A honeypot used as a security awareness tool

How to use honeypot to inform your users...

Alexandre Dulaunoy

ASBL CSRRT-LU (Computer Security Research and Response Team Luxembourg)
http://www.csrrt.org/

February 13, 2009

Introduction

- A large number of public/semi-public hotspot are installed in companies, libraries or alike. They generally provide an unlimited access to Internet with "very" limited security.
- Users are often very happy to find a hotspot and they used without thinking about security. (They often don't read the paper included with the Hotspot regarding security)
- The idea is to build a Honeypot on such hotspot to inform users on the weak security of some protocols.

POP3 as an example

- POP3 is described in the RFC1939
- ...and you can see that the security was not really considered

```
13. Security Considerations

...
 Use of the PASS command sends passwords
 in the clear over the network.
...
 Use of the RETR and TOP commands sends
 mail in the clear over the network.
 Otherwise, security issues are not
 discussed in this memo.
```

Security Awareness ?

- Gathering potential attackers is interesting but it's not the only use of honeypot.
- Informing the user about the weak security there are relying on. But how ?
- We will send an email directly in their mailbox. We'll do a kind of Man-in-the-middle attack in POP3.

How to proceed ?

- We assume that we redirect all TCP traffic to port 110 on a specific service
- Building a fake POP3 server
  - Integrating a script with honeyd ?
  - Building a custom POP3 Server (Net::Server)
  - Using and Extending existing POP3 honeypot

Q and A

- Thanks for listening.
- adulau@foo.be