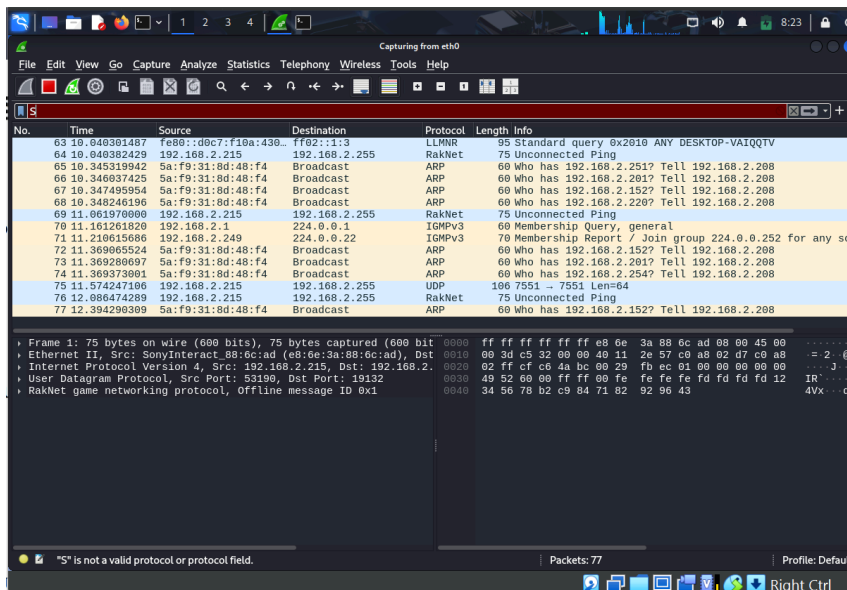


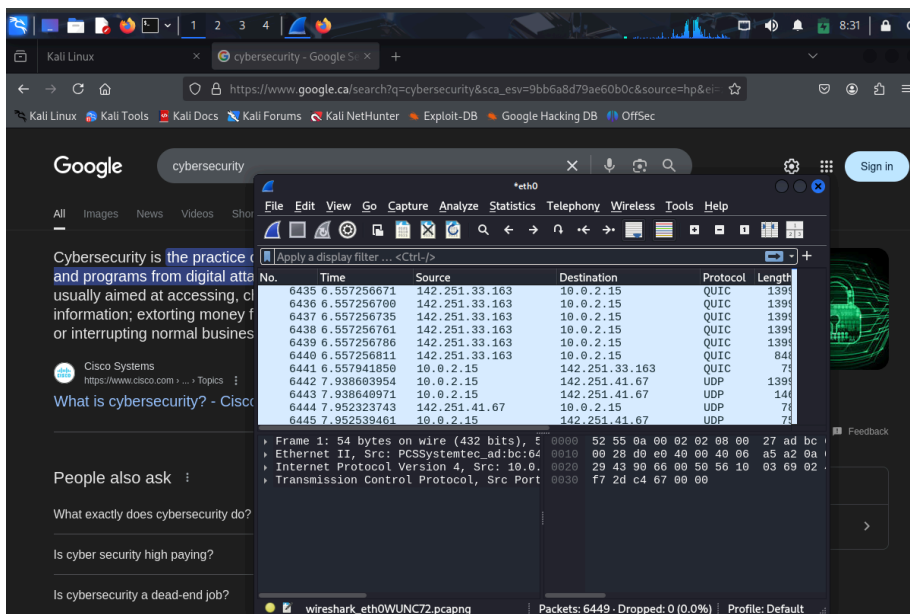
# Laboratoire 4 : Surveillance de réseau avec Wireshark et Zenmap

## Partie 1 : Analyse de trafic réseau avec Wireshark (8 pts)

Lancement:



Génération du trafic:



