
Picture credit: HZL Specialist Solutions

# CLOSE ENCOUNTERS

**Al Prescott** *explores the role of penetration testing in close protection and protective security*

**A penetration test within the close protection environment should seek to challenge the physical and online spaces. It should generate opportunities for an attacker to exploit and seek to expose the principal to physical and reputational harm. Penetration testing can be a valuable tool to highlight existing vulnerabilities and can be utilised early in the instruction/contract; it can be deployed to justify newly established measures.**

Confirmatory exercises should be regularly conducted, testing various elements, plugging any exposed gaps and delivering tangible feedback to the security manager. In short, pen testing is helpful for mature and established plans and undeveloped contracts needing total exposure.

## CLOSE PROTECTION

In a close protection environment, penetration testing can be used to identify weaknesses in the security posture of the principal's residence and temporary accommodations, and in doing so can ensure that all possible threats are identified and addressed. It is important to note that close protection environments are unique in that they often involve high-profile individuals who are targets for potential attackers or may have threats specific to them as individuals. As such, the physical security of these individuals and their residences is paramount. Conducting penetration testing particular to the principal and their prioritised threats will allow for gaps in procedures to be easily identified and the relevant mitigations to be implemented.

## ENHANCING PROTECTIVE SECURITY

Penetration testing of the principal's residence or external locations that a principal would visit can be conducted in two ways. Either externally provided by trained individuals brought in as and when required, the benefits of this include no additional burdens on internal staffing and ensure that an independent review is conducted that is free of bias by trained professionals that follow ethical guidelines and ensure the safety of any individuals involved. This option can prove particularly challenging when conducting CP duties overseas or in locations that are not easily accessible to external agencies.

The alternative is that a Close Protection Team member is trained in penetration testing and conducts internal assessments as and when required. This is a cost-effective option, however it can raise challenges such as legal requirements, bias and the availability of said trained persons depending on team size, shift rotations etc.

**Digital penetration testing helps close protection teams enhance their cyber security measures, protect sensitive information about the team and Principal, and prevent unauthorised access or data breaches**

## TESTING IN A CLOSE PROTECTION CONTEXT

**Reconnaissance:** Gather information about the residential property or temporary location occupied by the principal, including its layout, security features, and any existing security protocols. Identify potential vulnerabilities such as blind spots, weak entry points or gaps in surveillance coverage. Further surveys can be conducted on the CP team, specifically noting areas such as residential security rotations and human intelligence opportunities.

Planning: Develop a comprehensive plan that considers the unique aspects of close protection and residential security. This plan should include considerations for protecting individuals, secure perimeters and potential risks associated with the property.

Social Engineering: Assess the effectiveness of security protocols by attempting to exploit human vulnerabilities. This could involve accessing restricted areas or sensitive information by impersonating household staff, delivery personnel or other trusted individuals.

Physical Security Assessment: Evaluate the effectiveness of physical security measures such as access control systems, security cameras, alarms and perimeter defences. Particular attention should be given to areas where close protection personnel are stationed, ensuring their visibility and ability to respond to threats.

Unauthorised Access Attempts: Conduct simulated intrusion attempts to test the effectiveness of security measures. This may include attempting to breach perimeter defences, defeat access control systems or bypass surveillance cameras to gauge the response time of close protection personnel.

Documentation: Thoroughly document all findings, including any vulnerabilities or weaknesses identified within the close protection/residential security environment. This documentation should outline specific areas of concern and highlight any successful unauthorised access attempts.

**Reporting:** Prepare a detailed report presenting the findings and recommendations discovered during the physical penetration test. This should emphasise the impact on close protection and residential security, providing actionable steps to enhance overall safety and protection.

**Debriefing and Follow-up:** Discuss with relevant stakeholders, including close protection personnel, residents (Principal) and security management. Review the findings and recommendations, ensuring strong communication of any necessary follow-up actions to address identified vulnerabilities.

## GOALS OF CP PENETRATION TESTING

Physical penetration testing can contribute to the overall goals of close protection and residential security teams in several ways:

Threat Assessment: By conducting physical penetration testing, close protection teams can identify potential vulnerabilities and weaknesses in their physical security measures for a residence, the principal's workplace, meeting locations or transit accommodation. This assessment helps them understand the threats and risks the protected individual or facility may face, allowing for more effective threat assessment and mitigation strategies.

