DRAGON LABS

WHITE PAPER

COMODO

PROVEN SUCCESS IN PREVENTING BREACHES

TABLE OF CONTENTS

INTRODUCTION

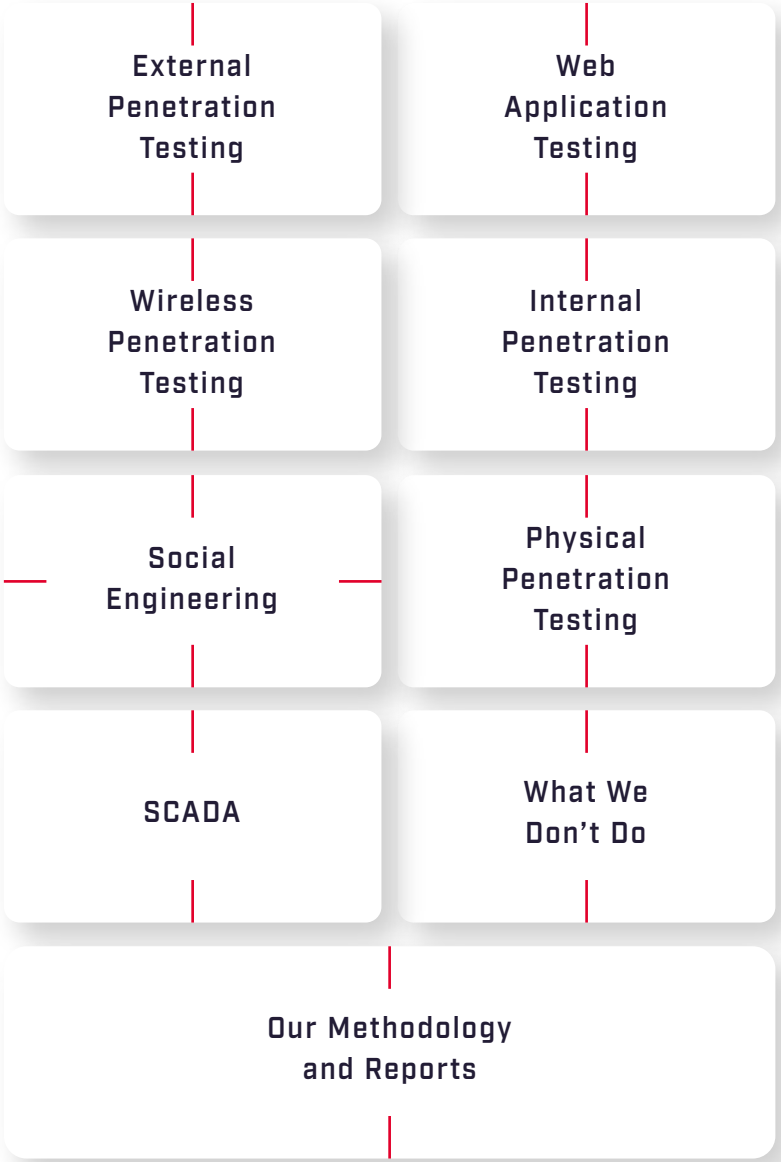
It is estimated that a data breach occurs every 39 seconds. This should not come as a surprise. The Internet, and more specifically the protocols on which it's based, were designed to make the free and open sharing of information easier and faster. At some point, we began, and today continue to use the Internet to communicate and store private information. Subsequently developed responses to this challenge such as the use of cryptography and secure coding standards have made commonplace the transfer of financial, medical, military, and the many other forms of sensitive information. In an open, largely unregulated network that is today's Internet, it remains incumbent on each organization which chooses to have any kind of presence on it to implement their security posture. Comodo Dragon Labs' provides advanced penetration testing for those organizations who wish to assess the effectiveness of their security.

WHO WE ARE

Comodo Dragon Labs brings together a wealth of talent, knowledge, and experience from around the globe. Our team of in-house hackers, all of whom have a minimum of 10 years of experience in information security, speak at least three languages and hold the OSCP/E certification. Besides, our parent entity, Comodo Cybersecurity, employs several hundred security experts in over a dozen countries around the World creating a vast talent pool from which we can draw knowledge and experience when necessary.

