Service Brief

Trustwave SpiderLabs® Penetration Testing Services

Version 1.2
December 2019

Table of Contents

Trustwave SpiderLabs® Application Penetration Testing

Applications – The Front Door of Your Organization

Applications represent an easily accessible target which may be open to attackers located around the globe as well as from within your own organization. From handling critical business processes to brochure-ware, these applications can be the first choice for an attacker looking to deface sites, steal your data, or gain a persistent foothold in your environment.

Why Application Penetration Testing?

Developing an application is hard work. The task of automating a business process which reflects the nuances of your organization's varying workflows can be a daunting challenge even to the most experienced of developers who are focused on ensuring that the application not only functions correctly but also performs efficiently. Software testing is often performed to positively verify functionality before the application is deployed to its larger audience. However, software testing rarely looks for the potential abuses of business logic, authentication/authorization implementations or the risks associated with the application's underlying environment.

Benefit from an In-Depth, Yet Straightforward Approach

Trustwave SpiderLabs® has performed numerous mobile application penetration tests giving them a unique insight into the issues which continuously affect applications. As a starting point, a "gray box" approach is used in conjunction with a combination of manual and automated testing. This approach provides the SpiderLabs consultant with various pieces of information about your application prior to the test in order to evaluate the application as it would exist in production. While these conditions would be made available over longer durations of time to an attacker through, for example, self-registered users and subsequent use of the application, SpiderLabs will work to balance the inherent time limitations of the engagement to ensure that both a breadth and depth of testing is applied to your application over the duration of the Mobile Application Penetration Test.

Automated vs Manual Testing

Attackers will use combinations of automated and manual testing in order to exploit your application. SpiderLabs uses their expert knowledge of best-of-breed security software along with their own custom tooling to ensure a breadth of coverage across the application's surface. Automation, however, never replaces the impact which an experienced hacker will bring to bear on the technology, environment, or workflows which your application exposes. The application's purpose and functionality seen through the eyes of an experienced SpiderLabs consultant is often where the most interesting or peculiar vulnerabilities can be found. From abusing the business rules and security constraints of software, to the exfiltration of sensitive data stored within an application binary, the SpiderLabs consultant's goal is to search out and expose these weaknesses which are then clearly reported and presented to you for their subsequent remediation.

Trustwave SpiderLabs® – Proven Experience

Since 2005, Trustwave SpiderLabs has been building and refining methodologies to assess the security posture of applications built across the varying platforms and languages used in decades worth of development. These methodologies map to proven OWASP standards while also accommodating the discovery of issues particular to your web applications, web services, or thick client applications.

Staffed with ethical hackers having diverse and deep technical backgrounds, Trustwave SpiderLabs is prepared to uniquely apply their refined methodologies to your application to quickly understand its purpose, its underlying environment and its potential abuses. As developers, we understand the flaws inherent to development. As system administrators, we know the weak points in environments. As ethical hackers, we can find these vulnerabilities allowing you to address, remediate, and guard your organization's front door.

Ensuring Success

You built custom applications because your organization's work is unique. Similarly, SpiderLabs Application Penetration Testing is not applied in a one-size-fits-all solution. Instead, it is applied in a way that looks to discover meaningful vulnerabilities as they affect your application and organization. With years of experience, we know the common pitfalls to avoid. This allows for the most effective testing which aims to mitigate any negative outcomes a test could have on an application's environment. Additionally, Trustwave is available to retest vulnerabilities discovered in your penetration test to help you ensure the success of any required remediation steps. Our consultants are ready to work with you to provide guidance on issues frequently encountered during testing to customize an approach which ensures that your goals are achieved during your Application Penetration Testing engagement.

Trustwave SpiderLabs® Mobile Application Penetration Testing

Mobile Applications –Your Application in the Public Domain

Mobile applications represent easily accessible targets for attackers. Many of these applications can be acquired from app stores or simply from lost/stolen devices. Mobile applications, the data which they handle and the backend systems which they communicate with will end up out in the wild and in the crosshairs of hackers.

Why Mobile Application Penetration Testing?

Mobile application development is difficult and time consuming. The task of automating a business process which reflects the nuances of your organization's varying workflows can be a daunting challenge even to the most experienced of developers who are focused on ensuring that the application not only functions correctly but also performs efficiently on their given platforms. Software testing is often performed to positively verify functionality before the application is deployed to its larger and often public audience. However, this testing is rarely aimed at discovering the potential abuses of business logic, authentication/authorization implementations or the risks associated with the application's underlying device.

