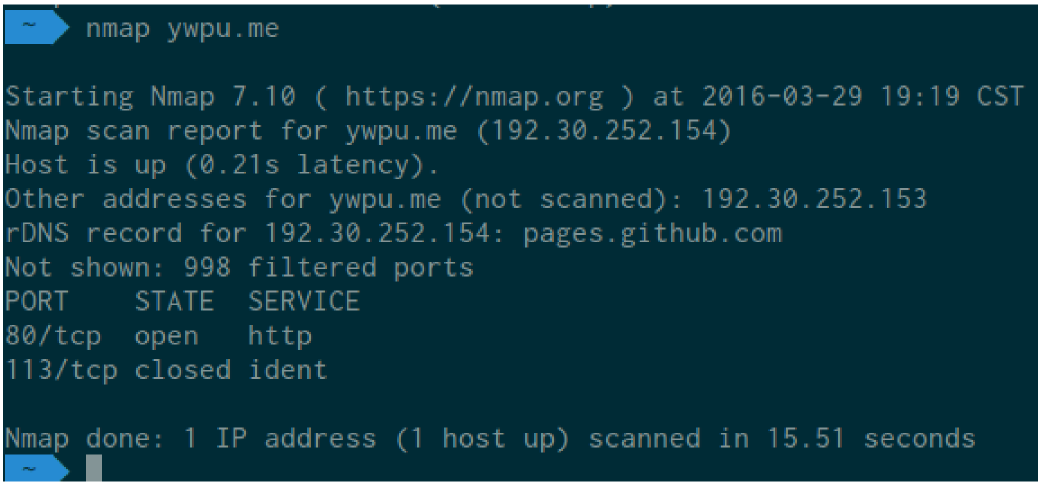
Introduction to Computer Security
Homework 2

0316213 Yu-wen Pwu

1.a. Select a target domain and use Nmap for: host discovery on the selected domain.



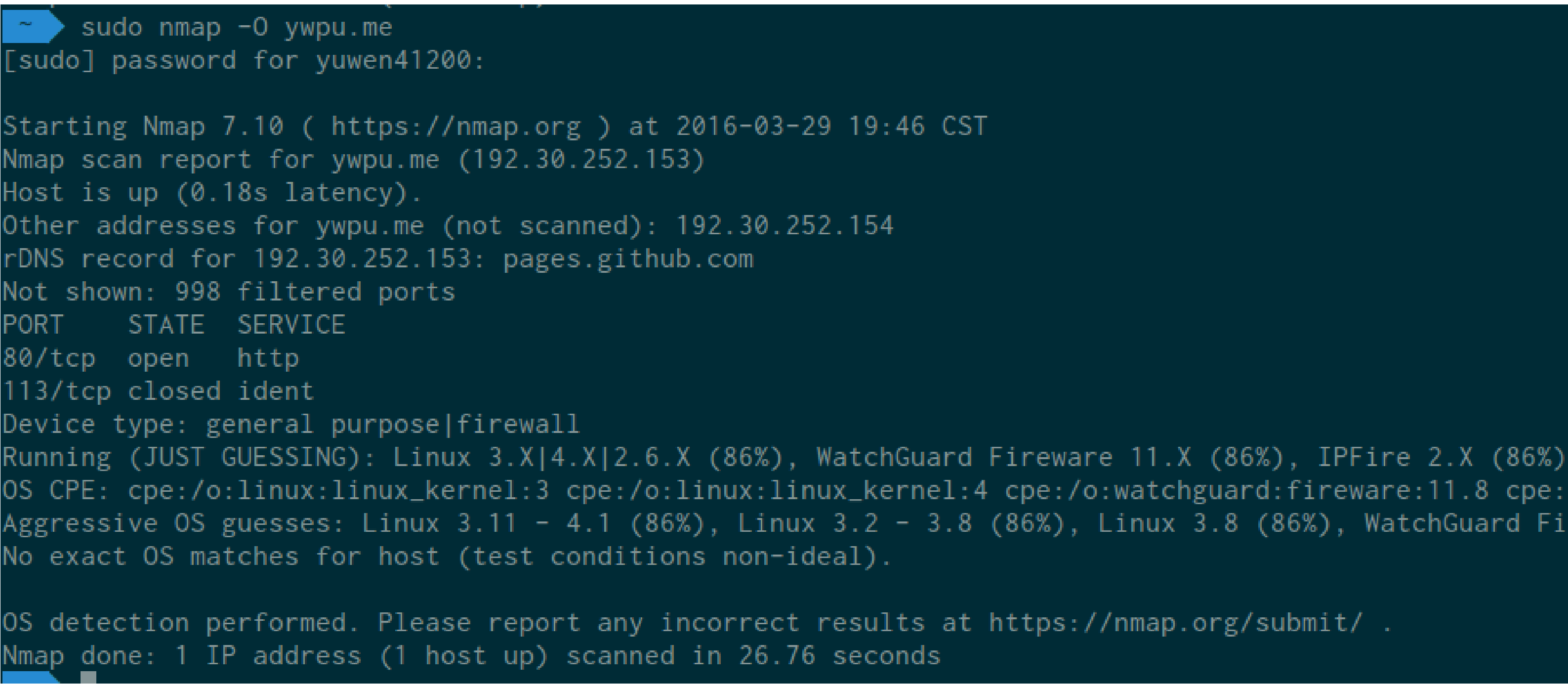
```
~  nmap ywpu.me

Starting Nmap 7.10 ( https://nmap.org ) at 2016-03-29 19:19 CST
Nmap scan report for ywpu.me (192.30.252.154)
Host is up (0.21s latency).
Other addresses for ywpu.me (not scanned): 192.30.252.153
rDNS record for 192.30.252.154: pages.github.com
Not shown: 998 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident

Nmap done: 1 IP address (1 host up) scanned in 15.51 seconds
~
```

→ Its IP is `192.30.252.154` (or `192.30.252.153`), having an alternative domain name `pages.github.com`. It is currently on-line.

1.b. Select a target domain and use Nmap for: port scanning on a selected host.

→ Following the previous question, its port 80 is opened for HTTP, port 113 is accessible (but closed), and there are 998 filtered ports (unreachable due to firewall, etc.)

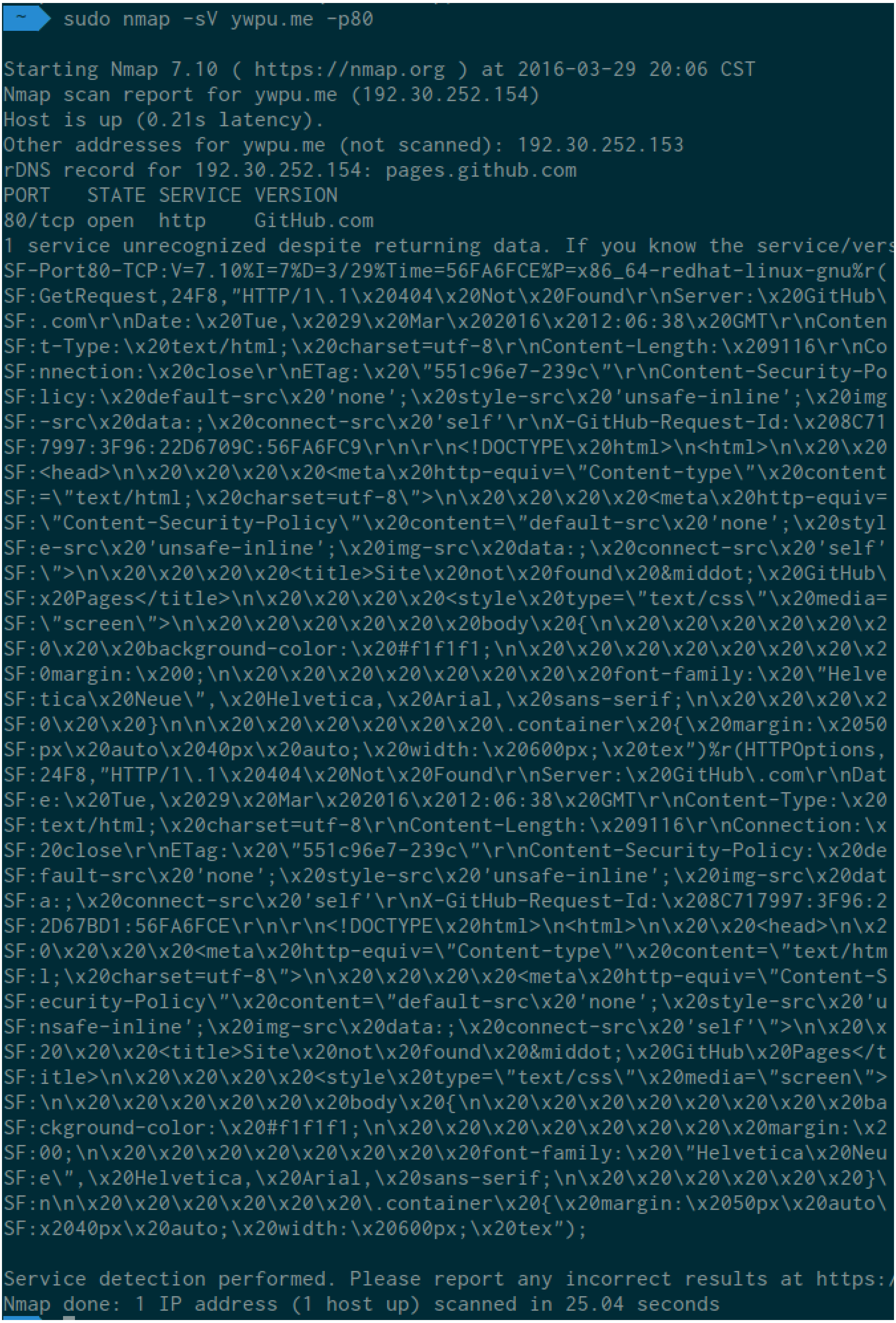
1.c. Select a target domain and use Nmap for: active stack fingerprinting on the selected host.



```
~  sudo nmap -O ywpu.me
[sudo] password for yuwen41200:

Starting Nmap 7.10 ( https://nmap.org ) at 2016-03-29 19:46 CST
Nmap scan report for ywpu.me (192.30.252.153)
Host is up (0.18s latency).
Other addresses for ywpu.me (not scanned): 192.30.252.154
rDNS record for 192.30.252.153: pages.github.com
Not shown: 998 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident
Device type: general purpose|firewall
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (86%), WatchGuard Fireware 11.X (86%), IPFire 2.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:watchguard:fireware:11.8 cpe:
Aggressive OS guesses: Linux 3.11 - 4.1 (86%), Linux 3.2 - 3.8 (86%), Linux 3.8 (86%), WatchGuard Fi
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.76 seconds
```

→ It may be running Linux with WatchGuard. Because it has setuped an Intrusion Prevention Service (IPS), it is difficult to know the real OS.

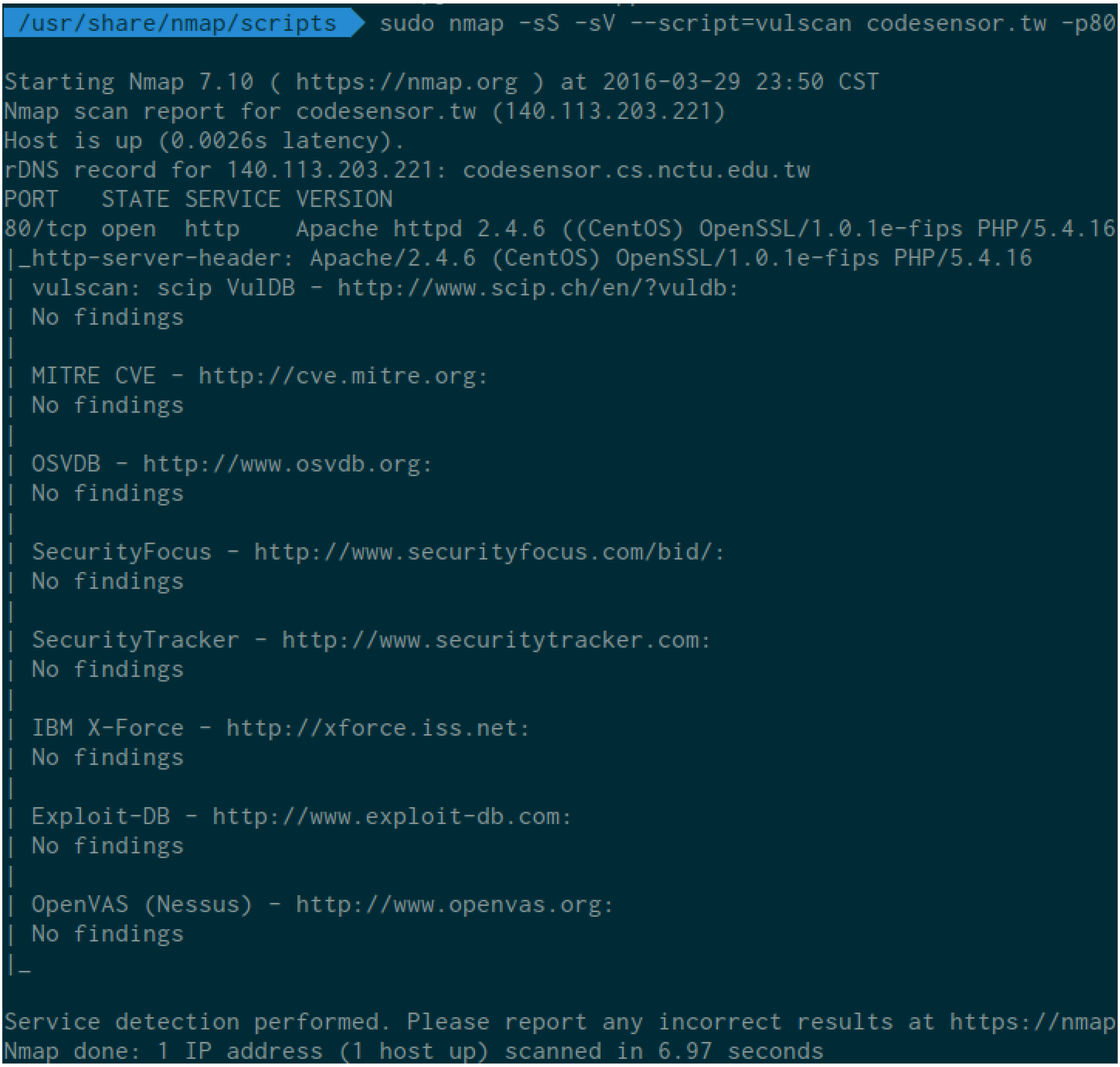
1.d. Select a target domain and use Nmap for: version scanning on a selected port.



```
~  sudo nmap -sV ywpu.me -p80

Starting Nmap 7.10 ( https://nmap.org ) at 2016-03-29 20:06 CST
Nmap scan report for ywpu.me (192.30.252.154)
Host is up (0.21s latency).
Other addresses for ywpu.me (not scanned): 192.30.252.153
rDNS record for 192.30.252.154: pages.github.com
PORT   STATE SERVICE VERSION
80/tcp open  http    GitHub.com
1 service unrecognized despite returning data. If you know the service/vers
SF-Port80-TCP:V=7.10%I=7%D=3/29%Time=56FA6FCE%P=x86_64-redhat-linux-gnu%r(
SF:GetRequest,24F8,"HTTP/1\.1\x20404\x20Not\x20Found\r\nServer:\x20GitHub\
SF:.com\r\nDate:\x20Tue,\x2029\x20Mar\x202016\x2012:06:38\x20GMT\r\nConten
SF:t-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x209116\r\nCo
SF:nnection:\x20close\r\nETag:\x20\"551c96e7-239c\"\r\nContent-Security-Po
SF:licy:\x20default-src\x20'none';\x20style-src\x20'unsafe-inline';\x20img
SF:-src\x20data:;\x20connect-src\x20'self'\r\nX-GitHub-Request-Id:\x208C71
SF:7997:3F96:22D6709C:56FA6FC9\r\n\r\n<!DOCTYPE\x20html>\n<html>\n\x20\x20
SF:<head>\n\x20\x20\x20\x20<meta\x20http-equiv=\"Content-type\"\x20content
SF:=\"text/html;\x20charset=utf-8\">\n\x20\x20\x20\x20<meta\x20http-equiv=
SF:\"Content-Security-Policy\"\x20content=\"default-src\x20'none';\x20styl
SF:e-src\x20'unsafe-inline';\x20img-src\x20data:;\x20connect-src\x20'self'
SF:\">\n\x20\x20\x20\x20<title>Site\x20not\x20found\x20&middot;\x20GitHub\
SF:x20Pages</title>\n\x20\x20\x20\x20<style\x20type=\"text/css\"\x20media=
SF:\"screen\">\n\x20\x20\x20\x20\x20\x20body\x20{\n\x20\x20\x20\x20\x20\x2
SF:0\x20\x20background-color:\x20#f1f1f1;\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:0margin:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20font-family:\x20\"Helve
SF:tica\x20Neue\",\x20Helvetica,\x20Arial,\x20sans-serif;\n\x20\x20\x20\x2
SF:0\x20\x20}\n\n\x20\x20\x20\x20\x20\x20\.container\x20{\x20margin:\x2050
SF:px\x20auto\x2040px\x20auto;\x20width:\x20600px;\x20tex")%r(HTTPOptions,
SF:24F8,"HTTP/1\.1\x20404\x20Not\x20Found\r\nServer:\x20GitHub\.com\r\nDat
SF:e:\x20Tue,\x2029\x20Mar\x202016\x2012:06:38\x20GMT\r\nContent-Type:\x20
SF:text/html;\x20charset=utf-8\r\nContent-Length:\x209116\r\nConnection:\x
SF:20close\r\nETag:\x20\"551c96e7-239c\"\r\nContent-Security-Policy:\x20de
SF:fault-src\x20'none';\x20style-src\x20'unsafe-inline';\x20img-src\x20dat
SF:a:;\x20connect-src\x20'self'\r\nX-GitHub-Request-Id:\x208C717997:3F96:2
SF:2D67BD1:56FA6FCE\r\n\r\n<!DOCTYPE\x20html>\n<html>\n\x20\x20<head>\n\x2
SF:0\x20\x20\x20<meta\x20http-equiv=\"Content-type\"\x20content=\"text/htm
SF:l;\x20charset=utf-8\">\n\x20\x20\x20\x20<meta\x20http-equiv=\"Content-S
SF:ecurity-Policy\"\x20content=\"default-src\x20'none';\x20style-src\x20'u
SF:nsafe-inline';\x20img-src\x20data:;\x20connect-src\x20'self'\">\n\x20\x
SF:20\x20\x20<title>Site\x20not\x20found\x20&middot;\x20GitHub\x20Pages</t
SF:itle>\n\x20\x20\x20\x20<style\x20type=\"text/css\"\x20media=\"screen\">
SF:\n\x20\x20\x20\x20\x20\x20body\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20ba
SF:ckground-color:\x20#f1f1f1;\n\x20\x20\x20\x20\x20\x20\x20\x20margin:\x2
SF:00;\n\x20\x20\x20\x20\x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neu
SF:e\",\x20Helvetica,\x20Arial,\x20sans-serif;\n\x20\x20\x20\x20\x20\x20}\
SF:n\n\x20\x20\x20\x20\x20\x20\.container\x20{\x20margin:\x2050px\x20auto\
SF:x2040px\x20auto;\x20width:\x20600px;\x20tex");

Service detection performed. Please report any incorrect results at https:/
Nmap done: 1 IP address (1 host up) scanned in 25.04 seconds
```

→ Nmap failed to know its version. GitHub does very well on security!

1.e. Select a target domain and use Nmap for: vulnerability scanning on the selected port.



