

Obrona przed Fingerprinting warstwy aplikacji- tutorial

Niniejszy dokument jest tutorialiem do artykułu "**Czy da się oszukać fingerprinting warstwy aplikacji?**" **Piotra Sobolewskiego**. Nauczysz się z niego, jak się obronić przed rozpoznaniem usług i programów uruchomionych na twoim komputerze.

Spis treści

[Koncepcja](#)

[nmap, amap, vmap](#)

[Serwer FTP](#)

[Serwer WWW \(Apache\)](#)

[I Metoda](#)

[II Metoda](#)

[httpprint, hmap](#)

[Serwer WWW \(Apache\)](#)

Koncepcja

Ćwiczenie wykonamy na jednym komputerze, zabootowanym z hakin9.live. Na porcie 21 należy zainstalować serwer FTP, my będziemy korzystać z vsFTPD wersja 2.0.4 Informacje dotyczące instalacji i konfiguracji znajdziemy [tu](#). Potrzebny też nam będzie na porcie 80 serwer WWW, użyjmy więc Apache'a wersja 2.2.3, którego instalacja opisana jest [tu](#). Z Apache'm zainstalować musimy także dodatkowy moduł: [mod_security](#). Oba serwery potrzebne nam są po to aby móc sprawdzić działanie programów skanujących oraz sprawdzenie możliwości zabezpieczenia się przed nimi. Na początku sprawdzimy proste narzędzia do fingerprintingu takie jak: nmap, amap, vmap, których oszukanie nie będzie czymś trudnym. Następnie zaś spróbujemy zmylić programy: httpprint, hmap.

nmap, amap, vmap

Serwer FTP

[1] Sprawdźmy jaka usługa i program kryje się na porcie 21. Najpierw użyjemy nmapa:

```
$ nmap -sV -p 21 127.0.0.1
```

```
ostapowicz@prak:/home/ostapowicz - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[root@prak ostapowicz]# nmap -sV -p 21 127.0.0.1

Starting Nmap 4.03 ( http://www.insecure.org/nmap/ ) at 2006-08-25 10:49 CEST
Interesting ports on prak.software.com.pl (127.0.0.1):
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.4
Service Info: OS: Unix

Nmap finished: 1 IP address (1 host up) scanned in 0.123 seconds
[root@prak ostapowicz]#
```

Widzimy że nmap wykrył na porcie 21 usługę FTP i poprawnie rozpoznał serwer vsftpd wraz z jego wersją.

[2] To samo zrobimy za pomocą programów: amap i vmap. Zobaczmy jaka jest włączona usługa na porcie 21:

```
$ ./amap 127.0.0.1 21
```

```
ostapowicz@prak:~/amap-5.2 - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[ostapowicz@prak amap-5.2]$ amap 127.0.0.1 21
amap v5.2 (www.thc.org/thc-amap) started at 2006-08-25 12:40:57 - MAPPING mode

Protocol on 127.0.0.1:21/tcp matches ftp

Unidentified ports: none.

amap v5.2 finished at 2006-08-25 12:40:57
[ostapowicz@prak amap-5.2]$
```

amap wykrył uruchomioną usługę FTP.

[3] Kiedy już wiemy, jaka to usługa, możemy uruchomić vmapa, żeby rozpoznał wersję demona:

```
$ ./vmap -P 21 127.0.0.1 ftp
```

```
ostapowicz@prak:/home/ostapowicz/vmap-0.6 - Powłoka - Konsola
Sesja Edycja Widok Zakładki Ustawienia Pomoc
[root@prak vmap-0.6]# ./vmap -P 21 127.0.0.1 ftp
Banner says: 220 (vsFTPd 2.0.4)
Fingerprinting...
Remote Daemon guess: vsftpd-1.1 with 98.90%.
2nd guess: vsFTPd-1.1.0 with 98.90%.
[root@prak vmap-0.6]#
```

vmap rozpoznał po banerze że jest uruchomiony demon vsFTPd 2.0.4. Jednak po serii testów stwierdził że może to też być vsFTPd 1.1 czy też vsFTPd 1.1.0.

