



Honeypots for hacker detection

Honeypots are an under-utilized security tactic

Security: Risk and Reward By [Andreas M. Antonopoulos](#), Network World
July 06, 2010 10:49 AM ET

5 Comments  Print

 Like Confirm  0

Most corporate networks lack serious oversight, that is, no one is really watching. [Watching the network](#) and computer systems is expensive, overwhelming and fraught with false positives. No wonder then that insider attacks go undetected for months, malware proliferates stealthily and hackers can spend their time gradually infiltrating deeper and deeper, [undetected](#). It's simply too hard to discern between legitimate activities and illegitimate or malicious activities. Without context, wading in the enormous volume of logs or network traffic leads to information overload. How to tell who's up to no good? Well, you shall know them by their deeds.

[FBI details most difficult Internet scams](#)

Honeypots are, in my opinion, an underutilized tactic. Every attack, whether manual or automated, has an exploratory component. When [hackers or viruses](#) go probing networks and systems they are usually able to do so unnoticed. Unless they cause a system crash or overwhelm a system, the chances of detection are pretty low. A honeypot is a system that detects unusual activity by creating false targets. In a network, for example, a simple honeypot may allocate the unused IP address space. Then if someone attempts to access an IP address that is not used, an alert can be generated. Similarly, a port-based honeypot could respond to requests on unused TCP ports, creating the illusion of services. Entire computers, or even networks of computers, can be created to lure attackers.

Some may object to the use of honeypots because they might be seen as "entrapment" under the law. I'm recommending the use of honeypots for detection and prevention of attacks, not prosecution. If someone is accessing a system that has no DNS name, no public or registered services, no legitimate function, then it is quite likely that they're up to no good. Alerting on such access can give security professionals advance warning of attacks with fewer false positives. Of course, there are network diagnostic tools and other management tools that probe entire networks, but it is not very difficult to exclude those. Honeypots can even automate intrusion prevention by temporarily blacklisting IP addresses, thereby acting as booby traps for attackers.

I've applied this tactic successfully on both personal and corporate networks. What perplexes me is that there are so few vendors offering honeypot-like solutions in their products as a standard security feature. Network equipment (routers and switches) could offer phantom honeypot networks that generated alerts. Virtualization software could create entire phantom honeypot data centers. Service providers could use honeypots on unallocated network space. Sophisticated honeypots can

even "lure" attackers by creating the illusion of success and escalating the intrusion, profiling

Related Content

- [What would your ultimate network security look like?](#) [BLOG](#)
- ["Help, I am stranded!" scam haunting social networks](#) [BLOG](#)
- [Four critical US cybersecurity projects that need constant pressure](#) [BLOG](#)
- [Coming soon: Ubiquitous surveillance from Big Brother's wayback machine](#)

[View more related content](#)



Get Daily News by Email

Most Read

- [Why Eric Schmidt's prediction about Android vs. iOS development is wrong](#)
- [2012 looking ripe for disgruntled IT pros to switch jobs](#)
- [Microsoft to start automatic updates of IE without asking the users](#)
- [Googler's LAN-party house sparks awe and envy](#)
- [LAN-party house guy spills important cost details](#)

[View more Most Read](#)

Videos



Latest News



Security White Papers

[Optimizing Performance for Backup and Recovery](#)

This paper describes the benefits and potential risks of three optimization technologies commonly...

[Sustainable Compliance for the Payment Card Industry Data Security Standard](#)

Organizations continue to struggle to achieve compliance with

the attacker all the way (see www.mykonossoftware.com for one example of this tactic)

There are very few legitimate reasons to go probing in the dark recesses of most networks, operating systems or applications. Honeypots give us an opportunity to set traps in those spaces, making an attacker's exploratory forays risky and more likely to be detected. A mirage of fake systems can waste attacker's time, giving us a head start in detecting, identifying and thwarting them. That's how you catch hackers with honey.

1 [2](#) [Next >](#)

5 Comments Print

Like Confirm +1 0

FREE Download: Who's who in IPv6 - The Leading Companies and People »

From CIO.com

- 2011's Hottest Holiday Tech Gifts
- CES 2012 Gadget Preview
- Facebook Security Tips to Stay Safe in 2012
- 6 Hot IT Jobs That Will Pay Well in 2012

[Read the latest from CIO.com](#)

Questions From IT Pros

- Best IT careers
- Favorite Unix commands
- MBA vs. Masters in Computer Science?
- Ubuntu vs. Mint vs. Fedora. Which do you prefer?

[Read more at ITworld Answers](#)



the Payment Card Industry Data...

[Oracle's Optimized Solution for CRM - A Business Case for Secured Siebel CRM on Oracle's SPARC T-Series](#)

Customer relationship management (CRM) applications have rapidly become mission-critical for...

[View more Security White Papers](#)

Security Webcasts

[CISO in the Know - Mitigating Modern Attacks: Zero-day's, Low&Slow's and APT's](#)

Cyber adversaries are in a position of strength and have overmatched traditional countermeasures....

[Build in Security and Drive Innovation](#)

Hear from Patrick Vandenberg, IBM Security & Compliance Marketing Manager and Ewa Hoyt, IBM...

[Demystifying Common Security Issues with the SecureX Files](#)

Watch new videos which simplify cybersecurity for people outside the security industry. Each video...

[View more Security Webcasts](#)

Security Downloads

[Protecting Your Organization from Internet-Based Threats](#)

Discover iPrism's rich, multi-layered feature set and award-winning proprietary defense technology...

[View more Security Downloads](#)

Newsletter Sign-Up

Receive the latest news, reviews and trends on your favorite technology topics

- Security Alert
- Compliance Alert
- Daily News Alert
- Data Center Alert

[View all newsletters](#)



- Industry
- Job Title
- Company Size
- Country

[Subscribe](#)

[Terms of Service](#)