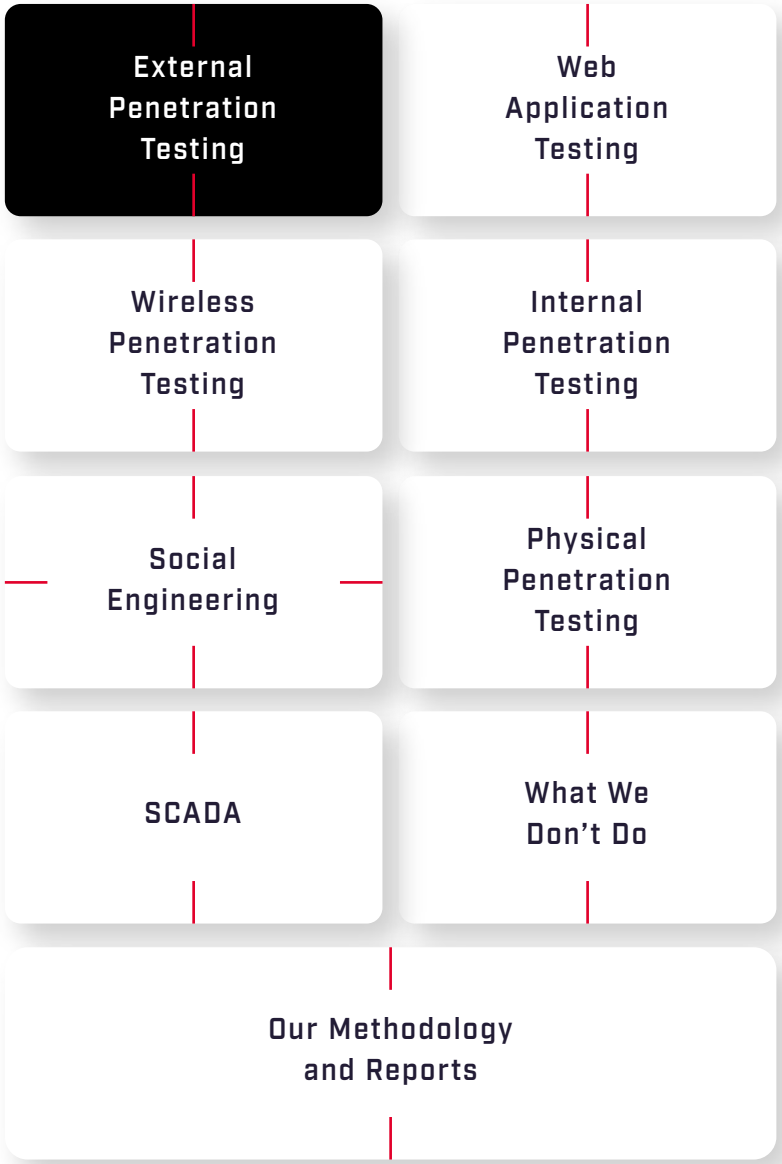
WHAT WE DO

Comodo Dragon Labs specializes in advanced penetration testing for high-security environments. Also known as 'mature' environments, these include but are not limited to intelligence, military, and law enforcement agencies, financial, medical, and legal institutions, as well as larger commercial entities. By no means limited to information systems, we also provide physical security assessments as well as security testing of industrial control systems and the environments in which they reside. Our tactical approach seeks to simulate as closely as possible an attack by a highly skilled and determined real-world adversary.



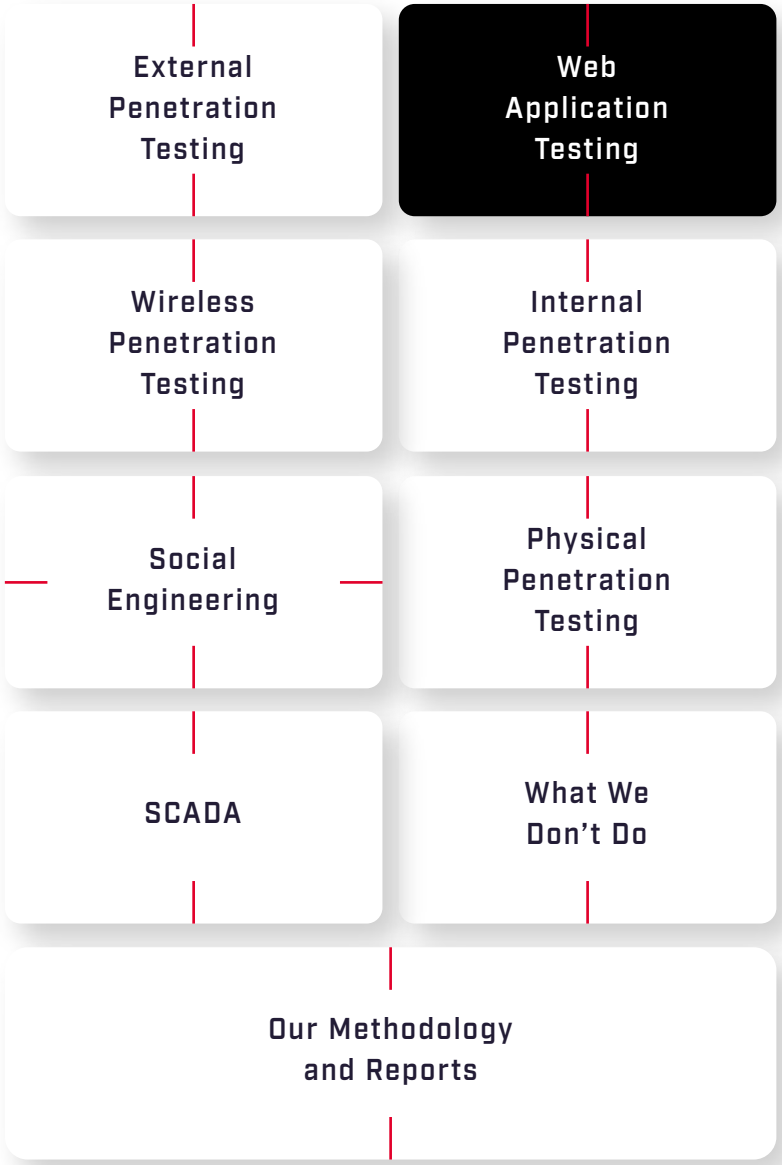
EXTERNAL PENETRATION TESTING

For organizations that maintain an Internet presence beyond web sites and applications, Comodo Dragon Labs will perform comprehensive network penetration testing. We will identify live hosts residing on networks either associated with or provided by the target organization, and the services provided by them. Vulnerable services will then be exploited to gain remote access and victim machines will be leveraged for lateral movement through the network or further penetration of the infrastructure.



