Analysis of Penetration Testing and Vulnerability Assessments with New Professional Approach

[1]Azhar Ali, [2]Dr. Mohd. Rizwan Beg, [3]Shish Ahmad, [4]Arshad Ali
[1,2,3,4]Dept. of C.S.E/IT, Integral University, Lucknow, Uttar Pradesh, India

Abstract
In today's modern era crucial company information is accessed, stored, and transferred electronically. The security of this information and the systems storing this information are critical to the reputation and prosperity of companies. Therefore, vulnerability assessment of computer systems to obtain a complete evaluation of the security risks of the systems under investigation. In current era there is more complex enterprise IT infrastructures consist of hundreds or thousands of systems. Each component of these infrastructures is meticulously configured and integrated into complex systems architecture. Professional IT staffs are responsible for securely establishing and maintaining these IT infra structures are assessing, on an ongoing basis, the real risks presented by system vulnerabilities. Attacks against computer systems and the data contained within these systems are becoming increasingly frequent and evermore sophisticated. Advanced Persistent Threats (APTs) can lead to ex filtration of data over extended periods. Organizations wishing to ensure security of their systems may look towards adopting appropriate measures to protect themselves against potential security breaches. One such measure is to hire the services of penetration testers (or "pen-tester") to find vulnerabilities present in the organization's network, and provide recommendations as to how best to mitigate such risks. This paper discusses the definition and role of the modern pen-tester and summarizes current standards and professional qualifications. The paper further identifies issues arising from pen-testers, highlighting differences from what is generally expected of their role in industry to what is demanded by professional qualifications. In this paper we can analysis of The paper further identifies issues arising from pen-testers, highlighting differences from what is generally expected of their role in industry to what is demanded by professional qualifications. In this paper we provide an overview of penetration testing, discuss security vulnerabilities, and summarize the results and benefits of penetration testing realized by the IT executives interviewed.

Keywords
Penetration Testing, Pen Tester, Cyber Security, Vulnerability Assessments, Risks, Attacks.

I. Introduction

There are two types of penetration:

1. Internal

This testing is often performed from different network access points that include both the physical and logical segments; this provides a more detailed view of the security.

2. External

This testing has its focus on the infrastructure components, servers, and the related software of the target. It also provides a detailed analysis of the information that is available from public sources, such as the Internet. Enumeration of the network is also performed and analyzed. The filtering devices, such as firewalls and routers, are also scrutinized for their vulnerabilities. Finally, the impact and consequences are accessed.
The two types of penetration have three variations, each depending on the degree of knowledge provided by the target company to the pen testing team.

3. Black Box

This testing does not provide the tester with any information and therefore is a much better testing method because crackers and script kiddies normally do not have any information that is directly obtained from the target company and need to gather their information from public sources. It simulates real-world attack scenarios. The steps of mapping the network, enumerating shares and services, and operating system fingerprinting are typical for black box testing.

4. White Box

For this, related information is provided and is done so to assess the security against specific attacks or specific targets. This is the chosen method when the company needs to get a complete audit of its security.

5. Grey Box

In this testing, some knowledge is provided to the testers but this testing puts the tester in a privileged position. This would normally be a preferred method when cost is a factor as it saves time for the pen testing team to uncover information that is publicly available. Also, this approach would be suitable when the organization needs to obtain knowledge of the security assessment practices.

A. Methods of Penetration

We have two choices when it comes to getting penetration done. However, we will describe the details of the manual alternative for this paper because this would be the preferred method in providing a nonbiased report that might be necessary to meet legal regulations.

1. Automatic

The automatic penetration is often chosen when cost is a key factor. Due to the free software availability of many penetration tools, a company could choose to have the penetration performed by this method. Also, commercial tools that could be used have a cost associated with them; however, this tool cost could be spread out and would still be a less costly solution than manual penetration.
However, the learning curve for each penetration tool is usually much higher, and the knowledge required and experience in doing such work demands the skills of an expert.

