جامعة سيدي محمد بن عبدالله بفاس
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵙⵉⴷⵉ ⵎⵓⵃⴰⵎⵎⴷ ⴱⵏ ⵄⴱⴷⵍⵍⴰⵀ ⵏ ⴼⴰⵙ
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES
المدرسة العليا للتكنولوجيا
ⵜⵉⵎⵙⵙⵓⵔⵉⵏ ⵜⵉⵏⵏⴰⵢⵏⵜ ⵏ ⵜⵉⴽⵏⵓⵍⵓⵊⵢⵜ
ECOLE SUPÉRIEURE DE TECHNOLOGIE

TP1:Analyse de vulnérabilitées

NOM/PRENOM :

Hasnae Derouich

Département :

Génie informatique

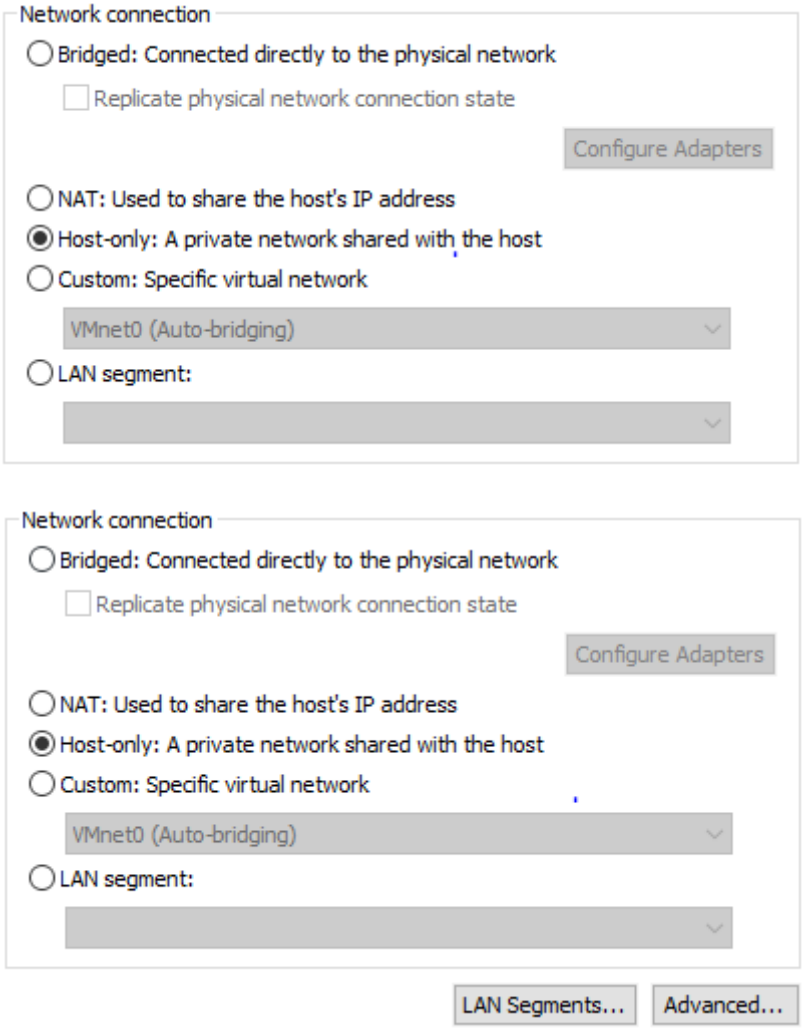
Objectif :

L'objectif de ce TP est la configuration une machine Metaspolotale2 ,en connectant avec une machine Ubuntu pour découvrir de vulnérabilités en utilisant des outils comme Nmap et Nikto .

Année universitaire 2025/2026

2-Configuration Réseau

Configuration de la carte réseau de deux machine en mode Réseau privé hôte 5Host-Only)

