ISACA

Physical Penetration Testing: The Most Overlooked Aspect of Security

Information Security

CONTENTS

ABSTRACT

This white paper offers a comprehensive overview of physical penetration testing, an often neglected yet crucial component of cybersecurity. It examines the definition of physical penetration testing and highlights its distinctions from other forms of penetration testing. It emphasizes the significance of physical security by exploring its potential advantages for companies, especially those in regulated industries, and addresses the challenges associated with its implementation. Additionally, it provides an exploration of the methodologies and tools employed by physical penetration testers throughout the process of breaching organizations by accessing their secured buildings.

Introduction

With the rapid growth of technology, cyberthreats have become increasingly sophisticated and complex, making it difficult for organizations to keep their sensitive data and critical assets secure. These bad actors' or hackers' motives range from political "hacktivism" to financial gain or fame. To stay ahead of hackers, security professionals have adopted the mindset and tactics of their adversaries.

Penetration testing, commonly known as "pen testing," is a simulated cyberattack designed to evaluate the security of a system, network or application to identify potential risk. As a result, penetration testing has become an essential tool for organizations to identify vulnerabilities in their systems and improve their security posture.

However, as technology advances, so do the methods of attackers. In addition to cyberthreats, physical threats can also be used as a way to exploit vulnerabilities and gain unauthorized access to systems and data.

Pro-Vigil's annual research survey reveals that 28 percent of respondents saw an increase in physical security incidents in both 2021 and 2022, up from just 20 percent of respondents in 2020.[1] According to the 2023 Data Breach Investigations Report (DBIR) from Verizon, "74 percent of breaches involved the human element, which includes social engineering attacks, errors or misuse."[2]

Physical Penetration Testing

Physical penetration testing involves simulating a physical attack on an organization's premises, such as a building, data center or server room.

This type of testing evaluates the physical security measures put in place to safeguard assets such as hardware, confidential information and personnel.

Physical penetration testing is designed to identify weaknesses in the physical security controls of an organization and simulate how a real attacker would try to gain access to restricted areas or information. This type of testing may include using social engineering techniques (such as impersonating an employee), attempting to enter restricted areas without authorization or stealing company assets.

Physical penetration testing is designed to identify weaknesses in the physical security controls of an organization and simulate how a real attacker would try to gain access to restricted areas or information.

This can be achieved through various means, such as covertly entering through a back door, disguising oneself to blend in with authorized personnel or taking advantage of a distraction.

However, most professionals in the physical security consulting industry would agree that gaining physical access to an organization's buildings is much easier than what we see in the movies. This is why, in today's rapidly changing threat landscape, regular physical penetration testing is essential for maintaining a strong security posture.

Methods of testing

When comparing physical penetration testing to network penetration testing, there are notable differences in scope and execution. Network penetration testing primarily focuses on identifying vulnerabilities and weaknesses

1 Pro-Vigil, "*The State of Physical Security Entering 2023*," https://pro-vigil.com/resources/2023-security-survey-report/
2 Verizon, "*2023 Data Breach Investigations Report*," https://www.verizon.com/business/en-au/resources/reports/dbir/

in digital systems, networks and software. It involves simulating cyberattacks to assess the security posture of an organization's digital infrastructure.

The following testing methods exist for physical penetration tests:

Social Engineering

Social engineering is the practice of manipulating people into divulging sensitive information or performing an action that allows an attacker access to a secure area. This can be accomplished through various tactics such as sending phishing emails or vishing calls to employees and tailgating employees through access-controlled areas.

The incorporation of social engineering techniques distinguishes physical penetration testing from other forms of cybersecurity and penetration testing methodologies. This form of testing aims to assess the vulnerabilities present in both physical infrastructure and employees.

The incorporation of social engineering techniques distinguishes physical penetration testing from other forms of cybersecurity and penetration testing methodologies.

Consequently, these attacks reveal weaknesses that exist both externally (in the physical realm) and internally (among the employees). Simply put, computers communicate without emotion in binary: 1's and 0's, yes or no, open or closed. Humans, however, weigh decisions based on emotion.

Will an employee who did not get a promotion yesterday challenge the delivery person walking behind them through the badge-accessed turnstile today?

Will an employee unaware of the risks try to "help out" a bad actor with a convincing story who asks for a password over the phone?

Through social engineering testing, organizations can determine where their employee awareness training is working and where more attention is needed to help prevent future physical and cyberbreaches.

Social Engineering Methods

Here are some social engineering methods physical penetration testers may use to gain access to a building:

- **Impersonation**—A social engineer may impersonate someone who has legitimate access to the building, such as a delivery person, IT technician or employee. They may dress the part and act confidently to convince security personnel or other employees to let them in.
- **Tailgating**—This involves following an authorized person into a secure area without presenting credentials or gaining proper authorization. The social engineer may act as if they are in a hurry or have a legitimate reason to be there. This can take the form of someone purposefully having their hands full and asking for the door to be held by an employee or conversely offering to hold the door to quickly gain the trust of the employee.
- **Phishing or Vishing**—A social engineer may send phishing emails or make phishing phone calls (vishing) to employees, pretending to be someone else and asking for sensitive information or passwords. With this information, the social engineer may be able to bypass security measures and gain access to the building.
- **Pretexting**—This involves creating a false scenario to gain access. For example, a social engineer may pose as a member of the IT department and contact an employee, claiming that there is a pressing issue with their computer that necessitates their immediate presence in the IT office. Once the employee arrives, the social engineer may be able to gain access to the building or sensitive areas within the building.

