University of Hertfordshire
School of Computer Science
BSc Computer Science (Networks)

Module: Computer Systems Security

Standard Operating Procedure and Attack Tree for Pen Testing

Anthonyc.co.uk

Your Name: Anthony Constant
Level 6
Academic Year 2020-21

Table of Contents

Anthonyc.co.uk

1.0 Introduction

1.1 Overview

Penetration testing also known as a pen test, is a form of security testing which assesses the security of the entire infrastructure of a network. Furthermore, it simulates a cyber-attack that a hacker would typically use to gain unauthorised accessed in order to check for exploits and vulnerabilities.

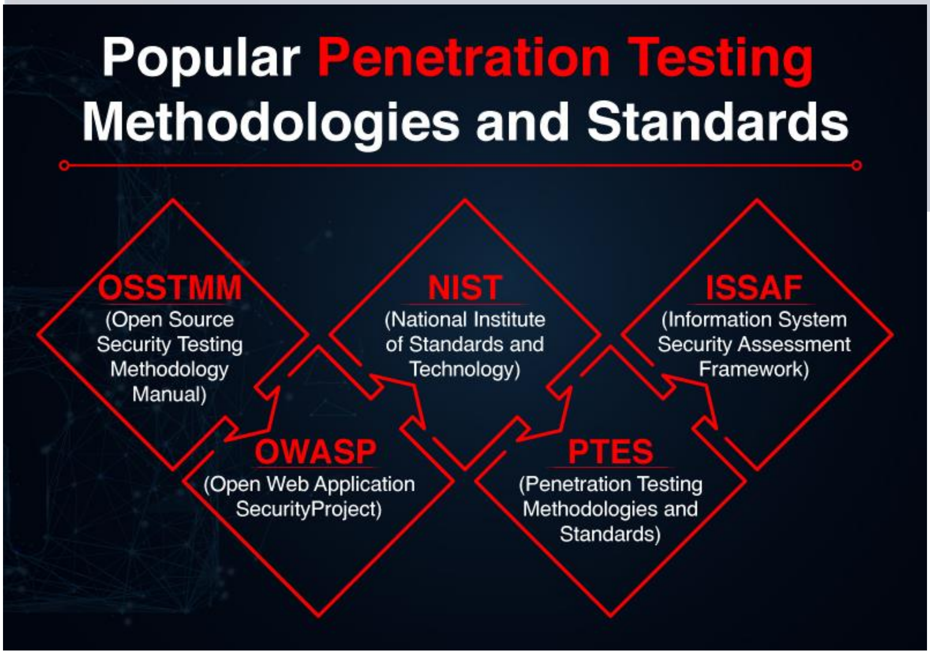
The phases of Penetration Testing consist of three unique steps in the following order, the pre-attack phase, attack phase and post-attack phase. Pre-attack phase consist of gathering information about the target. The Attack phase is the main basis of the attack strategy and post-attack phase is an essential part of the process where the tester must restore the network to its original condition. However, in this report we will be Defining the scope, Performing the penetration test and Reporting and delivering results.

There are different types of penetration testing such as internal, external or in between. Within systems security we refer to internal as White-box testing where the user has full knowledge whilst pen testing the network. Whereas Black-box testing is external, and the user has no knowledge which replicates an approach of an unprivileged attacker. Lastly, Grey-box testing is the most common approach to test vulnerabilities and the user is provided with limited information only. The different approaches mentioned are used to assess the different types of threats. However, the pen test being conducted in this report is a grey box test, as we have the IP address and are aware it’s a Linux operating server but limited to this information only.

This report describes and analyses the penetration testing methodologies such as OOSTM, OWASP, and PTES, with the purpose of performing the attack on a target and creating a report on it.

Anthonyc.co.uk

2.0 Penetration Testing Methodologies and Standards (Main Body Section 1)



Popular Penetration Testing Methodologies and Standards

OSSTMM (Open Source Security Testing Methodology Manual)

NIST (National Institute of Standards and Technology)

ISSAF (Information System Security Assessment Framework)

OWASP (Open Web Application SecurityProject)

PTES (Penetration Testing Methodologies and Standards)

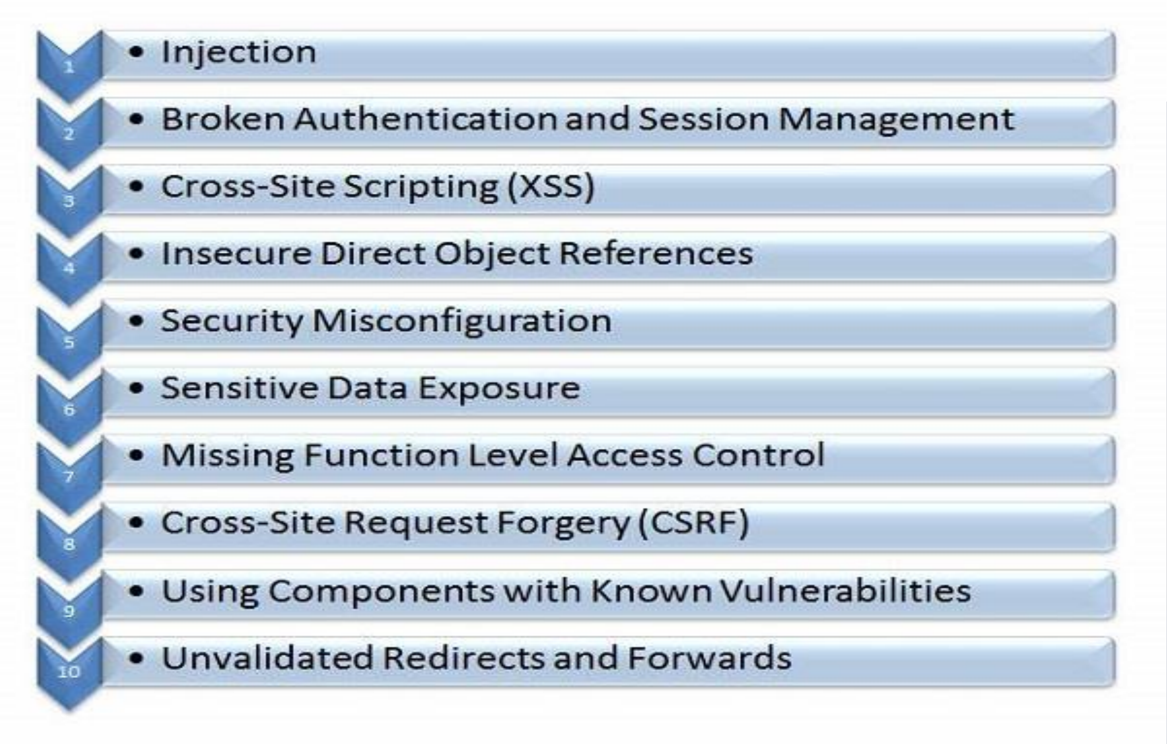
https://blog.eccouncil.org/5-penetration-testing-methodologies-and-standards-for-better-roi/

As mentioned previously, we will be describing and analysing pen testing methodologies in more detail with the purpose of understanding how each methodology operates.

2.1 Open Web Application Security Project (OWASP)

Open Web Application Security Project (OWASP) Methodology is best suited for testing web applications and is recognised as standard procedure within the industry. The OWASP method is based on an external approach therefore, it has black-box testing qualities and has some advantages. an advantage with OWASP is ensuring that web applications are better defended against cyber-attacks.

OWASP prescribes a very distinct number of steps in the following order:



1 • Injection
2 • Broken Authentication and Session Management
3 • Cross-Site Scripting (XSS)
4 • Insecure Direct Object References
5 • Security Misconfiguration
6 • Sensitive Data Exposure
7 • Missing Function Level Access Control
8 • Cross-Site Request Forgery (CSRF)
9 • Using Components with Known Vulnerabilities
10 • Unvalidated Redirects and Forwards

https://www.tutorialspoint.com/security_testing/hacking_web_applications.htm

One-way OWASP addresses web application risks is Injection and is perhaps one of the most common type of web hacking techniques that hackers use. For example, a hacker has acquired malicious SQL injection code, intended to inject and corrupt the database. However, OWASP is designed to implement strategies such as using Prepared Statements (with Parameterized Queries). Prepared Statements with Parameterized Queries is a method to precompile SQL statements and requires the correct parameters in order to be executed. Therefore, it's an effective method used to prevent SQL injection attacks and overcomes this issue found in most web applications.

