Intrusion Detection and Incident Response
Cuckoo's Egg Analysis

William Adams

2/7/2024

Cliff Stoll implemented a diverse set of techniques for detecting intrusions and responding to incidents in "The Cuckoo's Egg," where he aimed to uncover the hacker responsible for infiltrating the computer network at the Lawrence Berkeley National Laboratory and accessing various US army bases nationwide. This essay will outline these strategies, emphasizing the importance of a comprehensive approach to security and highlighting the value of proactive and thorough incident response and intrusion detection.

A primary and consistently employed technique by Stoll involved logging analysis. He vigilantly monitored system logs, utilizing them to identify unusual activities and trace the hacker's actions throughout the system. To maintain a documented analysis of the hackers' activities during his absence from the computer, Stoll utilized a printer to produce hard copies of the logs (Stoll, 1990, p. 71). Additionally, he examined the records of the accounting system to determine how the hacker gained network access and the specific actions they undertook. Stoll's scrutiny of the logs enabled him to track the hacker's movements and pinpoint the infiltrated systems.

Stoll's effectiveness in log analysis depended on his profound understanding of the systems, applications, and regular patterns of user behavior. He sought anomalies in the logs, such as logins from unfamiliar locations or at unusual hours, ultimately discovering that the hacker accessed the system through private computers using public access dial-in modems and ports. A key revelation from Stoll's log analysis was that the hacker exploited a compromised account instead of directly breaking in. Employing brute force techniques, the hacker gained administrative privilege by guessing usernames and passwords. To mitigate this vulnerability, Stoll suggested measures like disabling a user after three incorrect login attempts or enforcing regular password changes for all users.

The hacker's utilization of dictionary attacks was another significant finding from Stoll's investigation. These attacks involve trying numerous possible passwords to guess the correct one. The hacker automated this process using an English dictionary and a password cracking program (Stoll, 1990, p. 124). This program generated potential passwords by combining dictionary words with various combinations of numbers, symbols, and capitalization. Remarkably, the hacker even cracked encrypted passwords using a Unix password encryption program. These findings underscore the ongoing vulnerability to password-related attacks and emphasize the importance of robust security measures in the face of evolving intrusion techniques.

Subsequently, the program systematically tests each of these passwords until the correct one is identified. Prior to executing a dictionary attack, the hacker compiles a roster of usernames from the target system. Armed with a list of potential passwords derived from commonly used words, phrases, and patterns, they employ a cracking tool to test each combination. The primary objective of the dictionary attack is to discover a valid username and password pairing that grants unrestricted access to the targeted system. Once inside, the hacker employs various methods to elevate their access rights and gain entry to additional system components.

The prevalence of disabled security features and easily guessable passwords on many computers makes dictionary attacks the preferred method for unauthorized network access (Stoll, 1990, p.128). Systems with lax management are particularly susceptible to such brute-force attacks. Mitigating these risks involves implementing security controls, such as enforcing robust password policies, limiting login attempts, and incorporating two-factor authentication. Additionally, intrusion detection systems can alert administrators to potential breaches, while network monitoring tools aid in identifying and thwarting suspicious login attempts. Stoll directed his investigation towards user accounts, tracking the hacker from the directory and back doors created for themselves. Eventually, he located and disabled the compromised account. The hacker's establishment of multiple backdoor entrances into infiltrated networks, coupled with password modifications known only to them, underscored the complexity of the intrusion.

Exploiting a flaw in the Gnu-Emacs text editor, the hacker gained superuser access to the university's computer system through a buffer overflow vulnerability, also known as the "Gnu-Emacs hole." Utilizing a Trojan horse program disguised as a benign file, the hacker executed code with superuser rights when accessed in Gnu-Emacs. This allowed complete control of the system, enabling malicious actions like installing backdoors and manipulating system logs to conceal their activities.