2. Manual

Manual penetration is usually chosen to give an independent assessment of the penetration. Normally an external company that is experienced in the field and does it on a regular basis, with a good track record, is chosen. Regulation requirements could make this the only alternative a company has.

C. Vulnerability Assessment

A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed include, but are not limited to information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems. Such assessments may be conducted on behalf of a range of different organizations, from small businesses up to large regional infrastructures. IT infrastructures are assessing, on an ongoing basis, the real risks presented by system vulnerabilities. The task of correctly assessing the real security risks associated with a seemingly endless stream of vulnerability and patching reports is a critical and time-consuming activity for IT staffs. However IT professionals understand that despite their best efforts, vulnerabilities may still present significant security risks for their companies. During research and in-depth interviews, IDC found compelling reasons why IT executives and team members must adopt penetration testing as an integral part of their security and vulnerability management (SVM) processes and programs. Penetration testing enables users to:

D. Intelligently Manage Vulnerabilities

Penetration testing provides detailed information on actual, exploitable security threats. By performing a penetration test, an organization can identify which vulnerabilities are critical, which are insignificant, and which are false positives.

E. Avoid the cost of Network Downtime

Recovering from a security breach can cost millions due to IT remediation efforts, lost employee productivity, and lost revenue. Penetration testing allows an organization to prevent this financial drain by identifying and addressing risks before security breaches occur.

F. Preserve Corporate Image and Customer Loyalty

Even a single incident of compromised customer data can be costly. Penetration testing helps an organization avoid data incidents that put its goodwill and reputation at risk.

G. Justify Security Investments

Penetration testing can both evaluate the effectiveness of existing security products and build the case for proposed Investments.

H. The role of Penetration Testers

The role of a penetration tester is similar to that of a hacker in that they are access the information from a network system, but their motivation is to improve security. Initially the methods and patterns employed by the penetration tester would be similar to those utilized by hackers. However, penetration testers differ to hackers in that they only probe a network, instead of continuing to exploit and cause malicious damage. A penetration tester is limited to a specific set of systems they can analyze due to contractual obligations. These limitations may take into consideration the amount of time allocated for the test, which specific systems they may probe and the extent to which they may perform the analysis.

Corporate organizations generally desire the minimum amount of disruption to the functioning of the organization's main and back office operations. This means that the process of testing a network and its systems needs to be almost non-intrusive and that the services the organization provides should continue to work as normal during and after a test; ensuring high availability and minimizing the disruption to business processes. This means that the systems may not have been fully penetrated in order to determine the degree of risk these vulnerabilities may pose. Hackers on the contrary, do not care if availability of a system goes down and will attack it to achieve their set goals by any available means.

Usually, large corporations look at hiring a penetration tester to minimize any future damage or information leakage from a potential hacking incident. There is also increasing pressure for corporate organizations to comply to external standards (e.g., Sarbanes-Oxley, HIPAA, PCI DSS, ISO 27001) which usually require or recommend some form of security review (Bentley, L., 2006). This does mean that these can occasionally lead to a simple security exercise with a 'tick in the box' approach and therefore limiting the penetration tester to conducting a simple vulnerability assessment.

I. Penetration Testing vs. Vulnerability Assessment

The main focus of this paper is penetration testing but there is often some confusion between penetration testing and vulnerability assessment. The two terms are related but penetration testing has more of an emphasis on gaining as much access as possible while vulnerability testing places the emphasis on identifying areas that are vulnerable to a computer attack. An automated vulnerability scanner will often identify possible vulnerabilities based on service banners or other network responses that are not in fact what they seem. A vulnerability assessor will stop just before compromising a system, whereas a penetration tester will go as far as they can within the scope of the contract. It is important to keep in mind that you are dealing with a 'Test.' A penetration test is like any other test in the sense that it is a sampling of all possible systems and configurations. Unless the contractor is hired to test only a single system, they will be unable to identify and penetrate all possible systems using all possible vulnerabilities. As such, any Penetration Test is a sampling of the environment. Furthermore, most testers will go after the easiest targets first.

