

Honeypots Sweeten IT Security Controls

8/24/05

JOHN THOMPSON

www.jjthompson.net

Questions regarding Honeypots will continue to arise as companies continually improve their network defenses and alerting capabilities. Just like any other countermeasure, the pros and cons of potential deployment of a Honeypot should be carefully evaluated.

While evaluation metrics are beyond the scope of this document, this document serves three purposes: first, to answer a few frequently asked questions regarding entrapment, and cost of deployment; second, discuss the benefits of deploying a Honeypot; and third, to implore you to consider the risks.

First, entrapment by definition is: "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."^[1] Unless you or your clients are law enforcement, you should be in the clear with respect to entrapment issues. Before taking it upon yourself to make this judgment call, you should discuss this with your company's legal counsel.

To achieve the maximum benefit from the deployment of Information Security controls, one must deploy IT controls that enhance the client's overall IT control environment and reduce the risks associated with IT as it relates to their business. To accomplish this, two types of controls may be used: preventative controls used to prior to the occurrence of a risk, and detective controls to alert you or provide an audit trail once a breach has occurred.

Honeypots as a Preventative Control

Deployment of Honeypots adds marginal value as a preventative control, but it is still value. The case where they would help with prevention would be the case where you believe that to attract an attacker to the honey would cause them to waste time and effort attacking a non-production critical system. This delay would provide the IT organization with additional time to detect the attack before it spreads to critical hosts, increasing the likelihood of detection, allowing for a timely response to prevent the attacker from reaching critical systems (blocking the attacker, etc). In support of this, a paper on Honeypots stated that "'All warfare is based on deception.' The current poor state of

security on the Internet, the increasing level of Internet attacks, and the threat of terrorist action has created an environment we would characterize as unconventional 'information war' where the role of deception is very relevant." [2] If the cost in time and resources is greater to hack your network than the next potential target, the attacker will move elsewhere.

Honeypots as a Detective Control

Honeypots add value as a detection tool. Enterprise Security Administrators have the difficult task of reduction of false positives and negatives while responding adequately to legitimate attacks. On a production system, it is more difficult to adequately tune the IDS to reduce the false positives, increasing the risk that an attack may go undetected. Any and all traffic to a Honeypot is not legitimate and therefore makes it easier to detect true reconnaissance attempts and attacks.

Honeypot Cost

Cost of deployment can be next to none as a vanilla Win2K box can be deployed with netcat as the listening / capture device. Cost of maintenance is no more than any other desktop or server in the enterprise and monitoring should be automated, making the increased monitoring cost merely marginal as well.

Conclusion

Based on the believe that value is gained by using a Honeypot as either a preventative or detective control, it is my opinion that a formal assessment of the added benefits of a Honeypot deployment would be well worth the time as it is likely to improve your overall IT Security defenses by reducing the likelihood of compromise.

[1] <http://www.lectlaw.com/def/e024.htm>

[2] B. Scottberg, 2002 <http://www.sosresearch.org/publications/ISTAS02honeypots.PDF>