International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal |www.ijtsrd.com
No: 2456 - 6470 |Conference Issue – ICDEBI-2018
INTERNATIONAL CONFERENCE ON DIGITAL ECONOMY AND ITS IMPACT ON BUSINESS AND INDUSTRY
Organised By: V. P. Institute of Management Studies & Research, Sangli

New Era of Web Security by Implementing of Penetration Testing

Mr. Vibhurushi Chotaliya, Miss Fiyona Mistry
Student, B.P. College of Computer Studies, KSV University, Gandhinagar, Gujarat, India

ABSTRACT
Computer and network security are one in every of the foremost difficult topics within the data Technology analysis community. Web security could be vital subjects which will have an effect on a large vary of web users. People, who use web to sell, purchase and even to speak desires their communications to be safe and secure. This paper is discussing the various aspects of web and networking security and weakness. Main components of networking security techniques like the firewalls, passwords, encryption, authentication and integrity also are mentioned during this paper. This paper handles completely different net attacks and additionally offer some tricks employed by hackers to hack the net world equally it contains a shot has been created to investigate impact of DOS, SQL injection, Cross site scripting, Sniffing/ Request secret writing on net application in terms of outturn and latency etc. The anatomy of an internet applications attack and also the attack techniques also are lined in details. The protection of high-speed web because the growth of its use has stained the bounds of existing network security measures. Therefore, alternative security defense techniques associated with securing of high-speed web and laptop security within the world ar studied similarly like, DNS, One-Time word and defensive the network as a full. This paper is additionally surveyed the worm epidemics within the high-speed networks and their unexampled rates unfold.

KEYWORDS: *Network Security, Security Techniques, website protection, Penetration, website security investigation.*

1. INTRODUCTION
Penetration testing may be a accepted methodology for actively evaluating associate degreed assessing the safety of a network or associate degree in-formation system by simulating associate degree attack from an attacker's perspective. A penetration tester should essentially follow bound methodology therefore on with success establish the threats faced by associate degree organization's network or info assets from a hacker associate degreed scale back an organization's IT security prices by providing a stronger come on security investments. This paper provides an summary of methodology of penetration test-ing and also the tools used.

This approved arrange to appraise the safety of a network or associate degree infrastructure by safely making an attempt to use the vulnerabilities helps find the loop holes within the network. These loopholes might enable associate degree offender to intrude and exploit the vulnerabilities.

Penetration tests will have serious consequences for the net-work on that they're run. If it's being badly conducted it will cause congestion and systems blinking. Within the worst case situation, it may end up within the precisely the issue it's supposed to stop. This is often the compromise of the systems by unauthorized intruders. it's thus very important to possess consent from the management of a company before conducting a penetration check on its systems or network. [4]

1.1 Necessity of Network Penetration check
1. The IT infrastructure is changing into a lot of advanced and wider. the interior networks are given access over the net to the legitimate users beside the user credentials and also the privilege

level, after all placed outside the firewall. This will increase the surface of attack. Such infrastructure has to be assessed often for security threats.
2. Identification of what form of resources area unit exposed to the outer world, determinant the safety risk involved in it, detective work the attainable sorts of attacks and preventing those attacks.

1.2 advantages of Penetration Testing

1. Proactive identification of the criticality of the vulnerabilities and false positives given by the auto-mated scanners. This helps in prioritizing the remedy action, whether or not the vulnerability is to be patched straightaway or not supported the criticality.
2. Penetration testing helps compliant the audit regulatory standards like PCI DSS, HIPAA and GLBA. This avoids the massive fines for non-compliance.
3. A security breach might value heavily to associate degree organization. There could also be a network period resulting in an important business loss. Penetration testing helps in avoiding these monetary falls by distinguishing and ad-dressing the risks. [4]

Depending on the requirements, there are a unit 2 sorts of penetration testing.

1. External Penetration check – This check shows what a hacker will see into the network and exploits the vulnerabilities seen over the net. Here the threat is from associate degree external network from web. This check is performed over the net, bypassing the firewall.
2. Internal Penetration check – This check shows risks from at intervals the network. for instance, what threat an interior discontented worker will cause to the network. This check is performed by connecting to the interior local area network.

Depending on the data, there are a unit 3 sorts of penetration testing, Black box, White box and grey box. [6]

1. Recorder – This check is administrated with zero data concerning the network. The tester is needed to accumulate data victimization penetration testing tools or social engineering techniques. The in public offered info over web could also be employed by the penetration tester.
2. White Box – This check is termed complete know-ledge testing. Testers area unit given full info concerning the target network

   The information will be the host science addresses, Domains in hand by the company, Applications and their versions, Network diagrams, security defences like IPS or IDS within the network.
3. Grey Box – The tester simulates an enclosed employee. The tester is given AN account on the internal network and commonplace access to the network. This check assesses internal threats from workers at intervals the corporate.

2. STEPS IN PENETRATION TESTING METHODOLOGY

2.1 Preparation for a Network Penetration check

To carry out a thorough penetration testing and create it a hit, there ought to be a correct goal outlined for a penetration tester. A gathering between the penetration checker and also the organization which needs a penetration test should be command. The meeting ought to clearly outline the scope and also the goal of the check. The network Diagram should be provided to the Pen tester* just in case of a white box penetration testing to spot all the crucial devices that need penetration testing to be done, this is often not needed just in case of a recording machine check.

Another vital agenda of the meeting ought to be the time window and also the period of the check. The organization should clearly outline the time window which can be its non-business hours. This is often to make sure that the Pen tester isn't interrupted and conjointly the business of the organization is unaffected. Thanks to the weird traffic usage by the pen check might cause network congestion or might bring down the network by blinking the systems. for example, a Denial –Of- Service check meted out on a web payment entry might cause the disruption within the network and inflicting inconvenience to the purchasers thereby acquisition loss to the organization.

Pen checker ought to ensure that any data or knowledge obtained throughout the test ought to be either destroyed or unbroken confidential. this is often a awfully vital precaution to be taken. The organization will sue the pen testers otherwise.

2.2 The vital Steps followed in a thorough Penetration Testing

2.2.1 Intelligence or operation

This is a awfully vital step a Pen tester should follow. When the pre coming up with and also the goal definition, the pen tester should gather the maximum amount data as potential regarding the target net-work.vital to notice, this is often the case once it's a recording machine testing and once the organization has not provided any data to the tester.

A Pen tester should gather data from AN attacker's perspective. Something that's helpful to attackers is critical to be collected:

- Network Diagrams
- IP Addresses
- Domain names
- Device kind
- Applications and their versions.
- Security defenses like IDS, IPS.

To gather this data we glance into:

A. Google & Social or skilled networking web-sites
B. Monster.com
C. science Registries
D. DNS Registrars
E. The Company's web site.

2.2.1.1 Google & Social or skilled Networking Websites:

Search with the keyword beside the corporate name. The relevant data from the search results will be selected. For example, search with the keyword „AS A firewall" with the corporate name „Demo Bank". A LinkedIn profile of a worker performing at Demo Bank will be obtained because the search results. By this we will get to understand that Demo bank's network contains of AS a Firewall. Resumes of the employees provide out heap of knowledge.

2.2.1.2 Monster.com:

Lot of knowledge will be obtained from the task Sites. Search with the corporate name and also the list of search results seem, which provides data relating to the network de-vices or the applications victimization that the company's network infrastructure is made.

2.2.1.3 Science Registries:

When the science Addresses aren't provided by the organization, the Pen tester has got to resolve the block of science addresses be-longing to the organization. Science Address registries facilitate America to find them.

- ARIN – yankee register for net Numbers. US Region.
- RIPE - Réseaux science Européens. Could be a cooperative fo-rum receptive all parties curious about wide space science networks in Europe.
- APNIC – Asia Pacific Network data Centre. Asia Pacific region.

For instance, to seek out the block of science addresses happiness to Google. Enter the key word Google in http://whois.arin.net/ui. [1][5]

2.2.1.4 DNS Registrars:

Use the Whois.net or the other who is databases to seek out all the sub domains. lookup is another windows tool to seek out the science addresses related to the given name, to seek out the name server and for zone transfers. AN example is as shown within the screenshot below.

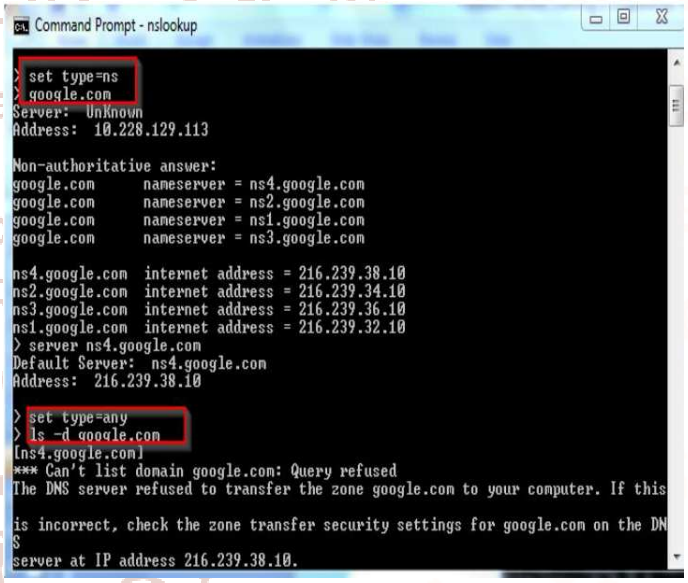

Figure 1: NSLookup

Techniques	Open Source Search	Name, admin, IPaddresses, name servers	DNS Zone Transfer
Tools	Google Search Engine	Who is ARIN APNIC	Nslookupls Dig deeper Sam spade

3. CONCLUSIONS

A network will ne'er be utterly secure. A Pen tester ought to have the data of however a hacker can work to penetrate the network by finding new loop holes and vulnerabilities. There square measure zero-day attacks that return up daily. The network ought to be totally patched with the newest OS and therefore the patches for the software package put in. Penetration take a look at ought to be frequently performed. each quarterly could be a recommended period of your time for a perfect pen take a look at. [3]

Amidst varied constraints like lack of your time and improper definition of scope of the project, penetration take a look ater has got to perform the test to the most effective of the potency by creating use of the tools well. it's higher to own tiny automation scripts for time intense tasks.

4. FUTURE SCOPE

Hackers square measure finding a lot of and other ways everyday to penetrate through the network. There square measure Zero-day attacks which require heap of your time and new tools to be discovered to safe guard the network. There's a demand to develop new penetration testing tools, than looking forward to the present previous ones. New methodologies and processes square measure to be discovered and enforced to create the penetration testing a lot of complete.

5. REFERENCES

1. Chan Tuck Wai "Conducting a Penetration Test on an Organization"
2. C. Edward Chow "Penetrate Testing". http://www.coursehero.com/file/2835086/penetrateTest/
3. AnandSudula, SSA Global Technologies " Penetration Testing". http://www.docstoc.com/docs/36432625/Penetration-Testing-Penetration-Testing-Anand-Sudula-CISA-CISSP-SSA-Global-Technologies
4. Hemil Shah "Writing NASL Scripts" URL: http://www.infosecwriters.com/text_resources/pdf/NASL_HShah.pdf
5. Nmap download URL: http://www.nmap.org
6. Nessus download URL: http://www.tenable.com/products/nessus
7. Owasp URL: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
8. Timothy P. Layton, Sr. "Penetration Studies – A Technical Overview". URL: http://www.sans.org/reading-room/whitepapers/testing/penetration-studies-technical-overview-267
9. SANS Institute InfoSec Reading Room " Penetration Testing: The Third Party Hacker " URL: http://www.sans.org/reading-room/whitepapers/testing/penetration-testing-third-party-hacker-264