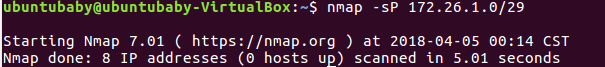
**HW02**

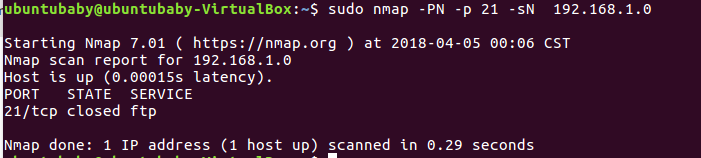
**0516208-黃郁恬**

1.

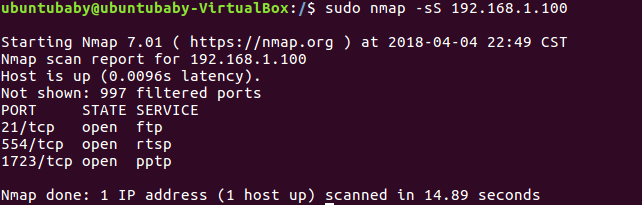
**(a)** **host discovery on the selected domain**

****

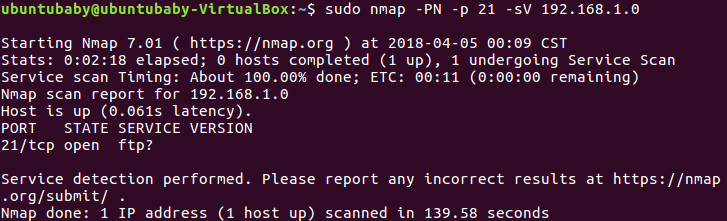
**(b)** **port scanning on a selected host**

****

**(c)** **active stack fingerprinting on the selected host**

****

**(d)** **version scanning on a selected port**

****

2.

**OS-fingerprinting**

The process of learning what OS is running on a particular device. By analyzing certain protocol flags, options, and data in the packets a device sends onto the network, we can make relatively correct guesses about the OS that sent those packets.

**Nmap(nmap-os-fingerprinting) -- active** **stack fingerprinting**

1. Sending packets to the target system
2. Transmitting packets to a remote host and analyzing corresponding replies

**Siphon(osprints.conf) -- passive stack fingerprinting**

1. It does not involve communicating with the host being examined. Based on the sniffer traces of these packets, you can determine the operating system of the remote host.
2. Less accurate than active scanners, cause they have less control over the data they are analyzing.
3. Does not put any traffic on a network

3.

**Nmap-service:**

A registry of port names to their corresponding number and protocol

By using the nmap-services database, Nmap would report those ports probably correspond to a mail server (SMTP), web server (HTTP), and name server (DNS) respectively.

**Nmap-service-probe:**

A file contains the probes that the Nmap service detection system uses during port interrogation to determine what program is listening on a port.

It contains probes for querying various services and match expressions to recognize and parse responses.

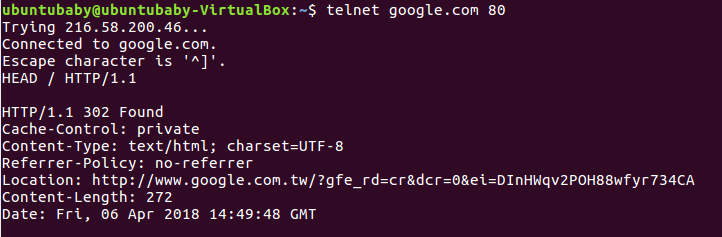
* Nmap-service-probe allows Nmap to give a detailed assessment of what is really running, rather than just what port numbers are open (known by nmap-service).
* Nmap-service-probe is more complex than nmap-services. Cause the benefits of it can be better. Nmap can be taught to actually recognize a company's custom services, rather than simply guess based on nmap-services port registration.
* Information: <https://nmap.org/book/vscan.html>

4.

