CSL3208 Ethical Hacking and Defence

Assignment 1 - Analysis Plan for an Ethical Hacking Activity

Glen TEAKLE 10532981

JO Campus (Online)

**INTRODUCTION**

A virtual machine has been supplied for the purpose of a penetration test. Using various applications, pen-testing tools and software, and by following the known phases of a pen-test, there are 3 main objectives which are as follows:

**OBJECTIVES**

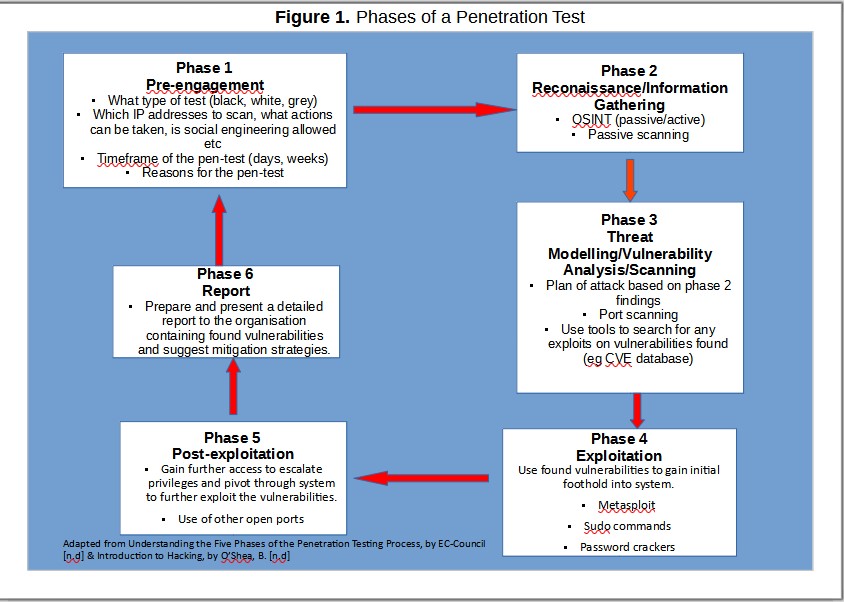
* Gain initial access to the target VM using various pen-testing tools, methods and software.
* Achieve admin/root level privileges of the machine.
* Uncover the 5 hidden flags that are located throughout the VM at specific points in the compromise. They may take on values such as: *“chahNaelia9zohlaseiPaich0QuoWoh8ohfaenaiQuaetaebushoakarai6lainohjongoneesoocahdei6guosiethae7uwuu5Kaid9ei sah8EChoo4kaiGh2eit2mu”*

This plan will cover each stage of the proposed pen-test including:

* Analytical process (scope of the test, pen-test phases, type of test).
* Resources required
* Ethical considerations
* Time frame

**PROPOSED ANALYTICAL PROCESS**

6 phases of pen-testing will be undertaken as shown below in Figure 1.



**PRE-ENGAGEMENT**

**In Scope**

As there is essentially no information supplied about the virtual machine (other than the hidden flags) this pen test falls under the category of a “black box test”. This means the test will be unbiased and conducted having no prior knowledge of the VM contents, system, network config or any usernames/passwords (O’Shea, n.d & Weidman & Eeckhoutte, 2014). There are no restrictions on the scanning of specific IP addresses, ports or devices.

**Out Of Scope**

The following items are considered irrelevant for this particular pen-testing scenario but would normally be considered in the plan.

* Social engineering tactics.
* A distinct range of IP addresses to scan.
* Start and end times allocated for conducting the test.
* Use of certain exploits to disable a particular service, system or device (O’Shea, n.d).

**RECONAISSANCE/INFO GATHERING**

This phase will begin with Open-Source Intelligence gathering (OSINT) also known as passive scanning. This will involve collecting as much information as possible about the target machine, while not directly interacting with it (O’Shea, n.d). Websites that may be used include: <https://who.is>, <https://shodan.io>, <https://bgp.he.net/> and https://searchdns.netcraft.com.

**THREAT MODELLING/VULNERABILITY ANALYSIS**

A plan of attack will then be created based on the findings in the previous phase.

* Using Kali Linux and Nmap to scan for all available IP addresses in the subnet, including the target VM machine.
* Active scanning to find any open ports and running services on the found IP addresses using a tool such as Nmap.
* Running a service version detection scan to discover the software versions in use on the relevant services/open ports on the target machine.
* Searching an online database such as Common Vulnerabilities and Exposures (https://cve.mitre.org/) for the discovered service versions, to find related exploits that can then be used to infiltrate the target VM.

**EXPLOIT VULNERABILITIES**

This phase will make use of the identified vulnerabilities in the previous step by exploiting them to gain initial access of the system. This process is known as gaining a foothold (O’Shea, n.d). From here, further attempts will be made to attempt privilege escalation to gain further access (admin and root) and pivot through the system.

**REPORT**

The final phase in the pen-test is writing and submitting a detailed report to the relevant stakeholders. It will list in detail all vulnerabilities found and exploited, flags found and recommendations to enhance security of the system.

**ETHICAL CONSIDERATIONS**

This pen-test will be conducted in a completely ethical manner, and any vulnerabilities exploited are purely for the purpose of the test. A nondisclosure agreement (NDA) will be signed by myself to ensure:

* No data will be modified, deleted or shared with any other party.
* No disclosure of any private and/or confidential information or data will occur during the pen-test, or after its completion (SHRM, 2023).

In accordance with the Australian Computer Society’s code of professional conduct, the pen-test will be undertaken with honesty, competence and professionalism while considering the interests of the public (Low, 2014).

**RESOURCES, HARDWARE AND SOFTWARE REQUIRED**

The pen-test may involve the use of any or all of the following:

* Host computer - Dell Desktop PC running Windows 10 Pro Version 21H2
* Kali Linux 2020.2 Config version 9.0
* Azure VM service running Metasploitable Config version 9.0
* Nmap Version 7.80
* Google Hacking Database - <https://www.exploit-db.com/google-hacking-database> - to search for vulnerable files, servers or usernames on the VM (Bock, 2021).
* Whois - <https://who.is> – to search for domain owner.
* SSL scan – to query SSL services on the network
* Shodan – <https://shodan.io> – to search for any known vulnerabilities on devices found on the target VM.
* CVE - <https://cve.mitre.org/index.html> - to search for information related to any vulnerabilities found on the VM.
* John the Ripper – password cracker tool

**TIME FRAME**

The pen-test will be undertaken over a period of 8 weeks, from 13/3 – 4/5 2023 inclusive.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Mon 13/03-Fri 17/3** | **Mon 20/3 – Fri 24/3** | **Mon 27/3-Fri 31/3** | **Mon 3/4-Fri 7/4** | **Mon 10/4-Fri 14/4** | **Mon 17/4-Fri 21/4** | **Mon 24/4-Fri 28/4** | **Mon 1/5-Thurs 4/5** |
| Phase 1 Pre- engagement | Phase 2  Reconnaissance | Phase 3  Threat Modelling | Phase 4  Exploitation | Phase 5  Exploitation/Post exploitation | Final checks | Assembling of report | 4/5-Report due for submission |
| 16/3-Analysis plan submission – approval for pen-test needed to continue |  |  |  |  |  |  |  |

**REFERENCES**

Bock, L. (2021, February 25). *Ethical hacking: footprinting and reconnaissance*. LinkedIn Learning. <https://www.linkedin.com/learning/ethical-hacking-footprinting-and-reconnaissance/search-engines-and-google-hacking-8337046?autoplay=true&resume=false&u=2072140>

EC-Council. (n.d). *Understanding the five phases of the penetration testing process*. EC-Council Cybersecurity Exchange. <https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/>

Low, G. (2014). ACS Code of professional conduct. Professional Standards Board. <https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Professional-Conduct_v2.1.pdf>

O’Shea, B. (n.d), CSL3208 *Introduction to hacking: Module 2* [Lecture notes]. Canvas. <https://courses.ecu.edu.au/>

O’Shea, B. (n.d), CSL3208 *Passive reconnaissance (OSINT): Module 3* [Lecture notes]. Canvas. https://courses.ecu.edu.au/

SHRM. (n.d). *Nondisclosure agreement (NDA)*. HR Glossary. <https://www.shrm.org/resourcesandtools/tools-and-samples/hr-glossary/pages/nondisclosure-agreement-nda.aspx>

Weidman, G., & Eeckhoutte, P. V. (2014). *Penetration testing : a hands-on introduction to hacking*. No Starch Press. Retrieved March 14, 2023, from https://ecu.on.worldcat.org/oclc/891400227.