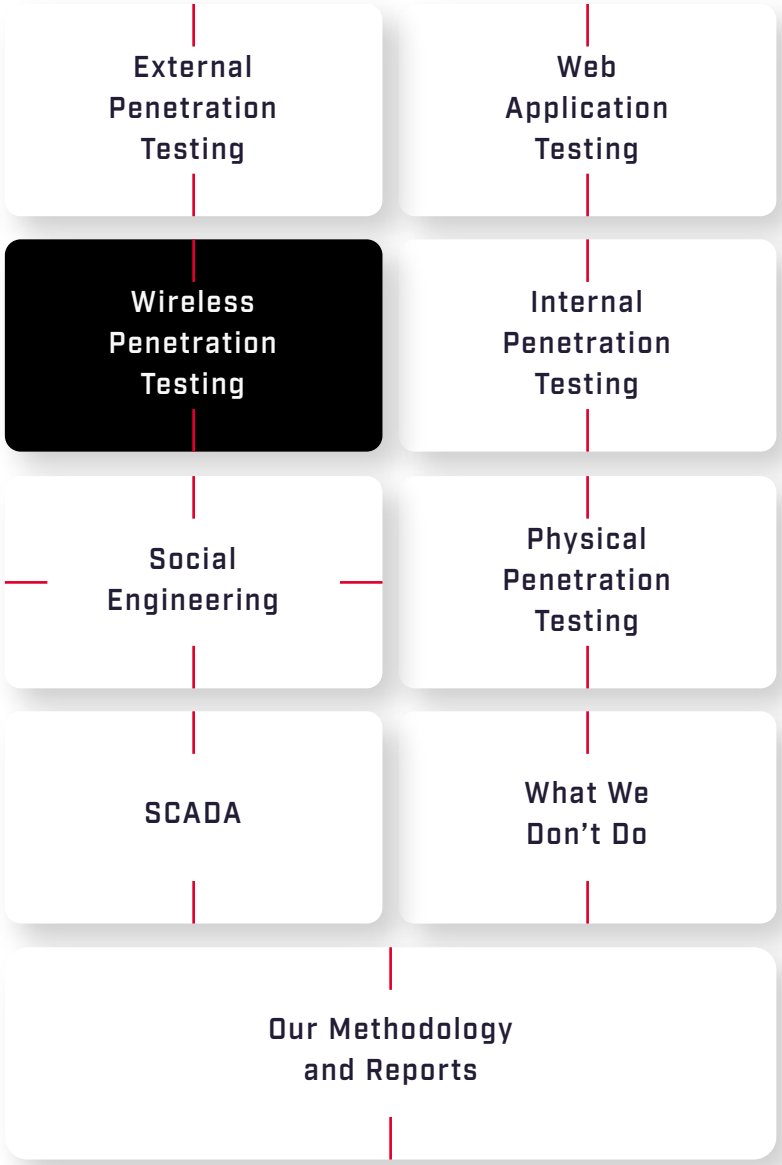
WEB APPLICATION TESTING

For web applications, we can provide both black and gray box assessments. In the former case, where authenticated users of an application are trusted however access to the application by the Internet public is not permitted, our attack will consist mainly of trying to gain unauthorized access. In the latter, where authenticated users of the application (those who have user accounts to which they can log in) are not trusted or when any member of the public can create and use an account on the application, we will perform a credentialed attack against its functionality. In all cases, testing will include but not be limited to authentication, session management, input validation, and business logic to name only a few. All testing is performed manually. We do not rely on automated scanning solutions. These are for vulnerability assessments which we do not provide currently.



WIRELESS PENETRATION TESTING

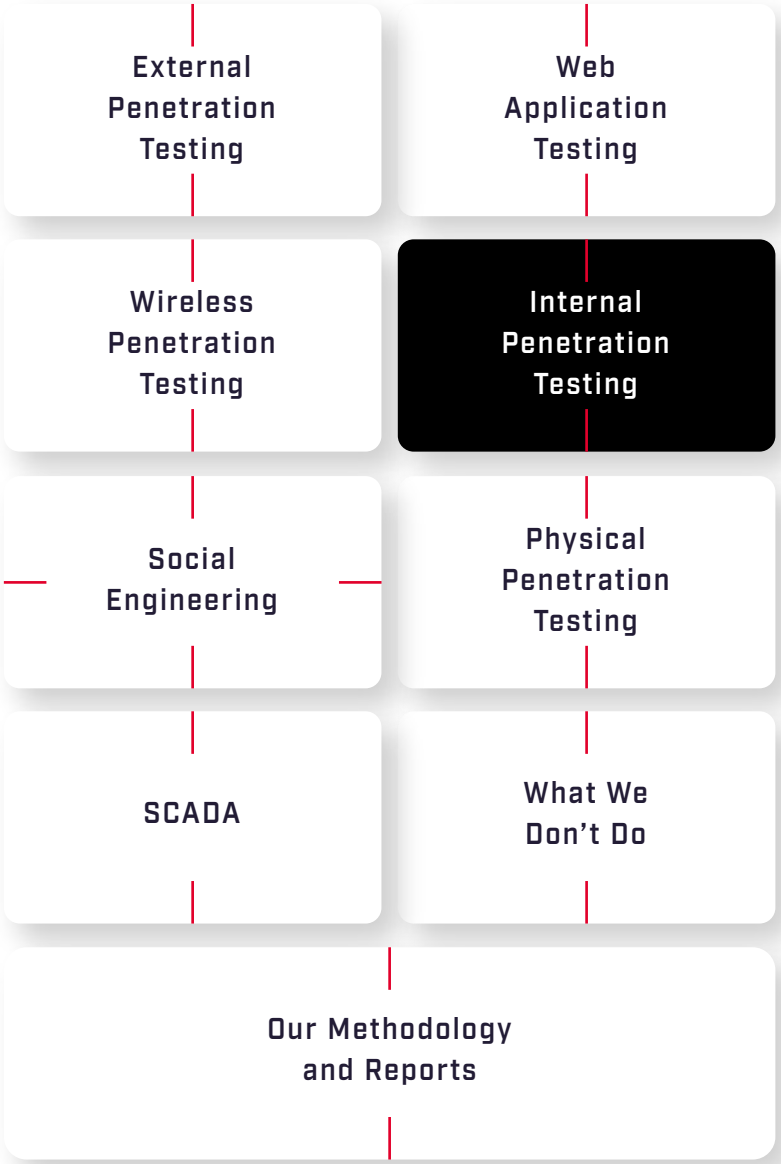
For entities whose wireless networks are accessible to potentially malicious actors, Comodo Dragon Labs can perform wireless penetration testing. This includes any organization that provides public, guest, or temporary Wi-Fi access and who's wireless network is used for the transmission of sensitive data or is connected to an internal network.