The incident highlights the critical need for prompt vulnerability patches and software updates. Despite the Gnu-Emacs developers having addressed and patched the vulnerability, the institution at Berkeley had not applied the update. Stoll's meticulous analysis of system logs identified the hacker's actions, including the insertion of backdoors, enabling their removal. To prevent similar vulnerabilities, Stoll implemented additional security measures, such as routine system updates and patches. Cliff Stoll encountered a minor discrepancy in the accounting records related to printer paper—specifically, an exact amount of seventy-five cents. Upon investigation, he discovered that a hacker had exploited a system-connected printer to produce multiple pages of documents. This oversight went unnoticed as the printer was not integrated

with the accounting software. Through meticulous log analysis, Stoll identified the specific printer used, along with the precise time and date of the print job. This information played a pivotal role in pinpointing the hacker and gathering evidence against them (Stoll, 1990, p.10).

In essence, Stoll's emphasis on log analysis underscores its crucial role as a fundamental tool for incident response and intrusion detection. It highlights the importance of having a comprehensive understanding of monitored systems and the ability to discern and comprehend unusual behavioral patterns. The documentation of hacker activities and commands through logs proves invaluable in tracking behavioral patterns and serves as a beneficial resource for future reference when confronted with similar behavior or commands within an organization.

In another instance, Stoll observed an unusually high volume of traffic originating from a specific machine on the network (Stoll, 1990, p. 22). Investigation revealed that this traffic emanated from a remote login session initiated by the hacker, as discerned from the system logs. Leveraging this insight into the hacker's orders, Stoll effectively denied the hacker access and prevented further damage to the system. The second method employed by Cliff Stoll in "The Cuckoo's Egg" to track the hacker was traffic analysis. Utilizing traffic analysis as a strategic tool, Stoll sought to identify the intrusion and understand the techniques employed by the hacker to gain system access. Examining network traffic to detect trends indicative of a hacker's presence, Stoll employed programs like tcpdump to capture and analyze real-time network packets.

Tcpdump, a network packet capture tool, enabled Stoll to record and scrutinize network traffic. By capturing data packets and filtering them based on criteria such as source and destination IP addresses, packet types, and port numbers, Stoll gleaned valuable insights into the hackers' network activities. He used tcpdump to examine various formats of data packets, including those from file transfers, remote login sessions, and other network activities by the hackers. This meticulous approach allowed Stoll to identify unusual behavioral patterns and apply this knowledge to uncover security threats and identify the root causes of problems.

The hacker employed a program called "Kermit" to transfer files and execute commands on remote computer systems (Stoll, 1990, p.54). Kermit is a file transfer protocol that enables users to transmit data between computer systems using various connection methods. Exploiting Kermit, the hacker ran commands on the compromised system and transferred files to their own machine. The hacker aimed to export the source code of two programs, telnet and rlogin, both allowing remote access to foreign computers and the transfer of commands. To counter this, Stoll employed a unique strategy—jangling his keys over the wires connected to the hacker's line, creating the appearance of network interference, and thwarting further

intrusion (Stoll, 1990, p.190). This example showcased Stoll's reliance on physical security and creative thinking to impede the hacker's progress.

Through traffic analysis, Stoll uncovered a major revelation—the hacker concealed their real identity and location through an IP spoofing technique. IP spoofing involved the use of fictitious source IP addresses in packets sent to Stoll's network, making it challenging to identify the true source of traffic. The hackers employed specialist software tools to modify IP addresses in packets, along with "source routing," which designated a specific path for packets through the network, obscuring their actual location.

Despite the hurdles posed by the hackers using IP addresses from other entities and constantly changing addresses, Stoll managed to identify patterns of network activity indicative of the hackers' actions. Overcoming these challenges, Stoll utilized the tracerouting method to trace the route of packets through the network. By sending packets with increasing Time-to-Live (TTL) values and analyzing responses from each hop, Stoll used the Traceroute tool to identify the route from source to destination, revealing IP addresses of routers or nodes along the way. Furthermore, traffic analysis allowed Stoll to pinpoint infected systems and understand the hacker's techniques for gaining access. For example, he discovered that the hacker remotely connected to the system using the X.25 protocol, a common practice for wide-area networking in the 1980s. This information enabled Stoll to trace the hacker's phone number, showcasing the effectiveness of traffic analysis in uncovering infiltration methods and tracking malicious activities.