No.	Time	Source	Destination	Protocol	Length	Info
169	1.235715139	10.0.2.3	10.0.2.15	DNS	103	Standard query response 0x2b8c A safebrowsing.googleapis.com A 142.251.41.74
170	1.235715199	10.0.2.3	10.0.2.15	DNS	119	Standard query response 0x2b8d AAA safebrowsing.googleapis.com AAAA 2607:f8b6:400b:80c::200a
190	1.297559516	10.0.2.15	10.0.2.3	DNS	70	Standard query 0x2248 A o.pki.goog
191	1.297570507	10.0.2.15	10.0.2.3	DNS	70	Standard query 0x2a4b AAAA o.pki.goog
197	1.380520871	10.0.2.3	10.0.2.15	DNS	121	Standard query response 0x2248 A o.pki.goog CNAME pki-goog.l.google.com A 142.251.32.67
199	1.380520950	10.0.2.3	10.0.2.15	DNS	119	Standard query response 0x2a4b AAAA o.pki.goog CNAME pki-goog.l.google.com AAAA 2607:f8b6:400b:80c::200a
452	1.496646307	10.0.2.15	10.0.2.3	DNS	89	Standard query 0x2b2c A lh3.googleusercontent.com
453	1.496647548	10.0.2.15	10.0.2.3	DNS	85	Standard query 0x2c6d AAAA lh3.googleusercontent.com
470	1.514236590	10.0.2.3	10.0.2.15	DNS	130	Standard query response 0x2b2c A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 172.217.1.1
486	1.514236630	10.0.2.3	10.0.2.15	DNS	142	Standard query response 0x2c6d AAAA lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com AAAA 2607:f8b6:400b:803::2
3941	4.120865514	10.0.2.15	10.0.2.3	DNS	75	Standard query 0x2a4b A www.gstatic.com
3942	4.120865210	10.0.2.15	10.0.2.3	DNS	75	Standard query 0x7874 AAAA www.gstatic.com
3943	4.121881740	10.0.2.15	10.0.2.3	DNS	80	Standard query 0x2a47 A encrypted-tbn.gstatic.com
3944	4.121094355	10.0.2.15	10.0.2.3	DNS	86	Standard query 0x2b2c AAAA encrypted-tbn.gstatic.com
3945	4.121315140	10.0.2.15	10.0.2.3	DNS	89	Standard query 0x1137 A lh3.googleusercontent.com
3946	4.121240178	10.0.2.15	10.0.2.3	DNS	85	Standard query 0x1234 AAAA lh3.googleusercontent.com
3947	4.120863401	10.0.2.3	10.0.2.15	DNS	91	Standard query response 0x2a4b A www.gstatic.com A 142.251.33.163
3948	4.128129291	10.0.2.3	10.0.2.15	DNS	151	Standard query response 0x1137 A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 172.217.1.1
3949	4.128330335	10.0.2.3	10.0.2.15	DNS	182	Standard query response 0x2a47 A encrypted-tbn.gstatic.com A 142.251.41.26

1. Quelle est l'adresse IP de www.google.com dans la capture ?

**142.251.41.36**

4133	4.658027228	10.0.2.15	10.0.2.3	DNS	74	Standard query 0x5cf1 AAAA www.google.com
4134	4.662360489	10.0.2.3	10.0.2.15	DNS	90	Standard query response 0xc5f3 A www.google.com A 142.251.41.36
4157	4.667402072	10.0.2.3	10.0.2.15	DNS	100	Standard query response 0x5676 A www.googleadservices.com A 142.251.41.34

2. Combien de requêtes DNS ont été envoyées ?

**40 dans mon cas**

Packets: 6449 · Displayed: 40 (0.6%) · Selected: 40 (0.6%) · Dropped: 0 (0.0%)	Profile: D
--	------------

3. Quel est le port utilisé pour HTTPS ?

443 (80 pour HTTP normal)

4. Quelle est la différence entre TCP et UDP ?

TCP envoie un paquet pour confirmer la réception de données, alors que UDP envoie plus rapidement, mais sans demander de réponse.



