Report Laboratorio Pentesting

Riccardo Bruzzese

**INDICE**

[**1.Strumenti che ho utilizzato per la penetrazione delle macchine**](#_h769t4q644u5) **2**

[1.1 Profilo VPN](#_mbgsxe2fcxvm) 2

[1.2 Software utilizzati per queste macchine: ssh2john, Dirbuster , JohnTheRipper, Exiftool e steghide](#_m3zcssqpn1k3) 2

[1.3 Siti che sono stati utilizzati per il Capture the Flag](#_pvzqx6scul44) 2

[**2. Scopo di questo laboratorio**](#_qoipjgsgm6wp) **3**

[**3. Introduzione e Prima sottorete 192.168.10.0/24**](#_3g0726ydzfi0) **4**

[3.1. Macchina 192.168.10.10](#_nm8kypmbonze) 5

[3.1.2 Considerazioni della macchina 192.168.10.10](#_bmgvg4i74xfm) 9

[3.2 Macchina 192.168.10.20](#_1zky55amxlat) 9

[3.2.2 Considerazioni della macchina 192.168.10.20](#_rw8fchgyvp7m) 11

[4. Macchine della seconda rete 192.168.20.0/24](#_c0jdse1xaihp) **12**

[4.1 Prima macchina della seconda sottorete 192.168.20.10](#_xuce2es03264) 12

[4.1.2 Considerazioni della macchina 192.168.20.10](#_tffyakh1t3ld) 17

[4.2 Seconda macchina della seconda sottorete 192.168.20.20](#_c05w5ljo4yri) 17

[**4.3 Ultima macchina 192.168.20.30**](#_458qlngsnvko) **19**

[4.3.3 Considerazioni della macchina 192.168.20.30](#_krd3bk44w1ar) 25

[**5.Conclusioni**](#_a8km3aibtoh5) **25**

# **1.Strumenti che ho utilizzato per la penetrazione delle macchine**

## ***1.1 Profilo VPN***

per effettuare la connessione alle dovute macchine della sottorete 192.168.10.0/24 e 192.168.20.0/24

## ***1.2 Software utilizzati per queste macchine: ssh2john, Dirbuster , JohnTheRipper, Exiftool e steghide***

ssh2john è stato utilizzato per fare riconoscere la chiave rsa .key.private.bak a JohnTheRipper mentre quest’ultimo è stato utilizzato per crackare la chiave private di root e quindi ottenerla. Dirbuster è stato fondamentale per questa esperienza per il motivo che è stato essenziale per lo scanning della macchina e attraverso esso abbiamo trovato diversi indizi come nel caso della macchina di max@192.168.20.10 che abbiamo trovato il file codebreakers.

Exiftool è stato utilizzato per caricare la shell nell’immagine sobs.jpg per poi entrare nella macchina di Karl.  
Steghide è stato utilizzato per la steganografia e attraverso la passphrase siamo riusciti a trovare la password di Max

## ***1.3 Siti che sono stati utilizzati per il Capture the Flag***

-Base64 (decodifica delle chiavi in base 64)

sito che ho utilizzato per le chiavi di Karl, Thomas e Max

-Base32 (decodifica della chiave in base32)

sito che ho utilizzato per la chiave di Alice per la macchina 192.168.20.20 -Cryptii (cifrario di cesare)

essenziale per trovare la chiave cifrata di Thomas

# ***2.* Scopo di questo laboratorio**

Ci sono state assegnate 5 macchine da bucare in particolare:

Prima sottorete (192.168.10.0/24):

* 192.168.10.10
* 192.168.10.20

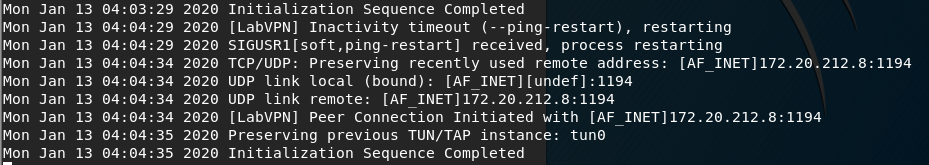
Seconda sottorete (192.168.20.0/24):

* 192.168.20.10
* 192.168.20.20
* 192.168.20.30

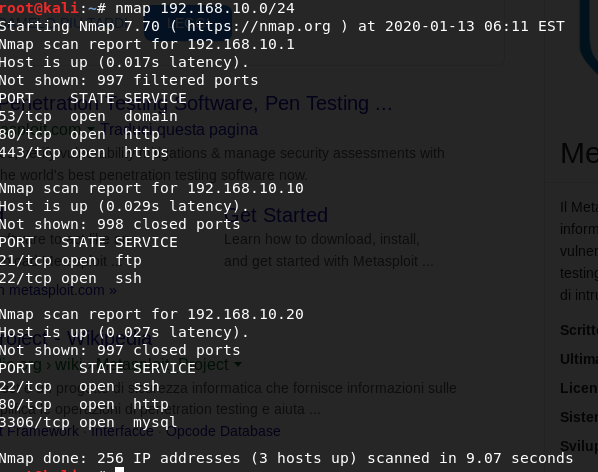
L’ obiettivo di questo laboratorio era di trovare le flag che si situavano in queste 5 macchine. Le rispettive flag si trovavano in /Desktop/flag.txt sia dell’utente a cui ci collegavamo e sia anche di root. Per scovare la flag di root si doveva applicare un privilege escalation.

