Skipfish - Web Application Recon Tool

Presented by
Aaron Grothe/NebraskaCERT
11-17-2010

Disclaimer

- Please do not do anything stupid with Skipfish
- If you do, please don't mention me
- Only use Skipfish if you are authorized to do it
- Skipfish is NOT stealthy – will light up an IDS like an X-mas tree
- Skipfish can launch a pretty effective DOS attack against your server

What is Skipfish?

- Simply Skipfish is a tool to get info from websites
- It will do checks for the following
  - SQL, XML, shell Injection
  - Cross-site scripting attacks
  - CSS attacks
  - Checking for some default directory paths
  - Pretty complete site map (including looking at commented out links)

How does Skipfish compare?

- It is written in good old “C” it is fast!!!
- It is a young tool that is evolving pretty rapidly
- Can't do some checks other tools can such as
  - LDAP injection
  - Cookie manipulation
- Looks for hidden links a lot better than any other system I've seen

Take a look at Skipfish options

- Lets take a look at skipfish -h
- Lets take a quick look at the wordlists usually in /usr/share/skipfish/dictionaries

Take a look at results from www.nebraskacert.org

- Http://www.nebraskacert.org Is a pretty simple site
  - No database back end
  - PHP5 and straight text
  - System is reasonably well locked down

Take a look at the results from www.certconf.org

- Runs on same webserver as www.nebraskacert.org
- Similar setup (no database backend, php5, etc)

What does it look like on the Wire

- Fire up wireshark and take a quick look at a simple skipfish check on a default apache install

Impact on the Scanned System

- You'll generate some pretty serious logs on the webserver
  - Www.nebraskacert.org - 9 Gb log files
  - Www.certconf.org - 33+ Gb log files not a complete scan
  - Default apache install - ~1 Gb log files
- Puts a good load on the system – figure 1x the number of apache processes on your system

5 Things you Should Know

- If you pass any values on the command line a simple ps will display them. E.g. Cookies
- You can crash a poorly configured system with it and a good pipe, pretty much crashed a DVL virtual machine
- It is a google product, so don't expect a non-beta anytime soon
- How to use screen
- It will give false positives, Don't panic

5 Tips

- Running it locally, running over a lan unless you have gig-e will slow things down
- It is evolving quickly so building from source isn't a bad idea
  - Debian Testing - Skipfish 1.32b
  - Fedora 13/14 – Skipfish 1.54b
  - Latest Souce – 1.70b

5 Tips Continued

- If you install the packaged version copy the wordlists to your local directory and then run with the -W option, so you can save results
- -F host:ip – lets you pretend a host has an IP, so you don't have to mess with /etc/hosts
- Trickle can help you hold it back a bit – http://monkey.org/~marius/pages/?page=trickle

5 Things Skipfish Needs

- Ability to save new wordlists to extension file, for packaged versions
- Ability to flush partial results
- Suspend/Resume
- Estimation of time/number of requests
- Ability to pass sensitive info safely to system

Is Skipfish Worth It?

- Quick answer – Yes – found several things I need to fix on the NebraskaCERT webserver
- It is a free tool, so there isn't any reason not to try it out
- For most systems is just an apt-get or yum install away
- Evolving, interested to see where it goes from here

Should I use skipfish or Nikto/W3af?

- Nikto is excellent at looking for specific components and shortcomings of default systems
- W3af is another web scanner with an easy to use GUI front end
- Each can be extended a lot more easily than Skipfish
- Both are written in higher languages (Perl & Python respectively)

References

- Homepage for skipfish – http://code.google.com/p/skipfish
- OWASP home page (every web talk is pretty much by law required to list them) – http://www.owasp.org
- W3af (another web application scanning tool) – http://w3af.sourceforge.net

Q & A – Thank You

- Questions?
- Thank you for listening