

POB 1596 Ramat Hasharon 47114, Israel  
www.c4-security.com  
info@c4-security.com

# C4



Command·Control·**Conquer**·Cure

## **When Protecting Critical Infrastructure and Command & Control Systems, the Best Defense is a Good Offense**

By using the same tools and methodologies that highly skilled and well funded attackers would use, C4 can test your security procedures, discover vulnerabilities and close any loopholes before they're exploited by someone else.



## THE THREAT

The world of Information Technology (IT) and the Internet has permeated every aspect of our lives, whether on a personal, business, national or even international level. Our global communication infrastructure is based on this technology and, as such, is vulnerable to attacks. The threat of a cyber attack on any level is daunting enough, but when considering the ramifications of cyber attacks on critical infrastructure and command & control systems, the potential damage is almost unthinkable.

But the possibility is very real and must be addressed. Our critical infrastructure, such as water treatment distribution, oil & gas pipelines, and electrical power transmission among others, uses SCADA systems which refer to central systems that monitor and control a complete site or a system spread out over a long distance. The applications used within the SCADA system are highly complex and sophisticated and are mostly proprietary command & control systems.

There are some that believe that their proprietary command & control systems are immune from attacks as they are not connected to the Internet. This could not be further from the truth for several reasons. Organizations that target these systems - whether terrorists, the underworld or enemies of the state - are extremely well funded and therefore have the means to hire highly skilled yet unethical attackers. In addition, the source of the threat does not necessarily need to be external, such as physically penetrating and overtaking a remote post and gaining access, but can also originate from the inner circle, such as from a disgruntled employee or bribed entity.



## THE SOLUTION

One of the most reliable ways to guard against cyber attacks is to regularly conduct Penetration Tests, also known as Ethical Hacking. Penetration tests, conducted by experts, are simulations of real attacks on the network, systems, and applications. These experts are able to identify weak spots and test the effectiveness of security controls within the system. While there are tools available in the market that can help repel or, in the worst case scenario, recover from these attacks, none is as powerful and effective as an ethical hack. In order to conduct a penetration test on a SCADA system, it's crucial to understand the controlled environment in terms of existing risks,

operational standards and critical infrastructure threats, and ensure that the tests are conducted by specialists who have the skills and experience to deal with proprietary systems and recreate the sophisticated and well funded attack scenarios that these unlawful organizations can perpetrate.



## INTRODUCING C4 - THE HIGHLY SKILLED TEAM OF EXPERTS

C4 consists of leading experts in the field of penetration testing and application security who have acquired an in-depth understanding of attackers' methodologies and unique knowledge and tools in analyzing protocols and reverse engineering. C4 specializes in attacking and protecting command and control systems and in the field of homeland security.

The main environments in which C4 concentrates include:

- SCADA/DCS and other civilian command & control systems
- Military command & control systems
- Trading applications of banks and other financial institutions

C4's unique knowledge and tools in analyzing protocols and reverse engineering applications are leveraged to ensure that all possible vulnerabilities are discovered and dealt with. C4 provides the following services:

- Penetration tests
- Tailored passive and active security products – loggers, IDS/IPS and firewall systems for the custom applications used in your environment.

The need for tailored security products arises from the long time period the SCADA software vendor needs to implement a fix. C4 provides a fast solution that does not interfere with the existing equipment.

C4's testing services are methodically applied to every component and application. The process of attacking and then securing a proprietary system is as follows:

- **Analysis** – Using our expertise and in-house toolkit for protocol analysis and reverse engineering, we obtain insight on how the system actually operates.
- **Attack** – Results of the protocol analysis are used in a two-pronged attack. Data is fed into C4's Intruder-L2™ which launches a wide spectrum of attacks; C4's highly skilled penetration experts use the data to challenge the system and use specific and tailored attacks. Results are analyzed by the team.
- **Protect** – Recommendations are provided for risk minimization. Furthermore, C4 can offer tailored passive and active products that add security functionality and control to the system.



C4 have provided their leading-edge expertise and unique knowledge and tools in analyzing protocols and reverse engineering to tier one companies including **Med1 Communications, Checkpoint, First International Bank of Israel, IDB Holdings, and Visa** among others.

**C4 - BECAUSE THE BEST DEFENSE IS A GOOD OFFENSE**