Understanding Trust: Student Instructions

In this workout, you will learn the danger of misapplying trust. The foundation of cybersecurity lies in establishing a basis for trust through secure engineering. Cyber attacks are often successful because people misapply trust or do not have a solid basis for trust in the systems they use.

In this workout, you will look at trust from an adversary's perspective and try to gain the trust of the target. You will do so through what is known as a credential harvesting attack. These attacks work by copying a website login page that the user trusts and tricking a user into entering their credentials for the site.

This type of attack is common with phishing, in which a fake email directs the user to a malicious site for the purpose of harvesting their credentials (i.e. password) to the site. For example, the attacker might use social media websites. Then, once they have the credentials, they either use the social media account or take advantage of the fact that people choose the same password for multiple accounts and login to their bank account.

> The tools you use in this workout are for educational purposes only. Using these tools outside of an educational environment on other people, even for experimental purposes, is harmful, unethical, and unlawful. Doing so may result in criminal penalties and fines.

Let's workout! Log into your workout through the landing page with the credentials you are provided (e.g. cybergym1). This will take you to your workout machine. On the desktop right-click and select to open a command terminal.

At the command terminal, type in ssh kali@10.1.1.30. At the password prompt, type `P@55w0rd!`. This will log you into your Kali Linux workstation.

Once in Kali, you will be using the tool Social Engineering Toolkit provided as open-source by TrustedSec and authored by David Kennedy. Follow these instructions to mount the attack:

1. To use the tool type `sudo setoolkit` at the command line and retype the password from above.
2. The tool will prompt you to agree to the terms of use. If you agree, type *y* to continue. Then a menu will pop up with various attack modules.
3. Select `1) Social Engineering Attacks`
4. For the type of attack to mount, select `2) Website Attack Vectors`
5. Next, select `3) Credential Harvester Attack Method`.

6. Then, you will be provided options for generating the fake website. Choose the first method, which pulls predefined web templates: `1) Web Templates`
7. The tool will take a few seconds to prepare, and then it will ask you the IP address of the attacker machine. Type in `10.1.1.30`. For this workout, the fake website and the harvester are the same. This would not typically be the case.
8. Finally, you will be provided with a template for the fake website. Use `2. Google`.

To see your new credential harvester, open a browser on your workout desktop, and go to http://10.1.1.30, and type in some fake credentials. When you return to the kali command line, you should be able to see the credentials entered.