SERVICE DESCRIPTION

SpiderLabs Wireless Penetration Test

Service Scope

The Trustwave SpiderLabs Wireless Penetration Test methodology results in a thorough test of the entire target environment and provides a detailed deliverable with both tactical and strategic recommendations to improve the security posture of the target environment. These recommendations are both actionable and advisory in nature and are presented to the customer.

The primary objective is to gauge the resilience of the Wireless Networks to various classes of attacks launched from both the radio side as well as the wired side. The assessment will determine the nature and extent of what further attacks could be leveraged against internal wired resources should a malicious individual gain unauthorized access to the wireless network.

The Wireless Penetration Test involves a number of separate phases including site surveys; network reconnaissance, wireless infrastructure device security testing; attempts to bypass Wireless Intrusion Prevention Systems (WIPS); as well as exploitation of identified vulnerabilities to provide a complete security assessment of the wireless environment.

The wireless penetration test can be performed as either a covert, or a collaborative exercise depending on the Client driven requirements and objectives of the assessment. The testing approach can be discussed with your consultant prior to test execution to leverage the maximum value to your organization from this exercise.

Scope and Project Phases

This security test actively validates the adherence to security policy and lists specific remediation items for each problem identified. The test is typically conducted in the following manner but is tailored to specific requirements.

Site Survey

To begin any test Trustwave SpiderLabs obtains the Site Service Identifier (SSID) information for all locations to be tested from the authorized Client point of contact (usually both the Extended Site Service Identifier (ESSID) and Basic Site Service Identifier (BSSID). Utilizing wireless scanning and global positioning (GPS) equipment, Trustwave will an attempt to identify the wireless network from an external location (usually a street, nearby public place, or parking lot). Trustwave SpiderLabs then performs a discrete site walkthrough using handheld equipment. The data from both of these activities is analyzed and compared. Signal strength calculations are made, and this information is used to calibrate equipment to acquire the strongest signal from the farthest, most

discrete location. The end result of the site survey is a site external signal strength profile (a geographic plot on a map of the area from which one could reasonably acquire signal to maintain a 1Mbps connection to the wireless network), and a location risk rating (based on the distance from which one could maintain a 1Mbps connection to the wireless network).

Network Reconnaissance

During this portion of testing Trustwave attempts to ascertain all of the security features present in the wireless network. These security features fall into four basic categories:

- Basic Security Features – basic security features include MAC address-based access control, broadcasting/non-broadcasting ESSID in beacons, and presence of Wireless Intrusion Detection / Intrusion Prevention systems
- Transport Layer Encryption – transport layer encryption can take many forms the most common being WEP, WPA, or WPA2, however VPN (IPSEC or PPTP), or SSL/TLS based systems may be used above the transport layer.
- Authentication – if the authentication type is not OPEN (i.e. no authentication); authentication may include one or more of Pre-Shared Key (PSK), Managed (Radius Based), 802.11x (EAP, LEAP, PEAP), IKE, or HTTPS.
- Access Controls – access control restrictions can take the form of firewall rules, access lists, or some other access restriction. Sometimes access controls on a network are apparent and can be enumerated in this phase.

Wireless Network Infrastructure Testing

Once all equipment has been calibrated, locations have been mapped, and Trustwave has insight into the nature of a site configuration (site security features), an attempt is made to penetrate the wireless network. The primary goal of this phase is to derive enough information utilizing various wireless attack techniques to associate and authenticate to the network. The exact techniques used will be entirely dependent on the site security profile. Trustwave will work with you and your team to detail the specific attack methodology used for each site tested. This phase is carefully coordinated with to minimize the potential of any unintended business impact.

Wireless networks normally provide a connection into a traditional corporate network and Trustwave SpiderLabs will evaluate any security risks that may result from the topology or configuration thereof. In the cases where the corporate wired LAN is protected from the WAP by access control devices (e.g. firewalls and routers) attempts will be made to exploit trust relationships to bypass these controls. For instance, Trustwave may make use of an open proxy server to mask the real IP address of the attacking machine, or may leverage a compromise of a trusted system on the wireless network to perpetrate attacks against the otherwise protected network. In some situations where wireless network access is protected via passwords on the base station, brute-force password attacks may be performed, if specifically requested.

Network Reconnaissance

If Wireless Network Infrastructure Testing is successful, Trustwave will attempt to map out the rest of the wired network once connected to a site AP. Where specifically requested, Trustwave SpiderLabs will continue the security testing from the wired side network. Port scanning, system and service fingerprinting, and network mapping techniques are utilized to build a system and network profile, and a complete target list is compiled from all the information gathered during the phase. If present, interrogation of organizational Domain Name System (DNS) servers is completed, and then the DNS servers themselves are probed for configuration related issues.

Vulnerability Identification

Each host and all associated listening service to be targeted for the test is probed, singularly and in tandem with the other hosts to locate potential vulnerabilities. Using a large working knowledge of exploit techniques, public information, and results of private vulnerability research, the Trustwave consultants catalog all the potential attack vectors.

Vulnerability Exploitation

If the plan of attack devised in the previous step includes any techniques that may impact production systems and infrastructure, for example when purpose-built exploits or potentially risky exploit code is required to exploit a system, permission in writing is first sought from an authorized Client point of contact

As a rule, any potential vulnerability found is manually investigated, researched, and an attempt is made to exploit. In exploiting vulnerability, Trustwave SpiderLabs will make an attempt to either gain unauthorized access to the target system, or extract sensitive data from it. An exploit is considered successful if it was possible to achieve either of these objectives. Where successful such compromises will be reported to the authorized Client point of contact.

Deliverables

Following the conclusion of the engagement, findings will be made available via the Trustwave SpiderLabs TrustKeeper Portal. The deliverables will be both strategic and tactical in nature, presented in a drill down format that will be highly accessible to both management and operational staff. Each finding will have a risk scoring associated with it as well as contain detailed technical information pertaining to the nature of the finding. Each finding will also be presented with clear guidance on how to remediate the issue.