Benefit from an In-Depth, Yet Straightforward Approach

Trustwave SpiderLabs has performed numerous mobile application penetration tests giving them a unique insight into the issues which continuously affect applications. As a starting point, a "gray box" approach is used in conjunction with a combination of manual and automated testing. This approach provides the SpiderLabs consultant with various pieces of information about your application prior to the test in order to evaluate the application as it would exist in production. While these conditions would be made available over longer durations of time to an attacker through, for example, self-registered users and subsequent use of the application, SpiderLabs will work to balance the inherent time limitations of the engagement to ensure that both a breadth and depth of testing is applied to your application over the duration of the Mobile Application Penetration Test.

Automated vs Manual Testing

Attackers will use combinations of automated and manual testing in order to exploit your application. SpiderLabs uses their expert knowledge of best-of-breed security software along with their own custom tooling to ensure a breadth of coverage across the application's surface. Automation, however, never replaces the impact which an experienced hacker will bring to bear on the technology, environment, or workflows which your application exposes. The application's purpose and functionality seen through the eyes of an experienced SpiderLabs consultant is often where the most interesting or peculiar vulnerabilities can be found. From abusing the business rules and security constraints of software, to the exfiltration of sensitive data stored within an application binary, the SpiderLabs consultant's goal is to search out and expose these weaknesses which are then clearly reported and presented to you for their subsequent remediation.

Trustwave SpiderLabs® – Proven Experience

Since 2009, Trustwave's SpiderLabs has been building and refining methodologies to assess the security posture of mobile applications built across the Android and iOS platforms. These methodologies map to proven OWASP standards while also accommodating the discovery of issues particular to your application and their effect on the devices which run them.

Staffed with ethical hackers having diverse and deep technical backgrounds, SpiderLabs is prepared to uniquely apply their refined methodologies to your application to quickly understand its purpose, its underlying environment and its potential abuses. As developers, we understand the flaws inherent to development. As sysadmins, we know the weak points in environments. As ethical hackers, we can find these vulnerabilities allowing you to address, remediate, and guard your organization's front door.

Ensuring Success

Your application was built to meet a specific need. Similarly, SpiderLab's Mobile Application Penetration Testing is not applied in a one-size-fits-all solution. Instead, it is applied in a way that looks to discover meaningful vulnerabilities both in your application and the backend services they communicate in order to determine the effects an attack would have on your application, data, and organization. With years of experience, we know the common pitfalls to avoid. This allows for the most effective testing which aims to discover vulnerabilities while at the same time mitigating any negative outcomes a test could have on an application's environment. Additionally, Trustwave is available to retest vulnerabilities discovered in your penetration test to help you ensure the success of any required remediation steps. Our consultants are ready to work with you to provide guidance on issues frequently encountered during testing to customize an approach which ensures that your goals are achieved during your Mobile Application Penetration Testing engagement.

Trustwave SpiderLabs® External Network Penetration Testing

The Enterprise Network – The Nerve System of Your Organization

The network is one of your organization's most critical assets. It allows everyone in the enterprise to access tools they need to be successful. External penetration testing provides perspective on a network from an attacker's eyes. Insecure settings, weak passwords, misconfigurations and missed patches can be footholds for attackers to gain access to your network and your data.

Each year, Trustwave conducts over 4,000 penetration tests for client around the world. Through the principles of offensive security, security leaders are able to obtain assurance that their network is secure from direct attacks by determined individuals.

Why Network Penetration Testing

A network penetration test is very different from a vulnerability assessment. Vulnerability assessments focus on identifying all potential vulnerabilities typically through fingerprinting, regardless of their potential impact on a network. Penetration tests on the other hand focus on exploitable conditions that can be chained together to allow an attacker to further access into the target network. The process of aggregating all vulnerabilities detracts from the true focus of a real world attacker, who is only looking for a singular weakness which can be exploited to gain a foothold on the target network, and potentially leveraged further to find deeper vulnerabilities likely not reachable from the network perimeter. The ultimate goal is to obtain control over the target systems so that sensitive data can be discovered and exfiltrated.

Attack Phases

A penetration test consists of three primary phases:

- Network Reconnaissance
- Vulnerability Identification
- Vulnerability Exploitation

Network reconnaissance is the process of mapping out the target network to identify open ports and services, which comprise the attack surface. TCP and UDP port scans, protocol scans and other techniques are leveraged to create a picture of the target network.

Vulnerability identification utilizes a combination of automated and manual techniques to identify potential weak choke points in the network. The results from the network reconnaissance phase are leveraged to provide a focus for manual testing, examining areas which are most likely to have exploitable conditions first and foremost.

Vulnerability exploitation. For network penetration tests, vulnerabilities are only given a higher than informational risk rating if it is possible to demonstrate a proof-of-concept or leverage an actual exploit against the vulnerability. Vulnerabilities identified on the basis of version alone which cannot be actively demonstrated are not reported; these types of issues belong in vulnerability assessment reports. In this way, the findings presented represent a profile of the true risk to the network, and attention can be focused on addressing the primary issues.

