Physical Attack Simulation

State and criminal threat actors are actively exploiting unauthorised physical access to bypass cyber security and facilitate access to confidential data.

A physical breach exposes your assets and liability and creates reputational risk. By simulating physical attacks, you can understand the efficacy of your controls, the levels of risk you carry and the impact such a breach would have on your organisation

Understanding how physical enabled cyber attacks impact your business is critical to holistic security.

The most advanced cyber security will not provide resilience to an organisation with a vulnerable physical security posture, and threat actors use both to achieve their objectives.

NCC Group's Physical Attack Simulation replicates the methodologies and attacks used by modern state and criminal threat actors to give you the evidence and understanding of your risks, their impact and how to increase your security posture.

These are not rushed, generic breach tests. Remediating a single breach technique does not improve your security. They are comprehensive and intelligence-led simulations designed to comprehensively improve your organisation's physical security posture.

All our physical services are carried out by dedicated physical security consultants. Their experience includes government security systems installation, specialist military and police departments, and private sector processionals.

Benefits

Assurance:
A Physical Attack Simulation identifies weaknesses that permit access to your estate, staff, and assets, whether they are utilised in the assessment or not.

Business Impact:
Physical Attack Simulations identify what the "post-breach" risk to your organisation is, allowing you to understand what a breach means for your organisation, including client specified objectives.

Comprehensive reporting:
Executive level summary of the business risks you face, along with meticulous attack timelines, detailed indicators of compromise and appropriate mitigation strategies, supported with thorough technical appendices and date & time stamped diary of assessment activities.

Throughout the entire engagement, physical specialists will observe the environment to identify vulnerabilities as they arise, whether they are used in the breach or not.

Throughout the entire engagement, physical specialists will observe the environment to identify vulnerabilities as they arise, whether they are used in the breach or not.

Throughout the entire engagement, physical specialists will observe the environment to identify vulnerabilities as they arise, whether they are used in the breach or not.

Physical Attack Simulation

A Physical Attack Simulation performed by NCC Group aims to replicate a targeted attack from real-world threat actors and achieve agreed set objectives. All engagements are unique to each organisation but, to ensure the assessment provides outputs required to improve your security posture, the following phases are included:

Open-Source Intelligence (OSINT)

During the OSINT phase, all publicly available information relating to the physical presence and security will be targeted.

Assessment objectives will be focused on and searches will include sources such as corporate, third party and staff social media, local council and authorities' sites and forum sites. This element may also include email and phone-based attacks. Significant findings are included in a dedicated section of the final report.

Reconnaissance

Reconnaissance takes place during the entire engagement. This runs from Sunday to Friday in order to observe the environment in a representative, one-week period.

Shorter engagements risk missing critical findings that may only occur on a specific day of the week. The Sunday is included to observe the environment during its quietest period. Reconnaissance never ceases during the engagement and is conducted even after the environment is breached.

Breach

Breaches are conducted after sufficient OSINT and reconnaissance has been carried out to plan strategic attack paths specific to your environment.

Breaches are then planned and carried out as "most likely to succeed / least likely to be detected", but opportunistic breaches may also be carried out if deemed appropriate at the time.

This method allows consultants to avoid detection and carry out subsequent attempts should initial attempts fail, thus maximising the value of the assessment.

Types of breach include:

- Social engineering techniques
- Tailgating
- Radio Frequency Identification (RFID) cloning
- Physical Access Controls System (PACS) attacks
- Physical barrier bypass
- Policy abuse
- Request to Exit (REX) attacks
- Lock-picking / bypass

All attempts are non-destructive in nature.

Persistence

Once the environment has been breached, consultants will attempt to obtain persistent access to the secure areas. If a method of persistence is identified but not achieved due to assessment time constraints, the method will be discussed with the client and an agreed method of persistence provided. This ensures your time is used efficiently to achieve the assessment goals.

Post-Breach Analysis

Once the environment has been breached, consultants will verify the location before carrying out any actions. Once confirmed, consultants will carry out the agreed objectives for the site.

Example objectives may include:

- Deploy listening devices
- Compromise end devices
- Network access
- Sensitive area access (laboratory, trading floor, server room, etc.)

In addition to your specified objectives, the physical team will assess your environments during the breaches in order to determine what additional risk is exposed from the perspective of a threat actor.

This will take into consideration what your specific threat actors are, the level of access acquired and the state of the environment during the breach. This ensures that as well as determining the risk of your known exposure, you are informed of your unknown exposure.

Objectives deemed dangerous or likely to cause risk to business operations will be discussed with client prior to being carried out. If appropriate, such objectives can be simulated in a controlled manor.

Clean Up

Consultants will remove methods of persistence and return / remove any devices. Any devices / persistence not removed will be detailed to the client on the final day of the assessment (typically Friday).

Reporting

Reports are written taking into full consideration the environment and organisation being assessed. Remediations are provided that are appropriate to the risk, taking into account the overall security posture.

The executive summary will detail the critical attack paths with the top five risks and recommendations. For multi-site engagements, an analysis of the security postures between environments will be conducted and reported. This allows recommendations to be applied at an organisation level as well as an individual site level.

Each finding will be detailed, including the proof of concept, evidence, location and recommendation. A time and date stamped “engagement diary” will be provided in the supplemental data section. This will be supported with imagery and consultant observations.

A debrief session is provided to go through the report with key stakeholders, with more extensive options available.

Engagement

Onsite activities are carried out by a minimum of two consultants for safety and practicality reasons.

Onsite consultants are supported by global practise team at no additional cost to client. Onsite time frame is 24 hours a day. Physical engagements are carried out by dedicated physical consultants.

Physical Security Done Right

NCC Group’s physical attack simulation is as close to a real targeted attack as possible without compromising your business operations.

It will provide you the information you need to understand your risk, how your organisation reacts to a real attack and how to significantly raise your overall security posture. This is not an opportunistic breach, this is assurance.

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com