5. Pourquoi est-il utile de filtrer les paquets ?

Pour analyser le trafic est observer des activités malveillantes ou non-conformes.

## Partie 2 : Scan de réseau avec Zenmap (12 pts)

Scan initiale:

Command: nmap -T4 -A -v 192.168.1.0/24

Hosts		Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
OS	Host		nmap -T4 -A -v 192.168.1.0/24				
	192.168.1.2		<pre>nmap -T4 -A -v 192.168.1.0/24   _ wuK6K0UfKie&gt; riags: &lt;group&gt;&lt;active&gt;  _ smb2-time: Protocol negotiation failed (SMB2)  _ smb-security-mode:     account_used: &lt;blank&gt;     authentication_level: user     challenge_response: supported     message_signing: disabled (dangerous, but default)  _ smb-os-discovery:     OS: Unix (Samba 3.0.20-Debian)     Computer name: metasploitable     NetBIOS computer name:     Domain name: localdomain     FQDN: metasploitable.localdomain  _ System time: 2025-05-26T14:57:03-04:00  _ clock-skew: mean: -1d16h50m02s, deviation: 2h18m47s, median: -1d18h09m59s  TRACEROUTE HOP RTT ADDRESS 1 0.69 ms 192.168.1.5  Initiating SYN Stealth Scan at 13:08 Scanning 192.168.1.2 [1000 ports] Discovered open port 3389/tcp on 192.168.1.2 Discovered open port 139/tcp on 192.168.1.2 Discovered open port 135/tcp on 192.168.1.2 Discovered open port 445/tcp on 192.168.1.2 Discovered open port 5985/tcp on 192.168.1.2 Discovered open port 5986/tcp on 192.168.1.2 Completed SYN Stealth Scan at 13:08, 0.06s elapsed (1000 total ports) Initiating Service scan at 13:08</pre>				
	192.168.1.5						
Filter Hosts							



Target: 192.168.1.5 Profile: Scan Cancel

Command: nmap -sS -sV 192.168.1.5

Hosts Services

OS Host

192.168.1.2

192.168.1.5

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sS -sV 192.168.1.5 Details

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec?	
513/tcp	open	login?	
514/tcp	open	shell?	
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	ccproxy-ftp?	
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

**MAC Address:** 08:00:27:E1:7D:3B (Oracle VirtualBox virtual NIC)

**Service Info:** Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

**Nmap done:** 1 IP address (1 host up) scanned in 181.94 seconds

Filter Hosts

Voir fichier XML pour le scan de vuln...

1. Combien d'hôtes actifs ont été détectés ?
- 2 - La machine Windows et Metasploitable

2. Quels ports sont ouverts sur l'hôte ciblé ?

23 ports

3. Quels services sont associés à ces ports ?

21/tcp open ftp vsftpd 2.3.4  
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp open telnet Linux telnetd  
25/tcp open smtp Postfix smtpd  
53/tcp open domain ISC BIND 9.4.2  
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp open rpcbind 2 (RPC #100000)  
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp open exec?  
513/tcp open login?  
514/tcp open shell?  
1099/tcp open java-rmi GNU Classpath grmregistry  
1524/tcp open bindshell Metasploitable root shell  
2049/tcp open nfs 2-4 (RPC #100003)  
2121/tcp open ccproxy-ftp?  
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5  
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp open vnc VNC (protocol 3.3)  
6000/tcp open X11 (access denied)  
6667/tcp open irc UnrealIRCd  
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)  
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

4. Y a-t-il des vulnérabilités visibles ?

Oui, beaucoup. Voir le XML pour la liste.

5. Quelle est l'utilité du scan dans une stratégie de cybersécurité ?

La cartographie du scan est cruciale pour la gestion des vulnérabilités, en aidant à repérer les logiciels obsolètes ou les configurations incorrectes qui pourraient être exploitables.