INTERNAL PENETRATION TESTING

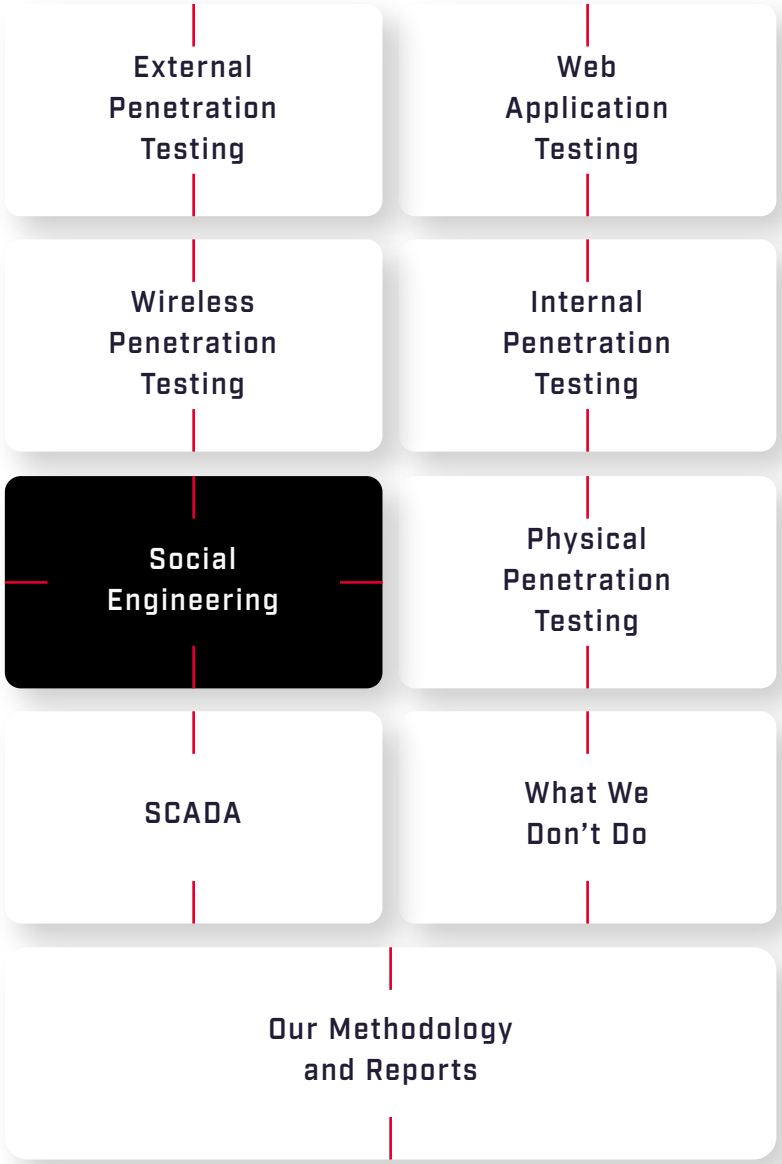
Are your data assets that are available on your internal network valuable enough for a determined advisory to send a malicious actor into your organization?

For those organizations that do indeed face such a threat, Comodo Dragon Labs can perform an internal assessment. After learning the requisite skills and applying successfully for a position within the organization (or gaining physical access employing some similar arrangement with upper management such as a consulting role) our team member will surreptitiously assess any internal networks to which his workstation can connect. Direct, face to face social engineering of employees or security personnel as well as unauthorized physical access to restricted areas such as server rooms may also be performed.



SOCIAL ENGINEERING

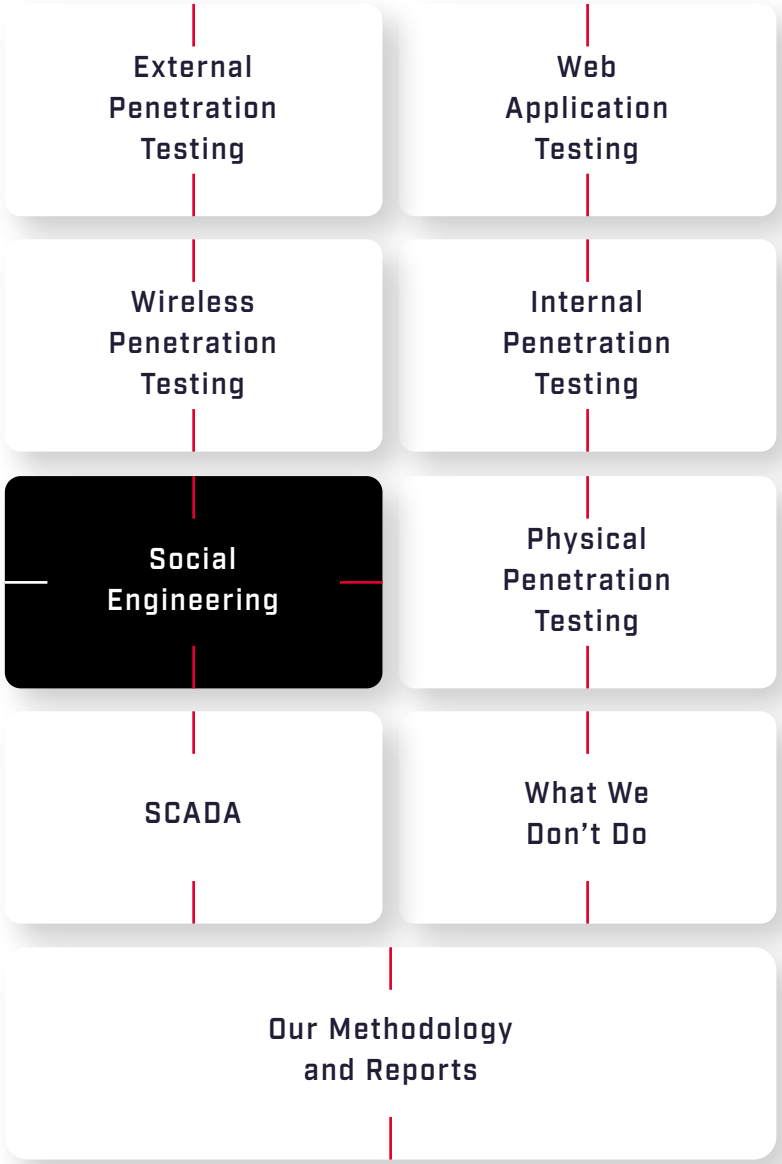
The estimate of data-breach frequency has been a reality for some time now. As such, better coding and software security standards have evolved. This makes web, application, and network-based attack vectors less common and more difficult to exploit successfully. In response, attackers have turned to other methods of compromise such as social engineering. Per Wikipedia "Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information." Attacks come in many forms, all which Comodo Dragon Labs can execute.



