B03102082
陳孝思

NA HW2

1. Flamestrike

(a) 在某些大型網路拓璞下為了避免單一 switch 故障導致網路停擺，會使用多個相同 switch 提供服務，當其中一個 switch 在發送廣播封包時，有時會讓別的 switch 也重複廣播一樣的封包，即使要廣播的對象已收到封包也不會停止廣播，而短時間內不同的 switch 不斷地大量廣播相同封包會耗盡網路資料，此為 Broadcast Storm

Ref:

http://www.netadmin.com.tw/article_content.aspx?sn=1203290001&jump=4

(b) 用 wireshark 過濾廣播封包，找出哪些 switch 在不斷廣播同樣的封包，找出是從那些 switch 中哪些 port 在不斷廣播，關掉那些 port，之後再檢查是否是網路拓璞配置不當還是中毒的關係

Ref: http://www.test104.com/tw/tech/303.html

(c) STP 透過控制哪些 switch 上的 port 能夠使用來建立一個沒有迴圈的網路拓璞，每個 switch 跟 port 根據 STP 的演算法會有不同的狀態，這些狀態會隨著時間或網路流通的狀況而改變

Ref:

http://www.netadmin.com.tw/article_content.aspx?sn=1208290002&jump=5

2. MAC Pro

(a) 先送 ARP REQUEST

ARP, 10.0.0.1/24 -> 10.0.0.2/24, fa:ce:b0:00:00:0c -> ff:ff:ff:ff:ff:ff

ARP, 10.0.0.2/24 -> 10.0.0.1/24, de:ad:be:ee:ee:ef -> fa:ce:b0:00:00:0c

ICMP, 10.0.0.1/24 -> 10.0.0.2/24, fa:ce:b0:00:00:0c -> de:ad:be:ee:ee:ef

ICMP, 10.0.0.2/24 -> 10.0.0.1/24, de:ad:be:ee:ee:ef -> fa:ce:b0:00:00:0c

Ref: https://www.netometer.com/qa/arp.html - A9

(b)

VLAN	MAC Address	Type	Port
1	fa:ce:b0:00:00:0c	Dynamic	Interface 1
2	de:ad:be:ee:ee:ef	Dynamic	Interface 2

Ref:
http://www.pearsonitcertification.com/articles/article.aspx?p=2339639&seqNum=3

(c)

ARP, 10.0.0.1/24 -> 10.0.0.254, fa:ce:b0:00:00:0c -> ff:ff:ff:ff:ff:ff

ICMP, 10.0.0.1/24 ->140.112.30.28, fa:ce:b0:00:00:0c -> ba:aa:aa:ad:c0:de

Ref: https://networkengineering.stackexchange.com/questions/6851/arp-request-outside-of-lan-target-machine-or-router-response

(d)

(1) 找出 gateway 的 IP

(2) 大量且不斷地廣播 Gratuitous ARP，source and destination IP 是 gateway 的 IP，source MAC address 是 Sonic 的 Mac Address，讓 subnet 內要連外的封包先送到 sonic

(3) 成功將 subnet 內要對外的封包全部導到 Sonic 後，再轉傳給 gateway，假裝網路連線正常

(4) 用 Wireshark 搜尋封包，找出使用 telnet 協定的封包，因為 telnet 沒有加密，密碼會明文顯示在封包裡

Ref: https://learningnetwork.cisco.com/thread/97335
https://security.stackexchange.com/questions/164756/arp-spoofing-why-does-the-attacker-constantly-send-arp-replys

3. Let’s IPv6

(a) ICMPv6

(b) ff02::2

(c) 625c83a8+8cfe40ed58a81e9ca8dcf40a47cdbe8a

```
b03102082@oasis2 [~] ncat -6 fe80::5054:ff:fe73:17dc%net0 9453
You have successfully connect me using IPv6!
Please write the follow message in your homework:
625c83a8+8cfe40ed58a81e9ca8dcf40a47cdbe8a
```

Ref: B05902002 李栢淵