Honeypots: Using Connection Redirection

by B. Pelletier
Norwich University, Northfield VT

[Note from M. E. Kabay, PhD, CISSP: My undergraduate research student, Bob Pelletier, an IA Scholarship winner, graduated from Norwich University this May and has started what I am sure will be a wonderful career in the computer security field. Here is his brief summary of his much longer, masters-quality report on his research this year in our information assurance program.]

Introduction

A honeypot is defined as any system designed for the sole purpose of being exploited. This is a broad definition that can be implemented in many ways. However one designs a honeypot, the underlying goal is to create a system that appears to be vulnerable.

Honeypots have been used for two main purposes. The first purpose is research. Research groups such as the Honeynet Project have used honeypots to capture information about blackhat methods for compromising computers.

The second purpose has been for attack detection and to a lesser extent, attack mitigation. In particular, these systems have been placed in some production atmospheres among critical machines. Honeypots can serve as lightweight intrusion-detection systems. They can also use deception to confuse blackhats. The theory behind deception assumes that by creating more targets for attackers the likelihood that they will hit a legitimate machine will decrease.

Theory

My recent work has focused on the possible attack-mitigation benefits of honeypot farms and similar architectures that use a routing device to redirect attacks. If attacks going to a legitimate system can be redirected to a honeypot posing as the original destination without the attacker’s knowing it, then this redirection will accomplish three things.

* First and most important, the attack against the legitimate server will be neutralized.

* Second, the attacker will not know he is attacking the honeypot and therefore will be less likely to fingerprint the system for what it really is. Most of the attacker’s network mapping will be done on the legitimate server and only actual attack traffic will be redirected to the honeypot such as exploits depending on the redirection criteria.

* Third, any successful attacks that compromise the honeypot can be studied in depth and used to better protect the legitimate server since it has the same vulnerabilities by the nature of the two mirrored systems. This strategy also provides a quantitative measure of success. Any malicious traffic that is captured by the honeypot would have reached the legitimate server if the redirection had not taken place. This strategy has many benefits over the traditional deception methodology where it is hard to prove attacks are actually being drawn away from legitimate systems through the use of unhardened honeypots.
Technology

The key to attack redirection is packet filtering. The deception methodology employed by some honeypot solutions can potentially help protect production computers. However, the deception methodology does have its limitations. The added mist of network nodes may confuse a hacker, but what happens when the attack finally hits a legitimate machine? Nothing is redirected and the attack does not have a chance to be studied.

Many filtering methods are available but this solution requires both full packet content examination and the ability to alter packet fields. Full packet content must be examined if the majority of attacks are going to be recognized and the packets must be altered to accomplish the redirection. The Linux based firewall _iptables_ is particularly suited for this task. With _iptables’_ string matching functionality and its ability to mangle packets, the proposed solution can be created. To make writing the attack identification rules easier there are a few programs available that will convert intrusion-detection system (IDS) rules into _iptables_ rules. One of these tools has been released by Bill Stearns called _snort2iptables_. Stearns’ tool is composed of a few scripts that are able to convert 92% of the rules written for the popular IDS called _Snort_. Using _iptables_ and _snort2iptables_, packets can be examined for attacks against well-written signatures and redirected to a honeypot system if they are deemed malicious.

Future

With honeypot technology improving, these systems will soon make their way into the common defense-in-depth strategy employed by many organizations today. With honeypots’ ability to capture a vast amount of information and their possible attack mitigation capability as described in this article, they are certainly a useful tool. The day is not far away when a sleek yellow server labeled “Company Honeypot” will sit right above the servers labeled “Company IDS” and “Company Firewall”. Of course other honeypots will be lurking, unlabeled, in the nearby closets to capture the actions of those devious insiders.

* * *

Author’s Note

I would like to thank the staff at NetBait for their unstinting support of my research over the last year. In particular, I received a great deal of help from Ilya Zeldin, Konstantin Strakovsky and Ivan Milovidov and much appreciate their kindness. To contact me, use <mailto:pelletib@eruditeaegis.net>.

* * *

FOR FURTHER READING


<http://www.honeynet.org/>

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 Bob Pelletier. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.