Sindh Univ. Res. Jour. (Sci. Ser.) Vol. 48 (3) 701-706 (2016)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Internal Vulnerability Assessment of IT Infrastructure

A. ALI M. N..BROHI,

Department of Computing, SZABIST Dubai, UAE.

Received 09th July 2015 and Revised 12th August 2016

Abstract: Today IT infrastructures are dynamic, requiring multitude of defense measures to effectively prevent attacks and efficiently mitigate vulnerabilities across the entire enterprise. Organizations must not only be aware of the threats, but also the impact of those threats on their infrastructure. Vulnerability assessment is a powerful proactive process for identifying vulnerabilities and securing an enterprise IT infrastructure. Vulnerability assessment is a continuous process, which mitigate the risk of any type of external attacks on an IT infrastructure. Compromising the organizational assets security leads to loss of valuable information, finances and even the invaluable reputation of the business. Foolproof security cannot be ensured and there is no guarantee of a 100% secure environment but still these methodologies try to find out any loopholes in the IT infrastructure, which can be taken care of in order to mitigate the risks involved. This work talks about the internal vulnerability assessment in details and touches the external vulnerability assessment on a basic level. The methodology of vulnerability assessment and how it can be done to achieve the desired outcomes is discussed. Various tools and techniques have been discussed for the vulnerability assessment. In the last part, recommendations are provided to organizations for ensuring their infrastructure security based on vulnerability assessment. This study focuses on the assessment of target organization's IT infrastructure for vulnerabilities and at the end summarizes recommendations for those vulnerabilities.

Keywords: Cyber Threats, Critical Infrastructure, information secuirty, Nessus Tool, Pen test, ethical hacking, Security Audits, Intrusion Detection System.

1. INTRODUCTION

Infrastructure vulnerability assessments, be it manual or automated are considered as key component of any security roadmap. These assessments enable organizations to find out the status of their information and infrastructure security and are designed to identify whether or not an unethical activity will happen in the form of hack attack that will bypass the security measures of the infrastructure and will exploit any vulnerable asset present in the environment. The breach of security parameters results in compromise of confidentiality, availability and integrity of information sacred to the business (Shrestha 2012).

Vulnerability assessment is a process that defines, identifies, classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure. In addition, vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.

A vulnerability assessment is an internal audit of your network and system security; the results of which indicate the confidentiality, integrity, and availability of your network. Typically, vulnerability assessment starts with a reconnaissance phase, during which important data regarding the target systems and resources is gathered. This phase leads to the system readiness phase, whereby the target is essentially checked for all known vulnerabilities. The readiness phase culminates in the reporting phase, where the findings are classified into categories of high, medium, and low risk; and methods for improving the security (or mitigating the risk of vulnerability) of the target are discussed.

If you were to perform a vulnerability assessment of your home, you would likely check each door to your home to see if they are closed and locked. You would also check every window, making sure that they closed completely and latch correctly. This same concept applies to systems, networks, and electronic data. Malicious users are the thieves and vandals of your data. Focus on their tools, mentality, and motivations and you can then react swiftly to their actions.

Vulnerability assessments may be broken down into one of two types:

- **Outside looking in**
- **Inside looking around**

When performing an outside looking in vulnerability assessment, you are attempting to compromise your systems from the outside. Being external to your company provides you with the cracker's viewpoint. You see what a cracker sees — publicly-routable IP addresses, systems on your DMZ, external interfaces of your firewall, and more. DMZ stands for "demilitarized zone", which corresponds to a computer or small sub-network that sits between a trusted internal network, such as a corporate private LAN, and an un-trusted external

++ Corresponding Author Email akhtaralicse@gmail.com mnbrohi@szabist.ac.ae

network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

When you perform an inside looking around vulnerability assessment, you are somewhat at an advantage since you are internal and your status is elevated to trusted. This is the viewpoint you and your co-workers have once logged on to your systems. You see print servers, file servers, databases, and other resources.

