Christian Green

CSCI 452

Dr. Lin

January 25, 2026

Network Pen Testing Ethics

A network pen tester's responsibility is to identify vulnerabilities of a computer network by attempting to gain access. The pen tester looks through the hackers' point of view and is supposed to mimic the actions of the hacker and therefore think like them. The difference between the real hacker and the pen tester is the ethics and their morals. The pen tester's attempted attacks on the network are to benefit the system by hardening it to reduce the span of the hackers' potential methods of attack. The hacker has malicious intent and wants to gain access to the network for their own reasons of exploiting the system like for financial gain or recognition. The quality that they share is the assumption that the system is security, is untrustworthy and can be compromised.

The users of a system and the pen testers should never assume a system is trustworthy. An attacker does not have to be an outsider. An attacker could be an everyday user of the system who is authenticated. It should not be assumed that the only threats to a system come from outside because anyone can have malicious intent. "The heart is deceitful above all things, and desperately sick; who can understand it?" (English Standard Version, 2001/2025, Jeremiah 17:9). People with authorized internal access to a network are human and are deceitful because the heart is deceitful. Therefore, there should never be an assumption that a system is safe and

that the environment is trusted. A pen tester needs to assume that threats can come from anywhere and secure a system from all people and not just from the dangers on the outside.

The goal of a pen tester is to reveal any shortcomings of a security system so they can be fixed or improved upon. By assuming that there are vulnerabilities and the system is untrustworthy, it opens the door for brainstorming and executing methods of attack. Devices on a network could have settings misconfigured and improper authorization methods in place that do not provide the level of protection they should. Software malfunctions and errors in application code could also cause errors. Network access points and firewalls should be checked repeatedly to ensure they are secured properly because no one should assume that everything is configured properly or has not been tampered with. All activity should be constantly monitored. The system should be checked to make sure that both horizontal and vertical privilege escalation are not possible without proper authorization. The protection of the system's security checks should be done on a consistent basis because what looks secure on the surface can have flaws. Jeremiah 17:9 warns against trusting things that seem unproblematic at the surface because people can be deceived.

Human factors pose a monumental risk to a system's security. As stated in Jermiah 17:9, the human heart is deceptive and should not be trusted. One method bad actors love to use to gain unauthorized access to and then compromise a system is social engineering. This directly involves one human attempting to deceive another to cause them harm. This could involve tricking them into downloading malware or sending confidential data that should be kept secure as well as many other tactics. Humans could also make honest mistakes that could result in an entire system being compromised, such as having weak passwords or poor security policies. These are on the side of the system administrators and network users but poor decisions here can have serious consequences. Without proper software to block access to a system, a hacker could use brute force methods to gain access by guessing a password that was too simple. This

relates to policy and the system's administrators should set basic security rules for all users of the system to ensure it stays safe. Effective policy could also help to prevent social engineering attacks by setting rules in place for users to follow. These rules should tell users when they should send out data and how to recognize something that is probably fraudulent. They should also have restrictions on what they are allowed to download. In this sense, preventing a network breach is not entirely on the work of the IT employees but also on the people in charge of the network and the policies they implement.

The tester must have respect for the people they work for and integrity. There are given a lot of power, so they must use it responsibly. The only differences between the hacker and the pen tester are their morals and intent. A tester could completely compromise a system the same way a hacker can. The tester must have the integrity to report any vulnerabilities that were discovered because of their work. Without the ability to trust the tester, the system could be in just as much danger as if they did not attempt to fix any of the system's vulnerabilities. One method of protecting a network is by using the architecture of the network itself as protection. This can be achieved through segmentation which has many layers to the network and subnets within it. This protects important servers and other devices that store crucial data that cannot be compromised. Network pen testers, however, are fully aware of the network architecture and could completely compromise devices and sensitive data during a security breach test. They need to have morals and restraint when conducting tests. The scope of the test should be clearly stated to the testers before they begin. They should be fully aware of the boundaries of what is allowed and only conduct their tests in an ethical manner.

The policies that should be implemented for the system to remain secure should involve the principle of least privilege. A system's users and applications should not have more permission than they need to perform their tasks. Each user and application should have minimum permissions to ensure they do not have access to files and data they do not need to

use. This will prevent them from manipulating them whether it was an accident or not. Humans cannot be trusted as stated in Jeremiah 17:9. This is the justification for limiting the allowed actions of users and it will maintain the system's efficiency and security.

Citations

English Standard Version Bible. (2001). ESV Online. https://esv.literalword.com/.