White Paper

Pentesting: The Required Human Ingenuity to Uncover Security Gaps

Introduction

> "The pen is mightier than the sword."
>
> Edward Bulwer-Lytton, 1839

In 1792, a crowd in Paris, emboldened by ideas of equality as expressed by Jean Jacques Rousseau and Thomas Jefferson, rushed past the swords of the French military and overthrew a monarchy that had ruled for a thousand years.

In modern times, ideas, expressed as carefully-crafted lines of digital code, have bypassed safeguards to covertly trash the nuclear centrifuges of one nation, and steal 18 million confidential government personnel files from another nation. In the business world, carefully-crafted packets of code are penetrating the defenses of many businesses to steal sensitive business and user data. Some of these attacks damage the trust and goodwill that multi-billion dollar global brands have taken decades to build.

The most elaborate, layered cyber security can still contain many vulnerabilities. It takes creative and persistent human ingenuity to discover those vulnerabilities and develop new ways to exploit them. This is the mission of a penetration tester.

An ethical hacking exercise can reveal the security weakness and digital risks within your organization, before someone else exposes them, either inadvertently or maliciously.

Why pentesting is important

A penetration test (or more commonly, "pentest") is a software, infrastructure and or network attack on your organization by a skilled attack team that probes for security weaknesses and seeks to exploit them to reach your assets.

The testing team surveys the breadth of potential damage that can be done in an attack, and delivers a report, associating a level of risk with each vulnerability they discover. A pentest report helps an organization prioritize its security weaknesses and reduce risk.

How is a pentest different from a vulnerability assessment?

A vulnerability assessment identifies and logs vulnerabilities, ranks them, and recommends needed mitigation. A pentest not only identifies vulnerabilities, it uses those vulnerabilities to simulate attacks that a skilled and determined attacker could carry out on your organization once inside your network.

What to look for in a pentester

When you evaluate a security partner for penetration testing, consider these criteria:

Strong track record: Your prospective partner should have a long involvement in the security community. They should have intimate knowledge of subjects such as:

- Enterprise development framework
- Networking protocols
- MiTM (Man-in-the-middle attacks)
- ARP spoofing
- Multi–platform system administration
- Password storage (LM, NTLM, shadow, etc.)
- Database systems
- Scripting (Ruby, Python, Perl, etc.)
- Other essential security toolsets

Pentesting: The Required Human Ingenuity to Uncover Security Gaps

Ask if they've done any of the following:

- Spoken at peer conferences such as DerbyCon, DEF CON, ShmooCon, etc.
- Contributed to open source projects
- Published new knowledge of vulnerabilities responsibly
- Written blog posts to contribute to security education

Look for evidence and ask for proof of the above criteria, and scenarios before choosing your pentest partner.

Communication skills: Pentesters need to be deeply technical, but they also should be able to explain their findings and recommendations in everyday language. This is especially important to obtaining buy-in from non-technical executives.

Test expertise and resources: What's the depth and breadth of their testing experience? Is testing part of their core business?

What testing resources does the company use? Do they have expertise in simulating real-world conditions and generating realistic traffic? It can be helpful if they have experience working with network equipment manufacturers to test traffic thresholds and identify breaking points.

When permitted (in a controlled environment), it's important to put a system under load and flood it; this can push malware/intrusion detection into the background and create a foothold for an attack. It can also be useful to have access to a test cloud that contains thousands of the latest applications. These can generate traffic with authentic payloads to test a network under realistic conditions.

Elements of a Pentest

As you work with your pentest partner to design a comprehensive test plan, here are elements, or test aspects you are likely to discuss and consider:

Where to test

- External: Tests and attacks on the perimeter are conducted from outside a firewall
- Internal: Tests and attacks are conducted from behind firewall or using VPN; this includes application-layer and network-layer tests, described below. Usually, both external and internal phases are typically part of a pentest
- Application-layer: This identifies insecure application design and configuration
- Network-layer: Automated tools probe the infrastructure's configuration and reveal attack surfaces, or potential targets for attack

Types of tests

Three types exist and are based on set-up, and how much prior information a tester has. They are as follows:

- Black-box: Client provides tester with no prior information about environment. This can help reveal what is discoverable and should be better shielded.
- Grey-box: Client provides tester with some information. This can help ensure certain aspects of the infrastructure are tested, but also reveal what is discoverable from the outside.
- White-box: Client provides tester with extensive information about environment. This can result in a worst-case attack that puts maximum pressure on security defenses.

