Web Presence Monitoring using Perl

SANS MSISE Community Project
First Oral Presentation
Kevin Bong
July 29, 2007
Web Service provider Management

- Due Diligence
- Periodic Vendor Review
- Business Continuity
  - Their plan and your plan
- Testing
- Monitoring
Monitoring your Service Provider

• Web server and Internet connection uptime
• Application and database uptime
• Response time and load testing
• DNS reliability
Security and Brand Monitoring

- Defacement
- DNS Spoof/Hijack
- Denial of Service
- Referrals and associations
- SPAM sites/corporate identity theft
- Brand/Graphic use
Web service monitoring options

1. Commercial Service Provider
2. Commercial Software
3. Code it yourself
   - Consider cost, skills, flexibility, Internet connectivity, and maintenance effort
Why PERL

• Free and open source
• Cross platform
• Many useful add-on modules are available
• Flexibility
• Powerful pattern matching/text manipulation abilities
• Easy to schedule with Windows Scheduler or cron
Perl Set Up

• Download and install Activestate ActivePerl distribution

• Install any needed additional packages using Perl Package Manager

C:\> ppm install Net-DNS
C:\> ppm install http://theoryx5.uwinnipeg.ca/ppms/Crypt-SSLeay.ppd
# set a High Resolution timer
$starttime = [gettimeofday];

# Lookup DNS
my $resolver = Net::DNS::Resolver->new;
my $query = $resolver->search('demo.sample.com', "A");
if ($query) {
    foreach $responserecord ($query->answer) {
        $returnedIPAddress = $responserecord->address;
        if ($returnedIPAddress ne '192.168.6.101') {
            send_mail($mailfrom, $mailto, $mailsubj, "Error: DNS Addr
        SaveToFile($logfile, "Error: DNS Address $returnedIPAdd
        } else {
            $responseTime = tv_interval ($starttime, [gettimeofday]);
            SaveToFile($logfile, "DNS Response Correct: $returnedAdd
my $req = new HTTP::Request('GET', "https://demo.sample.com/login.html");
my $response = $ua->request($req);
if ($response->is_success)
{
    SaveToFile( "content_Current.html", $res->content);
    if (compare("content_Current.html","content_Original.html") == 0)
    {
        SaveToFile($logfile, "Web page login.html has not changed\n");
    }
    else
    {
        SaveToFile($logfile, "Error: web page login.html has changed");
        send_mail($mailfrom, $mailto, $mailsubj, "Error: login.html changed"
    }
} else # web page unavailable, send an alert
Sample logfile output

9/26/06 19:11:25 DNS Response Correct: 192.168.6.101 in 5.056 seconds
9/26/06 19:11:30 Web page login.html has not changed
9/26/06 19:16:29 Web page login.html has not changed
9/26/06 19:21:24 Error: Page login.html has changed
9/26/06 19:26:15 Error: Bad DNS Response: 172.16.1.9 in 1.028 seconds
9/26/06 19:27:17 Error: Page login.html is unavailable
9/26/06 19:32:21 Error: DNS service for demo.sample.com is unavailable
Web Application Availability

- Script a Multi-step form submission
  1. Start a timer
  2. Load the login page
  3. Submit the login page using a test account
  4. Check the response page for expected content (i.e. “Account Balance:”)
  5. Submit the logout page
  6. Record the time elapsed
Use Ethereal (or other sniffer) to determine form fields
• Response time thresholds
  - Alert if the response time for the “Web Application Availability” script exceeds a preset threshold

• Web site load testing
  - Run multiple instances of the “Web Application Availability” script in a loop.
Referrals and Associations

• Who is talking about you, copying content from your site, or linking to your site?
• Automate monitoring of search engine results
• Track changes month to month/monthly email of new search engine hits
What to search for?

• Your URL
• Your organization name
• A block of text off your home page
• Filenames of key images/logos on your site (provided they are unique)
```perl
$searchurl = "http://www.google.com/search?q=" . uri_escape($searchstring);
$searchresultshash =;
while ($allcontents)
{
    # RegExp to cut each of the search results out
    @searchresults = ($allcontents =~ m/<h2 class="r">
        (.*)</h2>/igs);
    foreach $resultmatch (@searchresults)
    {
        if ($resultmatch =~ m/<a href="(.*)".*>/)
        {
            # searchresulthash contains the URL and the link text
            $searchresultshash{$1} = $2;
        }
    }
    # Look for the "Next" link...meaning there are more results available
    if ($allcontents =~ m/<div sid="nn">
        Next</a>/)
    {
        $onmoreresultsstart += 10;
        $allcontents = &geturlcontents($searchurl . 
            "&start=" . $onmoreresultsstart;
    }
```
Brand Monitoring Output Sample

Perl Brand Monitor Report - Message (Rich Text)

From:          Sent:     Tue 6/26/2007 8:37 AM
To:  Kevin Bong
Cc:          
Subject:  Perl Brand Monitor Report

Perl Brand Monitor Report
Search for:"Kevin Bong" SANS
Google Query:  http://www.google.com/search?q=%22Kevin%20Bong%22%20SANS&filter=0&btnG=Search

Last Run:  5/30/2007 3:45 pm
This Run:  6/30/2007 3:45 pm

Total New Search Results since last run : 16

Charlotte's Web Site Answers and Winners

http://www.giaco.org/certified_professionals/listing/gcfa_100_1346.php
803 GCFA Certified Professionals

The Business Journal of Milwaukee: People in the News

http://www.sans.edu/resources/security/ab/elfering_northcutt.php
Technology Institute. Interview with Stephen Northcutt
Web Presence Monitoring Wrap-up

- Critical component of vendor and service management
- Commercial or home-grown options
- Monitor for availability and performance
- Monitor security and brand protection
- Historical records and trending
Web Presence Monitoring sample scripts

• Perl scripts demonstrating these concepts are available at:

http://www.lapooh.com/presence/