[4] Oszukamy teraz te programy, zrobimy to przez podmianę banera powitalnego. Listę znanych nmapowi banerów znajdziemy w pliku konfiguracyjnym nmap-service-probes (na przykład `/usr/share/nmap/nmap-service-probes`). Wśród wielu znajdujących się tam banerów serwerów FTP znajdujemy na przykład taki: *VxWorks (5.4.2) FTP server ready*. Aby nakazać serwerowi vsftpd przedstawianie się takim banerem, musimy do jego pliku konfiguracyjnego (`/etc/vsftpd.conf` lub `/etc/vsftpd/vsftpd.conf`) dopisać linijkę:

```
ftpd_banner=VxWorks (5.4.2) FTP server ready
```

[5] Zrestartujemy serwer ftp (`/etc/init.d`):

```
$ vsftpd restart
```

[6] Sprawdzamy czy nmap dał się oszukać. W tym celu wydajemy polecenie:

```
$ nmap -sV -p 21 127.0.0.1
```

```
ostapowicz@praktykant2:~ - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[ostapowicz@praktykant2 ~]$ nmap -sV -p 21 127.0.0.1

Starting Nmap 4.03 ( http://www.insecure.org/nmap/ ) at 2006-08-30 09:16 CEST
Interesting ports on praktykant2.software.com.pl (127.0.0.1):
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      VxWorks ftpd 5.4.2
Service Info: OS: VxWorks

Nmap finished: 1 IP address (1 host up) scanned in 0.216 seconds
[ostapowicz@praktykant2 ~]$
```

Widzimy że nmap rozpoznał nasz serwer ftp jako VxWorks (5.4.2), pomylił się :)

[7] Sprawdzamy czy vmap dał się oszukać:

```
$ ./vmap -P 21 127.0.0.1 ftp
```

```
ostapowicz@praktykant2:~/vmap-0.6 - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[ostapowicz@praktykant2 vmap-0.6]$ ./vmap -p 21 127.0.0.1 ftp
Banner says: 220 VxWorks (5.4.2) FTP server ready
Fingerprinting...
Remote Daemon guess: vsftpd-1.1 with 98.90%.
2nd guess: vsFTPD-1.1.0 with 98.90%.
[ostapowicz@praktykant2 vmap-0.6]$
```

vmap także dał się zmylić.

Serwer WWW (Apache)

[1] Sprawdźmy jaka usługa i program kryje się na porcie 80. Najpierw użyjemy nmapa:

```
$ nmap -sV -p 80 127.0.0.1
```

```
ostapowicz@prak:~ - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[ostapowicz@prak ~]$ nmap -sV -p 80 127.0.0.1

Starting Nmap 4.03 ( http://www.insecure.org/nmap/ ) at 2006-08-30 08:29 CEST
Interesting ports on prak.software.com.pl (127.0.0.1):
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.3 ((Unix))

Nmap finished: 1 IP address (1 host up) scanned in 6.149 seconds
[ostapowicz@prak ~]$
```

Widzimy że nmap wykrył na porcie 80 usługę HTTP i poprawnie rozpoznał serwer Apache wraz z jego wersją.

[2] To samo zrobimy za pomocą programów: amap i vmap. Zobaczmy jaka jest włączona usługa na porcie:

```
$ ./amap 127.0.0.1 80
```

```
ostapowicz@prak:~/amap-5.2 - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[ostapowicz@prak amap-5.2]$ ./amap 127.0.0.1 80
amap v5.2 (www.thc.org/thc-amap) started at 2006-08-30 08:31:20 - MAPPING mode

Protocol on 127.0.0.1:80/tcp matches http
Protocol on 127.0.0.1:80/tcp matches http-apache-2
Protocol on 127.0.0.1:80/tcp matches webmin

Unidentified ports: none.

amap v5.2 finished at 2006-08-30 08:31:26
[ostapowicz@prak amap-5.2]$
```

amap wykrył uruchomioną usługę HTTP.

[3] Kiedy już wiemy, jaka to usługa, możemy uruchomić vmap, żeby rozpoznać wersję demona:

```
$ ./vmap -P 80 127.0.0.1 http
```

```
ostapowicz@prak:~/vmap-0.6 - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc
[ostapowicz@prak vmap-0.6]$ ./vmap -P 80 127.0.0.1 http
Banner says: Apache/2.2.3 (Unix)
Fingerprinting...
Remote Daemon guess: .Microsoft-ISS-6.0.swp with 78.33%.
[ostapowicz@prak vmap-0.6]$
```

vmap rozpoznał po banerze że jest uruchomiony demon Apache 2.2.3.

Metoda I

[4] Jak widać, wcześniej z serwerem FTP poszło łatwo. Trudniej jest zmusić Apache, żeby przedstawiał się jako IIS. Jedyne co można zrobić, to nakazać Apaczowi, żeby nie podawał swojej wersji. W tym celu w pliku konfiguracyjnym **httpd.conf**(/etc/httpd/conf/httpd.conf) musimy znaleźć linijkę o treści:

```
ServerSignature On
```

i zmienić ją na:

```
ServerSignature Off
```

Spowoduje to, że na stronach wygenerowanych przez serwer (informacje o błędach itp) nie będzie dodawana stopka z nazwą serwera. Następnie poniżej tej linijki dopisujemy:

```
ServerTokens Prod
```

To spowoduje, że Apache w banerze nie będzie podawał numeru wersji.

[5] Sprawdzamy czy nmap dał się oszukać. W tym celu wydajemy polecenie:

```
$ nmap -sV -p 80 127.0.0.1
```

```
ostapowicz@prak:~/vmap-0.6 - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[ostapowicz@prak vmap-0.6]$ nmap -sV -p 80 127.0.0.1

Starting Nmap 4.03 ( http://www.insecure.org/nmap/ ) at 2006-08-30 08:40 CEST
Interesting ports on prak.software.com.pl (127.0.0.1):
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd

Nmap finished: 1 IP address (1 host up) scanned in 6.145 seconds
[ostapowicz@prak vmap-0.6]$
```

Widzimy że nmap rozpoznał nasz serwer WWW jako Apache, jednak nie podał już jego wersji.

[6] Sprawdzamy czy vmap dał się oszukać:

```
$ ./vmap -p 80 127.0.0.1 http
```

```
ostapowicz@prak:~/vmap-0.6 - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[ostapowicz@prak vmap-0.6]$ ./vmap -P 80 127.0.0.1 http
Banner says: Apache
Fingerprinting...
Remote Daemon guess: .Microsoft-ISS-6.0.swp with 78.33%.
[ostapowicz@prak vmap-0.6]$
```

vmap zachował się podobnie jak nmap.

Metoda II

[7] Istnieje do Apache moduł **mod_security**, który wśród wielu funkcjonalności posiada możliwość zmiany banera. Aby to zrobić, trzeba do pliku konfiguracyjnego **httpd.conf** dopisać:

```
<IfModule mod_security.c>

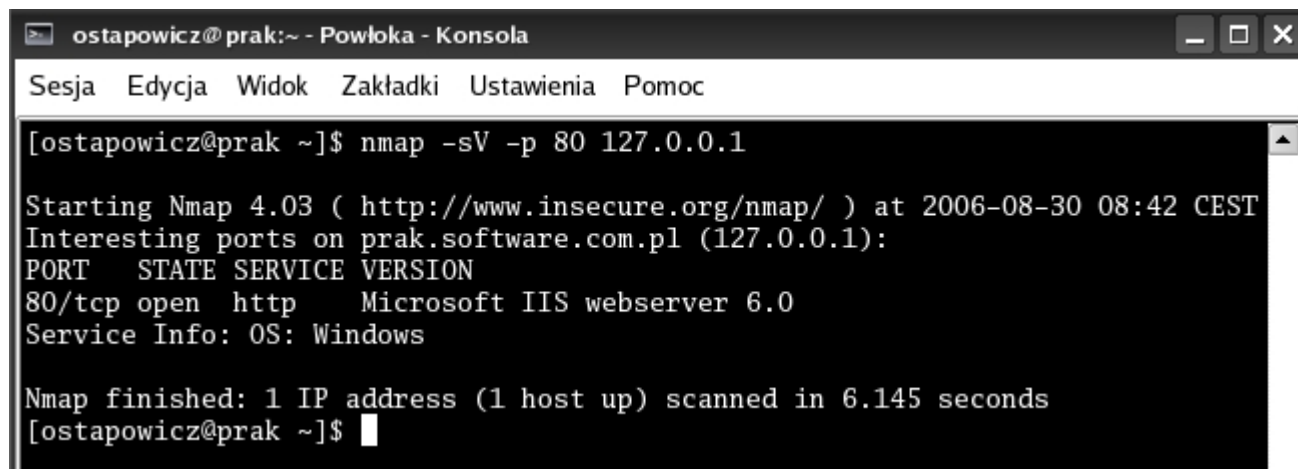
    SecFilterEngine On

    SecServerSignature "Microsoft-IIS/6.0"

</IfModule>
```