Vulnerability Analysis is the process of identifying vulnerabilities on a network, whereas a Penetration Testing is focused on actually gaining unauthorized access to the tested systems and using that access to the network or data, as directed by the client.

1. A Vulnerability Analysis provides an overview of the flaws that exist on the system while a Penetration Testing goes on to provide an impact analysis of the flaws identifies the possible impact of the flaw on the underlying network, operating system, database etc.
2. Vulnerability Analysis is more of a passive process. In Vulnerability Analysis we use software tools that analyze both network traffic and systems to identify any exposures that increase vulnerability to attacks. Penetration Testing is an active practice wherein ethical hackers are employed to simulate an attack and test the network and systems' resistance.
3. Vulnerability Analysis deals with potential risks, whereas Penetration Testing is actual proof of concept. Vulnerability Analysis is just a process of identifying and quantifying the security vulnerabilities in a system. Vulnerability analysis doesn't provide validation of security Vulnerabilities. Validation can be only done by Penetration testing.
4. The scope of a Penetration Testing can vary from a Vulnerability Analysis to fully exploiting the targets to destructive testing. Penetration Testing consists of a Vulnerability Analysis, but

it goes one step ahead where in you will be evaluating the security of the system by simulating an attack usually done by a Malicious Hacker.

5. For instance a Vulnerability Analysis exercise might identify absence of anti-virus software on the system or open ports as a vulnerability. The Penetration Testing will determine the level to which existing vulnerabilities can be exploited and the damage that can be inflicted due to this.
6. A Vulnerability Analysis answers the question: "What are the present Vulnerabilities and how do we fix them?" A Penetration Testing simply answers the questions: "Can any External Attacker or Internal Intruder break-in and what can they attain?"
7. A Vulnerability Analysis works to improve security posture and develop a more mature, integrated security program, where as a Penetration Testing is only a snapshot of your security program's effectiveness. A vulnerability assessment usually includes a mapping of the network and systems connected to it, an identification of the services and versions of services running and the creation of a catalogue of the vulnerable systems.
8. A vulnerability assessment normally forms the first part of a penetration test. The additional step in a
9. penetration test is the exploitation of any detected vulnerabilities, to confirm their existence, and to determine the damage that might result due to the vulnerability being exploited and the resulting impact on the organization.
10. In comparison to a penetration test a vulnerability assessment is not so intrusive and does not always require the same technical capabilities. Unfortunately it may be impossible to conduct such a thorough assessment that would guarantee that the most damaging vulnerabilities (i.e., high risk) have been identified.
11. The difference between a penetration test and a vulnerability assessment is becoming a significant issue in the penetration testing profession. There are many penetration testers that are only capable of performing vulnerability assessments and yet present themselves as penetration testers. If a company is unfamiliar with the process they may think a networked system has been fully assessed, when this is not the case.

J. Commonly Vulnerability Assessment Goes Through the Following Phases

Information Gathering, Port Scanning, Enumeration, Threat Profiling & Risk Identification, Network Level Vulnerability Scanning, Application Level Vulnerability Scanning, Mitigation Strategies Creation, Report Generation, and Support. Where as a Penetration Testing Service however have following phases: Information Gathering, Port Scanning, Enumeration, Social Engineering, Threat Profiling & Risk Identification, Network Level Vulnerability Assessment, Application Level Vulnerability Assessment, Exploit Research & Development, Exploitation, Privilege Escalation, Engagement Analysis, Mitigation Strategies, Report Generation, and Support.