# **3. Introduzione e Prima sottorete 192.168.10.0/24**

Dopo aver scaricato e installato correttamente il profilo VPN (riccardob):



Effettuiamo una scansione nmap delle macchine 192.168.10.0/24

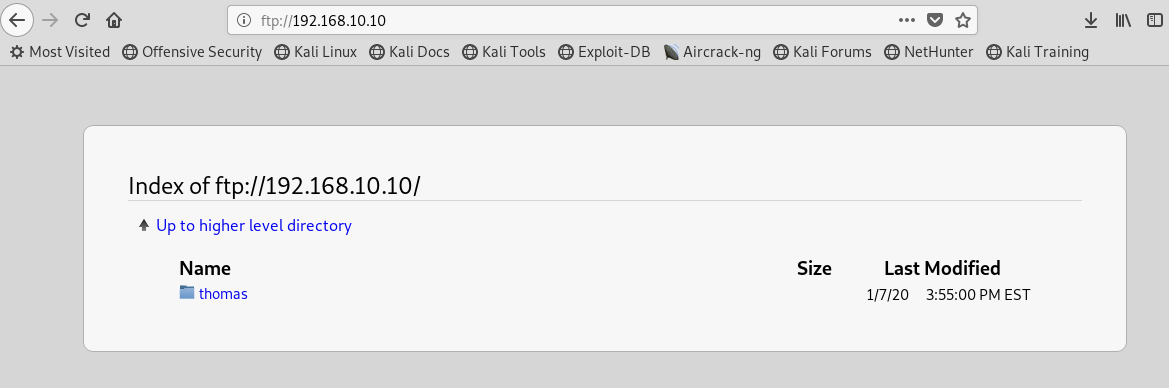


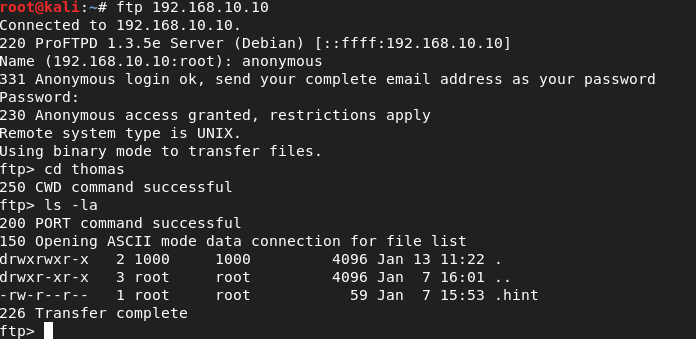
## 

## 

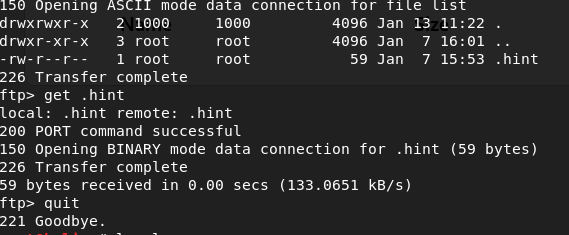
## 3.1. Macchina 192.168.10.10

Attraverso il nmap scopriamo che la macchina 192.168.10.10 dispone di un servizio ftp quindi decido di entrare attraverso Firefox:

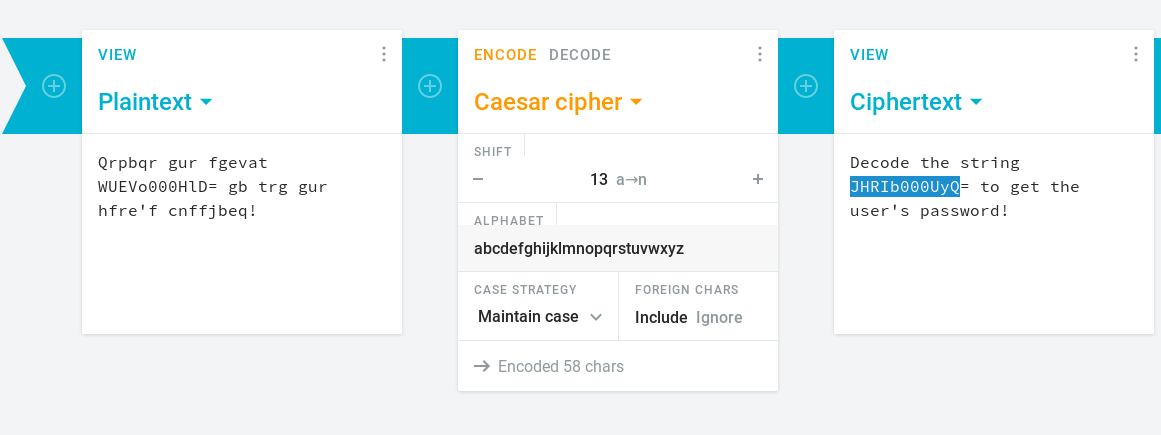
  
come si può vedere attraverso il browser scopriamo in nome utente thomas

Successivamente abbiamo effettuato l’accesso attraverso la macchina con l’utente anonymous 

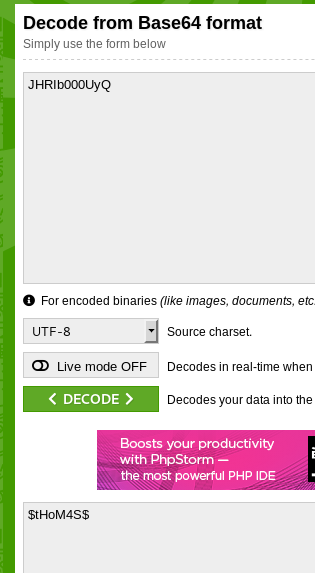
e troviamo il nostro primo indizio .hint

Otteniamo l’ .hint attraverso la richiesta get 

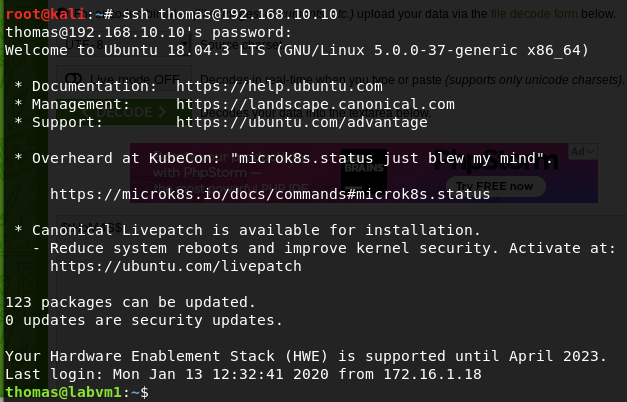
Successivamente facciamo un cat dell’indizio .hint

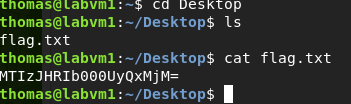


Attraverso il sito <https://cryptii.com/pipes/caesar-cipher> che ci dispone del cifrario di Cesare otteniamo la chiave cifrata di thomas

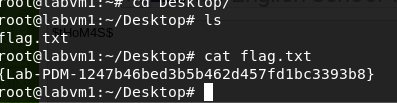


con base 64 decifriamo la chiave cifrata ed otteniamo la chiave ssh di Thomas





effettuiamo la connessione ssh thomas@192.168.10.10 e con il cat flag.txt della cartella Desktop troviamo la prima flag.txt



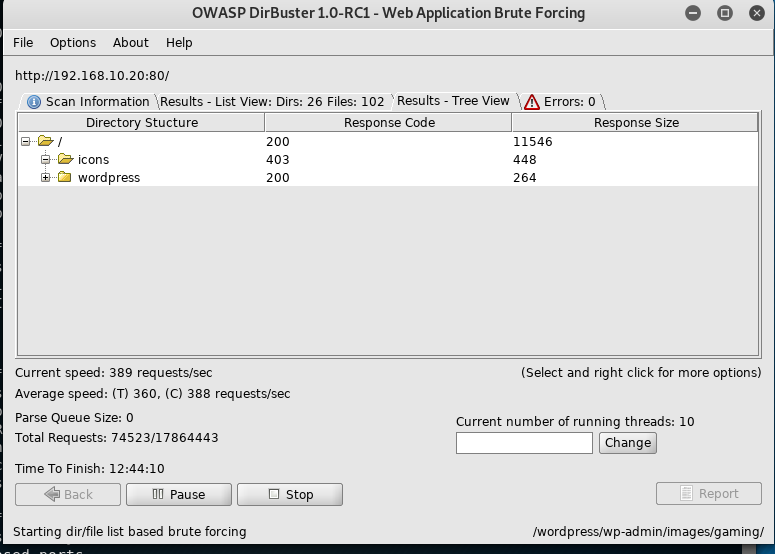
Attraverso il semplice comando sudo su diventiamo root e con il cat flag.txt troviamo la flag di root

### **3.1.2 Considerazioni della macchina 192.168.10.10**

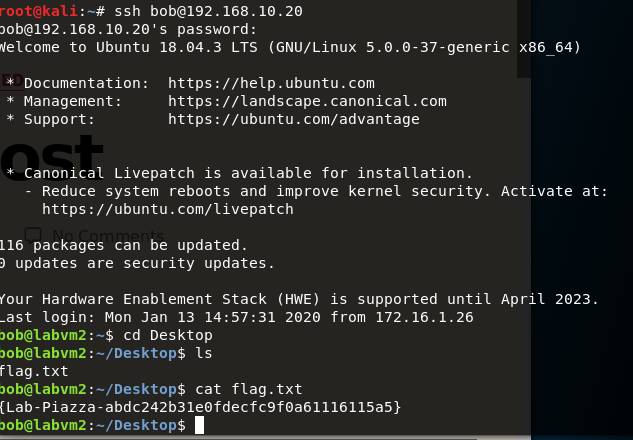
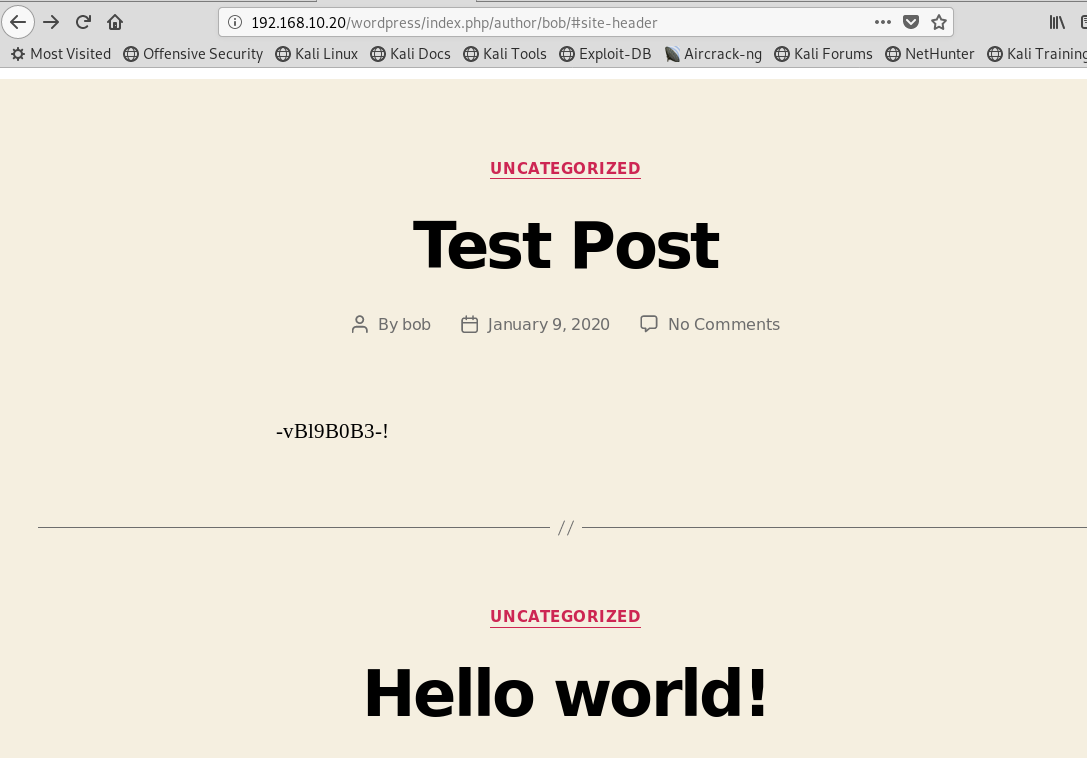
La macchina è stata abbastanza facile da bucare. L’unico punto che è ho riscontrato difficoltà è stato trovare il sito per cifrare il file .hint e quindi sapere che la chiave che aveva utilizzato per quel cifrario era 13.

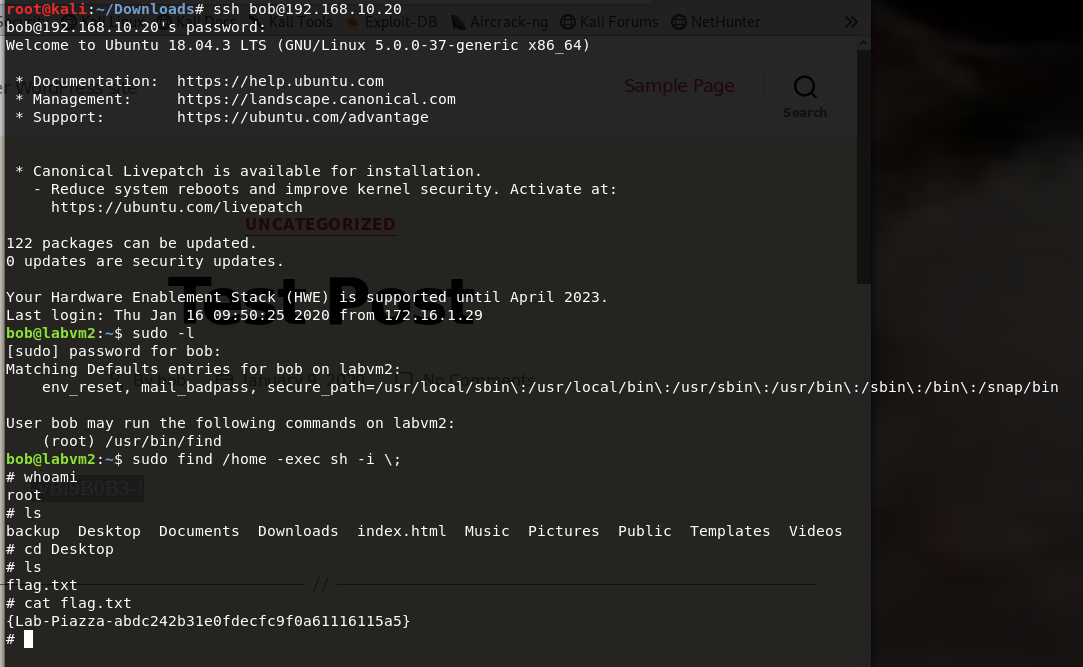
## **3.2 Macchina 192.168.10.20**

Attraverso il dirbuster della macchina 192.168.10.20 abbiamo trovato la cartella wordpress



Attraverso esso Firefox e siamo riusciti a trovare l’utente bob e anche la chiave in chiaro ssh

quindi attraverso esso abbiamo trovato la flag di bob



per la privilege escalation abbiamo fatto il comando sudo -l per vedere quali comando poteva effettuare per diventare root. Successivamente con il comando sudo find /home -exec sh -i \; diventiamo root e otteniamo anche la flag di root

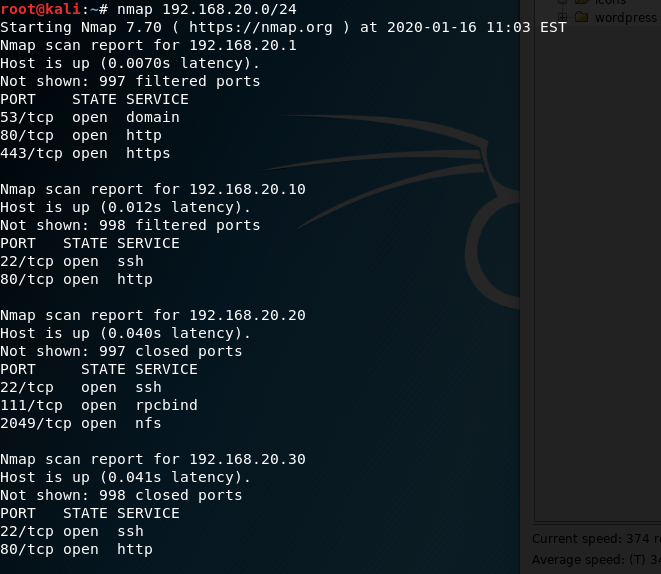
### 3.2.2 Considerazioni della macchina 192.168.10.20

Reputo che questa sia la macchina più facile da bucare a mio avviso. La password era in chiaro nonostante il privilage escalation era più “complicato” della macchina 192.168.10.10

# **4. Macchine della seconda rete 192.168.20.0/24**

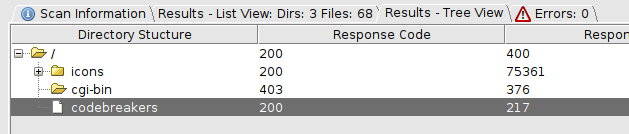
Ora si fa un pò più sul serio. Le macchine della seconda sottorete sono state molto più complesse a livello della prima sottorete.

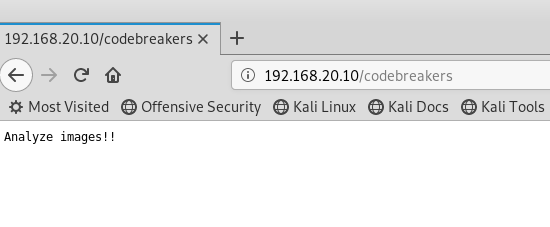
--Stessa procedura della prima sottorete quindi “Nmap delle macchine della seconda subnet” :

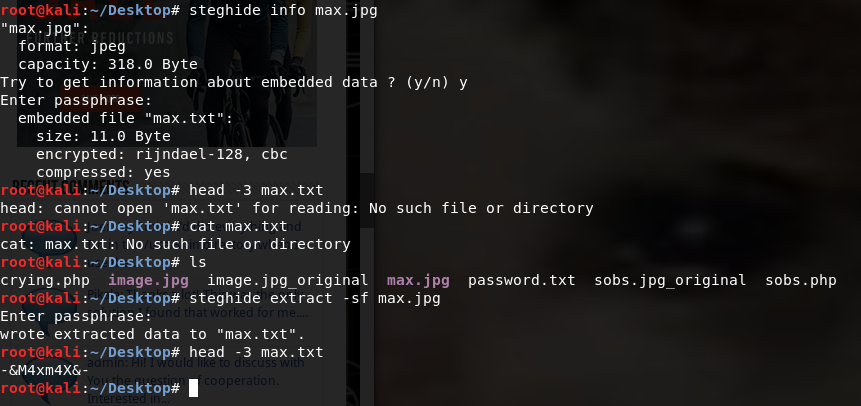


## **4.1 Prima macchina della seconda sottorete 192.168.20.10**

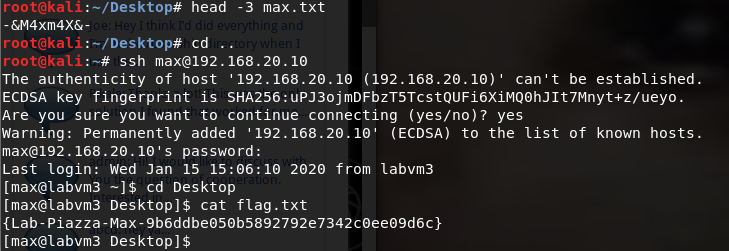
Dal dirbsuter notiamo che c’è un file codebreakers che ci offre un indizio di analizzare le immagini



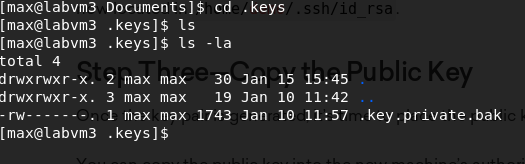


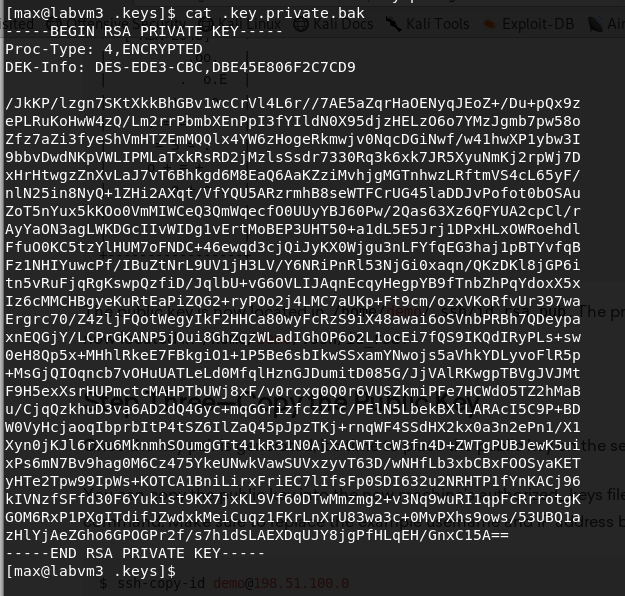
Documentandomi ho notato che per analizzare l’immagine avevo bisogno di un tool per la steganografia: steghide eseguendo il comando info di max.jpg ci chiedeva la passphrase:

La passphrase era l’indizio codebreakers che abbiamo trovato attraverso il dirbuster

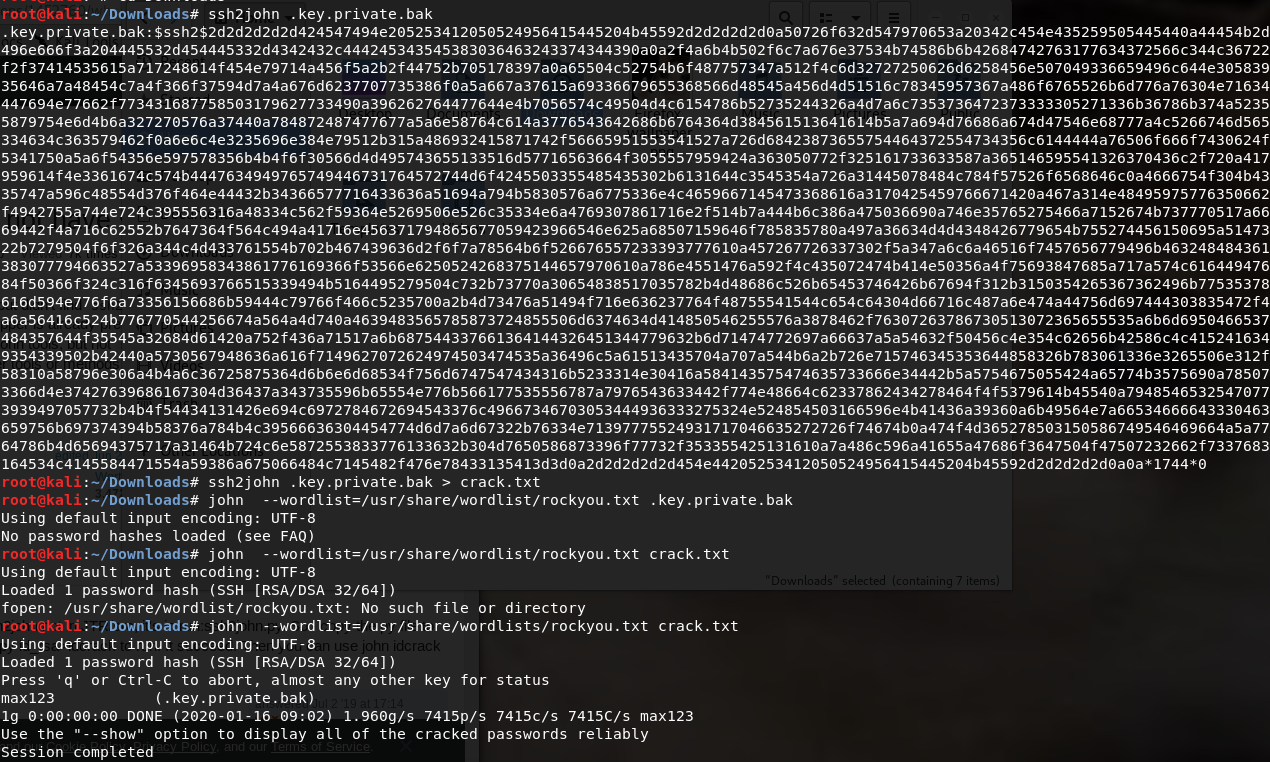
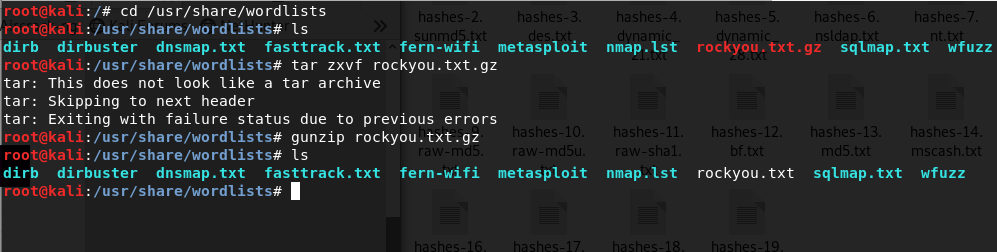
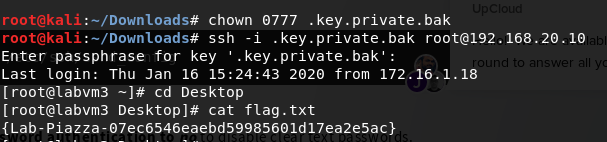
con la password abbiamo fatto l’accesso a max attraverso ssh e quindi anche trovato la flag dell’utente max

Successivamente navigando nelle cartelle abbiamo trovato in Documents un file nascosto .keys





Attraverso un cat scopriamo che una chiave privata in RSA e per decifrarla ci serviva john quindi abbiamo utilizzato gunzip per il file rockyou (wordlist che serve a john )

utilizziamo ssh2john in modo da essere riconoscibile a john The Ripper e successivamente la crackiamo con John The Ripper applicando le wordlist che abbiamo unzippato

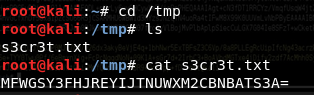
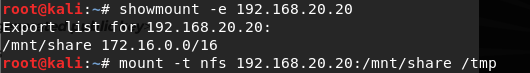
modifichiamo i permessi perchè disponeva di permessi troppo elevati quindi abbiamo messo un 0777 quindi sia utente che root poteva accedere a quella chiave.  
Successivamente effettuiamo la connessione ssh utilizzando come chiave privata max123 e riusciamo accedere alla macchina di max e quindi ottenere la flag anche di root.

### **4.1.2 Considerazioni della macchina 192.168.20.10**

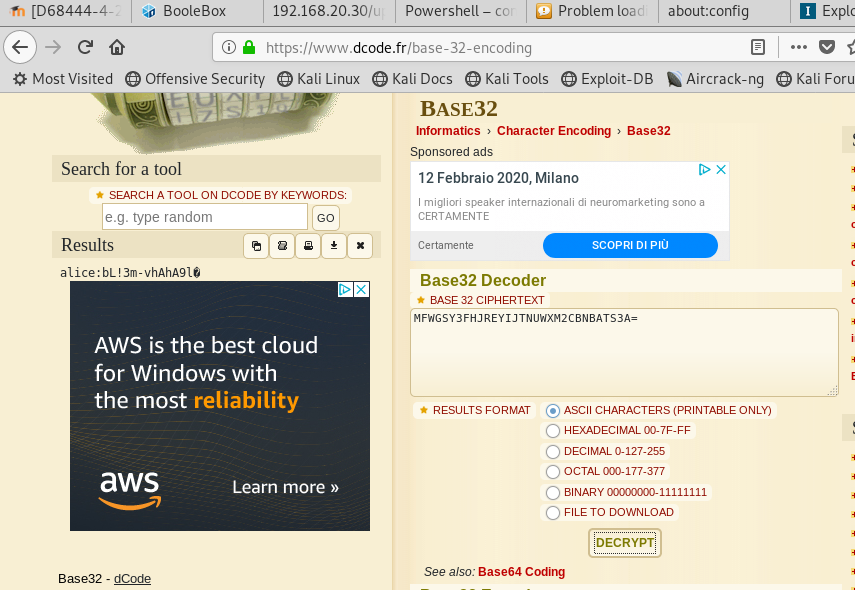
Finora la macchina più complessa per quanto riguarda la privilage escalation. Ho avuto parecchie difficoltà nel rendere riconoscibile la chiave a john per tutto il resto anche per la steganografia è stata la mia prima esperienza quindi è stato molto interessante bucare questa macchina.

## **4.2 Seconda macchina della seconda sottorete 192.168.20.20**

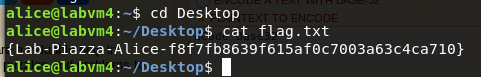
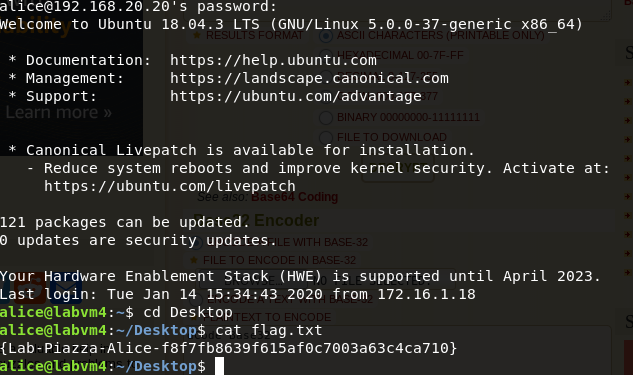
La macchina 192.168.20.20 disponeva del servizio NFS quindi sono partito subito con lo showmount della macchina 192.168.20.20

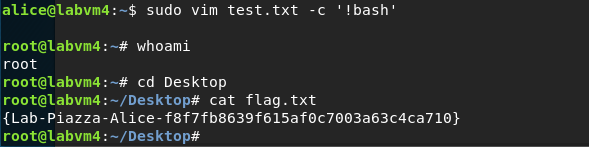


effettuo il mount e nella shared e noto che c’è il primo indizio della macchina 192.168.20.20



attraverso il base 32 troviamo le credenziali di alice per entrare nella macchina 192.168.20.20 in ssh

