Vulnerability Assessment of Web Servers using Honey Pots: Perspectives, Ethical Issues, Legal Implications

Seema Verma
[Reader] Associate Professor
Dept. of Electronics
Banasthali University, Rajasthan

Tanya Singh
Assistant Professor
Amity Institute of Information Technology, AUUP, NOIDA

ABSTRACT

With the growth of attacks and hacking activities, the organizations are becoming more security conscience. The scope has changed from technical problem to a business problem within an organization. High cost is incurred to implement security policy and procedures and is viewed as an investment. However, in the quest of getting secure, the organizations hastily employ hackers to exploit the vulnerability of their system. This paper is an attempt to identify the ethical problems and legal implications associated with such act and the care to be taken before employing any outsider or insider who can break into the network and find its weaknesses. If these issues are not addressed before the implementation and deployment of the given security policies and procedures, the organizations can land themselves in serious legal actions which they may repent later.

General terms

Web Server Vulnerability Assessment; Ethical Issues; Cyber Laws

Keywords

Log Monitoring; Risk Analysis; Legal Implications

1. INTRODUCTION

The prospect of vulnerability assessment of any web server, ethical and legal implications remains remote and unexplored. The issue has been discussed more as topic of panel discussion but the mindset is still not mature enough to accept to what extent the webserver is exposed to the threat from hackers, insiders and even security auditors [1].

Several analyses have been done on how to protect the web server and its related network infrastructure. There is a lot of literature regarding how efficiently any webserver can be secured. The three major verticals to secure any enterprise are Effective Network Planning and Design i.e. Defence in Depth approach, Firewalls to protect any malformed packets entering the system, Routers, deployed at the gateway of Internet, have access list implied on them [3]. However, a little has been discussed on the perspectives, ethical issues and legal implications of vulnerability assessment of web servers in general. With the use of honeypots as one of the tool to protect any web server, this problem simply aggravates and magnifies if proper measures are not adopted at the time of implementation and deployment of the web server.All the vital information about any enterprise is hosted on the Web Server. These host applications are accessible by anyone on the internet. Several security measures are taken by the organization to protect the vital information. One way to secure the network is Firewall. It is implemented at the door of the internet. These firewalls generally allow web-traffic through port 80 and 443 as they are treated friendly. Besides this the organizations also, implement the Intrusion Detection and Prevention system. Despite of these measures, many hackers still intrude into the system by finding vulnerabilities into the system [2].

It has been observed that if a hacker or intruder would like to intrude into a system, no security procedures, policy or technologies could stop him from entering the network. As the technology is changing at a faster pace [7], even before a method is devised to respond to a given vulnerability, threat or attack, the hackers may use the same technology to attack the network. Since new vulnerabilities are discovered on a daily basis, the organizations need to be more alert and must make security a priority and continue to stay current with security patches. The policies and procedures need to be updated as and when necessary. The current challenge is to internally look for any loopholes in the web server accessed by either external world or internal network and find solutions to it so that we can protect and safeguard the image of the system.

For any security system to be successful, a number of factors are equally responsible. They are:

1) Effective daily monitoring and surveillance of log files
2) The skill and expertise of system administrator responsible for the protection of the entire network and devices.
3) The timely audit for assessment of any vulnerability and the ability to patch and update the services and kernels quickly and efficiently.
4) Hiring the services of highly skilled security specialist to attempt to ‘break in’ to the network and the related systems to determine what vulnerabilities are present [8].

This paper is written with the aim to highlight the issue of growing security perspectives, ethical issues associated with it and legal implications which should be kept in mind while implementing any security measures. It also highlights the pros and cons of employing a hacker for vulnerability assessment or penetration testing. There is a need to understand that any decision taken to implement any security policy and procedure may have bounce-back effect. No decision should be taken by the security administrator in haste as these decisions may hamper the image of the organization in the long run.

2. VULNERABILITY ASSESSMENT AND RISK CATEGORIZATION

Vulnerability Assessment can be defined as the assessment of the network infrastructure design, implementation, operation, management and finding its weak areas. If these weak areas are not identified by the system administrator or security administrator, any intruder or hacker can intrude inside the system and can cause damage to the system. Assessment of Vulnerability is therefore, very important from the point of view of building a good immune system.

