# Exercise 7-1

1. host -t ns megacorpone.com | cut -d " " -f 4
2. 參見本章ppt: "自動取得每個nameserver的zone transfer資料“
3. dnsrecon -d megacorpone.com -t axfr

# Exercise 7-2

1.

nmap -sn -v -oG nmapped.txt 10.0.2.1-20

grep Up nmapped.txt | cut -d " " -f2

2.

#!/bin/bash

for p in $(grep Up nmapped.txt | cut -d " " -f2);

do

echo '---------------'

sudo nmap -p 80 -O $p

done

3.

nmap 10.0.2.7 --script=smb-os-discovery

4.

啟動wireshark, 選擇監聽eth0

執行 nmap –sT 10.0.2.7 (nmap TCP connect scan)

(TCP Scan): 在wireshark中檢視[SYN], [SYN, ACK], 和[ACK]封包 (open port)

(TCP Scan): 在wireshark中檢視[SYN], [RST, ACK]封包 (close port)

(FIN Scan): 在wireshark中檢視[FIN]

(FIN Scan): 在wireshark中檢視[FIN], [RST, ACK]封包 (close port)

(XMAS Scan):在wireshark中檢視[FIN, PSH, URG]封包

啟動wireshark, 選擇監聽eth0

執行 nc –zvn 10.0.2.7 21-80 (netcat port scan)

(結果與TCP connect scan類似)

5.

啟動wireshark, 選擇監聽eth0

執行sudo nmap –sS 10.0.2.7

通訊埠掃描器不會費心發送最終的 ACK 來完成三次握手

由於三次握手從未完成，因此資訊不會傳到應用層，因此不會出現在任何應用程式日誌中

SYN 掃描也因此更快、更有效，因為發送和接收的封包更少

# Exercise 7-3

1.

nmap --script=smb-os-discovery -p 139,445 10.0.2.1-20

2.

nmap -v -p 139,445 -script=smb-vuln-ms08-067 --script-args=unsafe=1 10.0.2.1-20