SOCIAL ENGINEERING

PHISHING

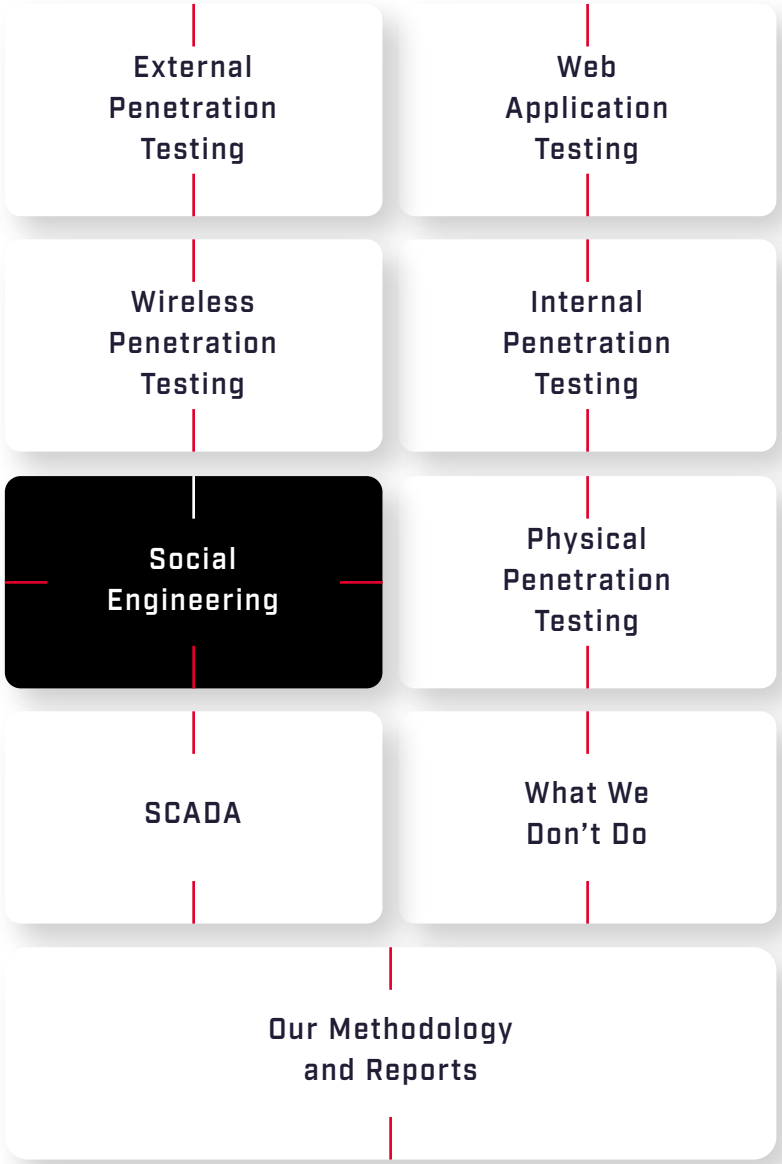
In a phishing campaign, an email containing content designed to manipulate and/or send a malicious payload to many recipients at a target organization. Following the instructions or performing an action (such as clicking a link or running a macro) will give an attacker control of the victim's workstation. Comodo Dragon Labs hackers' skill sets are not limited solely to technology. We seek and employ only individuals with diverse interests and backgrounds, especially those with experience in the Arts. This provides the strong creativity required to devise an email related to a target organization's industry or sector that will not simply promise some random reward for clicking a link but rather vastly increase the likelihood of targeted users' falling prey.



