Decoy Systems: A New Player in Network Security and Computer Incident Response

Kellep A. Charles, CISSP

Abstract

Interconnectivity on the Internet is growing, as more and more organizations, private companies and governmental institutions connect for critical information processing. This interconnectivity allows for better productivity, faster communication capabilities and immeasurable personal conveniences. It also opens the door to many unforeseeable risks, such as individuals gaining unauthorized access to critical enterprise information infrastructure. These organizations are discovering that traditional means of preventing and detecting network infringements with firewalls, router access control-list (ACLs), anti-viruses and intrusion detection systems (IDS) are not enough. Hackers are able to obtain easy to use tools to scan various networks on the Internet for system vulnerabilities, then use the information gathered from the scans to launch their attacks with script kiddies. A solution that has been catching on in the network security and computer incident response environment is to employ "Decoy Systems." Decoy Systems, also known as deception systems, honey-pots or tar-pits, are phony components setup to entice unauthorized users by presenting numerous system vulnerabilities, while attempting to restrict unauthorized access to network information systems.

Introduction

The concept of Decoy Systems is not new to the network security world, as Cliff Stoll first described it in his book entitled "The Cuckoo's Egg."[1] Stoll depicted a jail-type technology that captured an unauthorized user's access to a system to determine his intentions. It is just recently that the concept has been adopted by the masses for production implementation to assist in a defensive network security posture. A compromised decoy system offers a wealth of features that can assist with intelligence data gathering, incident response and network forensics, for a better understanding of who the attacker is, what method the attacker used to gain access and the results of the attacker's unauthorized attack for possible prosecution measures. These features include suspicious event alerts to a management workstation for visual and audible notification, the ability to capture the unauthorized user's keystrokes and send it to a remote syslog server, various customized logging and bogus system files and information to have the unauthorized user waste time as the security administrator prepares a countermeasure.

[1] C. Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of a Computer Espionage (New York: Pocket Books, 1990).

The Value of Decoy Systems

Incorporating decoy systems into an existing security structure adds a wealth of value, as they provide an additional level of security within the network infrastructure. Data from a properly implemented decoy system is usually more valuable than data from an intrusion detection system, due to the reduction of both false positive and false negative alerts. Decoy systems are considered "set and forget" IDS sensors, because they are composed of a single system or network of devices whose sole purpose is to capture unauthorized activity. This means any packet entering or leaving a decoy system is suspicious by nature and simplifies the data capture and analysis process, as well as providing valuable information on the motives of an attacker. Most production networks and servers do not have the latest Microsoft Windows security patches, or are set up with configuration errors that are well known to hackers. As a result, they are able to download free tools that will scan many different networks looking for those easy-open entry points. Employing decoy systems takes advantage of these traditional issues and uses it for its enticing benefit. They are constructed to sting hackers, not just keep them out.

Using Decoy Systems

Several products are available to assist in creating a decoy system, each of which has its own interpretation of what a decoy system is and how it should be used. The overall process of installing decoy systems on a network infrastructure is relatively simple. The main components are commonly an extra interface on the firewall to control data communications and the deception system. In choosing a form of decoy system, an organization's defense posture and financial situation must be taken into consideration. For example, Symantec's ManTrap and ManHunt software (formerly Recourse Technologies) is a commercially available product that depicts a form of decoy system. ManTrap accomplishes this task by running an image of an operating system within another operating system, while Manhunt attempts to locate the unauthorized user. ManTrap collects evidence necessary for prosecution and makes hackers believe they are attacking vital information systems. This approach assists in maintaining network performance by protecting the network and collecting logs without hindering legitimate traffic. ManTrap will log all keystrokes, processes, and files accessed during each attack. The ManTrap decoy system also uses a hardware token to digitally sign and time stamp log files to guarantee non-repudiation in the event they are needed for prosecution or legal actions. ManHunt and ManTrap products offer extensive customer support and carry an expensive price tag.

Fred Cohen's Deception Tool-Kit (DTK) is a programmable toolkit of scripts designed to make it appear that a system contains a large number of well-known system vulnerabilities. DTK exposes the results of these vulnerabilities by the inputs of the unauthorized users' scans or attacks. DTK listens for inputs and provides responses that seem normal, while logging the unauthorized users' action for analysis. This is not a very complex system, and experienced hackers will quickly realize that they are on a decoy system. Furthermore, no provisions are available in the application to assist in

non-reputable evidence collection for prosecution concerns. Fred Cohen has provided DTK free, via the Internet for download at http://all.net/dtk/.

