SOCIAL ENGINEERING

DATA SHEET

What is Social Engineering?

Social Engineering is the art of manipulating people in order to gain access to some sort of information that they usually wouldn't give up – in most cases, confidential information or access to systems and/or services. In today's world, social engineering attacks are one of the most commonly executed attacks as it is often times easier to manipulate a user into giving information than it is to exploit security technology. There are many kinds of social engineering attacks: pre-text calling, on-site human interaction, spear-phishing emails, as well as USB drops.

Social Engineering assessments can benefit an organization in a significant number of ways. Considering these attacks are extremely common and can actually be performed without any interaction with employees, attackers can simply craft a fake email and send it to as many users as they want. In recent studies, social engineering attacks have proved to be the source of many security breaches around the nation.

By performing a social engineering assessment, your organization can gain an understanding of the following:

- Effectiveness of user awareness training program
- Technical security controls that prevent attacks from occurring
- Potential impact of a successful social engineering attack
- Types of malicious activities performed as part of a social engineering attack

Vonahi Security offers a variety of social engineering assessments to test the effectiveness of your organization's user awareness training and security policies. By performing these assessments, your organization can understand and prepare for a real-world social engineering attack if ever targeted. Vonahi Security offers four types of social engineering assessments.

SPEAR-PHISHING

We can perform targeted research on your employees and craft custom phishing scenarios tailored specifically to the users targeted during the engagement.

ON-SITE ENGAGEMENTS

Our consultants can arrive at your physical facility and attempt to manipulate your employees into allowing us unauthorized access into sensitive areas within the facility.

PRE-TEXT CALLING

After researching information about your organization, we can perform pre-text calling and impersonate trusted management staff to elevate trust between the consultant and employees.

USB DROPS

Configuring USB devices with executable malware, we are able to deploy a number of USB devices around your physical location to assess whether or not users will plug them in to their systems.

Our Social Engineering Testing Activities

Based on our professional experience, research, and the activities performed by modern-day attackers, Vonahi Security consultants perform a variety of activities that combines both traditional and new attack techniques to attempt manipulating employees into providing us sensitive and/or valuable information about the internal infrastructure.

OPEN SOURCE INTELLIGENCE

Using Open Source Intelligence (OSINT), our consultants identify potential targets for the social engineering attacks. In many cases, management staff is targeted during this discovery phase. Impersonation of management staff, in some cases, helps expedite trust between the consultant and end-user.

TARGETED EMPLOYEE RESEARCH

Depending on the assessment, our consultants will perform targeted research against employees of interest. This allows for a more tailored social engineering attack, which would increase the chances of successfully gaining the user's trust and obtaining sensitive and/or valuable information.

CREDENTIAL HARVESTING

In some cases, credential harvesting is performed during our social engineering attacks. By obtaining credentials, it may be possible to gain access to resources within the environment or even the user's email inbox.

PERFORM EXPLOITATION

Exploitation may be performed as part of the social engineering assessment. Exploitation demonstrates that it is possible to gain an initial foothold into the environment or system due to an employee demonstrating the lack of user awareness.

POST-EXPLOITATION

Once our consultants gain access into the environment, we will attempt to gain unauthorized access to sensitive information and/or systems within the environment.

EVIDENCE-BASED REPORTING

Documentation is collected along the entire process to ensure your organization understands how, when, and why our attacks executed within your environment. These reports will also demonstrate the attacks through screenshots and a variety of supporting evidence.

What You Get

At Vonahi Security, we understand the demands and expectations for quality information security services. As part of our social engineering services, your organization can expect the following:

- **Project Management & Planning**
- **Daily Status / Progress Reports**
- **Quality Deliverables & Presentations**
- **Experienced & Certified Security Experts**

VONAHI SECURITY

ABOUT US

Vonahi Security is a cybersecurity consulting firm that offers comprehensive information security services. Our team is comprised of security experts experienced in offensive and defensive operations, allowing us to provide quality information security services. We ensure your organization is successful with achieving its security goals and remaining one step ahead of malicious adversaries.

HELLO WORLD. MEET MODERN SECURITY.

www.vonahi.io

info@vonahi.io

1.844.VONASEC (866-2732)

@vonahisec