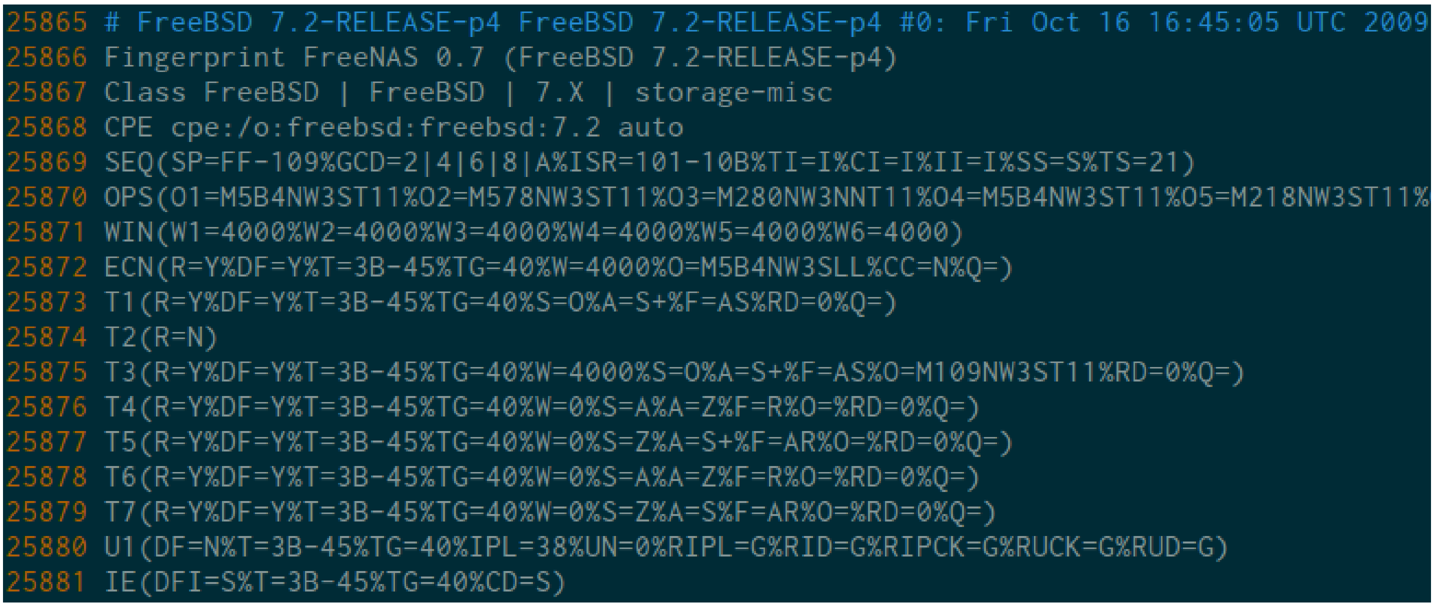
```
/usr/share/nmap/scripts  sudo nmap -sS -sV --script=vulscan codesensor.tw -p80

Starting Nmap 7.10 ( https://nmap.org ) at 2016-03-29 23:50 CST
Nmap scan report for codesensor.tw (140.113.203.221)
Host is up (0.0026s latency).
rDNS record for 140.113.203.221: codesensor.cs.nctu.edu.tw
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16
| vulscan: scip VulDB - http://www.scip.ch/en/?vuldb:
| No findings
|
| MITRE CVE - http://cve.mitre.org:
| No findings
|
| OSVDB - http://www.osvdb.org:
| No findings
|
| SecurityFocus - http://www.securityfocus.com/bid/:
| No findings
|
| SecurityTracker - http://www.securitytracker.com:
| No findings
|
| IBM X-Force - http://xforce.iss.net:
| No findings
|
| Exploit-DB - http://www.exploit-db.com:
| No findings
|
| OpenVAS (Nessus) - http://www.openvas.org:
| No findings
|_

Service detection performed. Please report any incorrect results at https://nmap
Nmap done: 1 IP address (1 host up) scanned in 6.97 seconds
```

→ Because `ywpu.me` is too secure, I decide to play `codesensor.tw`. But, still, I cannot find any vulnerability. The Nmap Scripting Engine (NSE) script I use is called `vulscan`, from `http://www.computec.ch/projekte/vulscan/`.

2. List and compare nmap-os-fingerprints used in Nmap and osprints.conf used in Siphon. Discuss how and why they differ.

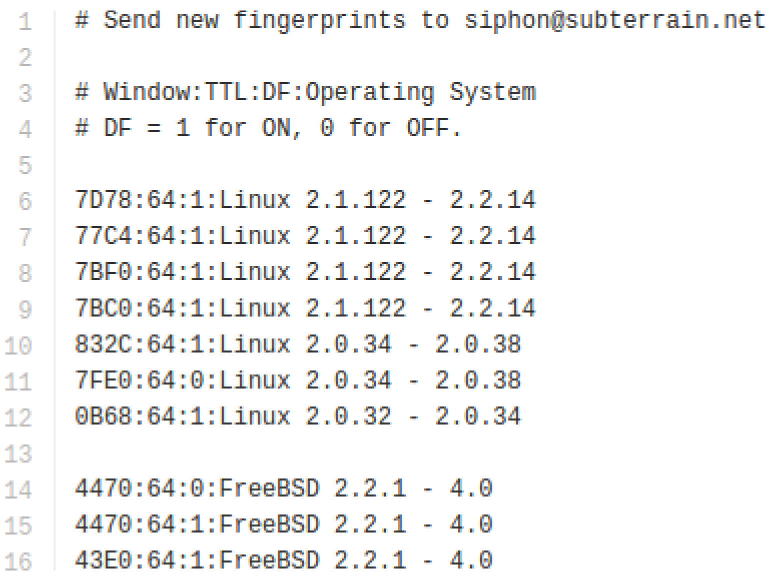
→ Siphon uses window and TTL, whereas Nmap uses more sophisticate rules (because it supports more scanning options, e.g. different protocols).

```
/usr/share/nmap  vim nmap-os-db
```



```
# FreeBSD 7.2-RELEASE-p4 FreeBSD 7.2-RELEASE-p4 #0: Fri Oct 16 16:45:05 UTC 2009
Fingerprint FreeNAS 0.7 (FreeBSD 7.2-RELEASE-p4)
Class FreeBSD | FreeBSD | 7.X | storage-misc
CPE cpe:/o:freebsd:freebsd:7.2 auto
SEQ(SP=FF-109%GCD=2|4|6|8|A%ISR=101-10B%TI=I%CI=I%II=I%SS=S%TS=21)
OPS(O1=M5B4NW3ST11%O2=M578NW3ST11%O3=M280NW3NNT11%O4=M5B4NW3ST11%O5=M218NW3ST11%
WIN(W1=4000%W2=4000%W3=4000%W4=4000%W5=4000%W6=4000)
ECN(R=Y%DF=Y%T=3B-45%TG=40%W=4000%O=M5B4NW3SLL%CC=N%Q=)
T1(R=Y%DF=Y%T=3B-45%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=Y%DF=Y%T=3B-45%TG=40%W=4000%S=O%A=S+%F=AS%O=M109NW3ST11%RD=0%Q=)
T4(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
U1(DF=N%T=3B-45%TG=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(DFI=S%T=3B-45%TG=40%CD=S)
```

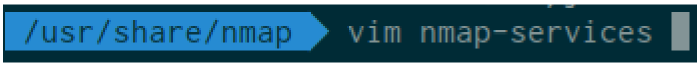
https://github.com/unmarshal/siphon/blob/master/osprints.conf



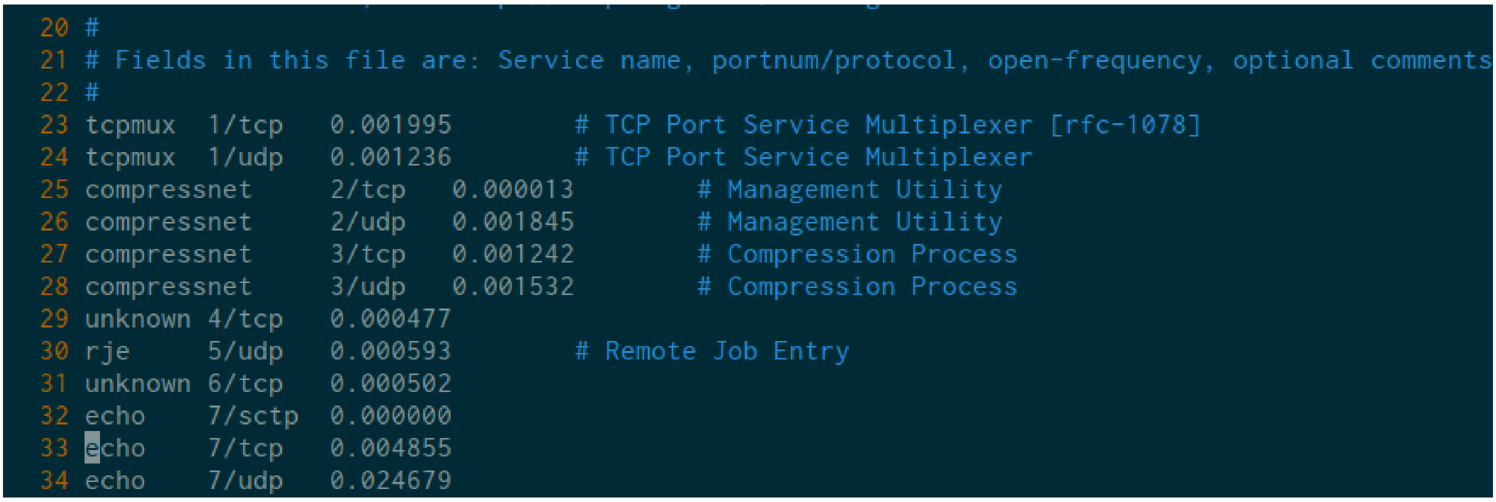
```
# Send new fingerprints to siphon@subterrain.net

# Window:TTL:DF:Operating System
# DF = 1 for ON, 0 for OFF.

7D78:64:1:Linux 2.1.122 - 2.2.14
77C4:64:1:Linux 2.1.122 - 2.2.14
7BF0:64:1:Linux 2.1.122 - 2.2.14
7BC0:64:1:Linux 2.1.122 - 2.2.14
832C:64:1:Linux 2.0.34 - 2.0.38
7FE0:64:0:Linux 2.0.34 - 2.0.38
0B68:64:1:Linux 2.0.32 - 2.0.34

4470:64:0:FreeBSD 2.2.1 - 4.0
4470:64:1:FreeBSD 2.2.1 - 4.0
43E0:64:1:FreeBSD 2.2.1 - 4.0
```

3. List and compare nmap-services and nmap-service-probe. Discuss how and why they differ.

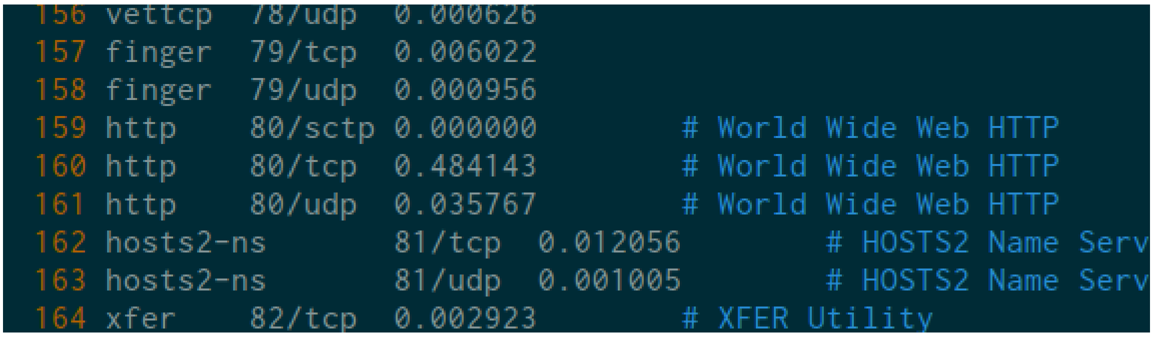
→ `nmap-services` lists all common services and protocols run on each port. Moreover, each of them are given a possibility value. For example, HTTP through TCP on port 80 is very popular, so it has a high possibility value. `nmap-service-probe`, on the other hand, lists all common headers returned from each service. For example, an HTTP server may return a string containing `HTTP`. so we can use this message to guess whether it is an HTTP server.