[8] Zobaczymy co nmap nam teraz powie:

```
$ nmap -sV -p 80 127.0.0.1
```

A screenshot of a terminal window titled "ostapowicz@prak:~ - Powłoka - Konsola". The terminal shows the command "nmap -sV -p 80 127.0.0.1" being executed. The output indicates that Nmap 4.03 is starting at 2006-08-30 08:42 CEST. It identifies an interesting port on 127.0.0.1: port 80/tcp is open and running the http service, which is Microsoft IIS webserver 6.0. The service info is OS: Windows. The scan finished in 6.145 seconds.

```
ostapowicz@prak:~ - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[ostapowicz@prak ~]$ nmap -sV -p 80 127.0.0.1

Starting Nmap 4.03 ( http://www.insecure.org/nmap/ ) at 2006-08-30 08:42 CEST
Interesting ports on prak.software.com.pl (127.0.0.1):
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS webserver 6.0
Service Info: OS: Windows

Nmap finished: 1 IP address (1 host up) scanned in 6.145 seconds
[ostapowicz@prak ~]$
```

Jak widać nmap błędnie wykrył naszego demona.

httpprint, hmap

Serwer WWW (Apache)

[1] httpprint jest naprawdę poważnym narzędziem do rozpoznawania wersji serwera WWW. Aby zeskanować nasz serwer używamy go tak:

```
$ ./httpprint -h 127.0.0.1:80 -s signatures.txt -P0
```



```
ostapowicz@prak:/home/ostapowicz/httpprint_301/linux - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[root@prak linux]# ./httpprint -h 127.0.0.1:80 -s signatures.txt -P0
httpprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httpprint/
httpprint@net-square.com

Finger Printing on http://127.0.0.1:80/
Finger Printing Completed on http://127.0.0.1:80/
-----
Host: 127.0.0.1
Derived Signature:
Apache/2.2.3 (Unix)
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C11DDC7D7811C9DC5811C9DC58A91CF57
FCCC535B6ED3C295FCCC535B811C9DC5E2CE6927050C5D336ED3C2959E431BC8
6ED3C295E2CE69262A200B4C6ED3C2956ED3C2956ED3C2956ED3C295E2CE6923
E2CE69236ED3C295811C9DC5E2CE6927E2CE6923

Banner Reported: Apache/2.2.3 (Unix)
Banner Deduced: Apache/2.0.x
Score: 140
Confidence: 84.34
-----
Scores:
Apache/2.0.x: 140 84.34
```

httpprint poprawnie rozpoznał serwer Apache wraz z jego wersją.

[2] To samo zrobimy za pomocą programu hmap, którego zasada działania jest bardzo podobna do httpprint'a:

```
$ python hmap.py -v -c 10 127.0.0.1:80
```

```
ostapowicz@prak:/home/ostapowicz/hmap - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[root@prak hmap]# python hmap.py -c 20 http://127.0.0.1:80
gathering data from: http://127.0.0.1:80

                                matches : mismatches : unknowns
Apache/2.0.40 (Red Hat 8.0)      110 : 4 : 9
Apache/2.0.44 (Win32)          109 : 5 : 9
IBM_HTTP_Server/2.0.42 (Win32) 108 : 6 : 9
Apache/1.3.9 (Win32)            107 : 8 : 8
Apache/1.3.12 (Win32)          107 : 8 : 8
Apache/1.3.14 (Win32)          107 : 8 : 8
Apache/1.3.17 (Win32)          107 : 8 : 8
Apache/1.3.22 (Win32)          107 : 8 : 8
Apache/1.3.27 (Red Hat 8.0)     90 : 25 : 8
Apache/1.3.23 (RedHat Linux 7.3) 89 : 26 : 8
Apache/1.3.26 (Solaris 8)      88 : 27 : 8
Apache/1.3.27 (FreeBSD 5.0)     87 : 28 : 8
Apache 1.3.27 (FreeBSD 4.7)     87 : 28 : 8
Apache/1.3.27 (Mac 10.1.5)     86 : 29 : 8
Apache/1.3.27 (Mac 10.2.4)     86 : 29 : 8
Apache/1.3.26_3 (FreeBSD 4.6.2-RELEASE) 73 : 40 : 10
NCSA/1.3 (Ultrix 4.4)          59 : 53 : 11
Microsoft-IIS/5.0 (Win32)      53 : 62 : 8
HP-Web-Server-2.00.1454 (Solaris 8) 41 : 68 : 14
JigSaw 2.2.2 (Solaris 8)       40 : 73 : 10
[root@prak hmap]#
```

hmap wykrył uruchomionego demona.