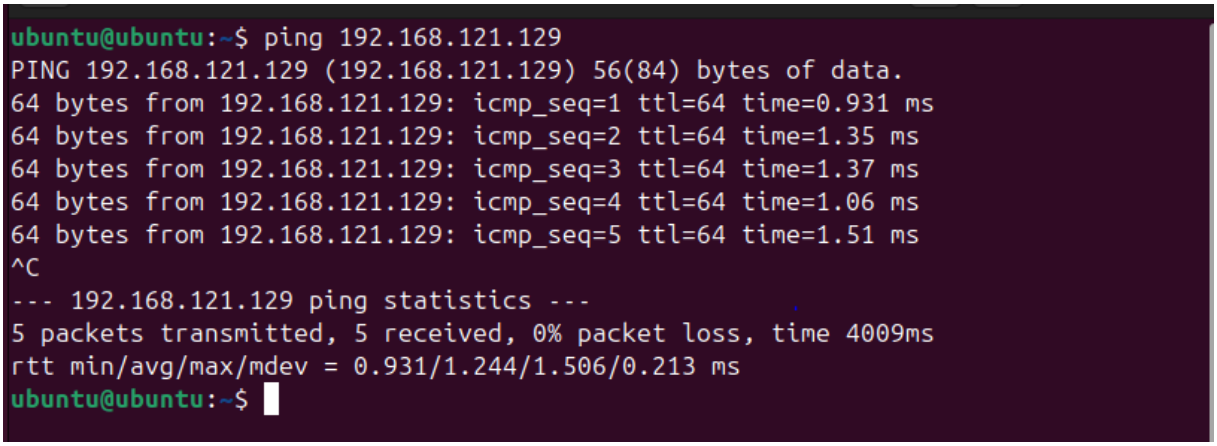


Vérification de la connectivité :

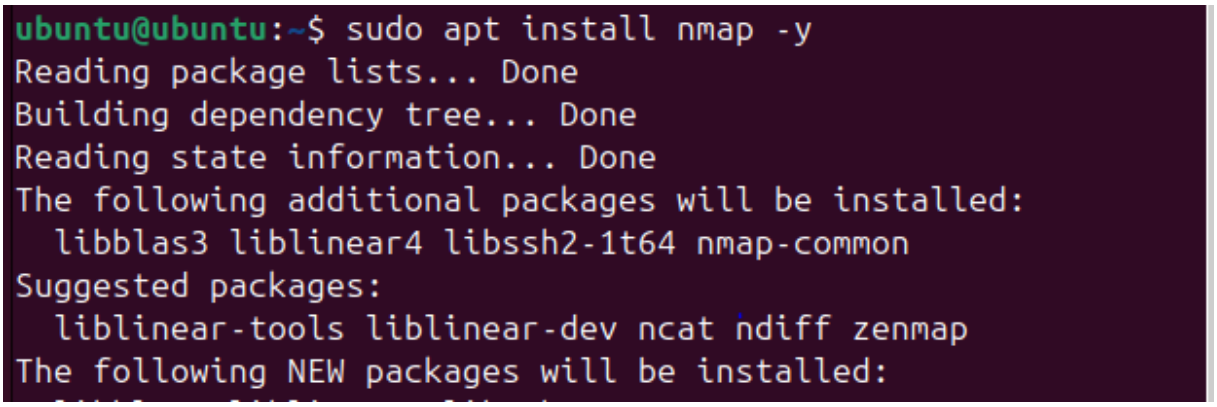
Identifier IP de Metasploitable 2 : 192.168.127.129

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:80:15:c9
          inet addr:192.168.121.129  Bcast:192.168.121.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe80:15c9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3452 (3.3 KB)  TX bytes:8893 (8.6 KB)
          Interrupt:17 Base address:0x2000
```

Un ping depuis Ubuntu vers Metasploitable 2

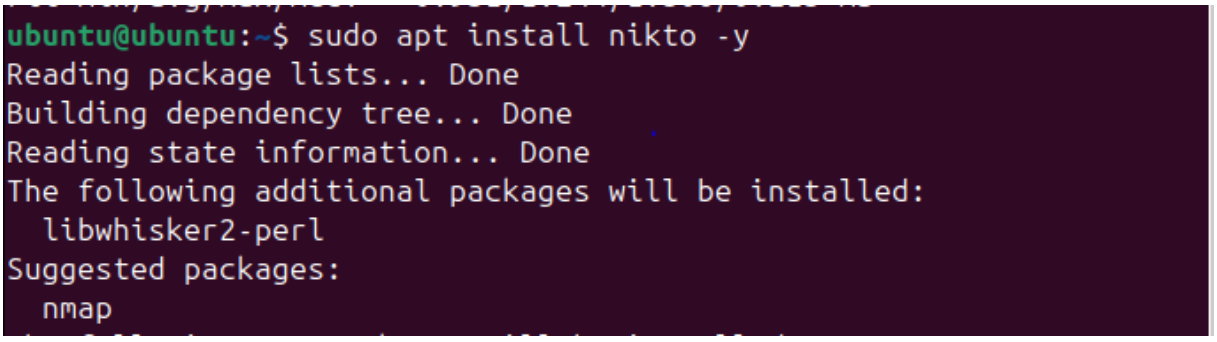


Installer Nmap (outil de scan réseau)



Nmap (Network mapper) est un scanner de ports qui permet d'identifier les machines actives sur un reseau

Installer Nikto (outil de scan web)



Nikto est un scanner de vulnérabilités pour les applications web il détecte les failles connus , les configurations dangereuses et les versions obsolètes des serveurs web

Installer net-tools Contient ifconfig

