Smoke 'Em Out

Presentation Handout and Quick Reference Sheet created by Rohyt Belani (rohyt.belani@intrepidusgroup.com) and Keith Jones (keith.jones@jrdcorp.com)

Presented at Black Hat Briefings Las Vegas 2007 on August 2, 2007
Slides available at www.blackhat.com.

Fighting the Insider Threat

Tracing a malicious insider is hard; proving their guilt even harder. In this talk, we discuss the challenges faced by digital investigators in solving electronic crime committed by knowledgeable insiders. These challenges are presented in light of three real world investigations conducted by the presenters. The focus of this talk will on the technicalities of the attacks, the motivation of the attackers, and the response techniques used by the investigators to solve the respective crimes.

Case 1: United States v/s Roger Duronio

The first case is the high-profile U.S. v Duronio trial, in which Keith Jones testified as the DoJ's computer forensics expert. Mr. Jones testified for over five days about how Mr. Duronio, a disgruntled employee, planted a logic bomb within UBS's network to render critical trading servers unusable. His testimony was key in the prosecution of the accused on charges of securities fraud and electronic crime.

UBS-Painewebber (UBS-PW) is a financial institution that provides stock trading to their customers. Like most companies, UBS-PW process the stock transactions from all over the United States using a large computer network consisting of over 2,000 important servers. According to public record, UBS-PW experienced a reduction in profits like most companies after the September 11, 2001 attacks. The result of this reduction effected the bonuses provided to employees. Most employees would not be taking home the bonuses they were initially promised in the preceding year.

As a result, on Monday March 4, 2002, a former UBS-PW systems administrator named Roger Duronio executed a logic bomb which disabled a large number of the important servers responsible for executing the stock trades when the stock market opened at 9:30 AM EST. A logic bomb is a malicious program that destroys computer data at a preset time. UBS-PW reported a loss of over 3 million dollars in the recovery effort. In addition, the recovery effort was not immediately and completely effective. It was reported that effects of the logic bomb attack were felt long after the attack was cleaned up.

Simultaneous to the attack, Mr. Duronio purchased PUT options on UBS-PW's shares, which effectively bet against the company and would make money for Mr. Duronio when the stock lost value due to the logic bomb attack. It was up to the computer forensic experts to piece together Roger Duronio's actions and present it to a jury that may not understand all of the technical details of what happened.

Case 2: The Invisible Insider

The second incident involved a potential insider at a large retail organization. The attacker made his way from a store wireless network into the company's core credit card processing systems. We will discuss the anatomy of the "hack", the vulnerabilities exploited along the way, and our sleepless nights in Miami honing in on the attacker.

This attacker was able to exploit an antiquated wireless network at a store and establish a launch pad for his attack. Vulnerabilities in a BDC at the store network allowed the attacker to gain valid domain administrative credentials. Armed with these credentials, the attacker was then able to make headway into the corporate network and eventually into the credit card processing network through extremely permeable firewalls. The attack would have almost certainly gone undetected had it not been for an IP address conflict caused by the OpenVPN software that was used by the attacker to shovel key files out to a server on the Internet. Verbose firewall logging that had been enabled by network engineering for a different project was of tremendous help to the investigators. Even though we were not able to confirm who the attacker was, the suspect was an insider based on the lack of a reconnaissance footprint, demonstration of deep knowledge of the credit processing systems and the timing of the attack. We physically identified the suspect, but were not able to pursue prosecution due to the investigation being called off – what an anti-climax!

Case 3: Who let the cat out of the bag?

The final case presented focuses on the technicalities of web browser forensics and how it facilitated the uncovering of critical electronic evidence that incriminated a wrong-doer, and more importantly freed an innocent systems administrator at a law firm from being terminated and facing legal music.

A law firm found that their documentation management system was being used as a warez server. More so, the unauthorized uploads were being performed under the context of the administrative account. Care was taken to perform all investigative activities off business hours; the administrator being the primary suspect makes for slippery grounds. One of the primary areas of investigation was reviewing web browser activity. We will discuss the challenges we encountered and the techniques used to surmount them. Analysis of the browsing activity revealed the exact nature of the attack. It was a combination of an insider spilling the beans and writing some crafty code to bypass the affected software’s licensing mechanisms. It was also evident that the guilty party was the stand-in administrator and not the primary administrator who was on vacation.

The common thread in all these cases—a malicious insider. We learnt some key lessons that may assist in detecting malicious insiders. Being a geek, I always snubbed auditors that threw big terms at you like “Separation of Duties”. But in the case of these attacks, logging mechanisms outside the control of the malicious insiders were key in solving the cases. So, if you want to catch those bad guys on the inside, log as much activity as you can – including administrative actions and store the logs in a centralized read-only location. Establishing appropriate procedures for background checks, mandatory vacations, and employee termination may serve as effective preventative measures. Unfortunately, in the case of insider attacks the odds are against you because the attacker already has the keys to the kingdom!