ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Penetration Testing in Wireless Networks

Harshdeep Singh
Department of Computer Engineering
Punjabi University, Patiala
Punjab, India

Dr. Jaswinder Singh
Department of Computer Engineering
Punjabi University, Patiala
Punjab, India

Abstract: Wireless technology has brought many changes in the way of communication in modern days. With the increased world wide employment of wireless technology, there is raising concern about the security standards of the technology. Many encryptions and decryption techniques have been implemented today to transmit data over the networks. Despite that, many authentication methods have also been applied. However, such methods must be validated to ensure the security of wireless networks. [1] Penetration testing is the one which can be used to identify the unknown void in the network. This makes pen test crucial to validate the security mechanisms of the system and outcomes of penetration testing could be used to secure the network. This paper will present an overview of penetration testing and tools. For this purpose, this paper will review the previous work done on the security of wireless networks using penetration testing.

Keywords: Network Penetration Testing, Pen Test, Pen Tester, Wireless Networks.

I. INTRODUCTION

Network Penetration Testing is also known as Pen Test. Penetration testing is an attack on the system to validate the security of the system by checking any potential vulnerabilities in the system. The Pen Test access the computer devices to check for entry flaws. It basically identifies the security flaws in s system, an infrastructure, web applications, or a network. Security flaws might present in an operating system, mal-configuration, application or endpoints. [9]

Penetration testing includes many reconnaissance scans with firewall, switches, servers, routers, workstations, and network devices. It uses different means to achieve the goal. It simply checks whether a particular machine is vulnerable to attack or not if the shielding is sufficient & defenses (if any) the test defeated. The threats & risk pen test discovery must be reported to the admin or owner of the organization for which test is being held. Penetration test reports also provide a list of potential impacts to the organization and suggest acure end the risk.

A. Pen Tester

A pen tester is an associate degree ethical hacker who is employed to aim to compromise the network of an organization with the aim of assessing its information security. A team of ethical hackers operating to interrupt into a network is termedas a tiger team. [12]Restrictions sometimes mandate what a penetration tester will and can't do. For instance, a penetration tester is often not allowed to perform DoS attacks on a target network or lease a computer virus. However, the possibility of testing done by ethical hackers differs counting on the requirements of that organization. [8]

Goals of Pen test may vary depending upon the consented activity for any given involvement with the major goal focusing on finding the risk that someone could utilize and telling the client/owner about these vulnerabilities along with recommended strategies. The Pen tests are part of a full security audit, e.g. the Payment Card Industry requires penetration testing on a regular schedule.

B. Methods of Pen Test:

Considering needs, there are two types of pen tests.

- **External Penetration Test**:

This test shows what a hacker would see into the network systems and use the vulnerabilities seen over the net. Here the threat is from the associated external network from the web. This check is performed over the web, overriding them firewall/IDS.

- **Internal Penetration Test:**

This check shows risks from inside the network. As an example, what threat a disappointed in side worker will cause to the network. This check is performed by connecting to the internal local area network.

C. Types of Penetration testing

- **Black box:**

This test is performed with zero data regarding the network. The tester does not have any prior information about the network or system architecture. The tester is needed to accumulate data victimization penetration testing tools or social engineering techniques. The penetration tester also utilizes the publically offered info over the web. [2]

- **White Box**:

The tester in this technique has complete knowledge of the system or network. Testers are given full info regarding the target network. The data may be the host IP addresses, domains in hand by the corporate, Applications and their versions, Network diagrams, security defenses like firewall within the network. [2] This technique is most accurate as it demonstrates the worst-case scenario when the attacker has full knowledge of the network.

