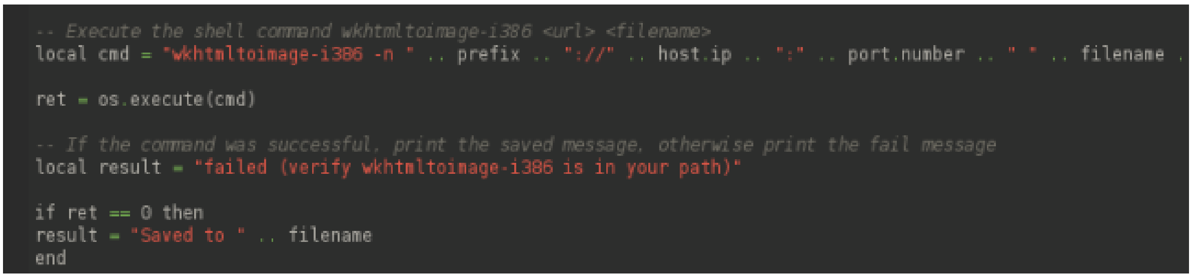
# Nmap Script to Screenshot Web Services

pentestlab.blog/category/network-mapping

June 24, 2012



```
-- Execute the shell command wkhtmltoimage-i386 <url> <filename>
local cmd = "wkhtmltoimage-i386 -n " .. prefix .. "://" .. host.ip .. ":" .. port.number .. " " .. filename .

ret = os.execute(cmd)

-- If the command was successful, print the saved message, otherwise print the fail message
local result = "failed (verify wkhtmltoimage-i386 is in your path)"

if ret == 0 then
result = "Saved to " .. filename
end
```

One common situation when conducting a penetration test in web servers and especially in non production systems is the fact that you can discover many services that are not even running a web application.In order to address this problem and to look only the specific services that are running applications Trustwave SpiderLabs have created a Nmap script which allows you to take a screenshot of the running web services.

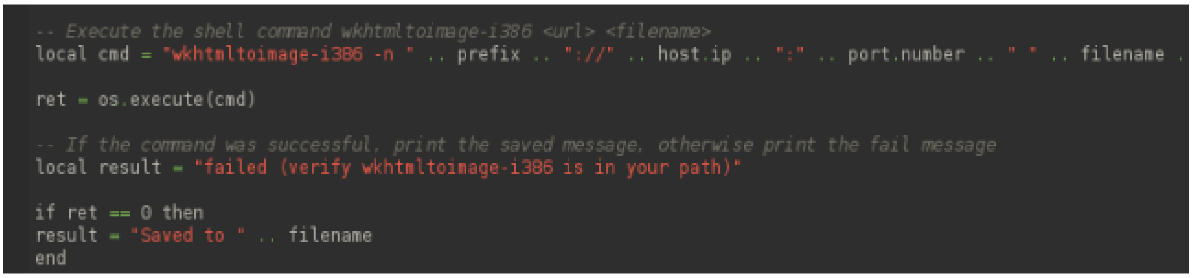
This script depends on the wkhtmltoimage tool in order to work efficiency.So the first step is to download it,extract it and copy it on the **/usr/local/bin** folder.In order to achieve that we need to execute the following command from our terminal.

**wget http://wkhtmltopdf.googlecode.com/files/wkhtmltoimage-0.11.0_rc1-static-i386.tar.bz2**
**tar -jxvf wkhtmltoimage-0.11.0_rc1-static-i386.tar.bz2**
**cp wkhtmltoimage-i386 /usr/local/bin/**

Now it is time to download the http-screenshot script and place it on the following path where all the nmap scripts are located.

**/usr/local/share/nmap/scripts/**

This script will call for the wkhtmltoimage executable in order to take the screenshot.So it is basically integrates this tool inside the nmap.

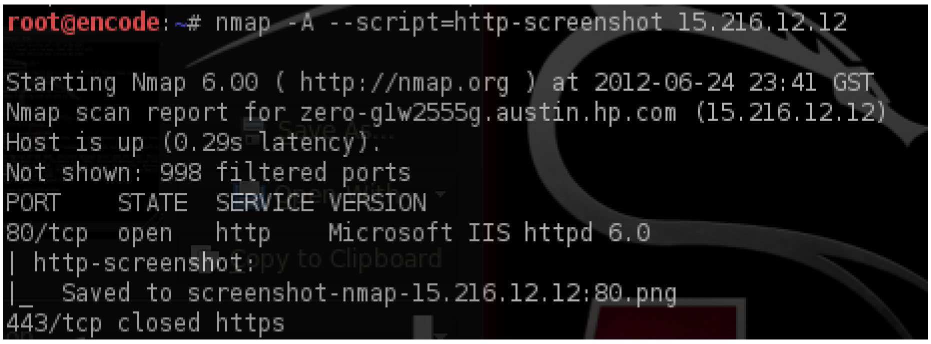


```
-- Execute the shell command wkhtmltoimage-i386 <url> <filename>
local cmd = "wkhtmltoimage-i386 -n " .. prefix .. "://" .. host.ip .. ":" .. port.number .. " " .. filename .

ret = os.execute(cmd)

-- If the command was successful, print the saved message, otherwise print the fail message
local result = "failed (verify wkhtmltoimage-i386 is in your path)"

if ret == 0 then
result = "Saved to " .. filename
end
```

http-screenshot script – code

Now its time to run the command **nmap –script-updatedb** in order to update our nmap script engine with the new script.

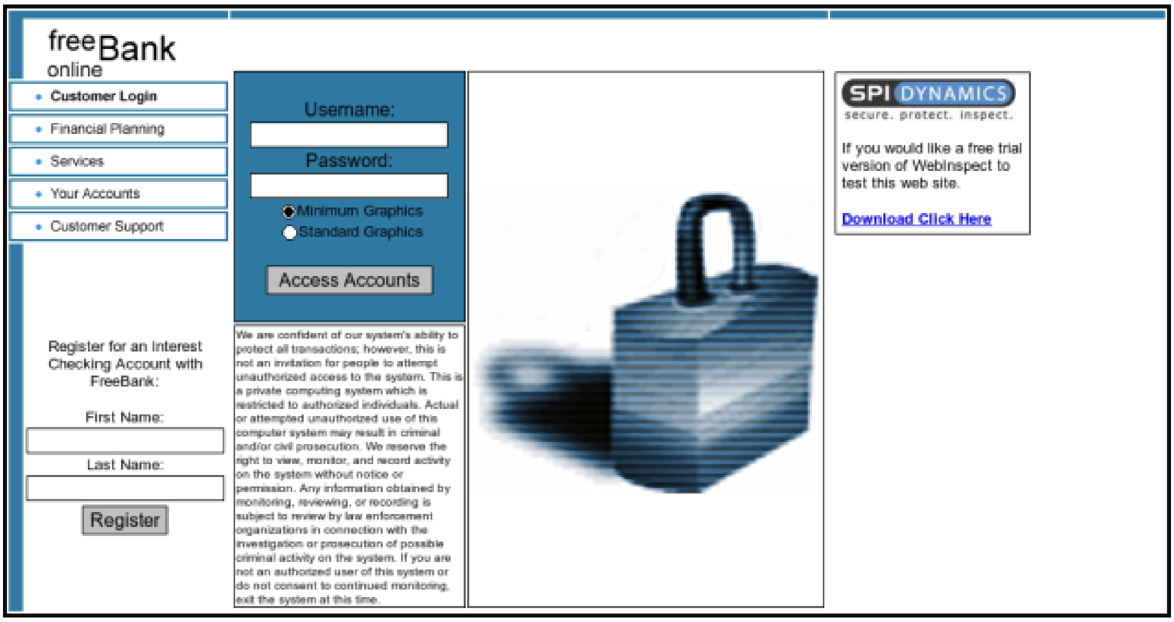
If we want to test this script all we have to do is to call the script in our nmap scans.For example:



```
root@encode:~# nmap -A --script=http-screenshot 15.216.12.12

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-24 23:41 GST
Nmap scan report for zero-glw2555g.austin.hp.com (15.216.12.12)
Host is up (0.29s latency).
Not shown: 998 filtered ports
PORT    STATE  SERVICE VERSION
80/tcp  open   http    Microsoft IIS httpd 6.0
| http-screenshot:
|_  Saved to screenshot-nmap-15.216.12.12:80.png
443/tcp closed https
```

http-screenshot script in use

As you can see from the example it saves the image with the IP of the host and with the port that the service is running.Lets see the saved screenshot:



Register for an Interest Checking Account with FreeBank:

We are confident of our system's ability to protect all transactions; however, this is not an invitation for people to attempt unauthorized access to the system. This is a private computing system which is restricted to authorized individuals. Actual or attempted unauthorized use of this computer system may result in criminal and/or civil prosecution. We reserve the right to view, monitor, and record activity on the system without notice or permission. Any information obtained by monitoring, reviewing, or recording is subject to review by law enforcement organizations in connection with the investigation or prosecution of possible criminal activity on the system. If you are not an authorized user of this system or do not consent to continued monitoring, exit the system at this time.

If you would like a free trial version of WebInspect to test this web site.

Screenshot of a web application from Nmap

## Conclusion

Nmap has a very powerful script engine that allows you to discover additional information regarding the hosts that you are scanning.Basically this script uses the tool wkhtmltoimage in order to perform the job but from the script engine of nmap making the scans of web services more effective.With this script that Trustwave SpiderLabs have created,you can have an idea of which services are worth looking for your penetration test from the moment of your scan reducing the time that you have to spend by examining every web service separately.