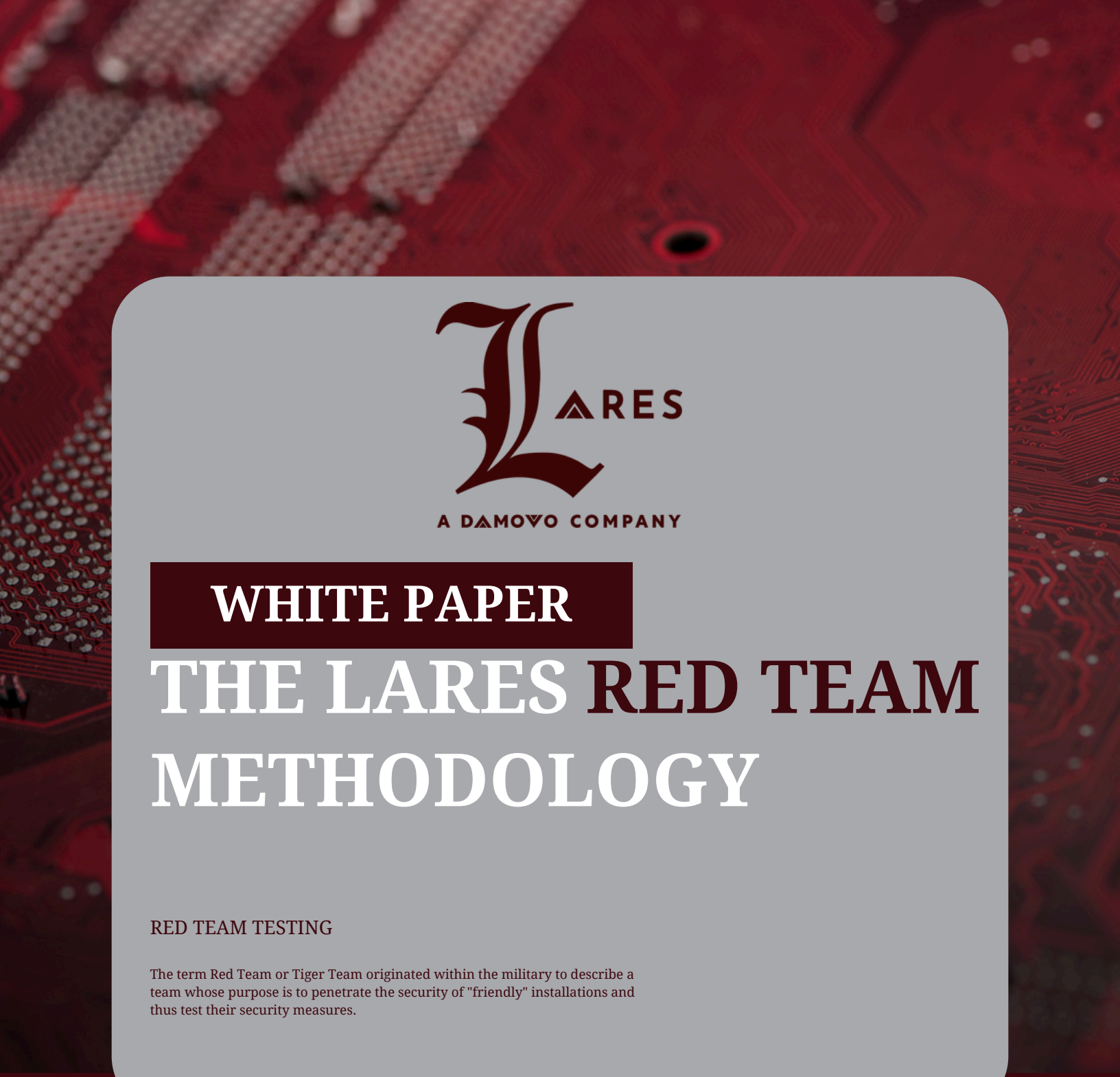


WHITE PAPER

THE LARES RED TEAM METHODOLOGY

RED TEAM TESTING

The term Red Team or Tiger Team originated within the military to describe a team whose purpose is to penetrate the security of "friendly" installations and thus test their security measures.

ABOUT LARES

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching since 2008.

For more information, visit lares.com, contact us at (720) 600-0329, or follow Lares on Twitter @Lares_.

CONTACT INFORMATION

1580 N. Logan St. Ste 660, PMB 79199, Denver, CO 80203, USA

+1 (720) 600-0329
sales@lares.com

Executive Summary

A Red Team exercise is a real-world test of your security controls, policy, technology, and infrastructure effectiveness. In this style of testing, the engineering team tested many types of attacks through a combination of the following Physical, Social and Electronic techniques.

Methodology Overview

- Intelligence gathering
- Phone conversations
- Onsite visits
- Electronic solicitation
- Wireless testing
- Penetration testing
- Physical security testing
- Infrastructure footprinting
- Email address details
- Documents and sensitive data
- Individual profiling
- Reporting

LARES
A DAMOVO COMPANY

Intelligence Gathering

The Lares Intelligence Gathering methodology is a custom-designed approach that analyzes multiple attack vectors across various levels of business and personal landscapes to provide a realistic assessment of the exposure an organization can face in today's business world. These various landscapes are combined during the assessment phases to deliver a unique view of the blended threats an organization must be adequately prepared to protect against.