II. Related Work

There has been considerable effort dedicated to the technical aspects of penetration testing. Arkin,Stender and McGraw (Arkin, B. et al 2005) inv-estigate the importance of the subject from the software pen-testers perspective, concentrating on where the role of the tester lies when assessing flaws during software development. Within the software development life cycle, Arkin et al. suggest without proper and timely assessment, organizations "...often find that their software suffers from systemic faults both at the design level and in the implementation" (Arkin, B. et al, 2005). The same can be said for the network security of an organization; without proper and rigorous assessment, the network design of an organization will lead to unknown flaws inherent in the network implementation. There has been limited work on the skills and abilities required of the pen-tester, and less so on the legal, social, ethical and professional issues arising from such sensitive work. A notable exception to this assertion is the work by Pierce, Jones and Warren (Pierce, J. et al, 2007). In their paper they provide a conceptual model and taxonomy for penetration testing and professional ethics. They describe how integrity of the professional pen tester may be achieved by "...avoiding conflicts of interest, the provision of false positives and false negatives, and finally legally binding testers to their ethical obligations in [their] contract" (Pierce, J. et al, 2007). This is certainly noteworthy and should be expected of an individual working with potentially sensitive infor-mation,however this appears mo re of a personal "ethical code of conduct" rather than something which can be enforced and assessed.

Pierce et al. (Pierce, J. et al, 2007) also discuss the then provision by universities "...toward offering security testing courses". Additionally, in 2006, McRue (McRue, A., 2006) commented on the "...first U.K. university to offer a dedicated degree course in hacking". This has certainly shown an emerging trend in the education sector for penetration testing courses, however these tend to be degree classifications and not necessarily an industry recognized certification standard.

A. Requirements of Penetration Testing

There are a number of organizational issues that need to be addressed before a network penetration test or security review. These requirements can include legal and contractual issues specifying liability etc. This may also include the technical requirements involved in the penetration test: The range of IP addresses over which the test is to be conducted, time constraints, the source IP address and the systems that are to be targeted (and also those that are not to be targeted) as part of the test. There may also be a requirement to inform specific individuals that the test is taking place. Theoretically there are a number of ethical and competency issues that penetration testers face in conducting an assessment, from testing systems or protocols not explicitly included or excluded from a test, to significant omissions that could possibly be disastrous to an organization. The penetration tester is contractually and ethically bound to abide by the customer's requirements, but should ensure the penetration tests is conducted correctly and does not lead to a false or misleading sense of security.

Although Code of Conduct and Best Practice is laid out by numerous professional bodies, in actual practice the individual is often required to take an informed decision given a particular situation. Therefore the individual should possess the necessary procedural, ethical and technical training.

B. Council Of Registered Ethical Security Testers (CREST)

The main purpose of CREST (CREST, 2010) is to provide assurance of competency for organizations, and for the individuals within those organizations. CREST was created to fill a niche in the UK security testing industry, by providing assurance for Non-Government Organizations (NGOs), i.e. the private sector. This

is because the existing CHECK standard is only applicable for Government organizations. Members are provided with guidance on standards, methodologies, further recommendations and a code of practice. However it should be noted that this information is not publicly available. The scheme provides assurances of professionalism to organizations, but not to individuals.

C. TIGER Scheme

The TIGER Scheme (Tiger Scheme, 2010) is focused on providing an independent method of determining the skill and ability of a penetration tester. The scheme has a number of levels from the Associate membership to the Senior Tester qualification. The structure of the scheme involves separate management committee, operating authority and examination body.

III. International Penetration Testing and Vulnerability Assessments

The introduction of the TIGER Scheme and CREST has shown how a governmental initiative has resulted in defining a requirement that industry can follow. When setting up a certification there must be trusted and experienced professionals that will propose and contribute to the certification standards and these in turn need to be assessed accordingly. Examination bodies have to be impartial and avoid any potential conflict of interest in the accreditation process and ensure a certain quality is maintained. This can only be achieved by having an independent examining body with staff that has the relevant expertise.

IV. Proposed Work

A risk means something is about to done or cause harm or reduces the operational utility of the system. Threats are those things which may occur independent of the system under consideration and which may pose the risk.

