

Are you ready to be a hacker?

?





Outline

- Definisi hacker
- Klasifikasi hacker
- Penetration Testing
- CTF
- Perintah-Perintah Dasar Linux dan CTF

Definisi Hacker

“One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.”

- <http://www.mithral.com/~beberg/hacker.html>

Definisi Hacker

“It means someone who enjoys playful cleverness, especially in programming but other media are also possible. [...]

One possible arena for playful cleverness **is breaking security.** Hackers never had much respect for bureaucratic restrictions. If the computer was sitting idle because the administrators wouldn't let them use it, they would sometimes figure out how to bypass the obstacles and use it anyway. If this required cleverness, it would be fun in itself, as well as making it possible to do other hacking (for instance, useful work) on the computer instead of twiddling one's thumbs. **But not all hackers did security breaking. Many never were interested in that.”**

--Richard Matthew Stallman, Founder of GNU
(<https://www.gnu.org/philosophy/rms-hack.html>)

Hacker Manifesto

The Hacker Manifesto

by
+++The Mentor+++
Written January 8, 1986

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

<http://www.mithral.com/~beberg/manifesto.html>

Klasifikasi Hacker

Black hat

Gray Hat

White hat



Black hat

“A black-hat hacker is a hacker who ‘violates computer security for little reason beyond maliciousness or for personal gain’”

- Moore, Robert on Wikipedia
(https://en.wikipedia.org/wiki/Black_hat)



Grey Hat

“The term "grey hat" refers to a computer hacker or computer security expert who **may sometimes violate laws or typical ethical standards**, but **does not** have the **malicious intent typical of a black hat hacker.**”

— Wikipedia (https://en.wikipedia.org/wiki/Grey_hat)



White Hat

“The term "white hat" in Internet slang refers to an **ethical computer hacker, or a computer security expert**, who specializes in **penetration testing** and in other testing methodologies **to ensure the security** of an organization's information systems”

— Wikipedia (https://en.wikipedia.org/wiki/White_hat_%28computer_security%29)



Penetration Testing

“Penetration testing (pen-testing or pentesting) is a method of testing, measuring and enhancing established security measures on information systems and support areas.”

--Technopedia

(<https://www.techopedia.com/definition/16130/penetration-testing-pen-testing>)

CTF (Capture the flag)

