CLEARNETWORK

Security Assessment and Penetration Test Services

We offer ten ways to test and assess security success.

1. Internal and External Vulnerability Testing

Also known as security assessment scanning, this type of testing identifies systems and network configurations that could expose the customer to a breach of the network and critical systems. Systems are scanned for improper configurations; missing security software patches; unnecessary services and protocols; and vulnerabilities related to clear text protocols, coding and/or applications. Then recommendations to securing the environment are provided.

2. Internal and External Penetration Testing

This testing protocol validates the risks associated with internal and external vulnerabilities exposed during security assessment scanning. By exploiting discovered vulnerabilities, we can demonstrate the potential outcome of a hacker attack. We attempt to achieve domain administrator status, uncovering unprotected databases and applications, improperly structured privileges, data leakage issues, rogue and hostile applications, improperly patched systems, missing and poor passwords, unprotected network devices and more. After our penetration testing is complete, we make appropriate recommendations to further secure the environment.

3. Telecom and Phone Service Penetration Testing (aka: War Dial)

This testing consists of dialing a range of phone numbers that belong to the customer. Each phone number is dialed and then monitored for a response.

Responding phone numbers that are connected to computer modems and network equipment are documented; a limited exploit is used to determine whether the phone numbers in question belong to the customer, and whether they pose any vulnerability.

For customers who have deployed Voice over Internet Protocol Systems (VoIP), this assessment involves identification of the specific VoIP hardware chosen and evaluates it for known security issues. This evaluation will confirm that the proper security settings have been chosen. Using a variety of assessment tools, the employment and functionality in the live environment will be confirmed. Testing of encryption will be accomplished by attempting to intercept audible VoIP packets. Lastly, all the VoIP hardware will be scanned during the normal security analysis of all devices on the network. Suggestions to mitigate exposed risks will be included in our report.

Security Assessment and Penetration Test Services
(Continued)

4. Wireless Security Penetration Testing (aka: War Driving)

This assessment involves physically scanning the perimeter of a facility using a wireless scanner. The wireless scanner probes the general vicinity for any emitted Wireless Access Point (WAP) signals that are in the area. Each responding signal is documented for ownership, whether or not it is a known corporate resource, and whether or not it is secured with encryption.

Testing begins within the vicinity of wireless signal(s). Using a commercial laptop outfitted with a special wireless antenna, signals are then collected and identified for ownership. Signals identified as the wireless system belonging to the customer are then targeted for penetration. The attempt to penetrate begins with initiating a request and response from the WAP. As users connect to the device, encrypted packets of information are captured. Depending on the encryption technology securing the wireless network, the number of packets being collected will vary. The packets collected are then examined with an attempt to decrypt them. If successful, the decrypted packets should provide the information needed to connect to the wireless network.

This service also identifies mobile devices connected to the 8-2.11 wireless and their exposure to an unsecured environment.

5. Wireless Security Architecture Review

This review examines the security aspects of the wireless topology and design—with the goal of determining the best possible security posture. Wireless components such as controllers, access points, client workstations and mobile device settings are reviewed to ensure proper security measures have been implemented. And wireless technology is reviewed for best use of security features and capabilities. Recommendations for securing the environment—and applying new technologies and capabilities to enhance security—are documented and included.

6. Firewall Configuration Review

In this review, we will evaluate the configuration and firewall policy with the goal of providing suggestions and best practices. This service examines considerations such as security concerns based on improper configuration and management, issues relating to the hosts the firewall is protecting, and issues relating to the services those hosts must offer through the firewall. Firewall review findings will be documented to include recommendations.

Security Assessment and Penetration Test Services
(Continued)

7. Network Security Appliance Configuration Review

This review examines the security features and settings of the customers' intrusion detection systems, intrusion protection systems, unified threat management and next generation security appliances for optimal security configurations. Components reviewed include the firewall rule set, threat policy configuration and protection settings, and antivirus/malware configuration and protection settings. Findings will be documented and will include recommendations.

8. Internal and External Vulnerability Testing

This testing determines if unauthorized access to applications data, and/or network can be achieved. The scope of the project can vary greatly, depending upon the desired level of information.

Web applications are probed, and testing identifies vulnerabilities such as coding flaws, buffer overflows, cross site scripting, SQL injection, broken access control and authentication, improper error handling, insecure storage and insecure configuration management. Recommendations for securing the environment are provided.

