Web Application Fingerprinting

pentestlab.blog/category/web-application/page/14

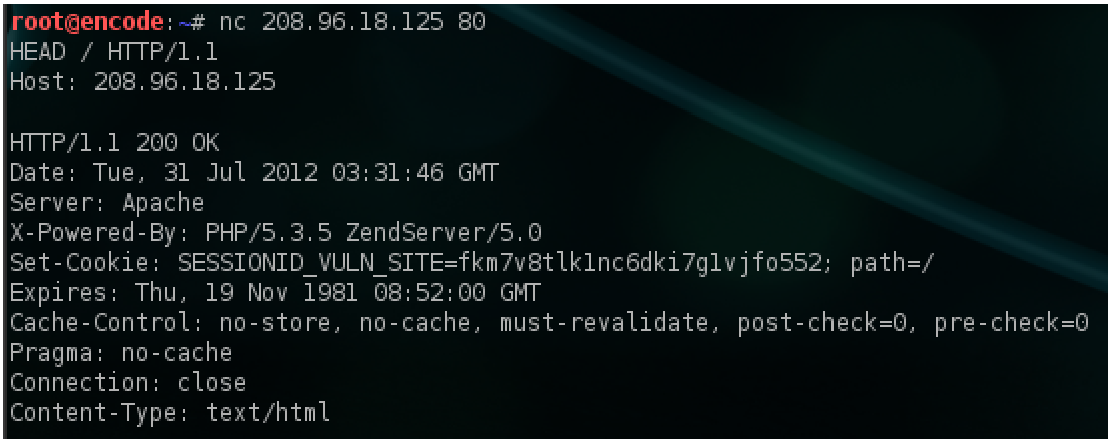
August 1, 2012

One of the first tasks when conducting a web application penetration test is to try to identify the version of the web server and the web application.The reason for that is that it allows us to discover all the well-known vulnerabilities that are affecting the web server and the application.This process is called web application fingerprinting and in this article we will see how to perform it.

The web application fingerprinting can be done with the use of a variety of tools or manually.

Manual Fingerprinting

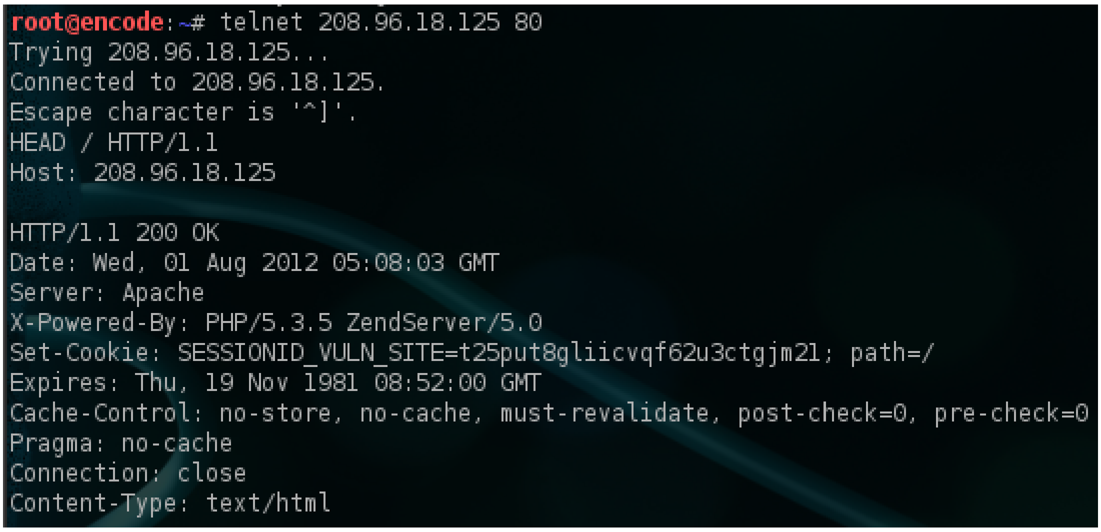
This can be done with the use of different utilities such as the telnet or the netcat.For example we can try to connect with netcat to the remote webserver that is running on port 80.We will send an HTTP request by using the HEAD method and we will wait for the response of the web server.



```
root@encode:~# nc 208.96.18.125 80
HEAD / HTTP/1.1
Host: 208.96.18.125

HTTP/1.1 200 OK
Date: Tue, 31 Jul 2012 03:31:46 GMT
Server: Apache
X-Powered-By: PHP/5.3.5 ZendServer/5.0
Set-Cookie: SESSIONID_VULN_SITE=fkm7v8tlk1nc6dki7glvjfo552; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html
```

Web Application Fingerprinting – netcat

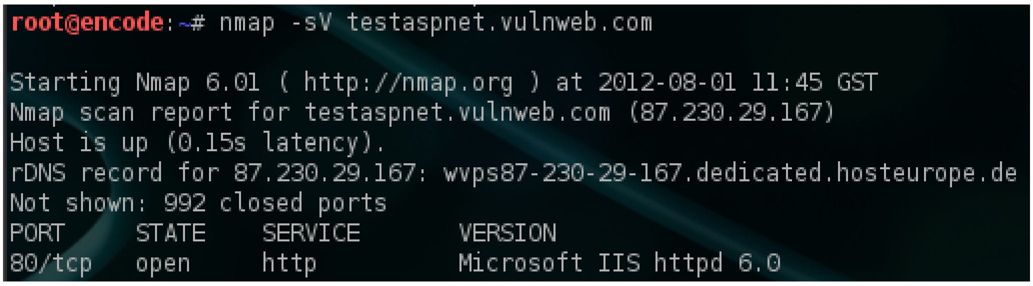
As we can see from the HTTP response header the type of the web server is Apache.Also we have managed to identify the technology from the X-Powered-By field name along with the version that supports the application which is PHP/5.3.5 and also the web application that is running on the web server which is a ZendServer.Alternatively if we don’t want to use the netcat utility we can use the telnet in order to obtain the header information from the web server.The image below is showing the usage of telnet in obtaining the HTTP Response Header from the same web server.



```
root@encode:~# telnet 208.96.18.125 80
Trying 208.96.18.125...
Connected to 208.96.18.125.
Escape character is '^]'.
HEAD / HTTP/1.1
Host: 208.96.18.125

HTTP/1.1 200 OK
Date: Wed, 01 Aug 2012 05:08:03 GMT
Server: Apache
X-Powered-By: PHP/5.3.5 ZendServer/5.0
Set-Cookie: SESSIONID_VULN_SITE=t25put8gliicvqf62u3ctgjm21; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html
```

HTTP Response Header – Telnet

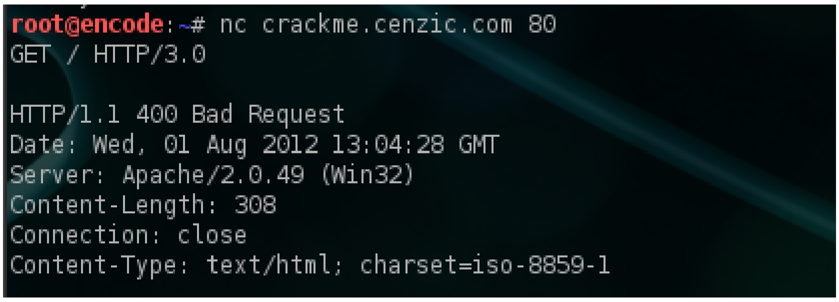
Another way is while we are performing our port scan with Nmap on the remote host to use the command -sV which will obtain as well the type and the version of the web server that is running.For example in the image below we can see from the output that Nmap discovered that the web server is IIS version 6.0.



```
root@encode:~# nmap -sV testaspnet.vulnweb.com

Starting Nmap 6.01 ( http://nmap.org ) at 2012-08-01 11:45 GST
Nmap scan report for testaspnet.vulnweb.com (87.230.29.167)
Host is up (0.15s latency).
rDNS record for 87.230.29.167: wvps87-230-29-167.dedicated.hosteurope.de
Not shown: 992 closed ports
PORT     STATE    SERVICE       VERSION
80/tcp   open     http          Microsoft IIS httpd 6.0
```