Risk Mitigation: Penetration testing helps close protection teams identify and address security weaknesses. By simulating real-world attack scenarios, they can proactively identify and mitigate potential risks, ensuring that the protected individual or facility is well-prepared to handle security incidents.

**INSIGHTS GAINED FROM TESTING CAN BE USED TO IMPLEMENT APPROPRIATE SECURITY MEASURES**

Emergency Response: Penetration testing helps close protection teams assess their emergency response capabilities. By simulating security breaches, they can evaluate the effectiveness of their response plans, identify areas for improvement and enhance their ability to handle emergencies.

Enhanced Awareness: Penetration testing raises close protection teams' awareness of potential security threats and vulnerabilities. By experiencing simulated security breaches, they are able to gain first-hand knowledge of any challenges they may face and can develop suitable strategies to address them.

Confidentiality: Penetration testing helps close protection teams ensure the confidentiality of sensitive information. By identifying weaknesses in physical security controls, they can strengthen measures to protect confidential data and prevent unauthorised access.

Proactive Measures: Physical penetration testing allows close protection teams to enhance security proactively. By identifying vulnerabilities and weaknesses, they can implement necessary improvements such as upgrading security systems, implementing stricter access controls or improving training programs.

## BENEFITS OF CP PENETRATION TESTING

Identifying Vulnerabilities: Close protection involves understanding the threats against a principal and identifying the associated vulnerabilities. Physical penetration testing helps close protection and residential security teams identify vulnerabilities in physical security measures, such as access control systems, surveillance systems and perimeter defences. By simulating real-world attack scenarios, penetration testing exposes weaknesses that can be exploited by malicious actors, allowing security teams to address and strengthen these areas.

Testing Response Capabilities: CP teams must assess response times to security breaches when conducting residential security duties or CP at transit locations and taking practical actions for dealing with their principal during such a breach. Penetration testing allows close

protection and residential security teams to assess their response capabilities in case of a security breach. By conducting unauthorised access attempts and exploitation techniques, security teams can effectively evaluate their ability to detect, respond to and mitigate potential threats.

## CONDUCT SIMULATED INTRUSION ATTEMPTS TO TEST THE EFFECTIVENESS OF SECURITY MEASURES

Enhancing Training and Awareness: Physical penetration testing provides an opportunity for close protection and residential security teams to evaluate the effectiveness of their training programs and raise team members' awareness of potential security risks. The testing results can be used to identify areas where additional training is required and to develop strategies for improving security awareness.

Enhancing Overall Security Posture: By conducting physical penetration testing, close protection and residential security, teams can enhance the overall security posture of the premises they are responsible for – whether it's a permanent residence or transit location occupied by the principal. The insights gained from the testing process can be used to implement appropriate security measures, update policies and procedures, and allocate resources effectively to mitigate potential risks.

The testing results should be documented, reported and used as a basis for remediation efforts to strengthen the security provided by the close protection team and residential environments at the discretion of the CP team leader, Security Management, and the Client/Principal.

### PHYSICAL PENETRATION TESTING

Physical penetration testing can also assess the effectiveness of residential security measures and CP teams. The process involves simulating real-world scenarios to identify weaknesses and vulnerabilities to strengthen security. For residential security, the testing may include mapping entrances and perimeter, testing alarm systems, assessing the effectiveness of access control measures, evaluating the response of the CP team to various simulated threats and testing their actions such as evacuation on a principal or movement to a safe room. The goal is to ensure that the residential security measures and CP teams are robust and capable of preventing unauthorised access and potential harm to the residents.

### DIGITAL PENETRATION TESTING

Digital penetration testing in a close protection environment refers to identifying and assessing vulnerabilities in the digital infrastructure and systems used within a close protection team/residential security team in a permanent or transit location occupied by a principal. It involves simulating real-world cyber attacks to test the effectiveness of security controls, identify weaknesses and recommend improvements. Digital penetration testing helps close protection teams enhance their cyber security measures, protect sensitive information about the team and Principal, and prevent unauthorised access or data breaches. Conducting digital penetration testing regularly is crucial, following industry best practices, and engaging experienced professionals to ensure comprehensive security planning and risk mitigation ●

**Al Prescott** is the owner and MD of HZL Specialist Solutions. With over 40 years of experience in Protective Security, he provides operational capability across many different security disciplines.

**It's vital to gather information about the property, including its layout, security features and any existing security protocols**


Picture credit: HZL Specialist Solutions