Vulnerability Assessment Using Nessus Scanner.

Saurabh Kulkarni[1] ,Chinmay Chiplunkar[2] ,Priyanka Khadase[3]

MCA II Yr Sinhgad Institute Of Management and Computer Application, Narhe

Abstract:

In the war zone that is the modern Internet, manually reviewing each networked system for security flaws is no longer feasible. Operating systems, applications, and network protocols have grown so complex over the last decade that it takes a dedicated security administrator to keep even a relatively small network shielded from attack. To combat these attacks, a network administrator needs the appropriate tools and knowledge to identify vulnerable systems and resolve their security problems before they can be exploited. One of the most powerful tools available today is the vulnerability assessment

*Keywords**: Vulnerability assessment, Security, Viruses, Attacker, IDS, Network, Vulnerability assessment tool, Nessus,CVSS, CVE, Metasploit, IP Address, This research paper explains the following points:***

I. VULNERABILITY ASSESSMENT

Vulnerability refers to any programming error or misconfiguration that could allow an intruder to gain unauthorized access. This includes anything from a weak password on a router to an unpatched programming flaw in an exposed network service. Vulnerabilities are no longer just the realm of system crackers and security consultants; they have become the enabling factor behind most network worms, spyware applications, and e-mail viruses. Spammers are increasingly relying on software vulnerabilities to hide their tracks; the open mail relays of the 1990s have been replaced by compromised.

Vulnerability assessments are simply the process of locating and reporting vulnerabilities.They provide you with a way to detect and resolve security problems before someone or something can exploit them. One of the most common uses for vulnerability assessments is their capability to validate security measures. If you recently installed a new intrusion detection system (IDS), a vulnerability assessment allows you to determine how well that solution works. If the assessment completes and your IDS didn’t fire off a single alert, it might be time to have a chat with the vendor.

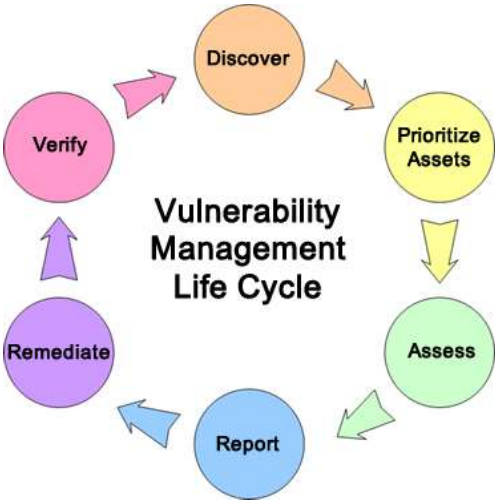
The actual process for vulnerability identification varies widely between solutions; however, they all focus on a single output—the report. This report provides a snapshot of all the identified vulnerabilities on the network at a given time.

Components of this report usually include a list detailing each identified vulnerability, where it was found, what the potential risk is, and how it can be resolved[1].

II: NEED OF VULNERABILITY ASSESSMENT?

A vulnerability is a weakness in the application which can be an implementation bug or a design flaw that allows an attacker to cause harm to the user of the application and get extra privilege . Vulnerability are the potential risk for the system. Attacker uses these vulnerability to exploit the system and get unauthorized access and information. Vulnerabilities are big flaw in system security and Information assurance. A vulnerability free system can provide more Information Assurance and system securityWhen anew vulnerability is discovered, the network administrator can perform an assessment, discover which systems are vulnerable, and start the patch installation process. After the fixes are in place, another assessment can be run to verify that the vulnerabilities were actually resolved. This cycle of assess, patch, and re-assess has become the standard method for many organizations to manage their security issues.

Many organizations have integrated vulnerability assessments into their system rollout process. Before a new server is installed, it first must go through a vulnerability assessment and pass with flying colors. This process is especially important for organizations that use a standard build image for each system; alltoo often, a new server can be imaged, configured, and installed without the



administrator remembering to install the latest system patches. Additionally, many vulnerabilities can only be resolved through manual configuration changes; even an automated patch installation might not be enough to secure a newly imaged system. It's much easier to find these problems at build time when configuration changes are simple and risk-free than when that system is deployed in the field.We strongly recommend performing a vulnerability assessment against any new system before deploying it.Assessments can give you a current and very useful understanding of the services offered on your network. Assessments assist in crises: when a new worm is released, assessment reports are often used to generate task lists for the system administration staff, allowing them to prevent a worm outbreak before it reaches critical mass [2].

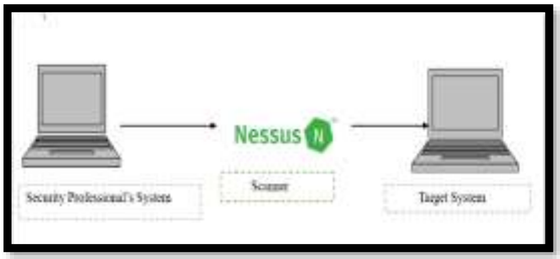
III: Diagrammatical Representation of Vulnerability Assessment

IV: Application -Vulnerability assessment tool:

Software Name – Nessus Professional Tool By Tenable. Nessus is the de-facto industry standard vulnerability solution for security practitioners.

Nessus helps the security pros on the front lines quickly and easily identify and fix vulnerabilities-Including software flaws, missing patches, malware and misconfigurations across a verity of operating Systems, devices and applications.Install Nessus Home, Professional, or Manager. This option installs a stand-alone versions of Nessus Home, Nessus Professional, or Nessus Manager. During installation, you will be prompted to enter your Nessus Activation Code; this Activation Code determines which product will be installed. Select the Custom Settings link to manually configure Proxy and Plugin Feed settings. Configuring Custom Settings allows you to override the default settings related to Nessus plugins [3].

Diagrammatical Representation of Nessus Scanner

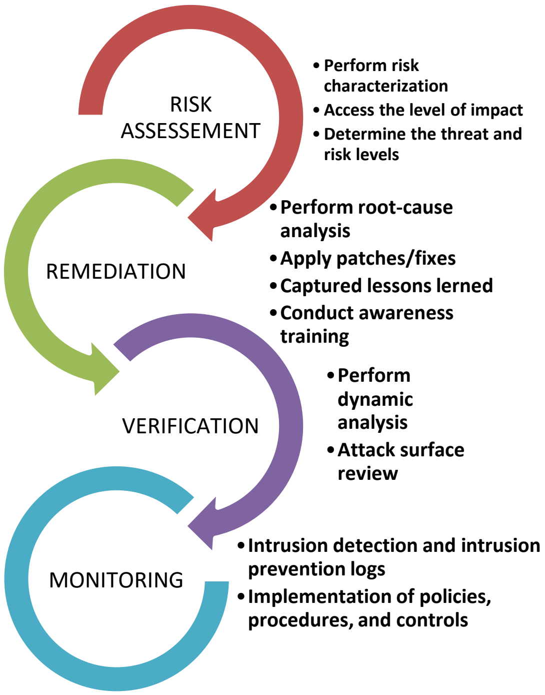


V:

METHODOLOGIES-

There are Phases of Vulnerability Assessment which we can say it's methodologies.Pre-assessment Phase – Creating a Baseline, Identify and understand business process.Identify the applications, data, and services the support the business.Create an inventory of all assets, and prioritize/risk the critical asset ,map the network infrastructure Identify the controls already in place,understand Policy implementation and Standards compliances to the business process. Create Information Protection procedure to support effective planning, scheduling, and coordination

Post Assessment Phase:


RISK ASSESSMENT
• Perform risk characterization
• Access the level of impact
• Determine the threat and risk levels
REMEDIATION
• Perform root-cause analysis
• Apply patches/fixes
• Captured lessons lerned
• Conduct awareness training
VERIFICATION
• Perform dynamic analysis
• Attack surface review
MONITORING
• Intrusion detection and intrusion prevention logs
• Implementation of policies, procedures, and controls