Scoping

The test team and client set goals and outline the systems to be tested

Discovery

The test team probes all paths into the network, including:

- Backdoors, legacy systems, disabled security, outdated patching, weak password policies, exposed back-up data, unused and unnecessary services
- Lack of controls and authentication, ability to escalate privileges and install malware
- Social engineering attacks on personnel to harvest information and credentials

Attack & Exploitation

The test team uses creativity to exploit and attack discovered vulnerabilities and spotlight the maximum severity of risk that each vulnerability represents

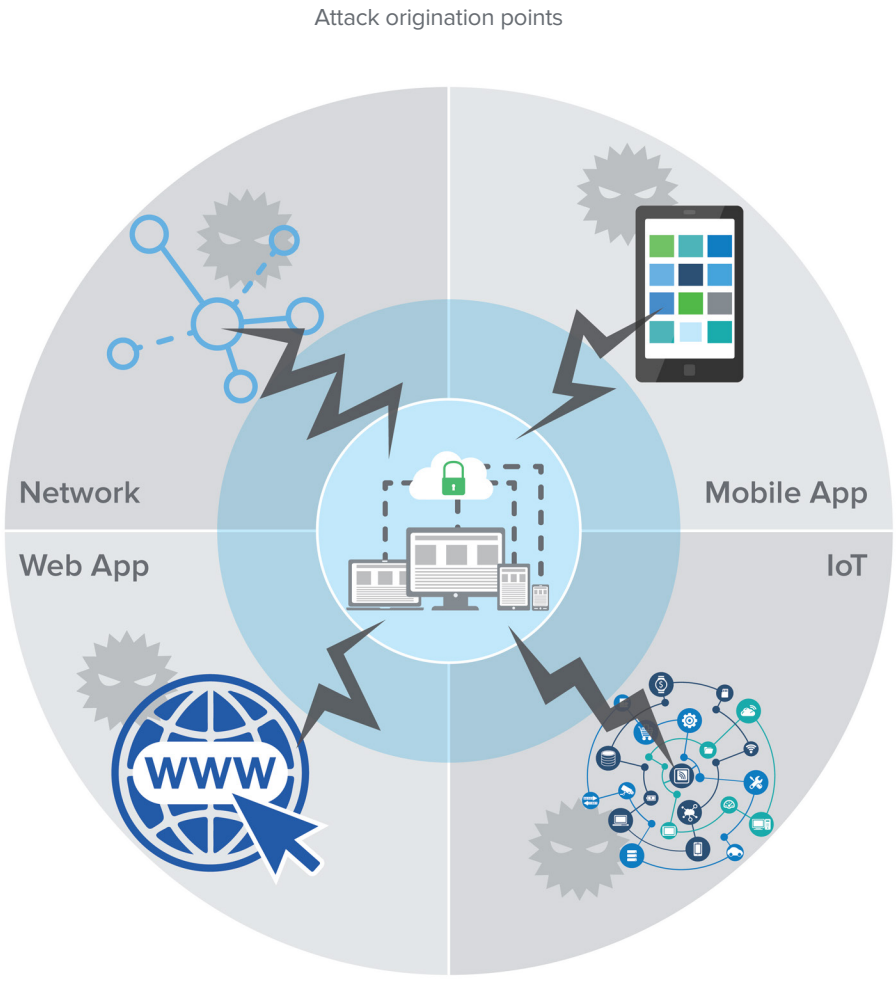
Post Exploitation

The test team methodically uses privilege escalation to pivot from compromised systems and gain additional access to systems and resources

Reporting

The test team lists and prioritizes risks and vulnerabilities, suggesting remediation for each discovered vulnerability

Pentesting: The Required Human Ingenuity to Uncover Security Gaps



Each type of environment offers unique vulnerabilities to explore.

SCADA attacks

Supervisory control and data acquisition (SCADA) networks are rich targets, not just because they control our electricity, natural gas, gasoline, water, waste treatment, and transportation networks, but also because they are especially vulnerable.

Most SCADA networks contain legacy equipment designed for efficiency and reliability, but not for security. Security solutions typically have been bolted-on, and that tends to introduce additional points of vulnerability.

As reported by CNBC, a hacktivist group, for instance, claimed responsibility for a cyberattack that gave them access to the control system for a dam in the suburbs of New York. An intruder accessed and read files—including user names and passwords—six times over a month-long period. The hackers never manipulated the dam, but they might have tried. Luckily, the controls to open the sluice gate, which was built in the 1940's, never fully worked. One U.S. Senator called the attack "a bucket of ice water to the face."

Some SCADA networks, unlike the dam, may be completely separate from the Internet, but this can give a false sense of security. Telecommunications networks offer many backdoors and holes; communications can be hijacked and reverse-engineered, for example, and re-routed in man-in-the-middle attacks.

