University of Hertfordshire

School of Computer Science

BSc Computer Science / IT

Module: Computer Systems Security

Assignment two

Standard Operating Procedure and Attack Tree for Pen Testing

Awais Hussain

Level 6

2020 - 21

Table of Contents

**1.0 Introduction3**

**2.0 Pen testing methodologies3**

2.1 OWASP (open web application security project)3

2.2 PTES (penetration testing methodologies and standard)4

2.3 OSSTMM (open-source security testing methodology manual)5

**3.0 SOP (standard operating procedure)6**

**4.0 Decision tree analysis for penetration testing7**

**5.0 Conclusion**8

**6.0 References8**

**7.0 Appendices11**

7.1 appendix SOP for pen testing11

7.2 attack tree (or decision tree) for testing a Linux server12

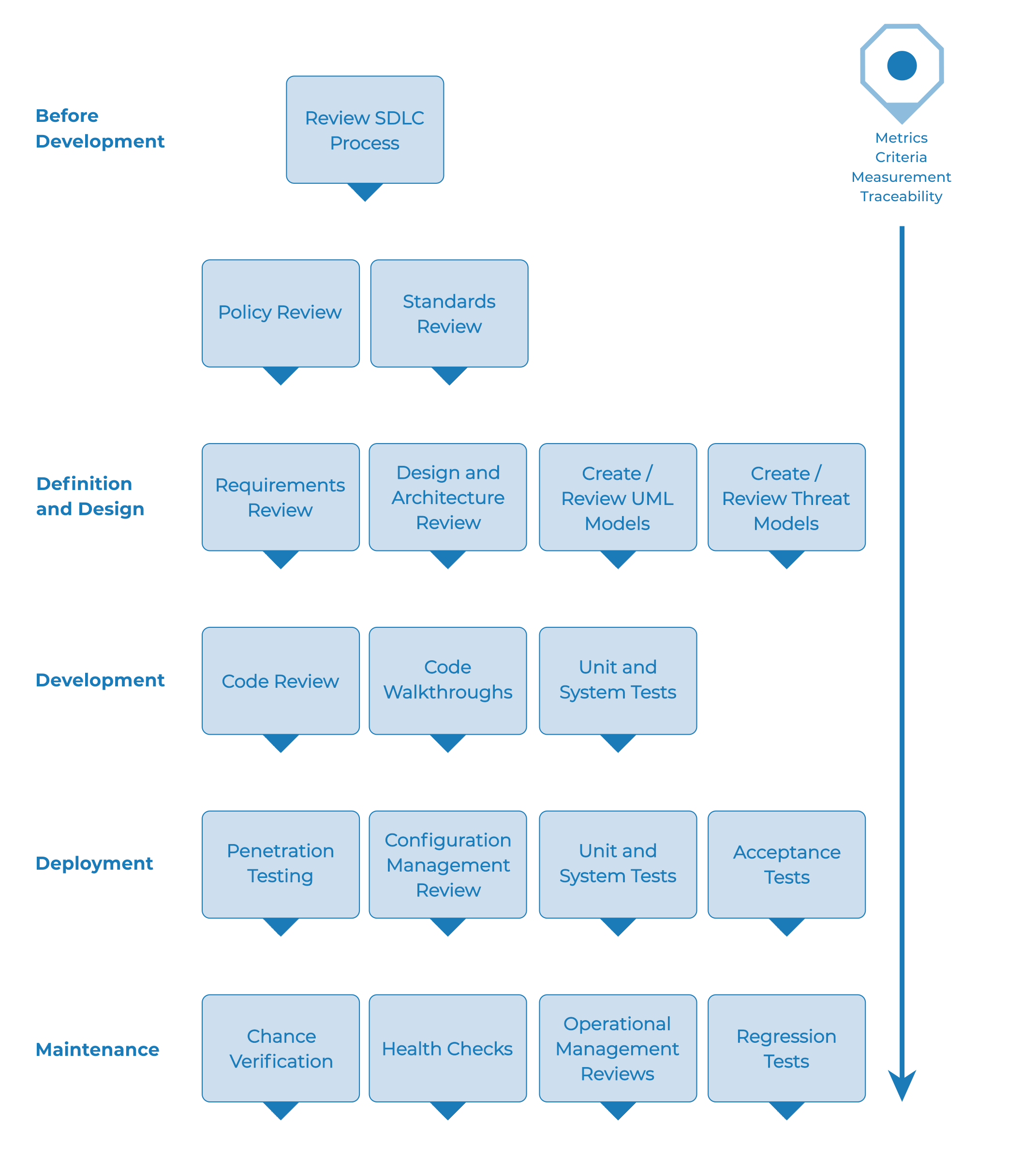
**1.0 Introduction**

The ENISA also known as the European Union of Agency for Cybersecurity had a report that consisted of the information that “742 reports about cybersecurity incidents with significant impact” since 2019 there was a 47% increase in the year of 2020. (ENISA, 2021). The point this reference is proving is that companies will task teams which can also be called pen testers to test the application before release. The reason as to why the application is tested is because ethe application can consist of sensitive and confidential information. If the information was leaked the reputation of the company along with the customers will plummet. That is where the pen testing comes in and aims to find vulnerabilities in the system before hackers do. To identify vulnerabilities within a company’s systems the most common approach taken is to preform penetration testing. The reason as to why penetration testing is done is to identify potential vulnerabilities that a malicious user could exploit (Malik, 2021). The three types of penetration testing consist of Black-box testing (external testing with no knowledge about the system/network), White-box testing (internal testing with complete access and in-depth knowledge of the system) and finally, Grey-box testing (external attack with limited knowledge on the system).