Social engineering attacks can take many forms and can be difficult to defend against because they exploit human weaknesses rather than technical vulnerabilities.

Nevertheless, it is imperative for individuals and organizations to remain vigilant about the threat posed by social engineering and to take action to protect themselves from these types of attacks.

Here are two real-world examples of social engineering:

- One of the most significant social engineering attacks on record involved a scammer group that targeted two prominent multinational companies. The team devised an elaborate scheme by creating a counterfeit company with the same name as an actual computer manufacturer that regularly did business with these major companies. To execute their plan, the scammers sent out phishing emails to specific employees within Facebook and Google, presenting invoices for legitimate goods and services that the real manufacturer had actually provided. However, the emails cunningly directed the employees to deposit funds into the scammers' fraudulent accounts. Over the course of two years, from 2013 to 2015, the group managed to defraud these prominent tech companies out of more than $100 million.[3]
- In February 2022, amidst escalating tensions between Russia and Ukraine, Microsoft issued a warning about a new spear phishing campaign conducted by a Russian hacking group known as Gamaredon,[4] which has actively targeted Ukrainian government agencies and non-governmental organizations. This group, identified by Microsoft by the name Actinium, has reportedly focused on infiltrating organizations crucial to emergency response and the security of Ukrainian territory since 2021. The attack strategy employed by Gamaredon involves the use of spear phishing emails embedded with malware. Additionally, these emails incorporate a tracking pixel, enabling the cybercriminals to monitor whether the email has been opened. This incident serves as a significant reminder of the prominent role cybersecurity now plays in international conflicts. It underscores the importance for all organizations to enhance their security measures and safeguard against social engineering attacks. By prioritizing cybersecurity, organizations can fortify their defense mechanisms and mitigate potential risk associated with such targeted campaigns.[5]

Physical/Technical Bypass

In addition to social engineering, physical penetration testing involves the use of tools and techniques that can bypass physical or technical security measures. This aspect of testing aims to uncover vulnerabilities in locks, access control systems and other security mechanisms that could be exploited by adversaries.

By understanding the methods that adversaries might employ to gain unauthorized access, organizations can take proactive steps to mitigate such risk.

One common method of bypassing physical security measures is lockpicking. With this method, skilled testers can demonstrate how easily traditional locks can be manipulated or bypassed, highlighting the need for more robust locking mechanisms. Another bypassing technique is radio-frequency identification (RFID) cloning, where testers clone RFID cards or badges to gain unauthorized access to secured areas.

Similarly, Bluetooth hacking can be employed to exploit vulnerabilities in Bluetooth-enabled security systems, granting unauthorized entry to restricted spaces. While the methods mentioned are some of the more common approaches to physical penetration testing, there are numerous other techniques designed to simulate a physical exploit.

Destructive vs. Nondestructive Testing

Covert entry is another widely accepted approach among the physical pen testing community. In gaining entry, it is understood by these professionals that they should be as nondestructive as possible.

Therefore, all entry methods, such as bypassing doors and locks, should be employed without causing any damage.

3 Romo, Vanessa; "*Man Pleads Guilty To Phishing Scheme That Fleeced Facebook, Google Of $100 Million*," NPR, 25 March 2019, https://www.npr.org/2019/03/25/706715377/man-pleads-guilty-to-phishing-scheme-that-fleeced-facebook-google-of-100-million
4 UA.gov, "*Gamaredon carried out 74 cyberattacks against Ukraine in 2022*," 17 March 2023, https://cip.gov.ua/en/news/gamaredon-carried-out-74-cyberattacks-against-ukraine-in-2022
5 Tessian, "*15 Examples of Real Social Engineering Attacks*," 7 February 2023, https://www.tessian.com/blog/examples-of-social-engineering-attacks/

Testers sometimes exploit preexisting vulnerabilities in locking mechanisms. They may also exploit weaknesses in building codes or the technical functions of physical security measures, usually attempting to operate as covertly as possible.

The objective of this methodology is twofold:

1. Cause minimal to no damage to the organization
2. Demonstrate how an adversary could compromise the organization virtually undetected

However, it is important to recognize that this nondestructive approach has limitations in terms of providing comprehensive security testing.

According to a *Newsweek* article in December 2022, about 35,000 people in Moore County, North Carolina lost power due to a targeted attack, in which suspects brought down the system by shooting electrical substations. The article mentions similar attacks in other parts of North Carolina, Oregon and Washington "using hand tools, arson, firearms and metal chains in response to an online call for attacks on critical infrastructure."[6]

Physical pen testers strive to think like the adversaries they safeguard against, which means they envision the different destructive ways that potential attackers could disrupt organizations. For example, a tester may simulate an attack by activating or turning off the water in the fire suppression system. This approach, while potentially troublesome for the business, allows testers to identify and address vulnerabilities before malicious actors can exploit them.

Advanced Persistent Threats

Advanced persistent threats (APTs) can utilize physical means to breach an organization's security. While APTs are commonly associated with sophisticated cyberattacks targeting networks and systems, they can also employ physical tactics to gain unauthorized access or compromise sensitive information.

Physical penetration techniques, such as social engineering, covert entry and tailgating, can be used by APT actors to bypass physical security measures and gain physical access to restricted areas. These are targeted attacks that are designed to remain undetected for long periods.

For example, an APT actor may impersonate an employee or contractor, using social engineering techniques to gain entry to a secure facility. Once inside, they can plant malicious devices, tamper with equipment or conduct reconnaissance to gather valuable information for further exploitation.