Note that the process of reconnaissance, vulnerability identification and exploitation are cyclical. When a vulnerability is exploited it may lead to further potential for reconnaissance and vulnerability identification once a foothold is gained on a target system. Similarly, vulnerability identification may not be completed before exploitation occurs. In the real world, an attacker would not wait to complete a vulnerability assessment before exploiting a weakness as their true goal is only to gain access to the target systems. Therefore, SpiderLabs penetration tests mimic the same behavior in order to most closely simulate a real-world attack. The goal of the test is depth of penetration, as opposed to breadth of deviations from best security practices on the surface of the network. However, our managed penetration testing services also provide a validated vulnerability assessment, which can be used to provide a picture of all confirmable vulnerabilities affecting the external surface of the network. Trustwave recommends that penetration tests are complemented by validated vulnerability scans to gain a complete picture of the network's security profile.

Phishing Attacks

Our more advanced external penetration tests also provide a social engineering/phishing service. It is common these days for firewalls to filter access to almost all services which would otherwise be reachable. Likewise, Web Application Firewalls (WAF) and other security devices such as Intrusion Prevention Systems (IPS) may be effective in protecting web applications and other external services from attack. It is not uncommon for a network penetration test which focuses exclusively on direct network-based attacks against the target systems to fail to affect penetration. Human beings with legitimate access to the target systems are the often therefore the primary target of attacks nowadays. Our advanced penetration tests simulate a real-world phishing attack.

The network perimeter of the target organization is assessed through a process of Open Source Engineering, to identify potential systems which could be cloned so as to appear as a legitimate service provided by the target organization. A fictitious scenario is then constructed as a ruse to attempt to coax recipients of the email into clicking on an attacker-supplied link. The link refers to a cloned website controlled by SpiderLabs. Victims of the attack may be tricked into providing credentials to the web server, which provides credentials that can then be used to access legitimate services. Phishing attacks are an effective way of assessing the level of security awareness training within an organization and can be used to train employees to identify phishing attacks.

Trustwave SpiderLabs® Internal Network Penetration Testing

The Enterprise Network – The Nerve System of Your Organization

The network is one of your organization's most critical assets. It allows everyone in the enterprise to access tools they need to be successful. External penetration testing provides perspective on a network from an attacker's eyes. Insecure settings, weak passwords, misconfigurations and missed patches can be footholds for attackers to gain access to your network and your data.

Each year, Trustwave conducts over 4,000 penetration tests for client around the world. Through the principles of offensive security, security leaders are able to obtain assurance that their network is secure from direct attacks by determined individuals.

Why Internal Network Penetration Testing

An internal penetration test differs from an external penetration test in that the prerequisite of access to the internal network is supplied. External penetration tests occur from the public Internet, while internal network tests begin from a position of privileged access to an internal network segment. Most real-world compromises occur from within a network's perimeter as external perimeters are often well secured by firewalls.

Benefit from Our Comprehensive Approach

A network penetration test is very different from a vulnerability assessment. Vulnerability assessments focus on identifying all potential vulnerabilities typically through fingerprinting, regardless of their potential impact on a network. Penetration tests on the other hand focus on exploitable conditions that can be chained together to allow an attacker to further access into the target network. The process of aggregating all vulnerabilities detracts from the true focus of a real world attacker, who is only looking for a singular weakness which can be exploited to gain a foothold on the target network, and potentially leveraged further to find deeper vulnerabilities likely not reachable from the network perimeter. The ultimate goal is to obtain control over the target systems so that sensitive data can be discovered and exfiltrated.

Attack Phases

A penetration test consists of three primary phases:

- Network Reconnaissance
- Vulnerability Identification
- Vulnerability Exploitation

Network reconnaissance is the process of mapping out the target network to identify open ports and services, which comprise the attack surface. TCP and UDP port scans, protocol scans and other techniques are leveraged to create a picture of the target network.

Vulnerability identification utilizes a combination of automated and manual techniques to identify potential weak choke points in the network. The results from the network reconnaissance phase are leveraged to provide a focus for manual testing, examining areas which are most likely to have exploitable conditions first and foremost.

Vulnerability exploitation. For network penetration tests, vulnerabilities are only given a higher than informational risk rating if it is possible to demonstrate a proof-of-concept or leverage an actual exploit against the vulnerability. Vulnerabilities identified on the basis of version alone which cannot be actively demonstrated are not reported; these types of issues belong in vulnerability assessment reports. In this way, the findings presented represent a profile of the true risk to the network, and attention can be focused on addressing the primary issues.

