Preuve AC0114 - Maîtriser les rôles et les principes fondamentaux des systèmes d'exploitation

Modules : R102, R108, SAE1.01, SAE12

Période : Septembre - Novembre 2024

Contexte technique

- Environnement Linux et Windows pour l'administration système

- Utilisation d'outils d'analyse réseau (Wireshark)

- Configuration et analyse de protocoles réseau (FTP, HTTP, ICMP)

- Travail sur la sécurisation des systèmes

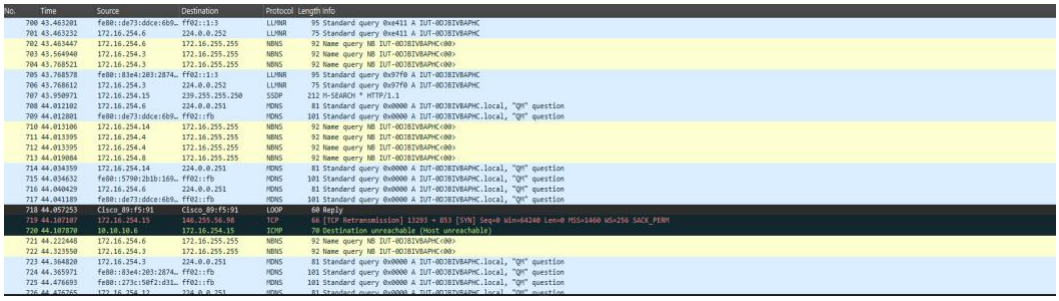
Réalisations techniques

Analyse de protocoles et trafic réseau

- Test initial de connectivité avec serveur

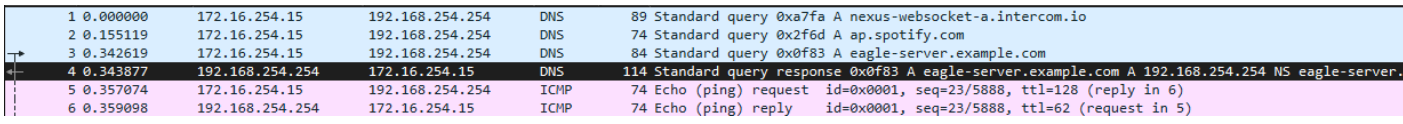
```
C:\Users\zeeni>ping 192.168.254.254

Envoi d'une requête 'Ping'  192.168.254.254 avec 32 octets de données :
Réponse de 192.168.254.254 : octets=32 temps=1 ms TTL=62
Réponse de 192.168.254.254 : octets=32 temps=2 ms TTL=62
Réponse de 192.168.254.254 : octets=32 temps=2 ms TTL=62
Réponse de 192.168.254.254 : octets=32 temps=2 ms TTL=62

Statistiques Ping pour 192.168.254.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

- Identification et analyse des protocoles principaux (NBNS, MDNS, LLMNR, SSDP, DNS) via Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
700	43.463201	fe80::de73:ddce:6b9…	ff02::1:3	LLMNR	95	Standard query 0xe411 A IUT-0D3BIVBAPHC
701	43.463232	172.16.254.6	224.0.0.252	LLMNR	75	Standard query 0xe411 A IUT-0D3BIVBAPHC
702	43.463447	172.16.254.6	172.16.255.255	NBNS	92	Name query NB IUT-0D3BIVBAPHC<00>
703	43.564940	172.16.254.3	172.16.255.255	NBNS	92	Name query NB IUT-0D3BIVBAPHC<00>
704	43.768521	172.16.254.3	172.16.255.255	NBNS	92	Name query NB IUT-0D3BIVBAPHC<00>
705	43.768578	fe80::83e4:203:2874…	ff02::1:3	LLMNR	95	Standard query 0x97f0 A IUT-0D3BIVBAPHC
706	43.768612	172.16.254.3	224.0.0.252	LLMNR	75	Standard query 0x97f0 A IUT-0D3BIVBAPHC
707	43.950971	172.16.254.15	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
708	44.012102	172.16.254.6	224.0.0.251	MDNS	81	Standard query 0x0000 A IUT-0D3BIVBAPHC.local, "QM" question
709	44.012801	fe80::de73:ddce:6b9…	ff02::fb	MDNS	101	Standard query 0x0000 A IUT-0D3BIVBAPHC.local, "QM" question
710	44.013106	172.16.254.14	172.16.255.255	NBNS	92	Name query NB IUT-0D3BIVBAPHC<00>
711	44.013395	172.16.254.4	172.16.255.255	NBNS	92	Name query NB IUT-0D3BIVBAPHC<00>
712	44.013395	172.16.254.4	172.16.255.255	NBNS	92	Name query NB IUT-0D3BIVBAPHC<00>
713	44.019084	172.16.254.8	172.16.255.255	NBNS	92	Name query NB IUT-0D3BIVBAPHC<00>
714	44.034359	172.16.254.14	224.0.0.251	MDNS	81	Standard query 0x0000 A IUT-0D3BIVBAPHC.local, "QM" question
715	44.034632	fe80::5790:2b1b:169…	ff02::fb	MDNS	101	Standard query 0x0000 A IUT-0D3BIVBAPHC.local, "QM" question
716	44.040429	172.16.254.6	224.0.0.251	MDNS	81	Standard query 0x0000 A IUT-0D3BIVBAPHC.local, "QM" question
717	44.041189	fe80::de73:ddce:6b9…	ff02::fb	MDNS	101	Standard query 0x0000 A IUT-0D3BIVBAPHC.local, "QM" question
718	44.057253	Cisco_89:f5:91	Cisco_89:f5:91	LOOP	60	Reply
719	44.107107	172.16.254.15	146.255.56.98	TCP	66	[TCP Retransmission] 13293 → 853 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
720	44.107870	10.10.10.6	172.16.254.15	ICMP	70	Destination unreachable (Host unreachable)
721	44.222440	172.16.254.6	172.16.255.255	NBNS	92	Name query NB IUT-0D3BIVBAPHC<00>
722	44.323550	172.16.254.3	172.16.255.255	NBNS	92	Name query NB IUT-0D3BIVBAPHC<00>
723	44.364820	172.16.254.3	224.0.0.251	MDNS	81	Standard query 0x0000 A IUT-0D3BIVBAPHC.local, "QM" question
724	44.365971	fe80::83e4:203:2874…	ff02::fb	MDNS	101	Standard query 0x0000 A IUT-0D3BIVBAPHC.local, "QM" question
725	44.476693	fe80::273c:50f2:d31…	ff02::fb	MDNS	101	Standard query 0x0000 A IUT-0D3BIVBAPHC.local, "QM" question
726	44.476765	172.16.254.12	224.0.0.251	MDNS	81	Standard query 0x0000 A IUT-0D3BIVBAPHC.local, "QM" question

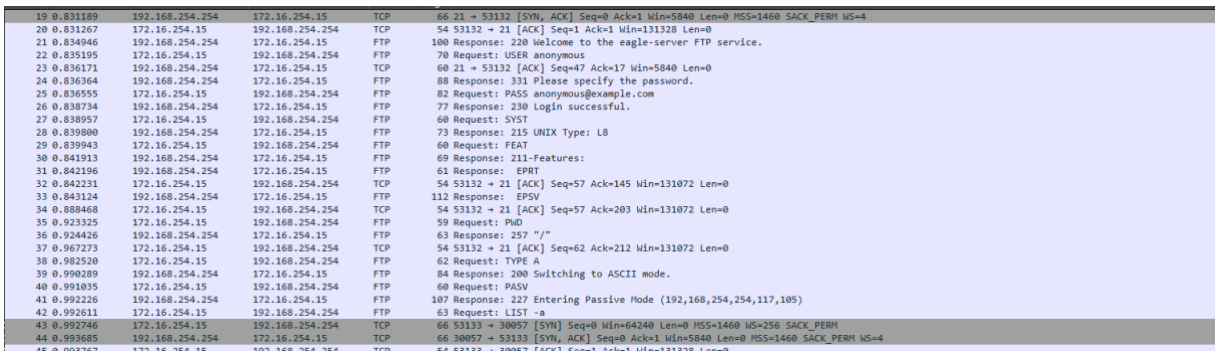
- Étude du mécanisme DNS pour association nom/IP



1	0.000000	172.16.254.15	192.168.254.254	DNS	89 Standard query 0xa7fa A nexus-websocket-a.intercom.io
2	0.155119	172.16.254.15	192.168.254.254	DNS	74 Standard query 0x2f6d A ap.spotify.com
3	0.342619	172.16.254.15	192.168.254.254	DNS	84 Standard query 0x0f83 A eagle-server.example.com
4	0.343877	192.168.254.254	172.16.254.15	DNS	114 Standard query response 0x0f83 A eagle-server.example.com A 192.168.254.254 NS eagle-server.
