1

Ping sweep để kiểm tra các host online

ip range: 10.11.1.0/24

`nmap -sn 10.11.1.0/24 -oG ping_sweep.txt` Kết quả:

```
kalicloud@320gb-kali-linux-full-options-node:~/tuanlt24/week2$ nmap -sn 10.11.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-25 11:40 +07
Nmap scan report for 10.11.1.5
Host is up (0.25s latency).
Nmap scan report for host8 (10.11.1.8)
Host is up (0.25s latency).
Nmap scan report for 10.11.1.10
Host is up (0.25s latency).
Nmap scan report for 10.11.1.13
Host is up (0.25s latency).
Nmap scan report for 10.11.1.14
Host is up (0.25s latency).
Nmap scan report for sv-dc01.dvcorp.com (10.11.1.20)
Host is up (0.25s latency).
Nmap scan report for sv-file01.svcorp.com (10.11.1.21)
Host is up (0.25s latency).
Nmap scan report for svclient08.svcorp.com (10.11.1.22)
Host is up (0.25s latency).
Nmap scan report for svclient73.svcorp.com (10.11.1.24)
Host is up (0.25s latency).
Nmap scan report for pippip (10.11.1.31)
Host is up (0.25s latency).
Nmap scan report for 10.11.1.35
Host is up (0.25s latency).
Nmap scan report for 10.11.1.39
Host is up (0.25s latency).
Nmap scan report for 10.11.1.44
Host is up (0.25s latency).
Nmap scan report for 10.11.1.50
Host is up (0.25s latency).
Nmap scan report for 10.11.1.71
Host is up (0.25s latency).
Nmap scan report for 10.11.1.72
Host is up (0.25s latency).
Nmap scan report for 10.11.1.101
Host is up (0.25s latency).
Nmap scan report for 10.11.1.111
Host is up (0.25s latency).
Nmap scan report for 10.11.1.115
Host is up (0.25s latency).
Nmap scan report for 10.11.1.116
Host is up (0.25s latency).
Nmap scan report for xor-dc01.xor.com (10.11.1.120)
Host is up (0.25s latency).
Nmap scan report for xor-app23.xor.com (10.11.1.121)
Host is up (0.25s latency).
Nmap scan report for xor-app07.xor.com (10.11.1.122)
Host is up (0.25s latency).
Nmap scan report for xor-app59.xor.com (10.11.1.123)
Host is up (0.25s latency).
Nmap scan report for 10.11.1.128
Host is up (0.25s latency).
Nmap scan report for 10.11.1.133
Host is up (0.25s latency).
Nmap scan report for 10.11.1.136
Host is up (0.25s latency).
Nmap scan report for 10.11.1.141
```