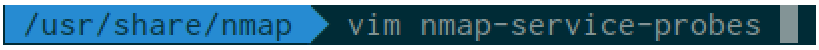
```
/usr/share/nmap  vim nmap-services
```



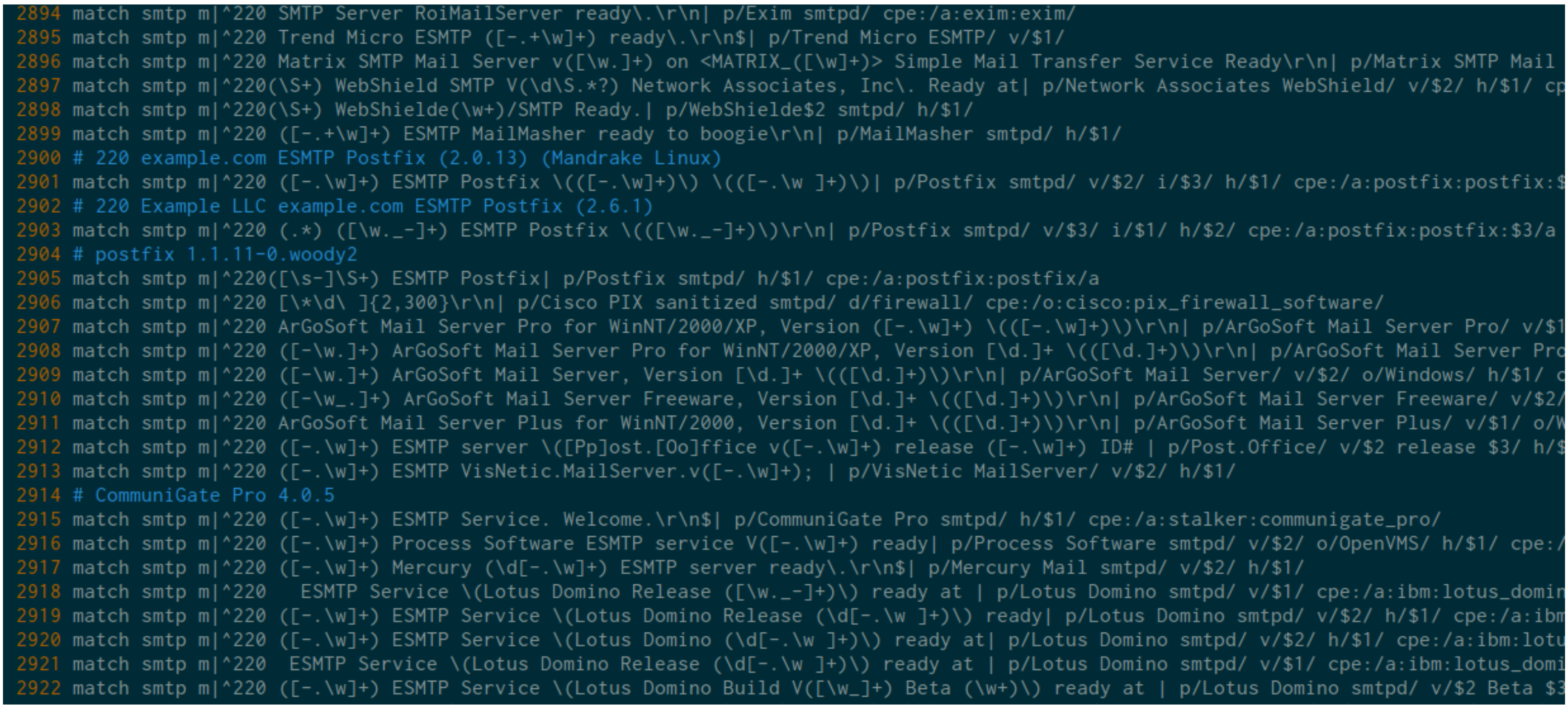
```
#
# Fields in this file are: Service name, portnum/protocol, open-frequency, optional comments
#
tcpmux  1/tcp   0.001995        # TCP Port Service Multiplexer [rfc-1078]
tcpmux  1/udp   0.001236        # TCP Port Service Multiplexer
compressnet     2/tcp   0.000013        # Management Utility
compressnet     2/udp   0.001845        # Management Utility
compressnet     3/tcp   0.001242        # Compression Process
compressnet     3/udp   0.001532        # Compression Process
unknown 4/tcp   0.000477
rje     5/udp   0.000593        # Remote Job Entry
unknown 6/tcp   0.000502
echo    7/sctp  0.000000
echo    7/tcp   0.004855
echo    7/udp   0.024679
```



```
vettcp  78/udp  0.000626
finger  79/tcp  0.006022
finger  79/udp  0.000956
http    80/sctp 0.000000        # World Wide Web HTTP
http    80/tcp  0.484143        # World Wide Web HTTP
http    80/udp  0.035767        # World Wide Web HTTP
hosts2-ns       81/tcp  0.012056        # HOSTS2 Name Serv
hosts2-ns       81/udp  0.001005        # HOSTS2 Name Serv
xfer    82/tcp  0.002923        # XFER Utility
```



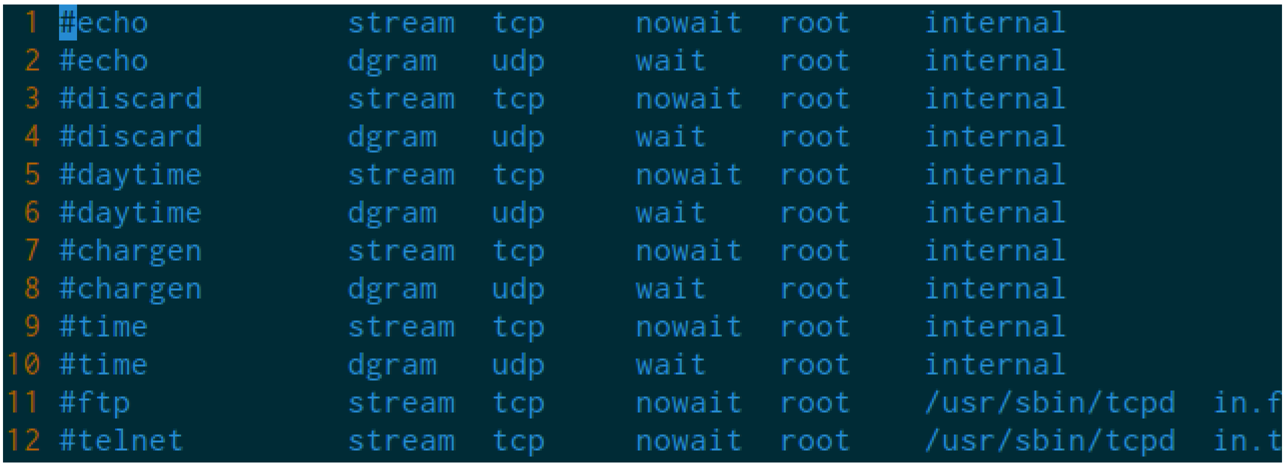
```
/usr/share/nmap  vim nmap-service-probes
```



```
match smtp m|^220 SMTP Server RoiMailServer ready\.\r\n| p/Exim smtpd/ cpe:/a:exim:exim/
match smtp m|^220 Trend Micro ESMTP ([-.+\w]+) ready\.\r\n$| p/Trend Micro ESMTP/ v/$1/
match smtp m|^220 Matrix SMTP Mail Server v([\w.]+) on <MATRIX_([\w]+)> Simple Mail Transfer Service Ready\r\n| p/Matrix SMTP Mail
match smtp m|^220(\S+) WebShield SMTP V(\d\S.*?) Network Associates, Inc\. Ready at| p/Network Associates WebShield/ v/$2/ h/$1/ cp
match smtp m|^220(\S+) WebShielde(\w+)/SMTP Ready.| p/WebShielde$2 smtpd/ h/$1/
match smtp m|^220 ([-.+\w]+) ESMTP MailMasher ready to boogie\r\n| p/MailMasher smtpd/ h/$1/
# 220 example.com ESMTP Postfix (2.0.13) (Mandrake Linux)
match smtp m|^220 ([-.\w]+) ESMTP Postfix \(([-.\w]+)\) \(([-.\w ]+)\)| p/Postfix smtpd/ v/$2/ i/$3/ h/$1/ cpe:/a:postfix:postfix:$
# 220 Example LLC example.com ESMTP Postfix (2.6.1)
match smtp m|^220 (.*) ([\w._-]+) ESMTP Postfix \(([\w._-]+)\)\r\n| p/Postfix smtpd/ v/$3/ i/$1/ h/$2/ cpe:/a:postfix:postfix:$3/a
# postfix 1.1.11-0.woody2
match smtp m|^220([\s-]\S+) ESMTP Postfix| p/Postfix smtpd/ h/$1/ cpe:/a:postfix:postfix/a
match smtp m|^220 [\*\d\ ]{2,300}\r\n| p/Cisco PIX sanitized smtpd/ d/firewall/ cpe:/o:cisco:pix_firewall_software/
match smtp m|^220 ArGoSoft Mail Server Pro for WinNT/2000/XP, Version ([-.\w]+) \(([-.\w]+)\)\r\n| p/ArGoSoft Mail Server Pro/ v/$1
match smtp m|^220 ([-\w.]+) ArGoSoft Mail Server Pro for WinNT/2000/XP, Version [\d.]+ \(([\d.]+)\)\r\n| p/ArGoSoft Mail Server Pro
match smtp m|^220 ([-\w.]+) ArGoSoft Mail Server, Version [\d.]+ \(([\d.]+)\)\r\n| p/ArGoSoft Mail Server/ v/$2/ o/Windows/ h/$1/ c
match smtp m|^220 ([-\w_.]+) ArGoSoft Mail Server Freeware, Version [\d.]+ \(([\d.]+)\)\r\n| p/ArGoSoft Mail Server Freeware/ v/$2/
match smtp m|^220 ArGoSoft Mail Server Plus for WinNT/2000, Version [\d.]+ \(([\d.]+)\)\r\n| p/ArGoSoft Mail Server Plus/ v/$1/ o/W
match smtp m|^220 ([-.\w]+) ESMTP server \([Pp]ost.[Oo]ffice v([-.\w]+) release ([-.\w]+) ID# | p/Post.Office/ v/$2 release $3/ h/$
match smtp m|^220 ([-.\w]+) ESMTP VisNetic.MailServer.v([-.\w]+); | p/VisNetic MailServer/ v/$2/ h/$1/
# CommuniGate Pro 4.0.5
match smtp m|^220 ([-.\w]+) ESMTP Service. Welcome.\r\n$| p/CommuniGate Pro smtpd/ h/$1/ cpe:/a:stalker:communigate_pro/
match smtp m|^220 ([-.\w]+) Process Software ESMTP service V([-.\w]+) ready| p/Process Software smtpd/ v/$2/ o/OpenVMS/ h/$1/ cpe:/
match smtp m|^220 ([-.\w]+) Mercury (\d[-.\w]+) ESMTP server ready\.\r\n$| p/Mercury Mail smtpd/ v/$2/ h/$1/
match smtp m|^220   ESMTP Service \(Lotus Domino Release ([\w._-]+)\) ready at | p/Lotus Domino smtpd/ v/$1/ cpe:/a:ibm:lotus_domin
match smtp m|^220 ([-.\w]+) ESMTP Service \(Lotus Domino Release (\d[-.\w ]+)\) ready| p/Lotus Domino smtpd/ v/$2/ h/$1/ cpe:/a:ibm
match smtp m|^220 ([-.\w]+) ESMTP Service \(Lotus Domino (\d[-.\w ]+)\) ready at| p/Lotus Domino smtpd/ v/$2/ h/$1/ cpe:/a:ibm:lotu
match smtp m|^220  ESMTP Service \(Lotus Domino Release (\d[-.\w ]+)\) ready at | p/Lotus Domino smtpd/ v/$1/ cpe:/a:ibm:lotus_domi
match smtp m|^220 ([-.\w]+) ESMTP Service \(Lotus Domino Build V([\w_]+) Beta (\w+)\) ready at | p/Lotus Domino smtpd/ v/$2 Beta $3
```