SOCIAL ENGINEERING

SPEAR PHISHING

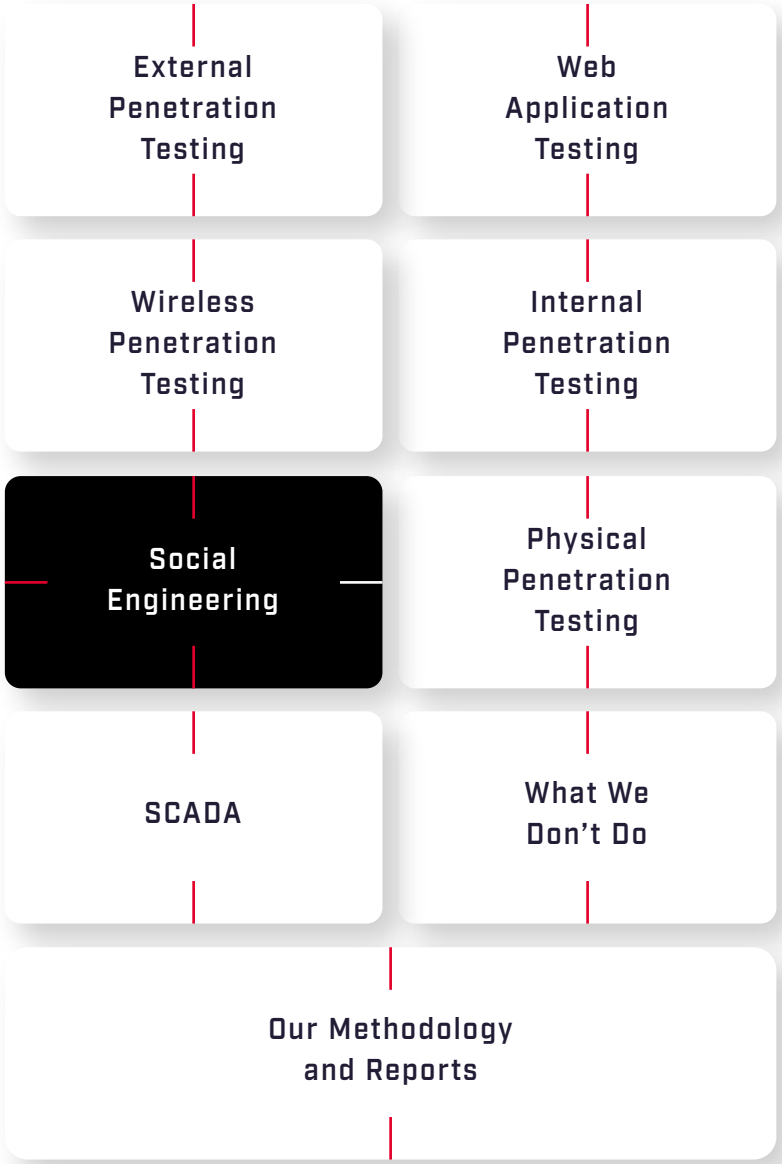
In some cases, a target entity's data assets are sufficiently attractive to attackers that they will spend the time and effort to target specific individuals within an organization with phishing emails designed specifically for them. After gathering intelligence against a individual, an email tailored to their interests, traits, or habits will be crafted and sent. This attack vector, although time-consuming, is extremely effective.



SOCIAL ENGINEERING

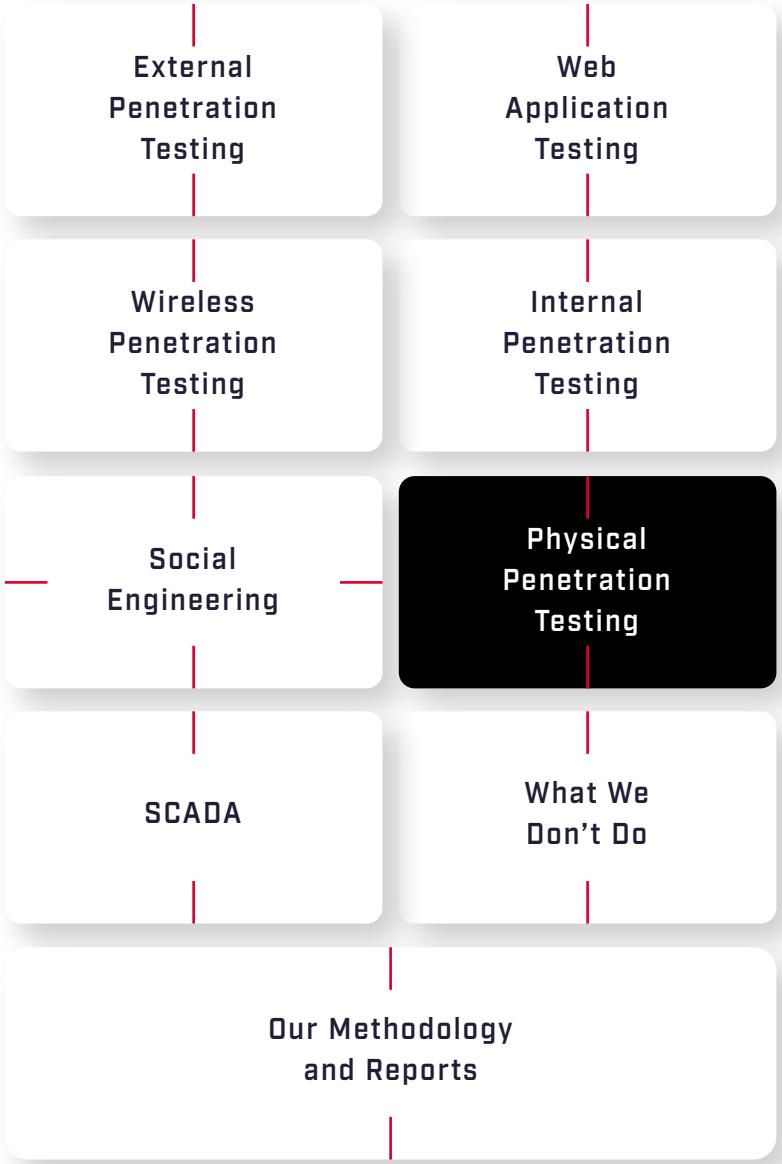
PHONING

Mature environments' IT infrastructures have been thoroughly tested and their security teams are highly accomplished at maintaining their security stacks. Software is kept up to date and secure with effective patch management strategies at every level. Servers are scanned regularly for vulnerabilities, workstations run the latest endpoint protection and most phishing attacks are thwarted by effective albeit resource-intensive anti-spam solutions. Comodo Dragon Labs team members are not solely technology experts. Our backgrounds include military, intelligence, and prior relationships with law enforcement. Our tradecraft includes fully undetectable accents in three widely spoken Western languages as well as very strong telephone and public speaking skills. For those organizations that face this category of threat, we'll phone you.