Web Server Fingerprinting – Nmap

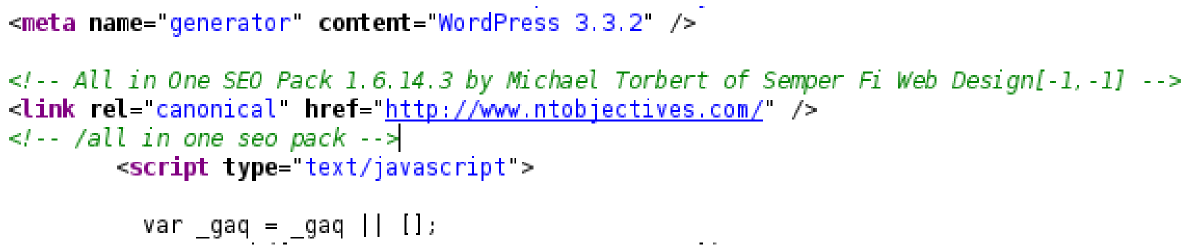
Another method is to send a malformed request to the web server that will cause the web server to produce an error page which will contain in the response header the version of the web server.



```
root@encode:~# nc crackme.cenzic.com 80
GET / HTTP/3.0

HTTP/1.1 400 Bad Request
Date: Wed, 01 Aug 2012 13:04:28 GMT
Server: Apache/2.0.49 (Win32)
Content-Length: 308
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Malformed request to the web server

In some cases the version of the application can be discovered through source code inspection.So it is always a good practice to look there as well.You can see in the following example that we have discovered that the application is WordPress 3.3.2 version by looking at the meta tag.

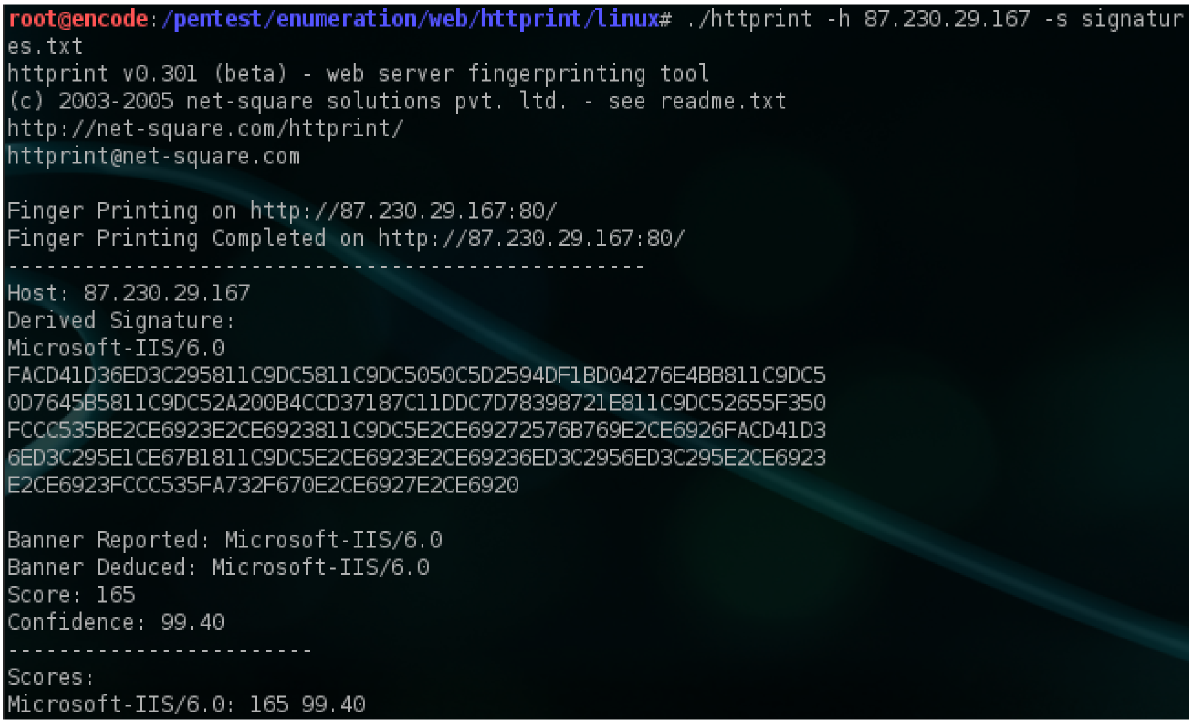


```
<meta name="generator" content="WordPress 3.3.2" />

<!-- All in One SEO Pack 1.6.14.3 by Michael Torbert of Semper Fi Web Design[-1,-1] -->
<link rel="canonical" href="http://www.ntobjectives.com/" />
<!-- /all in one seo pack -->
        <script type="text/javascript">