With this scenario in hand, Grey-box testing will be implemented. The reason for this is that we know the IP address and the fact that it will be conducted on a Linux server. This report will entail the analysis and explanations of the methodologies stated above. Also, the concept and establishment of SOP and for our penetration testing and finally an attack tree will be developed.

**2.0 Pen testing methodologies**

Based on the fact we are doing Grey-box testing we will now go into which methodology is best fitting for this penetration test. The most common methodologies used are OSSTMM, OWASP, NIST, PTES, and ISSAF (Vumetric, 2021). For any kind of study of data resources that is given, for instance, OSSTM and ISSAF provide recommendations and procedures for testing and security. On the other hand, OWASP focuses exclusively on the assessment of application security, while PTES offers advice on all types of penetration testing activities (Lee Allen, Shakeel Ali, Tedi Heriyanto, 2014). In this report we will be talking about three types of methodologies. These three types will be OWASP, PTES and OSSTMM.

 **2.1 OWASP (Open Web Application Security Project)**

**Fig.1 (OWASP)**

OWASP has two parts in which the methodology splits in to. The first being passive mode and the second being active mode. Also, this methodology is used for black box testing (Dewhurst Security Blog, 2010). In web and mobile applications this methodology is used to address vulnerabilities so faults or weak points can be easily and quickly discovered. This methodology has a total of sixty-six controls to access (Vumetric, 2020). The three advantages of this methodology are:

1. Teamwork is promoted with this methodology
2. Various situations can be applied to this methodology
3. Most suitable for testing services and web applications (Dalalana Bertoglio and Zorzo, 2017)

For the test that we will be performing however this methodology is not beneficial to us. There are two main reasons as to why this methodology is not fitting. The first being that this methodology is very time consuming (time that we don’t have in this test) that can be seen in the length of the figure 1. The second being that this methodology takes lots of human thought process accompanied with the skill needed for this methodology to be useful.

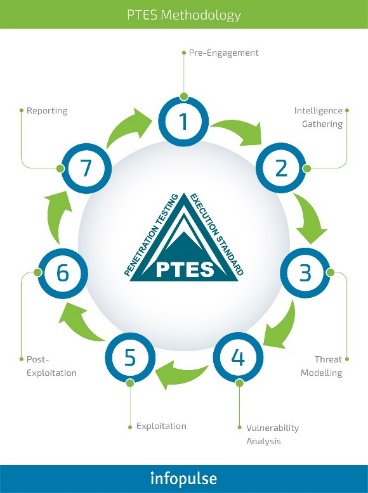
 **2.2 PTES (penetration testing methodologies and standard)**

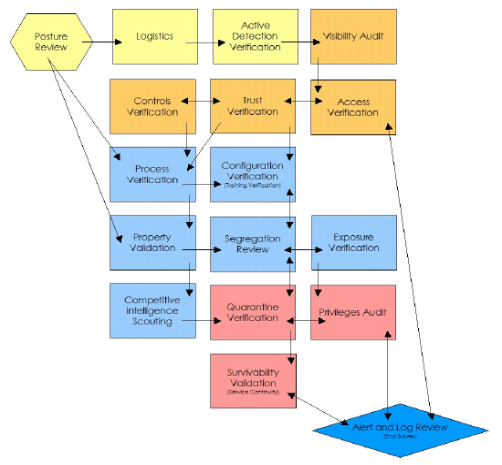
Fig.2 (Infopluse, 2018)

The steps that are within the structure of PTES consist of threat modelling, vulnerability analysis, exploitation, post-exploitation, gathering information, engagement, pre-engagement, and reporting (Lee Allen, Shakeel Ali, Tedi Heriyanto,2014). A team of experts in various industries built and still develop this methodology. A basic standard for penetration test requirements is established by PTES. Extending from the initial communication between client and tester to what a report includes (Harvey, 2019). Also, PTES is the most recommended approach (Harvey, 2019). The key features and benefits of PTES are:

* + 1. If the occurrence of a hacker/attacker does manage to find a vulnerability it will help to reduce material damage
    2. Potential clients might use PTES as a baseline to evaluate the quality of tests performed for them by qualified penetration testers (Dinis and Serrão, 2014)
    3. Own testing needs can be easily adapted and easy to understand

The disadvantage however of PTES is that the mapping between these processes and the practical applicability on the field is failed. (Dinis and Serrão, 2014). However, this methodology is good because for this test as it is easy to understand and as I am still new to pen testing it will be easier to understand.

**2.3 OSSTMM (open source security testing methodology manual)**

 **Fig.3 (Figeczky, 2021)**

With the OSSTMM, its primary goal is to offer a methodical scientific procedure for the precise characterization of operational security that may be applied to penetration testing, ethical hacking, and other security testing (Harvey, 2019). The purpose of this methodology is a peer-review for security testing. The maintaining of this methodology is done by the institute for security and open methodologies (ISECOM).

Because OSSTMM has a framework that consists of an extensive guide, for testers within the network (also components) to identify the security vulnerabilities in various attacks from any potential angle. The in-depth knowledge and experience from a tester are relied upon when a vulnerability is identified, human intelligence is needed to comprehend the impact that could happen within the network (Vumetric, 2020). Three advantages of OSSTMM consist of:

1. Regular updates and focus on interpretating the vulnerabilities.
2. A security guide that assists the team in conducting network development.
3. Consistent and repeatable tests are ensured.

The disadvantage that is in OSSTMM is that for completing modules there is no tools provided. Thus, other methodologies are more extensive (Shanley and Johnstone, 2015). This disadvantage and also because of the complexity of this methodology is the reason as to why this methodology is not suitable for this test.

Based on the information learned about the three methodologies explained above. The PTES methodology is felt to be the best methodology for the Grey-box testing. The simple reasoning as stated before is that it is simpler for a beginner because it provides a basic standard for the determent of quality. Also, the inclusion of well-structured stages of testing and pre-engagement phase and a reporting phase at the end.

**3.0 SOP (standard operating procedure)**

A description of a step by step procedure that that is a written instruction and commands that must be performed routine activity by an organisation (Brush Kate, 2021). This section will delve into the creation of a SOP for the PTES methodology. The SOP for the PTES methodology is described in the following way: (The full SOP for the test will be spoken about in Appendix A)

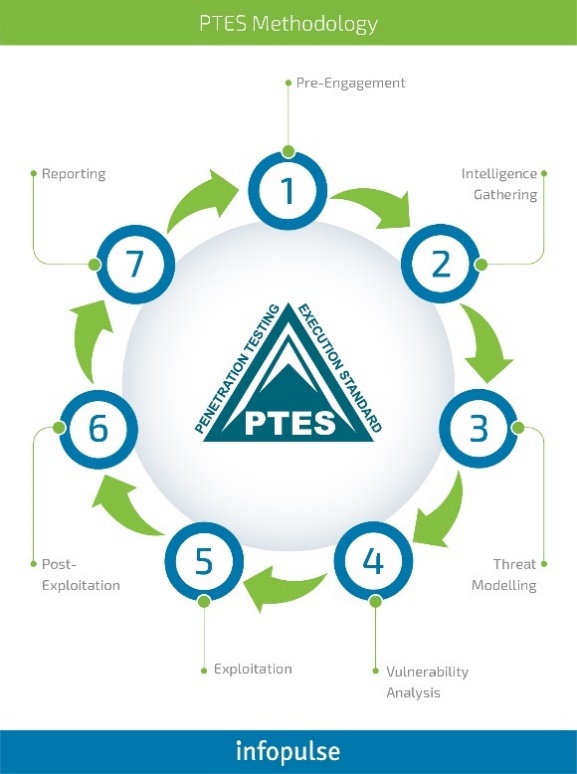


Fig.2 (Infopluse, 2018)

Phase 1 (Pre-engagement):

The main three points for the pen tester in this phase are to determine the type of test, the time needed for the allocation of the next phase of the test and finally the range of IP addresses that need to be evaluated. The completion of the requirements from this phase will allow the pen tester to move on to the next phase.

Phase 2 (Intelligence gathering):

The reconnaissance against a target (such as a typical corporate or related) and a high procedure of plan for attacking the target could help being produced if used properly. This phase is the most important phase of the penetration test (Penetration Testing – IT Security Concepts, 2020).

Phase 3 (Threat modelling):

To prevent the effect of the threat on the system the optimisation of the network security is done by the identification of vulnerabilities and then defining the assistance. This is all done is phase 3.

Phase 4 (Vulnerability analysis):

The importance of this phase is to validate any discovered vulnerabilities. This is done because it can then prevent the attackers from taking advantage of these flaws within the system.

Phase 5 (Exploitation):

The vulnerabilities from the last phase are carried over. This is so the pen tester can reach the security of the target system for this phase.

Phase 6 (Post-exploitation):

To verify the significance of the system the pen tester has full control over the target system and can collect all required data (Dinis and Serrão, 2014).

Phase 7 (Reporting):

The purpose of this phase is for the organisation to take the necessary precautions based on the document formed from the pen tester which consists of all the security vulnerabilities found in the previous phase.

The SOP that will be in the appendix section will follow the same phases. The five things that a SOP helps with is: minimalist of miscommunication, production of consistency, addressing safety concerns, compliance of government regulations is only approved, the mitigating of vulnerabilities found in the testing.

**4.0 Decision tree analysis for penetration testing**

Hierarchical attack trees are, graphical representations of low level hostile interactions that integrate each other's objectives, most frequently with detrimental effects for the attack target. (Amenaza, 2021). In a diagram the attack is formed as a tree and the nodes in the tree represent the attack. There are three types of nodes in a tree the main/root being the global goal which is at the top of the tree. The sub nodes that come off the global goal are called the child node and finally leaf nodes are the nodes that are without a child node (Mauw and Oostdijk, 2006). The appendix will hold the decision tree of a penetration test.

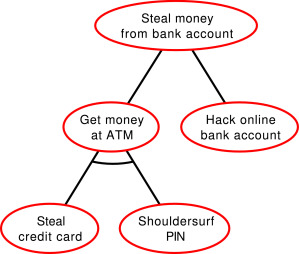


Fig.4 (Buldas et al, 2019)

In the example of the attack tree above, the main objective of the attack is to “Steal money from bank account” this will be the root/main goal. This goal is adversity strained into two sub attacks one being a child node and the other being a leaf node. The sub attacks being with “get the money at ATM” which is a child mode, or the other sub goal of “hack online bank account” which is a leaf mode. The sub goal of “get money at ATM” is further defined to “steal credit card” and “shoulder surf PIN” both nodes must be done together hence the arch connecting the two nodes.

Threat Modelling For Node.js Applications | Snyk

Fig.5 (Nemeth, 2016)

The second example of attack tree above has a main objective of “bypass authentication” which is the root/main goal in this case. This splits into three sub nodes (all child nodes) consisting of “stole cookie,” “learn user / passwd” and finally “modify credentials.” “Stole cookie” is further strained to “insecure dependency” and “modify credentials” is further strained into “get access to DB” these both are the leaf nodes as there is nothing branching off these nodes. Unlike the “stole cookie” and “modify credentials,” “learn user / passwd” is strained into a sub node of “get from the user” which is a child node and is even further strained to “get access to mail” and “get access to PW manager” which both end up being leaf nodes.

**5.0 conclusion**

The explanation and knowledge to understand of penetration testing, methodologies, SOP, and attack tree were the solid aim of this report.

With the knowledge of a Linux system with just an IP address of a target system the first aim was to find the best fitting methodology for this attack. Then with the knowledge gained a SOP was created and an attack tree which can be found in the appendix below.

**6.0 references**

* ENISA (2021). On the Watch for Incident Response Capabilities in the Health Sector. ENISA. [online] 11 Nov. Available at: https://www.enisa.europa.eu/news/enisa-news/on-the-watch-for-incident-response-capabilities-in-the-health-sector [Accessed 22 Nov. 2022].
* Malik, Keshav. “Learn Why Penetration Testing Is Important.” *Www.getastra.com*, 12 Oct. 2021, www.getastra.com/blog/security-audit/why-penetration-testing-is-important/. [Accessed 22 Nov. 2022].
* Figeczky, Boris. “Comparative Analysis of OSSTMM v3 and OWASP 4.0,” *Boris-Figeczky.medium.com*, 16 June 2021, boris-figeczky.medium.com/comparative-analysis-of-osstmm-v3-and-owasp-4-0-e3ae1bf95e9e. [Accessed 22 Nov. 2022].
* Vumetric.com. 2021. Top 5 Penetration Testing Methodologies and Standards | Vumetric. [online] Available at: [Accessed 22 Nov. 2022].
* Allen, L., Heriyanto, T. and Ali, S., 2014. Kali Linux – Assuring Security by Penetration Testing. [online] Google Books. Available at: [Accessed 23 Nov. 2022].
* Dewhurst Security Blog, 2010. OWASP Testing Methodology. [online] Blog.dewhurstsecurity.com. Available at: [Accessed 23 Nov. 2022].
* Vumetric, 2020. Top 5 Penetration Testing Methodologies and Standards | Vumetric. [online] Vumetric. Available at: [Accessed 23 Nov. 2022].
* Dalalana Bertoglio, D. and Zorzo, A., 2017. Overview and open issues on penetration test. Journal of the Brazilian Computer Society, 23(1). Available at: < https://link.springer.com/article/10.1186/s13173-017-0051-1#citeas/> [Accessed 23 Nov. 2022].
* Harvey, S., 2019. Stages of Penetration Testing According To PTES. [online] Kirkpatrickprice.com. Available at: [Accessed 24 Nov. 2022]
* Dinis, B. and Serrão, C., 2014. Using PTES and Open-Source Tools as A Way to Conduct External Foot Printing Security Assessments for Intelligence Gathering. [online] Infonomics-society.org. Available at: [Accessed 24 Nov. 2022]
* Harvey, S., 2019. What You Need to Know About OSSTMM. [online] Kirkpatrickprice.com. Available at: [Accessed 24 Nov. 2022].
* Shanley, A. and Johnstone, M., 2015. Selection of Penetration Testing Methodologies: A Comparison and Evaluation. [online] Pdfs.semanticscholar.org. Available at: [Accessed 24 Nov. 2022].
* Brush, k., 2021. What Is a Standard Operating Procedure (SOP)? Definition from SearchBusinessAnalytics. [online] SearchBusinessAnalytics. Available at: [Accessed 25 Nov. 2022].
* infopluse. “Guide to Modern Penetration Testing [Part 2]: Choose Your Box,” *Infoplus.com*, 15 Aug. 2018, www.infopulse.com/blog/guide-to-modern-penetration-testing-part-2-fifty-shades-of-grey-box. [Accessed 25 Nov. 2022].
* IT Security Concepts. 2020. Penetration Testing – IT Security Concepts. [online] Available at: [Accessed 25 Nov. 2022].
* Amenaza. 2021. What are Attack Trees?. [online] Available at: [Accessed 25 Nov. 2022].
* Mauw, S. and Oostdijk, M., 2006. Foundations of Attack Trees. [online] Citeseerx.ist.psu.edu. Available at: [Accessed 25 Nov. 2022].
* Buldas, Ahto, et al. “Attribute Evaluation on Attack Trees with Incomplete Information,” *Https://Www.sciencedirect.com/*, 30 Sept. 2019, www.sciencedirect.com/science/article/pii/S0167404819301774. [Accessed 26 Nov. 2022].
* Nemeth, Gergely. “Threat Modelling for Node.js Applications,” *Https://Snyk.io/*, 31 Aug. 2016, snyk.io/blog/nodejs-attack-tree-modelling/. [Accessed 26 Nov. 2022].
* OWASP. “The Web Security Testing Framework,” *Https://Owasp.org/Www-Project-Web-Security-Testing-Guide/V42/3-The\_OWASP\_Testing\_Framework/0-The\_Web\_Security\_Testing\_Framework*. Accessed [23 Nov. 2022].

**7.0 Appendices**

**7.1 Appendix SOP for pen testing**

Procedure for a Linux operating system penetration testing

1. **Purpose:**

The layout of establishment and then mitigate the vulnerabilities found throughout the penetration testing on the Linux system is the purpose of the SOP.

1. **Scope:**

The security vulnerabilities will be conducted of the target system in this penetration testing

1. **Testing type:**

This will be a grey box testing type as we know the IP address. However, as we only know the IP address and there is no other information available the intelligence gathering will be looked over.

1. **Procedure:**

Nmap will be the starting point of this vulnerability analysis with a port scan. This will be done to locate an open port with the target IP address. Then the use of vulnerability scanning tools such as OpenVAS or Nessus or even manual scanning will be done to find the exploits within the system. From the last phase a framework like Metasploit (for example) with the exploits found earlier the test will be performed to compromise the system.

1. **Post-procedure:**

The exploitation is complete. To gain root access the privileges are raised. The compromised system at this point will be maintained in control. Finally, the report will be constructed with a summary of the vulnerabilities and enormity of the risks in the pen testing with a list of ways to fix the problem in the system.

**7.2 attack tree (or decision tree) for pen testing a Linux server**

Diagram

Description automatically generated

The four main ways in which the attack on the Linux system will be preformed through penetration testing is:

1. Brute force attack – the basis from this attack will be from the user credentials being exploited. The methods to get past the brutal force stage will be hashcat or John ripper their mare many different ways but this however is the approach I will be taking.
2. Back door – resources grant remote access within the system. Type of malware that negates normal authentication to access system. The two tools to be used for this will be SSH key and corn job
3. Obtain from password file – the process in this will be the password hash and dictionary attack. The password hash will be split in shadowed password file and world readable password file
4. Obtain from entered – the two attacks will come from this will be visual observation and key logger.