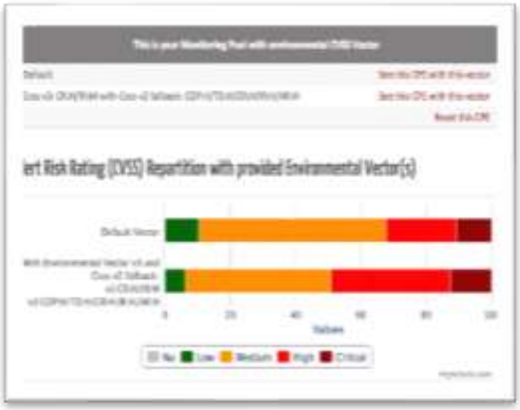
VI: Types of vulnerability assessment-

Active Assessment- Use a network scanner to find hosts, services and vulnerabilities. Passive Assessment- A technique used to sniff the network traffic to find out active systems, network services, applications, and vulnerabilities present External Assessment- Access the network from the hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world. Internal Assessment- A technique to scan the infrastructure to find out the exploits and vulnerabilities. Host-Based Assessment- Determines the vulnerabilities in a specific workstations or server by performing configuration-level check through the command line. Network Assessments- Determines the possible network security attacks that may occur on the organization’s system.Applications Assessments- Tests the web infrastructure for any misconfiguration and known vulnerabilities.Wireless Network Assessments- Determines the vulnerabilities in the organization’s wireless network [4]

VULNERABILITY SCORING SYSTEMS

Common Vulnerability Scoring System (CVSS)-CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores

Common Vulnerabilities and Exposures (CVE)-CVE is a publicly available and free to use list or dictionary of standardized identifiers for common software vulnerabilities and exposure [5]



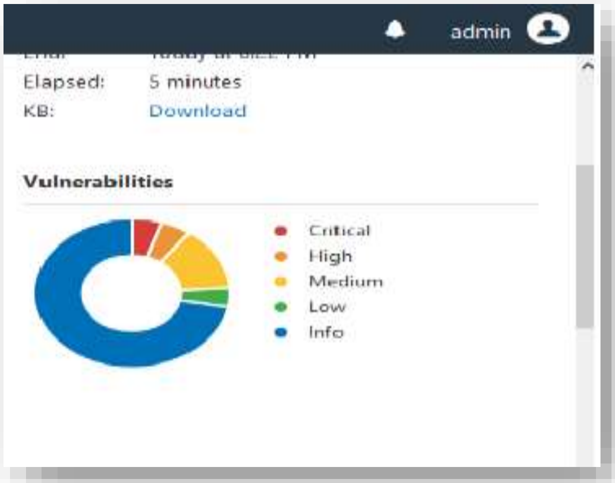
VII:LITERATE REVIEW:

Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology Jai Narayan Goela,b,*, BM Mehtreb a School of Computer and Information Sciences, University of Hyderabad describe- This paper clearly explain necessity to increase use of VAPT for complete system security. This paper would be very helpful for future researchers to get complete knowledge of VAPT process, tools, techniques and its use as a cyber-defence technology. It would be helpful to develop new VAPT techniques and tools.[6] First Principles Vulnerability Assessment ∗ James A. Kupsch Barton P. Miller University of Wisconsin {kupsch,bart} September 2009 describes- Improved the security awareness and processes of the assessed software development teams: As part of our assessment process, we worked with the development teams to incorporate vulnerability reports into their development, patch, and release processes.[7] Vulnerability Assessments in Ethical Hacking Ashiqur Rahman1 , Md. SarwarAlam Rasel2 , Asaduzzaman Noman3 , Shakh Md. Alimuzjaman Alim4 1 (M.Sc in Information Technology (IT), Jahangirnagar University, Bangladesh) 2 (CSE, Royal University of Dhaka, Bangladesh) 3 (CSE, Royal University of Dhaka, Bangladesh) 4 (EEE, Royal University of Dhaka, Bangladesh) describes-Statistics show that the most devastating attacks are partly or completely committed by the company’s own dissatisfied or angry employees, as they try to push an advantage that they believe to be rightful or just. Their intention is not necessarily to cause effective damage to company value.[8] Sensors (Basel). 2018 Mar; 18(3): 817.Published online 2018 Mar . doi: 10.3390/s18030817PMCID: PMC5876893PMID: 29518023Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart HomesBako Ali1 and Ali Ismail Awad1,2,* describes-Applying IoT technology to smart homes yields both opportunities and security risks. IoT-based smart homes are highly vulnerable to different security threats from both inside and outside the home. If smart home or smart device security is compromised, the user’s privacy, personal information and even safety will be at risk. Therefore, appropriate measures have to be taken to make smart homes more secure and suitable to live in. A careful assessment of security risks must precede any security implementation to ensure that all the relevant, underlying problems are first discovered.[9]

