Pentester and Network Security for a Secure Modern Society

P.D. Panditharathna , K.T Jayatunge , A.Nirojan , S.Srikanth, Mr. Dhishan Dhammearatchi

Sri Lanka Institute of Information Technology Computing (PVT) Ltd

Abstract- In this era attacks against computer system has increased and increasing significantly. Exploit which means component that can harm the system can buy from black-market even. Most of the organizations consider securing the data of their organization from security breaches. One of the way is hiring professional pen testers to find the vulnerability and fix such mitigating risks. To do this task pen testers using automated techniques to gather information of security breaches. Most of the companies willing to hire white, grey hat hackers which we called about as pen testers .In some cases companies consider to hire black hat hacker rather than pen tester who have already been into the system. Reason is it's easy to fix the vulnerability cause by the black hat hacker know the issue already. Sometime pen testers may not be able find that issue. This paper discussed about the current software tools which are using by pentesters, Types of security threats, How important is pen testing to current society?, evolution of pentesting, how secure data in these days and the new ways of pen testing .

Index Terms- Attacks, Exploit , Black-market , Security breaches , Vulnerability , Hackers , Society , Data , Software tools

I. INTRODUCTION

Effective penetration testing involves consist number of activities in real-world attackers with the goal of better understanding and managing business risk to improve the security of a organizations. Real-world attackers undermine modern organizations in a different ways, so penetration testers should be prepared to draw from a variety of different attack types, tools to simulate the real-world threats done by hackers. Skilled penetration testers are familiar with numerous different attack types, and strive to build and reinforce their capabilities in each of these areas.

There are different ways that penetration testing can describe, distributed and marketed. Doing a vulnerability scan, security assessment, penetration testing differentiates from these efforts in a few critical ways. They are,

- A penetration test doesn't stop at simply uncovering security threats
- Penetration tests may involve in use of automated tools and process frameworks, the focus is on the individual or team of pen tester, the experience they bring to the test, and the skills and they leverage in the context of an critical attacks
- A penetration test is designed to answer the question: "What is the real-world effectiveness of existing security controls against an active, human, skilled attacker?"
- A penetration test allows for multiple attack types to be explored against the same target

Basically there are two penetration tests types, they are black box and white box testing. Black box testing is where the third party tester is not willing to distribute any information about the system or network to be tested. It is the most preferable way because it tells you how an outside attacker would see the system and go about breaking into it. In white box testing, pen testers are giving most of the information they need including algorithms, IP addresses and network diagrams. Using this information, testers would be able to identify any weaknesses in the system

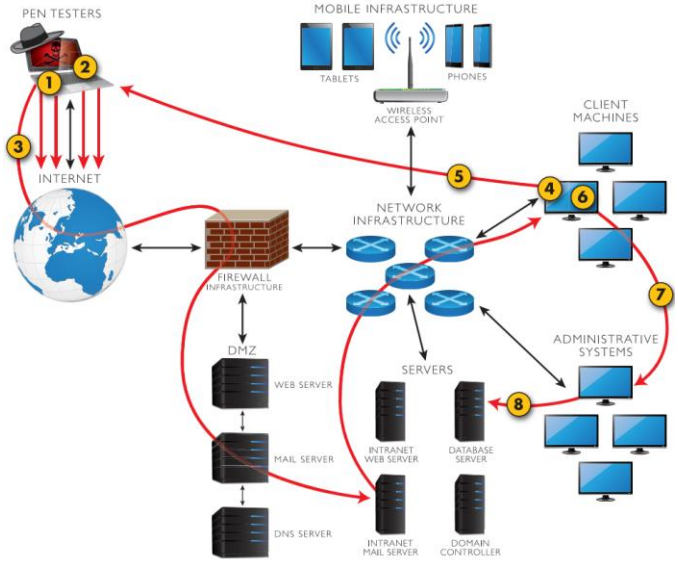

Figure 1
(Source: https://blogs.sans.org/pen-testing/files/2015/02/2015-Poster-Side-2.jpg)

It's difficult to find all security issues in a network using automated tools developed by a security company. There are some vulnerabilities should be conducted by manual scans only. Penetration testers can perform attacks on application according to their skills and knowledge of system being penetrated. Social engineering mostly pen testing can be only done by humans. Manual checking includes design, business logic as well as code verification. Identifying vulnerabilities presents in the target system is the first step in this pen testing process is correct action

is taken on these security risks and same penetration testing are repeating until system at least 90% of free of security attacks

1) Data collection: Various searching methods are used to get the data of a targeted system. One can also use web page source code analysis standards are used to get large amount of valuable information about the system, soft wares and plugins and the version of it. Many free tools and services available in the internet which can give you information like database or table names, Database version, software versions, hardware used in the system.

2) Vulnerability Assessment: Based on the data collected from the step one can find the security weaknesses in a not secure system. This helps penetration testers to launch attacks using identified starting points in the system.

3) Actual Exploit: This is crucial step. This required special skills and techniques to launch attack on the system. Professional penetration testers use their skills to launch attack on the system.

4) Result analyzing and report preparation after completion all the penetration test's detailed reports are prepared for taking reliable actions. All identified vulnerabilities and recommended corrective methods are listed in these reports. Reports can be customized in several formats such as, XML, Excel, MS Word, HTML, or PDF as organization needs.

There is no doubt that penetration tests are very critical where information security is very crucial. Organizations have to make a decision on whether or not to hire professional penetration tester. Costs of penetration tests are depending on the complex and size of the system. Pen testers charge for hourly fee this depends on the pen testers experience also [1]. .

In Section II will cover the background and related works which are similar to pen testing and network security

In Section III Types of security threats, how important is pen testing to current society? Evolution of pentesting, how secure data in these days? and how to prevent those kinds of network security attacks?

Section IV describes the Conclusion

Section V describes the Future works

II. BACKGROUND AND RELATED WORKS

Penetration testing probably feels like the part of security, but it is also a small part. It's also exceptionally broad. This penetration testing is significantly used to mean any one of the following as an umbrella:

- Vulnerability Assessment
- Security Assessment
- Security Audit
- Penetration Test
- Social Engineering

It could be argued that exploit development is actually outside the scope of the term, even though in some engagements custom exploit development may be performed. Just so we're on the same page, let's do a very brief description of what I mean by each of those.

Vulnerability Assessment

In this type of engagement the tester will be attempt to determine, the architecture and properly analyze it for weaknesses. It look to see what services are currently running, the software versions those are, try outs to capture how things are connected and configured together, how it uses the services, and the sort of security protections may be available in place. Taking all that information to identify prospective weaknesses and report on them. This will include findings relating to out of date software versions, weak configurations like using HTTP when they should use HTTPS, no of limited firewalls which are insufficiently used, etc. The whole concept in here is to look for problems and report about those, actually it is not to hack into systems.

Security Assessment

In mostly a security evaluation is a complete vulnerability evaluation followed up with an approach and procedure review. This will allow the assessor to judge, not only if the procedures are in line with policy, but also whether the business unit's plan needs arranged up. This is vital because a technical vulnerability assessment will not explain about whether or not files which are sensitive commonly stored in unlocked file cabinets in the main lobby, or discarded in the normal trash.

Security Audit

Audits can be more likely an assessment, with one specific differentiation. An audit is a strict formal test across a standard which is pre-determined or set of standards. An assessment may use standards like protocols. A report of an assessment will consist of anything the assessor thinks may become a drawback of the organization. An audit, somehow, is limited to testing only from which is described in the standard. The specific intent here is that an audit is very formal, repeatable, and predictable. Mostly audit reports may consist additional, or informational, findings very reminiscent of an assessment. They should not be binding, and they should be used to inform compliance against the tested standard.

Penetration Testing

This is effectively a more thorough form of a Vulnerability Assessment. Once the tester has analyze weaknesses they will then try to exploit those weaknesses. It helps determine whether the findings in the assessment are to be false positives, in the case of a software version that should be vulnerable but contains back ported patches in security. The vulnerabilities will be tested by it against mitigating controls. It is one thing to have a finding that the company's ERP solution is a year behind on patches. It is another to demonstrate that being behind on patches allowed an attacker to get details payroll information. A penetration test will not occasionally involve a specific approach or procedure review unlike a security assessment.

Social Engineering

During a social engineering engagement team will try to con or access the organization in case of ex-filtrate information. This is where you get into the types of things you will normally familiar with movies like spy shows. You will probably do some dumpster diving, experiments to badges, talk your way earlier security, pose as the CEO and attempt to convince the help desk to change your password, etc. As part of a penetration this may sometimes include test but may not sometimes.

In the end, all of these things require specific skills. Some of them are technical, some of them are personal, and some of them are organizational. Your best bet is to start somewhere else to break into the penetration field. It is generally the case that the best way is first know how to make it work and then how to break in to it. The people we have talked to, or read about, who do the best got their beginning as developers, administrators of systems, network administrators, or something more like that. It is essential that at the end of the day you are not hacking into a server for your own fantasy. You are figuring out how things should be break with a beneficial view to notify the client what they are allowed to do to fix it. If your report cannot be consisted of suggested recommendations on the TNS listener then it does not actually a problem whether you accessed the database.

Reporting a hack with proper recommendations are useful to the client. Therefore just simple report will not satisfied this need. And it would make your employer look bad as much you would be doing a harm to him [2][3].

Similar Researches

Acunetix an automated web vulnerabilities application security testing tool that audits web applications by checking for vulnerabilities such as SQL Injection, Cross site scripting, and other exploitable vulnerabilities It uses web-server based installation. For testing purposes, interacting with the console. . At the time of this writing, AcuSensor is used primarily with PHP and .NET web applications. It identifies more vulnerabilities than a traditional black box web security scanner and reduces false positives. Acunetix allows WVS to find such vulnerabilities, including XSS, Server Side Request Forgery and Email Header Injection. Another ability is search for subdomains based on DNS records automatically [4]

W3af Identify vulnerabilities like SQL Injection, Cross-Site Scripting, Guessable credentials, unhandled application errors and PHP misconfigurations. Web Service support. Exploits .OS commanding, remote file inclusions, local file inclusions, XSS, unsafe file uploads and more.WML Support (WAP). w3af is divided in two main parts, the core and the pluging.This coordinates the process and provides features that plugins consume. Plugins share information with each other using a knowledge base [5].

Burp Proxy is a HTTP/S proxy server for attacking and testing web applications. It operates as a man-in-the-middle between two end points of servers, and allows the user to intercept, inspect and modify the raw traffic passing in both directions. It uses various intelligent techniques to generate a content and functionality. It is developed for penetration testers, and to fit in closely with existing techniques and methodologies for performing manual and semi-automated penetration tests of web applications. Manually modifying and reissuing individual HTTP requests, and analyzing their response. Transforming raw data into encrypted format. It is capable of intelligently recognizing several encoding formats using heuristic technique. It is an automating customized attacks against web applications [6].

Grendel-Scan is an open-source web security testing tool which has an automated testing module for detecting common web application vulnerabilities. It has the ability to find simple web application vulnerabilities, but its designers state that no automated tool can identify complicated vulnerabilities, such as logic and design flaws. Grendel-Scan tests for SQL injection, XSS attacks, and session management vulnerabilities, as well as other vulnerabilities. Grendel Scan is a powerful web application scanner that can help identify potential security gaps across websites. It has many features which are useful tool for pen testers, in particular those who may not have much (or any) penetration testing experience across their web applications [7].

Web Scarab is a framework for applications that communicate using the HTTP and HTTPS protocols. It is written in Java, many other platforms. It has several modes of operation, implemented by a number of plugins. Common usage of Web Scarab operates is an intercepting proxy, allowing the operator to review and modify requests created from browser before data sent to the server, and to review and modify responses returned from the server before they are received by the browser. Web Scarab is able to intercept both HTTP and HTTPS communications. The operator can also review the conversations (requests and responses) that have passed through web Scarab. Web Scarab provides some features and plugins that will aid the pen-tester to get a solid understanding about a web application's behavior[8].

IronWASP is an open source system for web security vulnerability scanner.pentesters can create their own custom security. Expert user with Python/Ruby scripting expertise would be able get the full potential of the platform, a lot of the tool's features are simple to be used by absolute beginners.it has the features of Full & Semi Automated Scans, Scan Customization Option and High Scan Precision: Scan 1 Parameter of 1 Request for 1 Active Plugin. It did however, make a clean (and unexpected) take away by being the only winner in the new and hidden Invalidated Redirect category[9].

Qualys Express is a cloud-based kit for security and compliance solutions for small businesses with limited budgets and staff. It monitors browser whether Internet perimeter servers, websites and web apps are up to date and securely configured. It even lets you extend the same protection to internal computers to make your organizations secure, inside and out. It express from Qualys uses the software-as-a-service (SaaS) model to provide vulnerability and compliance management services to customers. It combines vulnerability scanner,PCI compliance, along with web application scanning and malware detection, into a single hosted console. This offers both security novices and veterans an easy way to maintain awareness and as this reduces the time it takes to do a full test, allows to work more efficiently. This does functions such as RXSS, SQLi, webapp scanner, WebApp Scanner, Web Service scanner, CGI Scanner. [10]

VEGA is a free and open source scanner and testing platform to test the security of web applications. It can help you

find and validate SQL Injection, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities. It is written in Java, GUI based, and runs on Linux, OS X, and Windows. Thus it includes an automated scanner for quick tests and an intercepting proxy for tactical inspection. The Vega scanner finds XSS (cross-site scripting), SQL injection, and other vulnerabilities. Vega can be extended using a powerful API in the language of the web: JavaScript. This contains with functions such as RXSS, SQLi, LFI, RFI, WebApp Scanner. Automated Crawler and Vulnerability Scanner, Customizable alerts, SSL MITM, Database and Shared Data Model are some of the features of it. [11]

III. Our Approach

Network Security Types

Network security is different kind of activities which is design to secure the network. These kind of activities mainly consider about usability, reliability, safety of network and data of network. The main topic which directly connect to the network security is network security attack. Current day's large number of companies, people, and governments willing know the others secrets which is more crucial to those parties. Those data can be cost more than millions of dollars. So in victim's side they are hiring the professional pentesters.in society side the hacker rate is increasing significantly. According to the Mcfee which is a largest network security technology company these types of attacks are commonly used by hacker.

DDOS (Distributed denial of service) attacks are used to make an online service unavailable by increasing the traffic to the source service from multiple sources. Most of the free software's are being downloaded from the torrent sites contains Trojans which can be used to DDOS attacks. According to the Arbor network's ATLAS threat report more than 2000 daily DDOS attacks are discovered. VeriSign/Merril Research states that 1/3 all the online downtime incidents happened because of DDOS attack. DDoS attacks come in many different forms, from Smurfs to Teardrops, to Pings of Death Common types of DDOS attacks are

1. Traffic attack : traffic flooding attacks send a huge volume of TCP, UDP and ICPM packets to the target.
2. Bandwidth attacks: overloads the target with massive amounts of junk data.
3. Application attacks: Application-layer data messages can deplete resources in the application layer, leaving the target's system services unavailable.

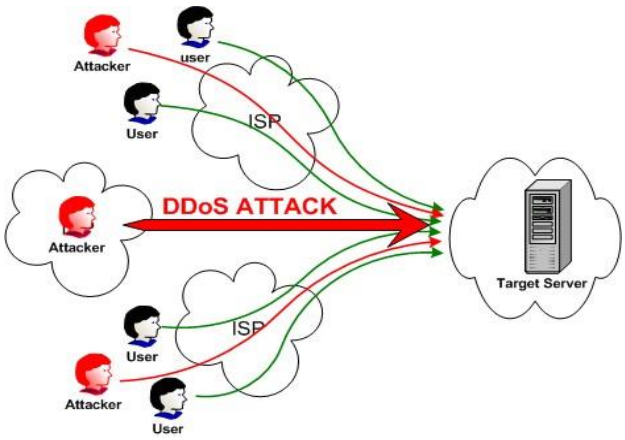

Figure 2
(Source:http://info.singtel.com/business/products-and-services/internet/singnet-ddos-protect)

Brute force is attack type use to decrypt a encrypted file with the help of a software. This encrypt file contains valuable datas. To brute force there is large portion of words in single file to test whether data file can be decrypt using those words one by one. This is very time consuming process. Time can be depend on the encryption algorithm also.so the hackers connect to fast server and execute the software. Ars Technical reported that a 25-GPU cluster could crack every Windows password which uses NTLM algorithm under 8 characters in less than six hours.

Eavesdropping (sniffing) is intercepting the communication between to end-points. To this there are many specialized eavesdropping tools available. Specialized program used to check the packet data transfer between to end point and then use cryptography to get the data from those packets. Depending on the network sniffing can be effective Lan Environment with hubs: Very easy because hubs duplicate every network frame to all ports Lan Environment switches only transfer a frame to the port.to this arp spoof mechanism used WAN Environment: to this sniffing pc router between the client server communications. One way to implement this exploit is with a DNS spoof attacks to the client.

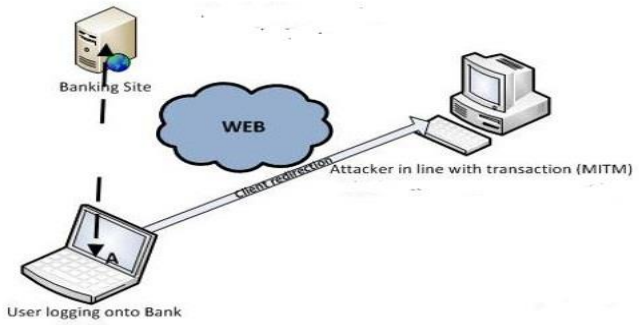

Figure 3
(Source: http://www.valencynetworks.com/images/mitm-attack1.png)

Earlier day's security risk affects only for Windows Systems' new vulnerability have found that affects the most versions of the Linux and UNIX operating systems this call shell shock and Bashbug. Bash used as command language interpreter in Linux and Unix systems. New vulnerability is Bash can also be used to run commands passed to it by application. One type of command send environment variables. Environment variable are affects the way processes run on computer. Symantec regards this vulnerability as critical, since Bash is highly used in Linux and UNIX operating systems running on Internet-connected computers, such as Web servers.

Browser attacks is security attack where attacker installs a Trojan horse in victim's computer and capable of modifying the web transaction happening real time .Many experienced web user are aware of scams and phishing. These can be identify trough link from any other notification. But the uniqueness of this browser attack method is the transaction happened only when normally expected prompts and password requirements.

Points of effect:

Browser Helper Objects – dynamically-loaded libraries loaded to Internet Explorer upon startup

Extensions – the equivalent to Browser Helper Objects for Firefox Browser

API-Hooking –Technique used by Man-in-the-Browser to perform its Man-in-the-Middle between the executable application and its libraries

JavaScript – By using a malicious Ajax worm, as described on Ajax Sniffer

Botnets (zombie army) are interconnected network computer which are infected with a malware which users doesn't know and controlled by hackers in order to perform tasks. Botnets use to send scam email transmit viruses and etc. Botnets are considered as a biggest online threat today. Botnets is capable of developing a large-scale DDOS attacks. Botnet uses left opened internet port and from a small Trojan horse program those left opened ports can be left for future activations. In a particular time, the zombie army controller can unleash the effects of the army by sending a single command, possibly from an Internet Relay Channel [12].

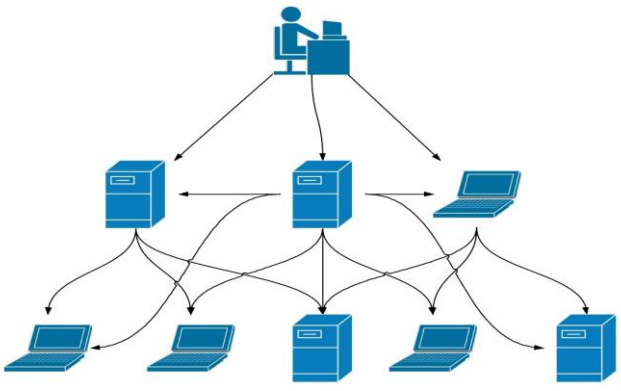

Figure 4
(Source:https://www.chmag.in/system/files/jan2011/momsguide_1.png)

Evolution of pen testing

A penetration test, occasionally pen test, is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat Hacker, or Cracker. Regarding the evolution of pentesting, it can be divided into four eras. In the first era, 1993 Dan Farmer and Wietse Venema have found Black hat methodologies which means that it improves the security of your site by breaking into it. Actual purpose was to Penetration from the Internet. Methods were not formal, state of art. Screenshots with shell and couple of words were the results of pentest.one of the main objectives at that time was to prove that networks are vulnerable those is shown in figure one. Therefore to show the business industry that there is a need in security because at that time many people were not believing it. After 2000, in the second era it used more complex pentesting. The purpose was to penetration from the internet and hacking web sites. The first version of OSSTMM, Programs like CORE IMPACT were the methods used back then. Report with vulnerabilities and their countermeasures were the results of pen testing. This was a part of SDLC for WEB development after secure development and code analysis.

Middle 2000, in the third era networking become better and there is a need to assess security more deeply. There were several objects such as Wireless, SCADA, Users (social engineering), DBMS, Applications, ERP and Mobile. The purpose was to Deep assessment of an application or technology.it used OWASP, WASC, OWASP-EAS, OSTMM, NIST and ISSAF as methods. Training: Blackhat/HITB/Offensive security and CEH, CREST, CPT, GPEN Certifications were the two main teaching. Standardized reports with the list of vulnerabilities, their risks and countermeasures gives the results of pen test. This was Part of PDCA for Application/Technology implementation.

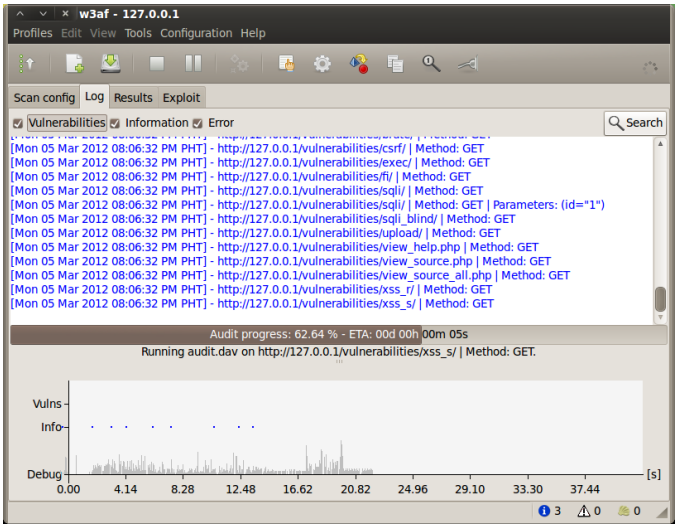

Figure 5
(Source:http://2.bp.blogspot.com/-DX7otj2qBdY/T1Ssp_poKhI/AAAAAAAAAWU/fiHjjX3Cyu8/s1600/w3af.png)

The fourth era is known to be the Business-oriented Pentest, Business-critical systems were the main objects. The purpose is to show how technical vulnerabilities can be used for

business threats. OSTMM, NIST, ISSAF with business process analysis were the methodologies. All that we have plus business-process analysis, specific knowledge of business area were the teaching. The results of pen test report that shows real business risks which can cause Fraud, Sabotage and Espionage [13].

How important is Penetration Testing to current society

As many Web applications are developed daily and used extensively, it becomes important for developers and testers to improve these application securities. Pen testing is a technique that helps these developers and testers to ensure that the security levels of their Web application are at acceptable level to be used safely. Different tools are available for Pen testing Web applications. Nowadays, Web applications are used worldwide by users for their personal needs but what make Web applications more and more important are the business intentions to use the Web. Currently, most of the businesses provide services to its customers using the Web and many of them depend on the Web to do their business in order to make benefits from the global accessibility of the Web. For example, E-commerce is a novel commerce model based on computer network; the E-commerce model depends mainly on money and whenever you find money in any filed, risks become higher and new type of attacker who have a mission to steal money from you not just for fun and self-motivation will be founded. The benefit of penetration testing is increased security and security awareness for organization. It will provide with in-depth, actionable reporting and analysis to facilitate planning, strategies, and provide practical solutions to the organization security deficiencies. Organization will learn the attacks their systems and networks are vulnerable to. We will understand whether or not your current defenses would protect your organization against viable attacks. Your high-risk vulnerabilities will be exposed. Possibly the most important benefit of penetration testing, using an external party, is that the knowledge gained will help both management and staff to see the "security truth" and will dispel myths of "it couldn't happen to us." A third party offers an unbiased, realistic measure of your existing security and provides expert remediation to help mitigate risk and align with best security practices. While penetration testing is the ultimate tool for hardening overall security to the organization.

Penetration testing occurs when organizations engage trusted third-party security professionals to simulate attacks by real intruders against their systems, infrastructure, and people. Penetration testing provides you with a thorough analysis of the current security of your organization. The results of penetration testing are presented in an executive report that contains details of the existing security posture of your organization, possible consequences of an actual attack, and, normally. Penetration testing is the most thorough possible analysis of your security because actual vulnerabilities found are exploited to understand the depth and breadth of how your organization can be compromised. Your organization will be able to understand its current level of security and the consequences of an attacker breaking in through your defenses. Application penetration testing is the ultimate, indispensable method for ensuring application security in the modern age of targeted cyber threats against software. Application penetration testing plays the critical role to any application against potential attacks. Until you have a third party, with no ties to the development or business attack it "full out", like a thief going for it all or siphoning off a piece of everything, or a saboteur who just wants to bring you down entirely and "erase" you. . . . Until you

Undergo these mock attacks, you will never know how well (or if) you will survive a targeted attack. Application penetration testing will expose any security weakness that is the result of your application's interaction with the rest of your IT infrastructure. You will be shown how our team exploited vulnerabilities to gain unauthorized access and violate security. You will also receive strategies and recommendations on the steps that you should take to mitigate these vulnerabilities. One of the most important organizational goals is security awareness regarding software development. It consistently find that the well-earned confidence of internal development team at making impressive software, with a great user experience, tends to lead to an overestimation of the development team's (or an application's) security capabilities. Software security is in itself a highly specialized field of study. After application passes through the application penetration testing process, and the normal depth and breadth of security flaws are uncovered, we will gravitate to a better understanding of up-to-date security requirements. System will help understand the flaws of software development lifecycle (SDLC), how we exploited them, and then instill better development and deployment practices moving forward [14].

How secure data in these days and the new ways of pen testing?

Tons of data store in the internet either business or individual it is important to keep secure the data from access to unauthorized people. Data protection and vulnerability assessment method reconstruct since the begin. In the current trend IT people they have wisely methods to protect the data. Recently they introduce white hat [15] , there they create a dummy hacker by themself who identify the security weakness in a computer system or network. Before the real hacker access the data, according to state the system owner that will fix it.

The next current trend is ethical hacking, Businesses and government-related organizations that are serious about their network security hire ethical hackers and penetration testers to help problem and improve their networks, ethical hacker [16] who will perform by an individual or company to aid to identify the security weakness in a computer system or network. Ethical hacker will attempt to bypass the security boarder this information will help to improve the system security and eliminate any potential attacks. By conducting penetration tests, they will look some basic question [17]

What information/locations/systems can an attacker gain access? What can an attacker see on the target? What can an attacker do with available information? Does anyone at the target system notice the attempts?

How to prevent security attacks?

Computer security is a process of prevention and detection unauthorized usage computers. Prevention helps to stop unauthorized access to a computer system. Detection helps you to determine whether or not someone attempted to break into your system. Team has found many preventing methods some of them discussed below.DLP appliances allows to track the travel

of data in real time or by collecting data and summarizing it in daily or weekly reports. DLP system that can intercept and read SSL or other encrypted messages, or users will be able to defeat the purpose simply by data encryption they send outside the network. DLP appliances and firewalls focus on traffic being sent outside the network. Use packet inspecting tools like Network Analysis and Visibility (NAV) products to inspect the data of packets moving within the internal network.NAV tools can examine the contents in deep and look for similar words or types of data inside a document or file.

Powerful way is using a firewall. Most modern firewalls are capable of filtering both inbound and outbound traffic, but many firewalls configured for only control the former. Set up outbound rules on firewall to explicitly block or allow the network traffic that matches the criteria. Encrypting sensitive data will make it more difficult for those inside the network be able to manage information even if they do manage to intercept it and take it outside. Encrypted data cannot be read without specific algorithms. even hacker got the data they cannot use them in any harm manner without decrypting it.This is a very effective way of securing the data from outsiders.Virus guards are very common way of securing the personal data. Installing virus guards does not let install any soft wares that are harmful to the computer system or misuse its specification(DDOS).There are many virus guard which are very powerful and easy to use (Kaspersky , Norton , AVG etc.)

Limits the number of allowed login attempts for an IP Address. It allows to manually block an IP address from logging into system. It delays execution after a failed login attempt helps to prevent brute force attacks.

If any critical data is required to register to a site it is good to make sure whether it is HTTPS secured sites. Most of browser are warning before go to harmful site.

IV. Conclusion

This paper discussed, for systems to remain secure, the security posture must be evaluated and improved continuously. Establishing the organizational structure that will support this ongoing improvements is essential in order to maintain control of cooperate information systems. Penetration tests offer unparalleled insight into an organization's security effectiveness as well as a road map for enhancing security. By hiring experts to simulate a cyber-attack, vulnerabilities can be identified and corrected before they are exploited by a hacker or malicious insider. Therefore team has found many general preventing methods such as limits the number of allowed login attempts for an IP Address, using HTTPS secured sites when critical data is required to register to a site, installing powerful virus guards, Encrypting sensitive data. Apart from these it has found powerful factors in the manner of DLP appliances and firewalls, which focus on traffic being sent outside the network. Use packet inspection tools such as Network Analysis and Visibility (NAV) products to inspect the contents of packets moving within the internal network.NAV tools can examine the contents in great depth and look for particular words or types of data within a document or file. However it is essential that appropriate efforts should be undertaken in the proposed methods to introduce effective network security, which could help mitigate the effect of security failures.

V. Future Work

Pen testing strategies are now converted from one shot a year exercise to annual programs, where secure code review, static and dynamic, is combined with penetration test of targeted areas. The financial sector, in particular, considers penetration testing as an annual product, versus a one-time service. Professional firms use human intellect and tools to make whole code exploitations of cybersecurity and development practices with emphasis on testing components. Effective penetration testing teams will consist of 3-5 highly trained professionals and specialists, executing the pen test assignment with well-rehearsed scrum efficacy, communication, division of tasks, re-prioritizing backlog, tracking, addressing new issues, and re-focusing to maximize value of both individual and the team contribution, commitment and ownership of the project from start to end. Teams adapting lean methodologies would typically achieve individual contributors of same background. As cyber security product vendors make products better at capturing the critical attacks, attackers will be forced to evolve their attacks as well as their skillset. The human factor is always play a big part since humans are the ones that can make the greatest security technology in the world completely useless by not configuring it correctly or by being social-engineered to turn it off. PowerShell in Windows also a growing attack vector as it does not trip AV. So team imagine using a system's tools against itself will also play a part in the types of attacks we see a lot of in the future.

Acknowledgement

We acknowledge with gratitude to the motivation, the valuable services and assistance contributed by Mr. Dhishan Dhammearatchi.

References

[1] Attack surfaces tools and techniques, in Sans org, available at https://uk.sans.org/posters/attack_surfaces_tools_and_techniques.pdf [Viewed- 1st March 2016]

[2] Pen tration testing, in pcsec.gr, available at: http://www.pcsec.gr/penetration-testing.html [Viewed- 2nd March 2016]

[3] 2016.[Online].Available: http://searchsecurity.techtarget.com/answer/How-security-audits-vulnerability-assessments-and-penetration-tests-differ.[Accessed:07- Mar- 2016]..

[4] 2016.[Online].Available:https://www.cccure.org/Documents/acunetix/acunetix.pdf. [Accessed: 07- Mar- 2016].

[5] "W3af",Wikipedia,2016.[Online].Available: https://en.wikipedia.org/wiki/W3af. [Accessed: 07- Mar- 2016].

[6] "BurpSuite - Proxy and Vulnerability Scanner", Sitexposure.net, 2016. [Online]. Available: https://sitexposure.net/b/BurpSuite---Proxy-and-Vulnerability-Scanner/bid/1000018/seqid/16. [Accessed: 07- Mar- 2016]

[7] 2016. [Online]. Available: http://securitymusings.com/article/927/test-web-applications-with-grendel-scan. [Accessed: 07- Mar- 2016].

[8] "Webscarab – An Overview - InfoSec Resources", InfoSec Resources, 2013.[Online].Available: http://resources.infosecinstitute.com/webscarab-an-overview/. [Accessed: 07- Mar- 2016].

[9] "IronWASP - Open Source Web Security Testing Platform - Darknet - The Darkside", Darknet - The Darkside, 2014. [Online]. Available: http://www.darknet.org.uk/2014/08/ironwasp-open-source-web-security-testing-platform/. [Accessed: 07- Mar- 2016].

[10] 2016. [Online]. Available: https://www.qualys.com/docs/qualys-express-lite-brief.pdf. [Accessed: 07- Mar- 2016]

[11] [3]"Windows | SOLDIERX.COM", Soldierx.com, 2016. [Online]. Available: https://www.soldierx.com/tools/Operating-System/Windows?page=4. [Accessed: 07- Mar- 2016]

[12] 2016. [Online]. Available: http://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/. [Accessed: 04- Mar- 2016]

[13] 2016.[Online].Available: http://dsecrg.com/files/pub/pdf/Evolution%20of%20Penetration%20Testing_eng_edited.pdf [Accessed: 01- Mar- 2016]

[14] K. Mitnick, "World's Best Penetration Testing by Kevin Mitnick & Mitnick Security", Mitnicksecurity.com, 2016. [Online]. Available: https://www.mitnicksecurity.com/S=0/security/information/penetration-testing. [Accessed: 01- Mar- 2016].

[15] SearchSecurity, "What is white hat? - Definition from WhatIs.com", 2016. [Online]. Available: http://searchsecurity.techtarget.com/definition/white-hat. [Accessed: 01- Mar- 2016].

[16] SearchSecurity, "What is ethical hacker? - Definition from WhatIs.com", 2016. [Online]. Available: http://searchsecurity.techtarget.com/definition/ethical-hacker. [Accessed: 01- Mar- 2016].

[17] Wiki.cas.mcmaster.ca, "Ethical Hacking - Computing and Software Wiki", 2016. [Online]. Available: http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking. [Accessed: 01- Mar- 2016].

AUTHORS

First Author – P.D Panditharathna, Sri Lanka Institute of Information Technology Computing (PVT) Ltd
Second Author – K.T Jayatunge, Sri Lanka Institute of Information Technology Computing (PVT) Ltd
Third Author – A.Nirojan, Sri Lanka Institute of Information Technology Computing (PVT) Ltd
Fourth Author – S.Srikanth, Sri Lanka Institute of Information Technology Computing (PVT) Ltd
Fifth Author – Mr. Dhishan Dhammearatchi, Sri Lanka Institute of Information Technology Computing (PVT) Ltd