By incorporating physical tactics into their overall attack strategy, APT actors can increase their chances of success and evade detection. This highlights the importance of considering both physical and digital security measures in an organization's overall security posture.

By incorporating physical tactics into their overall attack strategy, APT actors can increase their chances of success and evade detection.

There have been known cases where APT actors have utilized physical means as part of their attack strategies. One notable example is the Stuxnet worm, which was discovered in 2010 and attributed to a joint effort by intelligence agencies, likely including the United States and Israel.

Stuxnet was designed to target Iran's nuclear program and specifically aimed at compromising industrial control systems (ICS) used in uranium enrichment. The worm is believed to have been introduced physically into the Natanz nuclear facility, possibly through an infected USB drive or other means, and then propagated within the facility's network to disrupt its operations.[7]

This example demonstrates the potential for APTs to leverage physical means as part of their attack methodologies. It underscores the importance of holistic

6 Rahman, K.; "*Physical Attacks on Power Substations in Multiple States—Report*," *Newsweek*, 7 December 2022, https://www.newsweek.com/physical-attacks-power-substations-multiple-states-1765225
7 Malwarebytes, "*What is Stuxnet?*," https://www.malwarebytes.com/stuxnet

security approaches that consider both digital and physical vulnerabilities to defend against these persistent and evolving threats.

Types of Physical Penetration Testing

Physical penetration testing can be performed by a dedicated team or a third-party vendor that specializes in physical security assessments. Many cybersecurity consulting firms offer physical penetration testing services to organizations looking to evaluate their physical security measures.

Often, organizations request a physical penetration test alongside network and application penetration testing. The type of test agreed on by the organization and the testing firm will vary depending on several factors such as:

- Budget
- Scope of the engagement
- Inside information provided by the organization

These factors will affect how long the engagement runs, how many vulnerabilities are discovered and the authenticity of the test.

There are various types of physical pen tests, just like there are various types of network pen tests, and the definitions are quite similar. Because of the disruptive nature of some tests, the comfort level of the organization may play a part in determining which types are right for them.

Red Team

Red teaming typically involves a comprehensive and systematic approach, employing various methodologies and techniques to simulate real-world threats. The team may engage in activities such as penetration testing, social engineering, physical security assessments or even scenario-based simulations to evaluate an organization's ability to detect, prevent and respond to potential attacks or breaches.

The red team typically operates independently from the organization's internal security teams, allowing for an unbiased and objective evaluation of the security infrastructure. This approach helps to uncover blind spots and weaknesses that might be overlooked by internal teams who are more familiar with the system's design and limitations.

Black Box

A black box physical penetration test means there is very little to no information and/or access provided by the organization for the locations being tested. Typically, during a black box test, the testers would only be provided with the address(es) of the building(s). This type of testing would be closer to simulating a real-world adversary with little information provided, but the exercise would typically be more thorough than red teaming.

White Box

A white box physical penetration test means the organization provides the testers with comprehensive information and access to the locations being tested, including known vulnerabilities, technologies used and building layouts. This type of test would increase the testers' chances of success and the thoroughness of the vulnerabilities tested, thereby expediting the information-gathering part of the test and ultimately saving the organization money.

Gray Box

As indicated by the name, gray box testing is somewhere in the middle of white box and black box testing. A gray box physical penetration test means that the organization provides limited information and/or access to the testers. An organization may want to provide certain information to help speed up the testers' information-gathering process while still wanting the authenticity of the test to remain intact.

Due Diligence Assessment (Walkthrough)

Due diligence is not technically classified as a pen test. Rather, it is a more budget-friendly alternative for enterprises looking for many of the same benefits. A due diligence assessment is an authorized, often escorted,

walkthrough of the corporation's locations in which a testing provider identifies potential vulnerabilities that an adversary might exploit. This approach is a more efficient way to discover vulnerabilities and gives the corporation first-hand training, but it lacks the authenticity of testing the organization's security posture in real time.

Tools

Physical pen testers use a variety of tools to assess and exploit vulnerabilities in physical security environments. These tools are designed to aid in bypassing or compromising access controls, surveillance systems and other physical defenses.

Here are some common tools used by physical pen testers:

- **Lockpicking/Impressioning Tools**—As touched on earlier, lockpicking is a technique used to bypass physical locks. Physical pen testers may use lockpicking tools such as picks, tension wrenches and jiggler keys to manipulate lock mechanisms and gain unauthorized access. Impressioning is a technique used to create a working key for a lock by making an impression of the lock mechanism. Physical pen testers may use impressioning tools such as key blanks, files and impressioning materials to create a key that can open a lock without ever having access to the original key.
- **Bypass Tools**—Bypass tools are specifically designed to overcome or bypass security measures such as alarm sensors, motion detectors or other physical barriers without triggering an alert. They help pen testers identify vulnerabilities in alarm systems and test their effectiveness. These tools include different-sized thin metal rods bent in various shapes to quickly unlock and open doors from the outside without the need of a key.
- **RFID Tools**—As mentioned earlier, RFID tools are used to interact with RFID-based access control systems. These tools can scan and read RFID cards or badges, detect vulnerabilities in the system and even clone or emulate RFID credentials for unauthorized access.
- **Disguise and Social Engineering Tools**—Physical pen testers often employ tools and props to disguise themselves as authorized personnel and aid their social engineering efforts. These may include fake IDs, uniforms, badges, props related to the role they are impersonating (e.g., a dolly for a delivery person) and other items to enhance their credibility and deceive security personnel or other employees.

