ONCE AND FUTURE THREATS

What Security Testing Is And Will Be

Trustwave®

Table of Contents

A Message from Trustwave SpiderLabs

There is no single best way for businesses, organizations and government entities to defend against cybersecurity compromises. That's why Trustwave SpiderLabs performed millions of vulnerability assessments and thousands of manual penetration tests and red team exercises in the last 12 months... to help customers identify and secure weak points in their computer infrastructures.

In this e-book, we will define some of the most common security testing techniques and how they can be used to benefit your organization. Then, we will present some of what Trustwave security experts learned about significant threats that organizations will face in 2020 and beyond, and discuss how best to mitigate those risks. Use this information to empower your organization to fight the malicious actors it will face in the coming years.

On behalf of the entire Trustwave SpiderLabs team, we hope you find the topics discussed in this e-book helpful. To learn more about them, please visit the **Trustwave SpiderLabs Blog** for ongoing reporting on the challenges that Trustwave security experts encounter, and see **our guide** to red-teaming and pen-testing and the advantages and disadvantages of both.

Mark Whitehead
GLOBAL VICE PRESIDENT, SPIDERLABS CONSULTING

About Security Testing

METHODS OF SECURITY TESTING—AND HOW THEY CAN HELP

The rising public exposure of security testing in recent years is gratifying; however, many people still don't understand what it means and how it works. This lack of knowledge can lead to unfortunate results. For instance, when the state of Iowa, in the United States, tasked a security firm with penetration testing the security of a courthouse, two employees were arrested for burglary. The pair had tried to test the building's physical security rather than its computer security.

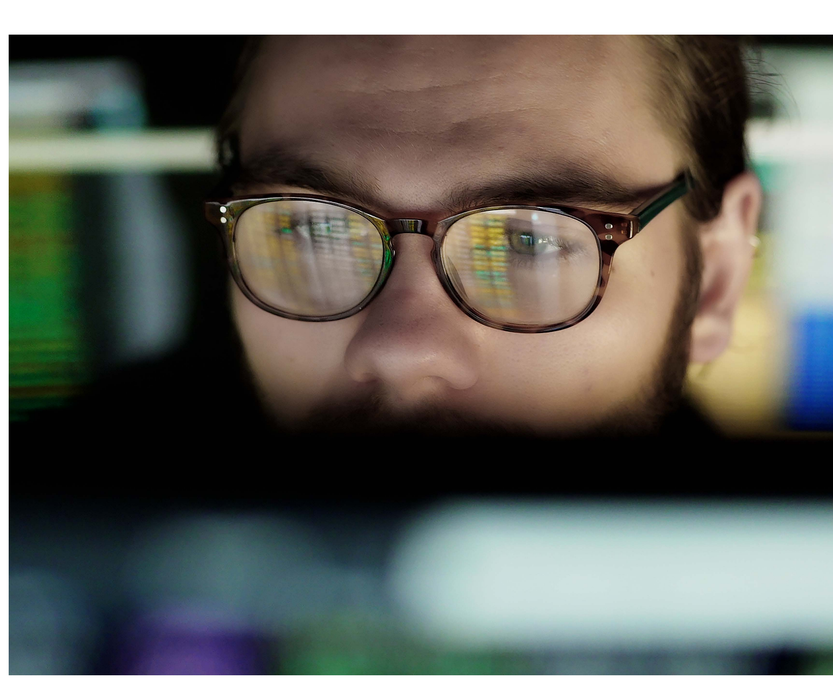
While the state ultimately dropped the charges, the incident highlights the need to educate the public about what security testing entails. In this chapter, we'll define the common testing services that Trustwave typically provide and discuss how they can be used to help improve your security posture.

AUTOMATED TESTING

The first level of testing an organization should take includes simple automated discovery and vulnerability scans that catalog an organization's internet-facing and internal assets and identify weaknesses. These can typically be performed at any time, with little to no disruption to production. These automated scans are a prerequisite for penetration tests and other, more advanced procedures, as Trustwave security experts use them to establish an organization's security baseline and provide a benchmark for progress. An organization at an advanced state of readiness can conduct these tests itself. In other cases, Trustwave professionals can come in and conduct the tests remote or on-premises with the cooperation of the organization's IT department.

PENETRATION TESTING

Penetration (pen) testing involves a degree of automated testing and requires security professionals who combine automation with advanced tools, manual tactics and their own expertise to find ways an attacker can compromise a target environment.