There are two primary methods of risk analysis and one hybrid method:

- Qualitative - Improve awareness of Information Systems security problems and the posture of the system being analyzed.
- Quantitative - Identification of where security controls should be implemented and the cost envelope within which they should be implemented.
- Hybrid method - A selected combination of these two methods can be used to implement the components utilizing available information while minimizing the metrics to be collected and calculated. It is less numerically intensive (and less expensive) than an in-depth exhaustive analysis.
- Metrics: IT security metrics can be obtained at different levels within an organization. Detailed metrics, collected at the system and network level, can be aggregated and rolled up to progressively higher levels, depending on the size and complexity of an organization.

Good metrics are goal-oriented and should have the following features: specific, measurable, comparable, attainable, repeatable, and time dependent.

A. Metrics to Evaluate the Security Vulnerabilities

A Common Vulnerability Scoring System (CVSS) which was designed to calculate the risk of a vulnerability. The score is derived from metrics and formulas. The metrics are in three distinct categories that can be quantitatively or qualitatively measured. Base metrics contain qualities that are intrinsic to any given vulnerability that do not change over time or in different environments. Temporal metrics contain vulnerability characteristics which evolve over the lifetime of vulnerability. Environmental metrics contain those vulnerability characteristics which are tied to an implementation in a specific user's environment. There are different type of attacks are occur according to these attacks which metrics is used and we can find the risk.

There are seven base metrics which represent the most fundamental features of vulnerability:

1. Access Vector (AV) measures whether the vulnerability is exploitable locally or remotely.
2. Access Complexity (AC) measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system (high or low).
3. Authentication (A) measures whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability. (Required or not required)
4. Confidentiality Impact (CI) measures the impact on confidentiality of a successful exploit of the vulnerability on the target system. (None, partial or complete)
5. Integrity Impact (II) measures the impact on integrity of a successful exploit of the vulnerability on the target system. (none, partial or complete)
6. Availability Impact (AI) measures the impact on avail abilty of a successful exploit of the vulnerability on the target system. (none, partial or complete)
7. Impact Bias (IB) allows a score to convey greater weighting to one of three impact metrics over the other two. The value can be normal (CI, II and AI are all assigned the same weight), confidentiality (CI is assigned greater weight than II or AI), integrity (II is assigned greater weight than CI or AI), or availability (AI is assigned greater weight than CI or II)

B. The Temporal Metrics Which Represent the Time Dependent Features of the Vulnerability are:

Exploitability (E) measures how complex the process is to exploit the vulnerability in the target system. The possible values are: unproven, proof of concept, functional, or high. Remediation Level (RL) measures the level of an available solution. (official fix, temporary fix, workaround, or un available) Report Confidence (RC) measures the degree of confidence in the existence of the vulnerability and the credibility of its report. (unconfirmed, uncorroborated, or confirmed) The environmental metrics represent the implementation and environment specific features of the vulnerability. Collateral Damage Potential (CDP) measures the potential for a loss of physical equipment, property damage or loss of life or limb. (none, low, medium, or high). Target Distribution (TD) measures the relative size of the field of target systems susceptible to the vulnerability. (none, low, medium, or high) Scoring is the process of combining all the metric values ac-cording to specific formulas. This is very useful to understand the nature of attacks for pen testers. With the help of these metrics we can find the nature of risk and take the action. The role of pen tester is not only achieve the certification but also known the behavior and nature of different types of vulnerabilities. So the role of pen tester is very important in the organization. There are different tools are used for pen test:

C. Port Scanners

Port scanning tools are used to gather information about a test target from a remote network location. Specifically, port scanners attempt to locate which network services are available for connection on each target host. They do this by probing each of the designated

(or default) network ports or services on the target system. Most port scanners are able to scan both TCP as well as UDP ports. Most can also target a specified list of ports and can be configured for the speed and port sequence that they scan.

