

Abstract

Title: When Not to Pull the Plug

Authors: Scott Knight, Sylvain Leblanc, Royal Military College of Canada

The classic response to attack in computer networks has been to disconnect the effected system from the network, preserve the information on the system (including evidence of the attack), and begin a forensic investigation. However, it can be argued that this type of response is not appropriate in many situations. Immediate removal of the effected machine from the network cuts off back-link communications with the attacker. Breaking contact with the attacker alerts the attacker to the fact that he was discovered and significantly impedes the effort to collect intelligence about the attacker and the attack. Understanding the adversary is essential to effective defence. Breaking contact often leaves the defender not knowing who the attacker is, what the current mission of the attacker was, what the capability of the attacker is, where else the attacker has been successful in infiltrating systems, and what the strategic goals of the attacker are. Therefore, the first response to an attack should not always be to immediately break contact. Instead it may be appropriate to respond with a defensive counter-information operation (IO counter-measure) to observe the activity of the attacker.

The aim of this research is to enable this new kind of operation through the identification and development of the new tools and techniques required. This paper is an omnibus presentation of a group of research projects associated with satisfying this aim.

A difficulty in conducting this type of operation is that the attacker may have administrator privileges for the operating system of the effected computer system. Observation tools risk being detected and subverted by a sophisticated attacker. An important capability is the development of the new tools a defender needs to maintain the "high ground," that is, to enable undetected observation of an attacker with administrator privileges. Another important capability is the provision of tools to maintain an active cover-story of routine operations on the system. For example, in order to convince the attacker that he is engaged with a valuable end-user computer system there is a need to provide an artificial stream of keyboard and mouse events consistent with a real user interacting with the system. The research also investigates the need for a firewall-like device that can be used to mitigate the risk the effected system poses to the rest of the network, without tipping-off the attacker. Maintaining contact with the enemy on our own systems has inherent risk. This risk can be controlled by carefully controlling, blocking, spoofing and modifying interactions between the effected system and the rest of the network.

The paper presents the results of the research projects addressing these issues and demonstrates that new tools and techniques can be developed to satisfy the requirements for conducting defensive counter-information operations. The argument for the tools and techniques described is presented in the context of an illustrative defensive counter-information operation.