[3] Żeby zmylić oba programy dobrym pomysłem będzie użycie modułu **mod_setenvif**. Trzeba po prostu do pliku konfiguracyjnego **httpd.conf** dopisać:

```
SetEnvIf Request_Method . BR_http=y

SetEnvIf Request_Method . BR_get=y

SetEnvIf Request_Protocol HTTP/1\.* !BR_http

SetEnvIf Request_Protocol HTTP/1\.1$ !BR_http

SetEnvIf Request_Method GET !BR_get

SetEnvIf BR_http y BadRequest=y

SetEnvIf BR_get y BadRequest=y
```

```
<Directory />

    Options FollowSymLinks

    AllowOverride None

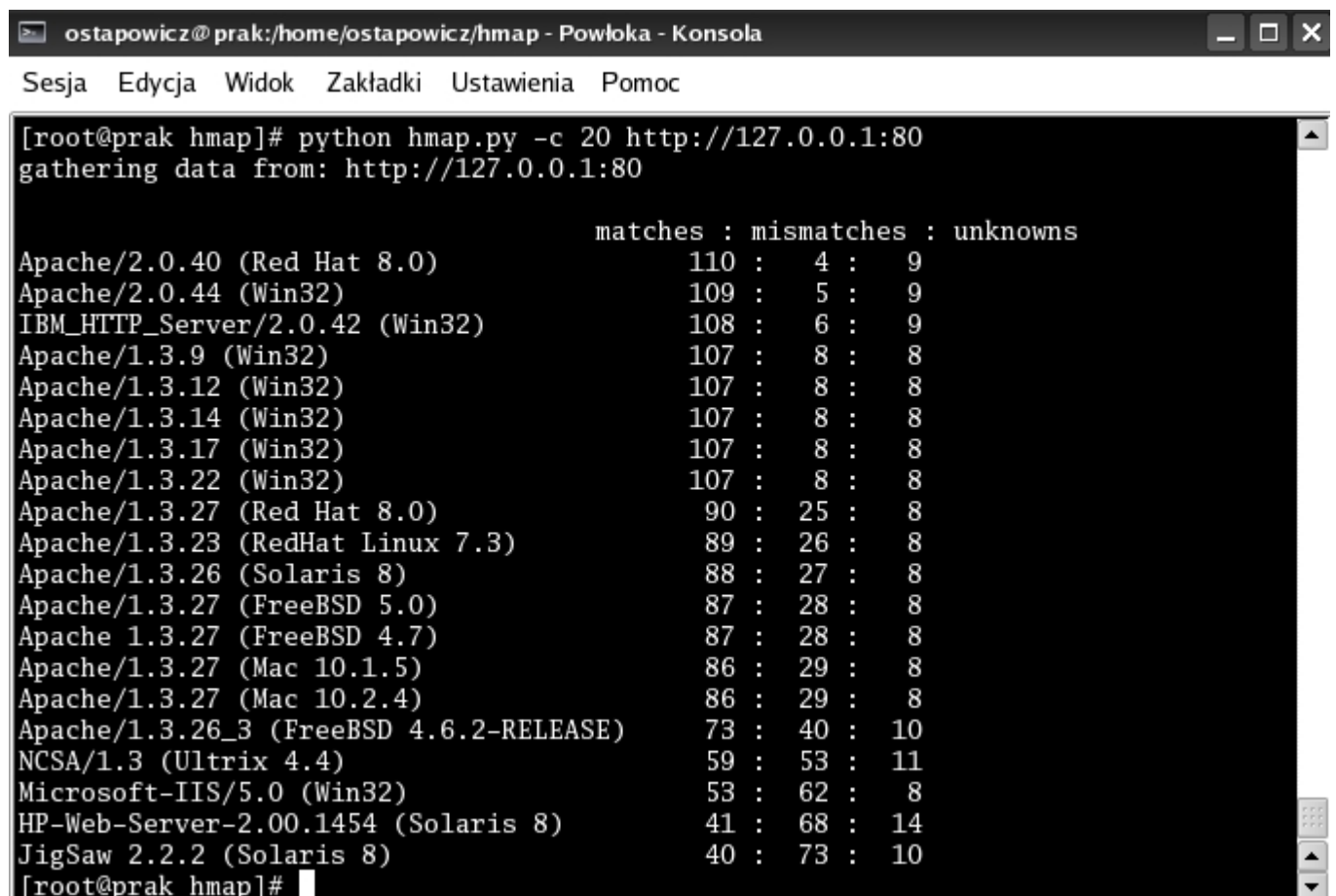
    Order Deny,Allow

    Deny from env=BadRequest

</Directory>
```