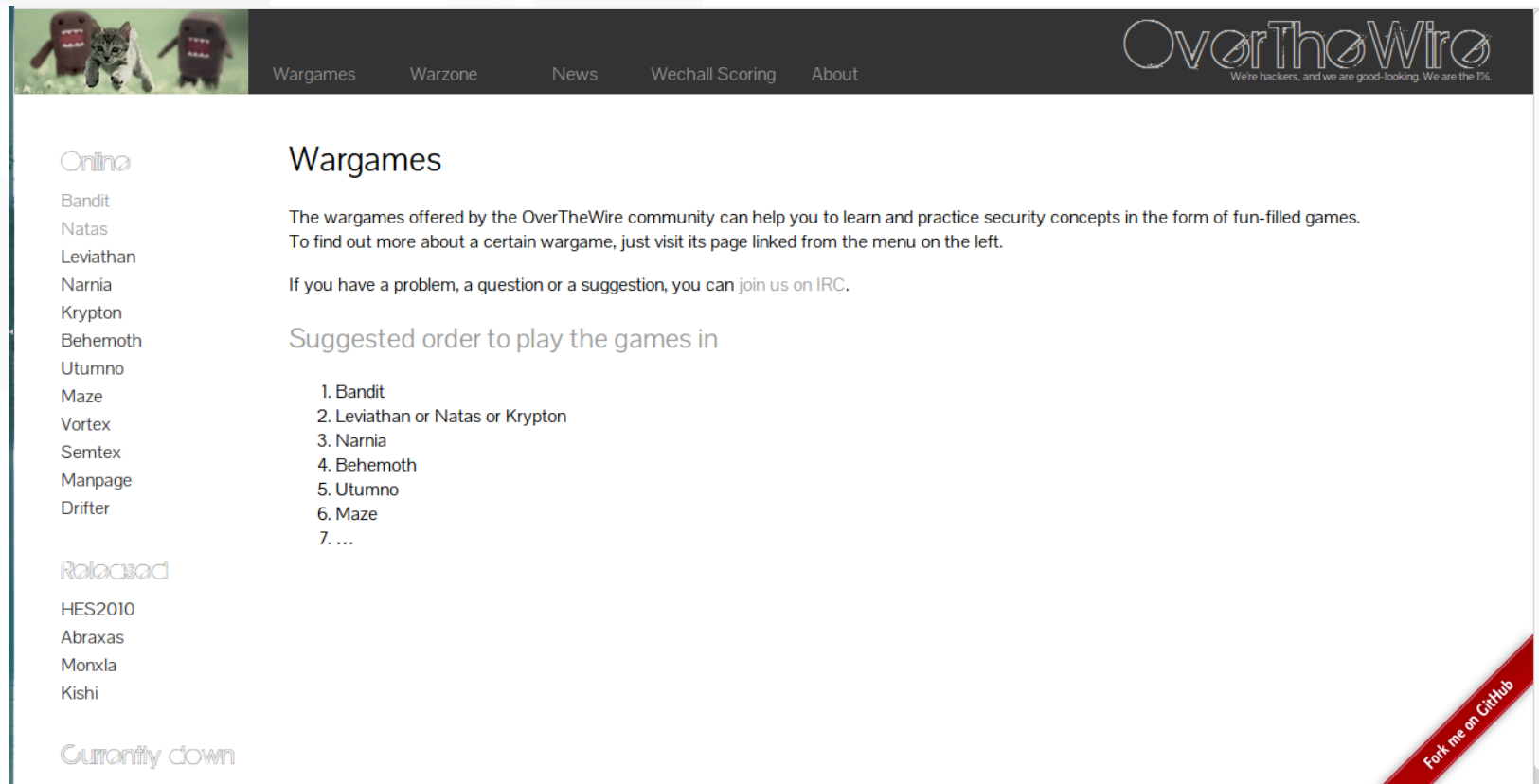
“CTF contests are usually designed to serve as an **educational exercise** to give participants experience in **securing a machine, as well as conducting and reacting to the sort of attacks found in the real world**. Reverse-engineering, network sniffing, protocol analysis, system administration, programming, and cryptanalysis are all skills which have been required by prior CTF contests at DEF CON.”

--https://en.wikipedia.org/wiki/Capture_the_flag

Beberapa sumber latihan CTF

- ▼ OverTheWire.org
- ▼ VulnHub.com
- ▼ www.owasp.org

Over the wire



The screenshot shows the OverTheWire website. The header features a navigation bar with links: Wargames, Warzone, News, Wechall Scoring, and About. The OverTheWire logo is on the right, with the tagline "We're hackers, and we are good-looking. We are the 1%." Below the header, the main content area is titled "Wargames". It contains a paragraph explaining that wargames help learn and practice security concepts. Below this, it says "If you have a problem, a question or a suggestion, you can [join us on IRC](#)." A section titled "Suggested order to play the games in" lists seven items: 1. Bandit, 2. Leviathan or Natas or Krypton, 3. Narnia, 4. Behemoth, 5. Utumno, 6. Maze, and 7. ... On the left side, there are two sections: "Online" with a list of games (Bandit, Natas, Leviathan, Narnia, Krypton, Behemoth, Utumno, Maze, Vortex, Semtex, Manpage, Drifter) and "Retired" with a list of games (HES2010, Abraxas, Monxa, Kishi). At the bottom left, there is a "Currently down" section. A red banner at the bottom right says "Fork me on GitHub".

OverTheWire
We're hackers, and we are good-looking. We are the 1%.

Wargames Warzone News Wechall Scoring About

Wargames

The wargames offered by the OverTheWire community can help you to learn and practice security concepts in the form of fun-filled games. To find out more about a certain wargame, just visit its page linked from the menu on the left.

If you have a problem, a question or a suggestion, you can [join us on IRC](#).

Suggested order to play the games in

1. Bandit
2. Leviathan or Natas or Krypton
3. Narnia
4. Behemoth
5. Utumno
6. Maze
7. ...

Online

- Bandit
- Natas
- Leviathan
- Narnia
- Krypton
- Behemoth
- Utumno
- Maze
- Vortex
- Semtex
- Manpage
- Drifter

Retired

- HES2010
- Abraxas
- Monxa
- Kishi

Currently down

-

Fork me on GitHub

Vuln Hub

The screenshot shows the Vuln Hub website interface. At the top is a dark navigation bar with links: HOME, SEARCH, HELP, RESOURCES, BLOG, and ABOUT. The main content area features a challenge titled "HackDay: Albania" by user R-73eN, dated 18 Nov 2016. The challenge description states: "This was used in HackDay Albania's 2016 CTF. The level is beginner to intermediate. It uses DHCP." To the left of the text is a terminal window showing a command prompt with the text "Ubuntu 16.04.1 LTS hackday tty1" and "hackday login:". Below the description, a SHA1 hash is displayed: "SHA1: E4875224BD7CB4A4F1F9F79E9D63F1F43DB7654C". Below this challenge, another one titled "SkyDog: 2016 - Catch Me If You Can" is partially visible. A cookie consent banner is present in the bottom right corner of the page.

HOME SEARCH HELP RESOURCES BLOG ABOUT

HackDay: Albania

R-73eN 18 Nov 2016

Ubuntu 16.04.1 LTS hackday tty1
hackday login:

This was used in HackDay Albania's 2016 CTF.
The level is beginner to intermediate .
It uses DHCP.

SHA1: E4875224BD7CB4A4F1F9F79E9D63F1F43DB7654C

SkyDog: 2016 - Catch Me If You Can

SkyDog Con CTF 2016 - Catch Me If You Can

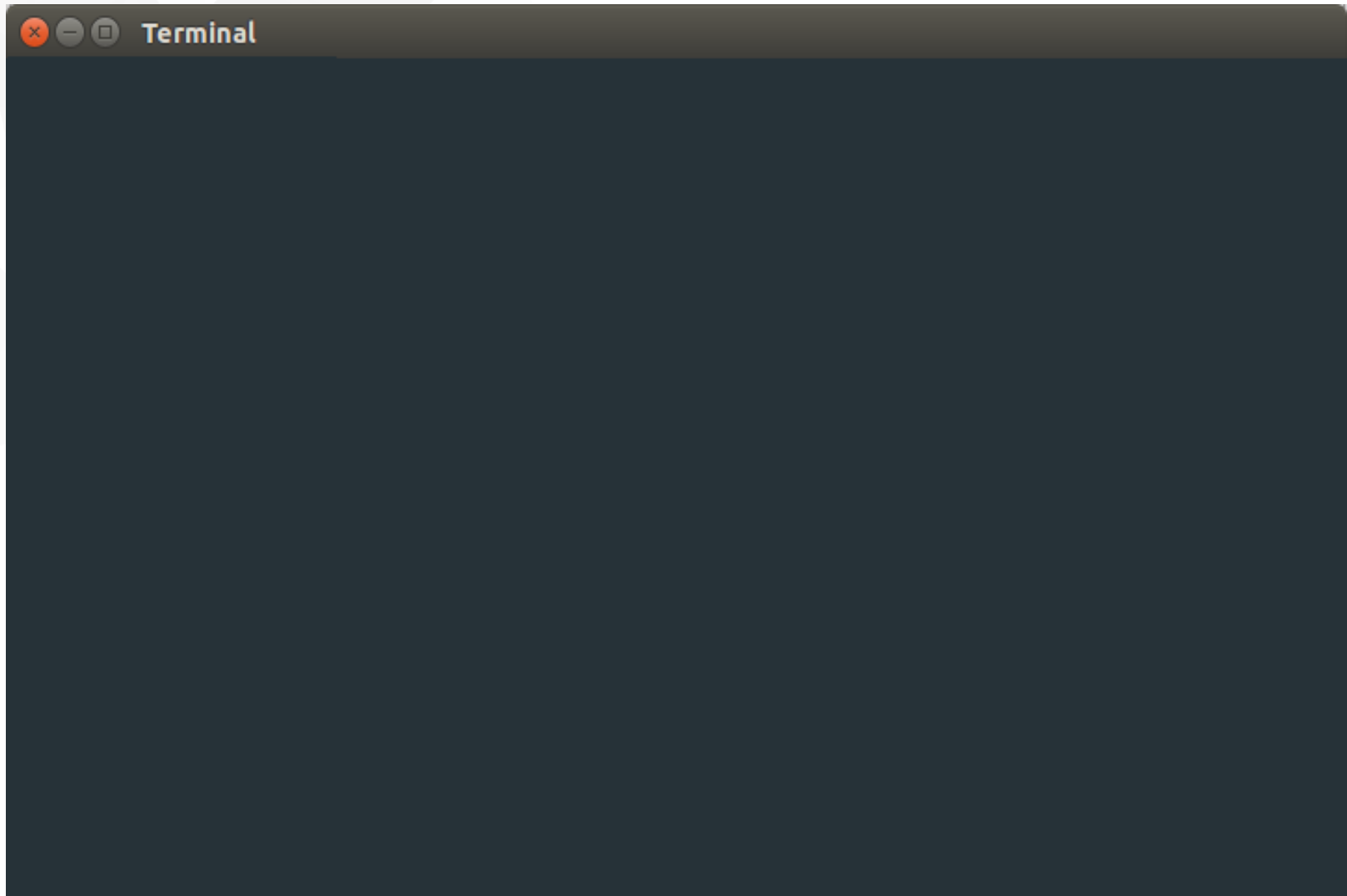
This website uses 'cookies' to give you the best, most relevant experience. Using this website means you're happy with this. You can find out more about the cookies used by clicking this [link](#) (or by clicking the 'Privacy Policy' link at the top of any page). [\[ok\]](#)

Root me

The screenshot shows the Root Me website interface. On the left is a dark sidebar with navigation links: Capture The Flag, Challenges, Community, Docs, Informations, and Tools. Below these links, it states '179 visitors now' and lists newest members: Augustin ROULIER yns06, chiboub Trikul geoff, and Kemanthe. A chatbox section shows a user profile for 'izutao' with the timestamp '30 November 2016 at 17:03'. The main content area has a top navigation bar with icons for help, users, messages, a heartbeat, a shopping cart, and a search bar. Below this is a breadcrumb trail: HOME / CAPTURE THE FLAG / CTF ALL THE DAY. The main heading is 'CTF all the day' with a flag icon. The text describes the goal: 'Improve your hacking skills in a realistic environment where the goal is to fully compromise, « root » the host !'. It explains that users face a vulnerable environment and must find vulnerabilities. A small skull and crossbones icon is on the right. Below, it lists game rules: each player votes for a virtual environment, games start when all players are ready, the virtual environment is at ctf0X.root-me.org, and games stop when a validation flag is used or time runs out. The 'Available rooms' section contains a table with columns: Room, Virtual machine chosen by players, State, and Attackers count.

Room	Virtual machine chosen by players	State	Attackers count
ctf01	Flick 1	running <small>Time remaining : 01:35:33</small>	1 <small>akaikuro77</small>
ctf02	Ultimate I AMP	running	2

Kawan setia anda: terminal



Beberapa perintah di Linux yang mungkin digunakan di CTF

- ▼ cd
- ▼ ls
- ▼ ssh
- ▼ cat
- ▼ file
- ▼ |
- ▼ grep
- ▼ find

Beberapa perintah di Linux yang mungkin digunakan di CTF

- ▼ sort
- ▼ tr
- ▼ tar
- ▼ gzip
- ▼ bzip
- ▼ xxd
- ▼ strings
- ▼ telnet
- ▼ nc
- ▼ openssl

Beberapa perintah di Linux yang mungkin digunakan di CTF

- ▼ s_client
- ▼ nmap

man command

- ▼ Perintah-perintah berikut ini penjelasannya disederhanakan bila ingin penjelasan panjangnya silakan buka “man nama-perintah” di terminal

cd (change directory)

Fungsi: pindah ke direktori lain di Linux

Contoh:

```
cd ..
```

```
cd nama-folder/
```

```
cd /
```

```
cd ~
```

ls

Fungsi:

menampilkan daftar file dan direktori di dalam sebuah direktori

Contoh:

```
ls .
```

```
ls ..
```

```
ls
```

```
ls -al .
```

ssh

Digunakan untuk mengendalikan sistem dari jarak jauh. Penggunaan:

ssh **nama-user@alamat-host**

misalnya:

ssh **udin@udin.com**

ssh **ika@10.10.1.55**

cat

Fungsi:
membaca file teks

contoh:
cat nama_file.txt

file

Fungsi:
menentukan jenis file

contoh:
file nama_file.txt

find

Fungsi:

menemukan file-file dengan kriteria pencarian tertentu di dalam sebuah direktori

contoh kriteria pencarian:

- ▼ -user nama-user
- ▼ -perm kode-izin
- ▼ -group nama-group
- ▼ -size: +n: lebih besar dari n; -n: lebih kecil dari n;
n: persis n

find

Contoh:

- ▼ Mencari file dengan ukuran 78 byte, owner rita, lokasi /home/:

```
find /home -size 78c -user rita
```

file

Fungsi:
menentukan jenis file

contoh:
file nama_file.txt

grep

Fungsi:

mencari karakter/ kata yang sesuai dengan masukan dan mencetak baris teks yang mengandungnya

contoh:

```
grep banana teks.txt
```



Fungsi:

menyalurkan output suatu perintah menjadi input dari perintah lain

contoh:

cat teks.txt | grep banana

sort

Fungsi:

mengurutkan baris-baris di teks di dalam suatu file menurut kriteria tertentu

contoh:

```
sort nama_file.txt
```

tr

Fungsi:

mengubah karakter/string tertentu di dalam sebuah teks dengan karakter/string yang baru. tr bekerja dengan redirection < atau pipe | dengan kombinasi perintah lain

contoh:

cat teks.txt | tr a b

- ▼ Artinya mengubah seluruh karakter a di tampilan file teks.txt menjadi huruf b

tr

contoh:

cat teks.txt | tr a-f g-l

- ▼ Artinya mengubah tiap karakter dalam rentang a-f di file teks.txt menjadi karakter dalam rentang gl, misalnya:
a menjadi g, b menjadi h

tar

Fungsi:

memasukkan file-file ke dalam suatu file arsip
bertipe tar

contoh:

memasukkan file: `tar -cf arc.tar file1 file2` atau
mengeluarkan file-file dari arsip: `tar -xf arc.tar`

gzip

Fungsi:

mengompres file ke dalam format gzip

contoh:

kompresi: `gzip -c a > g.gz`

dekompresi: `gunzip -k g.gz`

bzip2

Fungsi:

mengkompresi dan dekompresi file menggunakan algoritma Burrows-Wheeler dan Huffman coding

contoh kompresi:

```
bzip2 nama_file.txt
```

▼ Contoh dekompresi:

```
bzip2 -dk nama_file.bzip
```

Kombinasi tar dengan bzip2 dan gzip

- ▼ `tar -cvjf nama-file.tar.bz2 nama-file.txt`
- ▼ `tar -xvjf nama-file.tar.bz2`
kombinasi kompresi dan dekompresi tar dan bzip2
- ▼ `tar -cvzf nama-file.tar.gz nama-file.txt`
- ▼ `tar -xvzf nama-file.tar.gz`
kombinasi kompresi dan dekompresi tar dan gzip

strings

Fungsi:

membaca karakter yang dapat dibaca dari file

contoh:

strings namafile

xxd

Fungsi:

menampilkan/membuat hexdump (data hexadecimal) dari sebuah file dan sebaliknya

contoh:

menampilkan hexdump: `xxd namafile`

mengembalikan: `xxd -r namafile`



- Gunakan `>` jika ingin menuliskannya ke file

telnet

“The telnet command is used for interactive communication with another host using the TELNET protocol.” - from telnet manual page on linux



▼ Penggunaan:
telnet namahost port



▼ Contoh:
telnet localhost 80

openssl

“OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and related cryptography standards required by them.” - from openssl manual page on linux

nmap

“Nmap (“Network Mapper”) is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts” - from nmap manual page on linux

- ▼
- ▼ Contoh penggunaan:
`nmap -A -T4 scanme.nmap.org`