```
ubuntu@ubuntu:~$ sudo apt install net-tools -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 204 kB of archives.
After this operation, 811 kB of additional disk space will be used.
```

Installer Le client MySQL : utile pour tester la connexion a un serreur MySQL distant

```
ubuntu@ubuntu:~$ sudo apt install mysql-client -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  mysql-client-8.0 mysql-client-core-8.0 mysql-common
The following NEW packages will be installed:
  mysql-client mysql-client-8.0 mysql-client-core-8.0 mysql-common
```

Effectuer un scan rapide des ports ouverts

```
ubuntu@ubuntu:~$ sudo -ss
root@ubuntu:/home/ubuntu# nmap -sS 192.168.121.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 13:19 UTC
Nmap scan report for 192.168.121.129
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
```

```
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:80:15:C9 (VMware)
```

-sS : Effectue un scan furtif SYN il envoie des paquets SYN pour voir si le port répond sans établir complètement la connexion cela permet d'éviter d'être détecté par certains systèmes IDS

2. Quels ports sont ouverts ?

Les ports ouverts sur l'addresse ip 192.168.121.129 sont :

- **21/tcp 22/tcp 23/tcp 25/tcp**
- **53/tcp 80/tcp 111/tcp 139/tcp 445/tcp 512/tcp 513/tcp 514/tcp 1099/tcp 1524/tcp 2049/tcp 2121/tcp 3306/tcp 5432/tcp 5900/tcp 6000/tcp 6667/tcp 8009/tcp 8180/tcp**

3. Quels services tournent sur ces ports ?

- **21/tcp : FTP (File Transfer Protocol)**
- **22/tcp : SSH (Secure Shell)**
- **23/tcp : Telnet**
- **25/tcp : SMTP (Simple Mail Transfer Protocol)**
- **53/tcp : DNS (Domain Name System)**
- **80/tcp : HTTP (Hypertext Transfer Protocol)**
- **513/tcp : login (Remote Login)**
- **514/tcp : shell (Remote Shell)**
- **2049/tcp : NFS (Network File System)**
- **2121/tcp : CCProxy-FTP (FTP proxy service)**
- **3306/tcp : MySQL (Database Service)**

- **5432/tcp : PostgreSQL (Database Service)**

4. Pouvez-vous identifier plus d'informations sur ces services ?

- **FTP (21/tcp) : Utilisé pour le transfert de fichiers entre un client et un serveur.**
- **SSH (22/tcp) : Protocole sécurisé pour l'accès à distance.**

- **Telnet (23/tcp) : Ancien protocole d'accès à distance non chiffré.**
- **SMTP (25/tcp) : Utilisé pour l'envoi d'emails.**

- **DNS (53/tcp) : Résolution de noms de domaine.**

- **HTTP (80/tcp) : Service web**

- **MySQL (3306/tcp), PostgreSQL (5432/tcp) : Bases de données.**

5- Analyse approfondie avec Nmap

-sV identifier les vesion des services en cours d'execution

-A Active des options avancées (OS detection traceroute script scanning)

```
root@ubuntu:/home/ubuntu# nmap -sV -A 192.168.121.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 13:52 UTC
Nmap scan report for 192.168.121.129
Host is up (0.0029s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.121.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
```

```
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100003  2,3,4       2049/tcp   nfs
|   100005  1,2,3      37334/udp   mountd
|   100005  1,2,3      39685/tcp   mountd
|   100021  1,3,4      56017/tcp   nlockmgr
|_  100021  1,3,4      59780/udp   nlockmgr
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 13
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, Speaks41ProtocolNew, ConnectWithDatabase, Support41Auth, SupportsCompression, LongColumnFlag, SwitchToSSL
AfterHandshake
|   Status: Autocommit
|_  Salt: [m1J_!$1f3f-Kr{3+zI;
```