Note that the process of reconnaissance, vulnerability identification and exploitation are cyclical. When a vulnerability is exploited it may lead to further potential for reconnaissance and vulnerability identification once a foothold is gained on a target system. Similarly, vulnerability identification may not be completed before exploitation occurs. In the real world, an attacker would not wait to complete a vulnerability assessment before exploiting a weakness as their true goal is only to gain access to the target systems. Therefore, SpiderLabs penetration tests mimic the same behavior in order to most closely simulate a real-world attack. The goal of the test is depth of penetration, as opposed to breadth of deviations from best security practices on the surface of the network. However, our managed penetration testing services also provide a validated vulnerability assessment, which can be used to provide a picture of all confirmable vulnerabilities affecting the external surface of the network. Trustwave recommends that penetration tests are complemented by validated vulnerability scans to gain a complete picture of the network's security profile.

Pivoting

It is not uncommon for direct attacks against the target networks during an internal penetration test to fail. There may be extensive filtering in place, preventing access to sensitive services within the target network. In certain cases, there may be no direct access to the targets whatsoever. The methodology employed during internal penetration tests mimics that used by real world attackers. Even in the most basic penetration test service, systems within the local network are assessed for vulnerabilities which could be leveraged to compromise them. Even though these systems do not constitute the targets, there may be more privileged access from a system resident within the local network through network segmentation devices such as switches, routers or firewalls. In this way, the process of reconnaissance, vulnerability identification and exploitation is repeated. If a system within the local network is compromised, attempts are made to pivot towards the targets with fresh port scans, vulnerability identification and exploitation phases. For our more advanced tests, any system which can be connected to from the testing origin network is in scope. These include systems not within the local network or the target network(s).

Network Data Manipulation

Direct attacks against local, non-target systems or target systems may fail due to sufficient patching and hardening. However, unlike external tests, internal penetration tests do not rely exclusively on being able to directly exploit vulnerabilities resident within accessible systems. It is not uncommon for data to be transiting the network which can be manipulated. An example is Address Resolution Protocol (ARP) poisoning, where traffic can be redirected from its intended destination towards the SpiderLabs attacking system. There may be sensitive data such as passwords or credential handshakes traversing the network. Live network traffic data can be captured and potentially attacked via off-line brute-force techniques to gain access to credentials which can be exploited without having to directly gain access to any patched system via a binary exploitation. There are numerous protocols which can be poisoned or manipulated to trick local systems into interacting with the attacker machine. In this way, an internal penetration test can detect vulnerabilities which extend beyond those which are permanently resident within accessible running services. A vulnerability scan would not detect any vulnerability that can be exploited by protocol manipulation, as doing so relies on observation of typical traffic traversing the network. Therefore, an internal penetration test is the only way of assessing the true security posture of a network.

Trustwave SpiderLabs® Active Directory Testing

Active Directory Review

Operation issues and technical debt are the primary root cause issue for data breaches.

Active Directory (AD) is the beating heart of an organization and is ultimately where a malicious threat actor, either internal or external, will focus their efforts. The advantages of AD compromise to an attacker mean unlimited access to all internal resources, accounts and workstations.

Why SpiderLabs?

Our comprehensive and best of breed AD review methodology will evaluate the configuration and security of your Active Directory assets. Through our methodology, we will ensure that defense in-depth and resiliency are integral factors of your AD design to slow attackers down, create detection points for your internal team and protect critical assets. AD is a complex infrastructure; to ensure a comprehensive view, the SpiderLabs methodology covers four key categories:

Managing Domains and Forests

We focus on the configuration of Forest to Forest and Forest to Domain relationships and identify issues with Trusts, protocol configuration and control of core assets such as Domain Controllers.

- Configuration of Active Directory Forest and Domain
    - Network Isolation
    - Privileged Access Workstations
- Forest and Domain Functional Level
- Active Directory Trust configuration and security
- Forest and Domain Trust Directions
- Protocol Signing (SMB, LDAP)
- Organizational Units
- Network footprint of domain controllers, resilience (if any), orphaned user, group and computer objects

Controlling the Endpoints

The endpoints are the initial foothold for an attacker; therefore, how these are managed and controlled can be an effective tactic in disrupting attackers. We review their managed states, applied policies for endpoints, and logging of local access.

- Patching management policy across the Windows estate
- Domain Password policy configuration
- LAPS deployment
- Password hash storage techniques (LM/NTLM):
- Security Group Policy Review
- Security Template Baselines
- Auditing and Logging
- Auditing Service Accounts
- Group Policy Objects
- Application Whitelisting / Windows Defender Application Control (WDAC)
- Bit locker- Best practice review

User Access Controls

Users need access to network assets. We examine the permissions users have, explicit and implicit group membership, and local administrative controls.

- User access rights and privileges
- Group Memberships
- Delegated Administrative Rights
- Local Administrative Controls
- Kerberos – Best practice review
- DACLs/ACEs
- Token Impersonation

Additional Product Add-on:

Active Directory Attack Resilience

This extended area of the service analyzes how an attacker might enumerate the directory and helps identify privilege escalation routes.

