High-level Methodology for Carrying out Combined Red and Blue Teams

N Veerasamy
Defence, Peace, Safety and Security (DPSS)
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
nveerasamy@csir.

Abstract— **Security audits and penetration testing exercises serve to determine the baseline of the security in a network/system and to identify possible avenues of exploitation. Red and Blue Team is the name given to the combined execution of these risk assessments that consist of various operational, managerial and technical activities. However, to successfully complete a combined Red and Blue Team Mission a number of principles play a significant role. This paper proposes a combined Red and Blue Team Methodology to guide the process of carrying out such security auditing and penetration testing tasks.** *(Abstract)*

Keywords- audit, penetration testing, Red and Blue Team, security

I. INTRODUCTION

Assessing the current security baseline in an organisation has become a critical priority in preventing exploitation. Information and information assets have become the lifeblood of organizations and the protection of these assets is one of the major aspects that management has to deal with [1]. Red and Blue Teams are one such means of carrying out an evaluation to determine the current security level.

Red and Blue Team missions can be seen as a form of ethical hacking, whereby the security specialist is hired by the company to investigate vulnerable areas in the system. Palmer speaks about how organisations have come to realise that one of the best ways to evaluate the intruder threat would be to have independent computer security professionals attempt to break into their computer systems to evaluate the target system's security and report back to the owners with the vulnerabilities and possible solutions [2].

The approach of a Red Team is based on the premise that an analyst who attempts to model an adversary can find vulnerabilities in an information system that would otherwise go undetected [3]. However, from a Blue Team point of view vulnerabilities can also be detected early on. Thus, by carrying out Red and Blue Teams, a proactive approach at detecting and protecting a system from the exploitation of vulnerabilities is thus taken.

Red Teaming is a technique commonly used in the military to uncover system vulnerabilities or to find exploitable gaps in operational concepts, with the overall goal of reducing surprises, improving and ensuring the robustness of the Blue ops concepts [4]. It can thus be seen that Red Teaming explores the technical aspects through which the system can be manipulated while a major focus area of the Blue Team is to devise managerial and operational means to protect the system.

When done in simulations, the behaviour space is divided into two groups; one controlled by the Red Team which represents the set of adversary behaviours, while the other is controlled by the Blue Team which represents the sets of defenders [5].

However in practice, various areas of the technical and safeguarding activities do overlap and thus a merged methodology is proposed. For example, during a Red Team Exercise when technically investigating a vulnerability, it is also feasible to formulate possible solutions from a Blue Team perspective. Information gathering is also a task that crosses both domains as details about the target and avenues of manipulation impact both the Red and Blue Team evaluation. The two perspectives are linked in that threats identified by the Blue Team can be attempted to be exploited by the Red Ream when carrying out penetration testing. The Blue Team can then feed off the successful penetration attempts and highlight issues so that mitigation mechanisms can be implemented to prevent future attacks. In this way, it can be seen that a combined Red and Blue Team Methodology aims to provide a detailed security baseline of the system by providing information on both exploitable means and defensive strategies.

The proposed methodology helps to structure a complex field that often consists of various information security practices. The methodology serves to better guide the documentation of activities and ensure that a wider range of information security topics is covered. By clearly formulating a methodology some of the vagueness associated with carrying out a security audit (which consists of various information security activities) is hoped to be eliminated.

Security is a delicate balance among protection, availability and user acceptance [6]. A Red and Blue Team contributes to security in that the findings can reveal the means through which systems can be exploited and thereafter better secured.

A major benefit of a Red and Blue Team is to establish the security baseline in the organisation. This can be utilised for further audits and security assessments. Measurement data can be produced from a Red and Blue Team and is useful for the identification of critical issues and the formulation of strategic objectives. In addition, the recommendations provided by a Red and Blue Team can help reduce the occurrence of exploitations and develop other mitigation instructions.

The remainder of the paper is structured as follows: Section II introduces the high-level view of the methodology. Focus areas and objectives are discussed in Section III before the paper is concluded in Section IV.

