GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

A Guide to the Honeypot Concept

Mark Pickett
GSEC Practical
Version 1.4b (Option 1)
June 9, 2003

Abstract

Most security technologies are designed to prevent unauthorized activity to resources; systems are put into place as a defensive measure. The honeypot concept takes a more proactive stance by doing the opposite and attracting intruders. It allows them to bring out their best bag of tricks, all the while taking note of their moves and how their tools work.

The purpose of this paper is to give a complete overview of the honeypot concept by not only defining what a honeypot is but also describing the different types, objectives, and implementations. It will discuss the implementation and strategies of honeypots as well as the advancements in the technology. Additionally, it will examine some of the legal issues that may surface by deploying a honeypot. This paper should be used to get a basic understanding of the honeypot concept, its terminology and to open the door for further research by the reader.

Defining Honeypots

A honeypot is a computer system that appears to be an interesting target to hackers, but actually gathers information about them. It is designed to be probed, attacked and compromised and, at the same time, monitors the actions taken to complete these tasks. Many different manifestations of the honeypot have developed from the basic concept. In most cases, honeypots only imitate production resources and do not contain any mission-critical data. Since these systems are not relied upon by the organization as a production resource, legitimate users will have no reason to access them. As a result, any network traffic entering or leaving the honeypot system should be viewed as suspicious; there may be an intruder lurking about.

These systems can be broken down into two broad categories: low-interaction and high-interaction. A low-interaction honeypot is usually a single system that limits what activities the intruder can accomplish. For example, a honeypot that emulates an FTP server listening on port 21 may only allow a login attempt. It will not allow any other FTP commands. Since services are emulated, intruder activity can be contained which reduces risk. Also, low-interaction honeypots are simpler to deploy and maintain. The process can follow this pattern: install the software, select the operating systems and services to be emulated and then monitor for activity. On the other hand, one of its disadvantages is that low-

© SANS Institute 2003, Author retains full rights.

interaction honeypots cannot capture new exploits; they look for pre-defined activity. In addition, because they use emulated services, a skilled intruder can eventually detect them. The traditional honeypot fits in this category and can be a simple, low-cost solution that is easy to deploy and maintain. Examples are *Honeyd* and *BackOfficer Friendly* (Spitzner, "Honeypots: Definitions" 2-3).

In contrast, a high-interaction honeypot is not a simulated system or service. It is an authentic system and/or application. If a Linux honeypot running the FTP service is desired, an actual Linux system with the FTP service will need to be built. Since the intruder can interact with a real system, this allows an extensive amount of information to be captured including new tools, new exploits and intruder behavior. On the other hand, a larger risk factor comes into play due to the environment being so open. Intruders can use these same systems as a jump-off point to attack other systems outside of the honeypot. Accordingly, a higher skill level is required to deploy and maintain the systems and also to implement technologies to prevent intruders from accessing non-honeypot systems (Spitzner, "Honeypots: Definitions" 2-3).

The Honeynet Project uses a honeynet, a type of high-interaction honeypot, for their research. It is a non-profit research organization of volunteers dedicated to information security. They have deployed and studied honeynets since 1999 and have published their research and findings to the security community.

The Value of Honeypots

Honeypots are put into place for either research or production purposes. Even though both low-interaction and high-interaction honeypots can be used for either purpose, low-interaction honeypots are commonly used for production reasons and high-interaction honeypots are used for research. A research honeypot is capable of capturing a wider assortment of data than a production honeypot can and is used primarily for this function. The information that has been gathered can be used for many purposes such as discovering new hacker tools and techniques. Also, trending hacker activity and determining their motives can be performed. This can lead to early warning and prediction of future attacks and exploits.

A production honeypot is used to prevent or stop attacks against an organization's production systems. The honeypot can accomplish this in several ways: attack prevention, detection and response. First, attack prevention is accomplished through deception and deterrence. Simply put, intruders are deceived by being forced to waste their time and resources interacting with honeypots, thinking they are real systems. Also, an organization may have the time to detect the activity and respond to the attackers. Furthermore, if the attackers determine that there are honeypots on the network, they may be deterred from continuing due to concerns of being caught by the honeypots.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Attack detection is of significant importance since security is never absolute and failures in prevention do happen. When this occurs, unauthorized activity may be detected and it is possible to slow down or stop an attack before it can go into full swing. For instance, if it is determined that the network is being scanned, the administrator can take measures to prevent an attack from originating from that source. Also, if an attack in underway, the compromised system can be isolated from the rest of the network to reduce the amount of damage to that system and the rest of the network.