- Active Directory Password review
- Attack Path Discovery - Bloodhound
- Kerberoasting

Trustwave SpiderLabs® Segmentation Testing

The PCI DSS requires that any scope-reduction controls, where network segmentation is used to reduce the scope of assessment, are validated experimentally through segmentation testing. Trustwave's Segmentation Testing service can be used to confirm that scope-reduction controls are effective and truly isolate the assessed networks from the network where the assessment is taking place.

Our Approach

A segmentation test differs from a penetration test because it contains no vulnerability identification or exploitation phase against the target systems; the only goal is to demonstrate connectivity to the target systems. If connectivity is demonstrated to be possible, the segmentation test has failed and clients can choose to either enhance the ingress/egress filtering between the networks to eliminate the connectivity or perform a full network penetration test to characterize the access. If the out-of-scope networks are not segmented from the in-scope networks, they are brought into scope in accordance with PCI DSS regulations.

Methodology

A segmentation test has three primary phases, which are very similar to the methodology deployed in a network penetration test:

- Network Reconnaissance
- Vulnerability Identification
- Vulnerability Exploitation

Network Reconnaissance involves performing TCP, UDP and IP protocol scans against the target systems from the perspective of the out-of-scope testing origin network. The tests are done to confirm that no direct connectivity is possible.

Vulnerability identification is performed against gateway and network separation devices which are reachable from the testing origin network. In a real-world scenario, even if no direct connectivity is possible to the in-scope network, an attacker may be able to leverage a vulnerability in an adjacent or reachable system which could be exploited to gain connectivity to the targets laterally. Vulnerability identification is performed on network infrastructure systems to identify whether any weakness exists which could be used to modify the ingress/egress filtering rules or whether the system could be used as a 'jump host' to pivot towards the target networks.

Vulnerability identification and exploitation is not performed against the target network within a segmentation test, however vulnerabilities within separation devices or network infrastructure components which can be leveraged are exploited in this phase, in order to demonstrate that lateral access to the target networks is possible due to vulnerabilities within network components or connected systems. Please note that Trustwave takes special care to not cause disruption to network traffic flow, so it may not be possible to confirm whether connectivity is possible if doing so presents a quantifiable risk to network availability. In these cases, the vulnerabilities are documented but not exploited.

Trustwave SpiderLabs® Azure Cloud Assessment

With the proliferation of the cloud in recent years, organizations now more than ever need to ensure that they remain secure and vigilant against malicious cloud-based actors. Misconfigured cloud services are one of the top causes of data breaches.

Azure is a collection of cloud computing systems provided by Microsoft. It provides Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) options, all of which have the potential to be misconfigured.

How Can SpiderLabs Help?

Trustwave SpiderLabs brings our unique, comprehensive, and thorough methodology when looking at Azure based environments. As a client, you can rest assured that you'll receive more than an Azure audit; you'll have world class penetration testers applying cutting edge attack vectors to your Azure environments.

Being Thorough Increases Maturity

We take the security of your Azure instances very seriously and leave no stone unturned. Some of the areas where we focus our efforts and where we continuously see considerable benefit to the client include:

- Identity and Access Management
- Security Center
- Storage Accounts
- SQL Services
- Logging and Monitoring
- Networking
- Virtual Machine
- Active Directory Integration

The above is only a sample of some of the services we encounter on a typical Azure review; we would ensure that all appropriate services are fully analyzed for weaknesses and areas where security enhancements can be made. For example, we can review your O365 SaaS to ensure that it is secure and can repel attacks from threat actors.

Output

A final report will be created detailing all issues discovered with business impact, and appropriate recommendations will be made such that each issue can be successfully mitigated.

Trustwave SpiderLabs® Amazon Web Services

With the proliferation of the cloud in recent years, organizations now more than ever need to ensure that they remain secure and vigilant against malicious cloud-based actors. Misconfigured cloud services are one of the top causes of data breaches.

Amazon Web Services (AWS) is a collection of cloud computing systems provided by Amazon. It provides Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) options, all of which have the potential to be misconfigured.

How Can SpiderLabs Help?

Trustwave SpiderLabs brings our unique, comprehensive and thorough methodology when looking at AWS based environments. As a client, you can rest assured that you'll receive more than an AWS audit; you'll have world class penetration testers applying cutting edge attack vectors to your AWS environments.

Being Thorough Increases Maturity

We take the security of your AWS instance very seriously and leave no stone unturned. Some of the areas where we focus our efforts and where we continuously see considerable benefit to the client include:

- Key Management Service (KMS)
- Identify and Access Management (IAM)
- Virtual Private Cloud (VPC)
- Security Hub / Inspector
- AMI Hardening
- Directory Services

The above is only a sample of some of the services we encounter on a typical AWS review; we would ensure that all appropriate services are fully analyzed for weaknesses and areas where security enhancements can be made.

What Happens When the Worst Thing Happens? Logging to the Rescue.