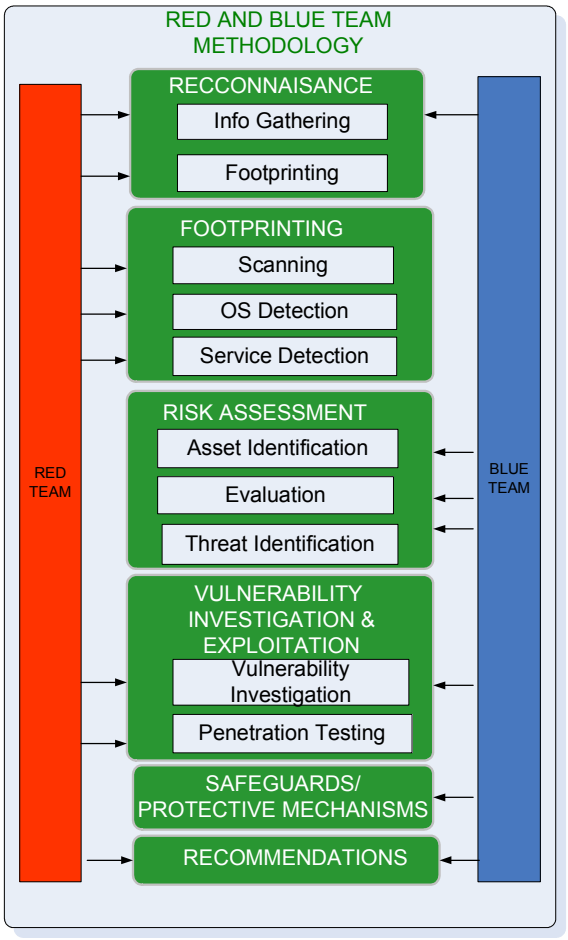

Figure 1. Red and Blue Team Methodology

II. PROPOSED METHODOLOGY

This section proposes a high-level methodology to guide the execution of Red and Blue Teams. Previous work in Red and Blue Teams formed the basis of the proposed methodology. Experience and applied knowledge was thus used to further formulate the approach and processes taken when carrying out Red and Blue Teams. Figure 1 schematically presents the proposed high-level framework.

Each grouping of activities will be elaborated on. The purpose of the various stages is to group similar activities together and to promote a progression of development. By using broad categories, the methodology can be adapted as new activities are identified. Activities do not exclusively belong to a single category. However, it is often the case that an action is repetitive or fulfils an objective in a number of the categories. For example, scanning can occur in the Reconnaissance and Footprinting tasks. Sniffing the network can fall into information gathering (studying network activity) and vulnerability exploitation (by getting access to sensitive data if it is transported in plaintext). An adaptive and collective approach is promoted, in that once a particular piece of information is found, the lead can be followed until achieving a successful exploitation.

That preliminary information discovered can serve other purposes and direct the way to other findings. For example, it is often found in exercises that an initial scan can lead to the identification of a user account with a blank password. This can be used to create a null connection to the machine and download the password file. Thereafter, the password file that has been retrieved can be cracked and a wider range of user accounts targeted. The initial scan can also provide information on dormant accounts or accounts not complying with the password policy.

The high-level approach of the Red and Blue Team Methodology is to gather as much information as possible, assess the situation, detect avenues of exploitation and thereafter to take advantage of the identified vulnerabilities to determine the extent that the system can be manipulated. The methodology depicts activities that have been grouped. However, in practice it has been found that the completion of a Red and Blue Team will not follow the methodology in a strict sequential order but rather disperse among the various activities. The methodology therefore serves as abstraction of principles guiding the execution of a Red and Blue Team. In the next few Sections, descriptions of each grouping will be provided

III. FOCUS AREAS

In this Section, the activities in each grouping will be further discussed, commencing with Reconnaissance.

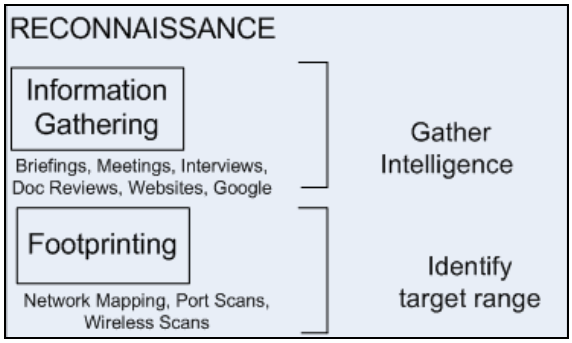

Figure 2. Reconnaissance

A. Reconnaissance

The Reconnaissance stage consists of the activities shown in Figure 2. The main objectives are initially to gather intelligence and thereafter identify the target range.

