Ethical Issues in Penetration Testing

In the security sector, there are multiple different actions, procedures, and policies that can border the line of ethics. However, none of these do so more than penetration testing. Penetration testing is the act of using an attackers methods of network hacking in order to find vulnerabilities within a network and help businesses and organizations remediate these vulnerabilities before hackers with mal-intent exploit them for personal gain. Penetration testing is on the very border of ethics based upon the person conducting the penetration test. Penetration testers have the ability to exploit vulnerabilities for malicious purposes on a day to day basis; however, they do not because they are driven by ethics and morals. This paper will delve into the situations where this could be possible, and the avenues taken by network penetration testers to avoid exploiting vulnerabilities with malicious intent.

When approaching a penetration test, the tester will follow five procedural steps: information gathering, exploitation, enumeration, privilege escalation, and covering tracks. During the first step of the test, the tester will gather information on the network, system of networks, or device they are looking to assess. The attacker will gather information including the operating system used and its version, the open ports on the device, the user currently on the device, the domain the device is a part of, etc. This information can be considered proprietary, confidential, or top secret depending upon the environment in which it set. With this in mind, penetration testers must keep the confidentiality of these devices a necessity when conducting this test, and after the test is complete. There is an abundance of information being sold on the dark web that is considered high confidential regarding government or organization data. The penetration tester must keep to their ethics and moral when viewing this information to ensure that the data does not fall into the wrong hands. Not only this, but the penetration tester should evaluate all information that is subject to the scope of the test. The tester should follow the

organizations guidelines for the test, and to never fall into the temptation of looking for more confidential information.

The next phase of the test includes exploitation. The tester should exploit vulnerabilities found within the information gathering stage and should only exploit vulnerabilities that were discussed in the scope of the test prior to it occurring. It can be tempting for the attacker to become curios on whether or not a certain exploit will work, but that can cause damage including loss of confidentiality or availability; however, all security control assessments should be done with the businesses continuity in mind.

The next part of the test is enumeration, and this phase assumes the exploitation has already occurred on a system or group of systems. The tester will now be looking into the internal data found on machines and the internal data flowing within a network. This data tends to be more critical and confidential because it is not easily-accessible by external means. Therefore, it is crucial that the tester never shares this confidential data with anyone not within the scope of the assessment and that has authorization to see this data. The tester must keep in mind the overall goal of the assessment, that is to assist the business or agency to better secure their data, both at rest and in transit. Any breach of confidentiality that is leaked to unauthorized parties can be seen as a failure by the tester as they did not take appropriate ethical manners in order to ensure this security principle.

After this the tester will look to escalate privileges. This can include password exfiltration, account impersonation, golden ticket attacks, remote code execution, or account compromise. Testers should keep the confidentiality of these accounts their top priority. The information regarding these accounts should never be accessed by those parties not authorized to see this information. Not only this, but often times privilege escalation can include the

exploitation of a vulnerability on a higher-level system. Therefore, the information regarding this vulnerability should never be released to the public eye but should instead be given to authorized parties in the encouragement of vulnerability remediation.

Finally, depending on the type of test, penetration tester will cover their tracks in hopes of not being caught by the active security controls in place. However, if found successful, the tester should never disclose their method of concealment, but to only authorized parties. In the end, the hope of a penetration test is to assess security controls in place, test systems based upon the vulnerabilities found, and help organization and internet technology professionals to remediate the vulnerabilities found.

The job of a penetration tester fully revolves around ethics and morals. That is what separates them from a regular hacker. Hackers hold no morals with the actions they take. However, a penetration tester uses their own tactics in order to help businesses and agencies better strengthen their security posture.