**Review Questions**

|  |  |  |
| --- | --- | --- |
| **1.** | Which of the following statements best describes a white-hat hacker?   1. Security professional 2. Former black hat 3. Former gray hat 4. Malicious hacker | [White-hat hackers are good guys who use their skills for defensive purposes.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N14) |
| **2.** | A security audit performed on the internal network of an organization by the network administration is also known as \_\_\_\_\_\_\_\_\_\_\_.   1. Gray-box testing 2. Black-box testing 3. White-box testing 4. Active testing 5. Passive testing | [White-box testing is a security audit performed with internal knowledge of the systems.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N42) |
| **3.** | What is the first phase of hacking?   1. Attack 2. Maintaining access 3. Gaining access 4. Reconnaissance 5. Scanning | [Reconnaissance is gathering information necessary to perform the attack.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N70) |
| **4.** | What type of ethical hack tests access to the physical infrastructure?   1. Internal network 2. Remote network 3. External network 4. Physical access | [Physical access tests access to the physical infrastructure.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N98) |
| **5.** | The security, functionality, and ease of use triangle illustrates which concept?   1. As security increases, functionality and ease of use increase. 2. As security decreases, functionality and ease of use increase. 3. As security decreases, functionality and ease of use decrease. 4. Security does not affect functionality and ease of use. | [As security increases, it makes it more difficult to use and less functional.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N123) |
| **6.** | Which type of hacker represents the highest risk to your network?   1. Disgruntled employees 2. Black-hat hackers 3. Gray-hat hackers 4. Script kiddies | [Disgruntled employees have information that can allow them to launch a powerful attack.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N148) |
| **7.** | What are the three phases of a security evaluation plan? (Choose three answers.)   1. Security evaluation 2. Preparation 3. Conclusion 4. Final 5. Reconnaissance 6. Design security 7. Vulnerability assessment | [The three phases of a security evaluation plan are preparation, security evaluation, and conclusion.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N173) |
| **8.** | Hacking for a cause is called \_\_\_\_\_\_\_\_\_\_\_.   1. Active hacking 2. Hacktivism 3. Activism 4. Black-hat hacking | [Hacktivism is performed by individuals who claim to be hacking for a political or social cause.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N207) |
| **9.** | Which federal law is most commonly used to prosecute hackers?   1. Title 12 2. Title 18 3. Title 20 4. Title 2 | [Title 18 of the US Code is most commonly used to prosecute hackers.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N232) |
| **10.** | When a hacker attempts to attack a host via the Internet, it is known as what type of attack?   1. Remote attack 2. Physical access 3. Local access 4. Internal attack | [An attack from the Internet is known as a remote attack.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N257) |
| **11.** | Which law allows for gathering of information on targets?   1. Freedom of Information Act 2. Government Paperwork Elimination Act 3. USA PATRIOT Act of 2001 4. Privacy Act of 1974 | [The Freedom of Information Act ensures public release of many documents and records and can be a rich source of information on potential targets.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N282) |
| **12.** | The Securely Protect Yourself Against Cyber Trespass Act prohibits which of the following? (Choose all that apply.)   1. Sending spam 2. Installing and using keystroke loggers 3. Using video surveillance 4. Implementing pop-up windows | [Sending spam, installing and using keystroke loggers, and implementing pop-up windows are all prohibited by the SPY ACT.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N307) |
| **13.** | Which step in the framework of a security audit is critical to protect the ethical hacker from legal liability?   1. Talk to the client prior to the testing. 2. Sign an ethical hacking agreement and NDA with the client prior to the testing. 3. Organize an ethical hacking team and prepare a schedule prior to testing. 4. Analyze the testing results and prepare a report. | [Signing an NDA agreement is critical to ensuring the testing is authorized and the ethical hacker has the right to access the client's systems.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N332) |
| **14.** | Which of the following is a system, program, or network that is the subject of a security analysis?   1. Owned system 2. Vulnerability 3. Exploited system 4. Target of evaluation | [A target of evaluation is a system, program, or network that is the subject of a security analysis. It is the target of the ethical hacker's attacks.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N357) |
| **15.** | Which term best describes a hacker who uses their hacking skills for destructive purposes?   1. Cracker 2. Ethical hacker 3. Script kiddie 4. White-hat hacker | [A cracker is a hacker who uses their hacking skills for destructive purposes.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N382) |
| **16.** | MAC address spoofing is which type of attack?   1. Encryption 2. Brute-force 3. Authentication 4. Social engineering | [MAC address spoofing is an authentication attack used to defeat MAC address filters.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N407) |
| **17.** | Which law gives authority to intercept voice communications in computer hacking attempts?   1. Patriot Act 2. Telecommunications Act 3. Privacy Act 4. Freedom of Information Act | [The Patriot Act gives authority to intercept voice communications in many cases, including computer hacking.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N432) |
| **18.** | Which items should be included in an ethical hacking report? (Choose all that apply.)   1. Testing type 2. Vulnerabilities discovered 3. Suggested countermeasures 4. Router configuration information | [All information about the testing process, vulnerabilities discovered in the network or system, and suggested countermeasures should be included in the ethical hacking report.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N457) |
| **19.** | Which type of person poses the most threat to an organization's security?   1. Black-hat hacker 2. Disgruntled employee 3. Script kiddie 4. Gray-hat hacker | [Disgruntled employees pose the biggest threat to an organization's security because of the information and access that they possess.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N481) |
| **20.** | Which of the following should be included in an ethical hacking report? (Choose all that apply.)   1. Findings of the test 2. Risk analysis 3. Documentation of laws 4. Ethics disclosure | [Findings of the test and risk analysis should both be included in an ethical hacking report.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=103598934&rowid=58&noteMenuToggle=0&leftMenuState=1#answer.N506) |