1) Information Gathering

Each security assessment begins with a rigorous attempt to gather all source information on the subject of interest [3]. During the information gathering process, technical details relating to the IP range, configuration settings and applications can be revealed. This will assist the Red Team with their interaction on the systems/networks. From a Blue Team perspective, information pertaining to policy compilation and conformance can be gathered. Information gathering, which helps describe the current status and problem areas can be carried out in the several ways and includes:

a) *Briefings and meetings*: Prior to the execution of a Red and Blue Team, briefings will be held to provide the Team members with contextual information. Thereafter meetings can be held at regular intervals. Meetings provide a means of tracking progress and providing updates.

b) *Interviews*: On-site interviews will be carried out with various personnel members (users, administrators, support personnel, managers, etc.). This helps provide insight from various operation levels (technical, managerial and varying degrees of control). A valuable output from the interview process is that issues that are normally overlooked can be raised. Assumptions and problem areas can be identified.

c) *Document Review:* It is essential to review security policies, operational guidelines and previous assessments. Network diagrams are also useful for describing the setup of the network. The documentation helps to better understand the current level of security and can provide previous measurement data.

d) *Internet and search engines*: Web sites are a wealth of information. Systems configurations, details of the target, contact information, IP ranges, etc. can all be sourced from online resources. Through the use of services like whois, nslookup and Domain Name Server (DNS), queries technical information relating to the target can be extracted.

Reconnaissance also consists of initial Footprinting activities, which will be discussed next.

2) Footprinting

Footprinting helps profile an organization by allowing for the discovery of domain names, network blocks and IP ranges. While there are many types of Footprinting techniques, they are primarily aimed at discovering information related to the following environments: Internet, intranet, remote access and extranet [7]. The main aim of the Footprinting stage is to identify the target range. A few Footprinting techniques are discussed next:

1) *Network mapping*: Network mapping helps to visualize the layout of the network and forms the baseline of the number of users and devices. With automated technology, convenient network maps can be constructed with different layout preferences. "Once you can see the data succinctly; it becomes much easier to understand [8]". However, network maps are also a rich source of information relating to the type of devices present and technical details pertaining to them (like services and location).

2) *Port scans*: Port scans assist in identifying open ports and the services running on these ports. This is especially important for identifying active devices, which can become possible targets and the means through which they can be exploited.

3) *Wireless scanning*: Deraison and Gula explain that when users add wireless access points, they may be opening the network for unsecured access by remote users and thus security breaches [9]. Through wireless scanning, insecure access points and possibly attackers can be detected. Wireless scans can thus provide information relating to vulnerable networks. Initially carrying out a wireless scan helps profile potential attackers and help with incident management. For example, the name of the wireless network, form of security (use and type of encryption), and registration details can be obtained from a wireless scan.

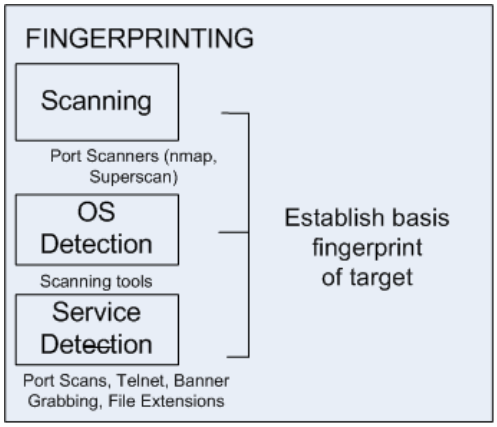

Figure 3. Fingerprinting

B. Fingerprinting

Fingerprinting activities relate to identifying the type of operating system that the (critical) system is running (Figure 3). Specific operating system (OS) information will be useful during the vulnerability mapping phase [7]. Fingerprinting can take place through scanning, operating system detection and service identification [10].

Operating system and service detection help identify specific means through which a system can be exploited. Thus, through the use of scanning technology, the fingerprint information of the system/network can be accurately captured. For example, the detection of a certain web server and version can indicate the type of operating system the machine is running. Port scanners also indicate services running in specific ports. In this way, the fingerprinting exercise serves to provide underlying

information on the target that can later be used to exploit the system.

C. *Risk Assessment*

Risk is the possibility that some incident or attack can cause damage to your enterprise [11]. A risk study helps to identify possible actions by adversaries to disrupt operations and also to assess critical resources. During Risk Assessment, the Blue Team will determine the importance of assets and determine possible threats. Figure 4 shows the activities in a Risk Assessment:

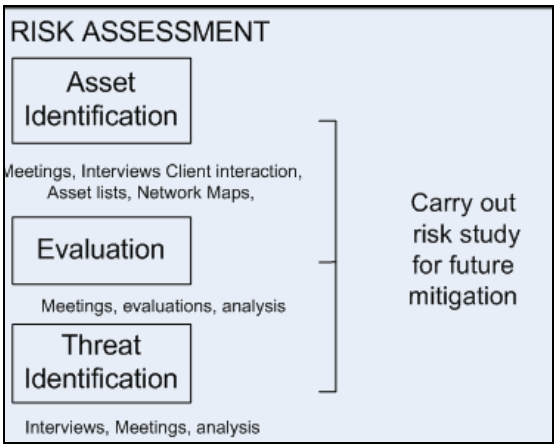

Figure 4. Risk Assessment

a) *Asset Identification*: Assets can be hardware, software, data/information or reputation [11]. Client-interaction in this task is encouraged as its helps identify critical assets in the organization. Protection and backup mechanisms can be checked.

b) *Evaluation*: In this task, the value of the asset is measured to determine its significance to operations. Considerations include, the monetary cost of the asset, replacement cost, insurance, the functional value of the device or data (classification and criticality), requirement for further operations and the availability and efficiency of the asset. Assets can be classified according to their level of importance: those that are essential for the continuation of the business operation; those that are required for effective functioning; and those that are not essential or can easily be replaced.

c) *Threat investigation*: This serves to identify possible actions than an attacker could use to damage assets and also determines whether protective mechanisms are sufficient.

An impact level can thus be allocated to each threat so that prioritization and mitigation techniques can be formulated. Different rating scales can be used to indicate the significance, impact and probability of the threat. A qualitative rating of high, medium or low can be assigned or a quantitative value between 0 and 5 for example. Threats can also be categorised as deliberate, unintentional or environmental.

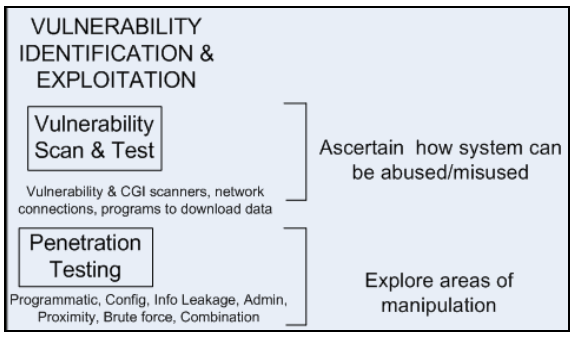

Figure 5. Vulnerability Identification and Exploitation

D. *Vulnerability Identification and Exploitation*

When carrying out Vulnerability Identification and Exploitation, vulnerabilities can be identified through through scans and other tests and thereafter attempted to be exploited through penetration testing exercise (see Figure 5). More details of these activities follow:

1) *Vulnerability Scan and Test*

A common technique for testing for vulnerabilities is through the application of automated scanners The Red and Blue Team can thus use scanners to provide direction as to how a system/network can be manipulated. Types of scanners include Common-Gateway Interface (CGI) scanners or cross-site scripting tools.

Another test for vulnerabilities is to probe the system. Probing can proverbially be considered as the "tossing out of the net into the sea" and gauging what can be found. By checking for unlawful network connections or the ability to download data inappropriately, these weaknesses can be identified and blocked in the future.

Another form of probing the system is through enumeration activities that attempt to gather basic user information. Null connections to the system can gather fundamental data like user names and the password policy, which can then be used to gain entry into the system. In this way, detection of vulnerabilities is initially attempted. This is important because from the Red Team perspective scanning and probing can indicate a route that can be used to gain access to a system/network whilst the Blue Team can identify gaps in the defensive capability. Thereafter, the actual pilfering of the system will occur by the Red Team during penetration testing.

2) *Penetration Testing*

Bishop explains that penetration testing or ethical hacking is not only the breaking into systems to see how hard it is but also the detailed analysis of threats and potential hackers in order to be most valuable [12]. Various exploits can be attempted, programmatic (architecture issues), configuration (password policy), information leakage (infer information from error messages), administrative (social engineering), proximity (utilise resources inappropriately) and combinations of

these attacks. Wireless data or password files can be cracked through brute force, which would allow for access to the system. Technical examples of penetration testing include the extraction and cracking of password files, creating a null connection and performing a zone transfer (creating an accessible share on the targets drive), sniffing the data to retrieve sensitive information, uploading and executing malicious programs, exploiting a service (e.g., Dameware) to remotely control a device and using collected information to spoof a device.

During penetration testing, identified vulnerabilities can be further investigated to determine their impact. For example, an account that has blank password can be attempted to be logged into and determine what data is accessible. Another example would be that whilst interacting with a web page and a Structured Query Language (SQL) error message pertaining to tables in the database is displayed, the tester could escalate this vulnerability and attempt an SQL injection attack. The security tester must probe directly and deeply into security risks (possibly driven by abuse cases and architectural risks) to determine how the system behaves under attack [13]. Thus, during the penetration testing phase, areas of manipulation are explored.

E. Safeguards

This area of a Red and Blue Teams described preventative, detective and reactive security mechanisms that have been implemented. The Safeguards review will look at safety mechanism implemented. Examples of safeguards/protective mechanisms include technical measures like intrusion detection mechanisms as well as procedural activities like disaster recovery planning. The main aim is to determine whether these measures are operational and sufficient.

F. Recommendations

In this phase, recommendations are provided to the key players so as to guide the mitigation of risks and the reduction of controllable vulnerabilities. Throughout the Red and Blue Team, vulnerable areas will have been identified. The security specialist will also be knowledgeable in preventative mechanisms/ methods that can be implemented to better improve the security. Guidelines and directives for corrective action can be promulgated to concerned parties so that informed and improved strategic, budgetary and tactical decisions can be made.

G. Conclusion

The main aim of this paper was to propose a methodology for the execution of Red and Blue Teams. Red and Blue Teams consist of various security auditing and penetration testing tasks which serve to determine the current security baseline in an organisation. The practice of Red and Blue Teams has demonstrated that various data gathering, assessment and technological based activities form the foundation. In this way, the different activities were organised so as to structure and guide the execution of a combined Red and Blue Team. Similar tasks were grouped together. It is often the case that tasks did not strictly belong to one category. In many instances activities will overlap. However, the methodology does helps to organise a field that consists of various computer and network security practices. The methodology thus consists of a high-level approach when carrying out a Red and Blue Team.

H. References

[1] H.A. Kruger, L. Drevin, and T. Teyne, “Towards a framework for evaluating ICT security”, in Proceedings of Information Security South Africa Conference (ISSA), June 2005.

[2] C. Palmer, “Ethical hacking”, IBM System Journal, Issue 40-3, 2001.

[3] B. Wood and R. Duggan, “Red Teaming of advanced information assurance concepts, Defence Advanced Research Projects Agency (DARPA)”. Information Survivability Conference and Exposition, Volume 2, 2000, pp. 112-118.

[4] C. Seng, C. Lian and T. Su-Han Victor, “Automated Red Teaming: A proposed framework”, Proceedings of the 9th Annual Conference on Genetic and Evolutionary Computing, July 2007.

[5] A. Yang, H. Abbassm and R. Sarker, “Characterizing warfare in Red Teaming, Systems, Man, and Cybernetics, Part B”, IEEE Transactions, Vol. 36, Issue 2, April 2006, pp. 268 – 285.

[6] E. Lo and M. Marchand, “Security audit: A case study”, Canadian Conference on Electrical and Computer Engineering, Vol.1, May 2004, pp 193-196.

[7] S. Mclure, J. Scambray and G. Kurtz, Hacking exposed, Network Security Secrets and Solutions, USA: Osborne/Mcgraw Hill, 2001.

[8] H. Burch and B. Cheswick, “Mapping the Internet”, Internet Watch, vol. 32, April 1999, pp.97-102.

[9] R. Deraison and R. Gula, “Using Nessus to detect wireless access points”, Whitepaper from Tenable Security, Available online from http://www.tenablesecurity.com/whitepapers/wap-id-nessus.pdf, Accessed 15 May 2008.

[10] Sensepost Training Providers, Hacking by numbers: Cadet Edition, Adapted from the Cadet Training Edition course slides, November 2007.

[11] D. Gollman, Computer security, West Sussex:Johan Wiley & Sons, 2006.

[12] M. Bishop, “About penetration testing”, Security & Privacy, IEEE, Volume 5, Issue 6, Nov.-Dec. 2007, pp. 84 – 87.

[13] B. Arkin, S. Stender and G. McGraw, “Software penetration tesing”, IEEE Security & Privacy Magazine, IEEE 2005.