After conducting this type of intelligence analysis on the organization, Lares will begin looking at the various attack vectors through testing and investigation, such as:

Phone Conversations

In this exercise, the engineer will engage internal employees via phone and perform various scripted dialogues. These scripts will portray the engineer in several possible roles, such as a helpless user, an important user, or a technical support engineer. In some cases, the engineer may directly question the user without pretext to assess how willing employees are to disclose confidential information.

If successful, the engineer will have gained the employee's trust and will attempt to extract different types of information from the user. Some examples of information the engineer may target include:

- Usernames
- Passwords
- Organizational chart structure
- Internal phone numbers
- Corporate Intelligence
- Financial Information
- Physical Access

Onsite Visits

In this exercise, the engineer will engage employees in person. The engineer may take on several roles to gain the employees' trust. Such functions include a helpless user, an important user, a technical support engineer, or a public authority. The onsite social engineering exercise aims not only to acquire internal corporate information but also to gain physical access to restricted areas. By gaining the trust of employees, the engineer may be able to:

- Gain physical access to employee-only areas of the building through tailgating
- Gain physical access to restricted network closets
- Gain physical access to restricted computer rooms and data centers
- Acquire visitor proximity badges
- Various forms of solicitation
- USB key and CD drops

Engineers may combine the exercise of phone conversations with an onsite visit in the form of a pretext call. This pretext call prepares an employee within the organization that a technical representative will be visiting them. This prepares the employee to expect the engineer and attempts to establish a path of least resistance for the engineer to gain physical access to the internal resources listed above.

Electronic Solicitation

In this exercise, the engineer will attempt to convince an employee to disclose internal information through email solicitation. The engineer will first construct an email visually resembling an internal email broadcast. Embedded within this email is a link to an externally hosted website. The exercise aims to convince the employee to click the link and connect to a website that the engineer controls.

The website may contain different forms of content. The first type of content is a web page containing a malicious payload. When viewed in a browser, the program attempts to exploit local vulnerabilities in locally installed software on the employee's workstation. Using this attack method, the engineer can assess an organization's patch management presence and diligence. If successful, a software agent will be deployed on the employee's workstation, allowing the engineer remote access to an internal network resource.

The second type of content is a web page that resembles an internal corporate intranet. This phishing attack solicits the employee for their username and password to obtain access to an internal resource. If successful, the employee will submit their username and password to a secure server that the engineer controls. This information is recorded and can be used at a later time to acquire access to externally-available resources such as email.

Wireless Testing

This type of testing will identify attempts at gaining access to wireless networks through open and available networks at the facility or identifying weaknesses in wireless implementations. In addition, compromising vulnerabilities in the wireless infrastructure to gain unauthorized access to networks and systems will be reviewed.

Penetration Testing

A penetration test is a proactive and authorized attempt to compromise information security and access sensitive data by taking advantage of vulnerabilities. A penetration test is a proactive and authorized attempt to compromise information security and access sensitive data by taking advantage of vulnerabilities.

Physical Security Testing

The process begins with a characterization of the facility, including identifying the undesired events and the respective critical assets. Guidance for defining a design basis threat is included for using the definition of the threat to estimate the likelihood of an adversary attack at a specific facility. Upon determination, the engineers attempt to understand the ability to carry out stated attacks on the facility to include, but not limited to:

- Lock Picking
- Magnetic Door brute forcing
- Alarm system avoidance
- Ventilation system entrance
- Social engineering
- Tailing
- Procurement of badge access
- Solicitation
- Access System bypass
- Camera redirection

Infrastructure Footprinting

In the Infrastructure Foot Printing section, the consultant will discover how much infrastructure exists, what type of infrastructure is used, where it is located, what technology is used, and how it is structured.

This type of information is useful for the following:

- Security assessments (as this is the first and most tedious phase of any external review)
- Gaining an idea of the organization’s Internet and geographical presence
- Gaining insight into the technology used by the organization
- Making connections between seemingly unconnected organizations (as they might be sharing common infrastructure)
- Gathering a list of brands or affiliations supported by the organization