An often-overlooked aspect of security and maturity is logging. AWS offers excellent logging facilities through CloudWatch and CloudTrail with enhanced anomaly detection. When our team views your configuration, we ensure that appropriate and recommended logging of AWS is achieved for enhanced peace of mind.

Output

A final report will be created detailing all issues discovered with business impact and appropriate recommendations will be made such that each issue can be successfully mitigated.

Trustwave SpiderLabs® Targeted Secure Code Review

Applications represent an easily accessible target which your organization can make available to attackers located around the globe as well as from within your own organization. From handling critical business processes to brochure-ware, these applications can be the first choice for an attacker looking to deface sites, steal your data, or gain a persistent foothold in your environment.

Your application's code base is where thought becomes tangible, where idea becomes reality. It is the culmination of your ideas – it's your product, your service, and ultimately, your reputation.

Developing an application is hard work. The task of automating a business process which reflects the nuances of your organization's varying workflows can be a daunting challenge even to the most experienced of developers who are focused on ensuring that the application not only functions correctly but also performs efficiently. Software testing is often performed to positively verify functionality before the application is deployed to its larger audience. However, software testing rarely looks for the potential abuses of business logic, authentication / authorization implementations, vulnerable third-party components or the risks associated with the application's underlying environment.

A Targeted Approach

Code review can be automated – there are numerous commercial products which will parse through millions of lines of code in the attempt to uncover insecure coding practices that may negatively affect your application and organization. Unfortunately, the output of these tools can often be a daunting list containing thousands of potential issues leaving the reader to sift through a sea of details in order to separate legitimate issues from noise.

Trustwave's Targeted Secure Code Review is designed to be added to our most advanced Application Penetration Tests (Targeted and Advanced Threat). When coupled with these test types, the Targeted Secure Code Review will maximize the effectiveness and validity of discovered vulnerabilities. By correlating dynamically discovered findings and other potentially sensitive areas of your application with their associated code locations, the Trustwave consultant will go deeper into your application and its code base to identify root issues associated with individual or systemic coding practices.

SpiderLabs – Proven Experience

Trustwave SpiderLabs has spent the last 15 years building and refining methodologies to assess the security posture of applications built across the varying platforms and languages used in decades worth of development. These methodologies map to proven OWASP standards while also accommodating the discovery of issues particular to your application.

Staffed with ethical hackers with diverse and deeply technical backgrounds, SpiderLabs is prepared to uniquely apply their refined methodologies to your application to quickly understand its purpose, its underlying environment and its potential abuses.

Going Down the Rabbit Hole

Evaluating hundreds of thousands of lines of code can be an ineffective approach to finding specific problem areas of your code base. Performing a Targeted Secure Code Review allows you to work with your Trustwave consultant to review these pinpointed areas to uncover issues such as authentication bypasses, authorization issues, business logic flaws, potential injection attacks and other vulnerabilities which an attacker could successfully use against your application. By combining your Application Penetration Test with a Targeted Secure Code Review, you can get a 360° view of your application's security posture showing you validated, meaningful results from their known underlying locations while leaving out the distracting noise often associated with pure static application security testing (SAST) approaches.

Ensuring Success

You know your code base – SpiderLabs knows hacking. Pair these two areas of knowledge to expose vulnerabilities in your application which could otherwise remain dangerously undetected. And what does a Targeted Secure Code Review look like for your organization? It may focus on business rule processes which, if exploited, could allow an attacker to abuse product ordering functionality. Perhaps it might allow an attacker to take advantage of a handful of unprotected administrative resources. An attacker with unlimited time may find a SQL Injection attack that gives them access to your most sensitive data. Regardless, these pinpointed reviews of your engagement are guided by Trustwave SpiderLabs' reliable penetration testing results and your security testing goals giving you a truly customized view into previously undetected vulnerabilities.

Trustwave SpiderLabs® Social Engineering

Social engineering is the practice of manipulating people into breaking company security policy and divulging sensitive information. Malicious actors often employ social engineering tactics to gain access to a business's confidential data. Trustwave SpiderLabs® offers a wide range of social engineering services that utilize these tactics to understand where vulnerabilities lie within a company's userbase, offering a view into the organization's security posture and helping to prevent an actual compromise.

Phishing

Phishing is an attempt to trick a group of users into opening a crafted e-mail with the goal of eliciting sensitive information or, through the executing of an attachment, gaining unauthorized remote access to the targeted environment.

Spear Phishing

The goal of phishing attacks is to send a spoofed email (or other communication) that looks as if it is from an authentic organization to a large number of people. Spear phishing-attacks are personalized to a particular target, or a small group of similar people. Due to a personalized attack it is more difficult to identify spear-phishing attacks than to identify phishing attacks conducted at a wide scale.

Vishing

Voice phishing, or "vishing", works similarly to an email-based spear-phishing attack by using personalized information to leverage trust, but uses the telephone as the medium. Vishing uses verbal pretexts to trick targets into behaviors they believe are in their best interests. Vishing often picks up where phishing leaves off.

