2.5.4 Legal and Ethical Compliance Facts

An ethical hacker's role is to break the rules and hack into a organization's network and systems. Before this is done, both the penetration tester and organization must know and agree to everything being done. Once the scope of work is finalized, there may be additional laws that need to be looked at and followed.

This lesson covers the following topics:

- Federal laws
- Cloud-based and third-party systems
- Ethical scenarios
- Corporate policies

Federal Laws

There are two key federal laws that apply to hacking: Title 18, Chapter 47, Sections 1029 and 1030. One thing that stands out in these laws is in most of the statements, the words unauthorized or exceeds authorized access are used. These keywords are what apply to the ethical hacker. The ethical hacker needs to ensure they access only the systems to which they have explicit permission and only to the level they have authorized access.

- Section 1029 refers to fraud and related activity with access devices. An access device is any application or hardware that is created specifically to generate access credentials.
- Section 1030 refers to fraud and related activity with computers or any other device that connects to a network.

In addition to the above two laws, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies was amended in 2013 to include intrusion software. This agreement is between 41 countries that generally hold similar views on human rights. The update in 2013 has led to a lot of issues and confusion in the cybersecurity field, as many of the tools used in the penetration testing process can also be used by black hat hackers for malicious purposes.

In 2018, the Wassenaar Arrangement was updated to clarify some of these policies. This will hopefully make things easier for some penetration testers involved in international testing.

Cloud-Based and Third-Party Systems

When dealing with cloud-based systems or other third-party systems, special considerations need to be made. If an organization is using a cloud-based system, that means the organization doesn't own the system and cannot legally provide permission for a penetration test to be carried out on that system. The penetration tester must make sure to get the explicit permission from the cloud provider before performing any tests.

Third-party systems can also cause some issues for the penetration tester. If systems are interconnected, such as in a supply chain, the penetration tester needs to ensure they do not accidentally access the third party's systems at all. The penetration tester may also run across vulnerabilities that can affect the third party. In this scenario, the penetration tester needs to report findings to the client and let the client handle the reporting.

Ethical Scenarios

Aside from the laws and regulations, the ethical hacker must be aware of scenarios where ethical decisions need to be made. One particular instance that can cause an issue is when the penetration tester resides in one state and the organization is in another state. The laws that govern computer usage and hacking can vary from state to state. When this occurs, the penetration tester and the organization need to agree on which set of laws they will adhere to. Whenever there are any questions or concerns regarding laws and regulations, a lawyer should be consulted.

There will be instances where the ethical hacker will run across data and may not be sure what to do with it. There are instances, such as child pornography, that is considered a mandated report - these sorts of findings must always be immediately reported, no exceptions. In any other situation where data is discovered that is not a mandated report, the data should be disclosed to the client. As always, when there is doubt about which course of action to take, a lawyer should be consulted.

Corporate Policies

Corporate policies also play a role in how a penetration test is carried out. Corporate policies are the rules and regulations that have been defined and put in place by the organization. As part of the risk assessment and penetration test, these policies should be reviewed and tested. Some common policies that most organizations have defined are password polices, update frequency, handling sensitive data, and bring your own devices. The organization needs to determine which, if any, of these policies will be tested during an assessment.