International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Network Infrastructure Vulnerabilities and Its Mitigation

Debalina Basu[1], Chandresh D Parekh[2]
[1]*M.Tech in Cyber Security, Raksha Shakti University, Ahmedabad, Gujarat, India*
[2]*Assistant Professor, Raksha Shakti University, Ahmedabad, Gujarat, India*

Abstract: ***Complexities of systems are increasing day by day. This prompts an ever increasing number of vulnerabilities in Systems. Assailants utilize these vulnerabilities to abuse the injured individual's framework. It is smarter to discover these vulnerabilities ahead of time before assailant do. The intensity of Vulnerability appraisal is generally thought little of. Vulnerability Assessment and Penetration Testing can be utilized as a cyber-resistance innovation to give proactive cyber guard. In this paper we present network infrastructure vulnerabilities and its alleviation, how we can give dynamic cyber safeguard utilizing Helplessness Assessment and Penetration Testing in network framework. We portrayed total life cycle of Vulnerability Assessment and Penetration Testing on systems or networks and proactive move made to determine that defencelessness and stop conceivable assault. In this paper we have depicted predominant Vulnerability evaluation procedures and some popular premium/open source VAPT tools. We have portrayed total procedure of how to utilize Vulnerability Assessment and Penetration Testing to tackle network foundation issues as an amazing Cyber Defence Technology. We likewise centre around a honeypot which is a framework that is set up with the particular reason for being assaulted. It is a framework intended to be misused, hacked, tainted with malware, and for the most part manhandled by a malicious outsider.***

Keywords: Vulnerability Assessment; Penetration Testing; Network VAPT Tools; System Security; Cyber defence Technology; Honeypots;

I. INTRODUCTION

Uses of the computers are expanding day by day. System's complexity is increasing. Most of the systems now are connected to Internet. New and complex Software are coming in the market. All these activities are increasing vulnerabilities in systems.

Vulnerability in networking system is a shortcoming in the use of networks which can be a usage bug or a structure imperfection that enables an assailant to make hurt the client of the application and get additional benefits. Vulnerability are the potential hazard for the system or the networks. Attacker utilizes this vulnerability to abuse the system or networks and get unauthorized access and information.

Vulnerabilities are huge defect in framework security and Information affirmation. A helplessness free framework can give more Information Assurance and framework security. In spite of the fact that it is practically difficult to have 100% weakness free framework, yet by expelling whatever number vulnerabilities as could be allowed, we can expand framework security. The need of Vulnerability Assessment and Penetration Testing is typically thought little of till now. It is simply consider as a convention action and use by less individuals. By utilizing ordinary and productive Vulnerability Assessment, we can decrease generous measure of hazard to be assaulted and have more verified frameworks.

Any digital device connected to a computing network is potentially vulnerable to an attack. Attacks are always taking place on the internet, at a rate of several attacks per minute on each connected machine. These attacks are mostly launched automatically from infected machines without their owner's knowledge. Now a days many attacks like DOS(Denial Of Service) attack, Session Hijacking, Direct URL access etc were done in the public area network like airport, shopping mall, etc which uses the open connection. When any crime happened then check the firewall setup rules, network bandwidth, inbound traffic, outbound traffic etc. After that done the analysis through the firewall syslog file, which I/o device connect maximum time in the connection etc.

Honeypots are regularly utilized by vast undertakings and by organizations engaged with cybersecurity investigate, to distinguish and guard assaults from cutting edge tireless danger entertainers. Honeypots can be a significant device for vast associations to take a functioning resistance position against aggressors, or for cybersecurity specialists who needs to get accustomed with the devices and procedures that assailants use.

For the most, a honeypot task comprises of a PC, applications and information that mimic the conduct of a genuine framework and shows up as a major aspect of a system; nonetheless, the honeypot is really detached and intently checked. Since there is no purpose behind authentic clients to get to a honeypot, any endeavors to speak with a honeypot ought to be viewed as antagonistic.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

II. BACKGROUND

Vulnerability Assessment and Penetration Testing (VAPT) approach gives an organization a progressively nitty gritty perspective on the dangers confronting its applications, empowering the business to more readily shield its frameworks and information from malevolent assaults. Loopholes can be found in applications from outsider sellers and inside made software, yet the greater part of these blemishes are effectively fixed once found. Utilizing a VAPT supplier empowers IT security groups to concentrate on moderating basic vulnerabilities while the VAPT supplier keeps on finding and order vulnerabilities.

There are various stages

A. Vulnerability Assessment

1) Defining and classifying network or system resources.
2) Identifying potential level of threats to each resource.
3) Developing a strategy to deal with most serious potential problem.

Once analysis has been completed, if security holes are found as a result of vulnerability analysis, a vulnerability disclosure may be required.

B. Penetration Testing

1) Map the internal network.
2) Scan the network for live host.
3) Port scan for individual machines.
4) Try to gain access using known vulnerabilities.
5) Enumerate users and identify domains of network.
6) Snuffing up the network using wireshark.
7) Sniff passwords and email messages.
8) Attempt ARP poisoning.
9) Attempt MAC flooding.
10) Manage Man-In-The-Middle Attack.
11) Attempt DNS poisoning.
12) Escalate user privileges.

C. Definition

This project includes various aspect of VAPT. Different apparatuses and systems are deployed in this project to perform web application penetration testing, android browser penetration testing, windows system penetration testing. This project leads with the step by step procedure of exploiting known vulnerabilities and gaining access to the system.

D. Scope

This project mainly focuses on existing known vulnerabilities reside in system and with the use them how one can exploit a system and gain unauthorized access to the system. It contains three various areas as explained below.

1) Web Application
2) Android Browser

III. LIFE CYCLE OF VAPT

Weakness Assessment and Penetration Testing is an absolute 9 stage procedure. These means are appeared in Fig. 1. Most importantly analyzer needs to choose the extent of the task (Black/dark/white box). Subsequent to choosing the degree, the analyzer gets data about the working framework, system, and IP address in observation step. After this analyzer utilize different defencelessness evaluation strategy (clarified further) on the testing article to discover vulnerabilities. At that point, analyzer examinations the established helplessness and make arrangement for penetration testing. Analyzer utilizes this intend to infiltrate the injured individual's system. In the wake of entering the framework, analyzer expands the benefit in the system. In result investigation step, analyzer examinations the all outcomes and devise proposal to determine the powerlessness from the framework. Every one of these exercises are reported and sent to the executives to make reasonable move. After these all progression, the injured individual's system and its program get influenced and changed. In cleanup step we re-establish the system in past state as it was before VAPT process was begun.

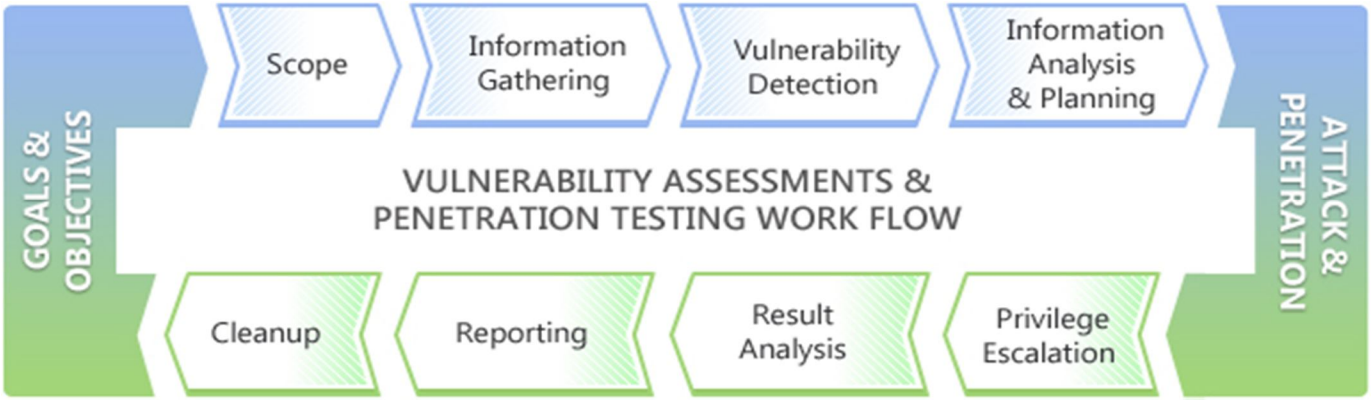

Fig. 1. Vulnerability Assessment and Penetration Testing Life cycle

IV. METHODS

In this phase we need to gather as much data as we can about the target. For example information about the Domain Name System (DNS) hostnames, IP addresses, Technologies and Configuration Used, username's organizations, documents, contact information etc.

A. *DNS Reconnaissance and Route Mapping*

An attacker can utilize data from a whois query to:

1) Support a social engineering assault against the area or people distinguished in the inquiry
2) Identify an area for a physical assault
3) Identify telephone numbers that can be utilized for a war dialing attack, or to lead a social engineering attack
4) Conduct recursive quests to find different areas facilitated on a similar server as the objective or worked by a similar client; in the event that they are uncertain, an aggressor can misuse them to increase managerial access to the server, and afterward bargain the objective server

a) *Getting Network Routing Information:* Learning of the system routing data will enable the penetration tester to comprehend the system of the objective machine, For example, which way is taken by the bundles sent from the penetration tester machine to the objective machine. The routing data will likewise provide some insight with respect to whether the specific target is ensured by firewall.
b) *Target Discovery:* It is the way toward finding machines on the target network. After we have assembled data about our objective system from outside sources, for example, web crawlers the subsequent stage is find our objective machines.
c) *OS Fingerprinting:* After we realize that the objective machine is a live we would then be able to discover the operating system utilized by the objective machine. This method is commonly known as Operating System (OS) fingerprinting.
d) *Vulnerability Mapping:* Vulnerability mapping is the process of identifying and analyzing the critical security flaws in a target environment. This phrasing is some of the time known as vulnerability evaluation. It is one of the key zones of a vulnerability the executives program through which the security controls of an it framework can be investigated against known vulnerabilities.
e) *Web Application Analysis and Exploitation:* Most applications that are built up nowadays coordinate diverse web innovations which expand the multifaceted nature and peril of exposing sensitive data. Web applications have dependably been a long standing focus for pernicious enemies to take control damage and coerce the corporate business. This expansion of web applications has advanced colossal difficulties for penetration testers. The key is to confirm both web based applications front end and databases back end over the system security countermeasures. This is essential since web applications go about as an information handling framework and the database is in charge of putting away touchy information (for instance Visas, customer details, authentication data, and so on).

B. *Denial of Service*

A "denial-of-service attack" (DoS) is a kind of assault that intends to make an association's administrations or assets inaccessible for an uncertain measure of time. More often than not, these assaults are gone for an organization's servers, so they may not be utilized or consulted.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Denial-of-service attack is a problem that can influence any organization server or any individual associated with the web. The objective of such an assault isn't to recover or modify information, yet to harm the notoriety of organizations that are available on the web and to possibly shield them from working appropriately if their movement depends on a data framework.

C. Attack Scenario

Any digital gadget connected to a computing network is potentially vulnerable to an attack. Attacks are always taking place on the internet, at a rate of several attacks per minute on each connected machine. These attacks are mostly launched automatically from infected machines without their owner's knowledge. In one IT company digital crime is happened. In this company one day suddenly in 1 minute 15gb traffic is arrived in the server. So, server will be not able to provide the services to the clients at that particular time. In the company firewall mechanism they capture the packet of the traffic which is arrived in the network at particular time interval.
So, using this pcap file analyzed the attack.

D. Analysis

For analysis we captured the traffic of that page using wireshark.
And we got some really important information from wireshark. For similar cases This is one of the techniques that can be helpful for investigating DOS/DDOS attacks.

1) Check the expert info of the wireshark. In this expert info you got duplicate ack tcp request.
2) Now in filter box type tcp and check the source IP address & Destination IP address.
3) After that select any tcp request and check in the tcp follow stream. In this stream we found the only browser detail which is the signature of slowloris attack. When we open the dos.pl file.. the code inin this file is same as the code, which is displayed in the "follow tcp stream". So, using this information we would conclude that, this was the slowloris attack.
4) We can assume the period of the attack using wireshark's IO graph.
5) Analysing the same pcap file in another interesting tool,network miner.we can find the host details like source IP address, sent packet details, etc.
6) Now analyze the sent packet in this tool and we got the details like source IP destination IP packet bytes, number of packets sent to that particular destination IP address etc.
7) Now we may check the session details. It shows the very important details time and date when the packet is sent between the client host and sever host. So, when any DOS/DDOS attack occurs, then this session details is used to check which time the bad tcp request was received.
8) After that we analyze the DNS timestamp, it was shows the starting time of the attack
9) The attacker may see the similar screen.

V. IMPLEMENTATION

The Cowrie Honeypot is a system designed to capture SSH and Telnet connections. Record the session information. These sort of honeypots is frequently associated with the Internet so as to screen the tools, contents and has being used by secret word speculating aggressors.
Cowrie is the new fork of the Kippo Honeypot. It has been refreshed with new highlights and gives imitating that record the session of an aggressor. With this session recording you can show signs of improvement comprehension of the aggressor's tools, tactics and procedures (TTPs). A term is expanding being utilized in Cyber Defence and Incident Response. Our setup will be exceptionally near a default establishment of Cowrie. The hosts SSH daemon tool will continue running on a high port (22222), Cowrie will continue running on 2222 and port 22 (default SSH) will be occupied to 2222 using ip-tables. So the SSH bot or aggressor will associate with port 22 be diverted to our honeypot on 2222.

1) *Step 01:* Install Cowrie on your machine.
2) *Step 02:* Now we will create a virtual environment for Python and Cowrie to run from.
3) *Step 03:* Next step is to activate the Python virtual environment and install the python packages that Cowrie needs to run.
4) *Step 04:* Editing the configuration file we will make a few changes from the defaults. Firstly I will change the hostname seen by a successful login by an attacker, keep it generic and non-obvious. Use vim or your favorite text editor to make these changes. The second change I will make is to enable telnet. SSH is enabled by default.

5) *Step 05:* As you can see in the configuration there are many options and things to play with, from logging and alerting to fake addresses and file downloads. Finally we are ready to start the daemon.
6) *Step 06:* From the Netstat we can see the SSH and Telnet daemons of our honeypot listening on 2222 and 2223 respectively.

Last step is to redirect traffic to 22 and 23 to the high ports 2222 and 2223 using IP-tables.

Now it is just a waiting game. However, due to the amount of SSH scanning that takes place on the Internet you will not have to wait long.

VI. CONCLUTION AND FUTURE WORK:

DoS/DDOS assaults are very best in class techniques for assaulting a system framework to make it unusable to real system clients. These assaults are an irritation at the very least, and on the off chance that they are against a basic framework, they can be seriously damaging. Loss of system assets costs cash, defers work, and cuts off correspondence between system clients. The negative impacts of a DOS/DDoS assault make it significant that arrangements and safety efforts be created to anticipate these sorts of assaults. Discovering strategies for counteracting and halting DOS/DDoS assaults will be significant for national security. Getting DOS/DDoS assaults and apparatuses is an initial move towards the system security world.

In this paper, we have recognised noxious web servers with our high association customer honeypot Capture-HPC. As a major aspect of future work, we might want to recognize malevolent web servers with our low collaboration customer honeypot HoneyC and think about the outcomes. We speculate that this correlation will give us experiences into the identification exactness, specifically bogus negatives, of every customer honeypot innovation.

Further, we might want to extend our exploration to customer side assaults that objective program modules just as non-program customer applications. The information we have gathered as a major aspect of this examination as of now demonstrates that program modules, for example, QuickTime and Winzip, are focused on. A more critical see program modules will enable us to evaluate the size of the issue. Notwithstanding program modules, we might want to assess the hazard to non-program applications, for example, Microsoft Office, Adobe Acrobat Reader, and so on. Numerous remote execution vulnerabilities have been freely revealed for these customer applications and it is suspected that they are likewise focused on. Our future research will decide the degree of the danger.

REFERENCES

[1] https://www.google.com/search?q=lifecycle+of+vapt&client=firefox-b-d&source=lnms&tbm=isch&sa=X&ved=0ahUKEwilz-WF9JDiAhWGbisKHZtQB74Q_AUIDigB&biw=1366&bih=654#imgrc=dvwRQiDBJSJjXM:
[2] https://searchsecurity.techtarget.com/definition/honey-pot
[3] https://searchsecurity.techtarget.com/definition/DOS