While simpler automated scans mostly identify potential weaknesses, pen testing uses techniques such as electronic social engineering, password brute-forcing, system specific gaps, network-layer indepth application analysis and legacy protocol attacks to demonstrate how those weaknesses can lead to compromise. Regular pen testing should be on the menu for just about every business as many organizations could have prevented high-profile breaches through pen testing alone. At a higher level, Trustwave professionals also conduct specialty tests on specific parts of the computing environment, such as mobile, internet of things (IoT) and cloud services.

RED TEAMING

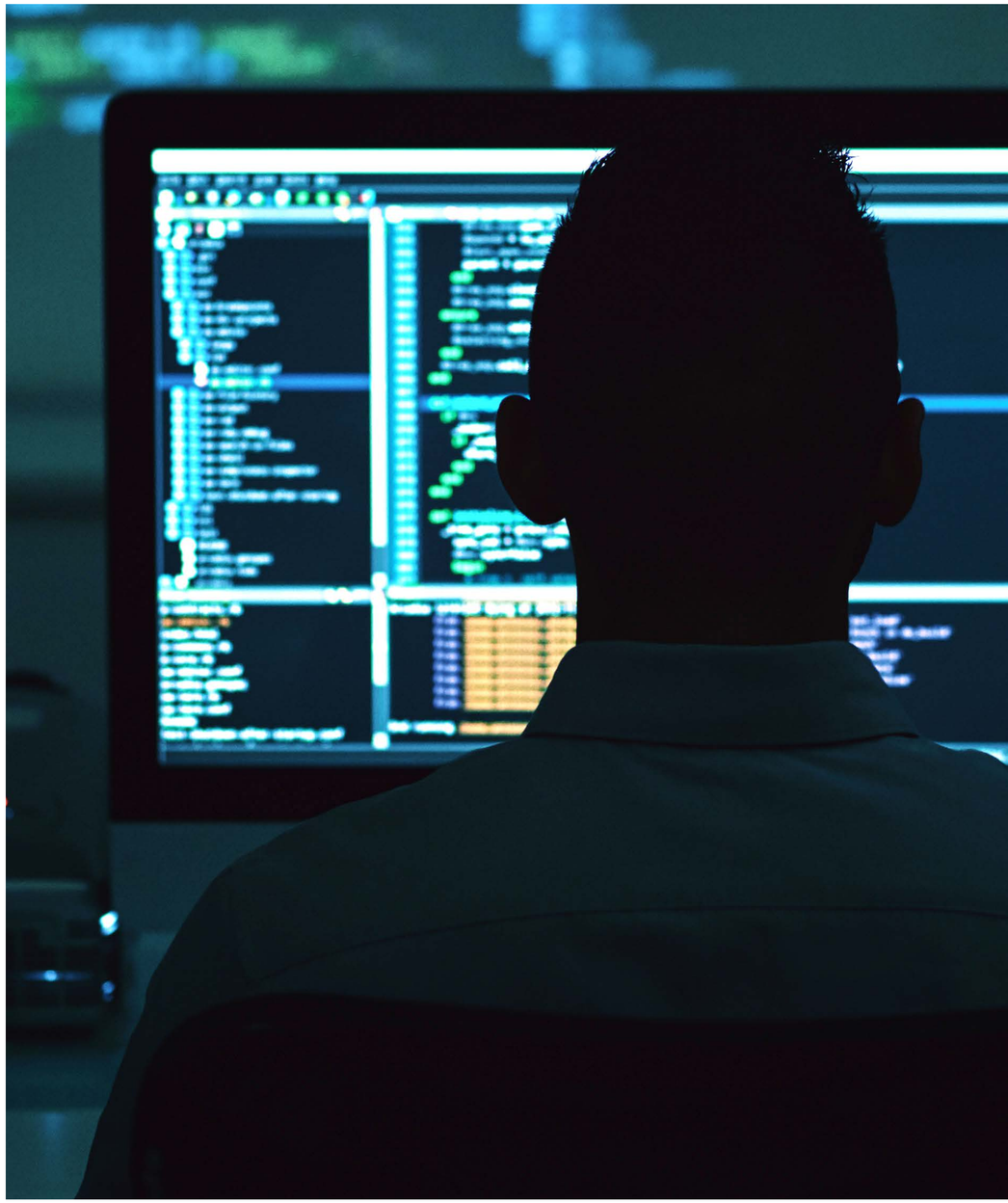
The more dramatic, as-seen-on-TV stuff includes red teaming. In a red team exercise, an elite group of Trustwave SpiderLabs security testers mount a focused attack with the goal of compromising an infrastructure. Unlike pen testing, which is still largely automated, red teams use the full range of tricks real attackers use. These include:

- Open-source intelligence (OSINT) gathering, or using third-party sources, to find information about the organization and its employees. OSINT can come from unexpected places, such as LinkedIn, Facebook, Twitter or other social media sites because employees sometimes reveal more than they realize in seemingly innocuous posts.
- Phishing and business email compromise (BEC) messages tailored to specific recipients using information learned from OSINT or other sources.
- Online and offline social engineering designed to catch employees unawares and test the security of the organization's physical infrastructure.
- Misconfigurations, gaps existing security products have not filled, and Tactic Techniques and Procedures used by real world threat actors.

In this testing, a blue team, composed of security personnel within the organization, must detect and stop the red team's attack. Blue teams typically function with limited information —as they would during a real attack. They do not know when the attack is coming, what systems it will target or, sometimes, that a red team exercise is taking place. Trustwave security professionals only perform red team testing with organizations capable of mounting an effective defense. In other cases, Trustwave experts can work with the organization to increase their strengths to a point where red teaming is possible.

PURPLE TEAMING

While most people connected with computing security are familiar with red teams, fewer are familiar with purple teams. They combine the functions of red and blue teams to attack specific systems in predetermined ways so responders can improve and refine their defense approaches. Unlike with red teams, defenders know when the attack is coming and what systems the purple teams will target. Purple teaming can be appropriate when an organization wants to focus on the best way to remediate specific areas of weakness. The information sharing before and during a purple team exercise gives defenders specific skills based on knowing the tools and techniques attackers use, what the attackers expect and what they don't expect.



Integrating Your Security Spheres

A 360° APPROACH TO SECURITY MANAGEMENT

Security is often thought of in terms of separate spheres of operation, such as on-premises security, cloud security and mobile security. In general, this is a mistake. Any modern organization is likely to have a presence in multiple spheres and should employ an integrated approach to security management that pays less attention to where data and assets live than to the best way to protect them. Nevertheless, in a world of cloud computing, smart phones and connected appliances, it's important to understand the unique risks faced by each environment and class of device.