Any customized information system with default settings can also be installed onto a network to depict a decoy system. Lance Spitzner took that approach in “The Honeynet Project,” when he decided to use default installations of Red Hat Linux, Windows 98 desktop, Windows NT server and Solaris server, with default parameters and minimal customization. Unfortunately, these very same default installations are a high percentage of systems connected to the Internet (Spitzner, 2002). The benefit to this approach is that a mirror of the organization’s production systems can be reproduced to mimic a decoy system. This method can assist in the evaluation process to validate the internal information systems from an attack. A customized decoy system is relatively inexpensive, especially when used with a Linux operating system. To analyze and collect data suitable for prosecution intentions from this form of decoy system, the examiner would use traditional forensics tools and procedures such as the UNIX “dd” and the “ncat” commands, as well as some well-known commercial applications like Guidance’s EnCase and New Technologies’ SafeBack 3.0 software. An excellent example of additional tools can be viewed at the Honeynet Project Forensic Challenge website (http://www.honeynet.org/challenge/).

The use of deception will aid in drawing the unauthorized user’s attention from the trusted network to the decoy network. There is an assortment of common schemes for deploying decoy systems. The first way is to create a separate network, preferably on a demilitarized zone (DMZ), and the other is based on "The Minefield" principle where the decoy systems are intermingled with the production systems.

Decoy systems placed on a DMZ to lure attackers away from the internal trusted network assets provide many benefits, as illustrated in Figure 1. An access control rule-set on the firewall can be less stringent on the DMZ network where the decoy systems reside. When the unauthorized user performs scans to locate system vulnerabilities, the decoy systems on the network would reply and move all focus away from the trusted network resources.

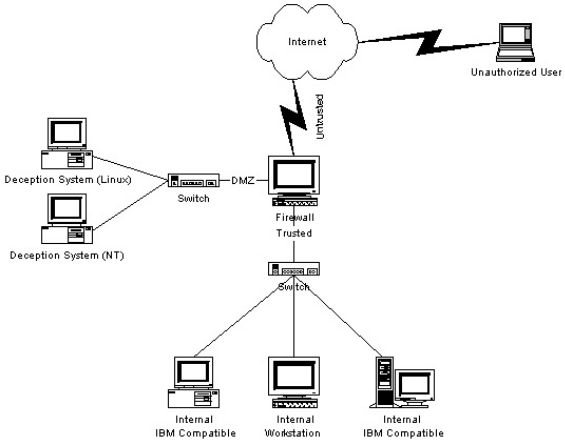

Figure 1 – Decoy Systems on a Separate Network

Once an unauthorized user compromises the systems on the DMZ, special data control mechanisms are put in place to prevent further harm to other information systems. The access control rule-set on the firewall allows data to enter the DMZ, but restricts certain data to depart from the DMZ. This prevents the unauthorized user from launching further attacks to other information systems. Figure 2 depicts an example of data control flow on a network infrastructure, using a DMZ concept to deploy decoy systems.

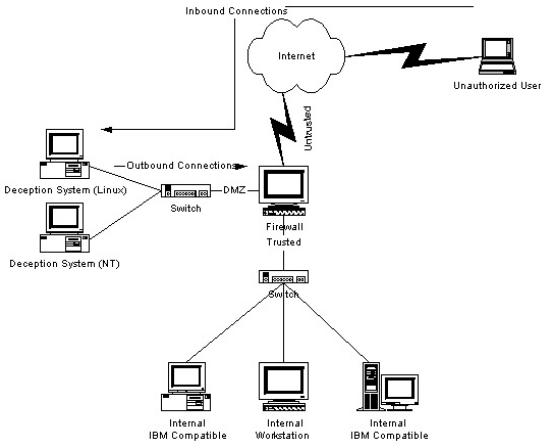

Figure 2 – Data Control of Decoy Systems on a Separate Network

The minefield principle of deploying decoy systems involves placing decoy systems with other production information systems on a trusted network and trusted DMZ network. This is depicted in Figure 3. Often the decoy systems will have an appealing server

with names such as "Primary Mail Server" and “HR File Server” and a lower IP address for quicker vulnerability scan detection.