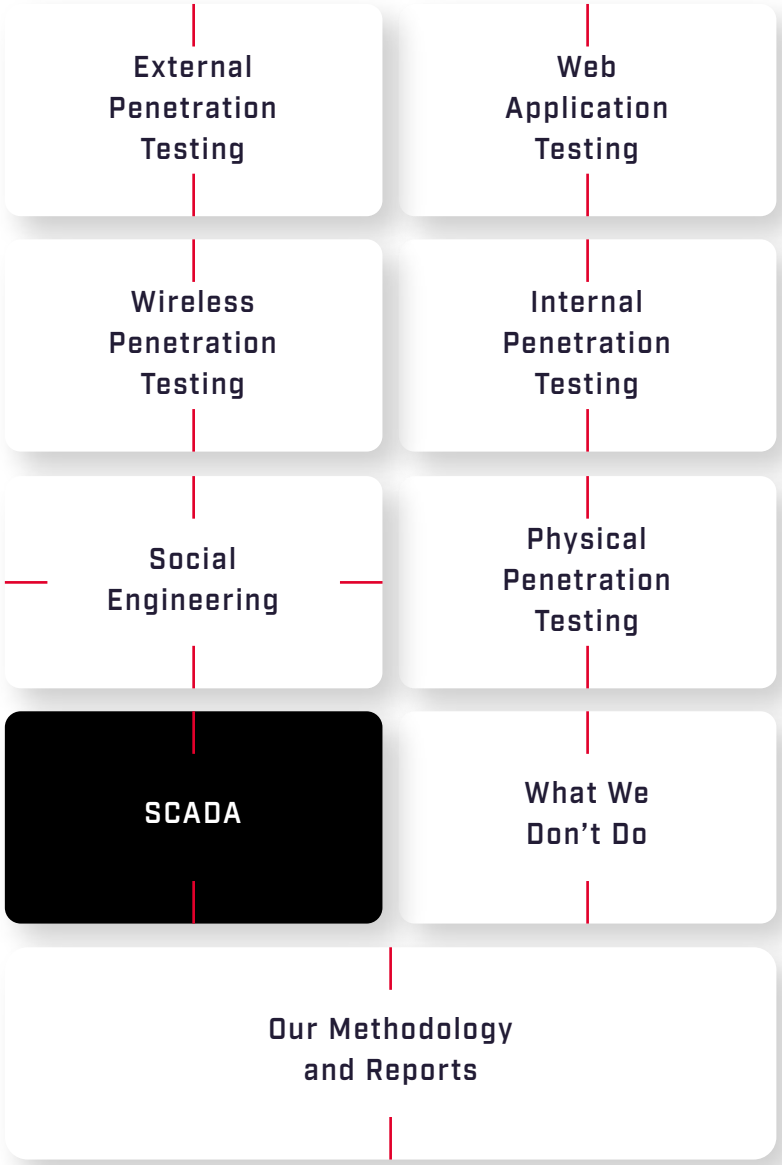
PHYSICAL PENETRATION TESTING

For entities whose threat models include highly determined adversaries with considerable resources in addition to wide skill sets and where the physical security of their data assets is a concern, Comodo Dragon Labs can provide physical penetration testing. Whether through personal effectiveness, interaction and intercession skills used for face to face social engineering or over 40 years of experience in black bag operations and extensive training in physical penetration and electronic access control hacking, if your organization faces a physical threat, we can simulate it.



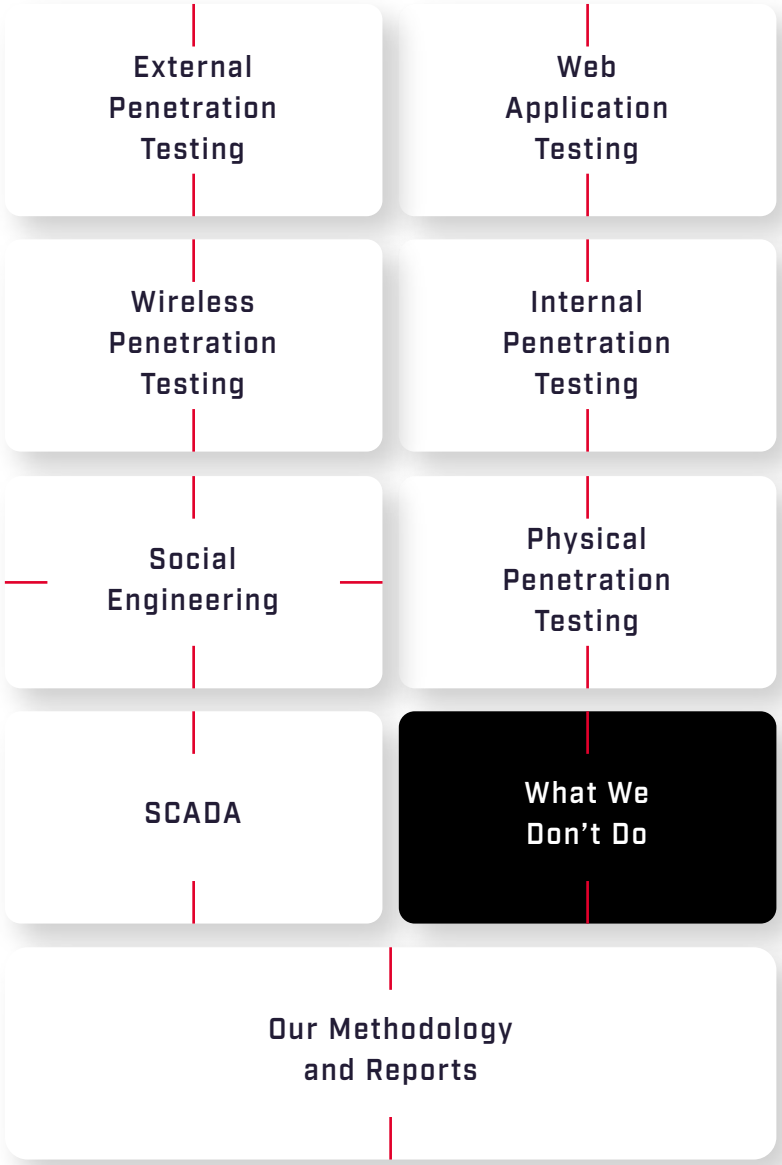
SCADA

For entities, such as utilities, transportation centers, medical facilities or any other whose industrial systems include supervisory control and data acquisition systems, the Dragon Labs team has training and experience for assessing their security. From business analysis and target selection to direct manipulation of controller environments, we can assess the overall security of your industrial infrastructure with minimal or no business impact. Unlike the other categories described above, we limit our level of exploitation to proof-of-concept.



