

SERVICE DESCRIPTION

SpiderLabs Internal Network Penetration Test

Service Scope

The Trustwave SpiderLabs Network Penetration Test service results in an in-depth 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 core ideal of the test is to methodically and iteratively test the target environment from the most general components to the most specific. In a large complex corporate environment, this is from the external network blocks presented to Trustwave at the beginning of the engagement down to the specific security controls utilized by external facing applications, as well as the effectiveness of ingress filtering, antivirus and other perimeter security systems.

The overarching philosophy of the engagement is to resemble expert adversaries utilizing intelligent attack techniques against systems, Clients, and networks. As such the entire testing process is primarily manual in nature to limit generic results, which would otherwise be returned by automated scanners or checklist methods used in more general vulnerability assessment.

The objective of the internal network penetration test is to determine the resiliency of the internal corporate network against users who:

- Gain logical access to the internal corporate network via the Internet (i.e. an external compromise)
- Are legitimate users of internal corporate resources with malicious intent (i.e. rogue employee)
- Compromised a legitimate employee's workstation (i.e. through a virus, Trojan or targeted attack)
- Gain unauthorized physical connectivity to the internal corporate network environment

The deliverable for this service is a report that documents the organization's existing security posture, identifies specific weaknesses and vulnerabilities, and provides purpose-built exploit code examples that tell a compelling story of risk associated with each vulnerability, and ultimately recommendations for their remediation.

The following illustrates some of the different vulnerability classes Trustwave covers during an external network penetration test. This list is not intended to be exhaustive and the actual testing performed depends on the specifics of the organization being tested.

Layer 2 Attacks

- 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 Attacks

- IP redirection
- Session hijacking
- Session replay
- Password capture

Network / Operating System Layer Attacks

- Network hash passing
- Exploitation of DHCP weaknesses
- Microsoft, Novell, Unix weaknesses

Logical Attacks

- Abuse of functionality

Cryptography

- Algorithm
- Key management

Data Protection

- Transport
- Storage

Buffer Overflow

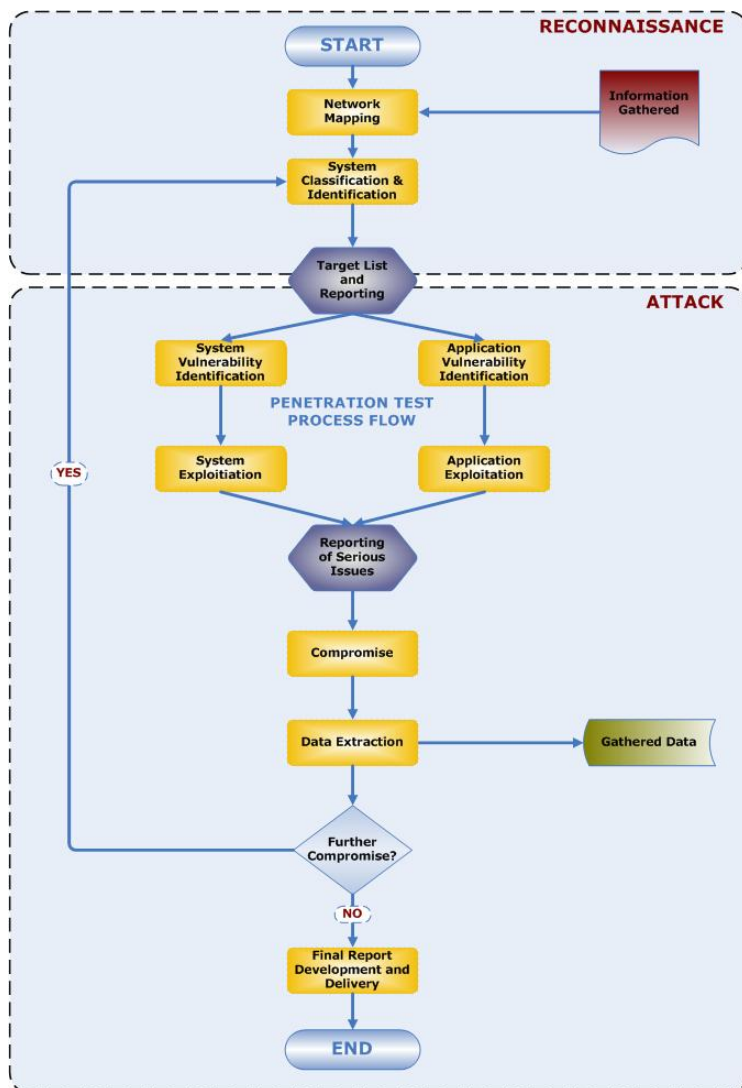
- Stack-based
- Heap-based
- Format string