SECURITY IN THE CLOUD

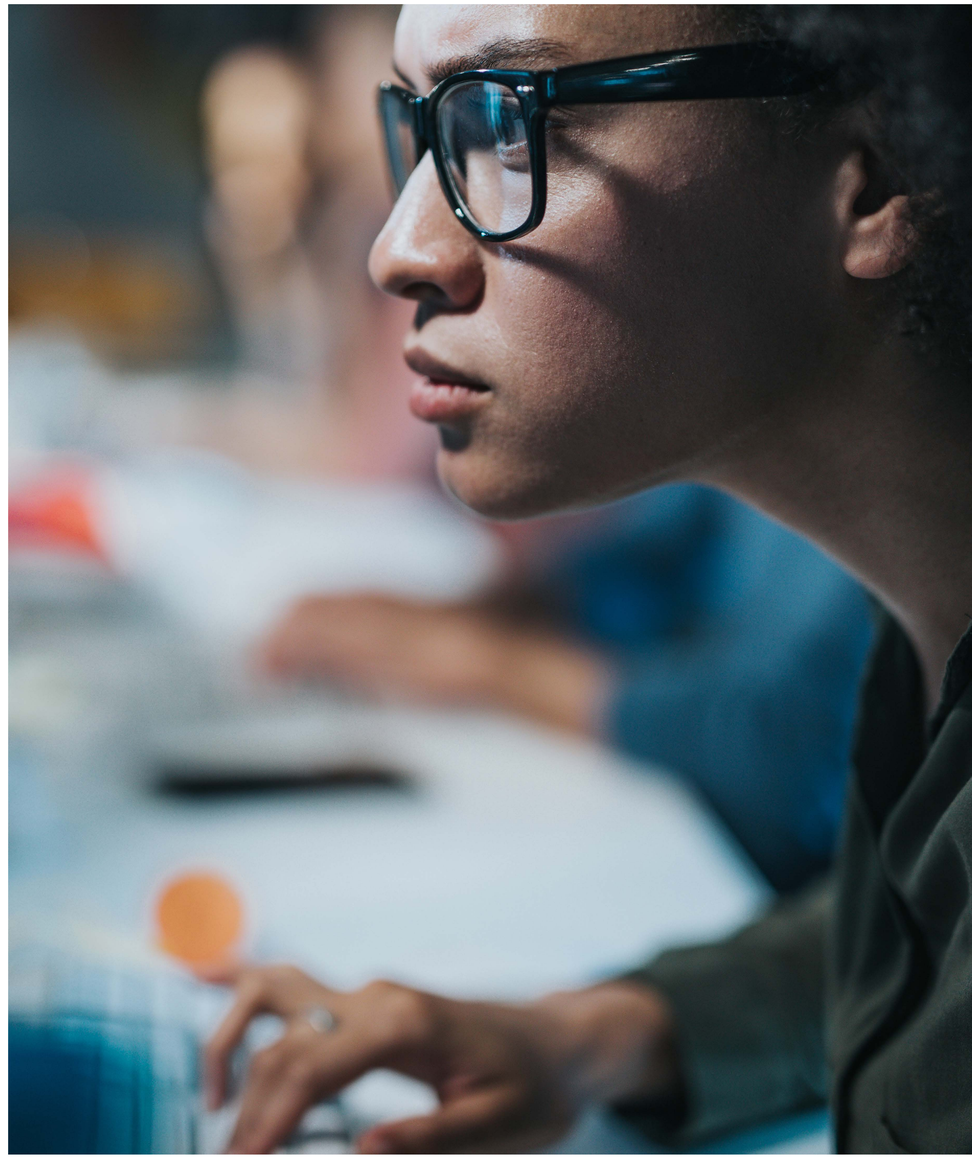
Many organizations that have moved operations to the cloud over the past decade did so, in part, because of the perceived security benefit of cloud services. Large cloud operators, such as Amazon, Microsoft and Google, prioritize keeping customer assets and data secure and devote abundant resources to defending their infrastructure against attackers. Customers sometimes assume they don't have to think much about testing outside of the on-premises testing, but that is a mistake. Customers with added cloud solutions cannot afford to sit on their hands about security.

Customer complacency about cloud security may be one of the most important weapons in cybercriminals' arsenals. For example, infrastructure-as-a-service (IaaS) platforms, such as Amazon Web Services, enable customers to build completely virtual environments of servers and other resources. This flexibility makes it easier to boot new machines as needed to satisfy demand, perform testing and meet other requirements. Yet, a virtual server is like any other server: There are plenty of opportunities for misconfiguration that can lead to weaknesses, such as ports and services being inadvertently exposed to the internet. If a system administrator creates an image of a misconfigured server, then every server created from that image will have the same vulnerabilities, potentially multiplying the base problem.

Misconfiguration isn't only a problem for IaaS infrastructures. The ready availability of predesigned resources in platform-as-a-service (PaaS) cloud environments can lead system administrators to make assumptions about the configuration and security of those resources, and incorrect assumptions can lead to breaches in operating systems, databases or web servers, for example.

Amazon's Simple Storage Service (S3), one of the most popular options for enterprise cloud storage on the internet, has seen a rash of high-profile data breaches in recent years due to misconfigured S3 storage buckets. S3 buckets are private by default. But that's easy to change, and it's not always clear what level of access control a particular bucket should have. Amazon has begun to educate customers about access levels and warn them when they appear to be setting access too broadly, but mistakes still happen. This is one of the most important areas Trustwave encourages customers to test and verify.

Even software-as-a-service (SaaS) offerings, such as Microsoft Office 365, that provide customers with relatively few options for misconfiguration compared with other services have emerged as big targets for attackers. Many organizations require multi-factor authentication (MFA) for Office 365 users, which is a good idea and should be considered a minimum for securing business-critical Office 365 deployments. But SaaS offerings can also enable legacy authentication for compatibility with some older clients, creating an opportunity for attackers to bypass MFA and find a way into systems. An attacker with access to an Office 365 mailbox, for instance, can use it as a launchpad into other parts of the organization.