```
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-03-08T00:59:43+00:00; -12h55m46s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 2:12:04
|   source ident: nmap
|   source host: 128FA83D.60A75799.FFFA6D49.IP
|_  error: Closing Link: sdhywpsjq[192.168.121.128] (Quit: sdhywpsjq)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:80:15:C9 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -11h15m46s, deviation: 2h53m12s, median: -12h55m46s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-03-07T19:57:51-05:00

TRACEROUTE
HOP RTT     ADDRESS
1   2.94 ms 192.168.121.129

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 165.56 seconds
root@ubuntu:/home/ubuntu#
```

6. Quels services semblent vulnérables ?

FTP (vsftpd 2.3.4, port 21)

Telnet (port 23)

SSH (OpenSSH 4.7p1, port 22)

SMTP (Postfix, port 25)

DNS (ISC BIND 9.4.2, port 53)

7. Pourquoi est-il important d'identifier les versions des services ?

- **Si un service est ancien et vulnérable, il est préférable de le mettre à jour ou de le remplacer.**
- **Si un service ne peut pas être mis à jour immédiatement, on peut ajouter des mesures de sécurité (pare-feu, correctifs, restrictions d'accès) pour réduire les risques.**
- **Utiliser des versions sécurisées réduit les chances qu'un pirate exploite une faille.**

8. Quelle est la différence entre un scan SYN (-sS) et un scan TCP complet (-sT) ?

Scan SYN (-sS, "Stealth Scan") :

- **Envoie un paquet SYN (demande de connexion).**
- **Attend une réponse SYN-ACK (port ouvert) ou RST (port fermé).**
- **N'envoie pas de ACK, donc la connexion ne s'établit jamais complètement.**
- **Plus discret, moins détectable par les IDS/IPS.**

Scan TCP (-sT, "Full Connect") :

- **Effectue une connexion complète avec un handshake TCP en 3 étapes (SYN, SYN-ACK, ACK).**
- **Plus facilement détectable car il laisse des traces dans les logs des services.**
- **Plus lent et intrusif qu'un scan SYN.**

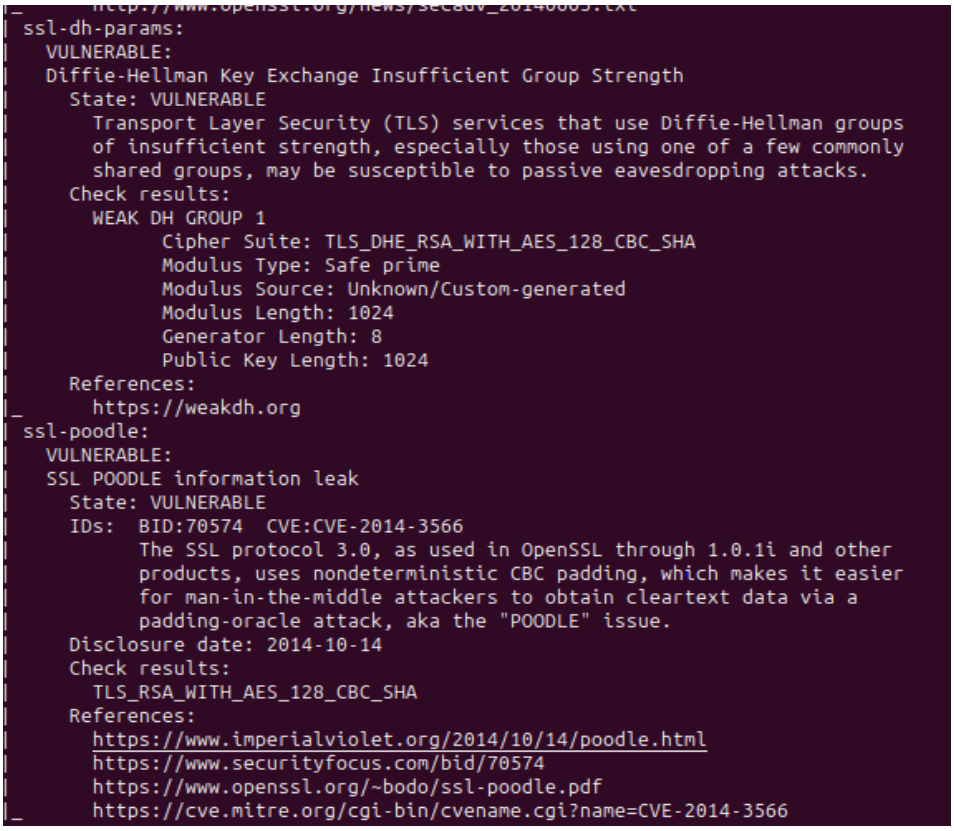
9. Quels outils, autres que Nmap, peuvent être utilisés pour la découverte de ports ouverts ?

- **Masscan : Très rapide, il peut scanner l'ensemble d'Internet en quelques minutes.**
- **Unicornscan : Conçu pour des scans à grande échelle, il offre plus de flexibilité qu'Nmap.**
- **ZMap : Optimisé pour les scans massifs et utilisé pour la cybersécurité offensive.**
- **Hping3 : Permet d'envoyer des paquets TCP/ICMP personnalisés pour tester les réponses des hôtes.**
- **Netcat (nc) : Utile pour tester manuellement la connectivité à un port.**
- **Metasploit (auxiliary/scanner) : Utilisé pour découvrir des services vulnérables et tester leur exploitation.**

Partie 2 : Détection de vulnérabilités des services détectés