**Answers**

|  |  |
| --- | --- |
| **1.** | White-hat hackers are "good" guys who use their skills for defensive purposes. |
| **2.** | White-box testing is a security audit performed with internal knowledge of the systems. |
| **3.** | Reconnaissance is gathering information necessary to perform the attack. |
| **4.** | Physical access tests access to the physical infrastructure. |
| **5.** | As security increases, it makes it more difficult to use and less functional. |
| **6.** | Disgruntled employees have information that can allow them to launch a powerful attack. |
| **7.** | The three phases of a security evaluation plan are preparation, security evaluation, and conclusion. |
| **8.** | Hacktivism is performed by individuals who claim to be hacking for a political or social cause. |
| **9.** | Title 18 of the US Code is most commonly used to prosecute hackers. |
| **10.** | An attack from the Internet is known as a remote attack. |
| **11.** | The Freedom of Information Act ensures public release of many documents and records and can be a rich source of information on potential targets. |
| **12.** | Sending spam, installing and using keystroke loggers, and implementing pop-up windows are all prohibited by the SPY ACT. |
| **13.** | Signing an NDA agreement is critical to ensuring the testing is authorized and the ethical hacker has the right to access the client's systems. |
| **14.** | A target of evaluation is a system, program, or network that is the subject of a security analysis. It is the target of the ethical hacker's attacks. |
| **15.** | A cracker is a hacker who uses their hacking skills for destructive purposes. |
| **16.** | MAC address spoofing is an authentication attack used to defeat MAC address filters. |
| **17.** | The Patriot Act gives authority to intercept voice communications in many cases, including computer hacking. |
| **18.** | All information about the testing process, vulnerabilities discovered in the network or system, and suggested countermeasures should be included in the ethical hacking report. |
| **19.** | Disgruntled employees pose the biggest threat to an organization's security because of the information and access that they possess. |
| **20.** | Findings of the test and risk analysis should both be included in an ethical hacking report. |