ISSN:0975-9646

Penetration Testing

Raghavendra Pokuri[1], Chanikya Merugu[2], Naveen Battula[3]

[1] *Jawaharlal Nehru Technological University, India,*
[2]*VNR Vignana Jyothi Institute of Engineering and Technology, India,*
[3]*Jawaharlal Nehru Technological University, India,*

***Abstract*- Use of existing popular technologies for network malware detection and management has been explored by several professionals in recent times. However, most of the works either deal with anomaly detection strategies or address the issue of network attacks control through routine, yet standard practices. To the best of our knowledge, no effort has been made so far to develop a comprehensive testing system that automatically detects, monitors and controls the network attacks. The aim of this paper is to draft a comprehensive and a systematic pen testing methodology for detection of malicious programs in real-time and to devise an effective scheme for management of a robust penetration testing environment. In this paper, we discussed some of the most widely used terms and their variants. Finally, we dealt with the intricacies of a robust penetration test based vulnerability detection and management scheme to overcome the existing problems. Further, we have mentioned the name of effective tools that are used in various stages of penetration testing.**

***Keywords*-Pen testing, Penetration testing, Attack Vector, Privilege Escalation, Remote Vulnerability, Local Vulnerability.**

Penetration testing is well known to the networking world as pen testing. It is the standard practice of assessing the applications, systems and protocols with the intention of determining the vulnerabilities that an attacker or a cyber criminal could exploit by simulating multiple threats. Several organizations perform penetration testing to obviate data breaches and to identify the poorly configured machines. By performing penetration testing, unauthorized access to critical systems and sensitive data can be curbed. More often than not, it becomes easier to identify the critical escalation points and ensures robust security mechanisms.

There is a profound difference between hacking and pen testing. Black hat hacking is deemed illegal. White hat hacking is deemed perfectly legal. However, pen testing is deemed absolutely legal. Penetration testing is associated with a well defined scope and clear intents. In a nutshell, penetration testing replicates and simulates the generalized cyber-attack praxis. To uncover and unfold the network vulnerabilities prior to a malicious hacker, penetration testing is your best bet. The contemporary methodology in pen testing involves testing from an external environment and internal environment. It unearths the potential strategies and countermeasures to effectively handle the vulnerabilities.

Before detailing out the phases in a typical penetration test, it becomes imperative to comprehend and acquaint ourselves with the key terms involved in the lexicon of a standard penetration tester.

1. *Attack Vector:*
   An attack vector is a mechanism or an avenue that assists a hacker or a cracker to gain unauthorized access to a workstation or a computer or a network server to deliver a payload or a malevolent consequence. Attack vectors permit the hackers to capitalize on system vulnerabilities without compromising on the aspect of human element.
2. *Privilege Escalation***:**
   Privilege escalation involves the technical maneuver of capitalizing the limitations of a bug or an error, prototype flaw or structural organization failure in an operating system or in a software application to obtain elevated access to resources that are usually protected from an application or a user.
3. *Remote Vulnerability:*
   Capitalizing on the unauthorized access to privileges and permissions of a workstation on a specific network from another source that is beyond the purview of the workstation being exploited. This is different from Local Vulnerability.
4. *Local Vulnerability:*
   Capitalizing on the unauthorized access to privileges and permissions of a workstation on a specific network from another source that is well within the purview of the workstation being exploited.

A typical Penetration Testing methodology encompasses the following stages:

- Information Solicitation
- Analysis and Planning
- Vulnerability Identification
- Exploitation
- Risk Analysis and Remediation Suggestions
- Documentation and Reporting

*Information Solicitation***:** This is the first stage in penetration testing. The best practice is to develop an information gathering template. The information gathering template should comprise the finer nuances such as the name of the organization, network diagram with details of the major network components such as routers, gateways, firewalls, servers, user machines and their associated communication paths. The template should typically incorporate other details such as the timings in which the testing may be performed and target machines IP address. It is likely that network penetration testing could auger the

network traffic considerably. Many a time, Denial of Service (DoS) attacks could increase network traffic considerably and may bring the network down. It is best to include the restrictions and conditions under which the test should be performed.

*Analysis and Planning***:** In this stage, verification of communication details, especially the details of clients for the sake of clarifications is completed. This stage aids the organization members in comprehending the network topology and communication mechanisms. To ensure a robust penetration testing implementation, identification of critical network components and their corresponding vulnerabilities is imperative. The testing team should take all the necessary initiatives to plan for internal and external network testing. The team has to focus on automation testing phase and exploitation phase. In addition, the team has to emphasize on risk analysis and reporting phases. It is better to have time estimates for each of these phases.

*Vulnerability Identification***:** In this stage, the testing team has to concentrate on privilege escalation and authentication. The key focus areas include OS fingerprinting, Cross-Site Scripting and ARP spoofing. In addition, the team has to lay emphasis on packet sniffing and remote command execution. An exhaustive list of vulnerabilities should be prepared for best results. The team can identify the vulnerabilities by performing automatic scanning of target machines and exhaustive manual penetration testing. For this purpose, effective tools such as BackTrack5, Nmap and SMTPScan may be used. BackTrack5 is an open source Linux based operating system which contains penetration testing toolkit. Open source PERL scripts may be used for Denial of Service (DoS) attacks.

Exploitation: In this stage, the team has to attack the application machines without causing any significant damage to the application resources and network topology. This phase in penetration testing discloses the vulnerabilities in the target machines. To potentially determine the list of vulnerabilities, the best practice is to use exploitation toolkits such as UDP Flood, SYN Flood, and Wireshark, Cisco global exploiter, Metasploit framework, and Smurf6.

Risk Analysis and Remediation Suggestions: In this stage, the team has to provide a well thought out estimate of the likelihood of attack. Further, it has to provide an estimate of the impact of a successful attack. Based on these estimates, it is feasible to estimate the overall risk of the vulnerability.

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

Remediation measures will be suggested for each vulnerability identified. The priority for remediation will be suggested based on the risk rating of the vulnerability.

*Documentation and Reporting***:** The report template should have a brief description of the networks, critical components of the networks, type of communication used, public IPs available etc. In addition, a brief description of the overall security status and the list of major security vulnerabilities identified should be included. Remediation suggestions and the tools used in various phases of the testing require a special mention.

CONCLUSIONS

Penetration testing is an industry recognized term. However, many organizations fail to comprehend the subtleties involved in penetration testing. Apprehensions about penetration testing can be allayed if the pen testers master the nitty-gritty of penetration testing. This comprehensive paper discusses the stages involved in penetration testing. Network security and data security can be accomplished if penetration testing is implemented both in letter and spirit, policy and execution.

ACKNOWLEDGMENT

The authors would like to thank their professors and research scholars for their everlasting support and valuable insights.

REFERENCES

1. IDC, (2009), “Number of Mobile Devices Accessing the Internet Expected to Surpass One Billion by 2013”, Reported on 9 Dec 2009, Available at: http://www.idc.com/getdoc.jsp?containerId=prUS22110509 [Accessed 25 July 2010]
2. Moses A., (2010), “Internet addresses running out”, Sydney Morning Herald, Available at: http://www.stuff.co.nz/dominion-post/national/technology/3958727/Internet-addresses-running-out [Accessed 25 July 2010]
3. ACPO, (2009), “ACPO e-Crime Strategy 2009 Report: A Strategic Approach to National e-Crime”
4. Markkoff, J. (2008). Before the Gunfire, Cyberattacks. New York Times. Available at: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1.2 [Accessed 25 July 2010]
5. Higgins, K. J. (2010). "Anatomy of a Targeted, Persistent Attack", DarkReading, 27 Jan. 2010, Available at: http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=222600139 [Accessed 25 July 2010]
6. Dekker, M. (1997). “Security of the Internet”, CERT Coordination Center Reports, Available at: http://www.cert.org/encyc_article/tocencyc.html [Accessed 25 July 2010]
7. Stoll, C. (1989), “The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.” Doubleday, NY, USA.
8. EC-Council, (2010). Certified Ethical Hacking Training Course. URL: http://www.eccouncil.org/certification/certified_ethical_hacker.aspx [Accessed 25 July 2010]
9. Bentley, L., (2006), “Penetration Testing Key to HIPAA Compliance for Care New England”, IT Business Edge, Available at: http://www.itbusinessedge.com/cm/community/features/interviews/blog/penetration-testingkey-to-hipaa-compliance-for-care-new-england/?cs=22127 [Accessed 25 July 2010]
10. Cabinet Office, (2009), “Cyber Security Strategy of the United Kingdom”, June 2009, Available at: www.cabinetoffice.gov.uk/media/216620/css0906.pdf [Accessed 4 August, 2010]
11. Arkin, B., Stender, S., McGraw, G. (2005). “Software Penetration Testing”, IEEE Security and Privacy, Volume 3, Issue 1.
12. Pierce, J., Jones, A., and Warren, M. (2007). “Penetration Testing Professional Ethics: a conceptual model and taxonomy”, Australasian Journal of Information Systems, 13(2). Available at: http://dl.acs.org.au/index.php/ajis/article/view/52 [Accessed 25 July 2010]
13. McRue, A. (2006). “University opens school for hackers”. URL: http://news.cnet.com/University-opens-schoolfor-hackers/2100-7355_3-6085375.html [Accessed 8 August 2010]