SERVICE DESCRIPTION

Segmentation Test/Discovery Scan

Service Scope

The Segmentation Test/Discovery Scan service is designed to provide an inventory of accessible services from a particular point of origin within an internal or external network. Utilizing reconnaissance techniques common to network penetration tests and vulnerability scans, the Segmentation Test/Discovery Scan results in an inventory of hosts and services that can be connected to from the chosen origin (either external Internet or from a device connected to a private internal network). In addition to network reconnaissance, the service includes vulnerability analysis of separation devices/network infrastructure and identifies vulnerabilities within such systems, which could affect the profile of accessible hosts and services.

Description

The Segmentation Test/Discovery Scan is designed to satisfy PCI DSS requirement 11.3.4, the requirement to perform segmentation checks during a penetration test for 11.3. It can be also be used for generalized asset discovery/inventorying of network connected devices. Utilizing techniques common to vulnerability scanning and the reconnaissance phase of network penetration testing, this service profiles the landscape of accessible systems and services from a given point of origin. The test can be performed from an external Internet origin, but is more commonly associated with tests performed from internal private networks.

Key Benefits:

- Utilizes network interrogation techniques to provide a proven list of devices and services, which are accessible from the testing point of origin.
- Eliminates any doubt associated with network ingress/egress filtering policies by demonstrating accessibility to services through experimental results from live network traffic.
- Identifies vulnerabilities within network infrastructure/separation devices that could allow a malicious party to modify network segmentation rules and gain access to additional systems and services.

The testing involves the following test categories.

Layer 2 Attacks (internal test origin only)

- VLAN hopping
- ARP cache poisoning
- Insufficient segmentation and access control

- Exploitation of weaknesses within the switched architecture related to trunking, STP, or failover protocols

Layer 3 Tests

- Port/protocol scanning of target infrastructure from the chosen testing origin
- Service identification probes

Trustwave will perform the Segmentation Test/Discovery Scan service at the locations identified by Client to Trustwave.

If the remote testing option is chosen, the appliance must be returned within five business days of completion of the test. If the appliance is not returned within that time, Client will incur a charge of $5,000.00 for the appliance.

Remote Testing Option

Client may choose to have the Segmentation Test/Discovery Scan testing performed remotely. The consultant will work with Client to ship one of Trustwave's Secure Remote Internal Penetration Testing Appliances to facilitate the remote access needed to conduct the Segmentation Test/Discovery Scan. Most commonly, a virtualized software version of the appliance will be used. Most of the following applies to the physical hardware appliance.

The consultant will first arrange a call to discuss the test parameters and gather all the needed technical information required to configure the appliance. The consultant will then fully configure the appliance and ship it to Client. At this point, Client will simply connect power and the primary interface to the data network. In case of any problems, the consultant can utilize a remote Cisco WebEx conference to facilitate remote access for the consultant to troubleshoot and fix the problem.

The appliance makes a secured, encrypted outbound connection from Client's network to a physically secured and hardened control station located at the Trustwave Security Operations Center (SOC). The Trustwave consultant will be able to access the appliance and conduct testing.

After testing is completed, there may be offsite data analysis. The final report will then be presented to for Client's review. The consultant will also securely destroy any data on the appliance and ask that Client ship it back to Trustwave within five (5) business days. Within five (5) business days after the date of termination or discontinuance of this Agreement for any reason, Client agrees to return, at its sole expense without setoff to any fees owed, the appliance to TRUSTWAVE. Client shall retain the risk of loss until such appliance is delivered to TRUSTWAVE's premises. Client shall be solely responsible for, and shall reimburse TRUSTWAVE for, any damage caused to the appliance while at Client's facilities, except to the extent such damage is caused by TRUSTWAVE personnel. If the appliance is not returned within five (5) days or is not in the same condition in which received by Client (except for normal wear and tear), Client agrees to pay a damage fee of $5,000 per appliance. Client shall pay all insurance, shipping, and handling charges, including without limitation, custom charges, taxes, and VAT.

About the Internal Penetration Test Appliance

The Internal Penetration Test Appliance is a secure appliance-based server meant to facilitate the type of remote access required to perform a proper Segmentation Test/Discovery Scan.

Functionally, the appliance is significantly better than a VPN connection to Client's internal network as with a VPN much of the actual attack surface of the network cannot be seen by the consultant. In this way, very severe, very high-risk issues can be missed. Because of these shortcomings with VPN access, Trustwave cannot perform a Segmentation Test/Discovery Scan remotely over a VPN.

The appliance however is a secured, hardened, appliance platform that will be shipped to Client fully configured by the penetration test consultant. Once the appliance is connected the Client network, it will initiate a secure encrypted outbound connection to Trustwave’s control server granting remote access to the penetration test consultant.

Most sites that allow basic outbound services such as HTTP/HTTPS will not require any sort of firewall or infrastructure changes to accommodate the appliance.