BREACH SIMULATION

DATA SHEET

What is a Breach Simulation?

A breach simulation is a demonstration of the activities that are performed by an attacker once a compromise is successful. Similar to the activities of a penetration test, a breach simulation starts where a penetration test ends. However, a breach simulation focuses on testing the organization's policies, procedures, and technical controls that are implemented to protect against such an incident. Unlike a traditional penetration test that focuses on identifying security vulnerabilities and gaining access to sensitive data, a breach simulation includes more interaction with your network staff to help increase awareness, knowledge, and understanding about the activities and implemented controls.

A breach simulation can help an organization understand what controls and procedures are lacking within the environment, including incident response and detection procedures, monitoring, alerting, and logging, and even host- and network-based intrusion detection and prevention.

Some of the benefits of a breach simulation include the following:

> Understanding the activities of malicious attackers post-compromise

> Opportunity to test technical security controls for deficiencies

> Demonstration of potential impact of a successful compromise

> Improvement of overall security posture

Vonahi Security breach simulation service includes several activities that provide value to your organization's information security program. These activities, combined with professional recommendations, allow your organization to improve its overall security posture.

SIMULATE AN ATTACKER'S ACTIVITIES

We simulate an attacker's activities, including traditional and modern day attacking techniques. Our consultants will attempt to perform zero-day attacks (if possible), simulate malware, and authentication-based attacks that target users and services.

ACTIVITY LOGGING

We log all of our activities during a breach simulation so that your network security team can correlate our activities with monitoring and alerting controls implemented within your organization. We help ensure your detection and response procedures are quick and accurate.

ASSESS YOUR CONTROLS

Our activities will assess your controls to identify security weaknesses and areas of improvement. Detecting a breach and tracking it down requires a quick and efficient process, and our consultants will help your organization improve these processes.

Our Breach Simulation Methodology

Based on our professional experience, research, and the activities performed by modern-day attackers, Vonahi Security consultants follow a breach simulation methodology that combines both traditional and new attack techniques to provide quality services.

EGRESS FILTERING TESTING
One of the methods that attackers use to gain persistent access into your environment is by leveraging the ability to connect to remote servers. We test your egress filtering controls to ensure that access to services and ports to the Internet are restricted to business needs.

AUTHENTICATION ATTACKS
We perform a variety of authentication attacks against your user accounts as well as service accounts within the environments. These activities allow your organization to set up monitoring and alerting in specific areas that may be targeted by malicious attackers.

SIMULATED MALWARE
We introduce controlled malware within the environment to allow your network security staff to understand the characteristics of malware.

PRIVILEGE ESCALATION & LATERAL MOVEMENT
To elevate our access into your environment, we perform a variety of privilege escalation attacks and lateral movement within your environment. These activities help your staff understand common paths that attackers take, allowing for better monitoring and alerting based on certain events.

DATA EXFILTRATION
Your critical data leaving your environment is a critical security concern if it's not through an approved channel (e.g. email, etc.). We attempt to exfiltrate sample pieces of sensitive information to unapproved destinations, such as our remote servers.

REPORTING
Our detailed deliverables will allow your network staff to cross reference our activities with monitoring and alerting controls.

What You Get

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

Project Management & Planning

Daily Status / Progress Reports

Detailed Activity Reports with Timestamps

Experienced & Certified Security Experts

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