Security Assessment of Web ApplicationThrough Penetration System Techniques Akhyar Lubis1 , Avinanta Tarigan2 1Faculty of Computer Science 1Universitas Pembangunan Panca Budi, 2Universitas Gunadarma 1Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing, 20122, Medan, Sumatera Utara, Indonesia 2Jl. Margonda Raya No. 100, 16424, Depok, Indonesia describes-The web application has been developing very fast with the development of programming technologies and newer database storage. It will be harder for testing if a system has been using the new technology. Another alternative is to use an automated application in testing. Success in penetration testing depending on the methodology used. From the discussion, it can be concluded that penetration testing is done to find a weakness or vulnerability to the web application domain and subdomain on www.pancabudi.ac.id. This shows that there are still gaps that allow for exploitation by SQL Injection. Susceptibility results obtained can be a reference to the exploitation of so network administrators can perform patch or covering the hole of these weaknesses.[10]

VIII:OBJECTIVES

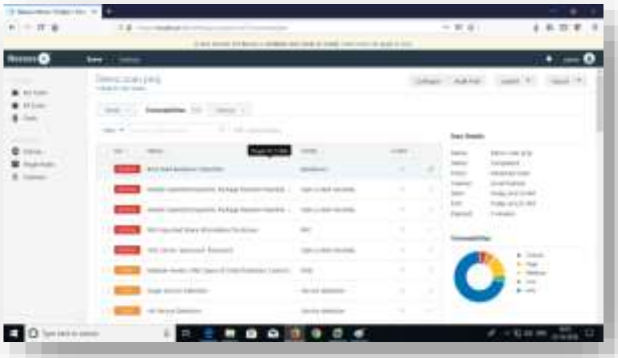
In this case we are using a tool which related to Vulnerability Assessment which represented in above information.In the Nessus scanner we take a target as Metasploitable OS.Metasploitable is an intentionally vulnerable Linux virtual machine that can be used to conduct security training, test security tools, and practice common penetration testing techniques. The scanning takes some time to find the vulnerabilities of the target. We can say the web server also for the metasploitable. After scanning the target Nessus scanner shows the vulnerabilities of the target system in his own format like in color codes. The color codes are used in the Nessus is to show the vulnerabilities level like Critical, High, Medium, Low, & Information.



Elapsed: 5 minutes
KB: Download

Vulnerabilities

We found some Critical Vulnerabilities in the targets IP address which shows in the scanner with the Description and Solution.



This dashboard presents the vulnerabilities discovered in each plugin family grouping and can assist an organization in identifying vulnerabilities, prioritizing remediation's, and tracking remediation progress.

BIND SHELL BACKDOOR DETECTION

It shows the Critical Vulnerability. Nessus Plugin ID 51988 Synopsis: The remote host may have been compromised.

Description:A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.Solution:Verify if the remote host has been compromised, and reinstall the system if necessary.

DEBIAN OPENSSH/OPENSSL PACKAGE RANDOM NUMBER GENERATOR WEAKNESS

It shows the Critical Vulnerability Nessus Plugin ID 32314 Synopsis:The remote SSH host keys are weak.Description:The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.Solution:Consider all ryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated. Debian OpenSSH/OpenSSL Package Random Number Generator WeaknessIt shows the Critical Vulnerability Nessus Plugin ID 32314Synopsis:The remote

SSH host keys are weak. Description:The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.Solution:Consider all ryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

IX:SCOPE:

• In this paper, the proposed scanner uses all possible attacks on the target system and then fined the vulnerabilities from the target. The Nessus scanner is one of the best automation tool in the security testing or for security Audit.

•In the near future, the use of these tool is for Security Audit in various sectors like Banking sector, Government websites and of course IT- Organizations MNC's, Small Scale industry, Mechanical Related Companies and so on.

•The possible use of Nessus Scanner is-Nessus helps the security pros on the front lines quickly and easily identify and fix vulnerabilities - including software flaws, missing patches, malware, and misconfigurations - across a variety of operating systems, devices and applications.

Disadvantages of vulnerability assessment-Vulnerability scanners can be used just as effectively (or even more so) by the "bad guys", otherwise known as black-hat hackers. The problem for websites comes from the fact that many websites are built using a variety of technologies so every update of those individual technologies has the potential to introduce new vulnerabilities. So every IT department is always playing catch-up to update software and, in an ideal world, they would be running a new vulnerability scan after each patch. Because of this, increasingly, hackers are using vulnerability scanners to find holes due to lapses in patching. And the truth is that vulnerability scanners are automated tools also known as bots that are being used all over the internet looking for weaknesses to exploit.

CONCLUSION

With the all above information regarding to the paper we see with the help of Nessus scanner tool it shows us that how many possibilities of vulnerabilities in any host, system and so on.

DYNAMIC ASSET TRACKING:

Track assets and their vulnerabilities with unsurpassed accuracy – even highly dynamic IT assets like mobile devices, virtual machines and cloud instances.

Passive Network Monitoring: Monitor network traffic continuously to detect and assess short-lived systems and hard-to-scan devices, such as sensitive OT and IoT systems.

Automated Cloud Visibility:Achieve continuous visibility and assessment into public cloud environments through our AWS, Microsoft Azure and Google Cloud Platform (GCP) Connectors.

Streamlined User Experience:Benefit from a modern, "data-comes-to-you" user interface with intuitive guidance as well as actionable dashboards to make common tasks like running and prioritizing an assessment easier than ever.[3].

X:REFERENCES-

[1] TechTarget https://searchsecurity.techtarget.com/definition/vulnerability-assessment-vulnerability-analysis

[2]TechTarget https://searchsecurity.techtarget.com/definition/vulnerability-assessment-vulnerability-analysis.

[3] Tenable-https://www.tenable.com/downloads/nessus

[4] Ethical Hacking and Countermeasures v10-EC-Council USA official courseware volumeI Module 05-143-145.

[5] TechTarget https://searchsecurity.techtarget.com/definition/CVSS-Common-Vulnerability-Scoring-System

[6] Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology

Jai Narayan Goela,b,*, BM Mehtreb a School of Computer and Information Sciences, University of Hyderabada School of Computer and Information Sciences, University of Hyderabad, Hyderabad 500046, India b Center for Information Assurance and Management, Institute for Development and Research in Banking Technology, Hyderabad 500057, India

[7] First Principles Vulnerability Assessment ∗ James A. Kupsch Barton P. Miller University of Wisconsin {kupsch,bart}@cs.wisc.edu Eduardo Cesar Elisa Heymann ´ Universitat Autonoma de Barcelona ` {Eduardo.Cesar,Elisa.Heymann}@uab.es September 2009

[8] Vulnerability Assessments in Ethical Hacking Ashiqur Rahman1 , Md. SarwarAlam Rasel2 , Asaduzzaman Noman3 , Shakh Md. Alimuzjaman Alim4 1 (M.Sc in Information Technology (IT), Jahangirnagar University, Bangladesh) 2 (CSE, Royal University of Dhaka, Bangladesh) 3 (CSE, Royal University of Dhaka, Bangladesh) 4 (EEE, Royal University of Dhaka, Bangladesh)

[9] Sensors (Basel). 2018 Mar; 18(3): 817.Published online 2018 Mar 8. doi: 10.3390/s18030817PMCID: PMC5876893PMID: 29518023 Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart HomesBako Ali1 and Ali Ismail Awad1,2,*

[10] Security Assessment of Web ApplicationThrough Penetration System Techniques Akhyar Lubis1 , Avinanta Tarigan2 1Faculty of Computer Science 1Universitas Pembangunan Panca Budi, 2Universitas Gunadarma 1Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing, 20122, Medan, Sumatera Utara, Indonesia 2Jl. Margonda Raya No. 100, 16424, Depok, Indonesia