



COLDSTREAM ENGINEERING LTD.

WHITE PAPER:

TACTICAL FIELD COMMAND AND
CONTROL FOR TIGER TEAMS

BY SEAN ROONEY

©ColdStream Engineering Ltd. 2000

All rights reserved. We provide this whitepaper with the intent of exchanging ideas. Use of this document, in full or part, cannot be made without consent of ColdStream Engineering Ltd. Modifications are expressly forbidden.

TACTICAL FIELD COMMAND AND CONTROL FOR TIGER TEAMS

The sudden proliferation of Internet connected networked systems has opened great potential and great vulnerabilities for companies that only recently began to truly understand the real power of the Internet. With this in mind, they have begun building network security mechanisms into their Internet connection points such as firewalls and packet screening routers. Some, who are engaged in the new world of “Electronic Commerce”, have started to use digital authentication and encryption in an effort to reduce the possibility of credit card number theft from attackers connecting to their sites through the Internet.

With all of this in mind, there is now a requirement that is ever expanding to perform testing of security systems to prove the real effectiveness of these mechanisms. However, some of the standard rules of audit require the use of impartial independent third parties. These practices have been standard in business accounting audit for many years. How does one then apply these basic concepts to third party computer security audit practices?

The basic element of any audit team is the use of at least two personnel. The reason for this is to ensure that audit findings can be cross verified and to prevent tampering. The auditors are generally trusted entities and are generally very careful about what they do and how they do it. Accounting auditors have a very easy job compared to that of a computer security auditor simply because accounting is relatively limited in scope where as a computer security auditor frequently finds his or her self working in totally new electronic environments that simply did not exist or were even technically possible as recently as the previous year.

The following structures are suggested as a possible way to proceed with the structure of a computer security penetration team [frequently referred to as a “Tiger Team”]. Tiger Teams are a reference originating in the military as the security audit teams, which investigated the effectiveness of military physical security by breaking and entering the premises. [This exercise frequently preceded a procedural security audit or base inspection by senior officers at which point, all hell broke loose].

The principle issues to be dealt with are as follows:

1. Verify the accuracy and validity of findings.
2. Prevent tampering or interference with the audit.
3. Maintain information and generate reports that are legally irrefutable.
4. Be able to introduce and use the findings in a court of law.

Let us take for example, a network manager knowingly builds a substandard Internet connected network system that introduces liability and vulnerabilities to his employer. This manager may not audit this system or use people directly involved in its construction to audit this system, as the pre-knowledge would invalidate the accuracy and validity of the findings. The audit by its nature would be tampered with simply by virtue of the manager knowing what the problems are but wanting to hide them either for political reasons, reasons of simple incompetence or for budgetary reasons that would be introduced in order to fix the problems. If the company then was exposed to liability by exploitation of one of these vulnerabilities, the manager AND the auditors he/she put in place under his direction would likely be responsible for that liability having occurred. *An example of this might be an improperly configured mail server that allows an external attacker to use it to forward offensive or illegal materials to millions of Internet users [including clients of the employer] in a way that makes it appear that this originated from the employer.*

The cure is to find an independent third party who is then directed and enabled to conduct an orderly and thorough audit of the system, compile the findings and generate a report of these findings, with the option to make recommendations for remediation of the vulnerabilities.

Structures:

A Tiger Team should ideally have the following:

1. A minimum of two or three personnel;
2. A clear set or Rules Of Engagement for the operation;
3. A clear set of objectives to meet;
4. Secured communications;
5. Centralized command and control; and
6. Principal responsibility centers.

With these requirements in mind, it may be suggested that the following structure diagram applies:

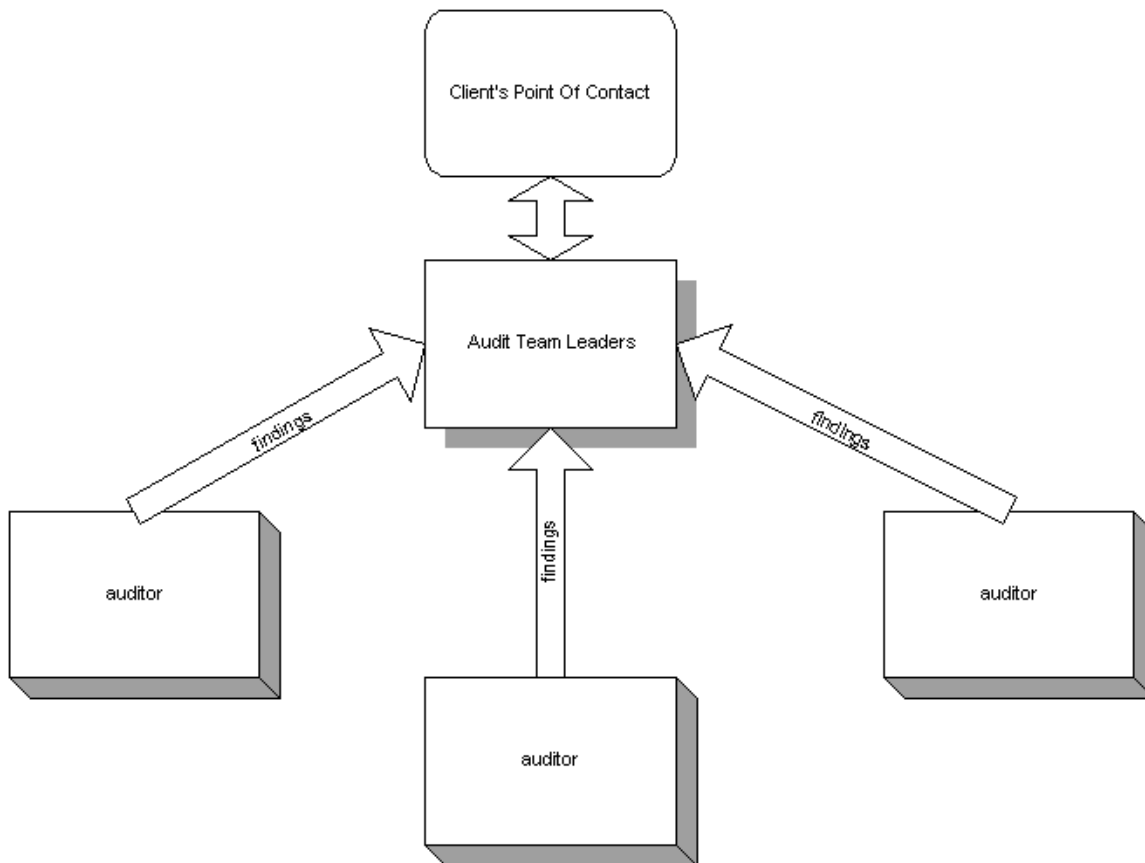


Diagram Definitions:

1. Group Leader [could be two personnel co-leading] [responsible for]
 - a. Commanding and coordinating the unit members
 - b. Ensuring the findings and operations of members is complete

- c. Ensuring compliance
 - d. Being principal point of responsibility
2. Team Members [responsible for]
- a. Conducting specific audit operations
 - b. Transmitting the findings to Group Leader

Team Member functions:

1. Connectivity specialist
2. Applications specialist
3. Firewall and network specialist

General rules of engagement:

1. The Team Leader should directly command the operations of each individual team member.
2. No single team member should be aware of the operations or [in some cases] identity of any other team member so as not to taint the findings of the audit.
3. ALL communications should be done using secured communications. This primarily could include the use of encrypted email, and STU-III secure telephone equipment, as well as trusted secured couriers.
4. ALL operations shall be conducted in coordination with the client.

Once completed, the findings of the audit should be released to the client in the following forms:

1. A summary [short]
2. A complete form of the audit report including ALL input data, description of actions taken, and the results.
3. Optionally; a set of recommendations to remediate the problems uncovered.

All reports should be considered to be extremely sensitive. The reports should be printed and bound as a paper set, numbered and signed by the principal responsibility center [Team Leader]. In some cases, the complete report may be so large as to preclude printing and binding. [i.e.: 8000 pages]. Therefore it is recommended that these be burned onto CDROM as it is immutable, clearly labeled and include the signature of the principal responsibility center [Team Leader] ON the CD label proper in immutable pen or marker. Electronic copies of this should be saved in a form that is difficult to tamper with. Adobe Acrobat format plus digital signature using an encryption tool such as PGP has been found to be acceptable for authentication of the electronic document when the digital signature is printed on paper and signed by the principal responsibility unit.

Some Legal Notes:

Given that the base operations of an electronic audit of a computer security system may accidentally cause damage to the clients systems and involves potential access to proprietary data, it is strongly recommended that the following procedures be applied *before* the start of any such operation in the field.

1. ALL members must sign Non-Disclosure Agreements with the team leader
2. The audit team must sign a Non-Disclosure Agreements with the client
3. The audit team leader must inform the client of potential damage that might result from the audit. [such as server crashes etc.]
4. The client must acknowledge this in writing with a signature of a principal of the client. [such as president or CIO]
5. The client should sign a temporary liability waiver for the audit team
6. The entire operation must be covered under a contract.
7. The audit team MUST be informed fully of the rules of engagement as agreed to jointly by the audit team leader and the client.

Closing Notes:

It can be argued that given the explosive growth of Internet connected commercial operations, new technological vulnerabilities dictate that due diligence is no longer merely a matter of a background check and a contract, but rather a complete examination of procedural, technical and policy environments.