Physical pen testers must stay informed regarding new lock mechanisms and other security technologies, practice their social engineering methods and continuously refine their techniques to effectively bypass physical security measures, as these abilities tend to deteriorate over time.

Improvised Tools

Many of the tools previously mentioned originated from prototypes. In certain situations, there may not be an existing tool that fits the specific requirements for a test, necessitating the creation of a new one. This is particularly true in high-security facilities where measures like x-ray scanners and metal detectors are implemented to prevent theft and ensure safety. In such cases, physical pen testers must rely on their creativity.

It is common for physical pen testers to utilize discarded items found in the organization's dumpster to bypass door locking mechanisms. Additionally, they recognize that vulnerabilities can exist due to fire codes and other building regulations. Armed with this knowledge, testers improvise and develop tools that exploit these weaknesses effectively.

Physical pen testers understand the importance of thinking outside the box and adapting to unique circumstances. Their ability to creatively address challenges and develop innovative solutions distinguishes them in the field of penetration testing.

Physical Penetration Testing Methodology

Physical penetration testing methodology typically aligns closely with widely accepted network penetration testing frameworks, such as the Open Web Application Security Project (OWASP) Testing Guide[8] and the Penetration Testing Execution Standard (PTES).[9]

These network pen test frameworks provide comprehensive guidelines and methodologies for assessing the security of digital assets, including web applications, networks and systems. While network penetration testing or industry specific frameworks may mention the implementation of physical security controls, the requirement for testing those controls is rarely, if at all, emphasized.

While network penetration testing or industry specific frameworks may mention the implementation of physical security controls, the requirement for testing those controls is rarely, if at all, emphasized.

Although there may not be as many widely recognized frameworks specifically tailored for physical penetration testing, the methodology used in physical pen testing draws upon the principles and practices established in network pen test frameworks. This ensures a systematic and comprehensive approach to evaluating an organization's security posture from both the digital and physical perspectives.

Skilled testers, leveraging their expertise, experience and specialized tools, meticulously assess an organization's physical security measures within a structured framework, as explained later.

Pre-Engagement

The pre-engagement phase is probably the most important part of the physical penetration testing engagement. When initiating discussions with an organization as a penetration tester, it is essential to first identify the organization's needs and objectives. This includes understanding their desired outcomes from the test, the goals they wish to achieve and any specific threats or scenarios they are concerned about. Additionally, it is important to determine whether the test is being conducted to fulfill regulatory requirements. These inquiries form the foundation for constructing a successful penetration test that meets the organization's needs and addresses their concerns.

Scoping

Scoping is a discussion back and forth between the testing firm and the hiring organization about the detailed nature of the test. The scope defines the boundaries, objectives and constraints of the testing activities. It includes identifying types of tests and locations, along with any specific testing methodologies or scenarios to be followed.

Through scoping, the organization should develop a clear idea of what they are looking for from the testing process and ultimately how much it is going to cost them. The testing firm, meanwhile, is trying to understand the organization's needs, the best ways to address those needs, how long the process will take and what level of resources will be required.

8 OWASP, *Open Web Application Security Project Testing Guide 4.0*, 2014, https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf
9 Penetration Testing Execution Standard, 2014, http://www.pentest-standard.org/

Cost

The cost of a physical security assessment can vary significantly, influenced by several factors that shape the scope and complexity of the engagement. The average cost of a penetration test can vary from $4,000 for a small, unsophisticated organization to more than $100,000 for a large, complex one.[10] However, it is important to note that these figures are approximate and subject to adjustment based on specific requirements.

One key factor for pricing is the type of test being conducted. Different types of tests, such as comprehensive facility assessments, targeted vulnerability assessments or specific component evaluations, may entail different levels of effort, resources and expertise, thereby impacting the overall cost.

The number of locations to be assessed also plays a role in determining the price. Organizations with multiple facilities or branches require a broader scope of assessment, involving additional time and resources to thoroughly evaluate the physical security measures across various sites. The complexity and size of each location further influences the effort involved, contributing to the overall cost.

It is worth noting that pricing can also be influenced by other factors, such as the reputation and expertise of the testing provider, any specific customization or additional services requested by the organization and the duration of the engagement.

Rules of Engagement

The rules of engagement (RoE) serve as a guiding framework that outlines the rules, limitations and expectations for the testing process. It establishes the agreed-upon parameters and norms of conduct between the testing team and the client organization.

The RoE help ensure that physical pen testing is conducted in a controlled and ethical manner, minimizing potential disruptions to normal operations and preventing any unauthorized access to sensitive areas or assets. It defines the objectives of the test, the allowed techniques and tools and any off-limits areas or assets that should not be compromised during the assessment.

By establishing clear and comprehensive RoE, both parties can align their expectations and ensure a smooth and effective testing process. The RoE help to prevent misunderstandings, mitigate legal and ethical risk and promote a collaborative approach to achieving the desired outcomes. Does the organization want the testers to simply try to get past the front desk and then stop, or continue up to the server room? Does the organization want the testers to attempt to gain "unauthorized" access to the network? These are the types of questions that should be addressed in the RoE.

Authorization

Authorization for a physical penetration test is a critical aspect of the testing process, ensuring that the test is conducted legally, ethically and with the explicit consent of the client organization. Authorization documents that consent, which is what testers need to access the organization's premises, facilities and assets for the purpose of conducting the physical penetration test. This may include obtaining access to restricted areas, testing security systems and interacting with employees or personnel during the assessment.