There are striking distinctions between these two types of vulnerability assessments. Being internal to your company gives you elevated privileges more so than any outsider. Still today in most organizations, security is configured in such a manner as to keep intruders out. Very little is done to secure the internals of the organization (such as departmental firewalls, user-level access controls, authentication procedures for internal resources, and more). Typically, there are many more resources when looking around inside as most systems are internal to a company. Once you set yourself outside of the company, you immediately are given an un-trusted status. The systems and resources available to you externally are usually very limited.

Internal Network Vulnerability Assessments frequently include but it is not limited to:

Physical Security Assessment
Wireless Network Security Assessment
PCI Compliance Testing
IDS/IPS Testing
Antivirus Configuration Testing
Social Engineering
Vulnerability Assessment

Vulnerability assessment consists of several steps:

1. Defining and classifying network or system resources
2. Assigning relative levels of importance to the resources
3. Identifying potential threats to each resource
4. Developing a strategy to deal with the most serious potential problems first
5. Defining and implementing ways to minimize the consequences if an attack occurs.

If security holes are found as a result of vulnerability analysis, a vulnerability disclosure may be required. The person or organization that discovers the vulnerability, or a responsible industry body such as the Computer Emergency Readiness Team (CERT), may make the disclosure. If the vulnerability is not classified as a high level threat, the vendor may be given a certain amount of time to fix the problem before the vulnerability is disclosed publicly.

The third stage of vulnerability analysis (identifying potential threats) is sometimes performed by a white hat using ethical hacking techniques. Using this method to assess vulnerabilities, security experts deliberately probe a network or system to discover its weaknesses. This process provides guidelines for the development of countermeasures to prevent a genuine attack.

With the advancements in the field of computing, information security is becoming an integral part of any organization and is having serious implication in today's challenging work environment. The world is connected through internet and businesses work regardless of their physical locations, this distributed nature of businesses makes information security a basic requirement for any organization irrespective of its size and volume. Special attention is required for the improvement of IT infrastructure in order to achieve the desired goals concerning information security. A general misconception is that external threats must be catered and usually organizations oversee the internal threats residing within the perimeters of the business. These internal security threats are always a major loss point for organization's IT infrastructure security. The security loopholes can be a result of misconfigured IT system or any other security devices, which enable the attackers (Hacker) to take benefit of it. Due to this reason, it is the cry of the day to do proper vulnerability Assessment of an organization's IT infrastructure. Vulnerability assessment is an important tool in proactive security of IT infrastructure, which is the very sole of information security (Shrestha 2012).

One can find news about security lapses and business loss in media these days. In recent days, Sony was hacked and resulted in reputational loss (Sony 2014). The threat of security breach is being recognized widely in the industry and organizations are investing in the field of information security to ensure their business continuity and protection of their invaluable assets and information. The need of information security compels businesses to do vulnerability assessment of their infrastructure on regular basis as a standalone process or part of any standardization like ISO 27001:2013. Vulnerability assessment and penetration testing is in general taken in same meaning, below the difference between these two approaches and techniques has been elaborated.

1.1 Vulnerability Assessment Versus Penetration Testing

Security audits as a part of vulnerability assessment identify vulnerable points and loopholes, which are vulnerable and prone to any kind of attack. Vulnerability assessment examines the IT infrastructure in terms of parameters such as how much the security level is compliant with the needs and goals of the organization

and if any standard is in place, how much it is efficient and to take care of any security. This assessment focuses on the security loopholes exploration without regard to exploiting them and breaking. In case of penetration testing, the assessment and examination is in depth and it gives more emphasis on identifying vulnerabilities and gaining as much access as possible of the system and then exploits them (Herivato 2011) .