[4] Najpierw sprawdźmy, co o tak skonfigurowanym serwerze powie hmap:

```
$ python hmap.py -v -c 20 http://127.0.0.1:80
```



```
ostapowicz@prak:/home/ostapowicz/hmap - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

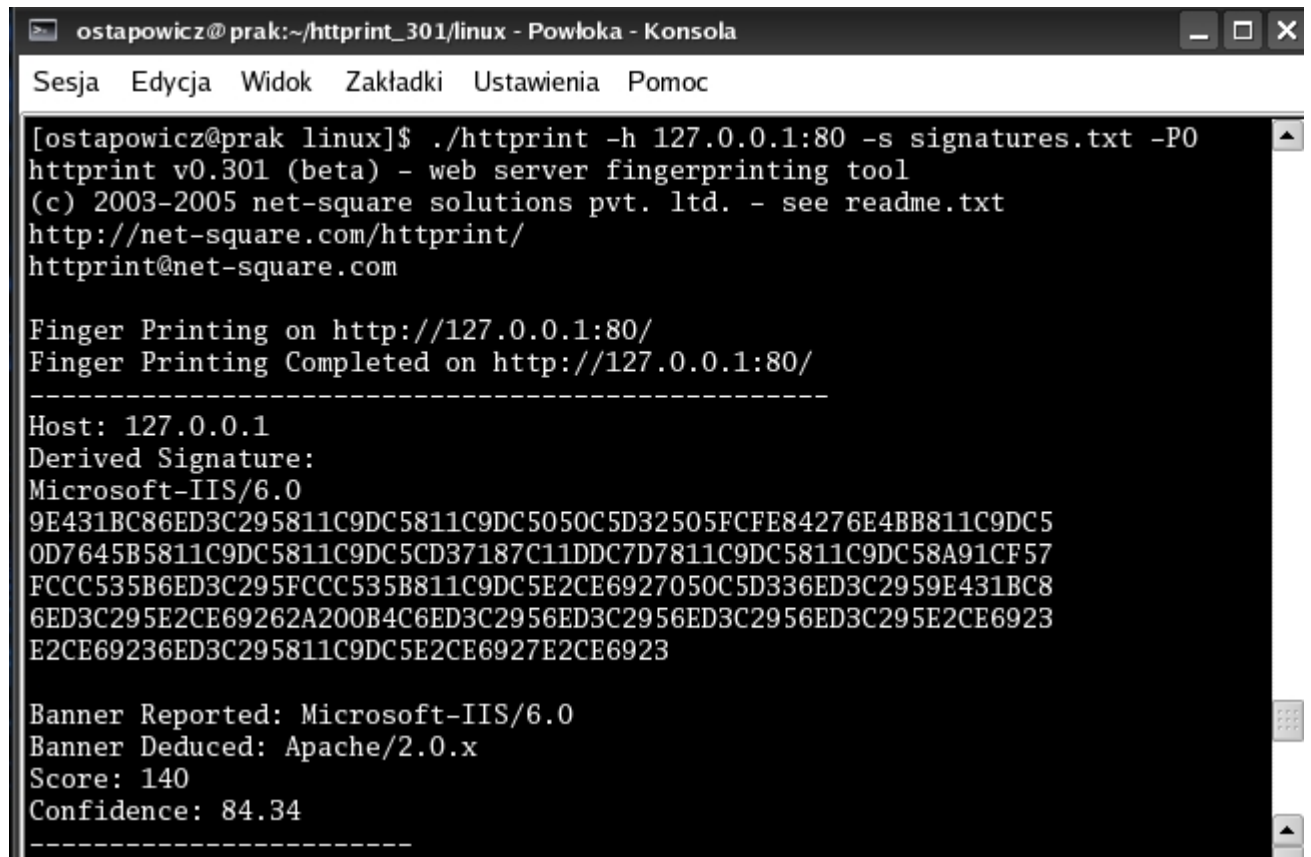
[root@prak hmap]# python hmap.py -c 20 http://127.0.0.1:80
gathering data from: http://127.0.0.1:80

                                matches : mismatches : unknowns
Apache/2.0.40 (Red Hat 8.0)      110 : 4 : 9
Apache/2.0.44 (Win32)           109 : 5 : 9
IBM_HTTP_Server/2.0.42 (Win32)  108 : 6 : 9
Apache/1.3.9 (Win32)            107 : 8 : 8
Apache/1.3.12 (Win32)           107 : 8 : 8
Apache/1.3.14 (Win32)           107 : 8 : 8
Apache/1.3.17 (Win32)           107 : 8 : 8
Apache/1.3.22 (Win32)           107 : 8 : 8
Apache/1.3.27 (Red Hat 8.0)      90 : 25 : 8
Apache/1.3.23 (RedHat Linux 7.3) 89 : 26 : 8
Apache/1.3.26 (Solaris 8)        88 : 27 : 8
Apache/1.3.27 (FreeBSD 5.0)      87 : 28 : 8
Apache 1.3.27 (FreeBSD 4.7)      87 : 28 : 8
Apache/1.3.27 (Mac 10.1.5)       86 : 29 : 8
Apache/1.3.27 (Mac 10.2.4)       86 : 29 : 8
Apache/1.3.26_3 (FreeBSD 4.6.2-RELEASE) 73 : 40 : 10
NCSA/1.3 (Ultrix 4.4)           59 : 53 : 11
Microsoft-IIS/5.0 (Win32)       53 : 62 : 8
HP-Web-Server-2.00.1454 (Solaris 8) 41 : 68 : 14
JigSaw 2.2.2 (Solaris 8)        40 : 73 : 10
[root@prak hmap]#
```