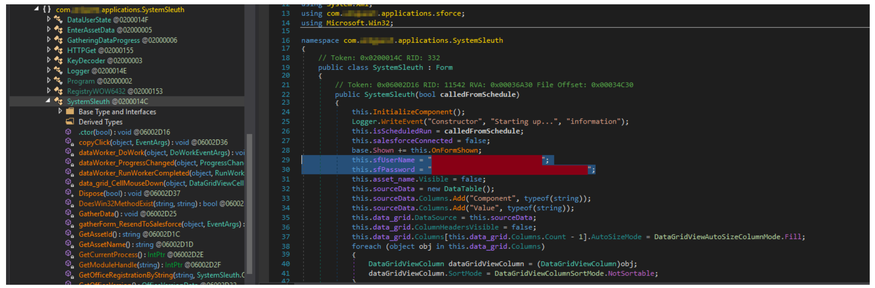


MOBILE, IOT AND BEYOND

Enterprise security extends beyond the bounds of protecting such real and virtual spaces as mobile devices, homes and coffee shops where telecommuting employees set up to work, and the rest of the world of connected smart devices that comprise the internet of things (IoT). Every integrated security plan must consider these areas along with factors some experienced security professionals may overlook.

Where desktop and mobile environments are largely known quantities, the IoT space is chaotic and features weak spots that include custom-built, embedded software that may have been inadequately tested or configured and can be difficult or impossible to update. Vendors, at the cost of security, sometimes take shortcuts that make it easier for customers or service technicians to access and administer the devices.

In 2019, a Trustwave SpiderLabs tester discovered a significant security hole in legacy IOT kiosks, which the hospitality industry widely uses to provide guests with the ability to check-in to flights, access the internet and perform other self-service functions. A leading IOT company published several management tools on a publicly accessible website, including one tool that could be decompiled to obtain credentials to download sensitive customer information. See the Trustwave SpiderLabs blog for more information.



Hard-coded credentials revealed in the C# decompiler

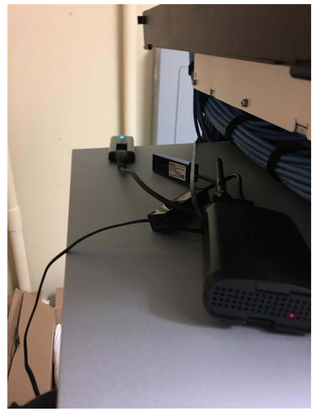
Mobile and IoT devices are also frequently physically accessible to outside parties, another way they are distinct from most enterprise computing assets. Physical access can provide attackers with multiple opportunities for compromise, with network taps and credit card skimmers, that would not otherwise be available.

PHYSICAL SECURITY

People often don't think about physical security as a component of computer security, but they should. Organizations that assume attackers are always remote overlook the risk that can come from attackers who are on-premises. The most secure virtual perimeter imaginable is useless against a malicious actor with physical access to sensitive hardware. These photos show equipment that a Trustwave SpiderLabs tester used to gain physical access to the network in a sensitive facility. When plugged into a computer, these devices allow a remote intruder — a Trustwave tester in this case, but potentially a malicious attacker — to access that computer from anywhere on the planet.

Organizations often have protocols that effectively control physical access to their facilities, but "physical security" here doesn't just encompass hands-on access to equipment. A comprehensive physical security plan must also include the close environs of a sensitive facility.

Wireless access, often taken for granted, is an additional risk that needs testing. In the picture below, a Trustwave SpiderLabs tester is exploiting a customer's wireless signal from the parking lot. After gaining initial access to the organization, the tester can then interact with systems as a corporate user or administrator would.