5.

6.

telnet:



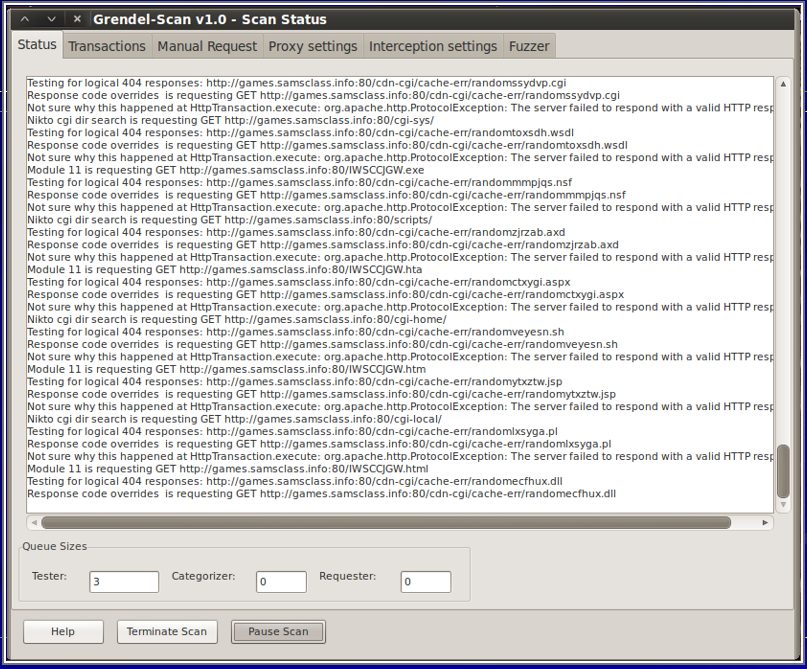
netcat:



Through this screen dump, we see that the result of banner-scan by telnet and netcat are almost the same.

It’s hard to find the way to install grendel, so I found a result from a website and compare it with the result above.

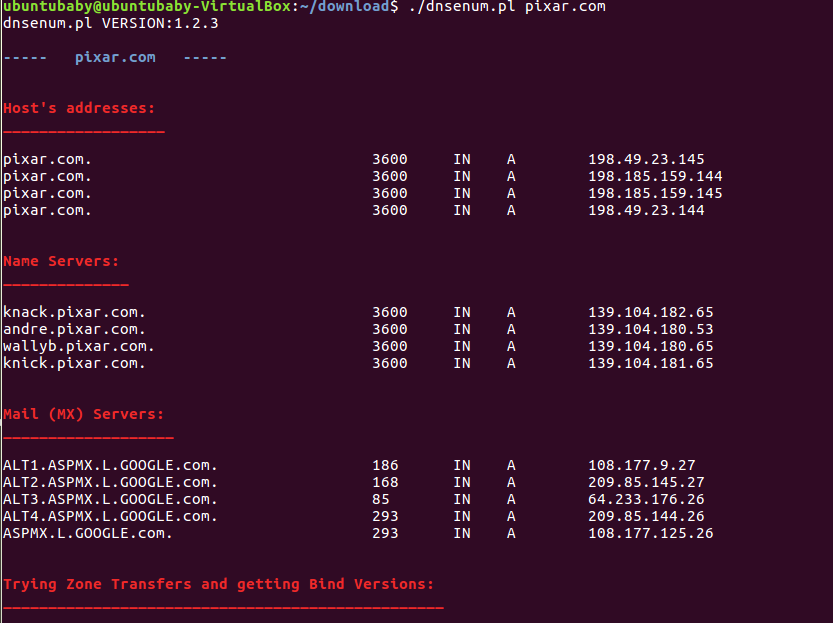
The following is what I found:



* It takes long time to finish banner-scanning
* It’s in backtrack

7.

Servers, IP addresses:



Subdomains: