The information system security essay sample

Law, Security

1. List the five (5) steps of the Hacking process.

Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks

2. In order to exploit or attack the targeted systems, what can you do as an initial first step to collect as much information as possible about the targets prior to devising an attack and penetration test plan?

The first step would be the reconnaissance or footprinting step of the hacking process.

3. What applications and tools can be used to perform this initial reconnaissance and probing step?

Whois query, ping sweeps, Nmap, etc

4. How can social engineering be used to gather information or data about the organization's IT infrastructure?

Social engineering is being used to by tricking people into giving out information that is not normally publicly available.

5. What does the enumeration step of the five (5) step hacking process entail and how is it vital to the hacker's objective?

Enumeration is used to extract more-detailed and useful information from a victim's system.

6. Explain how an attacker will avoid being detected following a successful penetration attack?

Attacker would avoid detection by covering tracks step of the hacking process where they cover up their tracks in the system they hacked into.

7. What method does an attacker use to regain access to an already penetrated system?

The hacker will use a backdoor into the system

8. As a security professional, you have been asked to perform an intrusive penetration test which involves cracking into the organization’s WLAN for a company. While performing this task, you are able to retrieve the authentication key. Should you use this and continue testing, or stop here and report your findings to the client?

You should follow the plan that was laid out in the planning stage of the penetration test

9. Which NIST standards document encompasses security testing and penetrating testing?

NIST 800-42 guideline on network security testing

10. According to the NIST document, what are the four phases of penetration testing?

Planning, Discovery, Attack, Reporting

11. Why would an organization want to conduct an internal penetration test?

By having the test done internally you don’t have to have an external company come in and test/see things about your network.

12. What constitutes a situation in which penetration tester should not compromise or access a system as part of a controlled penetration test?

Any situation where the testing can interfere with the companies operation

13. Why would an organization hire an outside consulting firm to perform an intrusive penetration test without the IT department’s knowledge?

Without the IT department’s knowledge of the test you would get a better understanding on how the system is day to day instead of having a test done on the network after the IT department puts effort into making the network more secure for the test.

14. How does a web application penetration test differ from a network penetration test?

A web application penetration test only deals with the web application or things that directly tie into the web application while the network penetration test you are testing every aspect of the network which could include the web application.

15. Explain both the information systems security practitioner and hacker perspectives for performing a penetration test.

The Information system security practitioner perspective of performing a penetration test is to try to increase or verify the security of the network while the hacker is trying to break into the network by using a penetration test.