Protocol Fuzzing

Scope and Project Phases

All testing phases will be carefully coordinated to minimize the potential for any unintended impact. Trustwave recommends full-disclosure of the testing to all individuals responsible for the network environment and related services and devices. Trustwave takes a number of precautions to minimize the potential of causing service interruption or unscheduled downtime, however Trustwave does not guarantee against service interruption or unscheduled downtime due to the inherent risk of conducting such testing. Trustwave recommends that incident response procedures be well defined in the event that any adverse impact or disruption of network services should occur. Trustwave is not responsible for ensuring adequate back-ups and/or other protections against data loss, damage or destruction are in place, either prior to or during any phase of the proposed services.

To visually depict our methodology for penetration testing, we have provided a process flow diagram followed by a narrative of each step.



Network Mapping

In the process of moving from general to specific, building an accurate network map of the externally facing devices is a critical task at the beginning of the penetration test.

Trustwave SpiderLabs will obtain the internal IP address space passively through manual investigation and traffic captures performed on the internal network. Findings such as network broadcasting, dynamic routing updates, CDP messages, SNMP polling and the like can provide much information about the network topology. Later, more active techniques are utilized such as layer 2 (ARP) pings of the local net, up to and including port scanning of more remote internal segments. At the end of this phase, Trustwave will build a comprehensive logical map of the internal network environment.

System Identification & Classification

TCP finger printing, service fingerprinting, and various methods to identify and classify systems and services are utilized to more completely understand the environment in question. The data gathered is used to classify the systems by function. Data gathered about the system helps to determine the nature and business purpose of each system. After each system is classified the network map is updated to reflect each system's functionality and operating system. Before the next testing phase begins, Trustwave SpiderLabs will provide an update on material findings thus far, as well as request confirmation of the intended target list to be used in subsequent phases.

Network & Systems Tests

System Vulnerability Identification

Each in scope host and all associated listening services are probed to locate potential vulnerabilities. Using a large working knowledge of exploit techniques, public information, and extensive private vulnerability research, the Trustwave SpiderLabs consultants catalog all the potential attack vectors that may be exploitable. Trustwave SpiderLabs consultants will then devise several attack strategies as planning step prior to the subsequent phases.

System 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.

Web Application Layer Test Cases (pre-authentication only)

Application Architecture Identification

Trustwave SpiderLabs will map specific applications running within the target test environment. When an application server is identified, other related systems will be identified within an application server group. This

grouping will help identify potential flaws in application trust relationships. This information is vital to the successful identification of application vulnerabilities. In addition to identifying applications, Trustwave SpiderLabs will attempt to discover Trojans and Backdoors that may be present in the environment.

Application Exploitation

Each application layer component will be targeted using a subset of application penetration testing techniques. These tests are not considered to constitute a full application penetration test as they only address the pre-authentication components of an application for the following classes of issues:

- Input Validation
- Buffer Overflow
- Cross-Site Scripting
- URL Manipulation
- SQL Injection
- Hidden Variable Manipulation
- Cookie Modification

System Compromise

As systems are compromised, key security contacts will be notified. When purpose-built exploits or potentially risky exploit code is required to exploit a system, the authorized point of contact(s) are given the opportunity to decide if the particular system should undergo additional tests. Upon granting such permission Trustwave SpiderLabs will utilize additional techniques to further penetrate the target system and the environment as a whole. This can include password cracking tools, network sniffers, remote management tools, etc. Successful execution establishes a new vantage point (pivot point) for additional attacks against the environment.

Data Extraction

Each system that is compromised will be examined for the existence of critical, sensitive or confidential data and files. If Trustwave SpiderLabs finds such data to be accessible, a sample of this data will be downloaded from the system and securely stored by Trustwave SpiderLabs for evidential purposes until the presentation of deliverables.

Further Compromise

Once a system has been compromised, there are many trust relationships that can be potentially exploited, or data exposed through a compromise might lead to the compromise of additional systems and applications. Taking an iterative approach to this methodology, Trustwave SpiderLabs will launch a new stage of discovery against the environment. For example, if a web server is compromised, that system may provide access to a system on the internal network that would otherwise not have been directly accessible.

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.