Authorization for a physical penetration test is a critical aspect of the testing process, ensuring that the test is conducted legally, ethically and with the explicit consent of the client organization.

The authorization process typically begins with the creation of formal documentation, such as a written agreement or contract, outlining the scope, objectives and RoE for the test. This document, commonly known as a "Get Out of Jail Free" letter, clarifies the purpose of the test, the identity of the testers, the activities that will be performed, the expected outcomes and any limitations or restrictions that the testers need to follow.

10 Manship, R., "*How Much Does Penetration Testing Cost?*", RedTeam Security, https://www.redteamsecure.com/blog/how-much-does-a-penetration-test-cost

It is essential that authorization be obtained from the appropriate stakeholders within the organization, including management, security personnel and legal representatives. These individuals have the authority to grant permission for the physical pen test and ensure that it aligns with the organization's goals, policies and legal obligations.

The pre-engagement phase as a whole is crucial for understanding the organization's needs and objectives, which lays the foundation for a successful penetration test. Scoping, cost, RoE and authorization are each essential; together, these elements contribute to a well-planned and -executed physical security assessment, promoting effective risk mitigation and protection of critical assets.

Information Gathering Using OSINT and Surveillance

Open source intelligence (OSINT) plays a crucial role in physical penetration testing, as it enables the gathering, analysis and interpretation of publicly available information. By using tools such as Google Maps and Street View, testers can leverage OSINT to identify nearby facilities such as businesses and parking garages, which may serve as potential surveillance points or access points for client facilities.

Physical penetration testers may also discover online videos and pictures that reveal information about security measures in place. For example, searching for pictures of employee badges from company events on social media or the company website can expose the design and features of the badges, potentially facilitating unauthorized access.

Another powerful means of gathering of OSINT is to analyze LinkedIn profiles to identify positions and titles within the organization, enabling targeted social engineering attacks.

While OSINT and surveillance are different, they can both be categorized under the information gathering portion of a traditional pen test. The key distinction between network penetration testing and physical penetration testing is that the former is conducted remotely using a computer, while the latter involves on-site testing in the presence of others. Surveillance represents the on-the-ground information gathering component for physical pen testing. Testers not only validate and verify the information discovered during OSINT, but also actively seek out additional vulnerabilities and methods of entry through discreet observation.

The key distinction between network penetration testing and physical penetration testing is that the former is conducted remotely using a computer, while the latter involves on-site testing in the presence of others.

During surveillance, testers utilize various tools such as cameras, binoculars and disguises to discreetly gather information on the target location, the people around it and any ongoing activities. Surveillance requires patience, and it should be focused on ingesting as much information as possible to enable testers to devise multiple methods for breaching the target building.

The most important part of surveillance is to "build a "pattern of life" for the target. Doing this requires observing and documenting the routines, behaviors and activities of individuals and groups on site. By understanding the regular patterns and habits of employees, cleaners, security personnel and deliverers, the tester can uncover potential vulnerabilities and exploit them effectively.

For physical pen testing, blending in with the environment is crucial. This can take the form of dressing appropriately for the weather to maintain comfort during long periods of standing or walking, but it also means dressing in a way that seamlessly blends with other people in the area.

It is important to note that actions taken during OSINT and surveillance are completely passive; it would not be considered illegal if a random person were to collect this type of information. That leads us to the next step, reconnaissance.

Reconnaissance

At this stage, testers transition to the active phase of the engagement. Any actions taken beyond this point without explicit permission from the organization could potentially be deemed unlawful. Reconnaissance, or "recon," is a gray area between surveillance and execution.

During the reconnaissance phase, the primary goal is to gather information. However, the tester will also actively probe the organization and its security measures. While the tester might use an opportunity to attempt to enter the building to meet the objectives of the engagement, the main purpose of the reconnaissance stage would be to obtain more information to solidify entry possibilities later on. The tester might, for example, dumpster-dive to not only try to find sensitive information that has been thrown out, but also to determine response time from security personnel. This exercise could help answer questions such as: Is the organization actively monitoring the cameras pointed toward the trash? Are there any cameras at all?

A more in-depth example would be a tester posing as a delivery person with supporting fake documentation such as a delivery invoice and order forms. The delivery would be to a targeted employee—possibly one found on LinkedIn. The tester would go to the front entrance to make the delivery, but also to get up close and personal to absorb more details about the organization such as visitor policy, badge information and security measures. The tester would use this opportunity to perform social engineering on the security guard or front desk personnel, whether to gain sensitive information or to access secured parts of the building. Just as a determined adversary would, a tester might make their fact-finding mission that much more valuable by wearing a hidden camera to record the entire interaction for later review.

However, if the opportunity arises, the tester might intentionally go to a delivery entrance at the back of the building rather than the front, looking for better means of entry. If the delivery entrance is unmonitored, the tester might explore the building and gather more information. Additionally, the tester might employ a tactic such as placing a piece of tape across a latch on a back door to circumvent the locking mechanism and establish a means of reentry at a later time.

Execution or Exploitation

The culmination of all preparatory efforts is the execution phase, where plans are put into action. Physical pen testers will take all the information gathered—whether provided by the client, found through OSINT or discovered during recon—and then devise ways to enter the building and compromise the organization. Upon completion of all necessary preparation, the plan is put into action and testers attempt to gain unauthorized access. During this phase, the physical pen testers employ various techniques to execute the break-in.

Here are some examples of how the execution phase may unfold:

- **Fake Delivery**—The physical pen tester poses as a delivery person, carrying a package or parcel, to gain entry into the building. This ruse allows them to blend in with regular deliveries and potentially bypass security measures.
- **Job Interview**—By pretending to be a job applicant, the tester can schedule a meeting or interview at the target location. This gives them an opportunity to access the building and explore sensitive areas under the guise of a prospective employee.
- **Lobby Distraction**—Creating a commotion in the building's lobby area can divert the attention of security personnel or staff. This diversion provides an opportunity for the tester to slip past and gain access to restricted areas.
- **Back Door Bypass**—If a tester happens to get access to a more discreet entrance as discussed in the section on reconnaissance, they might be able to quickly manipulate doors and locks so they can gain entry at a later time without being noticed.
- **Use of Cloned Badge**—If the target organization uses RFID badges or access cards, a physical pen tester might use a cloned or fake badge that matches the organization's security system. This allows them to pass through access control points as any employee would.
- **Shared Building Lease Tour**—If multiple organizations share the same building, a tester can pose as a representative from one of the tenant companies and request a tour of the premises. This

can allow them to gain familiarity with the building's layout and security measures. Additionally, testers can use this opportunity to sneak away from the tour to access the client organization's spaces.

- **Construction or Cleaning Crew**—Impersonating a member of a construction or cleaning crew, the tester gains access to the building by exploiting the trust and credibility associated with these roles.
- **Inspector (Water, Fire, Elevator, etc.)**—In this scenario, the physical pen tester gains access to restricted areas under the guise of conducting inspections or maintenance work. This can be accomplished by posing as a water inspector, fire safety inspector, elevator technician or the like.
- **Late Night Emergency IT Contractor**—Claiming to be an IT contractor responding to an urgent after-hours issue, the tester exploits a manufactured sense of urgency and confusion to gain entry to the building.
- **Piggyback/Tailgate**—In one of the simplest exploits, the tester discreetly follows closely behind an authorized employee who has legitimate access to a secured area. By blending in and appearing as if they belong, they can gain entry without arousing suspicion.

True adversaries—the bad actors that security measures are meant to stop—are constantly seeking new ways to exploit vulnerabilities in a company's physical security.Therefore, physical penetration testers must remain alert to the evolving landscape of physical attacks and stay abreast of the most recent methods and techniques employed by malicious actors.

Data Collection

Data collection is the phase when the physical pen tester gathers valuable information and insights while inside a target building. The objective is to identify potential vulnerabilities, assess the effectiveness of security measures and understand the organization's operational practices.

During the data collection phase, a tester may seek the following key types of information:

- **Physical Security Measures**—The physical pen tester assesses the effectiveness of various security measures, including access controls, surveillance systems, alarm systems and security protocols. They examine the placement and coverage of security cameras, the reliability of door locks, the response time of security personnel and the overall robustness of the physical security infrastructure.
- **Sensitive Areas and Assets**—The pen tester identifies areas within the building that contain valuable assets, sensitive information or critical infrastructure. This may include server rooms, data centers, executive offices, research and development labs or storage areas for confidential documents. Understanding the layout and accessibility of these areas helps in evaluating potential risk.
- **Network Infrastructure**—Testers may also gather information related to the organization's network infrastructure. This could include identifying network cabinets, patch panels, network switches or other networking equipment that may be accessible within the building. Such information can be useful in understanding the potential points of entry for a network-based attack.
- **Employee Habits and Behaviors**—The physical pen tester observes the behavior and habits of employees, including their adherence to security protocols, handling of sensitive information and response to security incidents. This information provides insights into potential weaknesses related to human factors and the organization's security culture.
- **Workflows and Operational Practices**—The pen tester pays attention to operational workflows and practices within the building. This could include observing how visitors are managed, the flow of employees in and out of secure areas, the handling of equipment or assets and the disposal of sensitive documents or electronic devices. Understanding these practices helps in identifying potential gaps or lapses in security procedures.
- **Documentation and Logbooks**—The tester may search for logbooks, visitor records or other documentation that can provide insights into the organization's operations, visitor management protocols or the presence of third-party contractors. These records may reveal vulnerabilities such as lax enforcement of access controls or insufficient documentation practices.
- **Security Policies and Procedures**—The pen tester may look for copies of security policies, procedures or guidelines that are accessible within the building. This information provides

insights into the organization's security posture and helps in identifying potential gaps between policy and practice.

- **Personally Identifiable Information (PII)**—While it is essential for the pen tester to maintain ethical standards, they may come across PII during their data collection. This could include sensitive employee or client information, financial records or confidential business documents.

It is important for the pen tester to handle all information collected with discretion and ensure that it is not misused. The organization has leeway in determining exactly how the test simulates theft of this information.

While some organizations are fine with testers leaving their premises with sensitive information or systems as a proof of concept demonstrating the organization's vulnerability, others may prefer that only a photograph be taken or that the information access simply be annotated in the final report.

Reporting

Upon completion of testing, the testing firm will compile a comprehensive report that includes all findings, vulnerabilities discovered and exploited and a narrative of what testers were able to do during the test and how they did it. The report can also include an executive summary and a technical summary broken down by function so that the appropriate departments within the organization can more easily take action to remediate vulnerabilities.

Benefits of Physical Penetration Testing

Any organization that has sensitive data or critical assets can benefit from physical penetration testing. This includes government agencies, financial institutions, healthcare providers and any other organization that handles sensitive information.

