Ethical Hacking

Name

Institution Affiliation

Ethical Hacking

1. **What is ethical hacking?**

Ethical hacking that is also identified as penetration testing is a controversial act that involve locating weaknesses and vulnerabilities of computer as well as information system. The hackers do that by duplicating the intentions and activities of malicious hackers. In this regard, the ethical hacker applies their skills of hacking in pursuit of defense. They also do that on behalf of the owners of the information systems. While conducting these actions the ethical hackers need to answer the following basic questions (Norman, 2016). One of the main questions to answer is to identify some of the information or locations that malicious hackers can get access to. Secondly, they need to rule out what the attacker might see when they attack. Thirdly, ethical hackers need to establish what the attacker can do with the information once they access it. Finally, they need to figure out if there is anyone at the system who is able to notice malicious attempts.

1. **What types of industries do ethical hackers come from?**

In most cases, ethical hackers come from industries that deal with information systems as well as cyber security. These hackers should exhibit their vast skills in computer operations. Organizations that deal with variety of computer system are likely to produce ethical hackers since they mostly deal with operating systems. Organizations that belong to industries that deal with network hardware platforms have the capability of producing ethical hackers (Lu, 2020). The possibility comes in because majority of cybercrimes are made possible due to incorporation of network hardware that ease these activities. However, due to controversies surrounding the profession of ethical hacking, different councils have come up with agencies that provide professional certification. The certification involves complete course work of twenty two modules.

1. **What types of organizations utilize ethical hackers and why? What types of operations do hackers conduct to test an organization’s vulnerabilities?**

Organizations across industries such as healthcare, finance, government, and many more utilize the services of ethical hackers as they offer them with security from malicious hackers. These companies use the ethical hackers’ services as they are the best in determining if there are possibilities for hackers to attack a network (Brill & Smolanoff, 2017). Also they help them understand if there is any possibility and what they can do in such cases. Ethical hackers also help these organizations in figuring out what they can do to protect the system from attackers. Ethical hackers carry different types of assessment to determine the vulnerability of a system. Network-based scans are one of the tests that these white hackers use to determine the vulnerability of systems. These scans help in identifying possible network attacks. Other tests include; wireless network scans, application scans, and database scans (Norman, 2016). These types of scans help identify vulnerability of a system in wireless networks, websites, and software as well as identify weak points in databases.

1. **Does it pay for companies to hire hackers? (Cost/benefit ratio?)**

Ethical hacking is an important hacking in organization as it offers them with security from external attacks. Although there are some instances that it might not work, its overall performance is significant for any company willing to conduct it. Cyber security threats are common issues affecting business in todays’ life. The cost related to cyber-attack is estimated to be around two trillion dollars worldwide and it is a problem that is going nowhere. Additionally, there is evolution of smart criminals that specialize in the threat (Najera-Gutierrez & Ansari, 2018). In this regard, the cost involved in hiring a hacker to access companies’ system as a way of protecting it will be beneficial to most companies. Therefore, the companies that hire hackers benefit from their decisions meaning it pays for hiring hackers.

1. **Are there any negative aspects or moral concerns with ethical hacking? What about professional or legal concerns.**

Ethical hacking is surrounded by controversies as the process does not guarantee an organization its security. Be it as it may, these actions identify security vulnerability and risks, but it does not explain what happens to hackers given mandate to intrude the system (Lu, 2020). Thus, one negative concern of ethical hacking is that it presents risk of information revelation. Legal issues that surround the acts involve lawsuits as a result of confidential information disclosure. Such revelation may lead to legal battle that involves the organization and the ethical hacker (Brill & Smolanoff, 2017). During the process the hacker can commit errors hence affecting the profitability of the organization. Professional issues involving ethical hacking may involve ineffective performance of e job. Since the hacker is limited to sensitive information of the organization, they may be unable to perform effective job as intended.

1. **Are there any government of Canada agencies who help safeguard organizations or conduct vulnerability assessments or are ethical hackers predominately from the private sector?**

The government of Canada introduced the office of Government Accountability (GAO) that is mandated to report any risk identified in the critical infrastructure in the systems. The office found out that the federal systems as well as critical infrastructure was growing and as a result they were able to identify several incidents that included computer attacks. According to Thomas, Burmeister, and Low (2018), some of the targeted systems included energy and nuclear sector, and number of banks. In this regard, the government equipped the office with relevant inputs that would ease the attempt to identify cyber-attacks. Also, the government dealt with the challenges that the office might face in pursuit to counter cyber threats. However, private sector in Canada has made several attempts of developing agencies that deal with cyber security. In this regard, different organization has trained ethical hackers that assist in providing with hacking services.

References

Brill, A., & Smolanoff, J. (2017). Hacking Back Against Cyberterrorists: Could you? Should you?. *Defense Against Terrorism Review,(ISSN. 1307-9190) is a peer-reviewed journal published by the NATO Center of Excellence-Defense Against Terrorism, Ankara, Turkey. This article appears in*, *9*.

Lu, D. (2020). When Ethical Hacking Can't Compete. Retrieved 31 January 2020, from https://www.theatlantic.com/technology/archive/2015/12/white-hat-ethical-hacking-cybersecurity/419355/

Najera-Gutierrez, G., & Ansari, J. A. (2018). *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux*. Packt Publishing Ltd.

Norman, A. T. (2016). *Hacking: Computer Hacking Beginners Guide how to Hack Wireless Network, Basic Security and Penetration Testing, Kali Linux, Your First Hack*. CreateSpace Independent Publishing Platform.

Thomas, G., Burmeister, O., & Low, G. (2018). Issues of Implied Trust in Ethical Hacking. *ORBIT Journal*, *2*(1).