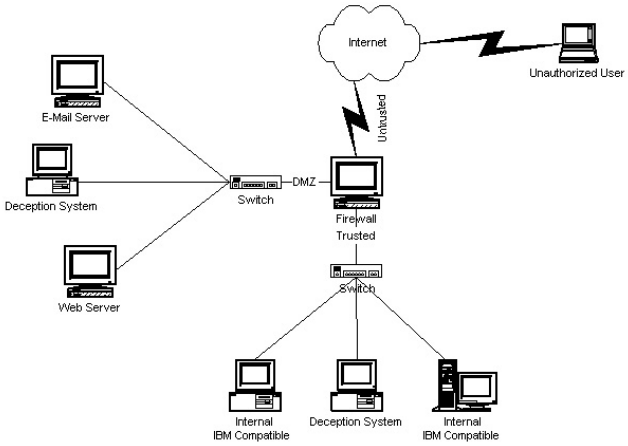

Figure 3 – Minefield Approach to Decoy Systems

Legal Issues with Decoy Systems

A common misconception surrounding decoy systems is that they are a form of entrapment because they lure attackers in. The issue then is that the evidence collected may not be used to prosecute the attacker. The reality is that decoy systems are not active lures and they do not advertise themselves. The only way that a hacker can find a decoy host is by running specific reconnaissance tools that are known to be used to compromise systems on a network. The definition of entrapment may vary with jurisdiction, but a typical definition reads:

> A person is 'entrapped' when he is induced or persuaded by law enforcement officers or their agents to commit a crime that he had no previous intent to commit.[2]

However, there is no entrapment when a person is ready and willing to break the law, and law enforcement officials merely provide what appears to be a favorable opportunity for the person to commit the crime. Furthermore, entrapment only pertains to law enforcement and government agents. Private decoy system owners will not be prosecuted with entrapment because they act independently of the government.

In many jurisdictions, it is prudent to place a special notice to all users accessing the enterprise information system. This notice must state: (1) the system is to be used only by authorized users, and (2) by continuing to use the system, the user represents that he/she is an authorized user. In previous prosecutions against an attacker who entered a system unlawfully, one of the most successful defense positions was that there was no notice saying they could not enter. Recent court cases have highlighted the need for organizations to put unauthorized users on notice that their systems are off-limits. The March 2, 1990 Defense Data Network Security Bulletin advises, "A court recently threw out a suit against a computer system intruder because the logon prompt was preceded with "Welcome to..." The advisory implored administrators to cease using "Welcome" in logon banners.[3] As a result, a system login banner displayed each time a user logs-in should provide the electronic equivalent of a no-trespassing sign. This should also be on the deployed decoy systems and the banners should be identical to those of the production systems on the network [6].

Displaying logon banners also prevents the unauthorized user from stating during prosecution proceedings that the system accessed was a decoy, and therefore, employed access-control restrictions to ensure no substantial harm occurred to the organization's information resources. Having a properly written logon banner will negate the unauthorized user's attempts to produce a loophole on the charges being brought against them.

[2] http://www.lectlaw.com/def/e024.htm
[3] http://csrc.ncsl.nist.gov/secalert/ddn/1990/sec-9004.txt

An example of a DoD banner is listed below in Example 1 – DoD Security Banner. Private companies, as well as educational institutes, also have versions tailored to their environments.

DoD Security Banner[4]

This is a DoD interest computer system. All DoD interest computer systems and related equipment are intended for the communication, transmission, processing, and storage of official U.S. Government or other authorized information only. All DoD interest computer systems are subject to monitoring at all times to ensure proper functioning of equipment and systems including security devices and systems, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for other similar purposes. Any user of a DoD interest computer system should be aware that any information placed in the system is subject to monitoring and is not subject to any expectation of privacy.

If monitoring of this or any other DoD interest computer system reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of this or any other DoD interest computer systems reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of DoD interest computer systems are subject to appropriate disciplinary action.

Use of this or any other DoD interest computer system constitutes a consent to monitoring at all times.