Organizations must be proactive to ensure security of their infrastructure. Vulnerability assessment plays an important role in achieving this proactive strategy and is followed by the penetration testing. The boundaries of both methodologies are that security assessment will stop just before compromising system, while penetration tests aims to compromise the system to check the severity of and nature of the attack and the reasons behind it (Herivato 2011). In the process of vulnerability, assessment systems and infrastructures are scanned for possible vulnerabilities and then the false positive is filtered out from the scanned output. This is achieved by mapping them with the actual vulnerabilities associated with the target host. While in the process of penetration, testing the main goal is to ensure the efficiency and effectiveness of the existing security measures placed in the environment (Bishop 2007).

The vulnerability assessment can be divided into external and internal vulnerability assessment. The External Vulnerability Assessment also named as penetration testing. The Penetration testing techniques involves the formulation of such real world attacks that are potential threats. The ethical hacker in this scenario does not have any information about the infrastructure and have no access to it. Some of the techniques used are Social Engineering, Network Scanning, remote access, Trojans etc. The ethical hackers are provided with only the public information e.g. the URL and then they try to hack the system based on their devised strategy (Akbari, *et.al.* 2010).

In the Internal Vulnerability Assessment, the Ethical hackers are provided with the access information of the infrastructure and system and they simulates attack based on it. This provided information includes OS details, IP address schema, network layouts and source code. The tester resides inside the network and simulates attacked on the network and finding vulnerabilities inside it (Akbari, *et.al.* 2010).

2. RELATED WORK

The field of information security is a well-established domain of knowledge and as the digital information is growing, the need of securing this information is becoming crucial. Researchers are working in this field of study and some phenomenal works are being published with the passage of time. In this section, some of the studies are discussed related to vulnerability testing and information security.

The researcher (Shrestha 2012) describes about the expansion and evolution of computer, internet and web technologies and how they have made society more dependent on computer network services than ever. As the time passes by hackers, come up with more innovative techniques to exploit the systems and infrastructure for their own gain. The complexity and intensity of these attacks results in loss in business and productivity along with business continuity. Apart from the monetary loss, organization's reputation is at stake, which is an invaluable asset and usually is formed after years of hard work and dedication. Thus providing a secure and risk free environment is becoming a challenge to the IT professionals in order to reduce the potential data and information loss. There should be a proper security assurance plan for organizations, which will ensure frequent vulnerability assessments to mitigate the risk of any external attacks (Shrestha 2012).

The researchers (Brohi, *et al,* 2012) are of the opinion that security is more of a major concern in virtual IT infrastructure as in case a single physical host is compromised the entire virtual infrastructure will be accessible. It mentions the importance of virtualization in cloud computing and emphasis on the security of virtual infrastructure. According to them Cloud Computing Infrastructure (CCI) consists of several Virtual Machines (VMs) running on same physical platform by using virtualization techniques. The VMs are monitored and managed by kernel based software i.e. Virtual Machine Monitor (VMM) or hypervisor which is main component of Virtualized Cloud Computing Infrastructure. Researchers stated that Due to software-based vulnerabilities, VMMs are compromised to security attacks that may take place from inside or outside attackers. This shows that security of virtual IT Infrastructure can be compromised and Vulnerability assessment is compulsory on a regular basis.

The researchers (Asif and Al-Harthi 2014) stated that with the advancement in the cyberspace technologies the likelihood of threats also increases to the security of critical infrastructure. This way the chances of well-planned cyber-attacks also increases and thus conventional security measures are not enough to cater these kinds of critical situations. They talk about an Intrusion detection system (IDS) designed by them that is based on the novel approach of honey token-based entry *et al.*, pointers to prevent critical infrastructure networks from cyber-attacks.

In the view of above studies security of IT infrastructure, both physical and virtual infrastructure is very important today. Different types of vulnerabilities are coming, proper vulnerability assessment and early

closure of the found vulnerabilities is very important to keep organization's IT infrastructure secure from any external attacks.

3. MATERIAL AND METHODOLOGY

The primary objective of this research methodology is to successfully conduct the vulnerability assessment of an organization's IT infrastructure. Security in infrastructure and networks has critical value in today's growing and dynamic businesses (Daud *et.al*, 2014). Security is becoming and is the basic requirement for any organization having a distributed infrastructure because distributive computing is inherently insecure. It is not the case that the size and volume of an organization be considered when we talk about security, every organization require some level of security measures and special attention is required for the improvement of IT infrastructure (Chen, *et.al*, 2013). Internal security threats are the main pain points for security professionals (Marconato 2012). These security risks are a result of no proper planning and misconfiguration of IT infrastructure. That is the reason that today's organization requires proper vulnerability assessment on regular basis along with an effective information security plan (Munir 2013).

Vulnerability Assessment of organization IT infrastructure consist of four phases as shown in **(Fig.1)** they are:



Fig.1 Process Flow of Vulnerability Assessment

Phase-1 Information Gathering

This phase include proper planning to collect required information for testing and assessments of vulnerabilities. Information required to define the scope of the testing is acquired using the information available on the public domain, using various tools including search engines. Personal interviews are conducted with organization's network team to get information regarding the network devices, IP ranges, about the OS and overall IT Infrastructure. This information is used to scan and map the infrastructure. Various Scan are then conducted using customs flags to identify the active hosts for the identification of services and the associated applications.

Phase-2 Assessment /Advance Testing

There are many tools available for the vulnerability scanning e.g. Nessus V6 Advanced Port Scanner and Open VAS. These tools will be used in this phase for the vulnerability scanning. Using these tools all network devices will be scanned. The discovered services and applications will be compared with the vulnerability databases and vulnerability chart will be defined. Outlined vulnerabilities were then tested on these systems and in this process detailed information about the host operating systems and any filtered services running on these hosts are obtained. All port on the Gateway device is scanned carefully and afterwards analysis is performed for finding the potential threats and vulnerabilities.

Phase -3 Analysis

This phase includes developing understanding of the state of security within a systems or a network and find out which vulnerability are real and which ones are false positive. This identification of vulnerabilities helps in improvement of the security of the environment by understanding and analyzing the security risks and issues existing in infrastructure. The analysis part focuses on the possible results and loss, which can be occurred if these security loopholes are compromised and are exploited by the attackers (Hanch 2014). The tools being used in this part have their own information base and databases which helps in relating the incidents and issues with any historical occurrences of the same kind of risks.

Information security is a vital part of organization plan for business continuity and market presence. It helps protect the organization from any unauthorized accesses to the infrastructure and minimizing the exploitation of any vulnerability (Sari 2014).

Phase -4 Recommendation

This phase categorizes the vulnerabilities based on the importance of being addressed. Thus, the vulnerabilities found during assessment are categorized as High, Medium and Low based on their potential threats to organization IT infrastructure (Sari 2014).

High: High priority observations require immediate attention and should be addressed in an expedited manner. While mitigating controls may exist, these issues present an increased level of risk associated with the protection and safeguarding of confidential and sensitive information and should be addressed as soon as possible.

Medium: Medium priority observation should be noted and implemented at later date, but May not pose a real threat to the network and connected systems at this time.

Low: Low priority observation should be noted and implemented at a later date, but May not pose a real threat to the network and connected systems at this time.

4. IMPLEMENTATION

Today's IT Infrastructure consist of many Network Component, Security devices, data storage devices, load balancer, Physical Servers and UPS

System. Network devices consist of routers and switches. Security devices include firewalls (core network firewall, data center firewall and application firewalls).Data storage consist of SAN and NAS. All these devices are interconnected with each other inside a data center. Every network device has a firmware or operating system, there is chance of two types of vulnerabilities in data center conponents. One is inside the firmware/operating system and the second is due to human errors like misconfiguration etc.

The right tools for the right job. That statement is just as true for the VA process as it is in any other situation. When conducting a vulnerability assessment the tool set being used should be very similar to that of the identified adversary. This will ensure that the systems are secure from attacks that are currently being employed out in the wild. Remember new weaknesses are discovered every day, and new tools to exploit these weaknesses usually follow close behind, so it becomes very important to stay current with security news.

Different tools are available for finding the vulnerabilities organization IT infrastructure, the most famous and reliable tools are Open VAS and Nessus. Nessus is one of the most well know vulnerability assessment tool having updated databases of all kinds of vulnerabilities (Hemanidhi 2014).These tools scan entire network devices like routers, switches, firewalls, servers (both physical and virtual),virtual host, NAS and SANS. It takes few hours to complete the scanning process, after the completion of scanning a detailed report of vulnerabilities is generated and is then categorize as high, medium and low base on its severity and risk to organization IT infrastructure in **(Fig. 2).**

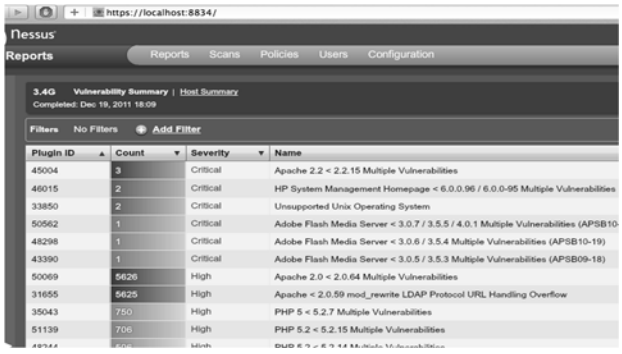


Fig.-2. Sample of Vulnerability testing

Firewalls also helps in monitoring the incoming and outgoing network traffic and any open ports, which are the main entry points to the Enterprise network. Ports are like doors, which enable hacker to enter any IT infrastructure (Noh 2008). All unused open port must be close to mitigate the risk of unwanted traffic to organization corporate Network. Monitoring of gateway traffic can be seen in the **(Fig.3).**

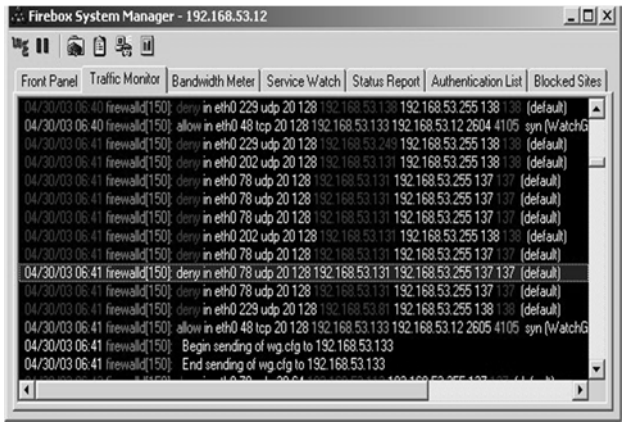


Fig.3. Incoming & Outgoing Traffic Monitor

One technique for finding and fixing of vulnerabilities is the use of scanning tools; other technique is to find vulnerabilities using technical skills and expertise by comparing the current configuration of network devices with the industry best practice configuration and implementation. Also comparing the discovered vulnerabilities with the known vulnerabilities database, which will help in mitigation of security risk?

5. CONCLUTIONS

As mentioned in the earlier sections vulnerability assessment plays a vital role to identify vulnerabilities present in an infrastructure the plan to mitigate and close them to ensure proper security, thus the importance of vulnerability assessment is very critical and depends upon the selection of proper underlying methodology and tools. Skilled resources with quite good amount of expertise are required in order to find the false positive vulnerabilities during testing and assessment of the infrastructure. The categorization of vulnerabilities to high, medium and low helps the infrastructure team to prioritize and plan for closing the critical risks and vulnerabilities. Below are few of the key points, which should be followed to mitigate these risks:

- The vulnerabilities should be addressed at early stage as it comes. This helps in minimizing potential big risks and small risks, which might become a big risk at latter stage, are catered properly.
- The process of vulnerabilities testing should be properly planned and it should happen on a predefined schedule periodically to ensure the security of the infrastructure. In case of a sudden security risk or breach these assessment can be done on demand as well.
- Strong Password Policy minimizes the chances of password hacking or compromising as it becomes difficult for hackers to predict it. Also changing the

passwords periodically is a good idea so that there is less chance of any possible security breach related to password.