Email Addresses

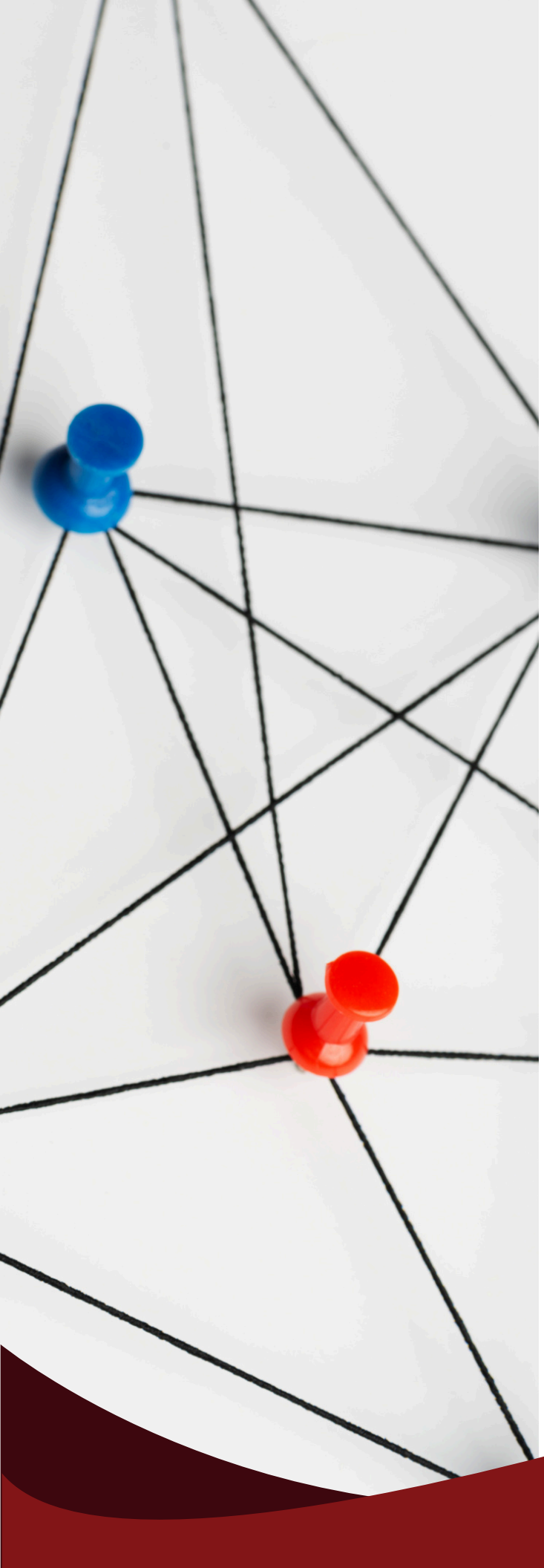
At this stage, the consultant will seek to provide a list of email addresses in any domains identified in the previous step. These addresses will be verified, and social network memberships will be determined where possible. These social networks will locate details such as full names, gender, and geographical location. Due to the nature of this service, full details can only be obtained on certain social networks.

This is interesting for:

- Gaining an idea of how many people are employed at the organization
- Geographical/age/gender distribution of organization's members (where possible)
- Where possible, information leaks have/could happen
- Where unauthorized communication between employees and competitors has or could happen

Documents and Sensitive Data

At this stage, the consultant will start looking for documents or files containing interesting or sensitive information about the organization. This may include confidential information that was leaked to the Internet, directories able to be indexed on web servers, internal memos and phone directories, internal presentations, budgets, minutes of meetings, etc., where possible, and metadata will be extracted from the documents and files.



Person Profiling

The consultant will attempt to profile a person by gathering publicly available information. Although such a profile can be compiled on any individual, it is envisioned that such profiles would be completed for key organizational personnel such as board members, executives, and upper management.

This information is useful for the following:

- Completing the due diligence process in a possible sale
- HR-related investigations on specific individuals
- Discovering and Minimizing information on the internet concerning high-profile individuals

Because the profile is constructed using public internet information, accuracy and completeness cannot be guaranteed. Such a report will consist of personal information, including:

- Full names
- Age
- Gender
- Work Experience
- Educational Background
- Family Relations
- Personal Interests
- Email addresses (both personal and work)
- Social network memberships
- Relevant postings to groups/forums/mailing lists
- Club and board memberships
- Articles / interviews
- Telephone numbers
- Known associates

Reporting

A detailed report will be delivered following the ISACA IT Audit Framework (ITAF) Reporting Standards. The report will include:

- Scope
  - The identification or description of the activities, the period under review and when the engagement was performed, the nature and extent of the work performed, and any qualifications or limitations in scope.
- Summary
  - A summary of the work performed to help better understand the nature of the assurance provided.
- Control deficiencies
  - Management shall be made aware of internal control deficiencies that are less than significant but more than inconsequential.
- Observations, findings, conclusions, and recommendations
  - Findings, conclusions, recommendations, and cost estimates (if available) shall be provided for corrective action.

At the end of a Lares Red Team engagement, a detailed debrief session with management and key stakeholders is always held to address any questions, comments, or concerns regarding the exercise.

Conclusion

A red team exercise is a real-world test of your security controls, policy, technology, and infrastructure effectiveness. In this style of testing, the engineering team tested many types of attacks through a combination of the following Physical, Social and Electronic techniques. If you want to learn more about red teaming or how our experts can help scope and execute an effective test for your business, please contact us. We would be happy to discuss the many ways in which we can help keep your organization safe. Thank you for reading!

ABOUT LARES

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching since 2008.

For more information, visit lares.com, contact us at (720) 600-0329, or follow Lares on Twitter @Lares_.

CONTACT INFORMATION

1580 N. Logan St. Ste 660, PMB 79199, Denver, CO 80203, USA

+1 (720) 600-0329
sales@lares.com