To identify potential security vulnerabilities, Stoll's examination of X.25 traffic involved monitoring packet movement through the network and scrutinizing their contents. This study unveiled various vulnerabilities, including attempts at unauthorized access, data exfiltration, and efforts to conceal the hackers' activities. Stoll incorporated an X.25 connection into his honeypot network, named "SDI Network" (Stoll, 1990, p. 268). Utilizing tools like tcpdump and packet sniffers, along with manual analytical techniques, he captured and analyzed packets to decode their contents. Packet sniffers, programs that log network data, enabled network administrators to inspect packet contents for security issues. Stoll strategically deployed packet sniffers at multiple locations, such as border routers and hosts, to record network traffic.

Subsequently, Stoll conducted a comprehensive analysis of the captured packets, identifying patterns of behavior and potential security risks like unauthorized access attempts and data exfiltration. The detailed insights into network traffic, including individual packet contents and source/destination addresses, demonstrated the value of packet sniffers in network monitoring and analysis.

Stoll's traffic analysis, complemented by traceroute, tcpdump, and packet sniffers, showcased the critical role of network monitoring in intrusion detection and incident response. It underscored the importance of understanding network protocols and recognizing trends in network traffic to trace hackers and their activities back to their source, even when they attempted to conceal their location and cover their tracks.

Stoll's third strategy involved the use of honeypots—a decoy system designed to attract and capture hackers, providing insights into their methods. Stoll created a honeypot system, the "SDI network," featuring fabricated sensitive documents and credentials to entice hackers. This system simulated insecurity, with lax security measures and easily guessable passwords. Stoll ensured that the network appeared legitimate by setting all fabricated files to be readable only by the owner.

Stoll constructed a fictitious military network, including the honeypot, and employed various tactics to enhance its authenticity, such as fabricating false log files and login screens (Stoll, 1990, p. 266). The hacker was lured in by the honeypot, spending considerable time attempting to breach the system. Stoll observed the hacker's actions and gained insights into their strategies, such as using the "who" command to list networks on the system and searching for the user "SDINET" in the password file. Although the hacker attempted to access the SDINET directory, they were unable to view the files due to ownership restrictions.

The hacker proceeded to implant a deceptive "atrun" program in conjunction with Gnu-Emacs software to attain superuser status and corresponding privileges. After gaining superuser access, the hacker listed files and began scrutinizing fictitious files labeled as "sensitive information" (Stoll, 2000, p.265, p.266). Atrun operates in privilege mode, granted full trust by the operating system, and the hacker exploited the Gnu-Emacs vulnerability, substituting it with the malicious atrun program to obtain complete privileges and system access. This deceptive atrun program was employed on multiple occasions, granting access to the Berkeley Institute and the fabricated honeypot network devised by Stoll. "Atrun" is a program designed for scheduling tasks to run at specific times, and the hackers capitalized on a flaw within it to execute commands with root privileges. They achieved this by crafting a shell script containing the setuid command, enabling the Emacs editor to run as root. Once the Emacs editor ran with root privileges, the hackers had unrestricted access to the system and could execute any desired commands. To conceal their actions, the hackers utilized various techniques such as removing log files and traces with the "rm" command and presenting file information using the "ls" list command with multiple settings, making their activities challenging for system administrators to discern.

The honeypot, purposefully designed to document the attackers' actions, including login information, instructions employed to access sensitive data, and tracking the hacker's address via telephone lines, played a crucial role. Stoll utilized the honeypot to gather essential information about the hacker's methods, tactics, and actions, ultimately preventing subsequent network intrusions. In addition to diverting hackers' attention and denying them access to critical data, the honeypot aided in defending real systems on the network. Stoll analyzed system logs as part of his investigation, using programs like grep and awk to identify suspicious activities, such as the unusual usage of atrun to schedule jobs.

A significant revelation from the honeypot was Stoll's discovery of the hacker's utilization of a "salami attack" method, subtly modifying the system to avoid detection by stealing minimal processing power or memory (Stoll, 1990, p. 185). Stoll's use of honeypots underscores the importance of proactive security measures and the need to anticipate potential attackers' strategies. It emphasizes the value of deception and misdirection in network security, illustrating the significance of studying hacker behavior to enhance security protocols and thwart future assaults.