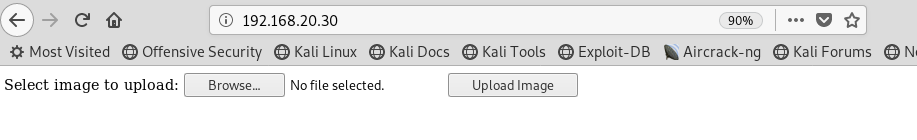
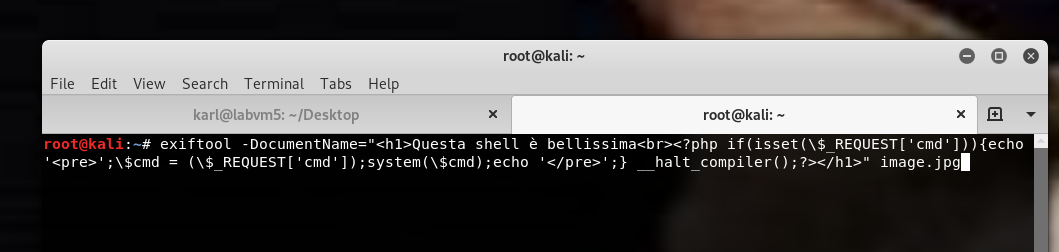
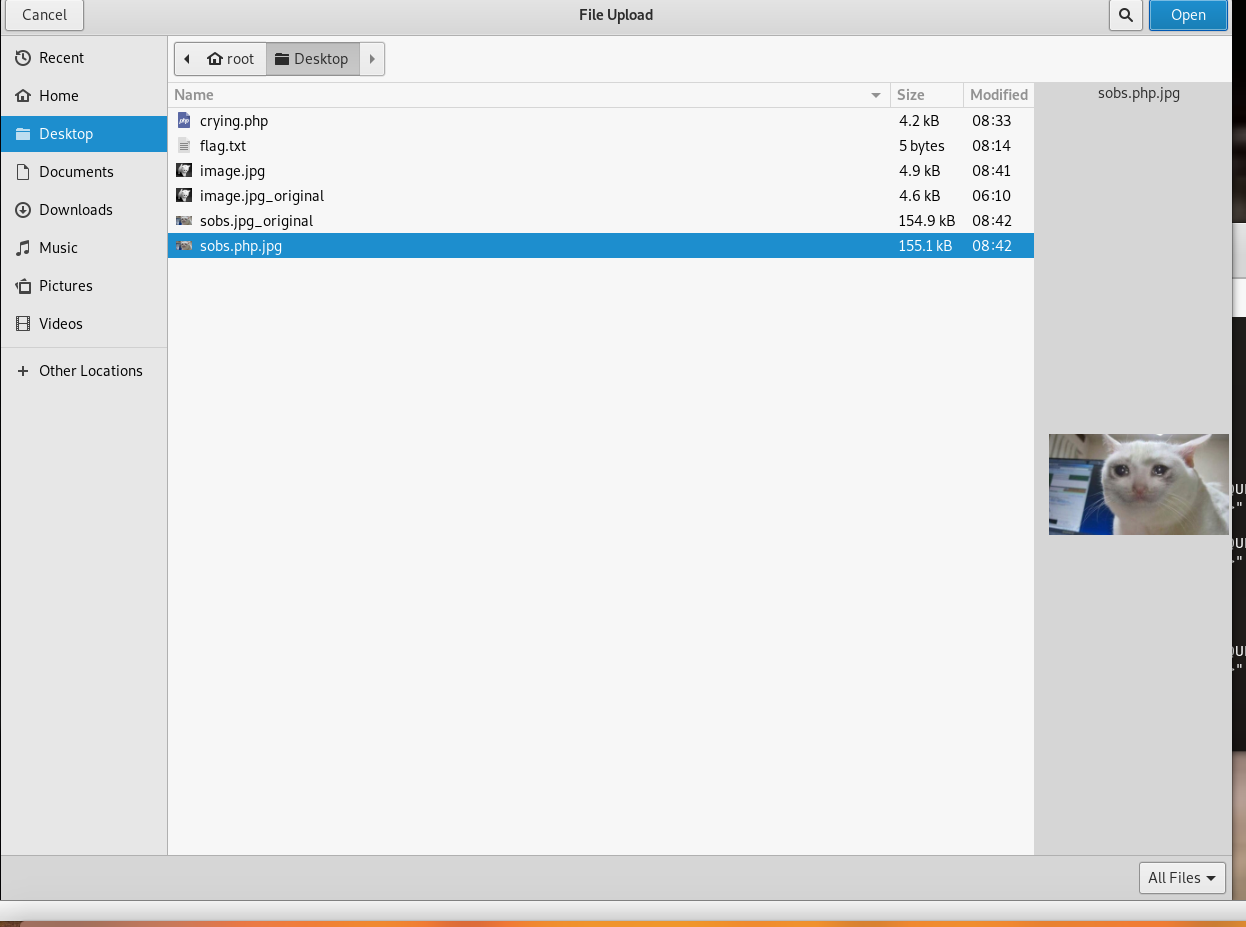
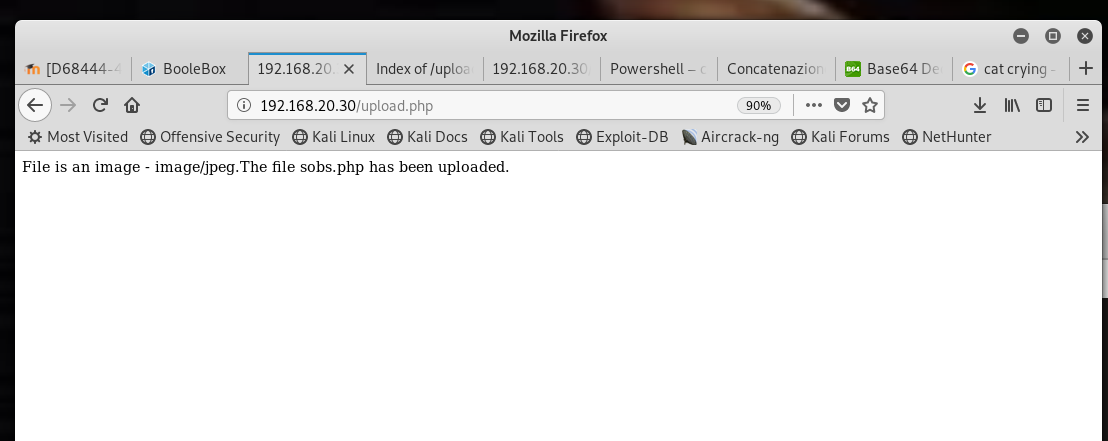
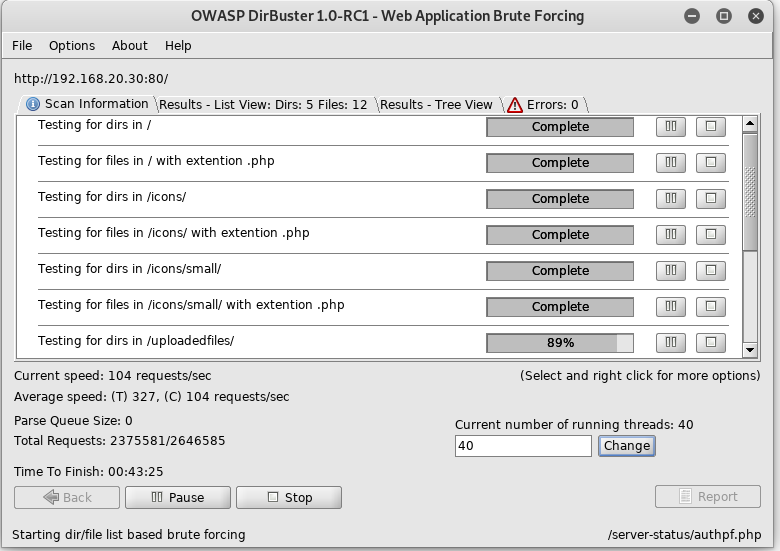


effettuando il ssh troviamo la flag di alice. Subito dopo effettuiamo il comando sudo -l e notiamo che alice possiamo diventare root attraverso il text editor Vim 

