


# 談UDP 放大攻擊

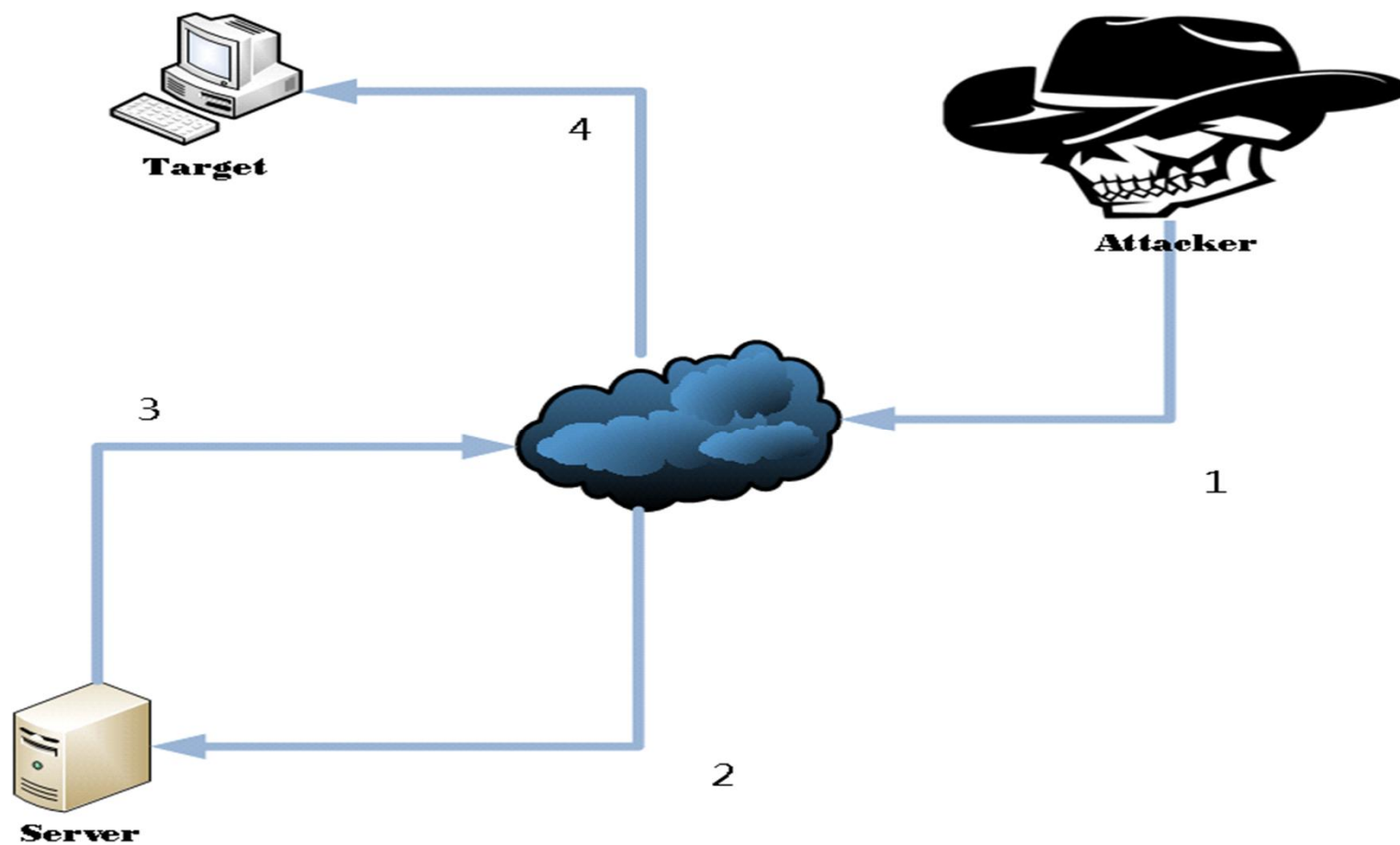
**Jonce kuo**

系統整合、資訊服務的第一選擇



2014/05/21

# 常見的攻擊型態



# 常見的攻擊型態

通訊協定	頻寬放大倍率	具有弱點的指令
DNS	28~54	DNS 遞迴查詢
NTP	556.9	monlist
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	3.8	Quote request
BitTorrent	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange

# 常見的攻擊型態NTP

## ntpd -c monlist SERVERIP

```
root@kali:~# nmap -sU -pU:123 -Pn --script=ntp-monlist 127.127.1.0
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-28 17:12 CST
Nmap scan report for 127.127.1.0
Host is up (0.0002s latency).
PORT      STATE SERVICE
123/udp   open  ntp
ntp-monlist:
  Target is synchronised with 127.127.1.0 (reference clock)
  Alternative Target Interfaces:
    0.0.0.0
  Other Associations (600)
    127.127.1.0 seen 3 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 1257 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 137866 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 2866 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 14 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 8596 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 3853 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 185 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 59 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 9279 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 6058 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 2395 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 3472 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 1678 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 3592 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 7959 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 2206 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 15 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 109 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 27 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 19 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 42 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 8 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 5 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 6 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 37 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 38 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 34 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 1660 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 46 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 42 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 359 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 28 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 1983 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 5 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 184 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 35 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 5 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 96 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 206 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 4 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 5 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 6 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 5 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 147 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 3 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 17007 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 39 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 14 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 9298 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 24 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 6 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 247 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 7 times. last tx was unicast v2 mode 7
    127.127.1.0 seen 50 times. last tx was unicast v2 mode 7
```

# 常見的攻擊型態Chargen

```
$ telnet localhost chargen
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
"#$$$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij
$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk
%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklm
'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmn
()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno
)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop
*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopq
+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqr
,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrs
-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstu
/0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuv
^]
telnet> quit
Connection closed.
```



# DNS UDP放大攻擊對策

停用DNS Server的遞迴查詢功能

```
options {  
    allow-query-cache { none; };  
    recursion no;  
};
```

僅允許內部網路能來做遞迴查詢: (此例中允許任何IP做查詢，但是只允許192.168.1.0/24，192.168.2.0/24 來做遞迴查詢)

```
acl corpnets { 192.168.1.0/24; 192.168.2.0/24; };  
options {  
    allow-query { any; };  
    allow-recursion { corpnets; };  
};
```

限制查詢的頻率: (此例子中限制為一秒5個查詢，bind 9.8以後支援)

```
rate-limit {  
    responses-per-second 5;  
    window 5;  
};
```

# DNS UDP放大攻擊對策

修改ntpd的設定檔，在Un\*x系列上 預設是在  
/etc/ntp.conf

restrict default kod nomodify notrap nopeer noquery

**restrict -6 default kod nomodify notrap nopeer noquery**

# SNMP UDP放大攻擊對策

**snmp-server community cisco-rlc RO 66**

#此行指令設定唯讀(RO Read Only)的snmp community為cisco-rlc並且指定套用存取列表66

**snmp-server community rlc-cisco RW 77**

#此行指令設定讀寫(RW Read Write)的snmp community為rlc-cisco並且指定套用存取列表77

**access-list 66 permit ip host 172.16.6.100**

**access-list 77 permit ip host 172.16.6.101**

這兩行存取列表 66僅允許172.16.6.100 ，存取列表77僅允許172.16.6.101



# 參考資料

- <http://www.us-cert.gov/ncas/alerts/TA14-017A>
- <http://www.us-cert.gov/ncas/alerts/TA13-088A>
- <http://www.us-cert.gov/ncas/alerts/TA14-013A>
- <http://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/20370-snmpsecurity-20370.html>