COGNISYS

PENETRATION TESTING

Physical security assessment

Our physical security assessment ensures that your organisation's security measures are effective in preventing physical breaches.

How does our physical security assessment work?

Working towards your organisation's goals, our consultants simulate a malicious threat actor attempting to breach the building and access sensitive areas like the server room. This is done using various techniques based on your current security procedures.

Scoping and planning

Define objectives

Cognisys will work closely with you to understand your organisation's operations and further information required to deliver this work. The goal is to understand the goals and objectives needed for the consultants to meet for this engagement. These goals and objectives typically start with gaining entry onto the site and end with physical access to critical infrastructure, such as entry to server rooms.

Requirements

You must provide the addresses for the sites that need testing, along with the contact details for the point of contact. A 'get out of jail free' card will be required for the assessments, which can be provided to staff when confronted. This would be used primarily to prove the consultant's identity, grant us permission to be in the facility, and have the point of contact's information.

Reconnaissance

This phase of the engagement involves the consultant performing OSINT to gather relevant information required for the assessment. This involves things such as scraping online resources to find the design for ID badges your organisation uses to craft a valid reason for being onsite. A visit to the site to scope out the environment may be required if limited information is available online. This includes finding unlocked areas of the premises and reviewing weakened and degraded doors/walls.

Attempt

On the assessment day, the consultant will attempt to gain access to the site through multiple techniques. Initial access from previous engagements has been achieved in various ways, ranging from tailgating an employee to impersonating a third-party contractor or employee. It should be noted that this is primarily done through social engineering attacks, with destructive entry being out-of-scope.

Guided walkthrough

If the consultant cannot access the site, a guided walkthrough of the assessment in a white-box setting would be requested. This allows the consultant to gather potential weaknesses, such as sensitive documents being left around or a lack of CCTV on the critical infrastructure that would have been missed on the initial entry attempts. This helps to ensure that if your organisation's security posture is strong enough to prevent access to the site, there will be places to help further harden the premises if initial entry is possible.

Reporting

After the engagement, it's essential to analyse the results, regardless of the findings. In a controlled physical assessment, the focus is on assessing the site's security. Focusing on every aspect that could be used to help gain access to sensitive information onsite. The report would detail the entire walkthrough for all entry attempts, along with reporting on the security recommendations to help further harden the building.

Why choose Cognisys' physical security assessment?

Tailored assessments
Our testers are experienced in constructing and creating effective physical security assessment campaigns. This allows the consultant to develop a bespoke campaign unique to the client's site, increasing the likelihood of performing a successful breach.

Full reporting and remediation advice
Post-assessment, we deliver detailed reports highlighting the findings from the physical security assessment campaign, such as a full breakdown of each break-in attempt and all findings from reconnaissance and test performance.

BACK TO CONTENTS