0.0
10.10.2.56	Services	0.0
10.10.2.56	Directory Scanner	0.0
10.10.2.56	wapiti (NASL wrapper)	0.0
10.10.2.56	Apache Web Server Version Detection	0.0

Bibliography

[1] Sudhanshu Chauhan,InfoSec Institute,**Windows Vulnerability Assessment**, Available at: http://resources.infosecinstitute.com/windows-vulnerability-assessment/

[2] G. Murali M.Pranavi Y.Navateja K.Bhargavi4,**NETWORK SECURITY SCANNER**,M Pranavi et al, Int. J. Comp. Tech. Appl. vol 2(6)

[3] Jim Orrill,**What Is the Difference Between Active & Passive Vulnerability Scanners?**, Demand Media, Available at: http://smallbusiness.chron.com/difference-between-active-passive-vulnerability-scanners-34805.html

[4] **Motion Computing LE1600 Supplementary Manual**, Customer Whitepaper: Motion Tablet PC Security Basics, Rev A03

[5] Kavita S. Kumavat, Ranjana P. Dahake, Dr. M. U. Kharat, **Overview of Vulnerability Analysis**, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 10, October 2013

[6] Kinney Williams,**Vulnerability list**, VISTA Penetration Study Internet and internal network security testing, Available at: http://www.internetbankingaudits.com/list_of_vulnerabilities.htm

[7] **Vulnerability Categories**,Available at: https://qualysguard.qualys.com/qwebhelp/fo_help/knowledgebase/vulnerability_categories.htm

[8] Patrick Toomey and Greg Ose,**Scanning Reality: Limits of Automated Vulnerability Scanners**,Strategy: Limits of Automated Vulnerability Scanners,Oct 2010

[9] Nick Hutton,**Understanding, Commissioning, & Maximising Value from Penetration Testing**, Three Sixty Information Security Ltd

[10] **Limitations of Penetration Testing**,Tutorials on Penetration testing tools, Available at: http://www.pen-tests.com/limitations-of-penetration-testing.html

[11] Alexey Polyakov,Head of the Global Emergency Response Team, **Corporate Incidents: Lessons Learned,Common and Avoidable Security Policy Mistakes for IT Management**,Kaspersky Lab International Press Tour, Malaga, 16-19 June, 2011

[12] Steven Drew,**Vulnerability Assessments Versus Penetration Tests**, EVP of Client Services, SecureWorks

[13] Gordon Lyon,**Nmap Network Scanning:Official Nmap Project Guide to Network Discovery and Security Scanning**, Insecure Press , ISBN-10: 0979958717

[14] Shakeel Ali,Tedi Heriyanto,**Backtrack 4,Security by Penetration testing**

[15] **About OpenVAS**, Available at: http://www.openvas.org/about.html

[16] **About OpenVAS Software**, Available at: http://www.openvas.org/software.html

[17] **OpenVAS Compendium**, Available at : http://www.openvas.org/compendium/openvas-compendium.html

[18] Derrick Cramer, **Corporate network vulnerability explained**, Available at: http://hackertarget.com/nessus-openvas-nexpose-vs-metasploitable

[19] VeriSign White Paper, **An Introduction to Network Vulnerability Testing**