Jak widać, hmap jest znacznie mniej pewien otrzymanych wyników. Nasz cel – ukrycie tożsamości serwera – osiągnęliśmy więc tylko połowicznie.

[5]Zobaczmy, czy lepiej pójdzie nam z httpprint'em:

```
$ ./httpprint -h 127.0.0.1:80 -s signatures.txt -P0
```

A screenshot of a terminal window titled "ostapowicz@prak:~/httpprint_301/linux - Powłoka - Konsola". The window has a menu bar with "Sesja", "Edycja", "Widok", "Zakładki", "Ustawienia", and "Pomoc". The terminal shows the execution of the command `./httpprint -h 127.0.0.1:80 -s signatures.txt -P0`. The output includes the tool's version (v0.301 beta), copyright information (© 2003-2005 net-square solutions pvt. ltd.), and the URL `http://net-square.com/httpprint/`. It then reports the fingerprinting process on `http://127.0.0.1:80/`, identifying the host as `127.0.0.1` and the derived signature as `Microsoft-IIS/6.0`. A long hexadecimal string follows, representing the derived signature. At the bottom, it reports the banner as `Microsoft-IIS/6.0`, deduced as `Apache/2.0.x`, with a score of 140 and a confidence of 84.34.

```
ostapowicz@prak:~/httpprint_301/linux - Powłoka - Konsola
Sesja  Edycja  Widok  Zakładki  Ustawienia  Pomoc

[ostapowicz@prak linux]$ ./httpprint -h 127.0.0.1:80 -s signatures.txt -P0
httpprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httpprint/
httpprint@net-square.com

Finger Printing on http://127.0.0.1:80/
Finger Printing Completed on http://127.0.0.1:80/
-----
Host: 127.0.0.1
Derived Signature:
Microsoft-IIS/6.0
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC5
OD7645B5811C9DC5811C9DC5CD37187C11DDC7D7811C9DC5811C9DC58A91CF57
FCCC535B6ED3C295FCCC535B811C9DC5E2CE6927050C5D336ED3C2959E431BC8
6ED3C295E2CE69262A200B4C6ED3C2956ED3C2956ED3C2956ED3C295E2CE6923
E2CE69236ED3C295811C9DC5E2CE6927E2CE6923

Banner Reported: Microsoft-IIS/6.0
Banner Deduced: Apache/2.0.x
Score: 140
Confidence: 84.34
-----
```

Jak widać, udało nam się go oszukać!

SUKCES !!!