Another advantage OWASP has is when an organisation applies this methodology to their software, it generally improves their overall reputation in terms of cyber defence. OWASP has set guidelines with the purpose to provide pen testers a way to tackling risks during the pen test. Furthermore, by pen testers adopting the OWASP approach, it allows them to refer to proven guidelines and improving the overall quality of the organisation's web applications.

However, one of the disadvantages is that the organisation is required trust the pen tester running the tests. As the pen tester has full knowledge of the organisations network (white-box testing). For example, the tester gets fired from the job and decides to go home and use this knowledge intended to cause damage to the organisation. OWASP methodology must be used in conjunction with another methodology to perhaps improve the prevention of an attack.

2.2 Penetration Testing Executing Standard (PTES)

The second methodology that is discussed here is Penetration Testing Execution Standard (PTES). The PTES methodology is a standard that was developed by a group of security experts, in order to test the cyber security of an organisation. This methodology also consists of seven phases in the following order:

1. Pre-Engagement - The pen tester organising and gathering the required tools to begin the pen test.

2. Intelligence Gathering – the pen tester is given information from an organisation, for the pen tester to gather more information using pen testing strategies.

3. Threat Modelling – an essential part to the phases in order to provide some clarification around which risks are most important.

4. Vulnerability Analysis - the pen tester is required to analyse the security risks found during a vulnerability test.

5. Exploitation – also known as the attack phase, it requires the pen tester to use the knowledge gathered to begin the exploitation phase.

Anthonyc.co.uk

6. Post-Exploitation – After exploiting the system, the pen tester is required to look further into the system for further potential vulnerabilities.

7. Reporting – an essential part of the phases which requires the pen tester to create a report consisting of all the knowledge gained from the previous phases and perhaps a conclusion for future work.

The advantage of this methodology is that it links in with the type of grey box test that will be conducted in assignment 3. Another advantage of the PTES method is that its overall guide contains good in-depth knowledge regarding the tools and commands for each stage of the pen test.

Intelligence gathering is an essential phase of the PTES methodology. It is used to gather as much information as possible against a target, then used to find vulnerabilities into an organisation. Information Gathering has three levels and level 1 uses automated tools to gather information on a target. Level 2 approach should match the organisation requirements using some of level 1 strategies. Level 3 involves full analysis of level 1 and 2, then a Red team is formed and ordered to attack the network to find vulnerabilities that could be exploited by potential hackers.

However, one disadvantage is that if the phases are not carried out correctly, it could perhaps cause damage to the servers and possibly corrupt the data. Within an organisation this could be damaging in terms of their reputation in cyber security.

As a result, it could be said that One goal of the PTES methodology is a structed approach in order to improve the overall quality of Penetration Testing within an organisation.

2.3 Open Source Security Testing Methodology Manual (OSSTMM)

The Open Source Security Testing Methodology Manual (OSSTMM) was developed in early 2000, in order to improve security testing. The manual is maintained by Institute for Security and Open Methodologies (ISECOM) and is updated every six months to remain valid with the most recent standards.

The OSSTMM consists of 5 phases in the following order:

1. Human Security– security revolving around human communications is required to be analysed by the pen tester.
2. Physical Security– OSSTMM requires testing the physical security that has a physical aspect of security.
3. Wireless Communications– any electronic communication or signal can be considered as wireless comms which is required to be tested.
4. Telecommunications– any communication regarding network lines are required to be tested by OSSTMM.
5. Data Network- OSSTMM requires the security testing of all data networks within an organisation, which are generally used for users to communicate over a network.

One advantage with OSSTMM is it provides guidance by focusing on these five phases that require a pen test to be carried out in order to test the security of an organisation. After analysing the five phases, it is built upon to find further vulnerabilities to be addressed accordingly.

Another advantage with OSSTMM is it also focuses on cloud computing, virtualisations and remote operations. It can be said because OSSTMM focuses on these 3 areas, it has more time invested to improving these areas than other methodologies.

Anthonyc.co.uk

However, one disadvantage with OSSTMM is that if each phase is not conducted correctly, it could perhaps give false positive results. Therefore, the organisation thinks they are safe however, if a genuine attack occurs without warning, it can be said it could have been prevented if the phase were carried correctly.

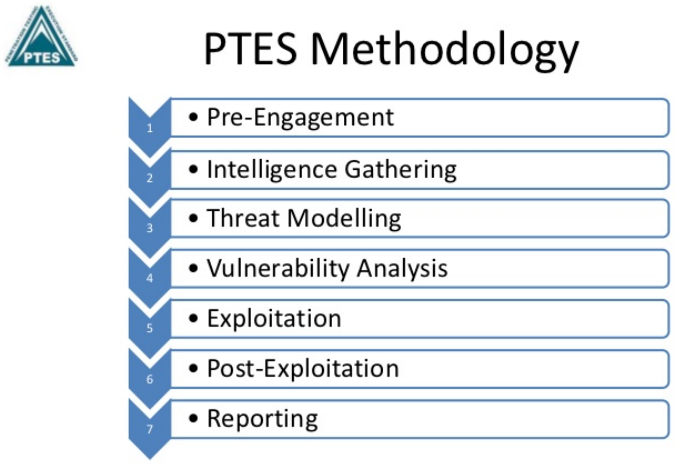
2.4 Summary

Based on the above analysis, it can be concluded that OSSTMM is the most suitable methodology based on the advantages been discussed. Furthermore, it has less phases than other methodologies mentioned previously, it can be said that because it consists of less phases that each phase is essential and has been revised well.

3.0 Standard Operating Procedure PTES Modified Document for a Pen Test (Main Body Section 2)

3.1 Introduction

A Standard Operating Procedure (SOP) for a pen test is a professional document which consists of procedures which is followed by a pen tester. It involves writing a set of instructions however, in this case we will be conducting an SOP on one of the methodologies discussed earlier. PTES describes a Standard Operating Procedure with these following steps however, it will be adjusted accordingly to our own attack for assignment 3:


PTES Methodology

1. Pre-Engagement
2. Intelligence Gathering
3. Threat Modelling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

https://pt.slideshare.net/SOURCEConference/ptes-pentest-execution-standard/11

3.2 Pre-Engagement

consists of the pen tester organising and gathering the required applications, software and hardware to start the penetration tests. Regarding the tests that will be carried out in Assignment 3, the required tools and software are:

- Virtual box (with Kali-Linux installed)
- Nmap – computer network tool to Scan for vulnerabilities (footprinting)
- Trace route – computer network tool for displaying exploiting possible routes.
- Wireshark – a free open source packet analyser to analyse the network activity in real time
- Metasploit - a computer security project that provides information about vulnerabilities
- OpenVAS – a framework to scan for vulnerabilities
- DOS attack – possibly to bring server down
- Worm Attack – to possibly infect a file

3.3 Intelligence Gathering

The pen tester is provided with general information given by the organisation including targets, for the pen tester to gather more information using network penetration testing. In this case for Assignment 3, we are provided with the target IP address to exploit further vulnerabilities to use in the attack phase.

3.4 Threat modelling

The process of prioritizing which strategies are implemented to maintain the security of the system. In this case, we will be prioritizing which is the best approach for an attack from the vulnerabilities found.

3.5 Vulnerability Analysis

Requires the penetration tester to identify, validate and analyse the security risks found during a vulnerability test. This is a way for the pen tester to find the vulnerabilities before the hackers do. In this phase for Assignment 3, the vulnerabilities which were found will be further analysed to gain more knowledge on the potential exploits.

3.6 Exploitation

This involves exploiting all the vulnerabilities found and gathered from the previous phases, in order to gain unauthorised access to a network or application breaking its security. In this case, the exploits that have been further analysed, will be used to gain access into the target's system/network.

3.7 Post-Exploitation

This is performed after the testing has been completed and the pen tester would generally consider an estimated value of the compromised network and list further potential to cause more harm if not fixed. In this case, after having performed the exploitation phase we generally look further into the attack that took place and find additional exploits and include this information in the next phase reporting.

3.8 Reporting

This is a technical report which consists of covering what has been tested, how it was conducted, the vulnerabilities found and lastly, how the pen tester manage to exploit the vulnerabilities. This will also provide an overview on how to improve the security of the exploitations found during these phases. It can be said that a report will be produced for Assignment 3 covering everything that occurred from the previous phases and conduct a conclusion.

Anthonyc.co.uk

3.9 Summary

As it can be seen from these steps, the SOP produced will have to follow the identical phases however, the Information Gathering phase will be ignored for the purpose of this test, because an IP address of the target is already provided. Furthermore, the PTES document has been modified accordingly to meet the brief for the attack conducted in Assignment 3.

The SOP is an essential document which provides an overall guide on each step on what to do and how to conduct it. It will also provide knowledge and feedback that can be analysed and discussed further to implement better security in the future.

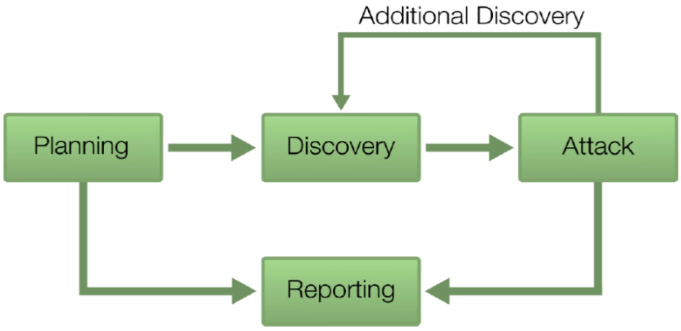
4.0 Decision Tree Analysis for Penetration Testing

4.1 Introduction

An attack tree is graphical representation of flow of actions that will happen during the attack however, we will be developing our own Decision Tree Analysis for a Penetration Test to be carried out in Assignment 3.

4.2 NIST Decision Tree Analysis

An example for an attack tree is the NIST methodology, which is intended to show a graphical representation of the steps taken requiring the tester to perform a pen test.



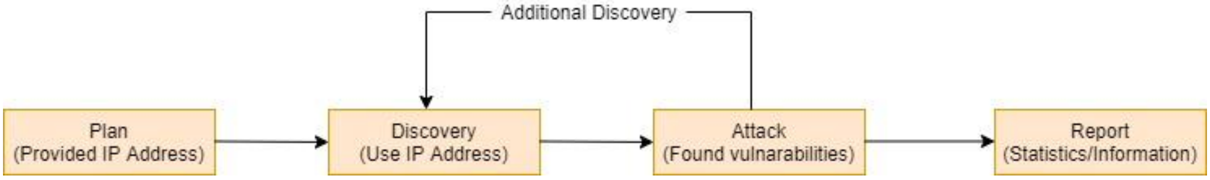
1. Planning – The process of brainstorming ideas of what will need to be done and how to do it in terms of pen testing. i.e. what tools/software are needed
2. Discovery – This involves the information that has been found to be gathered in order to carry out the next phase.
3. Attack – this consists of the pen tester carrying out the Penetration Test using the plan and information gathered from the previous phases.
4. Reporting – The process of producing a test report consisting of information gathered throughout the NIST Decision Tree.

Anthonyc.co.uk

In conclusion it can be said that NIST methodology is a suitable attack tree to be further extended on, using knowledge for the attack carried out in Assignment 3 and the information provided.

4.3 Developing a Decision Tree Analysis

As a result, it can be said that were going to create our own Attack Tree based on the NIST example above.

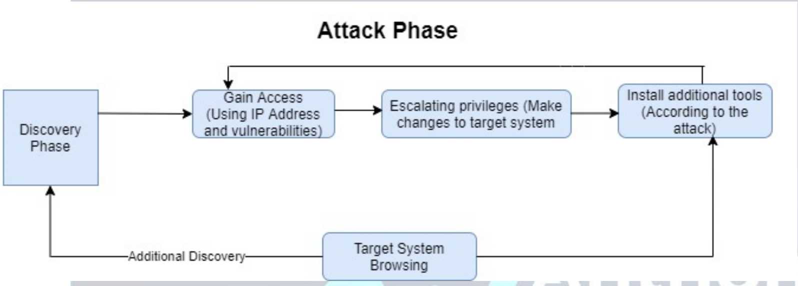


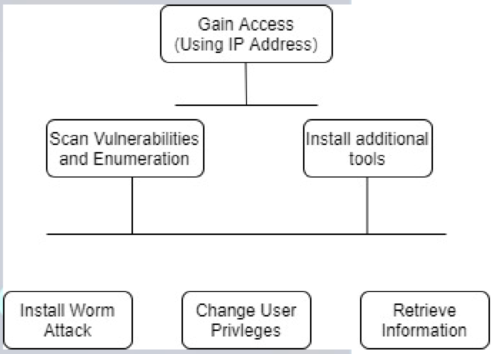
As you can see from the image above, the attack tree has been created and has been further developed using the NIST example. Furthermore, by adding brackets underneath with slightly more information provided to relate to our own attack in Assignment 3.

It can be said that in the Planning phase an IP address has already been provided. Next, in the Discovery phase uses the IP address to discover more information about the target. In the Attack phase, if any additional vulnerabilities are found they are logged back into the Discovery phase then proceed with Attack phase until no more vulnerabilities are found. Lastly, Report consists of all the Statistics and Information gathered from all the phases from the further developed NIST Decision Tree Analysis.

4.4 A Further Developed Attack Tree

An alternative Attack Tree has been created to provide additional information to the pen tester carrying out the tests, during the Attack phase. This Attack Tree shows that after the Discovery phase, will attempt to gain unauthorised access into the targets system. Next, once gained access into the targets system, change privileges accordingly. Next, install additional tools according to the attack and log it back into the Gain access phase, and continue target system browsing. Lastly, any additional discoveries made during the browsing phase, log it back into the Discovery phase.


Attack Phase
Discovery Phase
Gain Access (Using IP Address and vulnerabilities)
Escalating privileges (Make changes to target system
Install additional tools (According to the attack)
Target System Browsing
Additional Discovery



4.5 Summary

In conclusion, it can be said that after revising the different methodologies throughout this report, as a result I will be implementing the modified PTES methodology for Assignment 3. Furthermore, we are provided with an IP address and therefore, will be conducting a Grey-box Test on a Linux target. The SOP produced in this report, will be great guidance for each phase of the attack. Lastly, the Decision Tree Analysis created based on the example of NIST, will be implemented for assignment 3 as graphical guidance which now also matches the brief with suitable modifications.

6.0 References

Imperva. (2020) What is Penetration Testing. Available at: https://www.imperva.com/learn/application-security/penetration-testing/ [Accessed 14th November 2020]

The Redscan Team. (2020) Types of pen testing: white box, black box and everything in between. Available at: https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/ [Accessed 10th November 2020]

Vumetric (2020) Top 5 Penetration Testing Methodologies and Standards. Available at: https://www.vumetric.com/blog/top-penetration-testing-methodologies/ [Accessed 10th November 2020]

Dewhurst Security Blog. (2010) OWASP Testing Methodology Available at: https://blog.dewhurstsecurity.com/2010/03/08/owasp-testing-methodology.html#:~:text=The%20OWASP%20Web%20Application%20Penetration,and%20plays%20with%20the%20application. [Accessed 10th November 2020]

Communication Team. (2020) OWASP and its importance to Application Security. Available at: https://blog.convisoappsec.com/en/owasp-and-its-importance-to-application-security/ [Accessed 12th November 2020]

W3schools. (2020) SQL Injection. Available at: https://www.w3schools.com/sql/sql_injection.asp [Accessed 12th November 2020]

OWASP Cheat Sheet Series (2020) SQL Injection Prevention Cheat Sheet. Available at: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html [Accessed 12th November 2020]

Sarah Harvey. (2019) Stages of Penetration Testing According to PTES. Available at: https://kirkpatrickprice.com/blog/stages-of-penetration-testing-according-to-ptes/ [Accessed 13th November 2020]

Sarah Harvey. (2019) What You Need to Know About OSSTMM. Available at: https://kirkpatrickprice.com/blog/what-you-need-to-know-about-osstmm/#:~:text=The%20Open%20Source%20Security%20Testing%20Methodology%20Manual%2C%20or%20OSSTMM%2C%20is,and%20Open%20Methodologies%20(ISECOM).&text=The%20OSSTMM%20allows%20KirkpatrickPrice%20to,provide%20measurable%20and%20accurate%20results. [Accessed 13th November 2020]

Pentest-standard. (2014) High Level Organisation of the standard Available at: http://www.pentest-standard.org/index.php/Main_Page [Accessed 13th November 2020]

Pentest-standard. (2014) Intelligence Gathering. Available at: http://www.pentest-standard.org/index.php/Intelligence_Gathering#Level_1_Information_Gathering [Accessed 13th November 2020]

UKEssays. (November 2018) Standard Operating Procedure for Pen Testing. Available at: https://www.ukessays.com/essays/computer-science/standard-operating-procedure-for-pen-testing.php?vref=1 [Accessed 15th November 2020]

Toolshero. (2020) Decision Tree Analysis. Available at: https://www.toolshero.com/decision-making/decision-tree-analysis/#:~:text=A%20Decision%20Tree%20Analysis%20is,available%20to%20solve%20a%20problem.&text=A%20Decision%20Tree%20Analysis%20is%20created%20by%20answering%20a%20number,final%20choice%20can%20be%20made. [Accessed 17th November 2020]

Gani (2020) 'Penetration Testing as a Defence Operation' [PowerPoint presentation] *6COM1033 Computer Systems Security* Available at: https://herts.instructure.com/courses/77616/pages/lecture-unit-3-penetration-testing-as-a-defensive-operation-with-videos?module_item_id=1076195 (Accessed 17th November 2020)

Anthonyc.co.uk

7.0 Appendices

7.1 Appendix A Detailed SOP for Penetration Testing

1. Pre-Engagement consists of the pen tester organising and gathering the required applications to start the pen test. The applications and tools used in this test:

- Virtual box (with Kali-Linux installed)
- Nmap – computer network tool to Scan for vulnerabilities (footprinting)
- Trace route – computer network tool for displaying exploiting possible routes.
- Wireshark – a free open source packet analyser to analyse the network activity in real time
- Metasploit - a computer security project that provides information about vulnerabilities
- OpenVAS – a framework to scan for vulnerabilities

2. Intelligence Gathering in this case, will provide the pen tester with the IP address for the pen tester to gather more information on the target. The IP address of the target is provided there is no need for Intelligence gathering phase.

3. Threat Modelling will prioritize which strategy to implement to keep the system secure. Begin to prioritise the strategies to best implement defences using threat modelling strategies.

4. Vulnerability Analysis will require the pen tester to identify, validate and analyse the security risks exploited during the vulnerability testing phase. Begin to look at the vulnerabilities found from the previous phase and conduct an analysis on them.

Anthonyc.co.uk

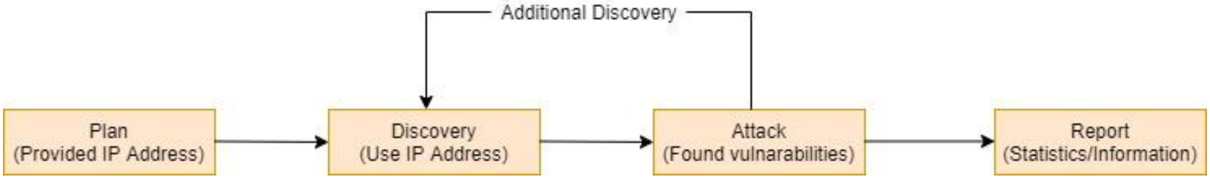
5. Exploitation phase will require the pen tester to exploit all vulnerabilities found to gain unauthorised access into the targets system. Begin the attack using the processed vulnerabilities found in the previous phase and break into the targets system. Possible attack scenarios:

- DOS attack – possibly to bring server down
- Worm Attack – to possibly infect a file
- Trojan horse – infect a file or application with malware

6. Post-Exploitation is handled after testing is complete and will require the pen tester to consider the vulnerabilities found and how the pen tester could potentially cause more harm. Begin to analyse the attack from the previous phase to find and exploit further attempts to attack the target.

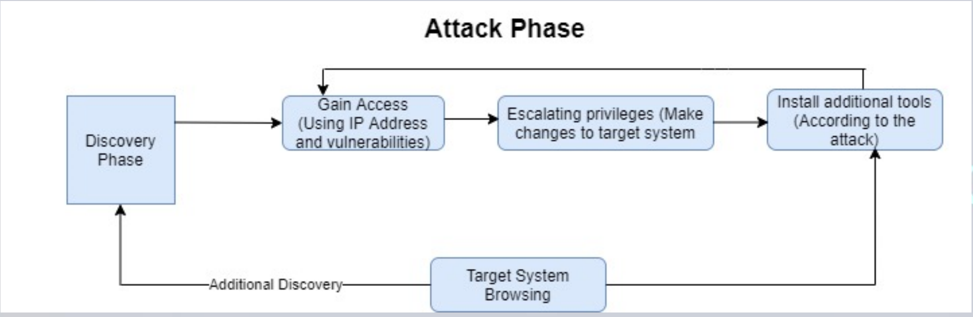
7. Reporting is a technical report which consists of all the information gathered from the seven phases. Therefore, the report should provide the pen tester more information to implement better security. Lastly, produce a report containing all the information from the previous phases in detail.

7.2 Decision Tree for pen testing a Linux Server



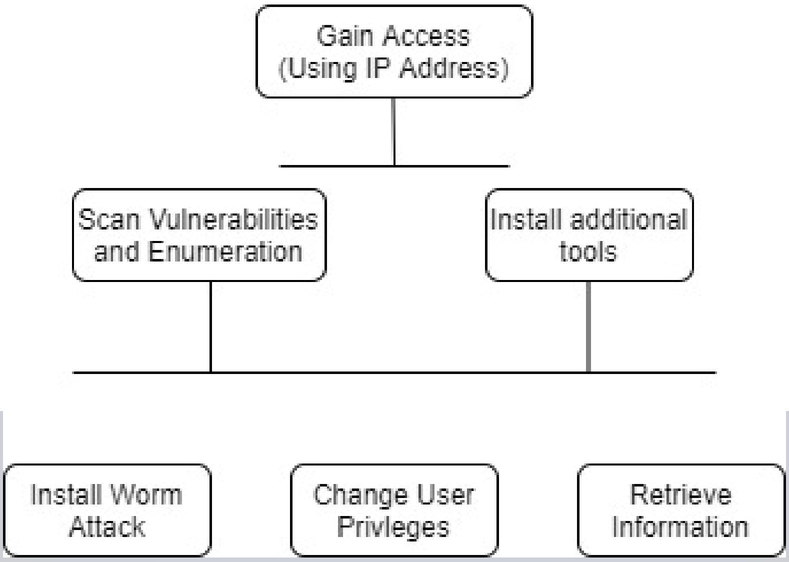
1. Plan phase will provide the pen tester with an IP Address to extend on the current plan.
2. Discovery phase will require the pen tester to use the IP Address to discover and gather intel on the target.
3. Attack Phase requires the pen tester to use the information acquired to carry out an attack on the target and report back to the Discovery phase, with any new intel attained during the Attack Phase.
4. Report phase is a technical document which consists of all intel gathered over all three phases.

7.3 Attack Tree for pen testing a Linux Server 1.0


Attack Phase
Discovery Phase
Gain Access (Using IP Address and vulnerabilities)
Escalating privileges (Make changes to target system
Install additional tools (According to the attack)
Additional Discovery
Target System Browsing

1. Discovery phase is apart of the Decision tree analysis then goes into the attack phase where it expands into a separate Attack Tree.
2. Gaining Access is apart of Attack Phase to attempt to gain unauthorised access into the targets system.
3. Escalating privileges generally consists of changing user rights to allow the pen tester to change information accordingly.
4. System Browsing phase means the pen tester has full access however, during this phase it can be said that you must install any additional tools to perhaps gain more information through an exploit. This must also be logged back into the Discovery Phase.
5. Installing additional tools if required and gain access through a different entry.

7.4 Attack Tree for pen testing a Linux Server 2.0



Attack Tree 2.0 has been developed based on Attack Tree 1.0. However, this attack tree expands on the Gain Access phase, as well as the attacks that could perhaps be carried out in Assignment 3.

Anthonyc.co.uk