Vulnerability Assessment and Penetration Testing Tools Analysis and Implementation.

Author - Abhishek Soni,
Student of,
Cyber Security,
Vikrant Institute of technology & management, Indore, India

Guided by- Mr. Paras Bhanopiya,
Assistant professor,
Cyber Security,
Vikrant Institute of technology & management, Indore, India.

Abstract: penetration testing is a method of reaching a vulnerable system and web application. An attacker can take advantage of vulnerability can get access to the vulnerable system. An attacker can execute or generate the exploit for the vulnerable system or application. In the paper, we are an analysis of the penetration testing tools and also developing script (Tool) that can give the full access of any remote machine or victim machine. For penetration testing, we have a standard model which called open web Application security project (OWASP) top 10. Using this model we can do manual and automated penetration testing. OWASP top consists of the top 10 vulnerability like injection, broken authentication, broken access control, XSS, cross-site request forgery, misconfiguration, buffer over, etc. In the IT Organization, there are many tools which are available based on free and premium. Sometimes free tools also perform accurate result. So we analysis which tools we should use. We should use free or premium tools for assessment or penetration testing. Selecting the best tools it is also very difficult to work. Because for the same testing there are many or more tools available.

Index Terms: Penetration testing, vulnerability assessment, tools, injection, analysis, script, and premium. Cross site request forgery, misconfiguration, and authentication. Buffer over flow, injection, OWASP exploit, web application.

I. Introduction

In the last few years. The hacking activity becomes the most common. Mostly hacker targets the web application. That why securing the web site is most import. In today digital era every person using social networking, online banking, e-commerce site and also doing a small transaction (bill payment, money transfer, credit card payment) using online media. A number of cyber-attack is increasing day by day and todays. The attacker is being more or more powerfully. That's why security web application becomes more challenging.

Any loophole or vulnerability is the backdoor for the attacker. Vulnerability comes from the misconfiguration, error of software code, lack of knowledge in server configuration, and software development. An attacker can use that vulnerability for getting access to your web application/network

Vulnerability assessment and penetration is the process of finding the bug and loophole in any existing system like in web application, databases, network and so on. Vulnerability assessment and penetration both are different.

In the meaning of vulnerability assessment find loophole and misconfiguration, error in the system and web application but we are no exploiting that vulnerability. We are no hacking any system/ application just checking that vulnerability are existing or not in the system.

Penetration testing is the process of finding and exploiting the vulnerability with the owner permission. Using penetration testing attacker can hack and exploit the vulnerability in the system. Only for demonstrating purposes which through we can justify the web application is consisting the vulnerability.

In this paper, we are Analysis the most frequently used tools that tools today's hacker and penetration tester are using. In the paper, we analysis on web application penetration testing tools and network penetrating tools, database penetration testing tools, exploitation tools and we are developing the tools that through we can hack the victim machine with full access the without any antiviruses and defender detection.

II. WEB APPLICATION VULNERABILITY ANALYSIS.

Vulnerability is a flaw which allows an attacker to take access to the victim system and application, and the attacker can take the full access in the computer system and application which decrease the system's information guarantee. Vulnerability Assessment is a process which tests the security of interactive applications such as e-banking, news broadcast, and e-Commerce web applications. Web application penetration testing involves techniques leading to the identification of potential vulnerabilities, which may compromise web applications.

2.1 Comprehensive XSS

Cross-site scripting through an attacker can execute the javascript code in the browser. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to different end-use.

Types of XSS

a. Reflected XSS
b. Stored XSS
c. DOM-based XSS

How to Hunt/ exploit XSS

a. Find an Input Parameter, Give any input there. If your input reflects or stored anywhere there may be XSS
b. Try to execute any JavaScript code there, if you succeed to execute any JavaScript there then there is an XSS.
c. Exploitation of XSS

2.2 Host header injection

The programmer is taking the HTTP host header value and using it to create links, import script and even create a password reset links with its values this is a very critical idea because the HTTP host header can be controlled by an attacker. This can be exploited by applying web cache poisoning and by exploiting alternative channels like password reset email.

Type of Host Header Injection.

a. open redirection.
b. Cache poisoning.
c. Password reset poisoning.
d. XSS through Host Header.

How to hunt host header injection.

a. Web site Interceptions.
b. Using burp suite.
c. Need to change host value.

2.3 URL Redirection

URL redirection is used as part of a phishing attack.

How to hunt URL Redirection

a. Find any URL parameter having some kind of tendency to redirect anywhere
.
b. The common parameter list (dest redirect, uri path, continue url, window to out , view dir, show navigation , Open url, file Val validate domain, callback return , page feed, host port next ,data reference site html)

How to Hunt URL Redirection.

a. URL-Redirection through-Get parameter.
b. URL Redirection on Path Fragments.

2.4 Parameter Tempering

The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

Background Concept about Parameter Tampering

a. The parameter modification of form fields can be considered a typical example of Web Parameter Tampering attack. For example, consider a user who can select form field values (combo box, checkbox, etc.) on an application page. When these values are submitted by the user, they could be acquired and arbitrarily manipulated by an attacker.

2.5 HTML injection.

HTML injection is a type of injection issue that occurs when a user can control an input point and can inject arbitrary HTML code into a vulnerable web page.

Impact of HTML Injection.

a. It can allow the attacker to modify the page.
b. DOM can be load there.

HTML Injection Finding.

a. find an input parameter Either get based or POST based.
b. If your input reflects your web page there may by HTML
c. Execute any HTML code if you succeed to execute any HTML code there. Then there us HTML.

2.6 File Inclusion Vulnerability.

Vulnerable code that allows executing the file in the server. User can submit their file using the input box form and file input box. There are two types of file inclusion remote file inclusion and local file inclusion

Impact of file inclusion vulnerability.

a. An attacker can control the web application server
b. An attacker can execute a malicious file in the victim computer system.

Finding File inclusion vulnerability.

a. Finding the parameter like [file, document, folder, root, path, pg, style, pdf, template, PHP _path, doc]
b. Also like [dest, redirect, uri, path, continue, url, window, next, data, reference, site , html, val, validate, domain, callback, return, page, feed, host, port, to ,out, view, dir, show, navigation, open]

2.7 Missing SPF Record.

Sender policy framework or SPF, its help to sender and receiver to verify the email receiving from a trusted source or not. It also verifies the spam, spoofing and phishing email.

Impact of Missing SPF record.

a. The attack can use any fake mailer to forge the mail into any person using the vulnerable domain

How to Hunt of Missing SPF record.

a. Using mxtoolbox.com be can find the web site that does not consist of the SPF record.

2.8 Source code disclosure.

Server-side code often contains sensitive information like database information the associate function. If source code has in the attacker than an attacker can take some advance action for hacking the web application. If the site is vulnerable with source code disclosure vulnerability than the attacker can view the source code the web application.

Impact of Source code disclosure.

a. The attack can use any fake mailer to forge the mail into any person using the vulnerable domain

How to hunt source code Disclosure.

a. Using response header using Burp suite.
b. GET / abc.php?file=login.php HTTP/1.1

2.9 Cross-site Request forgery.

CSRF is an attacker and forces the user where the user is already authenticated. Where the attacker forces the user to execute some unwanted action to the authenticated web page.

Impact of Cross-site request forgery.

a. The victim shows some unwanted message on the screen

How to hunt source code Disclosure.

a. Write HTML code in the text editor
b. Open this code with browser.

2.10 SQL injection.

An attacker can directory interact with the web application database take advance of no filter mechanism applied on an HTML page. We have many types of SQL injection like SQLI may be union based, error-based, double query injection, blind Boolean based, and blind time-based.

Impact of SQL injection

a. An attacker can take over access to web application
b. Without username password attacker can login on the web site

How to hunt SQL injection.

a. Passing sql query on the login page.

III. METHOD OF PENETRATION TESTING.

3.1 External Testing.

External penetration testing is a method of penetrating to the network and finding the information that is existing for the www (world wild web). And any person can find this information using the internet. Using external penetration testing attacker can find all information that exists in WAN (world wild web) network.

3.2 Internal penetration testing

The user gets the access of intranet and they try to simulate many attackers if any internal hacking or frustrated employee want to try to hack there internal server then it's helpful for the organization to find. Internal vulnerability in the network.

3.3 Blind testing.

Attacker or penetration tester knows only the organization name and they will Tester are don't know about their server or any technical information about an organization

3.4 Type of penetration testing

Manual penetration testing: In the manual penetration testing, penetration tester find and perform the testing without automation tools

Manual testing

a. SQL Injection
b. XSS
c. Directory traverse
d. File uploading
e. Browser cache weakness

Automation penetration testing- security analysist perform penetration testing using automation tools that can find vulnerability assessment using automatically.

Automated testing

a. SQL injection
b. XSS
c. Directory traverse
d. File uploading
e. Clickjacking
f. Cross-site request forgery

IV. VULNERABILITY ASSESSMENT TOOLS ANALYSIS AND IMPLEMENTATION.

4.1 SQLMAP

SQLMAP is an open-source tool for penetration testing that performs automated penetration testing and also responsible for detecting the backend database. SQL map was responsible for exploiting SQL injection on the web application.

Feature of SQLMAP

a. Support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP, Informix, HSQLDB and H2 database systems.
b. Its support the Boolean-based, error baes, Time based, UNION query-based Injection.

c. It’s able to pass query without passing SQL injection query and provide the DMBS credential, IP address, database name, Port number.
d. It’s can perform enumerate users, password databases, tables, column.
e. Support user privilege escalation using Meta exploit Meterpreter

4.2 Nessus

Nessus is a closed source / proprietary vulnerability scanner. It's developed by tenable Nessus cover/ scan the wide range of vulnerability assessment like operating system, network devices, Hyper visions, databases, web server, and more critical infrastructure vulnerability.

Feature of Nessus
a. Supported by multiple platforms.
b. Tenable publishes the new plugin in each week.
c. Update plugin within 24 hours of vulnerability disclosure.
d. We can import in vulnerability scanning result in many formats like Txt, XML, HTML, etc.
e. It also detects common password.

4.3 Wire shark

Wireshark is a packet analyzer. It is used for troubleshooting network, analysis the communication using packet capturing. The real name of Wireshark is Ethereal, but its rename the project and give the new name Wireshark.

Feature of Wireshark
a. It’s a free packet analyzer
b. Support by many different platforms
c. Its filter the packet bases of many IP header parameters
d. Its support of VoIP traffic detection.
e. Support the various filtering parameter for finding the specific packet from the captured data.

4.5 Burp Suite

Burp Suite is a graphical tool. Which is responsible for testing web application security. It checks the comprehensive web application security check. With the additional functionally such as a proxy server, scanner and intruder and also have the advanced tools as a spider, repeater, decode, comparer an extended and sequence.

Feature of burp suite
a. It’s come with two editions, community edition, and professional edition.
b. Main used for Manual testing
c. We can perform the brut forcing using burps suit
d. It’s also used as a proxy in the network
e. Supported by many platforms.

4.6 Hydra

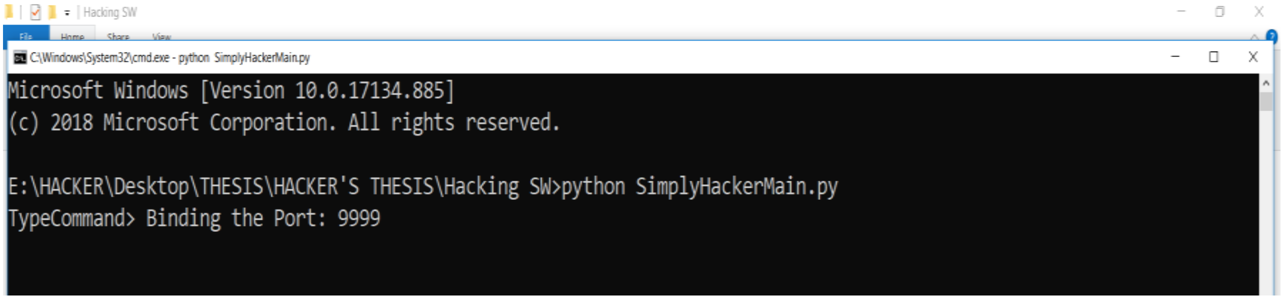
The Hydra does a smart system login password hacking tool. When it is compared and other similar devices, it explains why it is faster. New modules are anything but hard to include in the instrument. You can externally much of a stretch add modules and enhance the highlights. Hydra is accessible for Windows, Linux, Free BSD, and Solaris. The instrument supports different system rules, As of now, it supports Asterisk, telnet, ssh (v1,v2), VNC , VMware-Auth, TeamSpeak, SMB, SMTP, SMTP Enum, Exec Rlogin, IRC, HTTPS-FORM-POST, HTTP-HEAD, HTTP-Proxy , ICQ, HTTP-GET, AFP, Cisco Auth, Cisco empower, CVS, Firebird, FTP, Oracle.

Feature of Hydra
a. Hydra is a best and faster brut forcing tools
b. Support multiple protocols
c. Supported by the multiple Operating systems

4.7 Simply hacker

Simply hacker is a small tool that through attacker can hacker and take over access the full access of computer system or any server just executing the simple scripting on the victim computer system. No antivirus and defender can detect this script.

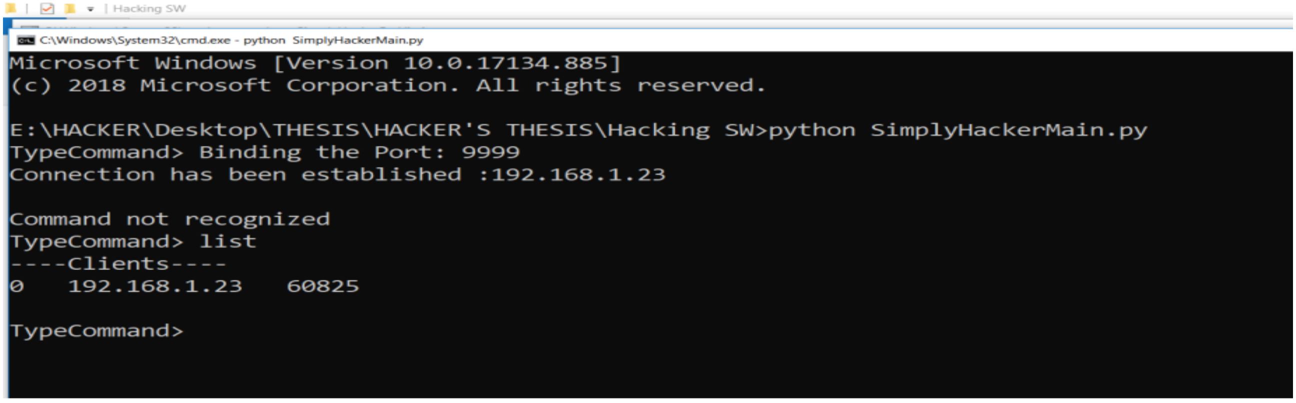
How simply hacker tools are work this developed in python socket programming which through this computer can give the full control of the victim computer system.



```
Microsoft Windows [Version 10.0.17134.885]
(c) 2018 Microsoft Corporation. All rights reserved.

E:\HACKER\Desktop\THESIS\HACKER'S THESIS\Hacking SW>python SimplyHackerMain.py
TypeCommand> Binding the Port: 9999
```

Fig 4.1



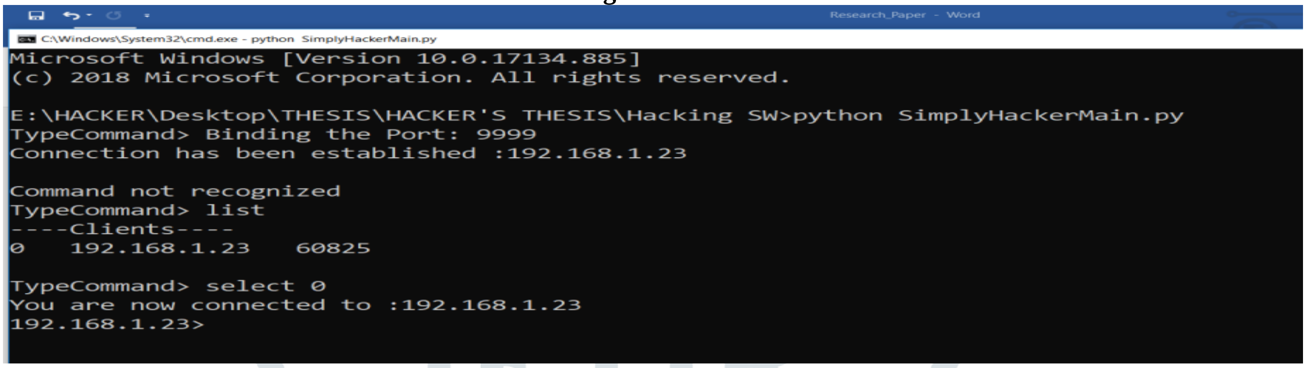
```
Microsoft Windows [Version 10.0.17134.885]
(c) 2018 Microsoft Corporation. All rights reserved.

E:\HACKER\Desktop\THESIS\HACKER'S THESIS\Hacking SW>python SimplyHackerMain.py
TypeCommand> Binding the Port: 9999
Connection has been established :192.168.1.23

Command not recognized
TypeCommand> list
----Clients----
0   192.168.1.23   60825

TypeCommand>
```

Fig 4.2



```
Microsoft Windows [Version 10.0.17134.885]
(c) 2018 Microsoft Corporation. All rights reserved.

E:\HACKER\Desktop\THESIS\HACKER'S THESIS\Hacking SW>python SimplyHackerMain.py
TypeCommand> Binding the Port: 9999
Connection has been established :192.168.1.23

Command not recognized
TypeCommand> list
----Clients----
0   192.168.1.23   60825

TypeCommand> select 0
You are now connected to :192.168.1.23
192.168.1.23>
```

Fig 4.3

Future work in simply hacker**.**
We can make them too much advance just sending the message on the computer system should be a hacker or give the full control of the victim computer system. It's possible.

The merit of Simply hacker.
a. Making the hacking too simple.
b. No antivirus detection.
c. No Defender can detect.
d. Easy to use.
e. Giving full access to the victim computer.
f. Can also use for remote administration

The demerit of simply hacker
a. Cannot Able to hacker computer without executing the exploit file.

V. RESULTS

5.1 Results

Feature | Tools	**Burp suit**	**SQLMAP**	**Nessus**	**Wire shark**	**hydra**	**Simply hacker**
Availability	Paid/free	Free	Paid	Free	Free	Free
Work	Manual web application testing	Testing only SQL Injection	Network /Web application Testing	Packet Analyser	Brute force attack	For Remote Access
Penetration testing	Yes	Yes	Yes	No	Yes	No
Manual testing	Yes	No	No	No	No	No
Scanning	Yes	Yes	Yes	No	No	No

Vulnerability /Assessment	Yes	Yes	Yes	No	No	No

VI. CONCLUSION

In this above discussion section. We discussed the Penetration testing tools and top attack in today IT field. The attacker becomes the more sophisticated so companies must educate themselves about the thread and how to defend against. The thread that through attacker can take access of their computer system and application. Penetration testing is most important to secure the system and application. In an insecure manner of web application outcome affect application availability or breaking of data confidential and reliability.

In this experiment, we have performed penetration testing and vulnerability assessment using manual and automated tools. Penetration tester performs testing on the application like a hacker and tries to find vulnerability on the application. Also, the tester uses the manual method of testing the application and try to find possible vulnerable on the application. We have a discussion about vulnerability like SQL injection, Cross-site scripting, file uploading, Directory traverse, cross-site request forgery, command injection, source code disclosure, critical file found, cross-origin resource sharing, missing SPF record, file inclusion vulnerability, HTML injection, HTML injection. We also used automated scanning tools that can find a vulnerability and generate the result.

In this proposal, we are trying to demonstrate the impotence of vulnerability analysis and penetration testing. If we try to aware of that vulnerability then the application can become more secure. And become the more available for the uses.

REFERENCES

[1] Prof. Sangeeta Mumbai India, “Vulnerability Assessment and Penetration Testing of Web Application" 2017 Third International Conference on Computing, Communication, Control And Automation (ICCUBEA).

[2.] Sandhya S, Assistant Professor, "Assessment of Website Security by Penetration Testing Using Wireshark" 2017 International Conference on Advanced Computing and Communication Systems (ICACCS -2017), Jan. 06 – 07, 2017, Coimbatore, INDIA

[3.] Jai Narayan Goel, "Ensemble Based Approach to Increase Vulnerability Assessment and Penetration Testing Accuracy", 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016).

[4.] Abdullah Ahmed Ali "Security Assessment of Libyan Government Websites"

[5.] Abdulrahman Alzahrani, "Web Application Security Tools Analysis 2017", IEEE 3rd International Conference on Big Data Security on Cloud

[6.] OWASP TOP 10-2017, The Ten most Critical Web application Security Risk
[7.] https://owasp.org.
[8.] https://www.Kali.org
[9.] https://www.wireshark.org
[10.] https://en.wikipedia.org › wiki › Password_cracking
[11.] https://www.veracode.com › directory › owasp-top-10
[12.] https://www.owasp.org › index.php › Top_10_2007
[13.] https://www.owasp.org › index.php › Category:OWASP_Top_Ten_2013_Pr
[14.] https://www.researchgate.net › publication › 329609399_Cyber_Security
[15.] https://www.researchgate.net › publication › 283180137_Systematic_Review
[16] https://www.researchgate.net › publication › 220846451_Evaluation_of_we
[17] https://thehackernews.com › search › label › Web Application Security
[18] https://en.wikipedia.org › wiki › Hacker
[19] https://www.springer.com › computer-science › security-cryptology
[20] https://blog.feedspot.com › hacker_blogs