Additionally, companies that rely on physical security measures such as access control systems, security cameras and security personnel would benefit from physical penetration testing. Companies that outsource their data center operations or use third-party providers to store sensitive data should also conduct physical penetration testing to ensure the security of their assets.

Regulatory Compliance

Certain industries are obligated by law to conduct regular evaluations as part of their security practices, and penetration testing is one recommended method for carrying out these assessments.

For instance, healthcare organizations that handle patient data must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which suggests that covered entities and business associates perform regular risk assessments, including physical penetration testing, to identify vulnerabilities and implement appropriate security measures.[11]

Similarly, financial institutions must adhere to the Gramm-Leach-Bliley Act (GLBA),[12] which necessitates regular risk assessments, including physical penetration testing, to safeguard customer data.

Multiple other regulations require organizations to implement physical security measures to protect sensitive data and assets. For example, the Payment Card Industry Data Security Standard (PCI DSS) mandates that organizations handling credit card data establish physical security measures such as access controls, surveillance cameras and alarm systems to safeguard cardholder information.[13]

11 US Department of Health and Human Services, "*Guidance on Risk Analysis*," 22 July 2019, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
12 Code of Federal Regulations, "*Standards for Safeguarding Customer Information*," 16 CFR § 314 (2023), https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314
13 Baykara, S., "*PCI DSS Requirement 9 Explained*," PCI DSS Guide, 7 April 2020, https://www.pcidssguide.com/pci-dss-requirement-9/

Additionally, the International Organization for Standardization (ISO) provides guidelines for implementing physical security controls, including access control, surveillance and environmental controls.

Personnel Safety

Physical penetration testing not only helps evaluate the effectiveness of physical security measures but also plays a crucial role in ensuring personnel safety.

By identifying vulnerabilities and weaknesses in the physical security infrastructure, organizations can take proactive measures to mitigate potential risk to their employees, visitors, customers and stakeholders.

During physical penetration testing, testers assess the response and effectiveness of security personnel in handling unauthorized access attempts or suspicious activities. This evaluation helps organizations identify gaps in training, protocols or procedures that may impact the overall safety and security of individuals within the premises.

Furthermore, physical penetration testing can simulate real-world scenarios, such as intruders attempting to harm or cause disruption to personnel. By testing the response capabilities of security teams, emergency procedures and communication systems, organizations can identify areas of improvement to enhance the overall safety and protection of their personnel.

Data/Asset Protection

Physical penetration testing is instrumental in safeguarding organizations' sensitive data and other valuable assets. While cybersecurity measures are essential, physical security also plays a critical role in preventing unauthorized access or theft of physical devices, confidential documents, intellectual property or other valuable assets.

By simulating attacks on physical security systems and measures, physical penetration testing helps identify potential weaknesses that could lead to unauthorized access or compromise of assets. This includes evaluating access control systems, surveillance cameras, alarm systems and physical barriers such as locks and fences.

Moreover, physical penetration testing provides insights into the effectiveness of policies and procedures related to data and asset protection. This includes testing the adherence to secure data handling practices, secure storage of physical media, secure disposal of sensitive information and physical access controls for data centers or server rooms.

By addressing vulnerabilities identified through physical penetration testing, organizations can implement necessary improvements to enhance the protection of their data and assets, reducing the risk of theft, unauthorized access or compromise.

Challenges of Physical Penetration Testing

Though there are many important benefits arising from physical penetration testing, there are also several challenges that make it difficult to safeguard assets and protect against physical attacks. One of the biggest challenges is the human factor.

Employees, contractors and visitors can inadvertently compromise physical security measures by leaving doors unlocked or propping them open, sharing passwords or keycards and failing to report suspicious activity. Additionally, physical security systems can be vulnerable to technological exploits, such as bypassing access control systems.

Another challenge is the ever-evolving nature of physical threats, as attackers constantly develop new methods and tools to circumvent security measures.

Physical penetration testing can be challenging for organizations due to the complexity of physical security measures and the wide range of techniques used by testers. Some common challenges organizations face during physical penetration testing include:

- **Cost**—Physical penetration testing can be expensive, particularly for large organizations with multiple facilities. Indeed, one of the biggest challenges associated with physical pen testing is resource allocation. As many organizations are aware, penetration testing can yield valuable insights but also requires significant financial investment.
- **Time**—Physical penetration testing can be time-consuming, and organizations may need to shut down certain operations during testing or borrow resources, taking them away from other projects. An organization should carefully think ahead about the time required for planning, executing tests, analyzing results and implementing remediation actions.
- **Legal and ethical considerations**—Physical penetration testing can raise legal and ethical concerns, particularly if testers attempt to gain access to sensitive areas or assets. Organizations must ensure that proper permissions and agreements are in place, and that the testing activities comply with applicable laws, regulations and ethical guidelines.
- **Armed Guards**—Testing activities must be carefully coordinated to avoid any potential conflict or misunderstanding with security personnel. Although most physical penetration testers are confident in their ability to navigate challenging situations through verbal communication, human behavior remains inherently unpredictable. There is a real-world possibility for testers of losing their lives doing this type of job, which makes physical pen testing dramatically different from network penetration testing.
- **Off Limits**—Certain areas or assets may be off-limits for testing. These areas could include highly sensitive locations, critical infrastructure or areas with legal restrictions. Organizations need to clearly define and communicate the boundaries of the testing engagement to ensure that testers do not inadvertently breach security or access prohibited areas.
- **Personnel**—Physical pen testing requires skilled professionals who have not only the technical expertise required to conduct on-site assessments but also the social acumen essential to the role. For example, "burning" refers to the scenario in which a tester attempts to breach a building's security but is identified or caught in the act. This scenario presents a unique challenge because once a tester's identity has been compromised, it becomes significantly more difficult for that individual to conduct subsequent infiltration attempts.