Third-parties such as business partners, vendors, and regulatory agencies often have access privileges to SCADA networks, and their access can be exploited. An attacker might physically survey remote, unguarded sites for live network access points, or identify cables that can be tapped, or radio and microwave links that can be compromised.

Weak passwords can be brute-force attacked. An attacker breached one unnamed public utility through its control system network using a brute force attack on its remote access capability.

The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported they responded to 245 attacks in 2014, with one third of these against the energy sector.

Attackers can look for a vulnerability such as the use of a very small aperture terminal, or VSAT. This is a small satellite dish-based computer system that provides broadband Internet access to remote locations; or it transmits point-of-sale (POS) credit card transactions, SCADA or other narrowband data.

Computerworld reports that 2.9 million active VSAT terminals are in use worldwide, with many serving the defense, financial, and industrial sectors to transmit sensitive and classified data. More than 10,000 of those devices are "open" for targeted cyber-attacks, with telnet access and weak or default passwords.

Internet of Things (IoT) attacks

A report from a global telecom predicts there will be more than 5 billion IoT devices by the end of this decade; a fourfold growth in just the next four years. One example of this proliferation is the sensors inside industrial control equipment that send notification alerts when parts need replacing. Even our garbage is online with wireless reporting capability that notifies how full trash cans are, and whether or not a pick-up is required.

The reason for rapid IoT growth is simple: when devices are connected, they create exponential value by communicating with each other. Cars and drones can be autonomous. A kitchen can replenish its food supplies. Networks of devices can learn from us and each other to boost our productivity and better suit our needs.

With the growth of the IoT, however, there are many new attack surfaces. One security researcher showed that a wireless hack from a powerful antenna half-a-mile away could remotely control an insulin pump and potentially kill a victim. Others have used successful brute-force attacks to find the unique code of a car's key fob, or listen and watch children by hacking web-enabled baby monitors.

An attacker will probe IoT devices for vulnerabilities such as remote code execution, unauthorized access, authentication bypass, or stealing unencrypted data or any personally identifiable information (PII.)

An attacker will also look for weaknesses in device firmware, the ability to download unsigned updates, or the use of low-security FTP protocol, etc.

Pentesting: The Required Human Ingenuity to Uncover Security Gaps

Lack of strong passwords is an obvious but common IoT device vulnerability. A security analyst found 10 out of 10 security systems accepted “123456” as a password. In another demonstration project, a website allowed access to 73,000 security camera locations that had been hacked because they used default passwords.

Network attacks

An article in Network World points out that network attacks are more likely to exploit older vulnerabilities than newer ones. The report found that 44 percent of breaches came from vulnerabilities that are two to four years old. Server misconfiguration is a top attack vector, and one of the main vulnerabilities that a tester will look for.

Once an attacker gets access to a network, he/she can begin to search for files and data, attempt to steal login credentials, execute brute-force password attacks, hack accounts, escalate privileges, infect a system, intercept network traffic, and scan network devices.

The attacker will download utilities to execute these steps, and try to shield them by masking the code in high traffic, downloading them in sections, or obfuscating or encrypting the code. Malware can even be masked within audio/video files or images.

Remote access and virtual private networks (VPNs) are important to businesses, and they’re useful to attackers. Many businesses don’t restrict access to authorized parties or keep VPN software up to date. Other networks such as some ATM terminals have components with insecure operating systems such as Windows XP.

An attacker looks within a network for privileged accounts and credentials that can still exist for employees who have left. It’s also common to find sensitive data unencrypted.

Weak administrator passwords, or shared local administrator passwords are two typical network vulnerabilities. Some network administrators set up an easy password for a new employee to use and change, but many employees don’t change it, or employees aren’t forced to change passwords because businesses don’t have password expiration dates.

Another attack vector that is useful in legacy networks is Link-Local Multicast Name Resolution (LLMNR) poisoning. This uses the LLMNR protocol in Microsoft Windows Vista and Server 2008 to enable access to internal networks.

Web App attacks

The web application layer is one of the most accessible attack vectors, and it is the hardest to defend. The magazine eWeek reports that SQL injections are responsible for 8.1 percent of all data breaches. An attacker will probe to see if SQL database commands can be injected into a data entry field, and cause a web application to deliver data, destroy data, plant malicious code, delete tables, or remove users.

Attackers also send phishing links via a cross-site scripting (XSS) attack. This can cause the relay of malicious scripts through a vulnerable application from an otherwise trusted URL. The goal is to compromise information such as the session data maintained in the victim’s browser.

Attackers explore whether an application accepts invalid parameters. If it does, they will try a command injection attack. This can make the application convey unsafe user-supplied data (forms, cookies, HTTP headers) to a system shell. The attacker can then execute operating system commands using the privileges of the vulnerable application.