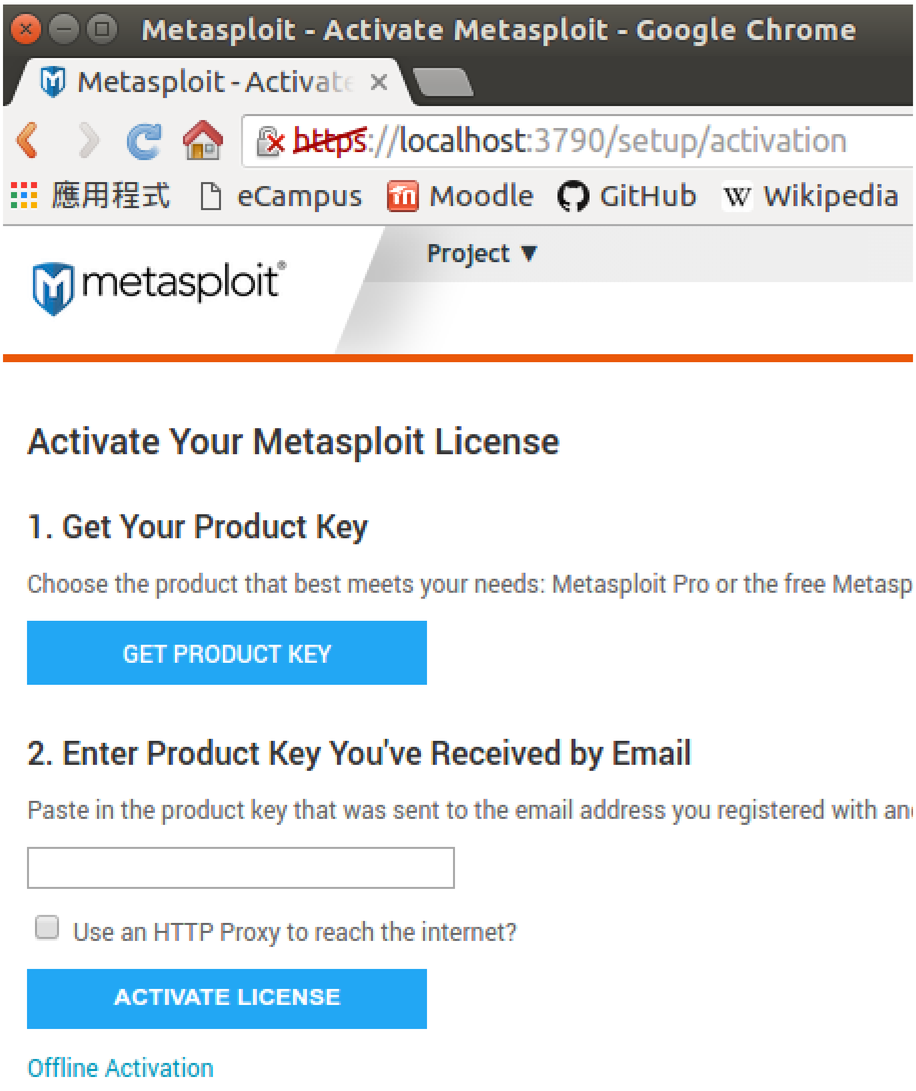
4. On a UNIX/Linux host, list /etc/inetd.conf. Discuss what services are being offered.

→ This system may be able to run Echo, FTP, Telnet, etc., but all theses services are disabled. (For security reasons, we should always disable unused services.)



```
#echo           stream  tcp     nowait  root    internal
#echo           dgram   udp     wait    root    internal
#discard        stream  tcp     nowait  root    internal
#discard        dgram   udp     wait    root    internal
#daytime        stream  tcp     nowait  root    internal
#daytime        dgram   udp     wait    root    internal
#chargen        stream  tcp     nowait  root    internal
#chargen        dgram   udp     wait    root    internal
#time           stream  tcp     nowait  root    internal
#time           dgram   udp     wait    root    internal
#ftp            stream  tcp     nowait  root    /usr/sbin/tcpd  in.f
#telnet         stream  tcp     nowait  root    /usr/sbin/tcpd  in.t
```

5. Select a target domain, run Metasploit with Nmap scans and import Nmap results into the database. Show found hosts and available ports.



Metasploit - Activate Metasploit - Google Chrome
Metasploit - Activat
~~https~~://localhost:3790/setup/activation
應用程式
eCampus
Moodle
GitHub
Wikipedia
metasploit
Project ▼

Activate Your Metasploit License

1. Get Your Product Key

Choose the product that best meets your needs: Metasploit Pro or the free Metasp

GET PRODUCT KEY

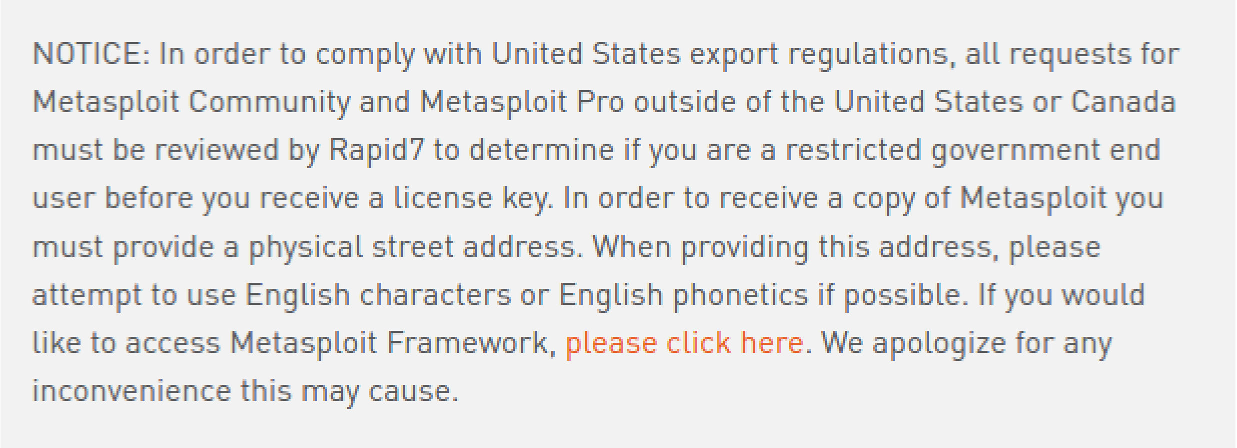
2. Enter Product Key You've Received by Email

Paste in the product key that was sent to the email address you registered with an

□ Use an HTTP Proxy to reach the internet?

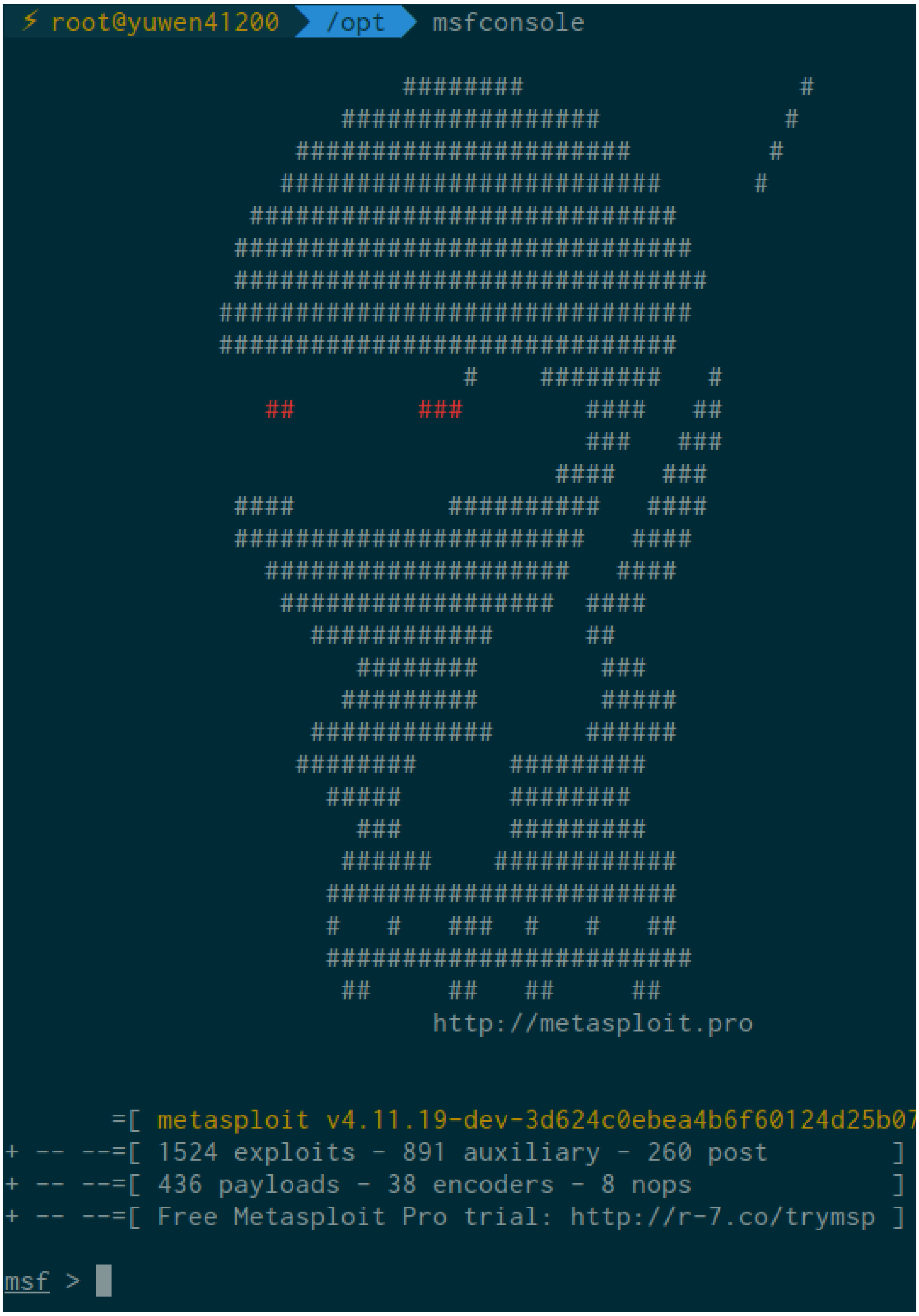
ACTIVATE LICENSE

Offline Activation



NOTICE: In order to comply with United States export regulations, all requests for Metasploit Community and Metasploit Pro outside of the United States or Canada must be reviewed by Rapid7 to determine if you are a restricted government end user before you receive a license key. In order to receive a copy of Metasploit you must provide a physical street address. When providing this address, please attempt to use English characters or English phonetics if possible. If you would like to access Metasploit Framework, please click here. We apologize for any inconvenience this may cause.

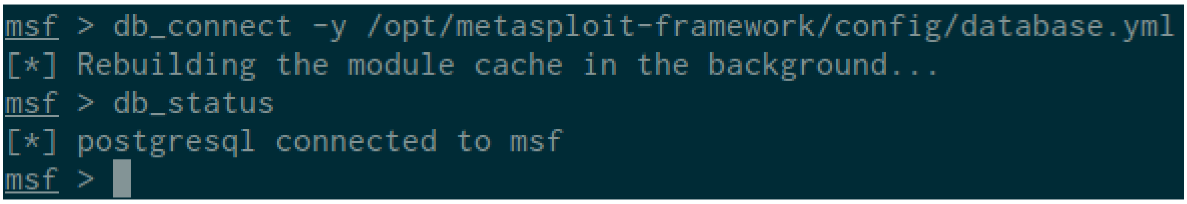
→ I cannot use it because I need a license, but I am a Taiwanese. I even try to install it, but it still need a license to launch. Then I try to install Metasploit Framework, which is a subproject of Metasploit. Here are the results.



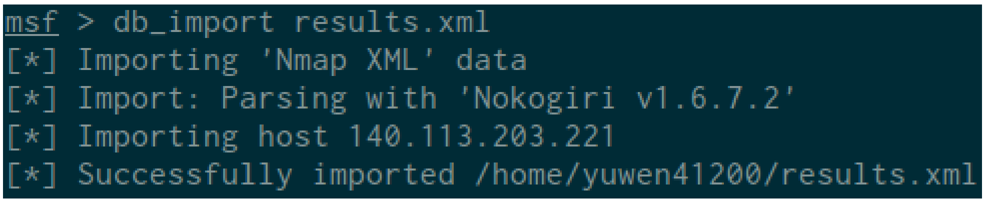
```
⚡ root@yuwen41200  /opt  msfconsole

                          ########                  #
                      #################            #
                   ######################         #
                  #########################      #
                ############################
               ##############################
               ###############################
              ###############################
              ##############################
                              #    ########   #
                 ##        ###        ####   ##
                                      ###   ###
                                    ####   ###
               ####          ##########   ####
               #######################   ####
                 ####################   ####
                  ##################  ####
                    ############      ##
                       ########        ###
                      #########        #####
                    ############      ######
                   ########      #########
                     #####       ########
                       ###       #########
                      ######    ############
                     #######################
                     #   #   ###  #   #   ##
                     ########################
                      ##     ##   ##     ##
                            http://metasploit.pro


       =[ metasploit v4.11.19-dev-3d624c0ebea4b6f60124d25b07
+ -- --=[ 1524 exploits - 891 auxiliary - 260 post        ]
+ -- --=[ 436 payloads - 38 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

```
$ sudo nmap -A -v codesensor.tw -oA results

Starting Nmap 7.10 ( https://nmap.org ) at 2016-03-30 17:25 CST
NSE: Loaded 138 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating Ping Scan at 17:25
Scanning codesensor.tw (140.113.203.221) [4 ports]
Completed Ping Scan at 17:25, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:25
Completed Parallel DNS resolution of 1 host. at 17:25, 0.53s elapsed
Initiating SYN Stealth Scan at 17:25
Scanning codesensor.tw (140.113.203.221) [1000 ports]
Discovered open port 80/tcp on 140.113.203.221
Discovered open port 443/tcp on 140.113.203.221
Discovered open port 21/tcp on 140.113.203.221
Discovered open port 554/tcp on 140.113.203.221
Discovered open port 1723/tcp on 140.113.203.221
Discovered open port 22/tcp on 140.113.203.221
Completed SYN Stealth Scan at 17:25, 35.00s elapsed (1000 total ports)
Initiating Service scan at 17:25
Scanning 6 services on codesensor.tw (140.113.203.221)
Service scan Timing: About 66.67% done; ETC: 17:28 (0:00:52 remaining)
Service scan Timing: About 83.33% done; ETC: 17:28 (0:00:30 remaining)
Completed Service scan at 17:28, 150.49s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against codesensor.tw (140.113.203.221)
Retrying OS detection (try #2) against codesensor.tw (140.113.203.221)
Initiating Traceroute at 17:28
Completed Traceroute at 17:28, 3.01s elapsed
Initiating Parallel DNS resolution of 16 hosts. at 17:28
Completed Parallel DNS resolution of 16 hosts. at 17:28, 4.97s elapsed
NSE: Script scanning 140.113.203.221.
Initiating NSE at 17:28
Completed NSE at 17:29, 31.07s elapsed
Initiating NSE at 17:29
Completed NSE at 17:29, 5.23s elapsed
Nmap scan report for codesensor.tw (140.113.203.221)
Host is up (0.46s latency).
rDNS record for 140.113.203.221: codesensor.cs.nctu.edu.tw
Not shown: 994 filtered ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp?
|_ftp-bounce: no banner
22/tcp   open  ssh      OpenSSH 6.6.1 (protocol 2.0)
| ssh-hostkey:
|   2048 7e:bb:a4:52:f3:fa:4a:f8:a3:60:68:67:85:d6:b3:c0 (RSA)
|_  256 d6:90:93:47:ab:7d:02:6a:ac:09:12:b7:f6:06:b1:01 (ECDSA)
80/tcp   open  http     Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16
|_http-title: Did not follow redirect to https://codesensor.tw/
443/tcp  open  ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16)
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
```

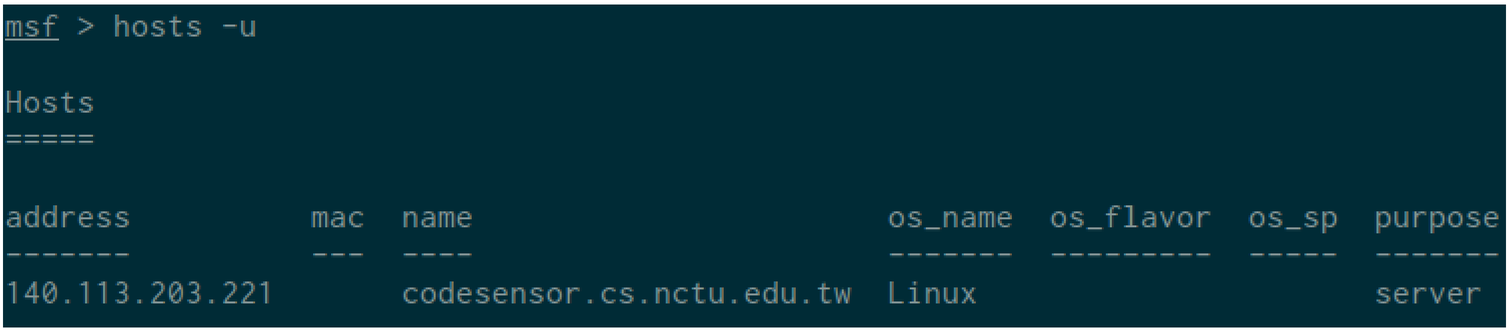
```
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16
|_http-title: SENSE Lab - Code Sensor
| ssl-cert: Subject: commonName=www.codesensor.tw/countryName=TW
| Issuer: commonName=AlphaSSL CA - SHA256 - G2/organizationName=GlobalSign nv-
sa/countryName=BE
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2015-12-23T08:23:15
| Not valid after:  2017-01-22T08:23:15
| MD5:   a316 4d89 be96 efde 37e3 db59 ba9d e148
|_SHA-1: 1610 c855 a760 d012 5cb3 abb8 878c 772a 1fa3 c6f8
|_ssl-date: 2016-03-30T09:28:59+00:00; -1s from scanner time.
554/tcp  open  rtsp?
1723/tcp open  pptp?
|_pptp-version: ERROR: Script execution failed (use -d to debug)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: load balancer
Running (JUST GUESSING): F5 Networks TMOS 11.6.X (87%)
OS CPE: cpe:/o:f5:tmos:11.6
Aggressive OS guesses: F5 BIG-IP Local Traffic Manager load balancer (TMOS 11.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 38.614 days (since Sun Feb 21 02:45:11 2016)
Network Distance: 17 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   44.83 ms  htc_frisbee.com (192.168.1.1)
2   ...
3   839.78 ms 10.158.65.1
4   847.52 ms 10.158.67.7
5   847.98 ms 10.158.67.17
6   969.49 ms tchn-3302.hinet.net (210.65.126.114)
7   767.44 ms tchn-3011.hinet.net (220.128.16.234)
8   684.65 ms tyfo-3012.hinet.net (220.128.17.50)
9   711.66 ms sczs-3201.hinet.net (220.128.8.37)
10  636.82 ms r4102-s2.tp.hinet.net (220.128.7.157)
11  633.51 ms 211-22-38-249.HINET-IP.hinet.net (211.22.38.249)
12  41.95 ms  140.113.0.106
13  969.21 ms 140.113.0.77
14  918.44 ms 140.113.0.53
15  847.40 ms 140.113.3.177
16  837.19 ms ge-1-0-12.dar01.ec2.colocation.cs.nctu.edu.tw (140.113.23.206)
17  837.12 ms codesensor.cs.nctu.edu.tw (140.113.203.221)