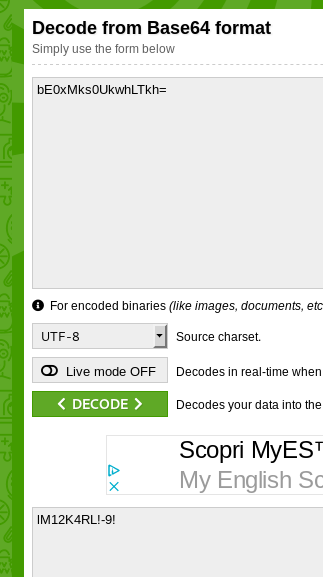
Otteniamo la root attraverso un semplice script in bash e con esso anche la flag.txt

# **4.3 Ultima macchina 192.168.20.30**

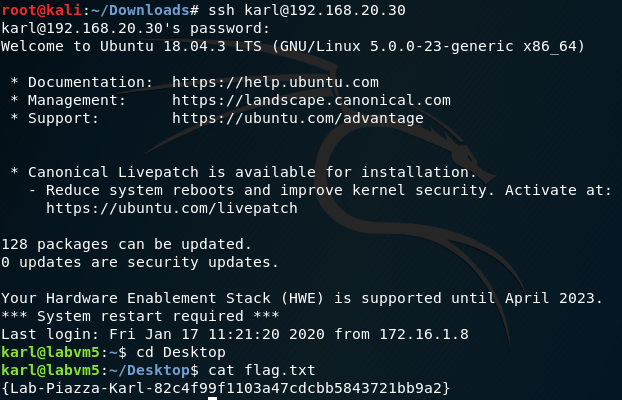
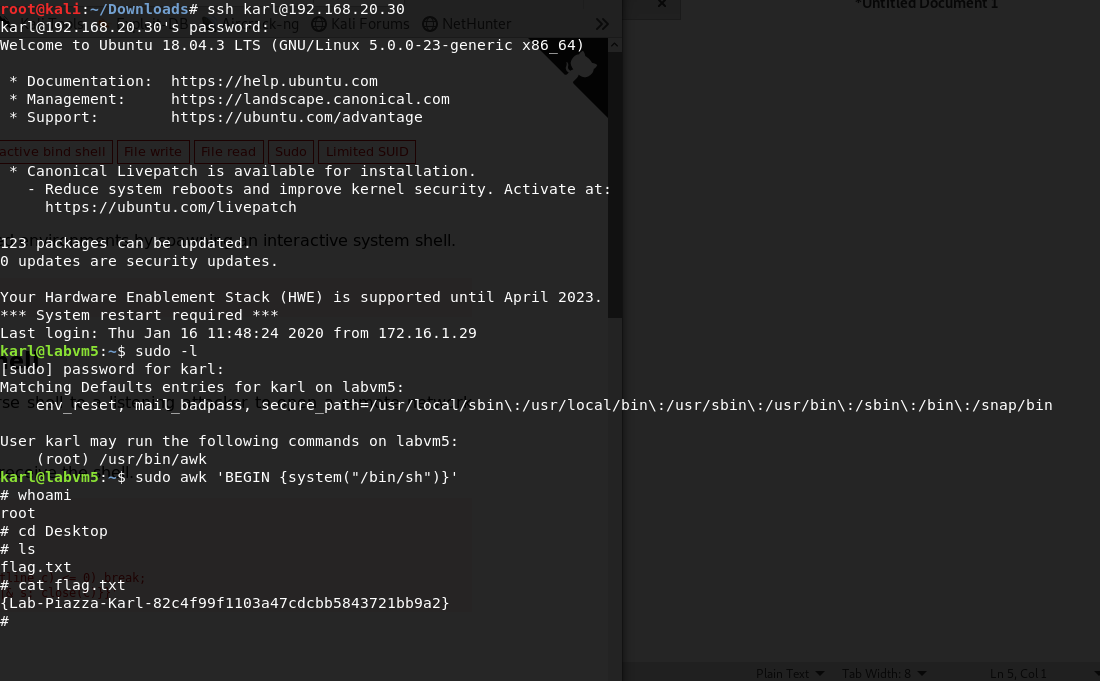
# 

Il sito si presenta così quindi la soluzione molto più probabile era quella di inserire una shell dentro una immagine ed eseguirla in modo da entrare dentro la macchina e ottenere la chiave e poi successivamente attraverso ssh entrare in root.Attraverso il tool exiftool inseriamo la nostra shell nell’immagine e successivamente facciamo un mv del file e gli cambiamo l’estensione in phpcarichiamo la nostra immagine nel sitoCaricata la shell utilizziamo dirbuster e attraverso la scansione notiamo che c’è uploadedfiles e attraverso esso troviamo anche la nostra shell di comando sobs.php

Trovata la nostra shell..navigando attraverso i file abbiamo trovato il file e con il comando cat del file user-karl.txt troviamo la password cifrata del nostro utente karl



decifriamo la nostra password cifrata attraverso base64 e accediamo alla connessione ssh

con cd Desktop e cat della flag otteniamo la flag.txtAttraverso il comando sudo -l troviamo che l’utente karl può ottenere root attraverso awk. Documentandomi ho trovato una shell attraverso awk e così ottenendo i privilegi di root e la rispettiva flag.txt

## **4.3.3 Considerazioni della macchina 192.168.20.30**

Macchina molto interessante. La scelta di inserire una shell di comando in un immagine è stata una scelta molto scaltra. Una delle macchine che mi ha incuriosito di più.

# **5.Conclusioni**

Questa esperienza mi ha cresciuto molto soprattutto nella fase di attacco. Molte di queste tecniche non avevo mai provate e riuscire a trovare queste flag è stato molto soddisfacente.