

Step -1 : detection of brute-force using grep 401 and get the ip address(203.0.113.45)

```
(kali㉿kali)-[~]
$ ls
Desktop  Documents  Downloads  Music  OneShot-C  Pictures  practise.sh  Public  Templates  Videos

(kali㉿kali)-[~]
$ cd Downloads

(kali㉿kali)-[~/Downloads]
$ ls
access_tarshasoftsec.log  nsu-cec

(kali㉿kali)-[~/Downloads]
$ cat -n access_tarshasoftsec.log | grep "401"
1 203.0.113.45 - - [06/Nov/2025:14:15:00 +0000] "POST /CRM/login.php HTTP/1.1" 401 160 "https://crm.tarshasoftsec.com/CRM/login.php"
2 203.0.113.45 - - [06/Nov/2025:14:15:01 +0000] "POST /CRM/login.php HTTP/1.1" 401 121 "https://crm.tarshasoftsec.com/CRM/login.php"
3 203.0.113.45 - - [06/Nov/2025:14:15:02 +0000] "POST /CRM/login.php HTTP/1.1" 401 146 "https://crm.tarshasoftsec.com/CRM/login.php"
4 203.0.113.45 - - [06/Nov/2025:14:15:03 +0000] "POST /CRM/login.php HTTP/1.1" 401 219 "https://crm.tarshasoftsec.com/CRM/login.php"
5 203.0.113.45 - - [06/Nov/2025:14:15:04 +0000] "POST /CRM/login.php HTTP/1.1" 401 135 "https://crm.tarshasoftsec.com/CRM/login.php"
6 203.0.113.45 - - [06/Nov/2025:14:15:05 +0000] "POST /CRM/login.php HTTP/1.1" 401 156 "https://crm.tarshasoftsec.com/CRM/login.php"
7 203.0.113.45 - - [06/Nov/2025:14:15:06 +0000] "POST /CRM/login.php HTTP/1.1" 401 167 "https://crm.tarshasoftsec.com/CRM/login.php"
8 203.0.113.45 - - [06/Nov/2025:14:15:07 +0000] "POST /CRM/login.php HTTP/1.1" 401 217 "https://crm.tarshasoftsec.com/CRM/login.php"
9 203.0.113.45 - - [06/Nov/2025:14:15:08 +0000] "POST /CRM/login.php HTTP/1.1" 401 183 "https://crm.tarshasoftsec.com/CRM/login.php"
```

Step-2 : get the verification login status using grep 200 status code

```
(kali㉿kali)-[~/Downloads]
$ cat -n access_tarshasoftsec.log | grep "200"
29 203.0.113.45 - - [06/Nov/2025:14:15:28 +0000] "POST /CRM/login.php HTTP/1.1" 401 200 "https://crm.tarshasoftsec.com/CRM/login.php"
200 203.0.113.45 - - [06/Nov/2025:14:18:19 +0000] "POST /CRM/login.php HTTP/1.1" 401 218 "https://crm.tarshasoftsec.com/CRM/login.php"
242 203.0.113.45 - - [06/Nov/2025:14:19:01 +0000] "POST /CRM/login.php HTTP/1.1" 401 200 "https://crm.tarshasoftsec.com/CRM/login.php"
277 203.0.113.45 - - [06/Nov/2025:14:19:36 +0000] "POST /CRM/login.php HTTP/1.1" 401 200 "https://crm.tarshasoftsec.com/CRM/login.php"
278 203.0.113.45 - - [06/Nov/2025:14:19:37 +0000] "POST /CRM/login.php HTTP/1.1" 401 200 "https://crm.tarshasoftsec.com/CRM/login.php"
317 203.0.113.45 - - [06/Nov/2025:14:20:16 +0000] "POST /CRM/login.php HTTP/1.1" 401 200 "https://crm.tarshasoftsec.com/CRM/login.php"
353 203.0.113.45 - - [06/Nov/2025:14:20:52 +0000] "POST /CRM/login.php HTTP/1.1" 401 200 "https://crm.tarshasoftsec.com/CRM/login.php"
370 203.0.113.45 - - [06/Nov/2025:14:21:09 +0000] "POST /CRM/login.php HTTP/1.1" 401 200 "https://crm.tarshasoftsec.com/CRM/login.php"
396 203.0.113.45 - - [06/Nov/2025:14:21:35 +0000] "POST /CRM/login.php HTTP/1.1" 401 200 "https://crm.tarshasoftsec.com/CRM/login.php"
404 203.0.113.45 - - [06/Nov/2025:14:21:43 +0000] "POST /CRM/login.php HTTP/1.1" 401 200 "https://crm.tarshasoftsec.com/CRM/login.php"
405 203.0.113.45 - - [06/Nov/2025:14:21:44 +0000] "POST /CRM/login.php HTTP/1.1" 401 200 "https://crm.tarshasoftsec.com/CRM/login.php"
531 203.0.113.45 - - [06/Nov/2025:14:23:50 +0000] "POST /CRM/login.php HTTP/1.1" 401 200 "https://crm.tarshasoftsec.com/CRM/login.php"
```

Step-3: get the hacker information using grep whoami

```
(kali@kali)-[~/Downloads]
$ cat access_tarshasoftsec.log | grep "whoami"
203.0.113.45 - - [06/Nov/2025:14:26:22 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 117 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:25 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 85 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:26 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 68 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:27 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 68 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:28 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 83 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:29 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 78 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:30 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 59 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:31 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 110 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:32 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 80 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:33 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 97 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:34 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 72 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:35 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 97 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:36 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 112 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:37 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 65 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:38 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 53 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:39 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 65 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:40 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 115 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:41 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 81 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:42 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 95 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:43 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 113 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:44 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 56 "https://crm.tarshasoftsec.com" "PF-API"
203.0.113.45 - - [06/Nov/2025:14:26:45 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 112 "https://crm.tarshasoftsec.com" "PF-API"
```

Step-4 : history

```
203.0.113.45 - - [06/Nov/2025:14:27:30 +0000] "GET /CRM/admin/exec.php?cmd=whoami HTTP/1.1" 200 55 "https://crm.tarshasoftsec.com" "PF-API"
(kali@kali)-[~/Downloads]
$ history
1 git
2 cd ..
3 ls
4 li
5 git
6 cd ..
7 ls
8 li
9 fuck cse
10 sudo vi /etc/apt/sources.list
11 exit
12 ls
13 sudo
14 sudo apt update
15 sudo apt full-upgrade
16 sudo apt install btop nala neofetch
17 sudo apt install btop nala
18 sudo apt install fetch
19 sudo apt install fastfetch
20 fastfetch
21 btop
22 nala
23 sudo nala full-upgrade
24 history
25 sudo nala full-upgrad
```

```
171 shodanx domain -d northsouth.edu
172 ls
173 cd Downloads
174 ls
175 cat access_tarshasoftsec.log
176 cat access_tarshasoftsec.log | grep "401"
177 cat -n access_tarshasoftsec.log | grep "401"
178 cat -n access_tarshasoftsec.log | grep "401"
179 cat access_tarshasoftsec.log | grep "401"
180 cat -n access_tarshasoftsec.log | grep "401"
181 cat access_tarshasoftsec.log | grep "401" | awk '{print $1}' | sort | uniq -c | sort -nr
182 clear
183 cd ..
184 cd ..
185 cd ..
186 cd ..
187 clear
188 ls
189 cd home
190 ls
191 cd kali
192 ls
193 clear
194 ls
195 cd Downloads
196 ls
197 cat -n access_tarshasoftsec.log | grep "401"
198 cat -n access_tarshasoftsec.log | grep "200"
199 cat access_tarshasoftsec.log | grep "whoami"
(kali@kali)-[~/Downloads]
```