SpiderLabs Penetration Testing

Service Scope

Trustwave's SpiderLabs is an industry leader in a variety of Penetration Testing Services. The organization is globally CREST certified, supports engagements with a number of certified staff, and is constantly supporting the security community with CVE's cutting edge research, and industry leading thought leadership.

Examples include:

2009 - First Trustwave Global Security Report published.
2010 - ModSecurity released an open-source web application firewall (WAF) powered by SpiderLabs.
2011 - SpiderLabs staff had 16 presenters at Defcon, giving 11 presentations, Jboss Autpwn released.
2012 - Newly launched Trustwave PenTest Manager wins 2012 SC Media Europe Security Innovation award, Leading Penetration testing tool RESPONDER released.
2013 - Ploutus malware family identified targeting ATMs.
2014 - RESPONDER 2.0 released. First to identify and name the Backoff point-of-sale malware that infected 1,000+ businesses in North America.
2015 - CVE-2015-8562 Joomla zero day discovered.
2016 - Multiple vulnerabilities identified in zencart. Publication of report on Carbanak "Operation Grand Mars".
2017 - CVE-2017-5521: Bypassing Authentication on NETGEAR Routers published.
2018 - Released DoHC2 which through protocol abuse allows for undetected Command and Control/Data Exfiltration via a newer protocol. Released Social Mapper which speeds up OSINT via facial recognition.
2019 - Released Sheepl, a tool for creating realistic user behavior for testing within lab environments.
2020 - SpiderLabs introduces CrackQ.

We focus on replicating real-world scenarios organizations may face in the current landscape for all types of environments whether on premise, cloud based, or hybrid. These engagements help organizations identity weakness and vulnerabilities, whether they are exploitable or pose risk to an organization, and potential ramifications of the weaknesses in their in-scope environment.

Spider Labs offers a number of different types of tests organizations can leverage:

Types of Tests:

Network – Standard penetration methodology for networks that do not fall into managed security testing (MST). This includes a level of effort using industry best practices and methodologies. This test looks for vulnerabilities and exploitable and unexploitable weaknesses in a client's infrastructure, as well as potential outcomes based on a Client's environment. These are for Internal and External network penetration testing.

Application – Standard application penetration methodology for networks that do not fall into MST. This includes a Level of effort using industry best practices and methodologies. This test looks for vulnerabilities and exploitable and unexploitable weaknesses in a client's application, as well as potential outcomes based on a Client's environment.

Active Directory Review – This involves reviewing a Client's Active Directory structure and is based on number of users, trusts, and forests. Clients can use this to understand strengths and weaknesses in the Microsoft Active Directory structure.

Red Team – This is an adversary simulation exercise aimed at a Client's organization. This is offered in an assumed breach, remote, remote + physical, and custom scoped engagement model. This exercise tests an organization's people, processes and technology, simulating real world threat actors' tactics, techniques, and procedures (TTPs).

Purple Team – This is a cooperative exercise aimed at working with a Client's defensive team to fine tune a problem area of their enterprise. This offering is mapped to the Mitre attack framework. This exercise improves an organizations' people, processes and technology, simulating real world threat actors' tactics, techniques, and procedures (TTPs).

Wireless -This is a wireless security test and is delivered onsite. This is based on the number of SSIDs the Client would like to test. Once all equipment has been calibrated, locations have been mapped, and SpiderLabs has insight into the nature of a site configuration (i.e. site security features), an attempt is made to penetrate the wireless network.

Physical – This is delivered onsite. It is delivered in supervised and unsupervised models. The process begins by gaining an understanding of the primary physical security control objectives. Once SpiderLabs has gained this understanding, a review of the facility takes place, which includes: a site survey, identification and assessment of physical security controls weaknesses and failures, and a networked physical access control system review. A "get out of jail free card is required from the Client".

Phishing – Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Cloud - This is a cloud assessment which leverages the Client access as well as SpiderLab's methodologies to test the controls in the Client's cloud environment, their implementation, and success during an audit-based review of security controls. Currently these are for AZURE and AWS.

Hardware: Embedded/ATM/IOT. This is physically testing hardware devices including internet of things (IOT) devices, ATMs, and other physical devices. Typical engagements range from 2-4 consultant weeks depending on complexity required.

OSINT – This is a level of effort open source intelligence engagements leveraging internally developed SpiderLab's tools, third party tools, and open source tactics, techniques and procedures.

Remediation – 10 hours of custom Remediation consultation to go over the findings of your engagement with the tester as well as a remediation consultant at the Client's request for further understanding and scoping.

Virtualization Technology Assessments- Virtualization has recently become one of the most rapidly and widely deployed IT initiatives, used by small businesses, and large corporate or government departments alike. Virtualization can be performed across server and desktop environments. Common examples include VMware ESX, vSphere, Hyper-V, Citrix, Solaris Zones, HPUX Virtualization and AIX LPARs.

Trusted Advisor – This is for testing services management approvals to allow for purchase in groups of 10 hours.

1.1.1 Client Responsibilities

Client is responsible for agreeing to scope PRIOR to start of testing. Should scope change prior to the start of testing the client has two options.

1) Continue with the test based on the original scoping during the sales process.
2) Adding funds to complete the test based on the new scope (if needed).
3) Client is responsible for all setup, verification of in-scope systems, and granting permissions for all activities contracted by the Client.

1.1.2 Deliverables

Following the conclusion of the engagement, the testing outcome will be made available. The deliverables will be both strategic and tactical in nature, presented in a format that is highly accessible to both management and operational staff. Each finding will be presented with clear guidance on how to remediate the issue.