+44 345 094 0945
www.waterstons.com
Article

Physical Security Penetration Testing

May 2023

Physical Security Penetration Testing

It’s difficult for organisations to know if every crack – or even hole – has been patched when it comes to cyber security, which is why we offer penetration (pen) testing.

Categories Cyber Resilience, Cyber Security Strategy

May 2023

-
-
-
-

Simon Evans

Principal Security Consultant

Email

simon.evans@waterstons.com

This exercise, conducted by our team of ethical hackers, replicates the same tricks and techniques as a well-trained adversary to identify weaknesses and issues.

But that’s all online, what about a firm’s physical assets? That’s where physical security pen testing comes in.

What is physical security penetration testing?

Physical security testing involves attempting to gain unauthorised access to a facility, building, or other physical space, in order to identify vulnerabilities that could be exploited by an opportunist, or determined, attacker, or validate the existing protection measures.

Unlike an IT network or application penetration test, the goal is to identify weaknesses in an organisation's physical security controls and posture such as access control, alarm systems, CCTV, or other measures that could be used to gain unauthorised access to sensitive areas or information.

During the penetration test, a team of trained professionals attempt to breach physical security barriers using a variety of tactics including social engineering, tailgating or physical bypass.

The results of the test are then documented to allow an organisation to prioritise addressing identified vulnerabilities and implementing additional security measures as needed.

Scope of testing

Our offering is designed around a six-step plan delivered over several days to allow for consistency of approach. Our six steps involve:

1. Client authorisation - setting the boundaries of the test
2. Information gathering - open-source intelligence research
3. Discreet observation of the site or facility to be tested - not covert observation
4. Design of the entry plan and protecting - how entry will be made and cover story of why we are there
5. Exploitation and post-exploitation - how we get in and what we do once we are in
6. Reporting and Presentation - delivery of an in-depth security and remediation report highlighting key risks.

Overview of service delivery

A penetration test should satisfy five requirements to be useful to the organisation:

- Realistic – employees should act normally, as they would in everyday life
- Respectful – the test is done ethically, by respecting the employees and the mutual trust between employees
- Reliable – the penetration test does not cause productivity loss of employees
- Repeatable – the same test can be performed several times and if the environment does not change, the results should be the same
- Reportable – all actions during the test should be logged and the test should be in a form that permits a meaningful and actionable documentation of findings and recommendations.

Use of social engineering

Targeted social engineering can be a very effective tactic in a physical security penetration test as it can help an attacker gain access to secure areas by exploiting the trust of an employee or other individuals with access to the facility.

An attacker may use social engineering techniques such as pretexting, phishing or impersonation to gain the trust of an employee. For example, by posing as a delivery person or IT technician and asking an employee to let them into a restricted area, or access to sensitive information.

Overall social engineering can be an effective tactic to help an attacker bypass normal physical security controls, so it's vital for organisations to train their employees to recognise as resist these attacks as part of the overarching security strategy.

Open-source research (OSINT)

OSINT can be used to gather information about the facility and its security controls such as employee names, job titles, security procedures and access controls. This information can be used to plan and execute a test with greater success.

By leveraging publicly available information, potential vulnerabilities can be assessed prior to the discreet observation and test occurring. An oversight of floor plans, unsecured entrances or weak access controls may be uncovered at this stage.

Organisations should be aware of the risks posed by OSINT and take steps to mitigate these risks though monitoring of their, and their employees', online presence, implementing robust access controls.

Who can benefit from a physical security penetration test?

A physical security penetration test can benefit a wide range of organisations and businesses that have a physical presence, particularly those that store sensitive data or valuable assets on their premises.

- Banks and financial institutions – these organisations store large amounts of valuable assets and sensitive data on their premises making them a prime target for physical attacks
- Data centres – these facilities contain servers and other critical infrastructure that are essential for the operation of many businesses
- Government agencies and Government suppliers of services – these agencies host larger volumes of sensitive information assets including classified data and nation security secrets making them a target for a number of threat groups and actors
- Hospitals and healthcare facilities – larger volumes of sensitive patient personal information are processed and stored making them a valuable target for an attacker
- Retail stores and shopping centres – these organisations and facilities store high volumes of valuable merchandise and cash on premises and may retain personal details relating to their customer base
- Manufacturing facilities – these facilities often contain valuable equipment and intellectual property essential to the production market
- Organisations holding ISO27001 certification – physical security controls, and testing, appear as important controls within the certification process. The new issue of the Standard requires that organisations continually monitor their facilities for unauthorised physical access.

Overall, any organisation that has a physical presence and is concerned about the security of their assets can benefit from a physical security penetration test. Get in touch with Simon directly, or contact our Cyber team, to find out more.

http://www.waterstons.com/print/pdf/node/8578