Strategies for Overcoming Challenges

Overcoming the challenges of physical penetration testing requires a multi-faceted approach. Here are some points to consider when addressing challenges.

- One of the primary challenges is gaining access to the premises and assets for testing. To overcome this, it is crucial for testers to establish clear communication and build a strong relationship with the client organization. The testing company should clearly explain the purpose and benefits of the test, provide proper documentation and obtain authorization from the appropriate stakeholders, including management, security personnel and legal representatives.
- Physical pen testers must operate covertly to accurately assess security measures. To address this challenge, testers can adopt various disguises or cover stories to blend in with the environment. Effective social engineering techniques, such as tailgating or impersonating authorized personnel, can also be employed to gain access without raising suspicion.
- Physical testing involves real-world scenarios, making it challenging to predict and control all variables. Testers should be prepared to adapt quickly in response to unexpected situations. Thorough planning, training and experience can help testers handle unforeseen challenges while maintaining professionalism and avoiding unnecessary risk.

- Physical penetration testing inherently involves certain risk, such as potential confrontations or encounters with law enforcement. To overcome this challenge, it is crucial to conduct a comprehensive risk assessment before each engagement, ensure the safety of the testing team and coordinate closely with the client organization's security and legal teams. Open and transparent communication is vital to mitigate potential misunderstandings or escalation of situations.
- Physical pen testers must operate within legal boundaries and ethical standards. They must familiarize themselves with applicable laws, regulations and policies, ensuring compliance throughout the testing process. Likewise, they should maintain clear documentation of project scope, rules of engagement and client authorization to demonstrate that the testing is being conducted legally and ethically.
- Physical penetration testing generates a significant amount of data and observations. To overcome the challenge of effectively documenting findings, testers should maintain thorough notes, photographs and video evidence. It is essential to provide actionable recommendations to the client organization, clearly identifying vulnerabilities and suggested improvements.
- Physical penetration testing is a specialized field that requires continuous learning and skill development. Testers must stay abreast of the latest techniques, tools and methodologies through professional training, certifications and participation in industry conferences and communities. They should regularly assess and enhance their physical security assessment skills to stay ahead of emerging threats and challenges.

By adopting these strategies, physical penetration testers can effectively navigate and overcome the challenges associated with this unique and critical aspect of security testing, helping organizations improve their physical security posture and mitigate potential risk.

Conclusion

Physical penetration testing brings numerous benefits to organizations across various industries. It helps identify vulnerabilities in physical security measures, assesses the effectiveness of security protocols and enhances the safety of personnel. Moreover, it plays a crucial role in safeguarding sensitive data and valuable assets, ensuring compliance with industry regulations and mitigating risk associated with physical security breaches. By recognizing the value of physical penetration testing, organizations can strengthen their overall security posture and protect their critical resources from potential threats.

Acknowledgments

ISACA would like to recognize:

Lead Developer

Brice Self

Founder/Owner, Fortified Solutions LLC

USA

Expert Reviewers

Howard Duck

CISA, CISM, CDPSE, CISSP

Senior Cyber Security Manager, Dexian, USA

Timo Huebner

CISM, CGEIT, CDPSE, TOGAF

Germany

Neil Lappage

CISM, CDPSE

Australia

Nandita Rao Narla

CISA, CISM, CRISC, CDPSE, FIP, CIPM, CIPP/US and CIPT

Head of Technical Privacy and Governance, DoorDash, USA

Sergiu Sechel

CISA, CISM, CRISC, CDPSE, CEH, CFE, CSSLP, GASF, GCFA, GCTI, GICSP, GPEN, GNFA, GREM, GWAPT, PMP

Boston Consulting Group (BCG), UK

Board of Directors

John De Santis, Chair

Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Brennan P. Baybeck, Vice-Chair

CISA, CISM, CRISC, CISSP

Senior Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Stephen Gilfus

Managing Director, Oversight Ventures LLC, Chairman, Gilfus Education Group and Founder, Blackboard Inc., USA

Niel Harper

CISA, CRISC, CDPSE, CISSP, NACD.DC

Chief Information Security Officer, Data Privacy Officer, Doodle GmbH, France

Gabriela Hernandez-Cardoso

NACD.DC

Independent Board Member, Mexico

Jason Lau

CISA, CISM, CGEIT, CRISC, CDPSE, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP

Chief Information Security Officer, Crypto.com, Singapore

Massimo Migliuolo

Independent Director, Former Chief Executive Officer and Executive Director, VADS Berhad Telekom, Malaysia

Maureen O'Connell

NACD.DC

Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Asaf Weisberg

CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P

Chief Executive Officer, introSight Ltd., Israel

Erik Prusch

Chief Executive Officer, ISACA, USA

Pamela Nigro

ISACA Board Chair 2022-2023

CISA, CGEIT, CRISC, CDPSE, CRMA

Vice President, Security, Medecision, USA

Gregory Touhill

ISACA Board Chair 2021-2022

CISM, CISSP

Director, CERT Center, Carnegie Mellon University, USA

Tracey Dedrick

ISACA Board Chair, 2020-2021

Former Chief Risk Officer, Hudson City Bancorp, USA

About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its 170,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

DISCLAIMER

ISACA has designed and created *Physical Penetration Testing: The Most Overlooked Aspect of Security* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA
1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/