Social engineering served as the fourth method employed by Cliff Stoll in "The Cuckoo's Egg." He utilized this tactic to glean insights into the hacker and their operations by manipulating people's minds to extract private information or influence their actions. Social engineering involved tactics such as setting up a counterfeit dial-up server likely to be used by the hacker. Stoll created a fake login page for the genuine system, recording the hacker's login information and enabling him to track their movements and gather information about their operations using the pilfered credentials (Stoll, 1990, p. 258). In a separate incident, Stoll employed a clever strategy to extract details about the hacker's behaviors by fabricating a "rogue" account. He simulated system access by creating a user account, engaging with the hacker, and establishing trust. Over time, the hacker unknowingly shared information with the deceptive account, providing Stoll with valuable insights into their operations and capabilities (Stoll, 1990, p. 268).

Additionally, Stoll utilized social engineering techniques to uncover the hacker's phone number. He posed as a customer service agent when contacting the phone provider, persuading them to divulge the hacker's phone number (Stoll, 1990, p. 138). A significant revelation from this effort was the discovery that the hacker operated from another country, allowing Stoll to focus his investigation on cross-border connections, ultimately leading to the hacker's identification and capture.

Through social engineering, Stoll underscores the importance of the human factor in cybersecurity and the need to be vigilant against potential social engineering attacks. It highlights the critical role of gathering information from diverse sources to develop a comprehensive understanding of the attack and the individuals involved. Stoll's use of social engineering revealed the hacker's location in Hannover, Germany, and hinted at the possibility of a second hacker. Trojan horses played a crucial role for the hacker in acquiring passwords. The trojan horse was designed to copy passwords into a specific location known only to the hacker (Stoll, 1990, p. 152). The hacker also violated the principle of "least privilege," as an unauthorized user operating beyond the intended scope of access in the systems and networks.

Furthermore, the hacker targeted the university's computer system using a logic bomb—an executable code set to perform a malicious action at a specific time or event. In this case, the logic bomb was programmed to delete a vital system file if a particular user account was removed. The hacker introduced the logic bomb into the university's network after gaining access to a privileged account. Stoll, vigilant over the university's computer system, detected the logic bomb by observing irregular visits to a specific file. He disarmed the logic bomb before it could cause harm and implemented additional security measures in response. This included deploying monitoring tools and restricting access to privileged accounts to identify and prevent similar attacks in the future.

A significant portion of the blame for the hacker's success can be attributed to the lack of technical awareness among security professionals and authorized users. Some software and computers were sold with a built-in backdoor password; for instance, upon installing Ingres, a pre-configured account with an easily guessable password is included (Stoll, 1990, p. 276). Security professionals must stay informed and vigilant about such vulnerabilities, taking proactive measures like changing passwords to more robust ones and mandating regular password changes, such as every thirty days.

In summary, "The Cuckoo’s Egg" is a compelling true story that underscores the significance of security awareness and network security. The narrative serves as an illustration of how organizations must implement robust security measures to safeguard sensitive data and vital systems effectively. The book sheds light on the increasing sophistication of hackers who exploit vulnerabilities using techniques such as packet sniffing, IP spoofing, trojan horses, and social engineering. Additionally, it emphasizes the value of adopting a multifaceted security approach, incorporating methods like incident response, physical surveillance, log analysis, and traffic analysis. Stoll's success in identifying the hackers is attributed to his strategic use of techniques such as log analysis, traffic analysis, tracerouting, and honeypots, among others. The book showcases the effectiveness of forensic analysis in detecting security flaws and

apprehending hackers. Furthermore, it underscores the importance of information exchange between businesses and law enforcement to enhance cybersecurity.

Work Cited

Stoll, C. (2024). *Cuckoo's egg: Tracking a spy through the maze of Computer Espionage*. GALLERY BOOKS.

Kermit - What is it? (n.d.). https://www.kermitproject.org/kermit.html