

Documentation Technique : Analyse de Trame avec Wireshark

L'outil Wireshark a été utilisé dans deux contextes techniques distincts au cours de ma formation. D'une part, pour valider les flux réseau et le cloisonnement de l'infrastructure Vénus dans le cadre du projet E6 (NIDS Suricata). D'autre part, lors d'un TP de cybersécurité visant à démontrer la vulnérabilité du protocole HTTP face à l'interception de données d'authentification.

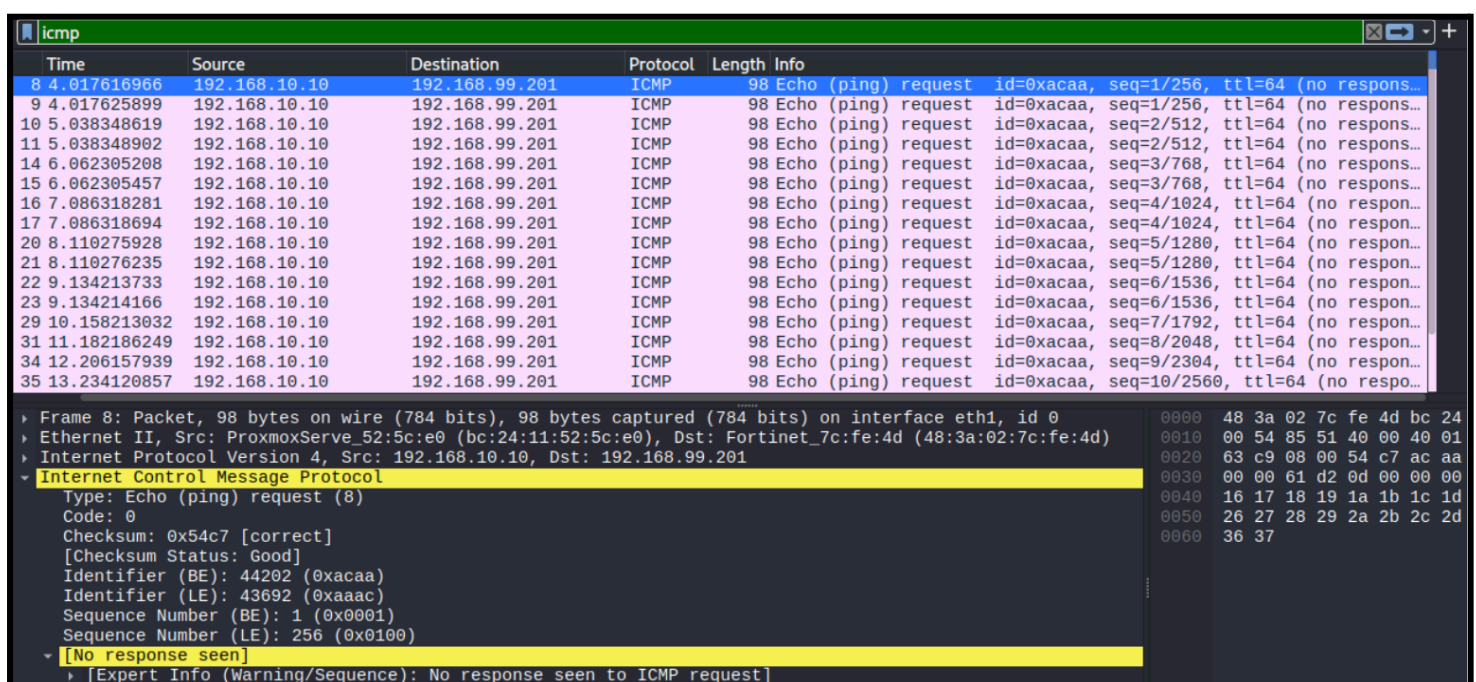
1. Contexte Projet Vénus : Analyse du trafic ICMP inter-VLAN

Dans le cadre du déploiement de la sonde Suricata sur l'infrastructure Vénus, Wireshark a été utilisé pour capturer et analyser les tentatives de communication entre différentes zones réseau. ([Documentation complète du NIDS - Projet 2 E6](#))

1.1. Validation du cloisonnement réseau

La capture réseau illustre une tentative de balayage ICMP (Ping sweep) initiée depuis une machine utilisateur du VLAN 10 (IP source 192.168.10.10) à destination d'un serveur critique situé dans le VLAN 99 (IP de destination 192.168.99.201). Un poste de travail standard n'ayant aucune raison légitime de vérifier la connectivité des serveurs d'infrastructure, ce trafic est considéré comme suspect.

L'analyse de la trame via Wireshark confirme que le pare-feu remplit son rôle de ségrégation : les requêtes "Echo (ping) request" restent sans réponse, comme l'indique le message d'avertissement "No response seen to ICMP request".



Time	Source	Destination	Protocol	Length	Info
8.4017616966	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=1/256, ttl=64 (no response seen)
9.4017625899	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=1/256, ttl=64 (no response seen)
10.5038348619	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=2/512, ttl=64 (no response seen)
11.5038348902	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=2/512, ttl=64 (no response seen)
14.6062305208	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=3/768, ttl=64 (no response seen)
15.6062305457	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=3/768, ttl=64 (no response seen)
16.7086318281	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=4/1024, ttl=64 (no response seen)
17.7086318694	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=4/1024, ttl=64 (no response seen)
20.8.110275928	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=5/1280, ttl=64 (no response seen)
21.8.110276235	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=5/1280, ttl=64 (no response seen)
22.9.134213733	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=6/1536, ttl=64 (no response seen)
23.9.134214166	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=6/1536, ttl=64 (no response seen)
29.10.158213032	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=7/1792, ttl=64 (no response seen)
31.11.182186249	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=8/2048, ttl=64 (no response seen)
34.12.206157939	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=9/2304, ttl=64 (no response seen)
35.13.234120857	192.168.10.10	192.168.99.201	ICMP	98	Echo (ping) request id=0xacaa, seq=10/2560, ttl=64 (no response seen)

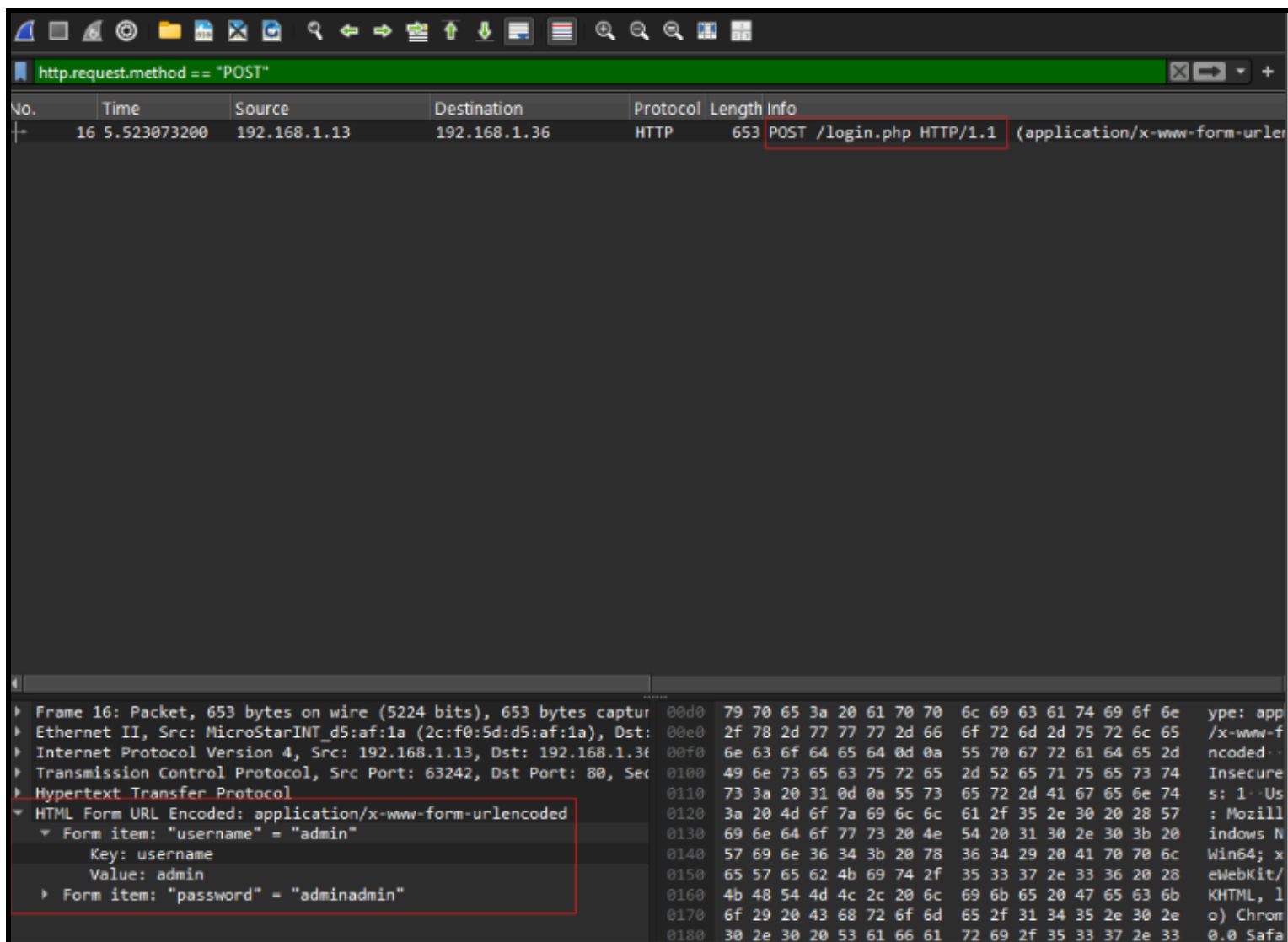
Frame 8: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth1, id 0	0000	48	3a	02	7c	fe	4d	bc	24
Ethernet II, Src: ProxmoxServe_52:5c:e0 (bc:24:11:52:5c:e0), Dst: Fortinet_7c:fe:4d (48:3a:02:7c:fe:4d)	0010	00	54	85	51	40	00	40	01
Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.99.201	0020	63	c9	08	00	54	c7	ac	aa
Internet Control Message Protocol	0030	00	00	61	d2	0d	00	00	00
Type: Echo (ping) request (8)	0040	16	17	18	19	1a	1b	1c	1d
Code: 0	0050	26	27	28	29	2a	2b	2c	2d
Checksum: 0x54c7 [correct]	0060	36	37						
[Checksum Status: Good]									
Identifier (BE): 44202 (0xacaa)									
Identifier (LE): 43692 (0xaaac)									
Sequence Number (BE): 1 (0x0001)									
Sequence Number (LE): 256 (0x0100)									
[No response seen]									
[Expert Info (Warning/Sequence): No response seen to ICMP request]									

2. Contexte TP Cybersécurité : HTTP vs HTTPS

Ce second cas d'usage de Wireshark illustre une vulnérabilité applicative classique : l'interception d'identifiants de connexion transitant en clair sur un réseau local.

2.1. Interception des identifiants en HTTP

Lors de la première phase du TP, un formulaire d'authentification a été hébergé sur un serveur web Apache classique (port 80). La capture Wireshark, filtrée avec l'expression `http.request.method == "POST"`, permet d'isoler la requête d'authentification. L'analyse du paquet démontre que les variables envoyées par l'utilisateur sont totalement lisibles : la section "HTML Form URL Encoded" expose le nom d'utilisateur et le mot de passe en texte clair. Cette démonstration prouve qu'un attaquant positionné sur le réseau local peut facilement compromettre des comptes utilisateurs.



2.2. Preuve de sécurisation par TLS (HTTPS)

Pour corriger cette faille, un certificat auto-signé a été généré via OpenSSL et déployé sur le serveur Apache pour chiffrer les échanges sur le port 443. Une nouvelle capture Wireshark a été réalisée (filtre `tcp.port == 443`) lors de la soumission du même formulaire.

L'analyse de cette nouvelle trame montre l'absence totale de la section "HTML Form URL Encoded". À la place, les identifiants sont encapsulés sous la mention "TLSv1.3 Application Data" et remplacés par un bloc nommé "Encrypted Application Data". L'outil Wireshark confirme ainsi visuellement que le chiffrement empêche toute lecture des données sensibles lors de leur transit sur le réseau.

7	0.002915800	192.168.56.105	192.168.56.104	TLSv1.3	1382 Server Hello, Change Cipher Spec, Application Data, Application Data
8	0.003307000	192.168.56.104	192.168.56.105	TLSv1.3	84 Change Cipher Spec, Application Data
9	0.003437700	192.168.56.104	192.168.56.105	TCP	54 59562 → 443 [FIN, ACK] Seq=1811 Ack=1329 Win=64000 Len=0
10	0.003547200	192.168.56.105	192.168.56.104	TCP	60 443 → 59562 [FIN, ACK] Seq=1329 Ack=1812 Win=62464 Len=0
11	0.003590100	192.168.56.104	192.168.56.105	TCP	54 59562 → 443 [ACK] Seq=1812 Ack=1330 Win=64000 Len=0
12	0.004085000	192.168.56.104	192.168.56.105	TCP	66 63109 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
13	0.004207500	192.168.56.105	192.168.56.104	TCP	66 443 → 63109 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
14	0.004270900	192.168.56.104	192.168.56.105	TCP	54 63109 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
15	0.004690100	192.168.56.104	192.168.56.105	TCP	1514 63109 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1460 [TCP PDU reassembled in 16]
16	0.004690100	192.168.56.104	192.168.56.105	TLSv1.3	359 Client Hello
17	0.004845200	192.168.56.105	192.168.56.104	TCP	60 443 → 63109 [ACK] Seq=1 Ack=1766 Win=62592 Len=0
18	0.006682500	192.168.56.105	192.168.56.104	TLSv1.3	1514 Server Hello, Change Cipher Spec, Application Data
19	0.006749700	192.168.56.105	192.168.56.104	TLSv1.3	1262 Application Data, Application Data, Application Data
20	0.006774700	192.168.56.104	192.168.56.105	TCP	54 63109 → 443 [ACK] Seq=1766 Ack=2669 Win=65280 Len=0
21	0.007081700	192.168.56.104	192.168.56.105	TLSv1.3	118 Change Cipher Spec, Application Data
22	0.007292500	192.168.56.104	192.168.56.105	TLSv1.3	927 Application Data
23	0.007432600	192.168.56.105	192.168.56.104	TLSv1.3	133 Application Data
24	0.007590600	192.168.56.105	192.168.56.104	TLSv1.3	133 Application Data
25	0.007615800	192.168.56.104	192.168.56.105	TCP	54 63109 → 443 [ACK] Seq=2703 Ack=2827 Win=65280 Len=0

▶	Frame 30: Packet, 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{8B...
▶	Ethernet II, Src: PCSSystemtec_17:14:f0 (08:00:27:17:14:f0), Dst: 0a:00:27:00:00:0e (0a:00:27:00:00:0e)
▶	Internet Protocol Version 4, Src: 192.168.56.105, Dst: 192.168.56.104
▶	Transmission Control Protocol, Src Port: 443, Dst Port: 63109, Seq: 3103, Ack: 2703, Len: 24
▼	Transport Layer Security
	[Stream index: 1]
▼	TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
	Opaque Type: Application Data (23)
	Version: TLS 1.2 (0x0303)
	Length: 19
	Encrypted Application Data: 348e6af69a1f1ad974dd381c3c93ae35a422dc
	[Application Data Protocol: Hypertext Transfer Protocol]

Preuve visuelle : plus de section « HTML Form URL Encoded » avec `username` / `password`. Tout est remplacé par « Encrypted Application Data ».

Comparaison avec HTTP

HTTP (Partie 1) :

- |— Protocol : HTTP
- |— Port : 80
- |— Contenu : username=admin & password=adminadmin (clair)

HTTPS (Partie 2) :

- |— Protocol : TLSv1.3
- |— Port : 443
- |— Contenu : Encrypted Application Data (illisible)