D. Vulnerability Scanners

The primary distinction between a port scanner and a network-based vulnerability scanner is that vulnerability scanners attempt to exercise (known) vulnerabilities on their targeted systems, whereas port scanners only produce an inventory of available services. That said, the distinguishing factors between port and vulnerability scanners are often times blurred. Apart from that, a good vulnerability scanner is a vital tool to a traditional penetration tester. They provide an essential means of meticulously probing each and every available network service on the targeted hosts. Vulnerability scanners work from a database of documented network service security defects, exercising each defect on each available service of the target range of hosts.

E. Application Scanners

Taking the concept of network-based vulnerability scanner one step further, application scanners began appearing several years ago. These attempts to do probing of general purpose web-based applications by attempting a variety of common and known attacks on each targeted application and page of each application.

F. Web Application Assessment Proxy

Although they only work on web applications, web application assessment proxies are perhaps the most useful of the vulnerability assessment tools listed here. Assessment proxies work by interposing themselves between the tester's web browser and the target web server. Further, they allow the tester to view and manipulate any and all data content flowing between the two. This gives the tester a great deal of flexibility in trying different "tricks" to exercise application weaknesses in the application's user interface and associated components. This level of flexibility is why assessment proxies are considered essential tools for all black box testing of web applications.

G. Important Feature for Selecting the Right Toolkit

Following are the features for right toolkit:
Visibility, Extensibility, Documentation, License flexibility.

V. Conclusion

Although penetration testing is an industry recognized term, there is still ambiguity as to what a penetration tester actually does and how they provide assurance that the work they carried out is fit for purpose. It is important to make a distinction between penetration testing and network security assessments.

A network security or vulnerability assessment may be useful to a degree, but do not always reflect the extent to which hackers will go to exploit a vulnerability. Penetration tests attempt to emulate a 'real world' attack to certain degree. The penetration testers will generally compromise a system with vulnerabilities that they successfully exploited. Hackers and intruders need to find only one hole to exploit whereas penetration testers need to possibly find all if not as many as possible holes that exist. This is a daunting task as penetration tests are normally done in certain time frame. Finally, a penetration test alone provides no improvement in the security of a computer or network. Action to taken to address these vulnerabilities that is found as a result of conducting the penetration test.

References

[1] IDC, (2009),"Number of Mobile Devices Accessing the Internet Expected to Surpass One Billion by 2013", Reported on 9 Dec 2009, [Online] Available:// http://www.idc.com/getdoc.jsp?containerId=prUS22110509.

[2] Moses A., (2010),"Internet addresses running out", Sydney Morning Herald, [Online] Available:// http://www.stuff.co.nz/dominionpost/national/technology/3958727/Internet-addresses-running-out

[3] ACPO, (2009),"ACPO e-Crime Strategy 2009 Report: A Strategic Approach to National e-Crime".

[4] Markkoff, J. (2008). Before the Gunfire Cyberattacks. New York Times. [Online] Available: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1. 2

[5] Higgins, K. J. (2010),"Anatomy Of A Targeted, Persistent Attack", DarkReading, 27 Jan. 2010, [Online] Available: http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=222600139

[6] Dekker, M. (1997),"Security of the Internet", CERT Coordination Center Reports, [Online] Available: http://www.cert.org/encyc_article/tocencyc.html

[7] Stoll, C. (1989),"The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage", Doubleday, NY, USA

[8] EC-Council, (2010). Certified Ethical Hacking Training Course. [Online] Available: http://www.eccouncil.org/certification/certified_ethical_hacker.aspx

[9] Bentley, L., (2006), "Penetration Testing Key to HIPAA Compliance for Care New England", IT Business Edge, [Online] Available: http://www.itbusinessedge.com/cm/community/features/interviews/blog/penetration-testingkey-to-hipaa-compliance-for-care-new-england/?cs=22127

[10] Cabinet Office, (2009), "Cyber Security Strategy of the United Kingdom", June 2009, [Online] Available: http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf

[11] Arkin, B., Stender, S., McGraw, G.,"Software Penetration Testing", IEEE Security and Privacy, Vol. 3, Issue 1, 2005.

