ROOK SECURITY

SOCIAL ENGINEERING

THE ART OF HUMAN HACKING

Social engineering is a method of intrusion malicious attackers employ that relies heavily on human interaction. Social engineering is reliant upon the ability to manipulate people into breaking normal security procedures; it tricks people into performing actions or sharing information. Nearly all of the recent major data breaches are the direct result of targeted phishing attacks - "spear phishing." Rook Security provides a wide range of social engineering services designed to emulate the techniques used by hackers and to assess the effectiveness of your security awareness training efforts.

SOCIAL ENGINEERING TESTS THE EFFECTIVENESS OF YOUR INFORMATION SECURITY CONTROLS AND PROVIDES AN ASSESSMENT OF YOUR SECURITY AWARENESS TRAINING.

EMAIL PHISHING

Rook works closely with your information security team and other stakeholders to design a phishing campaign that closely imitates email that your employees would reasonably expect to receive, but with content that indicates that the email should be treated with suspicion. The campaign can be conducted randomly or with specific targets. Hackers typically target finance personnel, executive assistants, and human resources teams.

PHONE PHISHING

Human interaction is the key to a successful phone phishing campaign. Rook will design and conduct an exercise that tests the ability of your employees to detect, deflect, and report suspicious calls. A commonly employed methodology is to pose as your organization's IT help desk and attempt to convince a user into allowing access to their computer or to persuade them to share their username and password.

RED TEAM EXERCISE

A Red Team Exercise incorporates attempts to gain physical access to an organization's computing assets. Rook Security specialists will pose as vendors, repairmen, visiting executives, or other familiar people and try to coerce your company's personnel into allowing them unsupervised entry into your facility. Our team will then plant non-disruptive evidence to indicate the level of access that would have been allowed by a malicious actor to compromise your controls and gain access to information.

WE ATTEMPT TO COMPROMISE YOUR CONTROLS AND GAIN ACCESS TO INFORMATION.

BLACK TEAM EXERCISE

The Black Team goes where most security professionals don't: into the mindset of an attacker. With Black Team Exercises, we take the handcuffs off and infiltrate an organization's system—getting to know everyone by name, how they take their coffee, what they read, and so on. We need to know everything we can about these people, just like a hacker would. If we truly want to test an organization's security, we need to redefine what we consider a penetration test. We need to take security to an entirely new class of service. This isn't something that can be done in a matter of days—it will take months, or even a year to complete a Black Team Exercise. But if attackers never back down, neither can we.

WE TAKE THE HANDCUFFS OFF AND GO ROGUE, INFILTRATING THE ENTIRE ORGANIZATION.