|  |  |
| --- | --- |
| **Ethical Hacking**  Diploma in IT  Year 2 (2014) Semester 3 | Week 1 |
|  |
| **Tutorial 1 – Fundamentals of EH** | |

**Outcomes**

To be able to explain the concepts and meaning of some basic terms in of Ethical Hacking.

**Questions**

1a. There are fundamental differences between Ethical Hacking and Penetration Testing.

* 1. Discuss these differences.

[www.pen-tests.com/penetration-testing-vs-ethical-hacking.html](http://www.pen-tests.com/penetration-testing-vs-ethical-hacking.html)

Ethical hacking refers to use of computer attack techniques to find security flaws with the permission of the target’s owner and the goal of improving security of the target.

Penetration testing is a subset of ethical hacking. It involves the use of methodology and following the model process to systematically locate and establish targets, find vulnerabilities, exploit the flaws to determine potential impact and business risk. It has to be carried out under a controlled and safe manner according to a carefully designed scope and rules of engagement pre-established between the Pen-testers and the owner.

* 1. Describe the different types of Penetration Testing.

[www.pen-tests.com/types-of-penetration-tests.html](http://www.pen-tests.com/types-of-penetration-tests.html)

* Wireless Network Security Testing
* Network Penetration Testing
* System Penetration Testing
* Web Application Testing
* Social Engineering Testing
* Shrink wrapped software test
* Physical security test

1b. There is a process model for Ethical Hacking and Penetration Testing.

1. Describe each of the phases in Ethical Hacking.

|  |
| --- |
| Reconnaissance involves the attacker gathering information on the target which may be valuable during the attack. Information of interest range from organization and people to terminology used by the organization. Methods of reconnaissance can be categorized into 2 types: active and passive, where active uses social engineering while passive is usually through the use of search engines and social networking sites.  Scanning refers to the act of gathering information that is technical in nature such as URLs of database servers, type of database server and availability of open ports. The aim is to probe for services that have known weaknesses or vulnerabilities which the attacker can later exploit.  Exploit involves gaining access to the target system. Possible ways to gain entry is through the cracking of passwords or even through pass the hash where the hash of the password is used to gain entry. Once entry is done, the attacker would be able to carry out other activities such as escalating privileges to an administrator. |

1. Describe the phases in Penetration Testing that are not mentioned in 1b(i) above.

<http://x3n0n.com/stages-of-hacking>

The two phases are Planning and Reporting

In practice, Penetration Testing is a professional task after a contract between 2 companies is signed.

Planning phase involves scheduling which contains details on the pen test.

Report has to be completed and submitted to the client at the end of testing. This is done during the Reporting phase and it also involves details on the findings from the tests, risk level of vulnerabilities found, business impact as well as recommendations to counter the vulnerabilties.

1. Explain the concept of “footprinting”?

It refers to the information gathering process and involves activities to establish security posture of the organization being investigated.

1c. Describe the contents and the purpose of Scope and Rules of Engagement Document in Pen Testing.

|  |  |  |
| --- | --- | --- |
|  | Scope | Rules of Engagement |
| Purpose | Discuss what are to be tested  Address what should be explicitly avoided | Define how the test to is be carried out. |
| Contents | Should contain information on specific hosts/applications that are and are not to be tested. | Includes contact information of pen testing team and target organizations’, Method for exchanging information such as password and test outcomes, daily debriefing frequency and time/location, date/time of pen test |