          var _gaq = _gaq || [];
```

Discovering the version via source code inspection

Automated Fingerprinting

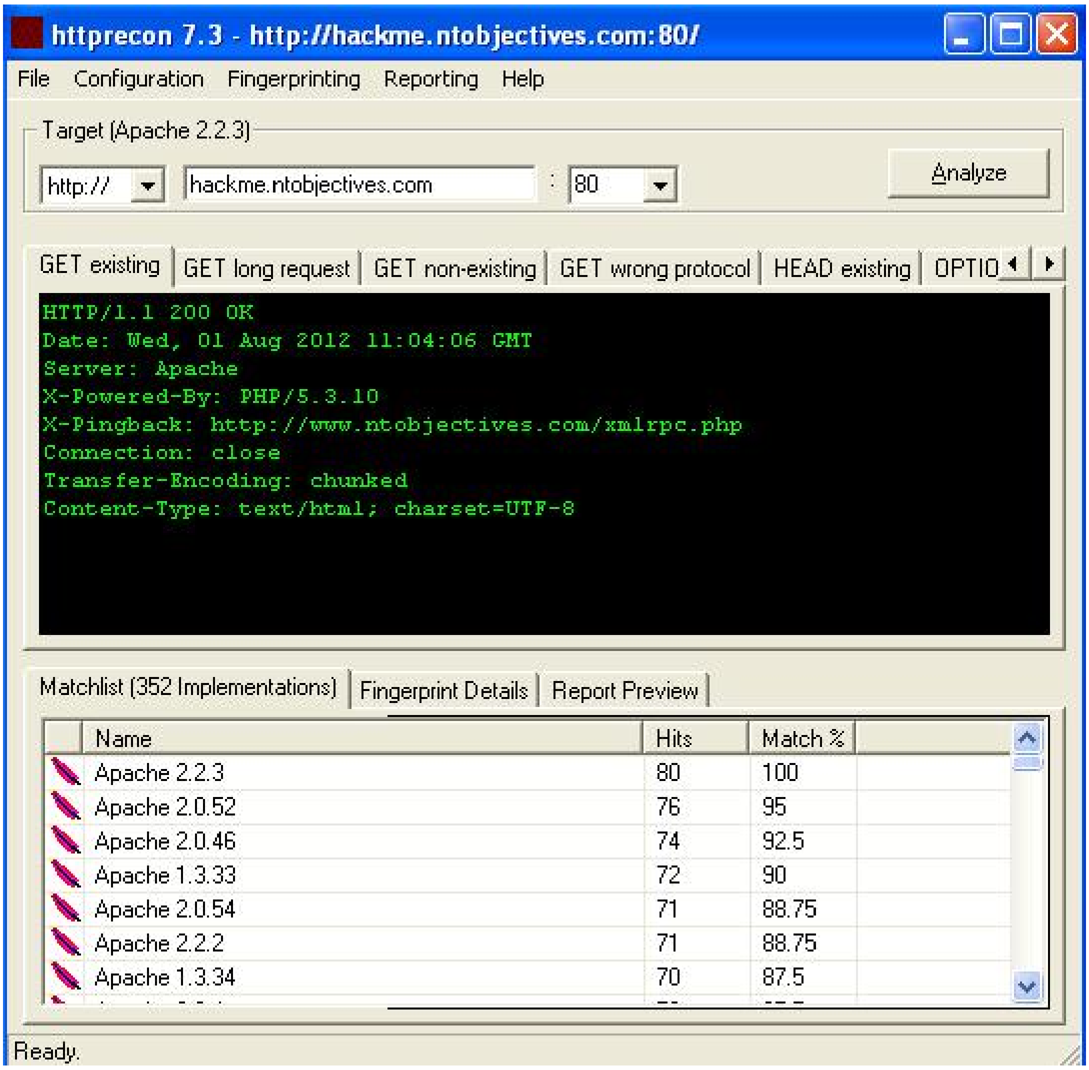
Web application fingerprinting can be done as well with the use of automated tools that have been designed for that purpose.One of the most famous tools is of course the httprint.This tool comes with Backtrack but there is a version as well for windows.In the example below we will use a .txt file that contains signatures of different versions of web servers.So the httprint will try to match the signature of the target web server with the list of known signatures that the signature file contains in order to produce an accurate result.



```
root@encode:/pentest/enumeration/web/httprint/linux# ./httprint -h 87.230.29.167 -s signatur
es.txt
httprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httprint/
httprint@net-square.com

Finger Printing on http://87.230.29.167:80/
Finger Printing Completed on http://87.230.29.167:80/
--------------------------------------------------
Host: 87.230.29.167
Derived Signature:
Microsoft-IIS/6.0
FACD41D36ED3C295811C9DC5811C9DC5050C5D2594DF1BD04276E4BB811C9DC5
0D7645B5811C9DC52A200B4CCD37187C11DDC7D78398721E811C9DC52655F350
FCCC535BE2CE6923E2CE6923811C9DC5E2CE69272576B769E2CE6926FACD41D3
6ED3C295E1CE67B1811C9DC5E2CE6923E2CE69236ED3C2956ED3C295E2CE6923
E2CE6923FCCC535FA732F670E2CE6927E2CE6920