- **Grey Box/Crystal Box:**

The tester has partial knowledge of the target system. The tester fakes an internal employee. The tester has specified an account on the inner network and normal access to the system. This test evaluates internal risks from staff among the corporate. This test could be performed on both internal or external network. [2]

D. Phases of Penetration testing

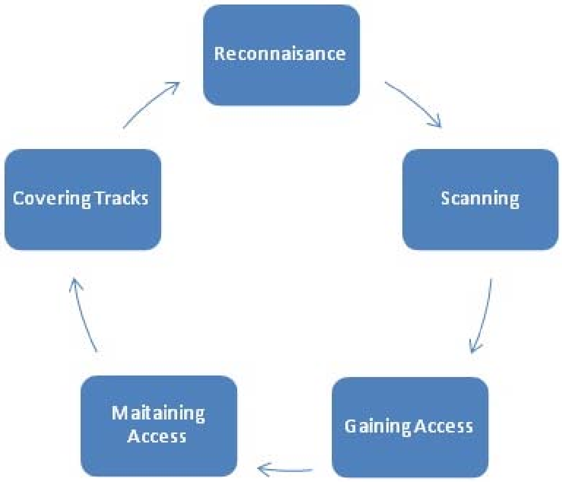

Figure 1: Phases of Penetration testing

1.D.1. Phase 1: Reconnaissance

Gathering preparatory information or knowledge about the target system or network.Reconnaissance could be executed actively or passively. The tester in this phase, acquire as much as could reasonably be expected of the objective system and how it works. It incorporates distinguishing the target, discovering the target system's IP address range, domain name, network, mail server, DNS information, and so forth. [12]

1.D.2. Phase 2: Scanning

Scanning internal and external network devices searching for shortcomings. Requires the utilization of specialized tools to collect more knowledge about the target network, about the systems which they have set up. It integrates scanning the target network for service running, firewall detection, open ports, firewall location, discovering vulnerabilities, OS identification, and so on. [12]

1.D.3. Phase 3: Gaining Access

This phase includes gaining control of at least one network devices to either separate data of significant value or utilize the network as a dispatch site for attacks against different targets. It incorporates social engineering, vulnerabilities exploitation, and so forth. [12]

1.D.4. Phase 4: Maintaining Access

After gaining access to the target system or network, the tester must now develop the steps and take actions required in having the capacity to maintain access sufficiently long so as to collect as much information as could be expected. In this stage, the tester should stay cautious, in order to not get caught when utilizing the host network. It incorporates privileges acceleration, backdoor installation on the target network to maintain the obtained entrance and interface with atarget at whatever time, and so on. [12]

1.D.5. Phase 5: Covering Tracks

Find a way to conceal the interruption and conceivable controls abandoned for future visits. Evaluate a wide range of logs, transferred backdoor(s) and anything identified with the attack.[12].

II. LITERATURE REVIEW

Wang, S., Wang, J., Feng, C., & Pan, Z. (2016), analyzed the vulnerabilities and types of attacks on IEEE 802.11 WLAN. IEEE 802.11 is a wireless network which uses radio to transfer data and hence is most susceptible to the security issues such as WPE/WPA/WPA2 cracking, Denial of Service (DoS), and rouge access points. The attacker could easily bypass the firewalls, access sensitive data, intercept packets and transfer malicious packets. The Penetration testing ensures the security of wireless networks. This research used WAIDPS as an auditing tool to detect the wireless attacks and wireless intrusion to mitigate the risks and protect WLAN. WAIDPS is an open-source wireless Swiss-Knife which works on Linux and is written in Python. This tool is designed to audit networks and detect wireless intrusion. The outcomes of this research found that WAIDPS can effectively detect the attacks to protect WLAN. [1]

Goel, J. N., & Mehtre, B. (2015) used Vulnerability Assessment and Penetration Testing (VAPT) for cyber defense. This research analyzed the performance of VAPT for cyber defense technology to give the proactive cyber defense as to find the vulnerabilities in advance before the attacker could attack the system. The study discussed the prevalent Vulnerability assessment techniques and some VAPT tools. VAPT is a step by step process, and its life cycle includes 9 steps in the process. The results of the study shown that VAPT is an effective technique for Cyber defense technology. The administer can save his resources and sensitive information using VAPT technique and achieve proactive cyber defense. [2]

B L V Vinay Kumar, K Raja Kumar, & V Santhi. (2016) investigated different Penetration testing tools using Kali Linux. This research helped to understand how to perform different penetration tests with virtualized tools, systems, and private networks. The test was performed to detect attacks such as Man-in-the-Middle attack and traffic sniffing. The technique used Ettercap and Driftnet for security auditing and computer network analysis. The implementation also used the Wireshark for traffic sniffing. The results showed that proposed technique for penetration testing could be used successfully in real time environment. [3]

Fiocca, M. (2009)presented an introduction of Penetration testing to address the vulnerability of computer systems. This paper included a literature survey of Penetration testing performed by security experts to find the vulnerabilities of thesystem. The study describes two main types of penetration testing white box and black box testing.

The study also analyzed different tools of penetration testing specifically vulnerability scanners included amore explained review of tools such as Nessus. [4]

Salas, M., & Martins, E. (2014) proposed a technique for security testing which used two techniques, namely Penetration Testing and Fault Injection to detect XSS attacks against Web services. XSS is cross-site scripting attack on Web services that raises new security challenges. This testing technique combined the WSS (WS-Security) and security tokens to identify the sender and ensure the authorized access to SOAP messages communication. Another injection tool that was used is WSInject to introduce faults or error on Web Services for checking the environment behavior. The results of the research shown that WSInject tool is better and improves the detection of vulnerability to compete with XSS attacks as compared to soapUI. [5]

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016) analyzed state of the art in cyber security risk assessment of SCADA (Supervisory Controland Data Acquisition) systems. the research identifies 24 risk assessment methods in the context of SCADA systems. This study reviewed previous work done over risk assessment of SCADA systems. The results of the findings shown that the Cybersecurity risk assessment technique for SCADA system can be improved by Vulnerability assessment using penetration test. [6]

Srivastava, A., Morris, T., Ernster, T., Vellaithurai, C., Pan, S., & Adhikari, U. (2013) Performed the vulnerability assessment of information and communication cyber network. The test was performed to model the attack using thevulnerability of electric grid with incomplete information which was analyzed using graph theory. The research simulated the modified IEEE 14 bus test case system using MATLAB and graph theory was used to analyze the IEEE 118 bus system. The results of thetest performed shown the possible effects on thegrid due to integrated cyber-physical attack. The results demonstrated the effect of Aurora attack on the considered test case. [7]

Reaves, B., & Morris, T. (2012) presented a survey of vulnerabilities and mitigations related to cyber security. The paper focused on the vulnerabilities in multiple industrial radio technologies such as IEEE 802.15.4, IEEE 802.11, WirelessHART, Bluetooth, and ZigBee. The paper discussed how vulnerabilities on industrial radio technologies could be used as vectors for attacks on control systems in complex infrastructures.Vulnerabilities were classified intofour sets; reconnaissance, packet injection, denial of service, and man-in-the-middle vulnerabilitiesThe paper also recommended some methods for securing wireless networks in control systems. The authors suggested that Wireless networks with denial of service, packetinjection, or man-in-the-middle vulnerabilities must not be used in acute control systems [8]

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2016) presented anSTPA (System Theoretic Process Analysis)-SafeSec methodology to analyze the vulnerabilities on Cyber-physical systems. the proposed methodology was used for both safety and security. The results of the research shown the dependencies among cybersecurity vulnerabilities andsystem safety. The paper suggested that by using this information, an effective mitigation strategy could be identified to ensure safetyand security of the system The paper applied STPA-SafeSec to a use casein the power grid domain, and highlight its benefits. [10]

Ten, C., Liu, C., & Manimaran, G. (2008) proposed aframework to evaluate vulnerabilities of SCADA systems at three levels:system, scenarios, and acces points. The proposed techniquewas based on cyber systems combined with thepassword models and firewall, the primary mode of defense in the electricity industry today. The effect of a possible electronic intrusion wasassessed by its potential loss of load in the Grid. This method wassupported by acombination of a logic-based simulation technique and a unit for the power flow calculation. The IEEE 30-bus system was used to assess the effect of attacks from outside or within the substation networks. In the end, countermeasures were given forimprovement of the cybersecurity. [11]

III. QUANTIZATION

The table below includes the overview of tools and techniques used by previous researchers for Penetration testing and their outcomes.

Table 1: Overview of tools and techniques for Penetration testing

Author and Year	Tools/Techniques	Results/Outcomes
Wang, S., Wang, J., Feng, C., & Pan, Z. (2016)	Penetration testing and security Auditing using WAIDPS	WAIDPS can detect the WEP/WPA/WPS attacks to protect WLAN
Goel, J. N., & Mehtre, B. (2015)	Vulnerability Assessment and Penetration Testing (VAPT) for cyber defense	VAPT is an effective technique to save resources, sensitive information and Cyber defense.
B L V Vinay Kumar, K Raja Kumar, & V Santhi. (2016)	Penetration testing tools using Kali Linux, Wireshark, Ettercap, and Driftnet	Successful in detecting Man-in-the-Middle attack and traffic sniffing
Salas, M., & Martins, E. (2014)	Penetration Testing and Fault Injection to detect XSS attacks against Web services	WSInject tool is better and improves the detection of vulnerability to compete with XSS attacks
Srivastava, A., Morris, T., Ernster, T., Vellaithurai, C., Pan, S., & Adhikari, U.	Vulnerability assessment of information and communication cyber network by simulating the modified IEEE 14 bus test case system	Results showed the possible effects on grid due to integrated cyber-physical attack

(2013)	using MATLAB and graph theory was used to analyze the IEEE 118 bus system.	
Reaves, B., & Morris, T. (2012)	Survey of vulnerabilities in multiple industrial radio technologies such as IEEE 802.15.4, IEEE 802.11, WirelessHART, Bluetooth, and ZigBee.	Wireless networks with denial of service, packetinjection, or man-in-the-middle vulnerabilities must not be used in acute control systems
Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2016)	STPA-SafeSec methodology to analyze the vulnerabilities on Cyber-physical systems	STPA-SafeSec can be used for safety and security.
Ten, C., Liu, C., & Manimaran, G. (2008)	Vulnerability assessment of SCADA systems using IEEE 30-bus system	Results showed the effects of attacks from outside and within the network.

IV. CONCLUSION

The wireless network is an essential part of today's' Information Technology. With this vast implementation of technology, security concerns also increased drastically. Despite the many security measures, new techniques of penetration testing are need to be introduced. Network Penetration testing is a method to detect vulnerabilities in network security before hackers could use them to access it. This paper describes the approach used previously for the network penetration test. The aim of this paper was to provide ageneral overview of the penetration techniques employed earlier in previous studies as well identifying the future research directions in penetration testing and wireless network security.

VIII. REFERENCES

[1] Wang, S., Wang, J., Feng, C., & Pan, Z. (2016). Wireless Network Penetration Testing and Security Auditing. ITM Web of Conferences, 7, 03001.

[2] Goel, J. N., & Mehtre, B. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. Procedia Computer Science, 57, 710-715.

[3]B L V Vinay Kumar, K Raja Kumar, & V Santhi. (2016). Penetration Testing using Linux Tools: Attacks and Defense Strategies. International Journal of Engineering Research andTechnology,V5(12), 153-158.

[4] Fiocca, M. (2009). Literature Study of Penetration Testing. Retrieved from https://www.researchgate.net/publication/254054590_Literature_Study_of_Penetration_Testing

[5] Salas, M., & Martins, E. (2014). Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security. Electronic Notes in Theoretical Computer Science, 302, 133-154.

[6] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56, 1-27.

[7] Srivastava, A., Morris, T., Ernster, T., Vellaithurai, C., Pan, S., & Adhikari, U. (2013). Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information.IEEE Transactions on Smart Grid, 4(1), 235-244.

[8] Reaves, B., & Morris, T. (2012). Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems. International Journal of Critical Infrastructure Protection, 5(3-4), 154-174.

[9]He, L., & Bode, N. (n.d.). Network Penetration Testing. EC2ND 2005, 3-12.

[10]Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2016). STPA-SafeSec: Safety and security analysis for cyber-physical systems. Journal of Information Security and Applications.

[11]Ten, C., Liu, C., & Manimaran, G. (2008). Vulnerability Assessment of Cybersecurity for SCADA Systems. IEEE Transactions on Power Systems, 23(4), 1836-1846.

[12]Antunes, N., & Vieira, M. Defending against Web ApplicationVulnerabilities. Retrieved 09 Oct, 2013, fromhttp://www.infoq.com/articles/defending-againstweb-applicationvulnerabilities