Honeypots

on embedded systems

Matt Coley
Outline

• Background on honeypots
• Glastopf on Raspberry Pi
• Overview of Glastopf
• Discuss key features
• Quick demo
Overview

• Honeypot – a trap set to detect attempts at unauthorized use of information systems

• Production honeypots
  – capture limited data
  – primarily used in corporations

• Research honeypots
  – more complex
  – used to research threats, gather information
Overview

• High interaction
  – imitate activities of real systems
  – more expensive to maintain

• Low interaction
  – simulate frequently targeted services
  – ex. Glastopf
Glastopf

• Low interaction web application honeypot
• Emulates many different vulnerabilities
• Based on vulnerability emulator vs modified templates
  – HIHAT, DShield, Google Hack Honeypot
Glastopf Overview

• Vulnerability emulator
  – not concerned with specific vulnerabilities, only concerned with what attacker expects to see
  – operates basically like a normal web server
Handling the Request

• Glastopf currently supports processing of the GET, POST, and HEAD requests
  – HEAD requests are answered with a generic header
  – POST requests will have their contents stored in a database
  – GET requests are what Glastopf mostly handles
Handling Get Requests

• Determine type of attack using predefined patterns
  • Example
    – request
      
      ```plaintext
      ```
    
    – pattern
      
      ```python
      if '=' in request:
        handle_rfi_request()
      ```
Remote File Inclusion

- Attacker includes malicious file in vulnerable code
- Send HEAD back to attacker and attempt to obtain file
- Search for echo (expected feedback)
- Search for called variables and replace with appropriate values
RFI Example File

```php
<?php

$un = @php_uname();
$up = system(uptime);

echo "uname -a: $un<br>";
echo "uptime: $up<br>";

?>
```

uname -a: GNU/Linux,"Linux my.leetserver.com 2.6.18-6-k7<br>
uptime: 19:42:43 up 3 days, 22:39, 1 user, load average: 0.9, 0.2 0.1<br>
Attracting Attackers

• How does Glastopf attract attackers?
• Attackers using search engines
• Dorks
• Dynamic dork list
Extensions

- MySQL plug-in
- PostgreSQL plug-in
- RawOut plug-in
- FileURL plug-in
- DbClient plug-in
Demo

- Glastopf on Raspberry Pi
- Remote file inclusion
References

• Glastopf Pi: A Simple Yet Cool Web Honeypot for your Raspberry Pi
  – http://resources.infosecinstitute.com/glastopf-pi-a-simple-yet-cool-web-honeypot-for-your-raspberry-pi/

• Know Your Tools: Glastopf