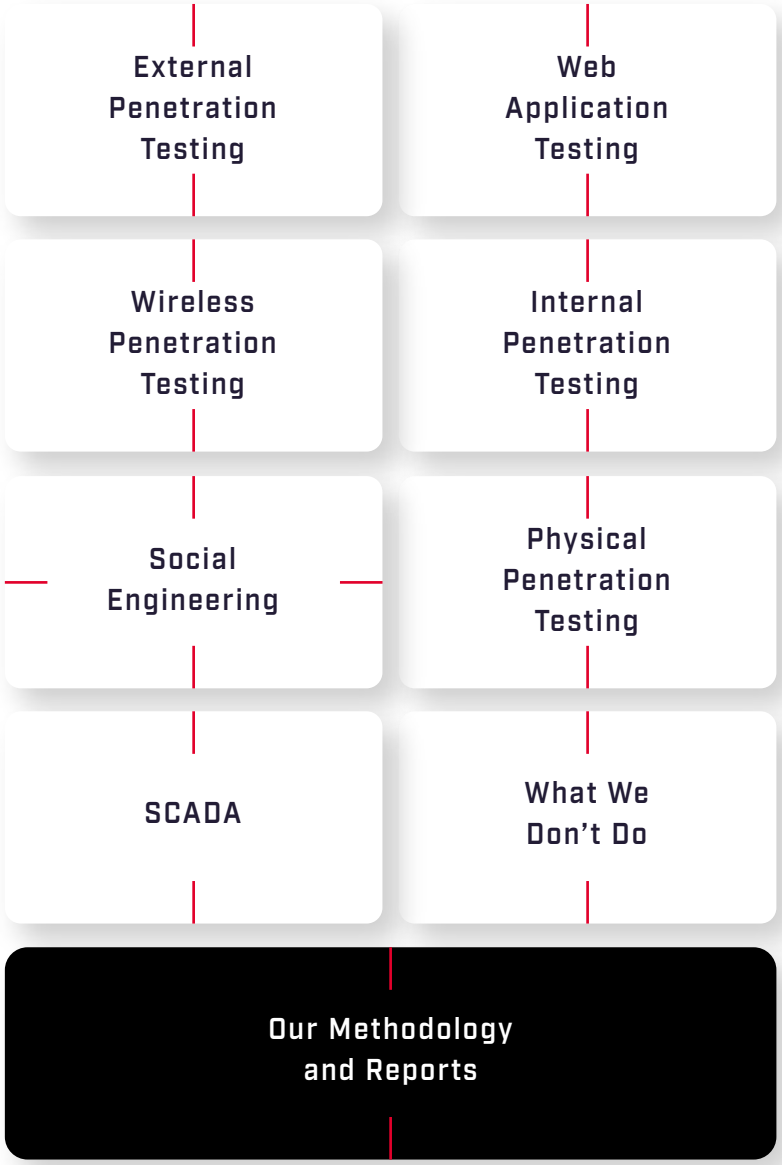
WHAT WE DON'T DO

- Checklist based assessments
- Assessments purely for standards compliance
- Automated Vulnerability Scanning
- Vulnerability Assessments
- Quarterly PCI Compliance Scanning
- DoS / DDoS Testing
- Revised Reports
- Brochure Reports
- Sample Reports from Past Clients
- Impact of Business Operations



OUR METHODOLOGY AND REPORTS

Our methodology is based on that taught as part of the OSCP certification course. It consists of passive reconnaissance, active intelligence gathering, network, host, and service enumeration, vulnerability identification and exploitation, privilege escalation, and access maintenance. We provide two reports, an executive summary, and a hack-log. The former will provide a high-level summary of the assessment. The latter will consist of complete, verbosely commented shell output from the attacking machine along with any screenshots necessary. This will allow administrators or developers to reproduce any actions undertaken by the assessor to understand and mitigate any vulnerability that was successfully exploited.



WHY DRAGON LABS?

Trust. Dragon Labs is a division of Comodo, a leader in the global certification authority and cybersecurity industry, for over 20 years, Comodo is a trust anchor for the Internet. Although definitions vary, in our view the most honest definition of a penetration test is simply a contracted attempt to hack an organization. As for ourselves, we make no pretense. We don't call ourselves 'white-hats' or even 'security professionals' and haven't used the word 'ethical' in this paper (yet). We're hackers and if you're going to hire hackers then they ought to be hackers you can trust.

As for ethics, while some vendors "focus on long term relationships with our clients to ensure they get the best penetration test possible" we at Dragon Labs know that the best penetration test possible is one performed by fresh eyes. Advanced penetration testing is as much an art as it is a science. Creativity is at least equally important as skill and nothing stifles creativity more than the tedium of repetitive tasks. With our clients' best interests at heart, we recommend that organizations either use a different vendor for every assessment or, if there are some vendors they prefer, to rotate them as much as possible. As for Dragon Labs, why not give us a try?

COMODO CORPORATE HEADQUARTERS
1255 BROAD STREET, CLIFTON, NJ 07013 USA

Experienced a breach? Contact us at (888) 551-1531
Visit **comodo.com** for your free 30 day trial