- Closure of unused open port should be done so that there is no open door left for hackers to penetrate the network and infrastructure.
- Patch management should be operated in an efficient manner. Updates to the security mechanism in the form of patches should be installed in the environment to enhance the ability of the system in coping any malicious activities.
- Networks should be designed in such a way that not all the network and its resources are in one segment. In case of having one large, network without segregation if the network is compromised by any chance, the whole environment and organization assets are at stake. When segregation of network is done, it minimizes such risks.
- Information Security Awareness is very important for the organization employees. Not only the technical people but all the human resources interacting with the system shall be aware of the information and data security with the organization. So that proper standard operating procedures regarding security are followed and carried out and hence resulting in minimal risks.
- Physical Security shall also be implemented in order to ensure authorized access only to the physical infrastructure resources. This minimizes the risks of tampering with the infrastructure and helps in reducing the internal risks related to information security within the organization.

REFERENCES:

Ali A. and Herivato. (2011). Backtrack 4: Assuring Security by Penetration Testing. Packt Publishing, 32 Lincoln Road Olton, Birmingham, B27 6PA, UK.

Akbari, M. and R. Azmi *(*2010) Vulnerability Detector using Parse Tree Annotation. Presented at 2nd international Conference on Education Technology and Computer (ICETC), Shanghai, China: 22-24.

Asif, M. K. and Y. K. Al-Harthi, (2014) Intrusion Detection System using Honey Token based Encrypted Bishop M. (2007) About Penetration Testing, IEEE Security & Privacy, 5 (6): 84–87.

Géraldine V., M. V. Nicomette and M. Kaâniche, (2012) Security-related vulnerability life cycle analysis. Presented at 7th International Conference on Risk and Security of nternet and Systems (CRiSIS), Oct. 10-12, Cork, Ireland: 1-8.

Hanch, N., Z. Benenson, (2014) Specifying IT Security Awareness. Presented at 25th International Workshop on Database and Expert Systems Applications (DEXA) Sept. 2014, Munich, Germany: 1-5.

Kai C., Y. Lian, (2013) Vulnerability-based Backdoors: Threats from Two-step Trojans. Presented at 7th International Conference on Software Security and Reliability, Washington, D.C, USA:169-177.

Noh, (2008) Active-Active High Availability of Information Infrastructure System for Effective Network Security.Presented at International Conference on Information Science and Security (ICISS), Jan. 2008, Seoul, South Korea: 187-191.

Nor I. D. K. Azmi, A. Bakar; M. Shafeq M. Hasan, (2014) A Case Study on Web Application Vulnerability Scanning Tools. Presented at Science and Information London, UK, 27-29 August:595 - 600.

Nrianasari, N. (2014). Information security awareness measurement with confirmatory factor analysis. Presented at International Symposium on Technology Management and Emerging Technologies (ISTMET), Bandung, Indonesia: 27-29

Pointers to Mitigate Cyber Threats for Critical Infrastructure Networks" Presented at IEEE International Conference on Systems, Man, and Cybernetics, San Diego, CA, USA: 5-8.

Rashid M., I. Awan and M. R. Mufti, (2013) A Quantitative Measure of the Security Risk Level of Enterprise Networks, Presented at Eighth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), Oct. 28-30, 2013, Compiegne, France: 437-442

Sarfraz N. B., B. M. Adib, M Nawaz B. R.Kamran,, (2012) Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures. Presented at the Proceedings of International of Cloud computing, Technologies, Applications and anagement (ICCCTAM 2012), December 2012, Dubai, United Arab Emirates: 151-155.

Shrestha (2012) Security Assessment via Penetration Testing: A Network and System Administrator's Approach, Master Thesis, Oslo University.

Sony-hack-explained (2014) http://www.vox.com, Retrieved Date: 15 November 2014.