9. Network Security Architecture Examination

This protocol inspects the topology of customer-deployed security devices within their network. Devices such as firewalls, security appliances, routers, switches and VPN aggregators are examined for proper placement, utilization and network security hardness. Recommendations are provided on how to expand the security posture of the present infrastructure.

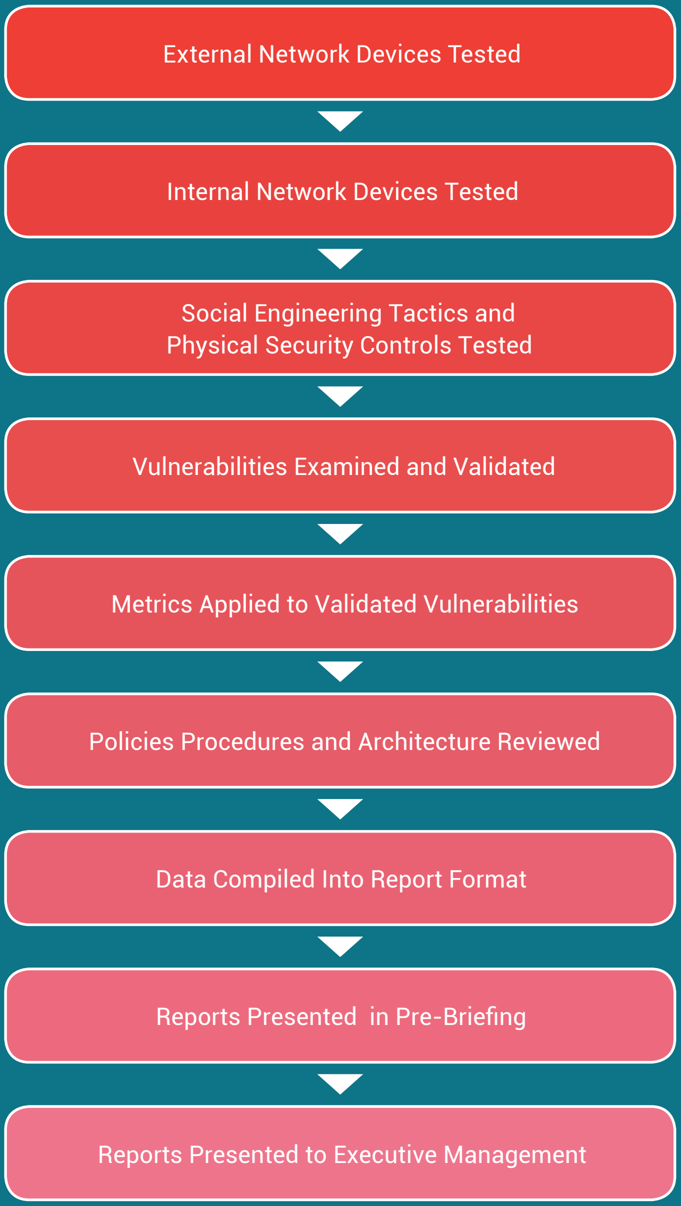
10. Social Engineering

Social engineering is a process in which access is gained to a network via people, process and technology—often using physical means. Companies may be exposed to potential social engineering threats daily—in the form of individuals posing as copier repair technicians, auditors from consulting firms, new employees, heating and ventilation technicians, food delivery personnel and more. Other avenues for attack include infected hardware or email phishing. We demonstrate these dangers and deliver recommendations to decrease overall risks.

Project Timeline

The time for completion of each project is dependent on the following criteria: the services purchased by the end user, the size of the network being tested, and the level of depth the testing will undergo (i.e., Security Vulnerability Assessment vs. Complete Penetration Test).

Delivered findings will include a metric of high, medium and low risk. We explain the exposure of the vulnerability and make recommendations for the remediation of the problem.



External Network Devices Tested

Internal Network Devices Tested

Social Engineering Tactics and Physical Security Controls Tested

Vulnerabilities Examined and Validated

Metrics Applied to Validated Vulnerabilities

Policies Procedures and Architecture Reviewed

Data Compiled Into Report Format

Reports Presented in Pre-Briefing

Reports Presented to Executive Management

A Variety of Reporting Formats

Reports can be broken down into a variety of formats. An executive-level report provides a high level of the findings, while data reports can be highly detailed, explaining the findings with significant granularity. Whatever decision makers are involved, we provide relevant reports that make it possible to take action and achieve more secure environments.