5	0.357074	172.16.254.15	192.168.254.254	ICMP	74 Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 6)
6	0.359098	192.168.254.254	172.16.254.15	ICMP	74 Echo (ping) reply id=0x0001, seq=23/5888, ttl=62 (request in 5)

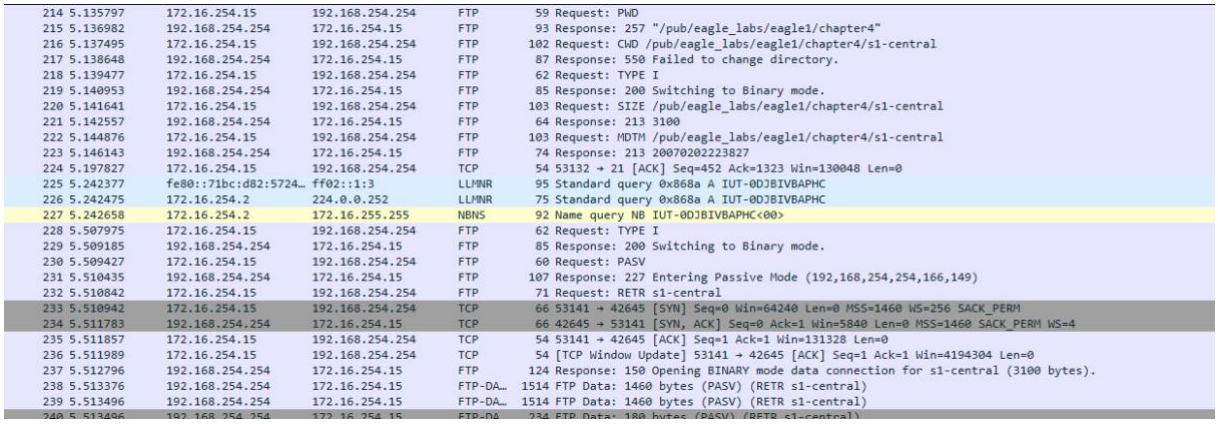
- Analyse des phases du protocole FTP :

 * Phase de connexion



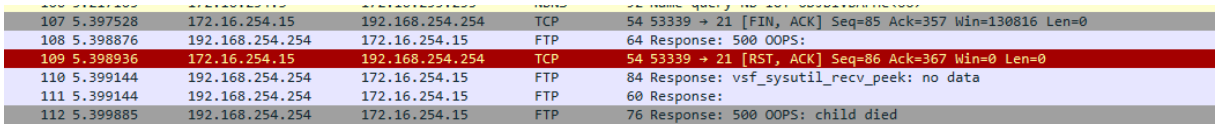
19	0.831189	192.168.254.254	172.16.254.15	TCP	66 21 → 53132 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=4
20	0.831267	172.16.254.15	192.168.254.254	TCP	54 53132 → 21 [ACK] Seq=1 Ack=1 Win=131328 Len=0
21	0.834946	192.168.254.254	172.16.254.15	FTP	100 Response: 220 Welcome to the eagle-server FTP service.
22	0.835195	172.16.254.15	192.168.254.254	FTP	70 Request: USER anonymous
23	0.836171	192.168.254.254	172.16.254.15	TCP	60 21 → 53132 [ACK] Seq=47 Ack=17 Win=5840 Len=0
24	0.836364	192.168.254.254	172.16.254.15	FTP	88 Response: 331 Please specify the password.
25	0.836555	172.16.254.15	192.168.254.254	FTP	82 Request: PASS anonymous@example.com
26	0.838734	192.168.254.254	172.16.254.15	FTP	77 Response: 230 Login successful.
27	0.838957	172.16.254.15	192.168.254.254	FTP	60 Request: SYST
28	0.839800	192.168.254.254	172.16.254.15	FTP	73 Response: 215 UNIX Type: L8
29	0.839943	172.16.254.15	192.168.254.254	FTP	60 Request: FEAT
30	0.841913	192.168.254.254	172.16.254.15	FTP	69 Response: 211-Features:
31	0.842196	192.168.254.254	172.16.254.15	FTP	61 Response: EPRT
32	0.842231	172.16.254.15	192.168.254.254	TCP	54 53132 → 21 [ACK] Seq=57 Ack=145 Win=131072 Len=0
33	0.843124	192.168.254.254	172.16.254.15	FTP	112 Response: EPSV
34	0.888468	172.16.254.15	192.168.254.254	TCP	54 53132 → 21 [ACK] Seq=57 Ack=203 Win=131072 Len=0
35	0.923325	172.16.254.15	192.168.254.254	FTP	59 Request: PWD
36	0.924426	192.168.254.254	172.16.254.15	FTP	63 Response: 257 "/"
37	0.967273	172.16.254.15	192.168.254.254	TCP	54 53132 → 21 [ACK] Seq=62 Ack=212 Win=131072 Len=0
38	0.982520	172.16.254.15	192.168.254.254	FTP	62 Request: TYPE A
39	0.990289	192.168.254.254	172.16.254.15	FTP	84 Response: 200 Switching to ASCII mode.
40	0.991035	172.16.254.15	192.168.254.254	FTP	60 Request: PASV
41	0.992226	192.168.254.254	172.16.254.15	FTP	107 Response: 227 Entering Passive Mode (192,168,254,254,117,105)
42	0.992611	172.16.254.15	192.168.254.254	FTP	63 Request: LIST -a
43	0.992746	172.16.254.15	192.168.254.254	TCP	66 53133 → 30057 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
44	0.993685	192.168.254.254	172.16.254.15	TCP	66 30057 → 53133 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=4

 * Phase de téléchargement



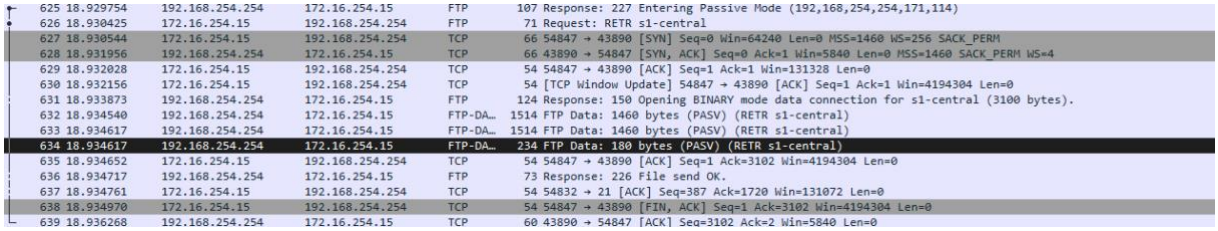
214	5.135797	172.16.254.15	192.168.254.254	FTP	59 Request: PWD
215	5.136982	192.168.254.254	172.16.254.15	FTP	93 Response: 257 "/pub/eagle_labs/eagle1/chapter4"
216	5.137495	172.16.254.15	192.168.254.254	FTP	102 Request: CWD /pub/eagle_labs/eagle1/chapter4/s1-central
217	5.138648	192.168.254.254	172.16.254.15	FTP	87 Response: 550 Failed to change directory.
218	5.139477	172.16.254.15	192.168.254.254	FTP	62 Request: TYPE I
219	5.140953	192.168.254.254	172.16.254.15	FTP	85 Response: 200 Switching to Binary mode.
220	5.141641	172.16.254.15	192.168.254.254	FTP	103 Request: SIZE /pub/eagle_labs/eagle1/chapter4/s1-central
221	5.142557	192.168.254.254	172.16.254.15	FTP	64 Response: 213 3100
222	5.144876	172.16.254.15	192.168.254.254	FTP	103 Request: MDTM /pub/eagle_labs/eagle1/chapter4/s1-central
223	5.146143	192.168.254.254	172.16.254.15	FTP	74 Response: 213 20070202223827
224	5.197827	172.16.254.15	192.168.254.254	TCP	54 53132 → 21 [ACK] Seq=452 Ack=1323 Win=130048 Len=0
225	5.242377	fe80::71bc:d82:5724…	ff02::1:3	LLMNR	95 Standard query 0x868a A IUT-0DJBIVBAPHC
226	5.242475	172.16.254.2	224.0.0.252	LLMNR	75 Standard query 0x868a A IUT-0DJBIVBAPHC
227	5.242658	172.16.254.2	172.16.255.255	NBNS	92 Name query NB IUT-0DJBIVBAPHC<00>
228	5.507975	172.16.254.15	192.168.254.254	FTP	62 Request: TYPE I
229	5.509185	192.168.254.254	172.16.254.15	FTP	85 Response: 200 Switching to Binary mode.
230	5.509427	172.16.254.15	192.168.254.254	FTP	60 Request: PASV
231	5.510435	192.168.254.254	172.16.254.15	FTP	107 Response: 227 Entering Passive Mode (192,168,254,254,166,149)
232	5.510842	172.16.254.15	192.168.254.254	FTP	71 Request: RETR s1-central
233	5.510942	172.16.254.15	192.168.254.254	TCP	66 53141 → 42645 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
234	5.511783	192.168.254.254	172.16.254.15	TCP	66 42645 → 53141 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=4
235	5.511857	172.16.254.15	192.168.254.254	TCP	54 53141 → 42645 [ACK] Seq=1 Ack=1 Win=131328 Len=0
236	5.511989	172.16.254.15	192.168.254.254	TCP	54 [TCP Window Update] 53141 → 42645 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
237	5.512796	192.168.254.254	172.16.254.15	FTP	124 Response: 150 Opening BINARY mode data connection for s1-central (3100 bytes).
238	5.513376	192.168.254.254	172.16.254.15	FTP-DA…	1514 FTP Data: 1460 bytes (PASV) (RETR s1-central)
239	5.513496	192.168.254.254	172.16.254.15	FTP-DA…	1514 FTP Data: 1460 bytes (PASV) (RETR s1-central)

 * Phase de fermeture avec séquence FIN/ACK



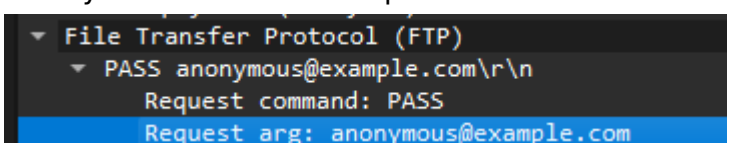
107	5.397528	172.16.254.15	192.168.254.254	TCP	54 53339 → 21 [FIN, ACK] Seq=85 Ack=357 Win=130816 Len=0
108	5.398876	192.168.254.254	172.16.254.15	FTP	64 Response: 500 OOPS:
109	5.398936	172.16.254.15	192.168.254.254	TCP	54 53339 → 21 [RST, ACK] Seq=86 Ack=367 Win=0 Len=0
110	5.399144	192.168.254.254	172.16.254.15	FTP	84 Response: vsf_sysutil_recv_peek: no data
111	5.399144	192.168.254.254	172.16.254.15	FTP	60 Response:
112	5.399885	192.168.254.254	172.16.254.15	FTP	76 Response: 500 OOPS: child died

- Compréhension de l'encapsulation des protocoles

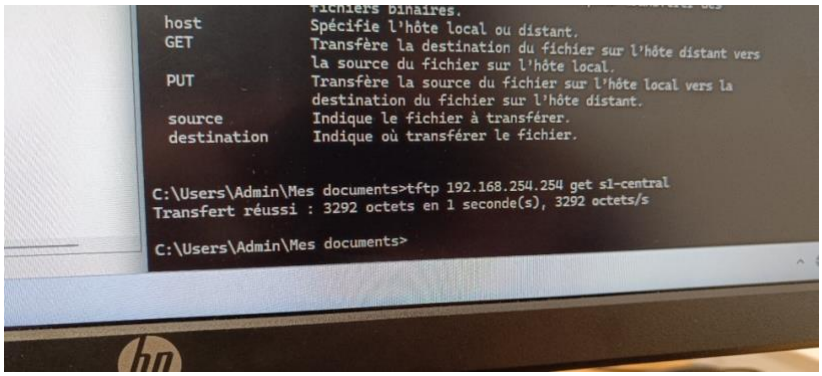


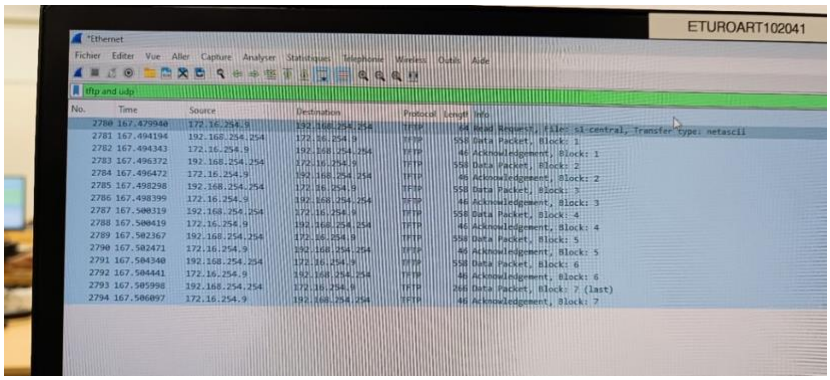
625	18.929754	192.168.254.254	172.16.254.15	FTP	107 Response: 227 Entering Passive Mode (192,168,254,254,171,114)
626	18.930425	172.16.254.15	192.168.254.254	FTP	71 Request: RETR s1-central
627	18.930544	172.16.254.15	192.168.254.254	TCP	66 54847 → 43890 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
628	18.931956	192.168.254.254	172.16.254.15	TCP	66 43890 → 54847 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=4
629	18.932028	172.16.254.15	192.168.254.254	TCP	54 54847 → 43890 [ACK] Seq=1 Ack=1 Win=131328 Len=0
630	18.932156	172.16.254.15	192.168.254.254	TCP	54 [TCP Window Update] 54847 → 43890 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
631	18.933873	192.168.254.254	172.16.254.15	FTP	124 Response: 150 Opening BINARY mode data connection for s1-central (3100 bytes).
632	18.934540	192.168.254.254	172.16.254.15	FTP-DA…	1514 FTP Data: 1460 bytes (PASV) (RETR s1-central)
633	18.934617	192.168.254.254	172.16.254.15	FTP-DA…	1514 FTP Data: 1460 bytes (PASV) (RETR s1-central)
634	18.934617	192.168.254.254	172.16.254.15	FTP-DA…	234 FTP Data: 180 bytes (PASV) (RETR s1-central)
635	18.934652	172.16.254.15	192.168.254.254	TCP	54 54847 → 43890 [ACK] Seq=1 Ack=3102 Win=4194304 Len=0
636	18.934717	192.168.254.254	172.16.254.15	FTP	73 Response: 226 File send OK.
637	18.934761	172.16.254.15	192.168.254.254	TCP	54 54832 → 21 [ACK] Seq=387 Ack=1720 Win=131072 Len=0
638	18.934970	172.16.254.15	192.168.254.254	TCP	54 54847 → 43890 [FIN, ACK] Seq=1 Ack=3102 Win=4194304 Len=0
639	18.936268	192.168.254.254	172.16.254.15	TCP	60 43890 → 54847 [ACK] Seq=3102 Ack=2 Win=5840 Len=0

- Analyse de la sécurité des protocoles de transfert



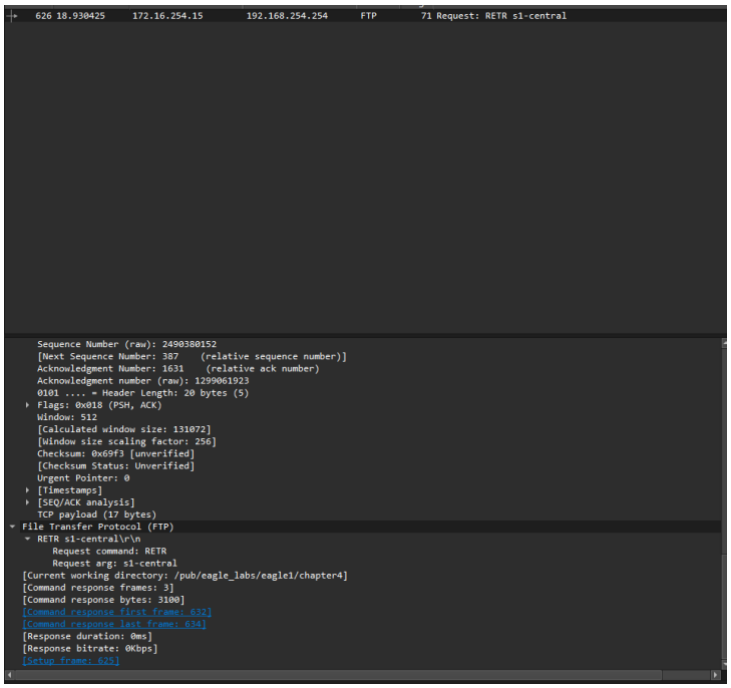
- Étude comparative FTP/TFTP





- Analyse HTTP et comparaison avec FTP

```
    31 2.119568     172.16.254.15     192.168.254.254   TCP        66 56850 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    32 2.120445     192.168.254.254   172.16.254.15     TCP        66 80 → 56850 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=4
    33 2.120494     172.16.254.15     192.168.254.254   TCP        54 56850 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
    34 2.120948     172.16.254.15     192.168.254.254   HTTP      555 GET / HTTP/1.1
    35 2.122897     192.168.254.254   172.16.254.15     TCP        60 80 → 56850 [ACK] Seq=1 Ack=502 Win=6912 Len=0
    36 2.123506     192.168.254.254   172.16.254.15     HTTP      500 HTTP/1.1 200 OK  (text/html)
    37 2.123506     192.168.254.254   172.16.254.15     TCP        60 80 → 56850 [FIN, ACK] Seq=447 Ack=502 Win=6912 Len=0
    38 2.123548     172.16.254.15     192.168.254.254   TCP        54 56850 → 80 [ACK] Seq=502 Ack=448 Win=130816 Len=0
    39 2.128895     172.16.254.15     192.168.254.254   TCP        54 56850 → 80 [FIN, ACK] Seq=502 Ack=448 Win=130816 Len=0
    40 2.129697     192.168.254.254   172.16.254.15     TCP        60 80 → 56850 [ACK] Seq=448 Ack=503 Win=6912 Len=0
```



Administration système Linux

- Prise en main de l'environnement shell et compréhension de la structure hiérarchique :
    - Utilisation du GameShell pour apprendre les commandes de base
    - Maîtrise des déplacements dans l'arborescence (cd, pwd)
    - Manipulation des fichiers et répertoires (touch, mkdir, rm, cp)
- Gestion des permissions et droits :
    - Compréhension du système de droits Unix (rwx)
    - Modification des permissions avec chmod en notation octale et symbolique
    - Configuration des droits par défaut avec umask
    - Création et gestion de liens physiques et symboliques
- Utilisation avancée du shell :
    - Manipulation des redirections d'entrée/sortie (>, >>, 2>)
    - Utilisation des filtres de base (head, tail, wc)
    - Composition de commandes avec les tubes (|)
    - Travail avec les méta-caractères (*, ?, [ ], { })
- Gestion des processus :
    - Lancement de processus en premier et arrière-plan
    - Manipulation des jobs (fg, bg)
    - Compréhension des signaux (SIGINT, SIGTERM)
    - Utilisation des commandes ps et top pour surveiller les processus
- Configuration de l'environnement :
    - Personnalisation du prompt
    - Configuration du PATH
    - Création d'alias personnalisés
    - Utilisation du fichier .bashrc

Sécurisation système

- Compréhension approfondie des vulnérabilités système et réseau (SAE1.01)

- Mise en place de mesures de sécurité basiques (droits d'accès, filtrage)

- Obtention de la certification SecNumAcadémie avec un score de 100% sur tous les modules [ATTESTATION_SECNUM/1]

Compétences démontrées

- Bonne compréhension des protocoles réseau fondamentaux

- Capacité à analyser et interpréter le trafic réseau

- Maîtrise des bases de l'administration Linux

- Sensibilisation aiguë à la sécurité informatique

Points d'amélioration identifiés

- Besoin de renforcer la maîtrise des commandes Linux avancées, particulièrement pour la gestion des processus et les variables d'environnement

- Améliorer ma compréhension et mon analyse des mécanismes de transfert de fichiers (FTP/TFTP) et des différences entre les protocoles de la couche application

Cette preuve montre une progression constante dans la compréhension et la maîtrise des systèmes d'exploitation, avec un accent particulier sur l'aspect sécurité. Les différents modules ont permis de développer des compétences complémentaires, même si certains aspects plus avancés nécessitent encore du travail.