UNCLASSIFIED, NON-SENSITIVE, NON-PRIVACY ACT USE ONLY

Example 1 – DoD Security Banner

Privacy and liability are two other legal issues that need to be addressed when deploying decoy systems. Decoy systems can capture extensive amounts of information about the attacker, which can possibly violate his privacy. Of all the privacy statutes, the one that most likely applies to decoy systems deployed in the US is the Federal Wiretap Act. Under the Federal Wiretap Act, it is illegal to capture the communications of an individual in real time without his knowledge or permission, as this violates his privacy. There are two general categories of data collection by decoy systems: transactional and content. Transactional is not the data itself, but information about the data. For IP, that means IP addresses, IP header information, time and date of the communication, etc. Content data is the actual communication itself, such as IRC

[4] http://www.sec.army.mil/aiew/dod_banner.htm

chats, emails, and keystrokes. Content data has more privacy issues then transactional data [11].

Liability issues in decoy system deployment imply that an organization could potentially be held liable if their decoy system is used to attack or harm other systems or organizations. For example, if used to attack other systems or resources, the owners of the affected systems may sue. Liability is a civil issue, involving the argument that if proper precautions to keep the systems secure had been taken, the attacker would not have been able to harm other systems, Therefore, the organization responsible for the decoy system would share the fault for any damage that occurred to another organization during the attack [11].

Conclusion

The defensive strategy of decoy systems is to deter, learn, conceal, impede, confuse and misinform the unauthorized user, while collecting valuable information to help identify and prosecute the malicious attacker. They are legal as long as they are used in the proper fashion. Lance Spitzner of "The Honeynet Project" stated, "In references to legal cases, you won't find any, there is no precedence in reference to honeypots. That is one of the challenges of it, the technology is simply too new."

As the use of decoy systems becomes more prevalent, new products will be developed and marketed. This means more variations of decoy systems with additional system features, better logging, and lower costs. Further research on decoy systems, such as that currently being conducted in academia, as in Georgia Tech's College of Computing[5] "Honeypot Test Bed Project," government institutions and by private industry such as RSA Security Inc.[6] will lead the way for advanced forms of decoy system technologies. Such advancements may include intelligent systems, using a variety of artificial intelligence techniques, and the ability to apply survivable system methods. The future of decoy systems should follow the evolution of intrusion detection systems, where many sectors applied numerous resources to make it an acceptable tool in defending our networks.

References

[1] William W. Martin, CISSP; Honey Pots and Honey Nets - Security through Deception; SANS, May 25, 2001

[2] Green D.; From Honeypots to a Web of SIN - Building the World-Wide Information System; [AUUG95]

[3] Krol, E. (1992). *The Whole Internet Guide and Catalog*. O'Reilly and Associates.

[5] http://www.cc.gatech.edu/people/home/srikanth/PADS.html
[6] http://www.rsasecurity.com/worldwide/pr/dk/09042003_6042.html

[4] Spitzner, L.; Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community. Addison-Wesley; 2002

[5] Stallings, W.; Kruse, W. & Heiser, J.; Computer Forensics – Incident Response Essentials; Addison-Wesley; 2002

[6] Brian Scottberg; William Yurcik; David Doss, "Internet Honeypots: Protection or Entrapment?" Illinois State University, 2002

[7] M. E. Kabay, **"**Honeypots, Part 2", *Network World Security Newsletter, 05/15/03*

[8] Mandia, K. & Prosise, C.; Incident Response – Investigating Computer Crimes.; Mc Graw-Hill; 2001

[9] www.all.net: Fred Cohen & Associates' ForensiX

[10] Michael Mullins, "Which honeypot should I use?**",** June 12, 2001, http://techrepublic.com.com/5100-6264-1042527.html

[11] Spitzner, L.; Honeypots: Are They Illegal?" www.securityfocus.com/infocus/1703 June 12, 2003

About the Author

Kellep A. Charles is a Ph.D. student in Computer Information Systems at Nova Southeastern University (www.scis.nova.edu) concentrating in Information Security and Artificial Intelligence. He also holds a Master of Science in Telecommunication Management from the University of Maryland University College and a Bachelor of Science in Computer Science from North Carolina Agriculture and Technical State University. Kellep work as a contractor at The Pentagon as a Network Security Analyst and is an Adjunct Professor at Capitol College in Laurel Maryland where he teaches in the Computer Science department and holds a CISSP certification.

Kellep heads "The Computer Incident Response and Forensics Center" (www.cirfc.org), an organization that provides educational and research information security services to small and medium sized establishments.

Kellep can be contacted at: kellep@kellep.com or www.kellep.com.