PHYSICAL SECURITY

DATA SHEET

What is a Physical Security Assessment / Penetration Test?

A physical penetration test is essentially an assessment of your organization's physical security controls. The purpose of this assessment is to identify weaknesses in the physical environment that could result in unauthorized access into sensitive areas within the facility. Such weaknesses could include unlocked doors that lead to network closets or server rooms, unmonitored elevators that provide access to the office, lack of security cameras, and more. A physical security assessment can also help organizations evaluate their employees' awareness of unauthorized visitors. Our consultants can attempt to manipulate employees into allowing access.

Although many attackers will target organizations by exploiting security weaknesses within the technical environment, the physical environment must be just as equally protected. A physical environment that lacks strong security controls can pose a significant threat to sensitive data since it may be possible to gain unauthorized access and plug in a rogue device into the internal production environment. Through a rogue device, an attackers could establish persistent, back-door access into the network environment.

Our assessment can help organizations improve the following physical security access controls:

- Increased user awareness and visitor tracking
- Improve/Implement formal escorting procedures
- Monitoring and alerting for unauthorized physical entry
- Network Access Controls

Our physical penetration test includes heavy reconnaissance and planning to ensure our consultants can simulate a scenario realistic to a malicious attacker. Some of the activities that we perform during testing include the following:

SIMULATE ATTACKER'S ACTIVITIES

Our consultants will simulate a malicious entity attempting to gain physical access into your facility. Once access is established, our consultants will attempt to plug in a rogue device with the intention of introducing a back-door into the environment.

IDENTIFY PHYSICAL SECURITY WEAKNESSES

While performing the physical security assessment, our consultants will note down any security flaws identified and controls that were bypassed for later discussion and review with network security staff.

EVALUATE USER AWARENESS

Our consultants will also evaluate the awareness of employees during the physical penetration test by attempting to blend in with employees without authorization. We equip fake IDs, uniforms, and any necessary disguise to appear legitimate.

Our Physical Penetration Testing Methodology

Based on our professional experience, research, and information published by security researchers, Vonahi Security consultants follow a physical penetration testing methodology that combines both traditional and new attack techniques to provide quality physical penetration testing services.

RECONNAISSANCE

Information about your physical facility is gathered to map out the entry/exit points, parking spaces, employee hang-out areas, and areas that may be possible for an attack. Our consultants may spend a few hours observing the pattern of your employees.

THREAT MODELING

An assessment of the organization's business is performed to identify areas that may be of value to an attacker. For example, after discovering that this location houses the IT department, our consultants will target the IT department and network/server closets.

VULNERABILITY ANALYSIS

Once enough data is gathered, our consultants will determine which method of attack should be executed. Our consultants will create fake badges on the fly and gather additional gear for disguise.

PERFORM EXPLOITATION

After cloning fake badges and additional necessary steps to disguise the consultant, an entry attempt will be made into the facility, which may also involve tailgating employees into employee-only areas.

POST-EXPLOITATION

If access is successfully gained into the facility and in an employee-only area, our consultant will attempt to plug into the network environment and continue with a small penetration test of the internal environment.

TIMELY REPORTING

During testing, our consultants will note down flaws that were observed during testing, including the lack of awareness by employees within the facility.

What You Get

At Vonahi Security, we understand the demands and expectations for quality information security services. As part of our physical penetration testing 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