[12] Pierce, J., Jones, A., Warren, M.,"Penetration Testing Professional Ethics: a conceptual model and taxonomy", Australasian Journal Of Information Systems, 13(2). [Online] Available: http://www.dl.acs.org.au/index.php/ajis/article/view/52

[13] McRue, A. (2006),"University opens school for hackers". [Online] Available: http://news.cnet.com/University- opens-schoolfor- hackers/2100-7355_3-6085375.html

[14] IEEE, (2010),"The Institute of Electrical and Electronics Engineers", [Online] Available: http://www.ieee.org/

[15] BCS,"BCS - The Chartered Institute for IT", (2010), [Online] Available: http://www.bcs.org

[16] IEEE, (2010),"IEEE Computer Society", [Online] Available: http://www.computer.org

[17] BCS, (2010),"BCS Information Security Specialist Group (BCS-ISSG)", [Online] Available: http://www.bcsissg.org.uk

[18] The Institute of Information Security Professionals (iisp), (2010) [Online] Available: https://www.instisp.org/SSLPage.aspx?pid=183

[19] The ISC2 Code of Ethics, [Online] Available: https://www.isc2.org/ethics/default.aspx

[20] Council of Registered Ethical Security Testers (CREST), (2010). [Online] Available: http://www.crestapproved.org/Pages/RequiredMembership.html

[21] Insititute for Security and Open meththologies, OSSTMM - Open Source Security Testing Methodology Manual, [Online] Available: http://www.isecom.org/osstmm
[22] Open Web Application Security Project (OWASP) [Online] Available: http://www.owasp.org/index.php/Main_Page
[23] Logan P.Y., Clarkson A.,"Teaching students to hack: curriculum issues in information security", Technical Symposium on Computer Science Education, Proceedings of the 36th SIGCSE technical symposium on Computer science education, pp. 157-161, 2005.
[24] Tiger Scheme, (2010), "Tiger Scheme" [Online] Available: http://www.tigerscheme.org
[25] CREST, (2010), "Council of Registered Ethical Security Testers", [Online] Available: http://www.crest-approved.org
[26] CESG, (2010),"CHECK – What is CHECK" [online], [Online] Available: http://www.cesg.gov.uk/products_services/iacs/check/index.shtml
[27] Council of Registered Ethical Security Testers (CREST), (2010). [Online] Available: http://www.crestapproved.org/Pages/MembersList.html
[28] Fyodor's Exploit World, Exploits for many Operating Systems including Linux, Solaris, Microsoft, Macintosh. For Hackers, Hacking, Computer Security Auditing & Testing. [Online] Available: http://www.insecure.org/sploits.html
[28] Pete Herzog. The Open Source Security Testing Methodology Manual, [Online] Available: http://uk.osstmm.org/osstmm.htm
[29] Wallyware, Inc. Hacker Whacker: See your computer the way hackers do, [Online] Available: http://hackerwhacker.com
[30] Lincoln d. Stein. The World Wide Web Security FAQ [Online] Available: http://www.genome.wi.mit.edu/WWW/faqs/www.security-faq.html
[31] Linet Solutions,"Firewall TCP/UDP Ports: Which Protocols to Filter", [Online] Available: http://www.ec11.dial.pipex.com/port-filter.htm
[32] The Penetraiton Testing Group. An Introduction to Penetration Testing", [Online] Available: http://www.penetration-testing-group.co.uk/index.htm
[33] Hideaway.net. Strategic Scanning and Assessment of Remote Hosts", [Online] Available: http://www.hideaway.net/Server_Security/Library/General/gentxts/ssarh.htm
[34] Victor-Valeriu PATRICIU, Iustin PRIESCU, Sebastian NICOLAES-CU Security Metrics for Enterprise Information Sysems 2007.
[35] [Online] Available: http://nvd.nist.gov/cvss.cfm?calculator

Azhar Ali, Dept. of C.S.E/IT, Integral University, Lucknow, Uttar Pradesh, India