```
$ 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.

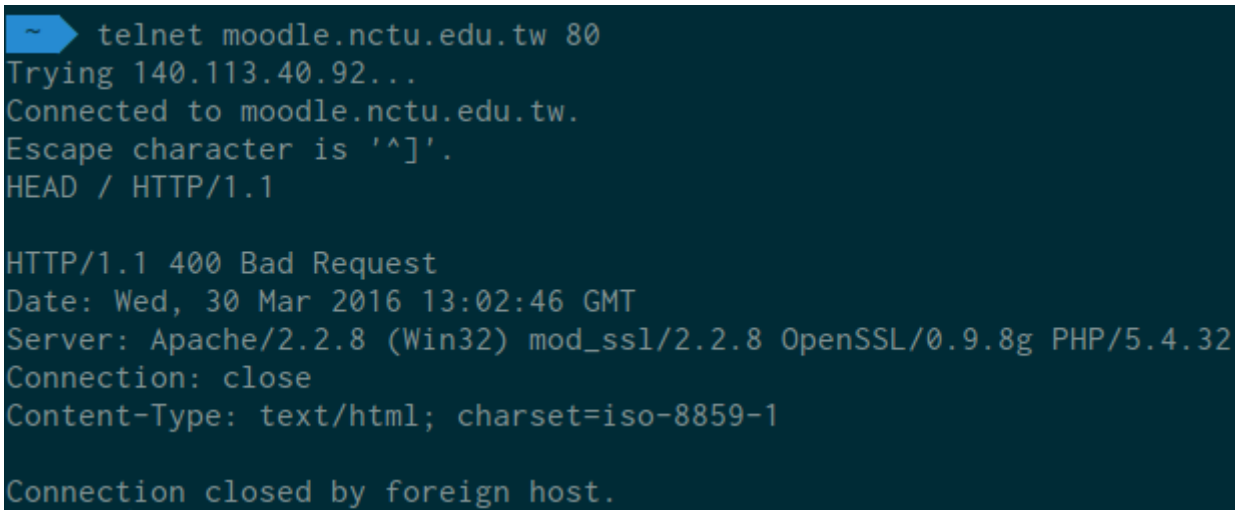
```
msf > use auxiliary/scanner/smb/smb_enumusers
msf auxiliary(smb_enumusers) > show options

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.



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
```