NSE: Script Post-scanning.
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 255.19 seconds
           Raw packets sent: 2074 (94.780KB) | Rcvd: 123 (7.424KB)
```



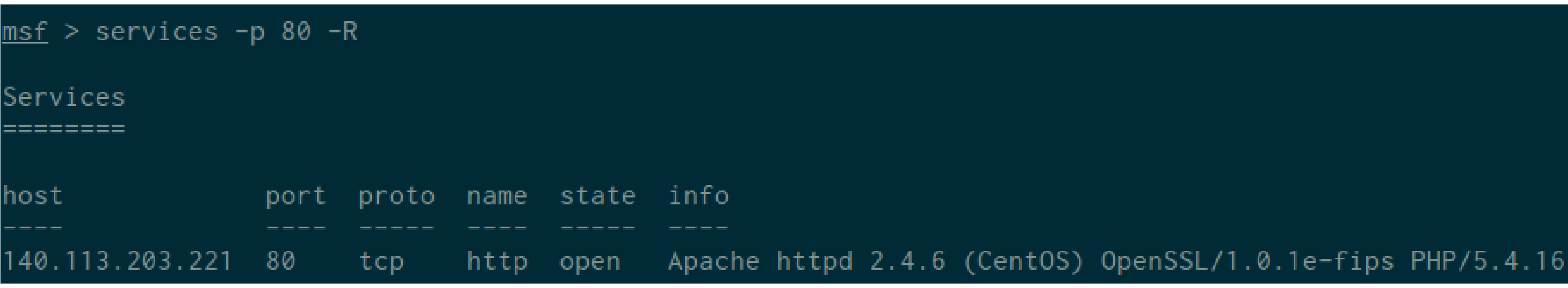
```
msf > db_connect -y /opt/metasploit-framework/config/database.yml
[*] Rebuilding the module cache in the background...
msf > db_status
[*] postgresql connected to msf
msf > 
```



```
msf > db_import results.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.6.7.2'
[*] Importing host 140.113.203.221
[*] Successfully imported /home/yuwen41200/results.xml
```

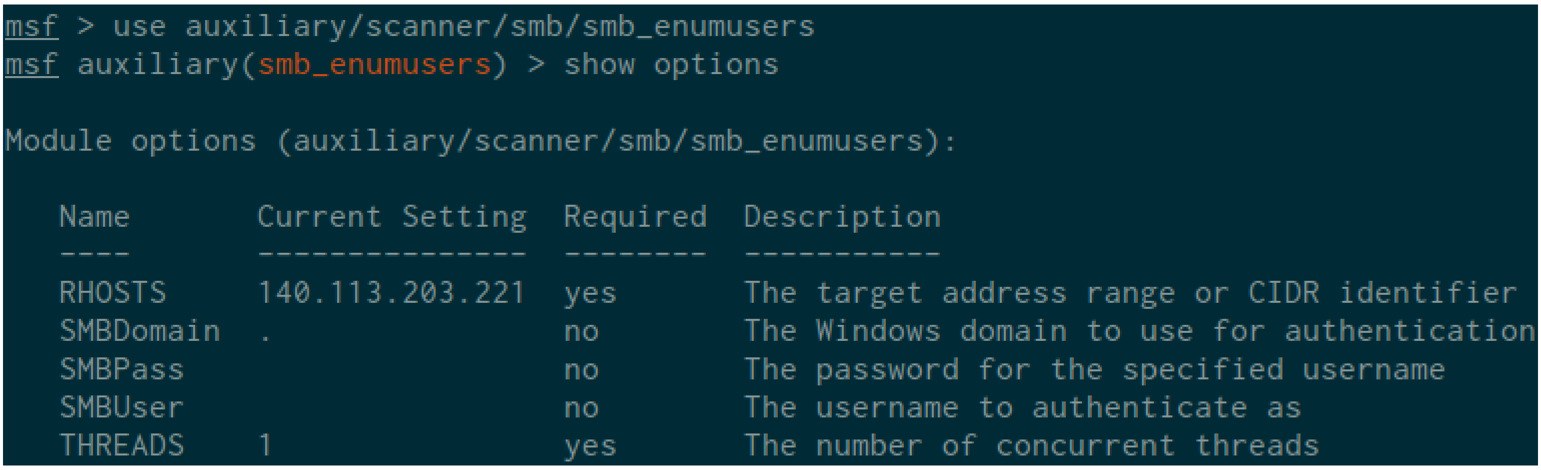


```
msf > hosts -u

Hosts
=====

address          mac  name                        os_name  os_flavor  os_sp  purpose
-------          ---  ----                        -------  ---------  -----  -------
140.113.203.221       codesensor.cs.nctu.edu.tw  Linux                       server
```

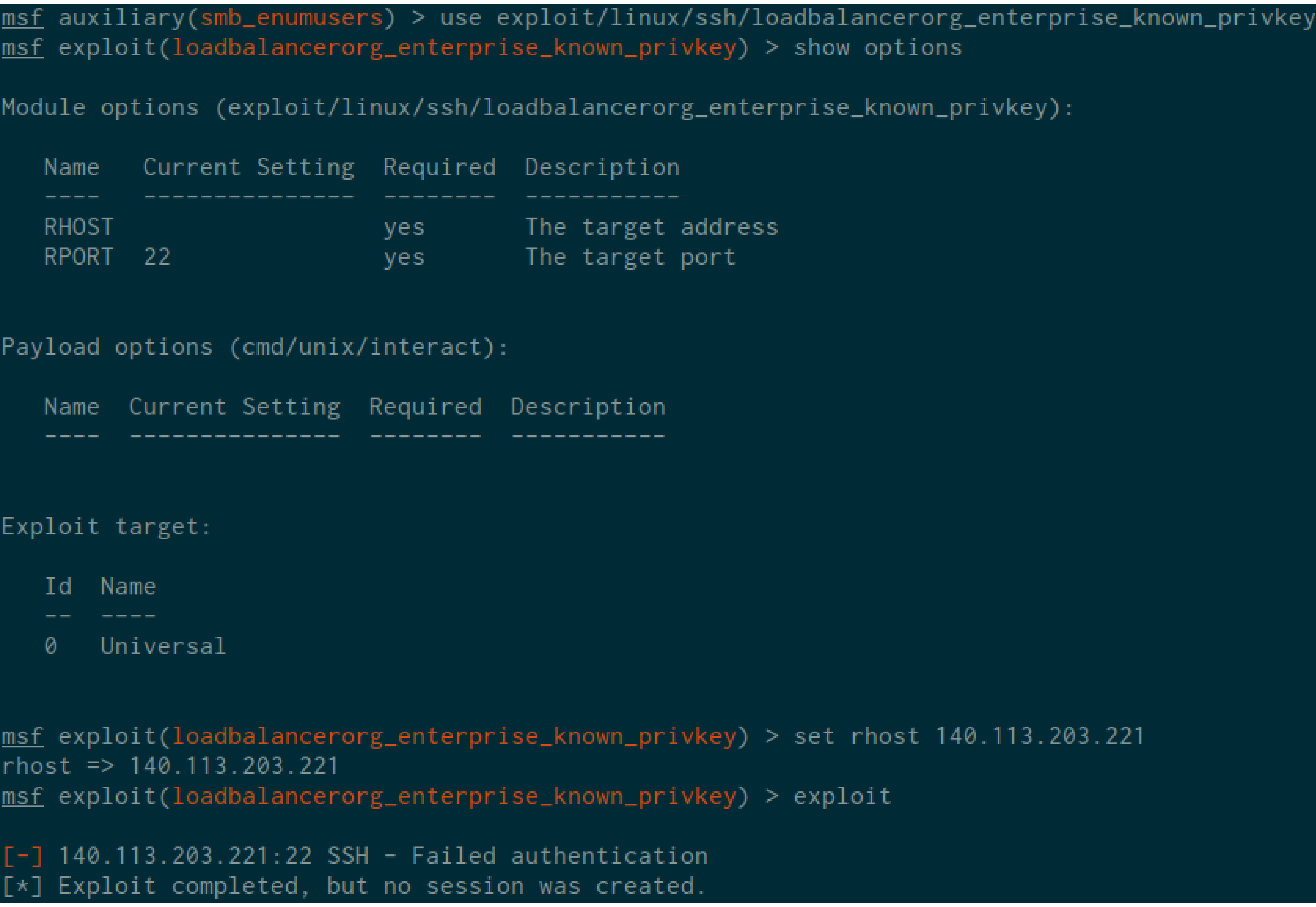


```
msf > services -p 80 -R

Services
========

host             port  proto  name  state  info
----             ----  -----  ----  -----  ----
140.113.203.221  80    tcp    http  open   Apache httpd 2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16
```

→ Port 80 on host 140.113.203.221 is opened for Apache HTTP server.