It's also common for attackers to check for:

- Lack of server-side validation
- Failure to expire the session on the server side when a user logs out or session expires on client side
- Unencrypted credentials, identifiers and other data
- Error messages or form caching that reveal useful information
- Out of date patches on web server
- Ability to change authentication level without needing a re-issued Session ID, enabling privilege escalation

A major telecommunications company reviewed data breaches in 2014, and observed that authentication and input validation attacks were not only reliable attack vectors, but were also quick and easy, with 60 percent of the compromises taking a few minutes or less.

Mobile App attacks

How popular are mobile apps? Users will have downloaded more than 100 billion of them worldwide between 2009 and 2017, projects Statista.com. The number of mobile users and time they spend on their mobile devices surpassed desktop users and desktop use for the first time in 2014, making mobile the leading channel for being online, according to smartinsights.com.

To meet the high demand for mobile applications, many organizations port their traditional applications to mobile too quickly, and many vulnerabilities result.

An attacker will probe a mobile application to see if it contains any of the following:

- Excessive permissions
- Unsecured data in transit
- Mobile device management capabilities that can be exploited
- Keys that are accessible with a mobile forensics tool
- Extractable data such as contacts, location, and archives
- Hard-coded sensitive information stored in .plist or .xml files

Attackers will also see if a mobile application can be

- Triggered by code injection to reveal protected information
- Accessed with a jail-broken device
- Tricked into horizontal and/or vertical privilege escalation attacks

Mobile traffic is more likely to be vulnerable than other types of network traffic because it travels through the air. Attackers sometimes use a fake cell tower or rogue base station to attract connections from targeted devices, as part of a man-in-the-middle attack.

.

White Paper

Pentesting: The Required Human Ingenuity to Uncover Security Gaps

A day in the life of a pentester

Sameer Dixit
Senior Director Security Consulting

Sameer is a leader in cyber security with over 15 years of experience in penetration testing and security research. At Spirent, Sameer is leading the ethical hacking and security research team called Spirent SecurityLabs.

Prior to Spirent, he has worked for leading security companies such as Trustwave-SpiderLabs and Cenzic Inc. where he led the penetration testing, vulnerability scanning and managed security testing services team

"No two pentesting engagements are ever the same," says Sameer. "There are surprises and unique challenges and frustrations. And there is almost always an 'ah-ha' moment."

When asked about his formula for getting inside a network, Sameer says there isn't one:

> *"A pentester might use various tricks such as a cross-site scripting, SQL injection, a man-in-the-middle attack to capture a user's session cookie, or a social engineering attack that gets someone to click on a link. The link can transparently download malware such as a key logger, or code that leads to remote control of the system. With roughly 70 to 80 percent of pentests revealing at least one critical vulnerability in the client's infrastructure, it's deeply satisfying to bring vulnerabilities to light"*

spirent.com

AMERICAS 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

EUROPE AND THE MIDDLE EAST
+44 (0) 1293 767979 | emeainfo@spirent.com

ASIA AND THE PACIFIC
+86-10-8518-2539 | salesasia@spirent.com

Because so many attacks begin with insiders, Sameer advises, every organization should use a system of checks and balances to control their users. "I always look to see if those checks and balances are missing," he says.

Many clients recognize the importance of pentesting and minimize the rules constraining the tester. They are quite clear that their best defense is a good offense, Sameer notes. "Some clients tell us to go ahead and do anything, as long as we don't remove any sensitive information," he says.

Even the same vulnerability presents different challenges in different infrastructures, Sameer adds. "The persistence, determination, learning, and creativity that are required every day make this the best job I've ever had."

Knowing your weakness is a major strength

Digital code is arguably the most powerful medium we've ever had. It can capture and share a surprising percentage of who we are and what we know. It can also help us explore what is still beyond our awareness.

Our thoughts, dreams, and memories; art and science; image, word and sound; finances and formulas; and music and poetry can be captured in digital code. And soon, perhaps, it will help us map and conceptualize dark matter and dark energy, the 95 percent of the universe not yet visible or understood. So much can be conveyed with binary sequences of one and zero, positive and negative, presence and absence, on and off.

Digital code is helping billions of people connect and collaborate across distance, time, and culture. It's being used individually and in groups to help build knowledge, wealth, and value faster and in more creative ways than we ever thought possible.

Although digital code is amplifying the best of humanity, it is also amplifying the worst. It can be used to build your organization, and it can be used to destroy it.

By showing you the worst that digital code can do, periodic pentests are your best defense for all that digital code has to offer

Rev A. | 01/16