The users' visit the web servers either through clicking on the hyperlink or keying the site's URL directly into the address bar of a browser. The websites which are hosted on these web servers are subject to various attacks. These attacks are result of various operational security risks which can be classified as [2][6]:

a) Actions of people
b) Systems and technology failure
c) Failed internal process
d) External events

The security policy implemented inside the organization usually amounts to total trust of the insiders and the total mistrust of outsiders. The people inside the firewall have access to the internal site which contains the sensitive data such as company strategy, business plans etc. They upload personal information such as their profile, work profile, personal profile, images, certificates of merit etc. for the information to be viewed and accessed by internal management for specific jobs as and when required. The latter is protected by simple passwords on the top of SSL connections. Access to the web server through the internal employess can cause serious threat and should be always be taken care of as a risk [10].

According to the CERT statistics, the total vulnerability catalogued has increased from 171 in the year 1995 to 1090 in the year 2000 to 6058 in the year 2008. This figure is growing everyday as new vulnerabilities are discovered every day [14].

The various attacks that the web server is exposed to could be many but an attempt has been made to categorize them as follows [2][4]:

1) SQL Injection (Risk High)
2) Remote code execution (Risk High)
3) Format string vulnerabilities (Risk High)
4) Cross site scripting (Risk High)
5) Username enumeration (Risk moderate)
6) Cookie poisoning (Risk moderate)
7) Errors triggering sensitive information (Risk moderate)
8) Weak session management (Risk Low)
9) Hidden field manipulation (Risk Low)
10) Server misconfiguration (Risk Low)

The monitoring of logs of the web server has an important role to play in risk mitigation. These logs can classify the attacks and can generate the alerts. The system administrator or a security administrator should be a skilled person who by reading the logs can identify which logs are critical. In this case, the role of auditor also plays an important role. While auditing the vulnerability of any web server, it is required that the detailed policies and procedures should be followed with the aim to find fault in an exhaustive manner. Also, there is a need to hire the security person who can actually 'break into' the system and find the weak areas.

The flowchart as proposed in Fig. 1 (attached in Appendix I) signifies the process of assessment of vulnerability by viewing the log monitor and its risk categorization.

Due to this categorization, we can have alerts generated on the screen monitor of the system administrator with the colour mapping of Red, Yellow, Blue and Green. The table below shows the mapping of each attack and its colour code generated.

Table 1: Categorize the various risk and the action plan associated with each.

S. No.	Colour	Alert Mechanism
1.	Red	The various countermeasures enlisted to mitigate the risk of attack on the web server and its data should be immediately look into and implemented. The part of the network should be detached from the entire network.
2.	Yellow	As this risk is moderate, there is no need of immediate action but the implementation to counter it should be planned in the near future.
3.	Blue	These risks are Low. However, an eye should be kept on it so that it should not escalate to very high category. Countermeasure implementation can be done in the near future.
4.	Green	The system is healthy.

In the above mentioned points, it becomes very necessary that precaution should be taken while hiring a security person who has been given rights to break into the system. And from this moment to take a decision to hire a security person (also known as pen tester) is the moment when the ethical issues just features in. In the coming sections, the focus is on the pros and cons of hiring a pen tester and the legal issues which needs to be taken care of before implementing the system.

3.0 VULNERABILITY ASSESMENT OF A WEB SERVER: ETHICAL ISSUES

With the growing attacks, organizations are hiring security professionals who can breach their network. These people are termed as Crackers or Pen Testers. They differ from the Hackers in that they only probe a network, instead of exploiting the network and it has been observed that the common mistake which the security administrators repeat again and again, is trusting them with the secrets of the networks. This trust on them makes our own network exposed and vulnerable to them.

Some of the issues which should be kept in mind while employing a security person from outside are:

1. Has the background of the security person been checked? Is he a starter, script kiddie, a hacker in the past or experienced cracker with good track record? The situation may arise that he may be a hacker and should not go by book and may not list the entire test, that he has performed on the network. The extreme could be that during the entire process when he was breaking into the network, he could have created back door so that any other hacker can enter the network later.

2. Is he belonging to an organization with name, fame and experience in this field? Has this job been given to the organization only once or is it in contract for a period of duration? If the job has been given to the person for a long duration, the person may actually bring forth the real issue. If the job has been given only for once as a try, there may be chances that not all weaknesses are spoken to the organization, a few weaknesses are not shared deliberately and are kept with these testers/ professionals.

3. Has the 'Code of Conduct' been signed? This is very important on the part of organization. The organization is sharing all sensitive information with an individual.

4. Since the network is designed not with proper plans but as per the increasing requirement, there is a need to understand the network infrastructure both at the design level and at the implementation level. Due to increase in the networks, there are design problems that remain dormant but can make the entire infrastructure weak. Is the person employed for this job has the competence and knowledge of the network management and design for the same?

5. Has the Operational Perspective, Design Perspective, Control and Monitoring perspective kept in mind while designing the methodology, the methodology followed by any hacker to breach into the network? Or, the organization have only allowed the professional individual to enter the network without cross-checking with them the Standard of Procedures followed by the tester/professional to assess vulnerability? Is the finding given by the tester/ professional superficial?

6. Has the scope of the project been defined? Is the professional hired understands to his best the clients' business objectives, associated risks and security controls. It could be that if the scope of the project has not been identified, the vulnerability assessment may not be completed on time and the organizations expectations are not fully met

7. Has the Individual quarantined the IP address on which the web server is hosted with other IP address. While performing vulnerability test, the tester may affect other servers that are out of scope and may cause harm to the other IP addresses.

8. Has proper permission been taken by the competent authority to perform the test on the web server? As web server contains extremely sensitive data depending upon the type of their business, the permission plays a major role in any test performed. In case of any data loss, the organization is prepared with another duplicated set of data.

9. Has the time and date of testing been circulated to all parties in the network infrastructure hosting web server such as Incident Response Team, NOC, Web Server Administrator? In case it is not done, they may be unnecessary bothered with the alarms that are generated.

10. A professional who have been given the access to the network should be given a temporary username and temporary password only till the time, he remains in the network.

11. The Professionals employed for the purpose of performing vulnerability assessment should have complete knowledge of patch management, server configuration management, log monitoring, incident response controls, its monitoring, and effective review of patch for testing the criticality and if the entire review has been properly documented.

12. Are the tools used by the professional licensed or free versions have been downloaded for testing. Many a times, the tools which are freely downloaded creates a trigger that remains dormant for some amount of time but by chance when activated due to some trigger can erase many confidential information that may have been of significant importance to the users.

4.0 THE PROS AND CONS FOR SECURING WEBSERVERS USING HONEYPOT

The web server can also be secured using honey pot [2]. The given model was proposed and tested for alarms. The questions discussed in section 3 regarding ethical issues are the result of the experiences that have occurred during the implementation. The real scenario could be worse if proper care is not taken while implementing any policy, procedures and Honeypot. In the next section, the legal implications for testing any web server have been discussed. The problem is more acute when honeypot is applied as a tool to monitor malicious activity.

4.1 Legal Implications

During the time of deployment of such a model, it is very important that security administrator must think like an attacker who will first map the web server, analyze the system configuration and then identify the loopholes inside the system. The serious concern is when honey pot is deployed; the administrator remains casual. He is only interested in deployment of honeypot and the good result it will fetch. Some of the odd circumstances that may occur are:

a) Network operators monitoring the activities of system users.
b) Research honeypot that detects improper activity and action plan in such a case
c) If the same honeypot which was used to monitor malicious users have been compromised and used as a launch pad for any attack.

Before implementing and deploying honeypot, the counsel within the organization and also outside, should be consulted. The counsel take into account a particular situation, will give suggestions on goals, regulations, state laws, local laws and help identify the future upcoming problems and solutions. There is a need to have a proper plan of action inline with the aim to deal with the criminal conduct before hosting it live [9].

In India, the above mentioned three cases are liable to Legal laws , IT Act 2000 Sec 66. It may cause imprisonment for the period upto three years and fine upto 2 lakhs may be charged from the person who has been charged guilty of misusing the computer under computer fraud and abuse act. In US, as per cyber security enhancement 2002, there could be a life sentence to a hacker who 'recklessly' endangers the lives of others [11] [12] [13]. There are many clauses which need to revisit while setting up any web server to avoid legal issues.

All the laws of various countries should be known to the hired professionals as well as organizations, if organization is working at a global domain. There are some countries where computer crime is dealt using existing laws as these countries may not be having specific computer laws [12].

4.2 Suggestions

For a professional who is testing the security of any organization, the scope of testing should be documented in writing. The organization should ask for clarification if required. For a security professional who is hired to test the web server and its related infrastructure should seek in writing the permission from the owner of the organization. If some of the processes are outsourced to a third party, their consent is equally required before the testing takes place to avoid any legal battle.

It is necessary to identify the issues, conduct an initial study of the website etc. The knowledge of relevant laws and statues of the particular country should be determined to host a web server in a given country where it is registered.

The Indian IT law is at a very premature stage and not every illegal activity are registered. There is a strong need to grow security awareness in India and most of the incidences of computer crime go unnoticed.

Care should be taken that if any confidential information is not complied with the data protection laws, it can attract legal penalties and sanctions. Hence, legal agreements such as non- disclosure agreements and confidential agreements need to be executed between the hired professional (an insider or an outsider) and the organization.

5.0 CONCLUSION:

This paper is an attempt to bring together the various issues related to the vulnerability assessment of any webserver, the ethical issues related to it which we just ignore while performing any assessment. The legal implications had also been mentioned in great detail. Generally, we find too many literatures on how to secure any network. However, with the growing number of attacks, there is a need to address these technology perspectives, ethical issues and its legal implications at great length in parallel to the measures implemented to secure any network. It may happen that any decision taken in haste to secure a webserver and its related infrastructure can lead to a disaster in long run of time.

6.0 REFERNCES

[1] Susan C., "Vulnerability Assessment", SANS Institute Reading Room Site, July 6, 2001, Version 1.2e

[2] Verma, S., Singh, T. 2012. Automated Multilevel Defence Model to Investigate Packets for Web Interface. 9th International Conference on Wireless and Optical Communications Networks

[3] Verma, S. , Singh, T. 2011. Multilevel Defence Model to Secure Large organizations using Effective Network Management Strategy and Honey pots. 3rd International conference on future computer and Communications, 231-236

[4] Shah S. 2002. Top Ten Web Attacks, Net –Square, Singapore

[5] Derek Cheng D. 2004 .Web Server Security Assessment: An Independent Auditor's Perspective. GIAC Practical Repository. SANS Audit.

[6] Vachon, R. G. 2008. Accessing the Wan, 190- 298. Pearson Education

[7] Cebula, J. J., Young, L. 2010. A Taxonomy of Operational Cyber Security Risks, Software Engineering Institute, Carnegie Melon

[8] Xynos, K. , Sutherland, I. , Read, H., Everitt, E., Blyth, A. 2010. Penetration Testing and Vulnerability Assessments: A professional Approach. Ist International Cyber Resilience Conference. Edith Cowan University. Australia

[9] Spitzner, L., Chapter 8. Know Your Enemy. Addison Wesley, 225- 253

[10] Gilmore C., Kormann D., Rubin A. D. 1999. Secure Remote Access to an Internal Web Server. AT& T Labs IEEE Network: The Magazine of Global Internetworking. NJ,USA. Volume 13 Issue 6, November 1999, 31-37

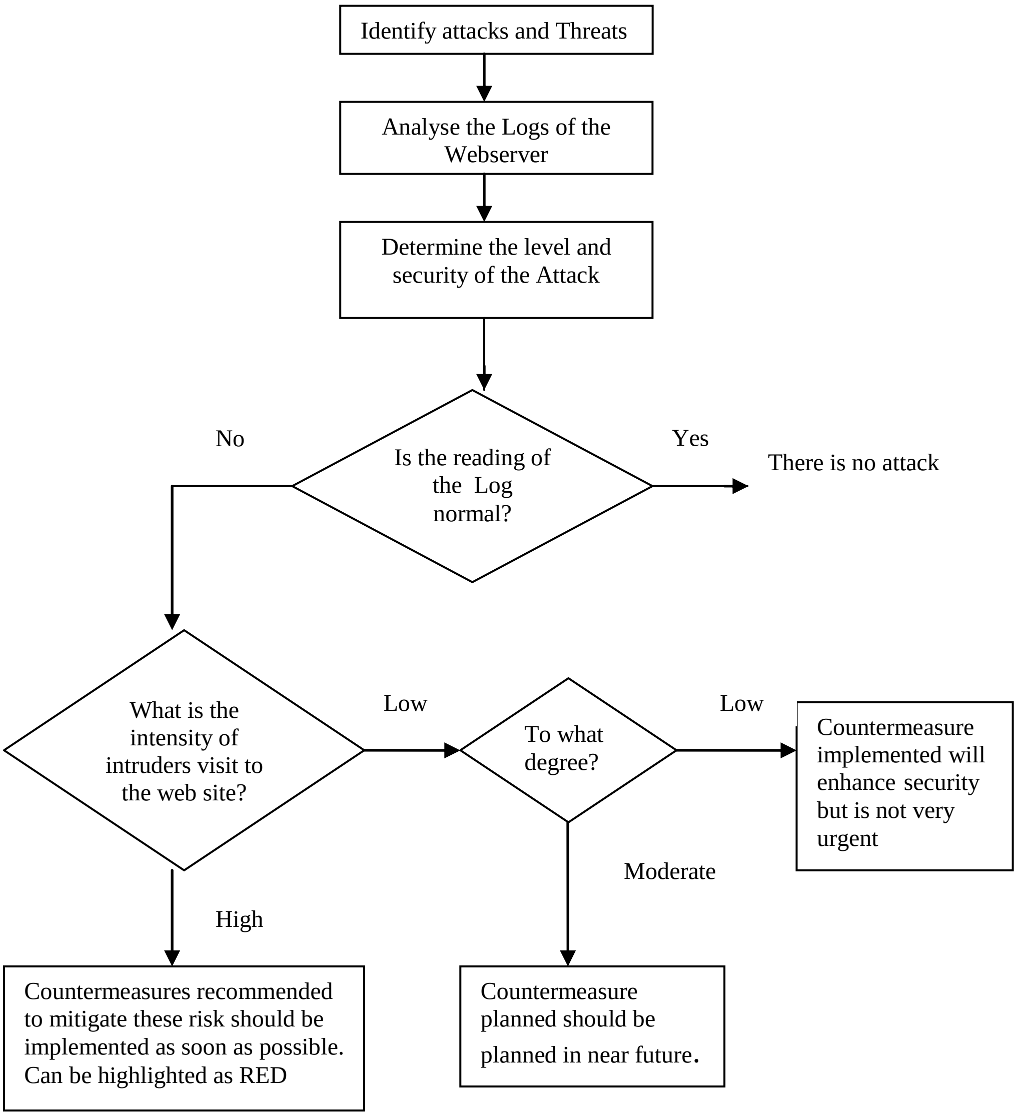
[11] Web Legal Audit, http://www.bizandlegis.com/casestudy/web-legal-audit.html

[12] Cyber Forensics in India, March2, 2013, http://cyberforensicsofindia.blogspot.in/2013/03/regulations-and-guidelines-for.html

[13] Information Technology Act 2000 http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/itbill2000.pdf

[14] CERT statistics (Historical), Software Engineering Institute, Carnegie Mellon, http://www.cert.org/stats/

Appendix I


Identify attacks and Threats
Analyse the Logs of the Webserver
Determine the level and security of the Attack
Is the reading of the Log normal?
No
Yes
There is no attack
What is the intensity of intruders visit to the web site?
Low
To what degree?
Low
Countermeasure implemented will enhance security but is not very urgent
Moderate
High
Countermeasures recommended to mitigate these risk should be implemented as soon as possible. Can be highlighted as RED
Countermeasure planned should be planned in near future.