```
msf > use auxiliary/scanner/smb/smb_enumusers
msf auxiliary(smb_enumusers) > show options

Module options (auxiliary/scanner/smb/smb_enumusers):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS     140.113.203.221  yes       The target address range or CIDR identifier
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads
```

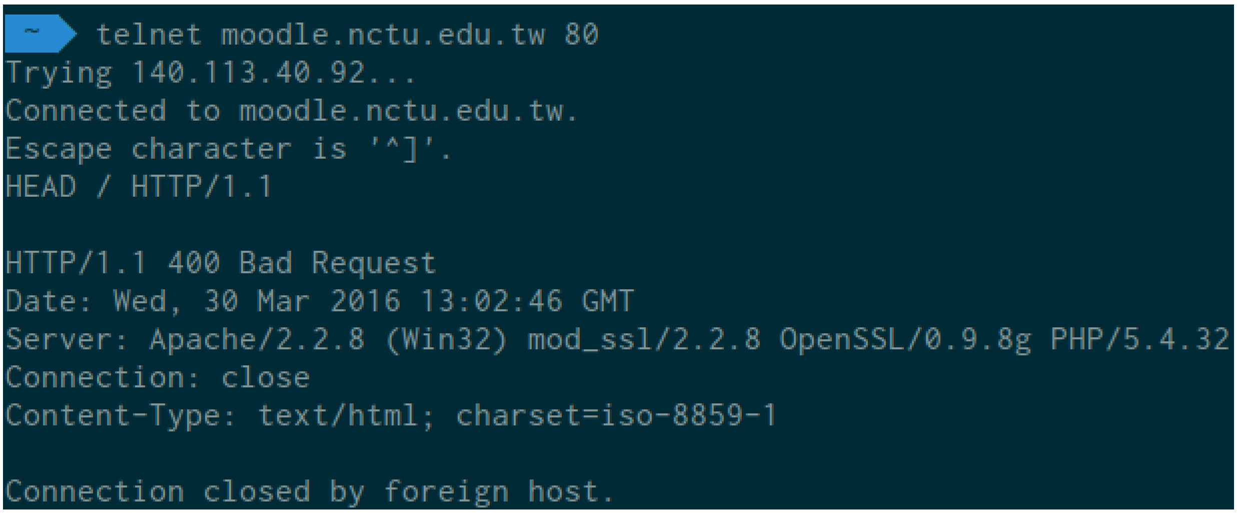


```
msf auxiliary(smb_enumusers) > use exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey
msf exploit(loadbalancerorg_enterprise_known_privkey) > show options

Module options (exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  22               yes       The target port


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Universal


msf exploit(loadbalancerorg_enterprise_known_privkey) > set rhost 140.113.203.221
rhost => 140.113.203.221
msf exploit(loadbalancerorg_enterprise_known_privkey) > exploit

[-] 140.113.203.221:22 SSH - Failed authentication
[*] Exploit completed, but no session was created.
```

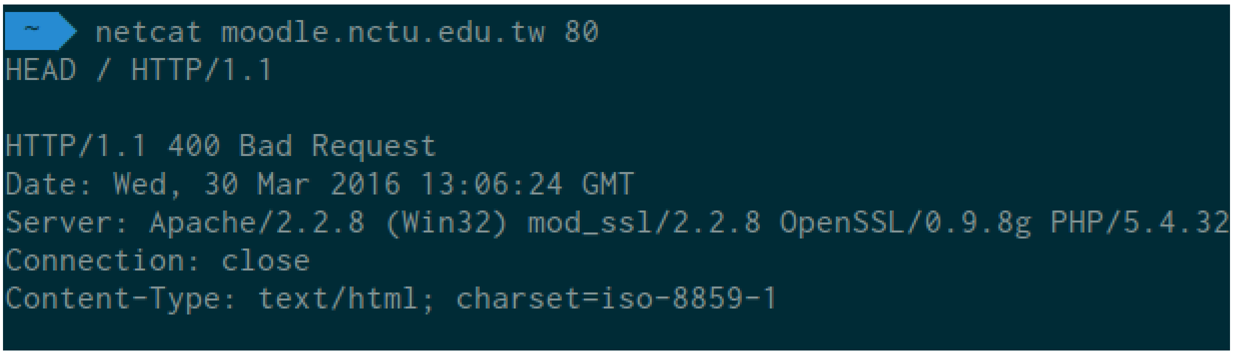
→ I have also tried some exploiting methods. Of course, I did not really find a possible CVE and hack it.

6. Select a website to do banner grabbing with telnet, netcat, and grendel-scan, respectively. Show and compare their results.

→ We can know that `moodle.nctu.edu.tw` is running Apache 2.2.8, mod_ssl 2.2.8, OpenSSL 0.9.8g, PHP 5.4.32 on a 32-bit Windows. But netcat is more preferable because it can transmit data in either TCP or UDP. Netcat also offers more functionality than telnet. Grendel-scan is not available now. Its repository on SourceForge only contains a `lib` folder.



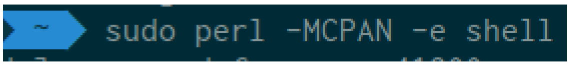
```
 ~   telnet moodle.nctu.edu.tw 80
Trying 140.113.40.92...
Connected to moodle.nctu.edu.tw.
Escape character is '^]'.
HEAD / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Wed, 30 Mar 2016 13:02:46 GMT
Server: Apache/2.2.8 (Win32) mod_ssl/2.2.8 OpenSSL/0.9.8g PHP/5.4.32
Connection: close
Content-Type: text/html; charset=iso-8859-1

Connection closed by foreign host.
```



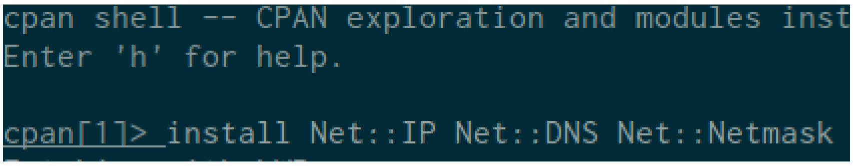
```
 ~   netcat moodle.nctu.edu.tw 80
HEAD / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Wed, 30 Mar 2016 13:06:24 GMT
Server: Apache/2.2.8 (Win32) mod_ssl/2.2.8 OpenSSL/0.9.8g PHP/5.4.32
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

7. Select a target domain to do automatic DNS enumeration by dnsenum to find sub-domains, servers, and their IP addresses.

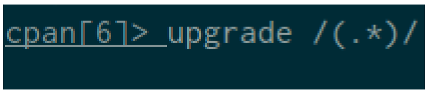
→ Download dnsenum, install and upgrade all necessary Perl modules, but it still does not work. According to some on-line resources, this may be caused by bugs in the Perl modules.



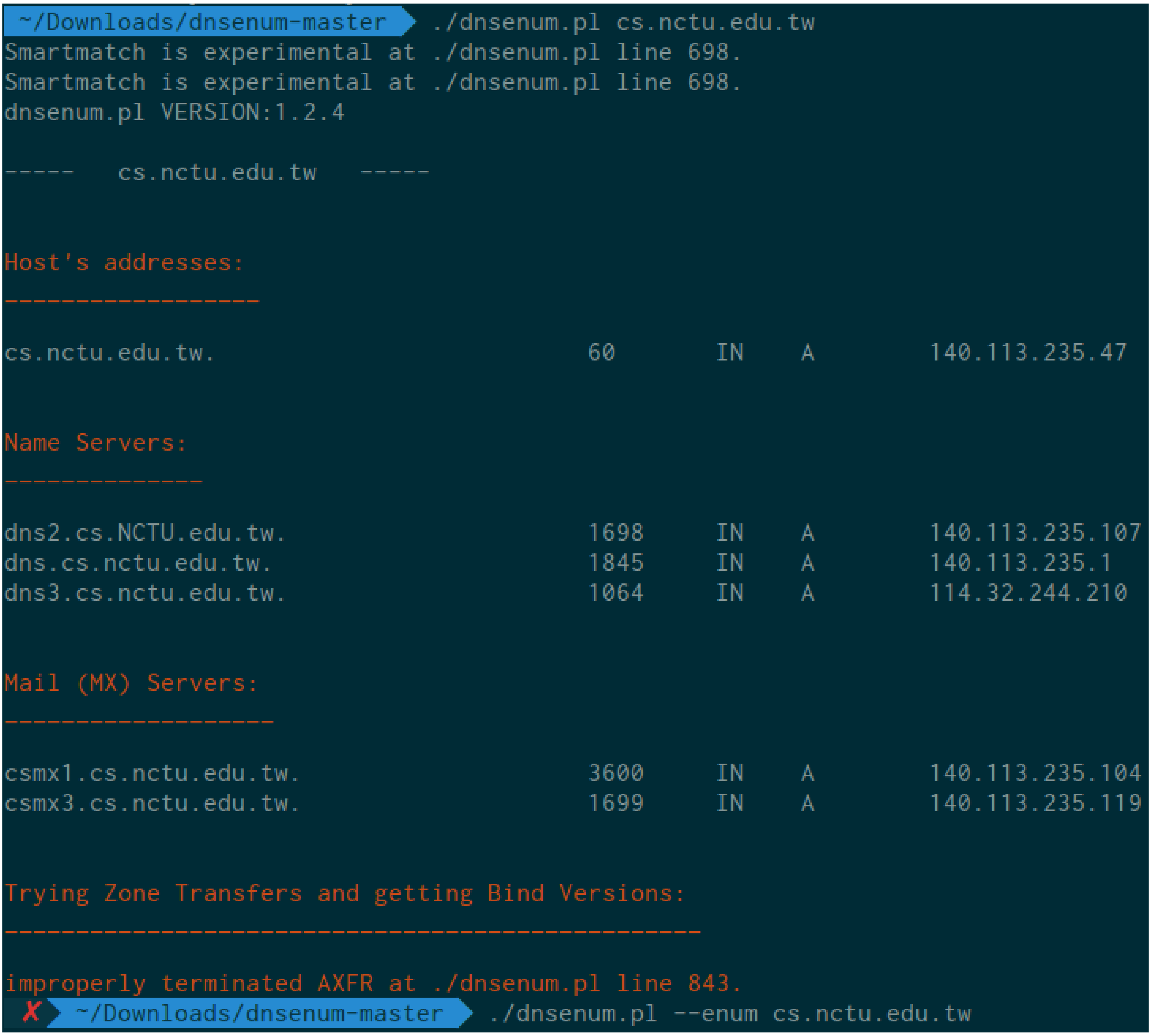
```
 ~  sudo perl -MCPAN -e shell
```



```
cpan shell -- CPAN exploration and modules inst
Enter 'h' for help.

cpan[1]> install Net::IP Net::DNS Net::Netmask
```



```
cpan[6]> upgrade /(.*)/
```



```
 ~/Downloads/dnsenum-master  ./dnsenum.pl cs.nctu.edu.tw
Smartmatch is experimental at ./dnsenum.pl line 698.
Smartmatch is experimental at ./dnsenum.pl line 698.
dnsenum.pl VERSION:1.2.4

-----   cs.nctu.edu.tw   -----


Host's addresses:
__________________

cs.nctu.edu.tw.                          60       IN    A        140.113.235.47


Name Servers:
______________

dns2.cs.NCTU.edu.tw.                     1698     IN    A        140.113.235.107
dns.cs.nctu.edu.tw.                      1845     IN    A        140.113.235.1
dns3.cs.nctu.edu.tw.                     1064     IN    A        114.32.244.210


Mail (MX) Servers:
___________________

csmx1.cs.nctu.edu.tw.                    3600     IN    A        140.113.235.104
csmx3.cs.nctu.edu.tw.                    1699     IN    A        140.113.235.119


Trying Zone Transfers and getting Bind Versions:
_________________________________________________

improperly terminated AXFR at ./dnsenum.pl line 843.
 ✗  ~/Downloads/dnsenum-master  ./dnsenum.pl --enum cs.nctu.edu.tw
```