SMiShing

Texting is the most common use of smartphones. Text, or SMS phishing (SMiShing) is an attack which a targeted phishing pretext or message is sent to a cell phone over SMS text messaging instead of email.

Onsite Physical Social Engineering

Bad actors often take advantage of vulnerabilities in an organization's physical environment to walk directly into a facility to compromise sensitive information or technological systems. Through conducting physical social engineering exercises such as tailgating, baiting dumpster diving, USB drops, picking locks, etc. in an attempt to circumvent security measures and identify vulnerabilities at specific locations and with physical network access one is able to gain insight to vulnerable points of attack.

Trustwave SpiderLabs® Open Source Intelligence Testing

An Open Source Intelligence (OSINT) Test provides a window into the public data exposure of your enterprise. This type of testing allows you to see how an advanced threat actor would go about the initial reconnaissance stages that would inform the next steps of a targeted attack. This test helps you pinpoint where you have potential data leakage and makes cracking the perimeter of your network more difficult for determined attackers. It also helps prevent opportunistic attacks when hackers are simply looking for an easy win.

Mapping Your Attack Surface

Open Source Intelligence tests can help map the attack surface of your organization. You get a simplified view of what an attacker will see when deciding which part of your organization to target. This part of the test will enumerate your subdomains and provide stealthy port scanning without ever touching the target. It can also help you identify any old or forgotten machines that have been missed from patching, update and testing cycles. You can also further engage Trustwave SpiderLabs to help you with remediation.

Targeting the Individual(s)

People are important to your organization and they are your greatest strength, but they can be your greatest weakness. The entry point for most modern sophisticated attacks is phishing an organization's users. We can help you identify which users are most likely to be targeted by phishing attacks. You can then use this information to provide security awareness training or perform mock phishing exercises to gauge their awareness.

Open Source Intelligence tests can also identify which of your employees have been involved in a public data breach. This information can be used to remind these employees of the dangers of password reuse by making them aware that their account has been compromised on another site, thereby making you more secure.

Benefits of Open Source Intelligence Testing

- Understand your organization's exposure on the internet and dark web that hackers can use against you.
- Protect staff from spear-phishing attacks and advanced persistent threats.
- Decrease the time it takes to determine if a breach took place.
- Gain actionable advice to reduce your organization's attack surface and increase security maturity and resiliency.

Trustwave SpiderLabs® Wireless Penetration Testing

The Wireless Enterprise Network – The Cableless Nerve System of Your Organization

The internal wireless network is one of the organization’s most critical assets, much the same as the internal cabled network. The internal wireless network is typically an expansion of the internal network, with different vulnerabilities characteristics.

The most significant difference is that it does not use the cable infrastructure and thus, by design, suffers from various problems and threats. For example, a cabled network will not be accessible by a neighboring building as the network connectivity is limited to where the network cable is installed, but wireless networks are more vulnerable as the wireless signal is not so precisely confined.

Service Description

The Wireless Penetration Test evaluates the resilience of the security protocols of the target wireless networks. The goal of the assessment is to determine the level of access that could be obtained by a malicious intruder if unauthorized access is achieved.

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 the exploitation of identified vulnerabilities to provide a complete security assessment of the wireless environment.

Your SpiderLabs consultant will help you define a testing approach that yields maximum value to your organization.

Site Survey

Trustwave SpiderLabs obtains the Site Service Identifier (SSID) information for all locations to be tested from the 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 discreet site walkthrough using handheld equipment. The data from both activities are 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 discreet 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 4 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), WPS (WiFi Protected Setup), 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 discuss the modus operandi during the initial kick-off meeting before the engagement starts. 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.

Trustwave SpiderLabs® Trusted Security Advisor

How Can SpiderLabs Help?

Trustwave's SpiderLabs is a team of world-renowned experts in application security, network security, forensics, physical security and social engineering. The team publishes research papers, provides speakers at leading industry events such as BlackHat, DEFCON and AppSec, and annually gathers data for Trustwave's Global Security Report.

Customers can elect to have a consultant within SpiderLabs as a Trusted Security Advisor who becomes a virtual extension of the corporate security team. This expert can be available for security strategy sessions, project management, vendor evaluations, compliance reviews and executive briefings. As appropriate, the Trusted Security Advisor will bring in members of the SpiderLabs team as subject matter experts.

Bespoke Solutions

Need assistance with an Information Security challenge that doesn't quite fit within any of SpiderLabs standard offerings?

From customized testing services to tailored reporting requirements, a SpiderLabs subject matter expert can assist you with delivering a bespoke security testing or assessment solution to meet your exact needs.

Common examples include:

- Large multi-part segmentation tests to gauge the effectiveness of network controls across a global network.
- Penetration Tests designed to meet specific industry compliance requirements.
- Customized reporting and presentations, above and beyond the standard penetration test report.