Banner Reported: Microsoft-IIS/6.0
Banner Deduced: Microsoft-IIS/6.0
Score: 165
Confidence: 99.40
------------------------
Scores:
Microsoft-IIS/6.0: 165 99.40
```

httprint usage

Another tool that performs pretty much the same job with the httprint is the httprecon.This tool is for windows platforms and it basically sends different kind of request to the target web server in order to identify its version.The image below is showing that we have a match 100% that host that we have scanned is running Apache 2.2.3 version.



Target (Apache 2.2.3)

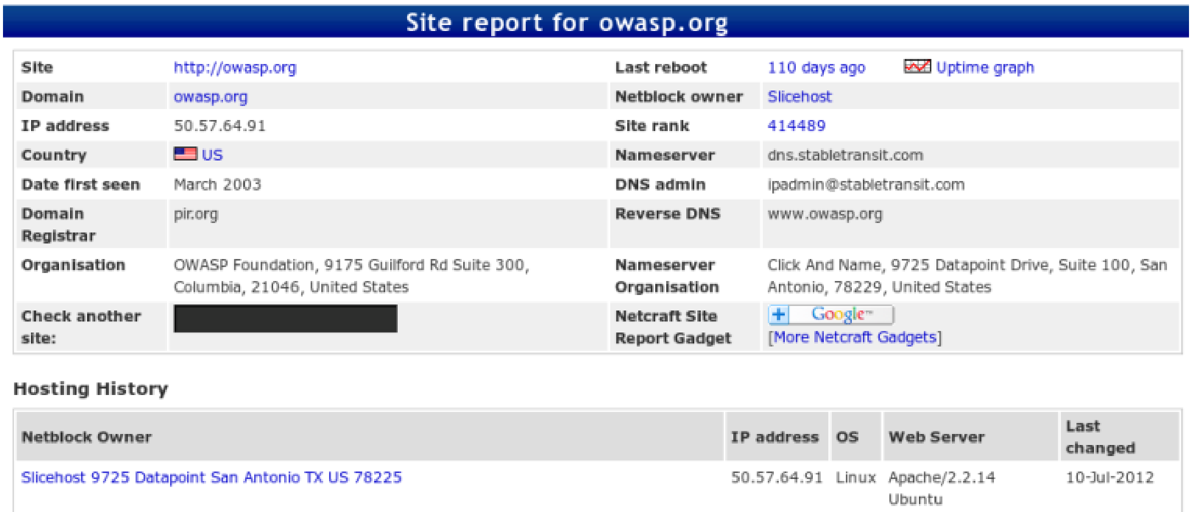
http:// hackme.ntobjectives.com : 80

```
HTTP/1.1 200 OK
Date: Wed, 01 Aug 2012 11:04:06 GMT
Server: Apache
X-Powered-By: PHP/5.3.10
X-Pingback: http://www.ntobjectives.com/xmlrpc.php
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Name	Hits	Match %
Apache 2.2.3	80	100
Apache 2.0.52	76	95
Apache 2.0.46	74	92.5
Apache 1.3.33	72	90
Apache 2.0.54	71	88.75
Apache 2.2.2	71	88.75
Apache 1.3.34	70	87.5

Web Server Fingerprinting – httprecon

Also if we are performing an external web application penetration test then might also want to use an online tool which is called netcraft.This tool can retrieve also the headers of the web server and it can provide us with much more information including the operating system,the nameserver and the netblock owner and much more.



Site report for owasp.org

Site	http://owasp.org	**Last reboot**	110 days ago Uptime graph
Domain	owasp.org	**Netblock owner**	Slicehost
IP address	50.57.64.91	**Site rank**	414489
Country	US	**Nameserver**	dns.stabletransit.com
Date first seen	March 2003	**DNS admin**	ipadmin@stabletransit.com
Domain Registrar	pir.org	**Reverse DNS**	www.owasp.org
Organisation	OWASP Foundation, 9175 Guilford Rd Suite 300, Columbia, 21046, United States	**Nameserver Organisation**	Click And Name, 9725 Datapoint Drive, Suite 100, San Antonio, 78229, United States
Check another site:	[redacted]	**Netcraft Site Report Gadget**	Google [More Netcraft Gadgets]

Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
Slicehost 9725 Datapoint San Antonio TX US 78225	50.57.64.91	Linux	Apache/2.2.14 Ubuntu	10-Jul-2012

Netcraft output

Conclusion

As we saw the web application fingerprinting is an important task for web application penetration tests.It will help us to identify the well-known vulnerabilities that are affecting the web server and the vulnerabilities that are affecting the application that is installed.So we will know what kind of exploits we will need to use in order to start the exploitation.However many web administrators are choosing in nowadays to modify the headers in order to fool any malicious attackers.So as a penetration testers we cannot rely fully on the results that we will get and we will need to use different methods and tools and to execute different commands in order to be sure about the exact version.