1.1.1 Overview

1.1.1 Overview

Protego Security Solutions

Alex here! We will be meeting periodically over the next few weeks so you can get oriented to working at Protego and also build your skills and knowledge as we increase your involvement in our customer engagements.

At the very heart of what we do is our purpose. You need to understand why we do what we do and who our enemies are. Once you have a strong foundation here, we can move on to understanding how we accomplish our purpose.

As a refresher, the term ***ethical hacker*** describes a person who acts as an attacker and evaluates the security posture of a computer network for the purpose of minimizing risk. The NIST Computer Security Resource Center (CSRC) defines a *hacker* as an “unauthorized user who attempts to or gains access to an information system.” Now, we all know that the term *hacker* has been used in many different ways and has many different definitions. Most people in a computer technology field would consider themselves hackers based on the simple fact that they like to tinker. This is obviously not a malicious thing. So, the key factor here in defining ethical versus nonethical hacking is that the latter involves malicious intent. The *permission to attack* or permission to test is crucial and what will keep you out of trouble! This permission to attack is often referred to as “the scope” of the test (what you are allowed and not allowed to test). More on this later in this module.

A security researcher looking for vulnerabilities in products, applications, or web services is considered an ethical hacker if he or she responsibly discloses those vulnerabilities to the vendors or owners of the targeted research. However, the same type of “research” performed by someone who then uses the same ***vulnerability*** to gain unauthorized access to a target network/system would be considered a nonethical hacker. We could even go so far as to say that someone who finds a vulnerability and discloses it publicly without working with a vendor is considered a nonethical hacker – because this could lead to the compromise of networks/systems by others who use this information in a malicious way.

The truth is that as an ethical hacker, you use the same tools to find vulnerabilities and exploit targets as do nonethical hackers. However, as an ethical hacker, you would typically report your findings to the vendor or customer you are helping to make the network more secure. You would also try to avoid performing any tests or exploits that might be destructive in nature.

An ethical hacker’s goal is to analyze the security posture of a network’s or system’s infrastructure in an effort to identify and possibly exploit any security weaknesses found and then determine if a compromise is possible. This process is called *security* ***penetration testing*** or *ethical hacking*.

TIP Hacking is NOT a Crime (*hackingisnotacrime.org*) is a nonprofit organization that attempts to raise awareness about the pejorative use of the term *hacker*. Historically, *hackers* have been portrayed as evil or illegal. Luckily, a lot of people already know that hackers are curious individuals who want to understand how things work and how to make them more secure.

1.1.2 Why Do We Need to Do Penetration Testing?

So, why do we need penetration testing? Well, first of all, as someone who is responsible for securing and defending a network/system, you want to find any possible paths of compromise before the bad guys do. For years we have developed and implemented many different defensive techniques (for instance, antivirus, firewalls, intrusion prevention systems [IPSs], anti-malware). We have deployed defense-in-depth as a method to secure and defend our networks. But how do we know if those defenses really work and whether they are enough to keep out the bad guys? How valuable is the data that we are protecting, and are we protecting the right things? These are some of the questions that should be answered by a penetration test. If you build a fence around your yard with the intent of keeping your dog from getting out, maybe it only needs to be 4 feet tall. However, if your concern is not the dog getting out but an intruder getting in, then you need a different fence – one that would need to be much taller than 4 feet. Depending on what you are protecting, you might also want razor wire on the top of the fence to deter the bad guys even more. When it comes to information security, we need to do the same type of assessments on our networks and systems. We need to determine what it is we are protecting and whether our defenses can hold up to the threats that are imposed on them. This is where penetration testing comes in. Simply implementing a firewall, an IPS, anti-malware, a VPN, a web application firewall (WAF), and other modern security defenses isn’t enough. You also need to test their validity. And you need to do this on a regular basis. As you know, networks and systems change constantly. This means the attack surface can change as well, and when it does, you need to consider reevaluating the security posture by way of a penetration test.

Revision #1
Created 30 August 2023 18:16:30 by naruzkurai
Updated 30 August 2023 18:17:46 by naruzkurai