Put SpiderLabs expertise to work for your organization.

Trustwave SpiderLabs® ATM Testing

Automated Teller Machines (ATMs) are a ubiquitous technology; however, due to their very nature, they are an extremely attractive target for criminals. ATMs can contain large quantities of cash, they have a steady flow of customers inserting cards, and they have a network connection back to the core banking infrastructure.

Common attacks against ATMs include ‘Jackpotting,’ where all the cash is stolen, and card skimming, where unsuspecting customers of the ATM have their cards cloned, allowing the criminals to withdraw cash elsewhere.

Almost all modern ATMs contain a desktop PC, which controls the operation of the unit, and a network connection to facilitate communication with the core banking systems.

Network Testing

Building upon tried and tested network penetration testing and segmentation testing, this area will focus on both the vulnerability of the ATM and its operating system to attacks over the network, as well as the vulnerability of the bank network itself should an attacker gain a foothold on an ATM.

As a typical ATM runs a general-purpose desktop operating system, many of the same vulnerabilities and misconfigurations are possible. Similarly, if weaknesses in the network layer are identified, an ATM in an easily accessible location could provide a foothold for attacks further into the bank’s network.

Physical Testing

A typical ATM consists of two cabinets – an upper cabinet containing the control PC, card reader, printer, etc., and a lower cabinet containing cash cassettes. Physical testing will aim to identify how easy it is to access either part of the ATM using a variety of techniques, e.g. lock picking, etc.

As well as attempting to gain access to the inside of the cabinets, testing will also seek to bypass any mechanisms that may be in place to detect unauthorized opening of the units.

Jailbreaking

Jailbreaking of an ATM assumes that physical controls have been breached and an attacker has gained physical access to the upper control cabinet of an ATM and is looking to deploy malware for the purposes of extracting cash or cloning card numbers.

Jailbreak testing will look at software and hardware level controls on the unit itself to prevent, delay or detect the loading of malicious code onto the unit.

Environmental Testing

Environmental testing will assess the physical environment where an ATM sits to determine if any of the attacks identified during physical testing would be practical. For example, an attack which requires several minutes of lock picking may be practical on a standalone ATM in a quiet location, but would not be successful on an ATM located in the foyer of a bank branch where it remains in full view of staff.

Environmental testing will look to assess the risks of physical attacks being successfully carried out in a real environment while avoiding detection. Specifically, whether any physical and/or jailbreaking attacks could be successfully carried out within a realistic timeframe to avoid the attacker being detected or caught.

Trustwave SpiderLabs® Remote Access Testing

Remote access or remote desktop services are widely used to allow secure program access to remote users. Excessive user privileges or a limited lockdown of the host can lead to the running of arbitrary programs and access to the file system.

This can allow privilege escalation, bypass of application-enforced access controls, and, potentially, the compromise of the server itself. If remote compromise of a server can be achieved, it can then be used to attack the internal network.

Test Highlights

Remote desktop services such as Citrix and Microsoft Terminal Services are widely used to allow remote users to access programs and services securely. These products are often misconfigured, allowing users more privileges and access than they require for their role.

Trustwave SpiderLabs will carry out a focused attempt to 'break out' of the locked-down environment provided by these programs whilst logged in as a user, and to use any access gained to attack the internal network. The assessment will be performed from the following positions:

- Without any knowledge of the system.
- Without any knowledge, but with access rights (valid credentials provided by the client).
- With knowledge of the configuration details and how the infrastructure has been configured.

Depending on your precise requirements and setup, a typical assessment may test:

- Ingress and egress firewalls
- Internal network routing - The ability to make a second remote desktop connection to another machine, internally. This is often the case in multi-tenanted environments.
- Active Directory integration, software restriction polices, network footprint of servers, patching policy across the Windows estate, password policy configuration, and local security policies.
- Whether the remote desktop server allows access to sensitive documents.
- Whether there are network shared directories which are accessible remotely and can be used to access other machines.
- Whether anti-virus is installed on the server with all definitions up to date.
- Whether the user is able to run macros and ActiveX controls on the server. While Visual Basic for Applications (VBA) macros are often used in a normal workflow, they are one of the biggest causes of malware infection through both targeted and generalized attacks.

- Which third-party applications are installed, and in which versions. Many organizations use old versions of software, such as older versions of Acrobat Reader, which have known security holes. This will, depending on circumstances, be combined with a client-side attack.
- Whether the remote desktop is set up for two-factor authentication. Many remote desktop servers are configured only to use single-factor authentication (such as a password). This is inherently less secure than two-factor authentication and may lead to security breaches if a user's password is compromised.

The report will highlight the security posture of both the remote access solution itself and the environment, from the perspective of a low-privileged user given that valid user credentials are provided.