In contrast is another technology called intrusion detection systems (IDS). IDS are a common technology used to discover unauthorized activity. These systems monitor a system or entire network and when suspicious activity is detected they generate an alarm. Unfortunately, IDS are known for generating a large amount of false positives (sending alarms for legitimate traffic). It is time consuming and resource intensive to analyze all of the alerts generated, which may cause actual alarms to be overlooked (a false negative). In comparison, since honeypots are not production systems and do not contain valuable information, they should not receive any network traffic. When they do receive traffic, it will almost always be malicious activity. This creates a much smaller set of data to review as opposed to large volume that an IDS generates.

In order to respond to an attack, detailed information is required. But, gathering information from a production system to determine who got in, how they got in and what has been done can be difficult. Add to this the fact that a production system may need to stay on-line even after an attack (such as a mail server) and the situation gets worse. Analysts will have to examine the system while it is being used. All the while users are accessing files and logging in and out. It becomes difficult to determine which activity was a legitimate user and which was the attacker. Thankfully, honeypots are not relied on as production resources so they can be taken off-line and analyzed at any time without concern about data pollution.

Honeypots Taken Further

The information that has been covered so far has pertained mostly to the traditional honeypot. That is, a single system that has been set up to be probed, attacked and compromised. The next area of discussion will center on honeynets.

As mentioned earlier, a honeynet is a high-interaction type of honeypot. It consists of an entire network of fully functioning systems and applications designed primarily for research. The honeynet network can contain different operating systems with different applications and this more accurately portrays a production network. The gateway into the honeynet is called a honeywall and is similar in placement as a firewall would be to a conventional network. Intruders that have compromised any of the systems in this environment can be monitored

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

and new threats, tools, or attack patterns can be discovered. This is due to the fact that the systems are real systems and attackers have the freedom to use all of their techniques.

However, since intruders have the flexibility of actual systems, there is a greater risk that they may harm non-honeynet systems. To mitigate this risk, an environment must be created to prevent the honeynet from being used as a resource for attacks. When a honeynet is built, there are three requirements that must be put into place: Data Control, Data Capture and Data Collection. When instituted, these requirements produce a highly controlled environment.

Data Control is the process of containing the activity of an intruder. While a system within the honeynet is compromised, traffic flow into and out of the honeynet must be controlled. But at the same time, intruders must remain unaware that they are being monitored. Intruders most commonly need access to the Internet in order to accomplish tasks such as downloading toolkits or sending email. In order to track and learn their activities, they must have the flexibility to execute these and other actions. Intruders should be afforded the room to accomplish this but, at the same time, not allowed to use the compromised systems to attack others. The more they are allowed to do, the more there is to learn and the greater the risk.

Data Capture is capturing the activities of the intruder. In order to learn intruder tactics and tools, the actions of the intruder must be captured. This may seem like a simple task but there are two challenges that must be overcome. First, all traffic entering and leaving the honeynet as well as activity on the compromised system must be captured without being detected by the intruder. If detected, the intruder may wipe the system drives and depart the honeynet leaving nothing to be analyzed. The second challenge is that captured information cannot be stored on the compromised system. Intruders typically will attempt to modify logs and other actions in an effort to erase their tracks. The data must be stored remotely.

Data Collection involves gathering information from multiple honeynets that are logically or physically distributed. Most organizations have only one honeynet and, accordingly, only need to accomplish Data Control and Data Capture. When an organization has more than one honeynet, all of the captured data must be securely collected and stored in a centralized location. The information that has been assembled analyzed as a whole, greatly increasing its value.

Implementation

Now that you know the requirements of a honeynet, we can briefly discuss how they are implemented. There are two types of honeynets: 1st Generation and 2nd Generation. 1st Generation (or GenI) honeynets use layer-3 technologies such as firewalls and routers to implement Data Control. By limiting the number of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

outbound connections for a given time period, intruders are allowed to execute commands and complete the actions they want without letting them have too much freedom. At the same time, automated attacks to non-honeynet systems can be stopped by blocking new outbound connections after the limit has been reached. Furthermore, since traffic must flow through the firewall, its logs can be used to achieve the Data Capture requirement. Another way is to capture the keystrokes used on the system. GenI honeynets are the simpler of the two but have been proven in the field longer.

By employing 2nd Generation (or GenII) honeynets, greater Data Control is achieved over actions of intruders and simultaneously gives them more flexibility. This is accomplished through the use of a layer-2 gateway device. All inbound and outbound traffic must go through the gateway but, since it has no IP stack, it is more difficult to detect. As well as counting the number of outbound connections, the GenII honeynet can either block or modify an outbound attack to make it harmless. GenII technologies can also fake responses to the intruders attempted attacks in order to increase the deception and keep intruders unaware of the honeynet. Additionally, while GenI honeynets could have information hidden from them through the use of encryption, Data Capture has also been improved for GenII technologies to prevent this.

Other Advantages and disadvantages

Some of the advantages and disadvantages of building a honeypot have been reviewed. These included a reduction of false positives, creating smaller data sets of information and the risk of attacks on systems of other organizations. There are a few other conditions that need to be explained.

Disadvantages:

- Limited view – A honeypot can only see and interact with traffic that is directed at it. It will not capture activity on other systems.
- Risk – Even though it was mentioned above, risk cannot be overstated. In any situation, risk must be analyzed and managed in a way that is comfortable for that organization. Each honeypot has its own level of risk and each implementation must be viewed on a case-by-case basis.

Advantages:

- Cost effective – Since, the only traffic it sees is malicious, it does not need the high performance resources of other systems. Older systems such as "an old Pentium computer with 128MB of RAM can easily handle an entire class B network sitting off an OC-12 network" (Spitzner, "Honeypots: Definitions" 1).
- Monitor unused IP space – While honeypots do have a limited view, some honeypots can be told to listen for traffic destined for IP addresses that don't have computers assigned to them. LaBrea, a tool designed this purpose, can set up to take over unused IP addresses and interact when

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

traffic is sent to them. The process can slow down or stop the spread worm on the Internet.

Strategy and Placement

There is no single defined way to deploy a honeypot. The strategies that follow illustrate some of the more established ways to set them up and show how versatile the concept and technology is.

- Deception Ports on Production Systems – An example would be a production FTP server that does not provide web services. Simulated web services can be installed so that server will react as a Honeypot would but only for web traffic. The FTP services will still be authentic (Moran 3; Scottberg, William, and Doss 3).
- Minefield – Deploying a relatively large amount of honeypot systems. They are placed at the edge (forefront) of the network to function as the first targets of attack (Moran 3; Scottberg, William, and Doss 3).
- Proximity Decoy – Honeypot systems are deployed on the same network as production systems (Moran 3; Scottberg, William, and Doss 3).
- Sacrificial Lamb – A honeypot system that is placed in such a way that it has no connection to any production system (Moran 3; Scottberg, William, and Doss 3).
- Shield (or Redirection Shield) – A router or firewall uses port redirection to forward traffic destined to disallowed services on production systems to a honeypot. For instance, attempts to use telnet to access a web server are forwarded to a honeypot that is a copy of the production server. Connection attempts to are sent to a honeypot while the attackers believe they are connecting to production systems (Moran 3; Scottberg, William, and Doss 3).

When considering the placement of honeypots, most discussions usually position them to monitor activity going to or from the Internet. But, organizations face threats from other sources such as remote gateways and wireless networks as well as internal attacks. Honeypots can be situated to watch for threats from these locations as well.

Remote access usually takes the form of connecting via a modem or using a virtual private network (or VPN). Intruders can scan a range of telephone numbers looking for modems that are connected to computers. This is another way into an organization's network. It is possible for an intruder to identify the intended target's operating system through a modem. They can also conduct penetration testing by making log on attempts using a list of common usernames and passwords. The scanning of modem number, operating system detection and penetration testing can all be accomplished through an automated program called a war dialer. To mitigate the risk of an intruder entering a network in this manner, modems can be connected to a honeypot to monitor for this type of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

activity. Of course, the phone numbers used for the modems should be spares that are not used for any other purpose.

Similarly, a honeypot can be configured to be a termination point for a VPN. A VPN allows users to access an organization's systems via the Internet but appear to be on the organization's network. This allows individuals to share resources no matter what their location is. The use of a honeypot in this situation would be to simulate a VPN termination device, except that the network that it connects the "users" to can be, in actuality, a honeynet.

Wireless networks are added to an organization's existing network for various reasons. It can be a cheaper solution than having to run cable lines for a new department or to allow existing users the freedom to move from office to meeting room without disconnecting from their resources. Whatever the reason, a wireless implementation can allow access to unauthorized parties due to the fact that the range of the wireless network can easily extend beyond the wall of the organization's office building. This has lead to a practice called war driving (related to the act of war dialing previously discussed), which is driving around in a vehicle while locating and exploiting wireless networks. A solution similar to the VPN situation above can be set up so that a separate wireless network is established to monitor for malicious activity.

Internally, there are certain areas of an organization where extra precautions should be taken. They can be departments such as human resources (HR) or payroll. Other areas include the sales department where the client databases are kept or possibly the research and development department (R&D), which contains trade secrets. All of these areas should already have security functionality in place that controls the traffic between departments. For example, it may be justified that the HR department could need access to information from payroll. However, R&D will probably need to explain why they need payroll records. That being said, honeypots can also be added to ensure that the current security strategy stays up to par. And if attempts are made to get at proprietary or confidential information by disgruntled employees, it may well be the decoy system that is attacked. Alerting administrators to the situation before any data can be tampered with (Kilpatrick 2).

Maintenance

A honeypot is not a system that can just be put into place and forgotten about. Many of its advantages can only be achieved if it is dutifully monitored and maintained. By keeping a watchful eye on the honeypot, the activities of intruders can be seen in real-time. This means that tasks such as reviewing logs must be an on-going process. It also means that an organization's response-time to an incident is increased.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In addition, when a honeypot is compromised, it needs to be taken off-line and analyzed. It may, however, take many hours to completely understand what has happened. After a determination of what had been done is completed, the system may need to have files restored, accounts deleted, etc. Basically, this is resetting the honeypot. The information that has been learned from the attack can be used increase the security posture of the production systems.

Another important concern is ensuring that the system is working correctly. In the normal use of any system, some of the processes may stop or disks may become full. The honeypot needs to be regularly checked to ensure its functions are in tact. Also, new attack signatures may need to be installed and systems may need to be patched. These tasks and others are required to keep the honeypot running smoothly.

Honeypot Legalities

The following section will examine some of the legal concerns that can arise when setting up a honeypot. However, this paper is only meant to make the reader aware of some of the legal issues surrounding the deployment of a honeypot in the United States. Depending on the particular situation of the operator, there may be others. Furthermore, the items listed do not cover state statutes or policies and agreements that may have different restrictions. Please consult a qualified lawyer for legal counsel and guidance in the jurisdiction that the honeypot will be installed in. With that said, there are three common issues concerning honeypots: liability, privacy and entrapment.

Liability

Liability can be a concern for an organization that installs a honeypot. By deploying a honeypot, the operators assume the risk that these systems can be taken over by intruders. The risk also extends to the situation that the system and its bandwidth can be used for illegal activates. Intruders may use the systems to participate in a Distributed Denial of Service attack on an E-commerce site or to distribute contraband such as pirated software. Consequently, an organization may be liable for damage to other systems that are not part of the honeypot. This is called downstream liability and it is decided at the state level, not federal (Kabay, “Honeypots, Part 4” 1). For these reasons, it is in honeypot operators’ best interests to mitigate the risk attacks launched from the honeypot systems. The requirement of Data Control for honeynets helps to accomplish this, but there is the chance that intruders can develop techniques or tools that will circumvent this and other controls. Administrators must pay attention to their honeypot systems and take care to react when they are compromised.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Privacy

Privacy is another issue; given that one of the greatest benefits of a honeypot is that all activity can be monitored. However, even though the operators are responsible for keeping the computer network running and secure, they may not have the right to monitor activity. And since there is no single statute concerning privacy, there is the potential that the honeypot operators may run into legal problems. There are several laws in place to prevent improper monitoring and there may be others in your state.

- Federal Wiretap Statute – The Wiretap Act makes it illegal to intercept communications. But, there are exemptions that may be applied which could permit monitoring. The "consent or a party" and "provider exception" exemptions can be used for that purpose.

    - The "consent of a party" exemption allows interception of communications if one of the parties agrees to the monitoring. Consent can be obtained by displaying a banner message stating that activity will be monitored. If the system is used after the banner page is displayed, the intruder has consented to monitoring. The downfall of this use is the fact that an intruder may not use the ports that have the banner message. It is also possible that the port that the intruder is using is not able to show a banner or that the banner is not in a language the intruder can read.
    - The exemption may also be applied if it can be argued that the honeypot system itself is a party to the communication. However, it can't be used once the intruder uses the honeypot to connect to another computer; it will be intercepting communications between two or more different parties.
    - The "provider protection" exemption applies if the interception of communications is to protect rights or property. This exemption has not been defined for honeypots but may have limited application for their use.

- USA Patriot Act – The "computer trespasser" exemption comes from this act and allows the government, or someone under the direction of the government, to monitor activity. The exemption applies under certain conditions:
    - the network operator has authorized the interception
    - the interception is part of a lawful investigation
    - relevant to the investigation

- Fourth Amendment – If a honeypot is being used under the direction of the government, the Fourth Amendment may come into play. It protects the privacy of individuals from government intrusions by requiring a warrant before a "search and seizure" takes place. Monitoring an intruder's

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

activities can fall into this description. Private honeypot operators need not worry about Fourth Amendment violations as long as they are not acting under the direction of the government.

- Entrapment – There are claims that the use of a honeypot is a form of entrapment. Entrapment is a legal defense not a criminal offense. It is used as an attempt to prevent conviction by claiming that the government acted in a way that persuaded the defendant to commit the crime charged, which the defendant would not have normally done. Honeypots merely respond to intruders that have taken the initiative to find them. Also, entrapment only applies to the government so this claim cannot be brought against private honeypot.

- Other laws
  - Electronic Communication Privacy Act of 1986
  - Pen Register Trap and Trace Statute

Future of Honeypots

Honeypots are a relatively new technology, but there have been many advances since they first arrived on the scene. New ideas are still being formulated on how the honeypot concept can be used. Some of these are only minor improvements on existing tools while others bend the paradigm of what a honeypot is.

Honeytokens

A slightly different take on the honeypot concept is a honeytoken. A honeytoken is a new term coined by Augusto Paes de Barros, but not a new idea ("Frequently" 3; Thompson 1). It is a piece of data that has no production value that is inserted into real databases and systems. They are, however, placed in such a way that authorized users won't access them accidentally. The honeytoken will trigger an alarm when attempts to view or retrieve them are made. An example would be using an intrusion detection system (IDS) to look for anyone accessing or downloading a particular filename.

Virtual honeynets

A virtual honeynet is a solution that combines the elements of a traditional honeynet into one system. This is accomplished through the use of a separate software application that allows multiple operating systems to run on the same computer at the same time. Rather than using several pieces of hardware, a honeynet can be deployed using one computer. The reduced cost and management requirements are noticeable benefits. However, some of its disadvantages are that the operating systems that run on the x86 Intel chip architecture are the only ones that can be used. Also, when intruders have

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

compromised one of the honeynets, they may determine that they are in a virtual environment. Lastly, if the software that creates the virtual environment is compromised, the intruders can control all of the honeynet systems (Honeynet Project, "Defining" 1-3).

Virtual honeynets have been categorized into two different categories: Self-Contained and Hybrid. Both types meet the requirements of Data Control and Data Capture. Each can also use both GenI and GenII technologies. A self-contained virtual honeynet puts the entire honeynet onto a single computer. A hybrid virtual honeynet runs the Data Control components (the honeypots) on one system and the Data Capture elements (logging systems) on a different system (Honeynet Project, "Defining" 2).

Honeynet on CD

The Honeynet Project has divided its research into four phases. One of the phases, Phase III, involves putting the honeynet technologies onto a bootable CD-ROM. An organization can boot from the CD-ROM and create a honeywall that deploys the Data Control and Data Capture requirements. It will also allow an organization the capability to log information to a central system so multiple honeynets may be deployed. This feature will, of course, meet the Data Capture requirement (Honeynet Project, "About" 2).

Honey Inspector

The Honeynet Project is currently working on a new tool called the Honey Inspector. It will allow honeypots to managed and analyzed via a GUI interface.

Summary

The honeypot concept is a powerful tool to not only understand attackers but also to protect organizations. It has tremendous applications in these areas as shown in its advancement and evolution. The research so far has shown that systems are continuously under the risk of being compromised. Attackers are ready, willing, and able to take over systems or entire networks if the opportunity arises. Honeypots can address many of the disadvantages of traditional security technologies such as intrusion detection systems. They may also deter intrusions just by attackers knowing that honeypot deployments are increasing in number. At the same time, care must be taken not to fall into any legal pitfalls that may arise including the liability that a neglected honeypot system may bring.

However, it is important to remember that honeypots are not intended to replace conventional security technologies. They work with and compliment the existing security strategy to provide a much stronger defensive posture. In addition, lessons learned from an attack on a honeypot can be applied to an organization's production system.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Over the course of reading this paper, many topics have been covered. There are many aspects of the honeypot concept to address; from deciding which strategy to take to the legal ramifications of deploying a honeypot. The reader is encouraged to delve deeper into this technology by using the list of references to open the door for further research.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

BIBLIOGRAPHY

Blackhat.com. “The Honeynet Project.” URL: http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-honeynet.ppt (16 May 2003).

“Frequently Asked Questions.” 17 March 2003. URL: http://www.tracking-hackers.com/misc/faq.html (16 May 2003).

Honeynet Project. “About the Project.” URL: http://www.honeynet.org/misc/project.html (23 May 2003).

---. “Honeynet Definitions, Requirements, and Standards.” Ver 1.5.2 12 April 2003. URL: http://project.honeynet.org/alliance/requirements.html (20 May 2003).

---. “Know Your Enemy: Defining Virtual Honeynets.” 27 January 2003. URL: http://www.honeynet.org/papers/virtual (27 May 2003.)

---. “Know Your Enemy: Honeynets.” 18 January 2003. URL: http://project.honeynet.org/papers/honeynet (20 May 2003).

---. “Know Your Enemy: Learning with VMware.” 27 January 2003. URL: http://www.honeynet.org/papers/vmware (27 May 2003.)

---. “Know Your Enemy: Statistics.” 22 July 2001. URL: http://www.honeynet.org/papers/stats/ (23 May 2003).

Kabay, M. E. “Honeypots, Part 2.” 15 May 2003. URL: http://www.nwfusion.com/newsletters/sec/2003/0512sec2.html (4 June 2003).

---. “Honeypots, Part 3.” 20 May 2003. URL: http://www.nwfusion.com/newsletters/sec/2003/0519sec1.html (4 June 2003).

---. “Honeypots, Part 4.” 22 May 2003. URL: http://www.nwfusion.com/newsletters/sec/2003/0519sec2.html (4 June 2003).

Kilpatrick, Ian. “Set a Honey Pot Trap to Improve Your Security.” 18 July 2001. URL: http://www.itsecurity.com/papers/honeypot.htm (7 April 2003).

Lemos, Robert. “New Honeypots Get Sticky For Hackers.” 14 April 2003. URL: http://zdnet.com.com/2102-1105-996574.html (16 May 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Liston, Tom. “LaBrea-Intro History.”
URL: http://labrea.sourceforge.net/Intro-History.html (30 May 2003).

Moran, Douglas B. “Trapping and Tracking Hackers: Collective Security for Survival in the Internet Age.” URL:
http://www.cert.org/research/isw/isw2000/papers/15.pdf (30 May 2003).

Poulsen, Kevin. “Use a Honeypot, go to Prison?” 16 April 2003.
URL: http://www.securityfocus.com/printable/news/4004 (16 May 2003).

Rapoza, Jim. “LaBrea Makes Life Sticky for Net Worms.” 1 October 2001.
URL: http://www.eweek.com/article2/0,3959,48623,99.asp (30 May 2003).

Salgado, Richard P. “Honeypots: Legal Issues.”
URL: http://project.honeynet.org/speaking/legal-issues.ppt.zip (1 June 2003).

---. “The Legal Ramifications of Operating a Honeypot.” IEEE Security and Privacy. March/April 2003 (2003): 16-17.

Scottberg, Brian, William Yurcik, and David Doss. “Internet Honeypots: Protection or Entrapment?” URL:
http://www.sosresearch.org/publications/ISTAS02honeypots.PDF (30 May 2003).

SearchSecurity.com. “War Dialer.” URL:
http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci546705,00.html (29 May 2003).

---. “War Driving.” URL:
http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci812927,00.html (5 June 2003).

Spitzner, Lance. “The Honeynet Project: Trapping the Hackers.” IEEE Security and Privacy. March/April 2003 (2003): 15-23.

---. “Honeypots: Definitions and Value of Honeypots.” 9 May 2003.
URL: http://www.tracking-hackers.com/papers/honeypots.html (5 May 2003).

---. “Honeypots: Simple, Cost-Effective Detection.” 30 April 2003.
URL: http://www.securityfocus.com/printable/infocus/1690 (20 May 2003).

Thompson, Nicholas. “New Economy.” 28 April 2003. URL:
http://www.newamerica.net/index.cfm?pg=article&pubID=1205 (19 May 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.