```
ubuntu@ubuntu:~$ sudo nmap --script=vuln 192.168.121.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 14:15 UTC
Stats: 0:03:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.04% done; ETC: 14:19 (0:00:02 remaining)
Nmap scan report for 192.168.121.129
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://www.securityfocus.com/bid/48539
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
53/tcp   open  domain
80/tcp   open  http
| http-sql-injection:
|   Possible sqli for queries:
```

```
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.cvedetails.com/cve/2014-0224
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_      http://www.openssl.org/news/secadv_20140605.txt
```



2. Quels résultats obtenez-vous ?

- **Port 21 (FTP - vsftpd 2.3.4) : Il est vulnérable à une backdoor (CVE-2011-2523).**
- **Port 80 (HTTP) : Il y a une potentielle vulnérabilité à l'injection SQL, ce qui signifie qu'un attaquant pourrait manipuler la base de données via des requêtes malveillantes.**

```
ubuntu@ubuntu:~$ nikto -h http://192.168.121.129
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.121.129
+ Target Hostname:    192.168.121.129
+ Target Port:        80
+ Start Time:         2025-03-08 14:25:54 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that co
ings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Cookie phpMyAdmin created without the httponly flag
+ OSVDB-3092: /phpMyAdmin/: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /icons/README, inode: 412190, size: 5108, mtime: 0x438c0358aae80
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ 6544 items checked: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2025-03-08 14:26:31 (GMT0) (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
ubuntu@ubuntu:~$ nmap -p 21 --script=ftp-anon 192.168.121.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 14:28 UTC
Nmap scan report for 192.168.121.129
Host is up (0.00049s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
ubuntu@ubuntu:~$
```

```
ubuntu@ubuntu:~$ sudo -i
root@ubuntu:~# ssh msfadmin@192.168.121.129
Unable to negotiate with 192.168.121.129 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
root@ubuntu:~#
```

```
root@ubuntu:~# ssh -o HostKeyAlgorithms=+ssh-rsa -o PubKeyAcceptedAlgorithms=+ssh-rsa msfadmin@192.168.121.129
msfadmin@192.168.121.129's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Fri Mar  7 17:51:57 2025
msfadmin@metasploitable:~$
```

```
root@ubuntu:~# nmap -p 3306 --script=mysql-info 192.168.121.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 14:53 UTC
Nmap scan report for 192.168.121.129
Host is up (0.00048s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 548
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, LongColumnFlag, SupportsCompression, ConnectWithDatabase, SwitchToSSLAfterHandshake, Speak
s41ProtocolNew
|   Status: Autocommit
|_  Salt: {!+SC7'\}}~!$3p^d]$<
MAC Address: 00:0C:29:80:15:C9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.19 seconds
```

```
root@ubuntu:~# nmap -p 23 --script=telnet-encryption 192.168.121.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 15:03 UTC
Nmap scan report for 192.168.121.129
Host is up (0.00031s latency).

PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:0C:29:80:15:C9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 20.72 seconds
```

```
root@ubuntu:~# nmap -p 25 --script=smtp-open-relay 192.168.121.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 15:12 UTC
Nmap scan report for 192.168.121.129
Host is up (0.00037s latency).

PORT   STATE SERVICE
25/tcp open  smtp
|_smtp-open-relay: Server doesn't seem to be an open relay, all tests failed
MAC Address: 00:0C:29:80:15:C9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 41.32 seconds
```