Version 1.0

31, August 2020

Penetration Testing Report Plan

Case #423

Presented by: Dakshitha Navodya Perera
+61 984 2349
Presented To: Ryan Nye
Information security and network manager
+61 8473 284

Contents

Introduction

The purpose of this report is to obtain permission or warrant to carry out a vulnerability analysis and penetration test in order to identify, detect the vulnerabilities of the internal and external Target system as the client requested. The penetration testing and active exploitation techniques will be utilized in a manner that a malicious hacker engaged in an attack to penetrate the Target system. However, the ultimate intention of this penetration testing is to gain access to the root privilege. Penetration testing allows organizations to shape their information security strategies over detecting vulnerabilities, proactive elimination of detect vulnerabilities and implementing the correct measures. Furthermore, The Penetration test helps to identify and prioritize risk that could damage the organization's reputation, regulation and compliance as well as completion and rivalry. (McGrew, 2019) However, Penetration testing should not be limited to one or two tests. It could be conducted regularly. Regular testing should be performed in order to:

- Detect the vulnerabilities in the infrastructure, application and people
- Make sure controls have been actualized and are successful
- Determine any software bugs. [6] it is true that hardening a system is very expensive. Nonetheless, during data breach could lose even more.

Moreover, the penetration testing will be conducted on a periodic basis, and it depends on the criticality of the organization system. The trial-and-error method will be the nature of the test with unexpected consequences in the systems being tested. (McGrew, 2019)

Contact Details:

Name	**Email**	**Phone**	**Position**
David Cook	devid@cook.com	+94 221 413 43	System Administrator
Elon Musk	elon@musk.com	+94 325 234 32	Chief Information Officer

Proposed Analytical Process

1. **What Analyse & Process:**

This penetration testing some methods will be used to analyse the given case.

- During this test, Information gathering will be conducted as the initial step. In order to gather information about the system there are few methods will be used.
    - Search engine queries – Google Dork
    - Domain name searches – WHOIS looks up
    - Social Engineering
    - Internet Footprinting – email adds, username, social network, ping sweeps, port scanning, reverse DNS, packet sniffing. (Hussain, Hasan, Chughtai, 2017)
- After enough gathering information about target will move to the treat modelling. During treat modelling will develop an attack based on information gathered. If an attacker could gain into internal development systems and could sell organization data for competitors.
- Next step would be vulnerability analysis. Hence, this step will be discovered vulnerabilities to figure out how successful exploit strategies might be. However, during this step failed exploits can crash the system and services. Thus, it could be valuable to set off Intrusion-detection system anyway. This phase some vulnerability scanners will be performed to detect vulnerabilities in the system. Furthermore, manual analysis will be and verify the results found during automatic analysis.
- Then next step would be exploitation. During this step exploitation will be used against the vulnerabilities. Tools like Metasploit Framework will be used in order to gain access to the target system.
- Also, during post exploitation will be gathered information about the target system and looking for interesting items such as dump passwords hashes, files in order to escalate the privileges up to the root. Tools like Niko, SQLmap, fsociety could be helpful in this phase.

- Then as final step reporting will be conducted. For reporting and editing Microsoft Word will be utilized, and Microsoft PowerPoint will be used for presentation if needs. Moreover, the tool that will be using during each step have been mentioned in the required resource section. (McGrew, 2019)

This test will demonstrate risk, a combination of threat, vulnerabilities and impact to the consumer and it will provide recommendations in order to mitigate them. Furthermore, all the results will be clearly mentioned in the report with found flags details. During reporting, the Common Vulnerability Scoring System (CVCS) will be utilized in order to illustrate rating based on the characteristics and severity of each identified vulnerabilities. (Weidman, 2014) However, if there is a data leakage found during the penetration test, the test will be suddenly terminated and will be informed authorized personal. (A Complete guide to the phases of penetration testing, 2020).

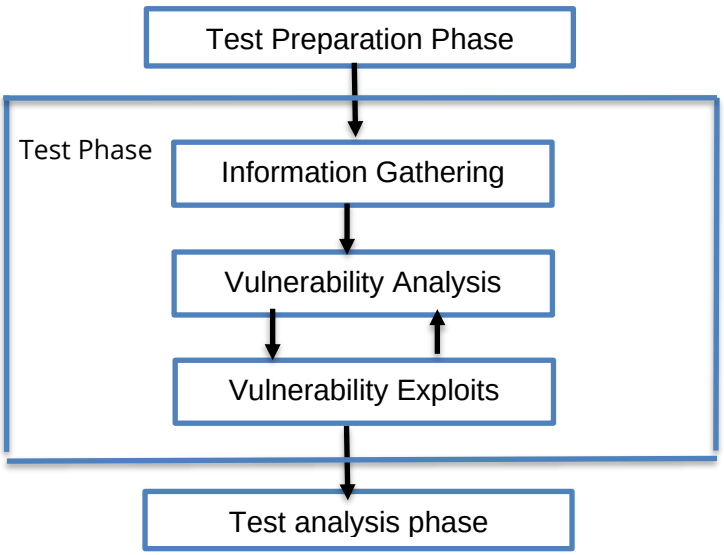
Furthermore, each testing that is going to be conveyed contains an expected level of effort. For instance, tasks with a dataset that involves cryptographic keys would be served under the medium level of effort. Each level of efforts consists of indigenous timeframe:

Low level of Efforts	1 to 5 hours
Medium Level of Efforts	6 to 15 hours
High Level of Efforts	16 to 40 hours
Extremely High Level of Effort	41+ hours

Therefore, High or Extremely high level of efforts may or may not be able to complete with the support of a team.

2. Phases:

Furthermore, this penetration test follows the National Institute for Standards and Technology (NIST) recommended loop back and forth between a discovery phase and an attack phase. Nonetheless, the pre-engagement phase is already conveyed with the client. However, information-gathering, threat-modelling, vulnerability analysis, post-exploitation and reporting phases are ahead to be implemented. Furthermore, During the Attack phase following process and phases will be adopted. (Hussain, Hasan, Chughtai, 2017)



3. Scope:

During the pre-engagement phase, there is a brief description of scope has been provided by the client. The customer expects to conduct the testing on one system which is connected to the main

organization network. Moreover, the client has decided not to provide the physical access to the organizations' system. Hence, Physical and Wireless penetration testing will not be available in this case. Thus, this test will only occur over the network. (A Complete guide to the phases of penetration testing, 2020).

The client agrees to use social engineering. Thus, this penetration test will not be restricted to the scope, and it could go beyond that, and it will include:

- Scan all the IP addresses in the network this may or may not include the cloud services and ISPs.
- Internet-Based Open-Source Intelligence which is also known as OSINT information gathering.
- Social Engineering and interaction with employees in the target organization
- Web Application and Mobile Application testing may or may not be a part of this penetration testing.
- During the final phase, the report will implement the recommendations in order to harden the system. (Weidman, 2014)

4. Provided Information

In this scenario, there is no information has been provided about the organization or any sensitive data about the target system. However, the client has contributed limited information about the system that required to be penetrated. For instance, there is a supplied system which is a virtual machine that has been provided in order to conduct the test. Therefore, it is fair to assume this penetration test as a Grey Box Test.

Furthermore, the client has informed about five flags that have been situated inside the system in order to validate the infiltration of the system. (McDermott, 2001)

Ethical Considerations:

The test conceivably uncovers sensitive data about the company, the system, and /or its users. Therefore, handling sensitive data requires special attention in RoE and proper storage and communication measurements will be taken.

- Therefore, computers and storage that utilized for the penetration testing will be fully encrypted.
- Furthermore, the regular meeting will be scheduled between penetration testing and the client in order to mitigate miscommunication as well as to share workflow and vulnerabilities found so far. (McDermott, 2001)

The client has requested to sign a non-disclosure agreement (NDA) beforehand which guarantee the privacy organization's sensitive information. [9] According to this non-disclosure agreement,

- there will not be any copies of the client's data
- There will never perform unauthorized testing during the testing.
- Moreover, the findings will not be revealed to unauthorized personals
- Perceived vulnerabilities will not be published to public without the client's permission.

Basically, even the mere sensitive information will only be remaining among ones who need to know. (Hussain, Hasan, Chughtai, 2017)

As aforementioned, the customer agreed to conduct social engineering testing along with this test. However, Denial-of-Service attacks will only be available during off-peak hours which is 11.30 pm to 7.30 am as the client requested. Moreover, the penetration testing team will be in touch with the client in order to inform unannounced or announced tests. (Weidman, 2014) If it is announced test, the team will make sure to inform the client of time and date. Finally, when the penetration testing is finished all the data about the client will be removed from all the devices that used to conduct the test. ("Penetration Testing and Network Defense", 2020)

Required Resources:

This penetration testing requires:

- The supplied system (virtual machine) will require in order to carry the penetration testing

- Computer with Approx. 60GB of storage of HDD & Minimum of 16GB RAM
- Need to use VMware Workstation 15 Pro – To run guest Operating systems (kali Linux) on the host OS.
- Need 8GB Pen drive and 5 DVDs(writable, 2GB) & 512GB External Hard Drive – As additional storages.
- Kali Linux Operating System – Kali Linux OS is one of the best Operating Systems to conduct Pen tests most tools will be pre-build or pre-installed in the Kali Linux. And it will be using as the guest Operating System in the computer.
    - Version 2020.3
- Parrot Operating System & BlackBox Operating System – Use as redundant Operating system along with Kali Linux
- Windows Operating System – Windows OS will be used in order to run software's and Hardware's that is not supported to Kali Linux.
    - Version 10 HOME. (Weidman, 2014)

Moreover, During the test quite a few software may require:

Information Gathering & Threat Modelling Tools:

Name of Tool	Specific Purpose	Cost	Version & Vendor
WireShark	To use as a packet analyzer	Free	Version -3.2.6 , Vendor - The Wireshark Team
SuperScan	Malware and URL scanner	Free	Version -3 or later Vendor - Chronicle Security
P0f	Web server & OS fingerprinting and firewall detection	Free trial versions	Version – 3.09 Vendor – Michel Zalewski

Furthermore, in order to gather furthermore details about the client search engines such as Google dork, Duckduckgo will be used along with social media such as Facebook. (Bacudio, Yuan, Chu, Jones, 2011)

Name of Tool	Specific Purpose	Cost	Version & Vendor
Nmap	Network scanning Port scanning OS detection	Free	Version - 7.80 Vendor - Insecure.org
OpenVas	To conduct a vulnerability scan		Version - 8.11.1 Vendor - tenable
SuperScan	To detect TCP & UDP ports and running services of them and run whois, ping hostname lookup	Free	Version – 4.0 Vendor – SuperScan

Vulnerability Analysis Tools:

Name of Tool	Specific Purpose	Cost	Version & Vendor
Nessus	Detect Vulnerabilities that allow remote attacks Detect misconfiguration, default password and DOS	Free	Version - 8.11.1 Vendor - tenable
Iss Scanner	To identify network vulnerabilities.	Free Trial Version	Version – 7.2 Vendor – ACUNTIX

Exploitation Tools:

Name of Tool	Specific Purpose	Cost	Version & Vendor

Netspacker	To identify vulnerabilities in web applications and web APIs	Paid	Version - August 2020 Update Vendor - Netspacker
Nikto	To identify vulnerabilities in webserver. And Identify web server type, version and other interesting files.	Free	Version - 2.0 Vendor - cirt.net
John the Ripper	To crack passwords	Free	Version - 1.9.0 Vendor - OpenWall
Cain and Abel	Windows password recovery tool, can be useful to perform brute force and crypto-analytic attacks on the encrypted passwords	Free	Version - 4.9.56 Vendor - Massimiliano Montoro
Brutus	ftp, ssh, and http password cracker.	Free	Version – AET2 Vendor - ehacking
Metasploit Framework	To develop and execute exploit code against a remote server.	Free	Version - 5.0.0 Vendor - Rapid7
SQLmap	To attack target system with SQL injections.	Free	Version - 2 (or Late) Vendor – Free software foundation.
BurpSuite	To utilize as a scanner with some intruder tool	Paid or Free	Version - 2.1.0 Vendor - PortSwigger

- Trojans, APTs and C2s – To gain access to the system remotely. (Bacudio, Yuan, Chu, Jones, 2011)

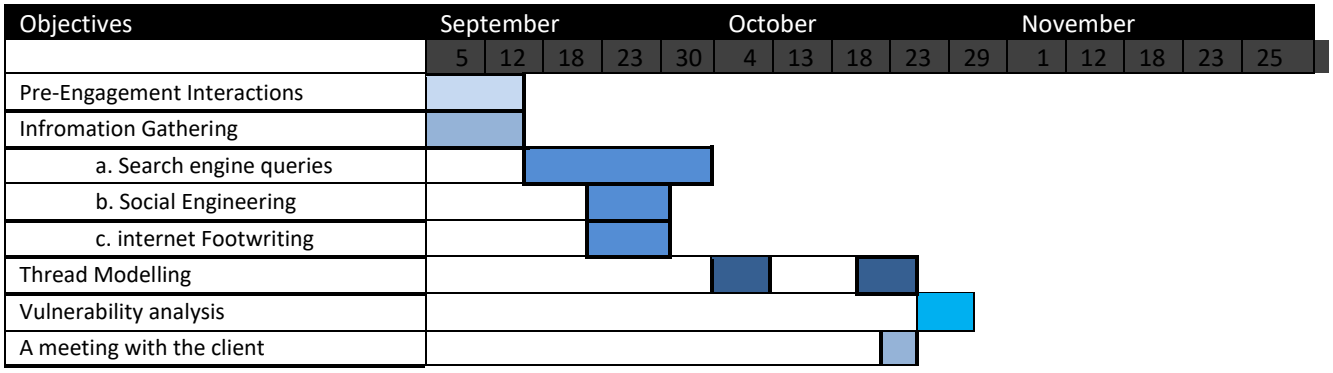
Reporting Tool:

Name of Tool	Specific Purpose	Cost	Version & Vendor
Microsoft Word	To write and edit the report	Paid	Version – 16.1 Vendor - Microsoft

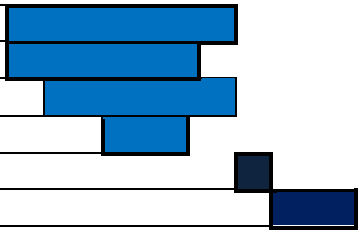
Moreover, "*Penetration Testing A Hands-on Instruction to Hacking, Second Edition by Georgia Weidman*" the book will be exceptionally valuable to conduct this penetration test effectively.

Timeline:

The final analysis and report relating to this case are expected no later than November 25th, 2020. Furthermore, On 13th and 14th October the penetration testing team will not available due to the Poya days. On 4th of October a meeting has been scheduled with the client in order to discuss findings and penetration results so far. This penetration testing may or may not require the time-consuming process such as decryption. In this manner, these days are not permanent, and it could be varied based on the tasks. Nonetheless, the best-case scenario, the final report could be able to submit on 25th November 2020.



Exploitation	
a. Network Attacks	
b. Web Application	
c. Social Engineering	
Post-Exploitation	
Reporting & presenting	



My Resume

DAKSHITHA PERERA

pdakshi@our.ecu.edu.au
123 Main.st, Colombo, Sri Lanka
+94 213 123 12
dakshithanavodya.com

SECURITY PENETRATION TESTER
06/2019 – Present

- Perform web application, mobile application and network penetration tests
- Develop processes and implement tools and techniques to perform ongoing security assessments of the environment
- Analyze security test results, draw conclusions from results and develop targeted testing as deemed necessary
- Providing technical consultation on Security Tools and Technical Controls
- + Development of 'rules of engagement' with partners
- Develop security standards, policies, automation scripts
- Perform security reviews of application designs and source code review

Colombo

EDUCATION

EDITH COWAN UNIVERSITY

- **Bachelor's Degree in Computer Science (Cyber Security)**

SKILLS

- Strong attention to detail in conducting analysis combined with an ability to accurately record full documentation in support of their work
- Ability to continually refine the vulnerability offerings and deliverables
- Strong technical ability in security related architecture design and assessment (manual approach to penetration testing)
- Ability to communicate detailed technical information to a non-technical audience
- Demonstrated ability to work on multiple projects simultaneously and to work in a highly dynamic, rapidly changing environment
- Strong knowledge of information security frameworks and standards
- Strong technical ability in current application and infrastructure testing methodologies
- Personal development. All our professionals receive comprehensive training covering business acumen, technical and professional skills development
- Demonstrated proficiency in basic computer applications, such as Microsoft Office software products
- Strong organizational skills and ability to multi-task

Reference:

1. Penetration Testing and Network Defense. (2020). Retrieved 30 August 2020, from https://learning.oreilly.com/library/view/penetration-testing-and/1587052083/ch02.html
2. A Complete guide to the phases of penetration testing (2020). Retrieved 30 August 2020, from https://cipher.com/blog/a-complete-guide-to-the-phases-of-penetration-testing/
3. McDermott, J. P. (2001, February). Attack net penetration testing. In *Proceedings of the 2000 workshop on New security paradigms* (pp. 15-21).
4. Bacudio, A. G., Yuan, X., Chu, B. T. B., & Jones, M. (2011). An overview of penetration testing. *International Journal of Network Security & Its Applications*, *3*(6), 19. (Bacudio, Yuan, Chu, Jones, 2011)
5. Hussain, M. Z., Hasan, M. Z., & Chughtai, M. T. A. (2017). Penetration testing in system administration. *International Journal of Scientific & Technology Research*, *6*(6), 275-278. (Hussain, Hasan, Chughtai, 2017)
6. Why is penetration testing necessary?. (2020). Retrieved 30 August 2020, from https://www.itgovernance.co.uk/media/press-releases/why-is-penetration-testing-necessary#:~:text=Penetration%20testing%20looks%20at%20vulnerabilities%20and%20will%20try%20and%20exploit%20them.&text=Organisations%20need%20to%20conduct%20regular,in%20order%20to%20develop%20controls
7. Wesley McGrew, 2019, Protecting Penetration tests: recommendations for improving engagement security. https://www.blackhat.com/docs/us-17/wednesday/us-17-McGrew-Protecting-Pentests-Recommendations-For-Performing-More-Secure-Tests-wp.pdf (McGrew, 2019)
8. Weidman, G., & Eeckhoutte, P. V. (2014). Penetration testing : a hands-on introd uction to hackin. No Starch Press. INSERT-MISSING-URL. (Weidman, 2014)
9. Engebretson, P. (2013). The basics of hacking and penetration testing : ethical ha cking and penetration testing made easy (2nd ed.). Syngress, an imprint of Elsevi er. INSERT-MISSING-URL. (Engebrestson, 2013)