ELSEVIER

Computer Networks 34 (2000) 671–697

COMPUTER NETWORKS

www.elsevier.com/locate/comnet

Intrusion-detection for incident-response, using a military battlefield-intelligence process

J. Yuill *, F. Wu, J. Settle, F. Gong, R. Forno, M. Huang, J. Asbery

Computer Science Department, North Carolina State University, Box 8206, Raleigh, NC 27695, USA

Abstract

A network device is considered *compromised* when one of its security mechanisms is defeated by an attacker. For many networks, an attacker can compromise many devices before being discovered. However, investigating devices for compromise is costly and time-consuming, making it difficult to investigate all, or even most, of a network's devices. Further, investigation can yield false-negative results. This paper describes an intrusion–detection (ID) technique for incident-response. During an attack, the attacker reveals information about himself and about network vulnerabilities. This information can be used to identify the network's likely compromised devices (LCDs). Knowledge of LCDs is useful when limited resources allow only some of the network's devices to be investigated. During an on-going attack, knowledge of LCDs is also useful for tactical planning. The ID technique is based on the US military's battlefield-intelligence process. Models are constructed of the network, as the battlespace. Also, models are constructed of the attacker's capabilities, intentions, and courses-of-action. The Economics of Crime, a theory which explains criminal behavior, is used to model the attacker's courses-of-action. The models of the network and the attacker are used to identify the devices most likely to be compromised.

Keywords: Computer security; Intrusion detection; Incident response; Military intelligence; Economics of crime

1. Introduction

When a network is under attack, its intrusion-detection system (IDS) faces unique difficulties and opportunities. This paper explores those difficulties and opportunities, and it presents a new intrusion-detection (ID) technique based upon them. The technique is an adaptation of the US military's battlefield-intelligence process, named *Intelligence Preparation of the Battlespace* (IPB) [10]. We have descriptively named the ID technique *Cyber-IPB* (C-IPB).

1.1. The problem

A system-administrator discovers that a hacker has broken into a network device. Unfortunately, for many networks, this discovery is just the tip of the proverbial iceberg. ID tends to be a weak element of network security, giving a hacker opportunity to compromise many devices before finally being detected. Also, network devices often have security *trust-relationships* with other network devices. After compromising one device, the hacker can use trust-relationships to easily compromise additional devices. By the time a successful attack is discovered, many other devices may well be compromised.

* Corresponding author.
E-mail address: jimyuill@pobox.com (J. Yuill).

1389-1286/00/$ - see front matter
PII: S1389-1286(00)00142-0

After discovering one compromised network-device, the system-administrator would like to identify all compromised devices. However, investigating the network for compromise can be a difficult and time-consuming task: (1) devices can be checked manually for telltale signs of compromise, such as strange accounts in /etc/passwd, or suspicious log-file entries, (2) IDSs that run periodically, e.g., Tripwire® [19], can be run immediately, and (3) IDSs can be configured to be more sensitive or to look for specific indications of compromise [1,9]. For networks with more than a few dozen computers, the system-administrators will typically not have time to investigate all, or even most, devices for compromise. In addition, investigating devices for compromise is an uncertain task. The absence of evidence of compromise does not guarantee there is no compromise – investigation is subject to false-negative results.

When network-devices have security trust-relationships, the system-administrator needs to identify and repair *all* compromised devices. If a single compromised device is left on the network, the hacker may be able to continue compromising devices. Also, during an on-going attack, compromised devices must be identified quickly, to minimize attack damage.

The difficulty of identifying compromised devices is exacerbated by the complexity of the network's topology, administration, and use. For the system administrator, the identification of compromised devices can be overwhelming, as the process is resource intensive, urgent, uncertain, and highly complex. In addition, an active threat makes the environment dynamic.

1.2. Current incident-response techniques

In the larger perspective, incident-response (IR) is the overall process for handling the problems of computer misuse, after misuse is discovered. During IR, three measures used to secure a compromised network are: (1) *attack repair*: repairing devices altered by the attacker, (2) *attack neutralization*: fixing vulnerabilities which the attacker has exploited, or which he could exploit, and (3) *attack containment*: temporary measures for limiting an active attack, e.g., blocking all ftp sessions at the firewall. We will refer to *attack repair*, *neutralization*, *and containment* as *ARNC*. [1]

To repair a compromised device, the system-administrator performs, roughly, these tasks: (1) the attacker's active processes are removed, (2) damage from the attack is assessed and repaired, (3) the exploited vulnerability is determined, (4) an appropriate countermeasure for the vulnerability is chosen, based on risk analysis, and (5) the vulnerability is removed by repairing or improving the system. [2]

The identification of compromised devices is an essential part of ARNC, and ARNC is an essential part of IR.

1.3. An overview of the solution

A new ID technique is presented. Its purpose is to assist the system-administrator with the previously described intrusion-detection problems, encountered during incident-response. The objective of the technique is to identify the network devices that are likely to be compromised by the attacker. The devices' degree of likely compromise is also identified. By identifying the devices that are most likely to be compromised, the system-administrator can make effective use of the limited resources for investigating devices for compromise.

As previously mentioned, the ID technique is named C-IPB, and it is an adaptation of a military battlefield-intelligence process. C-IPB provides a systematic method for identifying *likely compromised devices* (LCDs), based on models of the network and the attacker.

A network is attacked by a particular set of individuals. During the attack, each individual reveals information about himself. [3] This information can be used to create models of the attacker' *capabilities* and *intentions*.

[1] *ARNC* is this paper's summary of the measures taken to secure a compromised network. Similar summaries can be found elsewhere, e.g., [20] summarizes the measures as analyze, contain, eliminate, and return [to normal operations].

[2] The repair process is not always this difficult – at times it is possible to just reinstall system software.

[3] This paper's masculine pronouns are used in a gender-neutral manner.