Remote access devices

A security tester remotely "attacking" a network over Wi-Fi

Attack Trends and Techniques

GUARDING AGAINST ONCE AND FUTURE THREATS

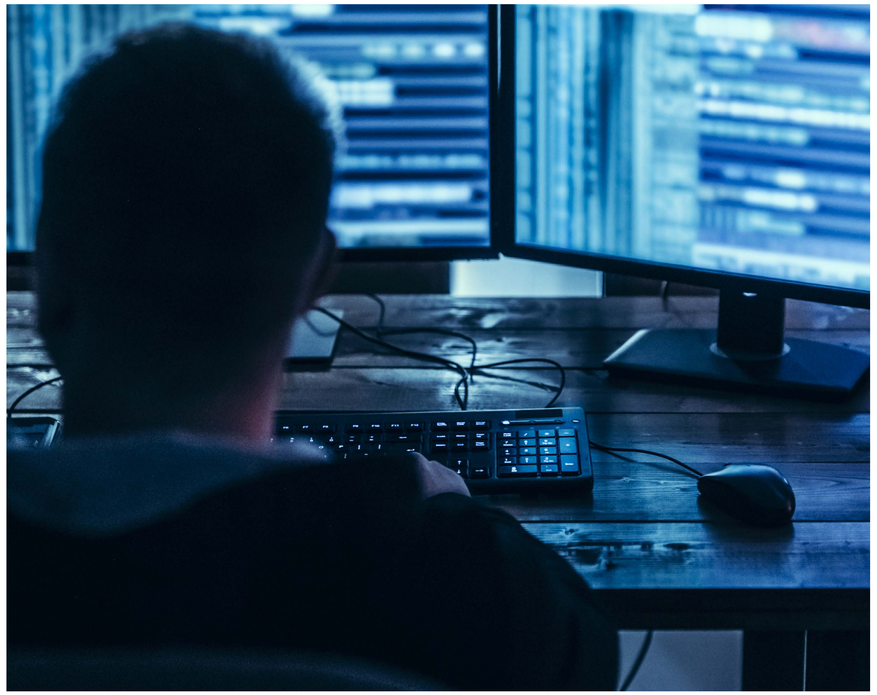
The worst thing a security tester can do is stand still. Cybercriminals frequently shift tactics and develop new ideas. A tester's job is to keep up with developments and anticipate the new ones whenever possible. There isn't enough space to cover the variations and evolutions Trustwave SpiderLabs testers encountered over the years, but here are just a few of the trends they have discovered recently.

ATTACKING APPLICATIONS AND NETWORK PROTOCOLS

Whether on-premises, in the cloud or in mobile or IoT devices, cybercriminals love attacking applications and network protocols. Trustwave experts extensively test web applications for vulnerabilities and flaws that could lead to compromise. Any application with a public-facing component can become a target for an innovative attacker looking for an obscure entry point, and newly developed attack techniques are always in demand. Automated testing alone may not always pick up these weaknesses. See the paragraph on vulnerability chaining, on the next page, for an example.

Every internet-connected device and system, regardless of function, form factor or location, relies on a suite of low-level protocols that attackers often target, not just for exploitation but also to carry out their own attacks.

For example: The Domain Name Service (DNS), which matches domain names with numeric IP addresses, is one of the most fundamental building blocks of the internet. When gaining access to a system, one of the first things attackers often do is query DNS to enumerate servers and other resources on the network. These queries can be hard to distinguish from legitimate network traffic; but under the right circumstances, it can be possible to construct an early warning system to help responders stop an attack as it begins.

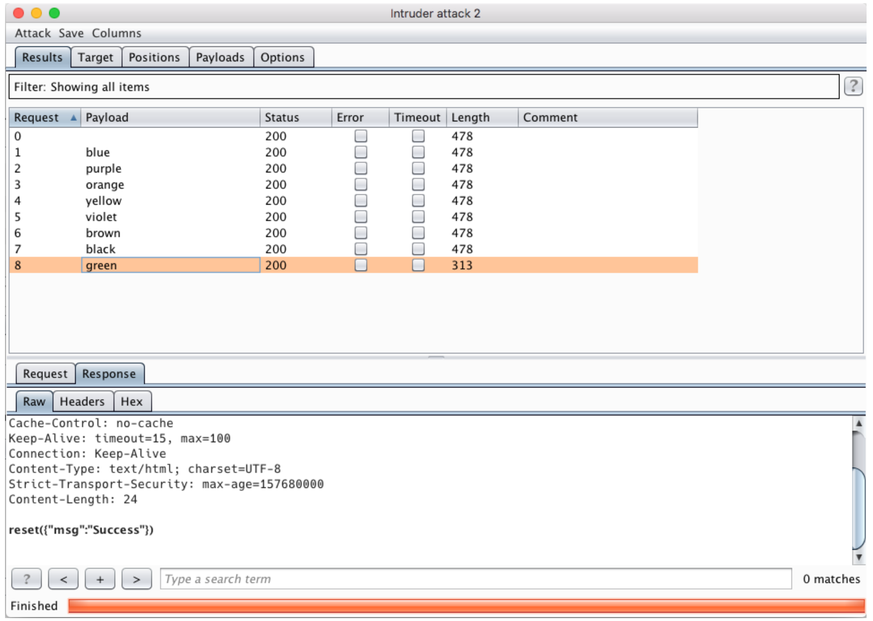


VULNERABILITY CHAINING

Chained vulnerabilities are another problem human security testers can detect more easily than automated tools can. Trustwave scanners check web applications for a wide range of weaknesses and other problems and assign them risk levels, ranging from critical and high for the greatest risks to low and informational for the lowest risks. However, a savvy attacker can compromise a website by chaining together several low- and informational-severity vulnerabilities. On their own, these vulnerabilities do not pose a significant threat; but collectively, an attacker can use them to gain unauthorized access to a system and potentially jeopardize sensitive data.

For example, many websites allow users to designate security questions they can answer to reset their passwords or log-in from unfamiliar devices. In the last 12 months, a Trustwave penetration tester discovered that the security question feature on a customer website made it possible to determine whether a given account name existed on the site. If the tester used a nonexistent account, the site would ask a different question each time the attacker tried the account name. If the account existed, the site would repeatedly ask the same question.

The tester used statistically likely usernames — along the lines of “jsmith” — to compile a list of existing accounts and their associated security questions. Many of these account holders had selected the question “What is your favorite color?” The question is weak because most account holders use common colors for their answers. By brute-forcing the answers, the tester gained access to the password reset screen for several accounts — revealing another weakness. A more secure application would send a password reset link to the email address on file for the account. Instead, the compromised website would provide the attacker complete control over the compromised account.



A successful attempt to guess an account’s secret answer

By themselves, each of these weaknesses — guessable account names, one security question per account, weak security questions allowed, password reset allowed on the spot — may not be rated as high as critical vulnerabilities or might not be detected by automated tools at all.
Yet, a knowledgeable attacker could put them together to compromise multiple accounts quickly and without using a malicious code exploit. Security testing makes it possible for security professionals to find and mitigate such problems.

OPEN-SOURCE INTELLIGENCE (OSINT)

The rise of social media in the industrialized world has led to a generation of people living their lives online. This has led to a bonanza of open-source intelligence (OSINT)—information about people, places and organizations gathered from publicly available sources and used for intelligence purposes.

For example: A proud new employee might post a picture of her badge on Facebook and link to a LinkedIn page displaying her job title and work location. A lot of data from leaks, breaches and data exposures is also available on the internet and the dark web. Unfortunately, attackers realize this and are better able to quickly gather, parse and execute on this information. What used to take weeks and months can now be done in a matter of hours.

AttackSurfaceMapper (ASM) is an open-source tool developed by Trustwave SpiderLabs penetration testers that automates the process of gathering information about a domain from OSINT sources and active reconnaissance methods. Given a domain name or a list of IP addresses, ASM compiles information from sources such as DNS records, WHOIS, social networks, breach information databases and password dumps, and more to create a picture of the domain's attack surface and potential weak spots. This greatly shortens the time a pen tester needs to gather the information needed for a thorough test.

AttackSurfaceMapper

AttackSurfaceMapper can be downloaded from GitHub.

While the attack trends listed here represent an overview of what Trustwave SpiderLabs testers have encountered, new techniques are always being developed—we encourage you to follow the Trustwave SpiderLabs blog to stay up-to-date on our findings.

Trustwave is a leading cybersecurity and managed security services provider that helps businesses fight cybercrime, protect data and reduce security risk. Offering a comprehensive portfolio of managed security services, consulting and professional services, and data protection technology, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.

Proactive security testing can help you understand where your risks and vulnerabilities reside, enabling you to better prevent, detect and respond to security incidents. Trustwave makes it easy for you to stay ahead of cyber attackers with solutions like:

SECURITY TESTING SERVICES

Trustwave makes it easy to get the insights you need to improve your security posture, even for resource-deprived businesses.

TRUSTWAVE DBPROTECT

This highly scalable database security platform enables organizations to secure their relational databases and big data stores, both on premises and in the cloud, with a distributed architecture and enterprise-level analytics.

SPIDERLABS TESTING

With vast insight into the latest vulnerabilities, attack vectors, exploits, malware and breaches, Trustwave SpiderLabs applies deep knowledge to help you stay ahead of cybercriminals.

trustwave.com

©2021 Trustwave Holdings, Inc.