Lưu vào file

```
nmap -sn -oG ping_sweep.txt 10.11.1.0/24
```

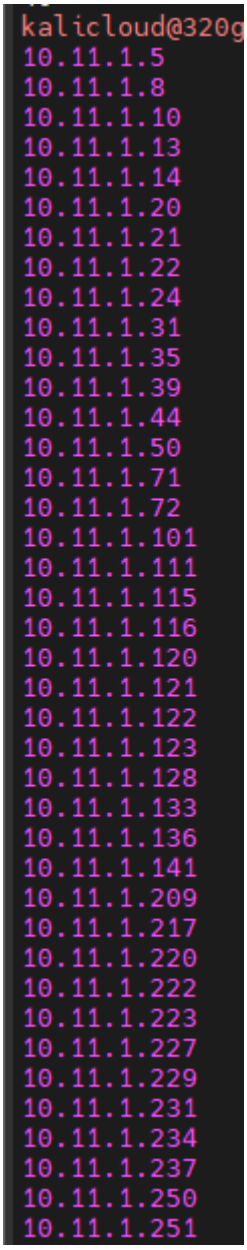
Kết quả cat ping_sweep.txt

```
kalicloud@320gb-kali-linux-full-options-node:~/tuanlt24/week2$ cat ping_sweep.txt
# Nmap 7.80 scan initiated Thu Aug 25 11:44:26 2022 as: nmap -sn -oG ping_sweep.txt 10.11.1.0/24
Host: 10.11.1.5 ()      Status: Up
Host: 10.11.1.8 (host8) Status: Up
Host: 10.11.1.10 ()     Status: Up
Host: 10.11.1.13 ()     Status: Up
Host: 10.11.1.14 ()     Status: Up
Host: 10.11.1.20 (sv-dc01.dvcorp.com)   Status: Up
Host: 10.11.1.21 (sv-file01.svcorp.com) Status: Up
Host: 10.11.1.22 (svclient08.svcorp.com)        Status: Up
Host: 10.11.1.24 (svclient73.svcorp.com)        Status: Up
Host: 10.11.1.31 (pippip)       Status: Up
Host: 10.11.1.35 ()     Status: Up
Host: 10.11.1.39 ()     Status: Up
Host: 10.11.1.44 ()     Status: Up
Host: 10.11.1.50 ()     Status: Up
Host: 10.11.1.71 ()     Status: Up
Host: 10.11.1.72 ()     Status: Up
Host: 10.11.1.101 ()    Status: Up
Host: 10.11.1.111 ()    Status: Up
Host: 10.11.1.115 ()    Status: Up
Host: 10.11.1.116 ()    Status: Up
Host: 10.11.1.120 (xor-dc01.xor.com)    Status: Up
Host: 10.11.1.121 (xor-app23.xor.com)   Status: Up
Host: 10.11.1.122 (xor-app07.xor.com)   Status: Up
Host: 10.11.1.123 (xor-app59.xor.com)   Status: Up
Host: 10.11.1.128 ()    Status: Up
Host: 10.11.1.133 ()    Status: Up
Host: 10.11.1.136 ()    Status: Up
Host: 10.11.1.141 ()    Status: Up
Host: 10.11.1.209 ()    Status: Up
Host: 10.11.1.217 ()    Status: Up
Host: 10.11.1.220 (thinc)       Status: Up
Host: 10.11.1.222 ()    Status: Up
Host: 10.11.1.223 ()    Status: Up
Host: 10.11.1.227 ()    Status: Up
Host: 10.11.1.229 ()    Status: Up
Host: 10.11.1.231 ()    Status: Up
Host: 10.11.1.234 (core)        Status: Up
Host: 10.11.1.237 ()    Status: Up
Host: 10.11.1.250 (sandbox.local)       Status: Up
Host: 10.11.1.251 ()    Status: Up
# Nmap done at Thu Aug 25 11:44:31 2022 -- 256 IP addresses (40 hosts up) scanned in 4.61 seconds
```

Dùng grep để show kết quả các host up

```
cat ping_sweep.txt|grep Up | awk '{print $2}'
```

kết quả:



2 Scan các ip tìm được ở bài 1 để tìm webserver ports. Dùng nmap để xác định phiên bản webserver và os

Kiểm tra các port 80.443 để kiểm tra host nào có dịch vụ webserver đang bật, lưu vào file webserver_mining.txt:

```
nmap -p 80,443 10.11.1.0/24 -oG webserver_mining.txt
```

```
root@320gb-kali-linux-full-options-node:/home/kalicloud/tuanlt24/week2# cat webserver_mining.txt
# Nmap 7.80 scan initiated Thu Aug 25 16:22:26 2022 as: nmap -iL iplist.txt -p 80,443 -sV -oG webserver_mining.txt
Host: 10.11.1.5 ()      Status: Up
Host: 10.11.1.5 ()      Ports: 80/closed/tcp//http///, 443/closed/tcp//https///
Host: 10.11.1.8 (host8) Status: Up
Host: 10.11.1.8 (host8) Ports: 80/open/tcp//http//Apache httpd 2.0.52 ((CentOS))/, 443/open/tcp//ssl|http//Apache httpd 2.0.52 ((CentOS))/
Host: 10.11.1.10 ()     Status: Up
Host: 10.11.1.10 ()     Ports: 80/open/tcp//http//Microsoft IIS httpd 6.0/, 443/filtered/tcp//https///
Host: 10.11.1.13 ()     Status: Up
Host: 10.11.1.13 ()     Ports: 80/closed/tcp//http///, 443/closed/tcp//https///
Host: 10.11.1.14 ()     Status: Up
Host: 10.11.1.14 ()     Ports: 80/open/tcp//http//Microsoft IIS httpd 5.1/, 443/open/tcp//https?///
Host: 10.11.1.20 (sv-dc01.dvcorp.com)   Status: Up
Host: 10.11.1.20 (sv-dc01.dvcorp.com)   Ports: 80/closed/tcp//http///, 443/closed/tcp//https///
Host: 10.11.1.21 (sv-file01.svcorp.com) Status: Up
Host: 10.11.1.21 (sv-file01.svcorp.com) Ports: 80/open/tcp//http//Microsoft IIS httpd 10.0/, 443/closed/tcp//https///
Host: 10.11.1.22 (svclient08.svcorp.com)        Status: Up
Host: 10.11.1.22 (svclient08.svcorp.com)        Ports: 80/closed/tcp//http///, 443/closed/tcp//https///
Host: 10.11.1.24 (svclient73.svcorp.com)        Status: Up
Host: 10.11.1.24 (svclient73.svcorp.com)        Ports: 80/closed/tcp//http///, 443/closed/tcp//https///
Host: 10.11.1.31 (pippip)       Status: Up
Host: 10.11.1.31 (pippip)       Ports: 80/open/tcp//http//Microsoft IIS httpd 10.0/, 443/filtered/tcp//https///
Host: 10.11.1.35 ()     Status: Up
Host: 10.11.1.35 ()     Ports: 80/open/tcp//http//Apache httpd 2.4.6 ((CentOS) PHP|5.4.16)/, 443/closed/tcp//https///
Host: 10.11.1.39 ()     Status: Up
Host: 10.11.1.39 ()     Ports: 80/open/tcp//http//nginx 1.6.3/, 443/filtered/tcp//https///
Host: 10.11.1.44 ()     Status: Up
Host: 10.11.1.44 ()     Ports: 80/closed/tcp//http///, 443/closed/tcp//https///
Host: 10.11.1.50 ()     Status: Up
Host: 10.11.1.50 ()     Ports: 80/open/tcp//http//Microsoft IIS httpd 8.5/, 443/filtered/tcp//https///
Host: 10.11.1.71 ()     Status: Up
Host: 10.11.1.71 ()     Ports: 80/open/tcp//http//Apache httpd 2.4.7 ((Ubuntu))/, 443/closed/tcp//https///
Host: 10.11.1.72 ()     Status: Up
Host: 10.11.1.72 ()     Ports: 80/open/tcp//http//Apache httpd 2.2.20 ((Ubuntu))/, 443/closed/tcp//https///
Host: 10.11.1.101 ()    Status: Up
Host: 10.11.1.101 ()    Ports: 80/open/tcp//http//Apache httpd 2.4.18 ((Ubuntu))/, 443/closed/tcp//https///
Host: 10.11.1.111 ()    Status: Up
Host: 10.11.1.111 ()    Ports: 80/closed/tcp//http///, 443/closed/tcp//https///
Host: 10.11.1.115 ()    Status: Up
```

Sau đó lọc các host đang có dịch vụ web open, lưu vào file web_open_ip.txt:

```
cat webserver_mining.txt | grep open | awk '{print $2}' > web_open_ip.txt
```

```
root@320gb-kali-linux-full-options-node:/home/kalicloud/tuanlt24/week2# cat web_open_ip.txt
10.11.1.8
10.11.1.10
10.11.1.14
10.11.1.21
10.11.1.31
10.11.1.35
10.11.1.39
10.11.1.50
10.11.1.71
10.11.1.72
10.11.1.101
10.11.1.115
10.11.1.116
10.11.1.123
10.11.1.133
10.11.1.217
10.11.1.223
10.11.1.227
10.11.1.229
10.11.1.234
10.11.1.237
10.11.1.250
10.11.1.251
```

Scan thông tin OS của các host có webserver đang bật:

```
nmap -O -iL web_open_ip.txt -oG os_detect_raw.txt
```

```
root@320gb-kali-linux-full-options-node:/home/kalicloud/tuanlt24/week2# cat os_detect_raw.normal
# Nmap 7.80 scan initiated Fri Aug 26 17:01:26 2022 as: nmap -iL web_open_ip.txt -oN os_detect_raw.normal -O
Nmap scan report for host8 (10.11.1.8)
Host is up (0.24s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
25/tcp   closed smtp
80/tcp   open   http
111/tcp  open   rpcbind
139/tcp  open   netbios-ssn
443/tcp  open   https
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3306/tcp open   mysql
Device type: firewall|general purpose|proxy server|WAP|PBX|media device|storage-misc
Running (JUST GUESSING): Linux 2.6.X (93%), Cisco embedded (93%), Riverbed embedded (93%), Ruckus embedded (91%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:cisco:sa520 cpe:/o:linux:linux_kernel:2.6.9 cpe:/h:riverbed:steelhe
Aggressive OS guesses: Cisco SA520 firewall (Linux 2.6) (93%), Linux 2.6.9 (CentOS 4.4) (93%), Linux 2.6.9 - 2.6
7363 WAP (91%), Linux 2.6.11 (90%), Linux 2.6.18 (90%)
No exact OS matches for host (test conditions non-ideal).
```

3 Dùng nse script để scan những máy đang chạy smb

```
nmap --script /home/kalicloud/test/smb.nse 10.11.1.0/24 -oN smb_nse.txt
```

Lọc output bằng script:

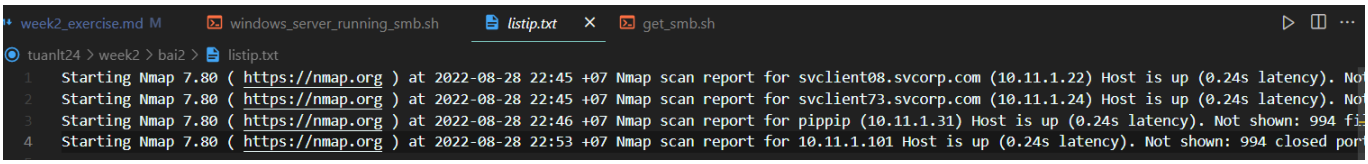
```
#!/bin/bash
for i in {1..254}
do
    output=$(nmap --script /home/kalicloud/test/smb.nse 10.11.1.$i)
    if [[ $output != *"ERROR"* && $output == *"Host script results:"* ]]; then
        printf $output >> smb_scan.txt
    fi
done
```

2

1: lọc các lab chạy windows và smb

```
#!/bin/bash
for i in {1..254}
do
    output=$(nmap --script /home/kalicloud/test/smb.nse 10.11.1.$i)
    if [[ $output != *"ERROR"* && $output == *"Host script results:"* && $output
== *"Windows"* ]]; then
        echo $output | grep "Nmap scan report for" >> listip.txt
    fi
done
```

Kết quả:



2: Scan smb vulner by script nse

Dùng awk lọc các ip từ kết quả lưu vào file listip2.txt

```
cat listip.txt | awk '{print $15}' > listip2.txt
```

Dùng nse script để quét lỗi trên ip đã lọc được

```
nmap --script /usr/share/nmap/scripts/smb-security-mode.nse -iL listip2.txt
```

Kết quả:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-28 23:17 +07
Nmap scan report for svclient08.svcorp.com (10.11.1.22)
Host is up (0.25s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap scan report for svclient73.svcorp.com (10.11.1.24)
Host is up (0.25s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap scan report for pippip (10.11.1.31)
Host is up (0.25s latency).
Not shown: 994 filtered ports
```

```
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
3389/tcp open  ms-wbt-server

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

Scan lỗi ms06-025

```
nmap --script /usr/share/nmap/scripts/smb-vuln-ms06-025.nse -iL listip2.txt -oN
vuln_scan_smb.txt
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-28 23:22 +07
Nmap scan report for svclient08.svcorp.com (10.11.1.22)
Host is up (0.24s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for svclient73.svcorp.com (10.11.1.24)
Host is up (0.24s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for pippip (10.11.1.31)
Host is up (0.24s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
3389/tcp open  ms-wbt-server

Nmap done: 3 IP addresses (3 hosts up) scanned in 61.97 seconds
```

3

1. Scan your target network with onesixtyone to identify any SNMP servers.

```
onesixtyone 10.11.1.0/24
```

Result:

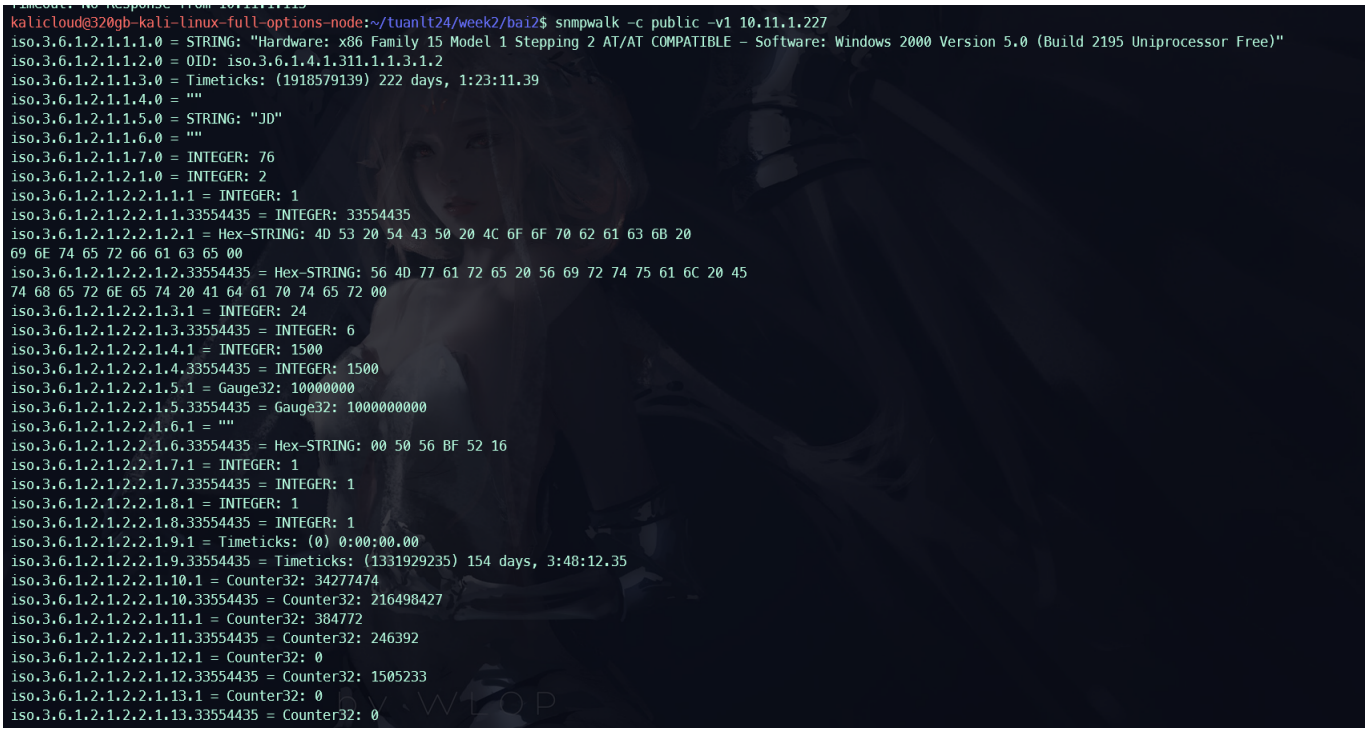
```
Scanning 256 hosts, 2 communities
10.11.1.115 [public] Linux tophat.acme.com 2.4.20-8 #1 Thu Mar 13 17:54:28 EST
2003 i686
10.11.1.227 [public] Hardware: x86 Family 15 Model 1 Stepping 2 AT/AT COMPATIBLE -
Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
```

2. dùng snmpwalk và snmp-check để thu thập thông tin ip tìm được

Thực hiện với ip: 10.11.1.227

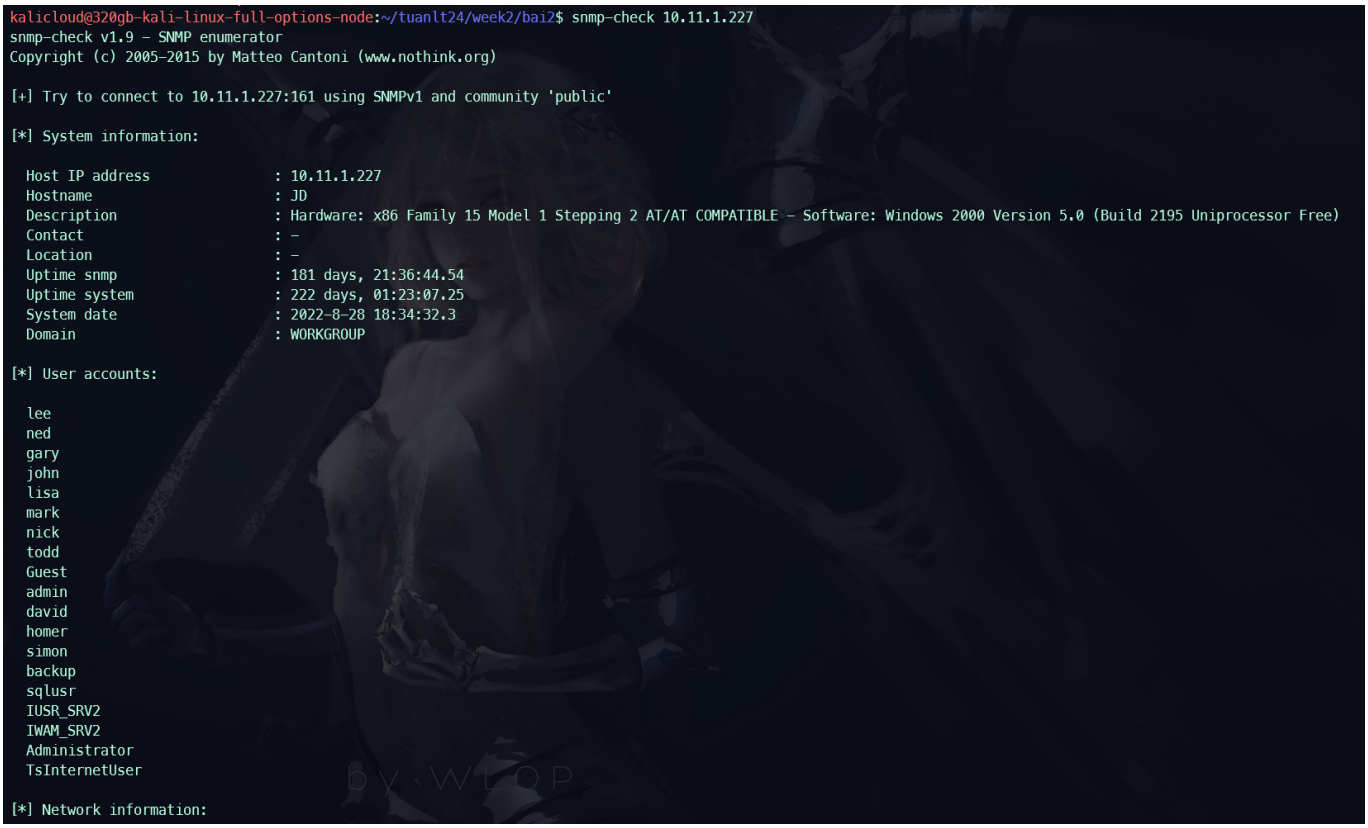
```
snmpwalk -c public -v1 10.11.1.227
```

kết quả:




```
snmp-check 10.11.1.227
```

kết quả:


kalicloud@320gb-kali-linux-full-options-node:~/tuanlt24/week2/bai2$ snmp-check 10.11.1.227
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)
[+] Try to connect to 10.11.1.227:161 using SNMPv1 and community 'public'
[*] System information:
Host IP address : 10.11.1.227
Hostname : JD
Description : Hardware: x86 Family 15 Model 1 Stepping 2 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
Contact : -
Location : -
Uptime snmp : 181 days, 21:36:44.54
Uptime system : 222 days, 01:23:07.25
System date : 2022-8-28 18:34:32.3
Domain : WORKGROUP
[*] User accounts:
lee
ned
gary
john
lisa
mark
nick
todd
Guest
admin
david
homer
simon
backup
sqlusr
IUSR_SRV2
IWAM_SRV2
Administrator
TsInternetUser
[*] Network information: