FISE A5
Informatique
Cybersécurité

Livrable 3 : Fouille

DESGRANGES Thomas
FALIGOT Clémence
NGUYEN Frédéric
SUBTS Yann

CESI_
ÉCOLE D'INGÉNIEURS

SOMMAIRE

DESGRANGES Thomas
FALIGOT Clémence
NGUYEN Frédéric
SUBTS Yann

ADMEC

Catégorie	Outils	Attaque	Criticité	Correction	Prévention
pfSense	Console	Tentatives d'intrusion	15	Améliorer la configuration de pfSense	Autoriser des IPs précises
Proxmox	Syslog	Tentatives d'intrusion	15	Améliorer la configuration de pfSense	Alertes Syslog. Réduire le nombre de tentatives d'accès
Application Web	Logs Wireshark	Tentatives d'intrusion	12	Améliorer la configuration de pfSense	Restreindre l'accès à l'application via un VPN
BDD	Logs Wireshark	Tentatives d'intrusion	20	Restreindre l'accès via IP et empêcher l'accès à la page de connexion	Restreindre l'accès via un VPN.

Gravité	
Gravité = 1	Sans gravité aucune
Gravité = 2	Gravité faible
Gravité = 3	Gravité moyenne
Gravité = 4	Gravité forte
Gravité = 5	Catastrophique
Fréquence	
Fréquence = 1	Rare
Fréquence = 2	Fréquence faible
Fréquence = 3	Fréquence moyenne
Fréquence = 4	Fréquence forte
Fréquence = 5	Certain
Détection	
Détection = 1	Détectable longtemps à l'avance avec possibilité de réaction
Détection = 2	Détectable peu de temps à l'avance avec possibilité de réaction
Détection = 3	Non détectable à l'avance avec possibilité de réaction
Détection = 4	Non détectable à l'avance sans possibilité de réaction

Catégorie	Fréquence	Détection	Gravité	Criticité
pfSense	1	3	5	15
Proxmox	1	3	5	15
Application Web	2	2	3	12
BDD	2	2	5	20

DESGRANGES Thomas
FALIGOT Clémence
NGUYEN Frédéric
SUBTS Yann

POSTE CLIENT

Nous ne remarquons rien sur le poste client qui a été fourni. Pas de compte n'a été ajouté localement, les mots de passe des sessions locales n'ont pas changé.

Le PC Client n'a été accédé.

SERVEUR

Ubuntu

Ls /var/log

Tous les logs de la machine Ubuntu se trouvent dans ces fichiers.

```
pasroot@pasroot-Standard-PC-i440FX-PIIX-1996:/var/log$ ls
alternatives.log  cups              gdm3              openvpn
apache2           dbconfig-common   gpu-manager.log   private
apport.log        dist-upgrade      hp                speech-dispatcher
apport.log.1      dmesg             installer         syslog
apt               dmesg.0           journal           syslog.1
auth.log          dmesg.1.gz        kern.log          syslog.2.gz
auth.log.1        dmesg.2.gz        kern.log.1        ubuntu-advantage.log
auth.log.2.gz     dmesg.3.gz        kern.log.2.gz     ufw.log
boot.log          dmesg.4.gz        lastlog           ufw.log.1
boot.log.1        dpkg.log          mail.log          ufw.log.2.gz
bootstrap.log     faillog           mail.log.1        unattended-upgrades
btmp              fontconfig.log    mysql             wtmp
```

Figure 1 - Différents logs du serveur Linux

Ls -lrt /var/log

Nous pouvons également les lister par date.

```
-rw-r--r--  1 root             root              11056 oct.   4 11:18 fontconfig.log
drwxrwxr-x  2 root             root               4096 oct.   4 11:19 installer
drwxr-sr-x+ 3 root             systemd-journal    4096 oct.   4 11:19 journal
drwx--x--x  2 root             gdm                4096 oct.   4 11:20 gdm3
-rw-r-----  1 root             adm               15195 oct.   4 11:20 dmesg.4.gz
-rw-r-----  1 root             adm                 841 oct.   4 12:05 apport.log.1
-rw-r-----  1 root             adm               15466 oct.   4 13:51 dmesg.3.gz
-rw-r-----  1 root             adm               15257 oct.   4 14:15 dmesg.2.gz
-rw-r-----  1 root             adm               15394 oct.   4 16:44 dmesg.1.gz
drwxr-x---  2 root             adm                4096 oct.   4 22:40 unattended-upgrades
-rw-r-----  1 root             adm               58120 oct.   5 12:34 dmesg.0
-rw-r--r--  1 root             root               1309 oct.   5 17:08 gpu-manager.log
-rw-r-----  1 root             adm               58196 oct.   5 17:08 dmesg
-rw-rw-r--  1 root             utmp               9216 oct.   5 17:08 wtmp
drwxr-xr-x  2 root             root               4096 oct.   5 17:36 dbconfig-common
-rw-r-----  1 root             adm                   0 oct.   6 00:00 apport.log
-rw-------  1 root             root              56871 oct.   6 00:00 boot.log.1
-rw-------  1 root             root                  0 oct.   6 00:00 boot.log
-rw-r--r--  1 root             root              32032 oct.   6 10:32 faillog
-rw-rw-r--  1 root             utmp             292292 oct.   6 10:32 lastlog
-rw-r--r--  1 root             root              39623 oct.   6 10:45 alternatives.log
drwxr-xr-x  2 root             root               4096 oct.   6 10:48 apt
-rw-r--r--  1 root             root            1313900 oct.   6 10:48 dpkg.log
-rw-r-----  1 syslog           adm                4462 oct.   6 11:14 mail.log.1
-rw-r-----  1 syslog           adm                9353 oct.   7 23:23 ufw.log.2.gz
-rw-r-----  1 syslog           adm               11969 oct.   7 23:39 auth.log.2.gz
-rw-r-----  1 syslog           adm              120519 oct.   8 00:00 kern.log.2.gz
-rw-r-----  1 syslog           adm                   0 oct.   8 00:00 mail.log
-rw-r-----  1 syslog           adm              399054 oct.   8 00:00 syslog.2.gz
-rw-r-----  1 syslog           adm              442701 oct.  14 23:35 ufw.log.1
-rw-r-----  1 syslog           adm              442956 oct.  14 23:35 kern.log.1
-rw-r-----  1 syslog           adm              165740 oct.  14 23:39 auth.log.1
-rw-r-----  1 syslog           adm             1050633 oct.  15 00:00 syslog.1
drwxr-x---  2 root             adm                4096 oct.  20 00:00 apache2
```

Figure 2 - Logs du serveur Linux par dates

La phase d'Audit a commencé le 9. Ainsi, ayant repris l'infrastructure le 19, seuls les logs du 9 au 19 nous intéresse.

Après observation des différents logs, nous ne trouvons rien de suspect pour ce qui concerne purement la machine Ubuntu.

Wiresharck

Voulant voir les échanges qu'il y allait avoir sur le réseau, nous avons laisser tourner un wiresharck sur la machine Ubuntu.

Statistiques d'échange

Dans un premier temps, nous avons regardé les statistiques d'échanges afin de repérer toute activité suspecte.

Adresse A	Adresse B	Paquets	Octets	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Début Rel	Durée	Bits/s A → B	Bits/s B → A
10.0.0.46	224.0.0.251	428	54,180 Kio	428	54,180 Kio	0	0 octets	1402.017795	3528.36	0 octets	0 octets
10.0.0.46	224.0.0.252	45	2,845 Kio	45	2,845 Kio	0	0 octets	1402.019384	3528.35	0 octets	0 octets
10.0.0.46	239.255.255.250	984	204,395 Kio	984	204,395 Kio	0	0 octets	1402.246492	3703.19	1 octets	0 octets
10.0.1.3	10.0.0.11	20 683	5,010 Mio	9 121	1,122 Mio	11 562	3,888 Mio	59044.055838	210.15	13 octets	46 octets
10.0.1.3	10.0.0.15	4	336 octets	4	336 octets	0	0 octets	59735.729252	10.862	0 octets	0 octets
10.0.1.3	10.0.3.255	1 002	166,025 Kio	1 002	166,025 Kio	0	0 octets	47778.589349	437.04	1 octets	0 octets
10.0.1.3	224.0.0.251	3 657	448,517 Kio	3 657	448,517 Kio	0	0 octets	47778.594259	446.22	5 octets	0 octets
10.0.1.3	224.0.0.252	560	37,554 Kio	560	37,554 Kio	0	0 octets	47779.018579	349.46	0 octets	0 octets
10.0.1.3	239.255.102.18	360	489,814 Kio	360	489,814 Kio	0	0 octets	23013.711607	602.48	9 octets	0 octets
10.0.1.3	239.255.255.250	4 031	914,329 Kio	4 031	914,329 Kio	0	0 octets	47780.133779	441.65	10 octets	0 octets
10.0.1.4	10.0.3.255	24	2,578 Kio	24	2,578 Kio	0	0 octets	26613.149225	306.285	41 octets	0 octets
10.0.1.4	224.0.0.251	65	8,941 Kio	65	8,941 Kio	0	0 octets	26613.093603	71.514	84 octets	0 octets
10.0.1.4	239.255.255.250	59	25,186 Kio	59	25,186 Kio	0	0 octets	26614.639559	21.825	223 octets	0 octets
10.0.1.5	10.0.0.11	101	6,480 Kio	99	6,363 Kio	2	120 octets	31785.360971	6.3885	3,105 Kio	58 octets
10.0.1.5	10.0.3.255	75	8,004 Kio	75	8,004 Kio	0	0 octets	30735.493530	11.701	13 octets	0 octets
10.0.1.5	224.0.0.251	124	10,009 Kio	124	10,009 Kio	0	0 octets	30735.436370	16.983	16 octets	0 octets
10.0.1.5	224.0.0.252	27	1,722 Kio	27	1,722 Kio	0	0 octets	30735.562520	07.278	2 octets	0 octets
10.0.1.5	239.255.255.250	233	94,712 Kio	233	94,712 Kio	0	0 octets	30735.572740	76.649	152 octets	0 octets
10.0.1.55	10.0.3.255	393	43,762 Kio	393	43,762 Kio	0	0 octets	79070.182801	748.267	4 octets	0 octets
10.0.1.55	224.0.0.22	302	16,434 Kio	302	16,434 Kio	0	0 octets	79070.107103	842.422	1 octets	0 octets
10.0.1.55	224.0.0.251	126	12,305 Kio	126	12,305 Kio	0	0 octets	79070.112074	745.149	1 octets	0 octets
10.0.1.55	224.0.0.252	65	4,761 Kio	65	4,761 Kio	0	0 octets	79070.112781	745.157	0 octets	0 octets
10.0.1.55	239.255.255.250	96	16,781 Kio	96	16,781 Kio	0	0 octets	79443.991511	474.335	1 octets	0 octets
10.0.1.56	10.0.3.255	276	36,059 Kio	276	36,059 Kio	0	0 octets	53858.416201	837.005	19 octets	0 octets
10.0.1.56	224.0.0.22	320	17,016 Kio	320	17,016 Kio	0	0 octets	53858.418423	134.192	9 octets	0 octets
10.0.1.56	224.0.0.251	205	20,011 Kio	205	20,011 Kio	0	0 octets	53858.427161	133.824	10 octets	0 octets
10.0.1.56	224.0.0.252	100	7,324 Kio	100	7,324 Kio	0	0 octets	53858.427951	133.824	3 octets	0 octets
10.0.1.56	239.255.255.250	19	3,321 Kio	19	3,321 Kio	0	0 octets	54850.964948	303.035	2 octets	0 octets
10.0.2.3	10.0.3.255	77	11,663 Kio	77	11,663 Kio	0	0 octets	16168.067893	01.041	317 octets	0 octets
10.0.2.3	224.0.0.251	83	13,187 Kio	83	13,187 Kio	0	0 octets	16168.022563	62.333	298 octets	0 octets
10.0.2.3	224.0.0.252	5	357 octets	5	357 octets	0	0 octets	16168.026531	38.867	20 octets	0 octets
10.0.2.3	239.255.255.250	62	14,620 Kio	62	14,620 Kio	0	0 octets	16169.566923	04.982	392 octets	0 octets
10.0.2.4	10.0.0.11	16 245	1,513 Mio	11 504	732,633 Kio	4 741	816,277 Kio	47805.160972	147.41	83 octets	92 octets
10.0.2.4	10.0.0.15	2	148 octets	2	148 octets	0	0 octets	47805.285594	99.699	0 octets	0 octets
10.0.2.4	10.0.2.255	6	552 octets	6	552 octets	0	0 octets	47881.815946	60.008	2 octets	0 octets
10.0.2.4	10.0.3.255	423	45,176 Kio	423	45,176 Kio	0	0 octets	47800.487077	426.92	0 octets	0 octets
10.0.2.4	224.0.0.251	1 774	220,712 Kio	1 774	220,712 Kio	0	0 octets	47800.414109	445.78	2 octets	0 octets
10.0.2.4	224.0.0.252	123	8,465 Kio	123	8,465 Kio	0	0 octets	47805.147637	699.51	0 octets	0 octets
10.0.2.4	239.255.255.250	3 876	1,274 Mio	3 876	1,274 Mio	0	0 octets	47801.971529	457.52	17 octets	0 octets
169.254.33.31	169.254.255.255	33	3,387 Kio	33	3,387 Kio	0	0 octets	1105.432526	595.188	17 octets	0 octets

Figure 3 - Statistiques Wireshark

On remarque alors des adresses qui n'étaient pas dans notre configuration d'origine, à savoir :

- 10.0.1.3
- 10.0.1.4
- 10.0.1.5
- 10.0.2.3
- 10.0.2.4

On peut donc appliquer des filtres sur ces adresses afin de filtrer tous les échanges ayant eu lieu durant la période d'attaque.

Filtre : 10.0.1.3

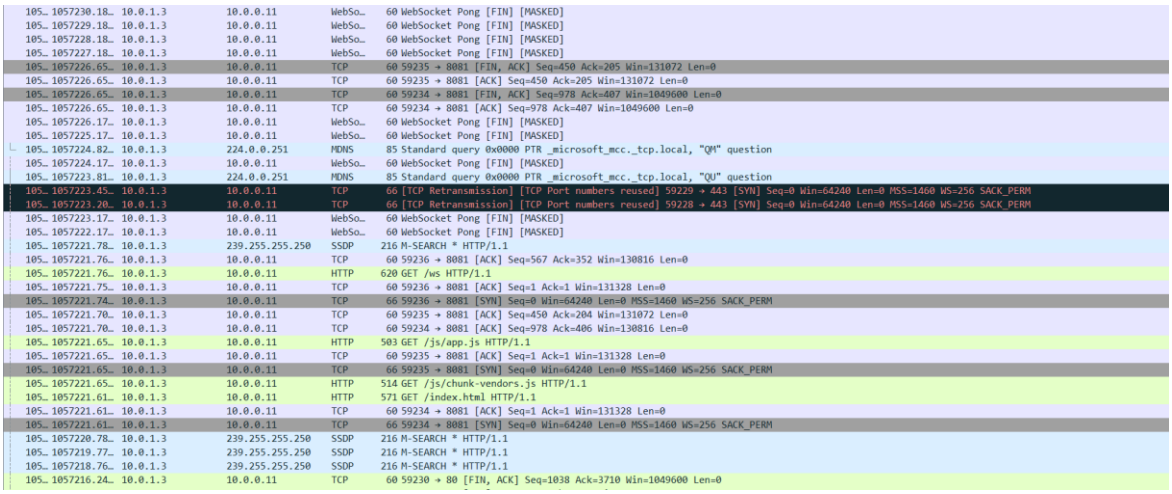


Figure 4 - Requêtes HTTP (port 80), découverte de la BDD (port 8081)

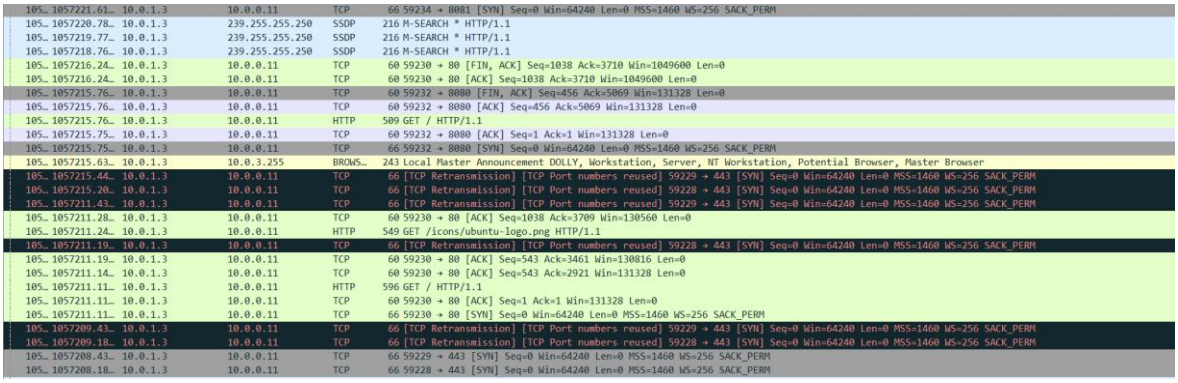


Figure 5 - Requêtes HTTP (port 80), découverte de la BDD (port 8080)

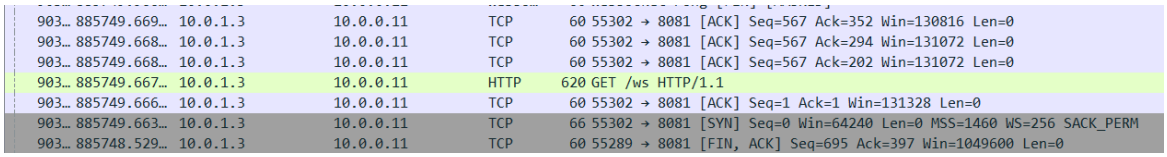


Figure 6 - Requêtes HTTP (port 80), découverte de la BDD (port 8081)

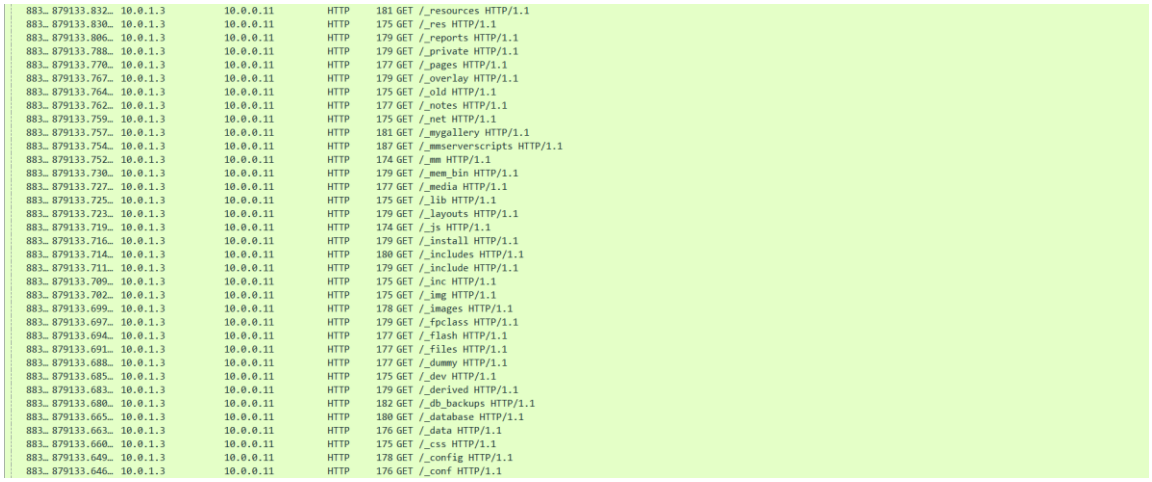


Figure 7 - Requêtes http sur le panneau administrateur de la BDD

DESGRANGES Thomas
FALIGOT Clémence
NGUYEN Frédéric
SUBTS Yann

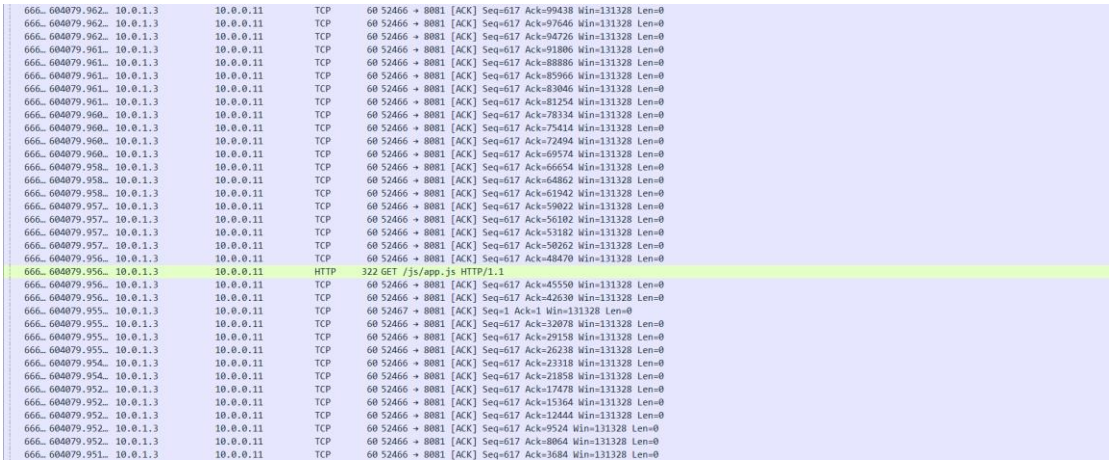


Figure 8 - Requêtes HTTP sur notre application, découverte de la BDD (port 8081)

Filtre : 10.0.1.4

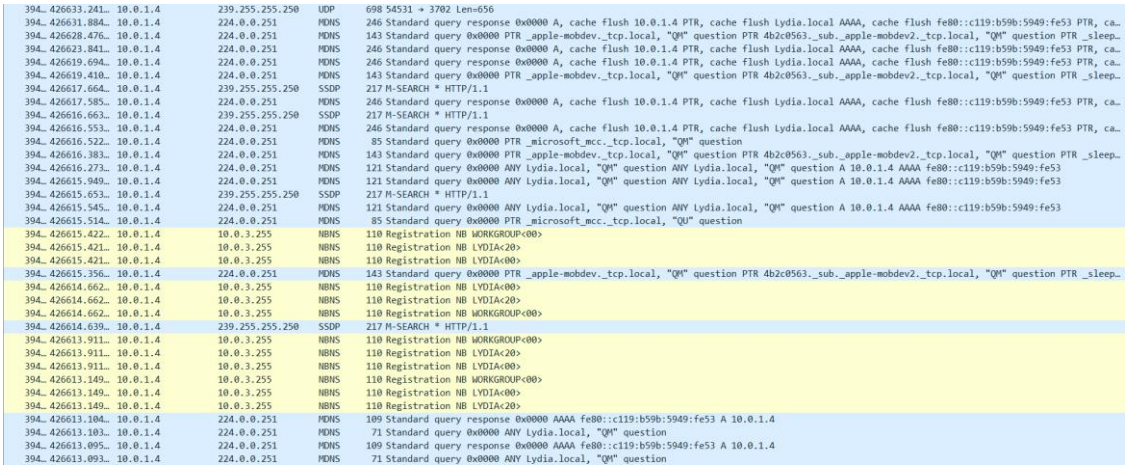


Figure 9 - "LYDIA", il s'agit donc de l'IP d'un membre de l'équipe attaquante

Filtre : 10.0.0.5

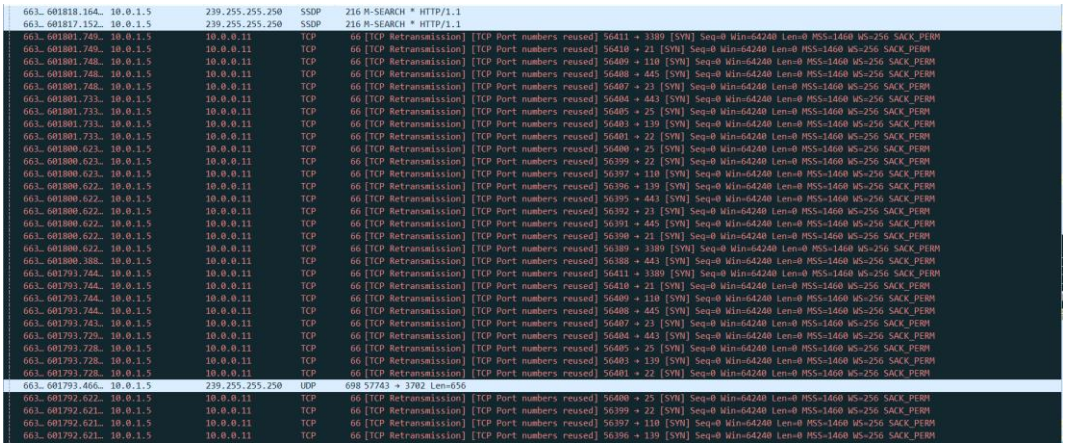
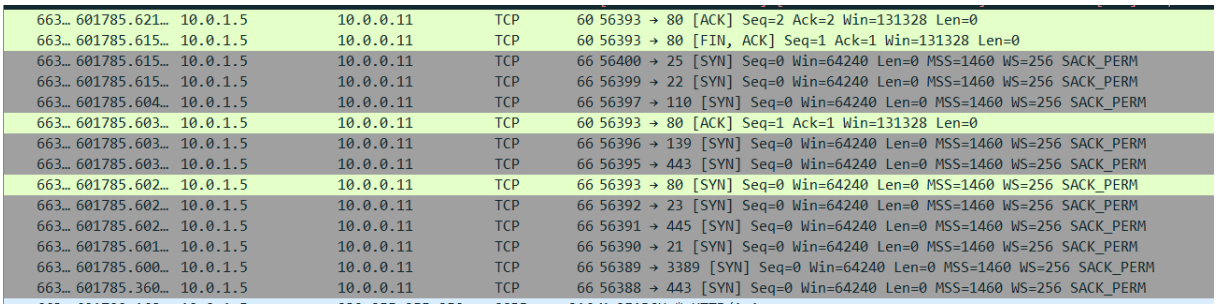


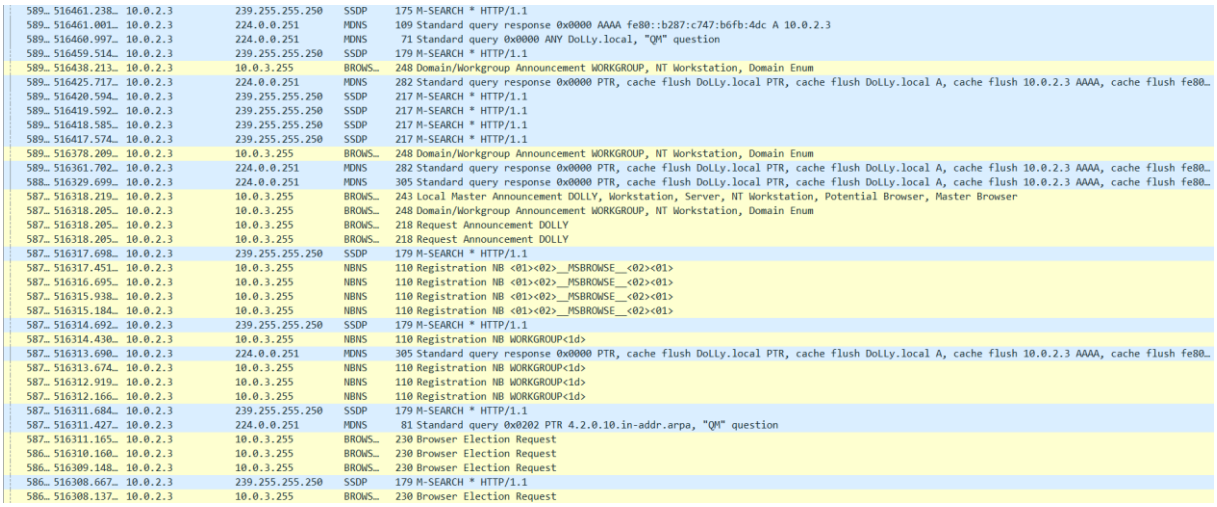
Figure 10 - Tentatives sur plusieurs ports



663…	601785.621…	10.0.1.5	10.0.0.11	TCP	60 56393 → 80 [ACK] Seq=2 Ack=2 Win=131328 Len=0
663…	601785.615…	10.0.1.5	10.0.0.11	TCP	60 56393 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
663…	601785.615…	10.0.1.5	10.0.0.11	TCP	66 56400 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
663…	601785.615…	10.0.1.5	10.0.0.11	TCP	66 56399 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
663…	601785.604…	10.0.1.5	10.0.0.11	TCP	66 56397 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
663…	601785.603…	10.0.1.5	10.0.0.11	TCP	60 56393 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
663…	601785.603…	10.0.1.5	10.0.0.11	TCP	66 56396 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
663…	601785.603…	10.0.1.5	10.0.0.11	TCP	66 56395 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
663…	601785.602…	10.0.1.5	10.0.0.11	TCP	66 56393 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
663…	601785.602…	10.0.1.5	10.0.0.11	TCP	66 56392 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
663…	601785.602…	10.0.1.5	10.0.0.11	TCP	66 56391 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
663…	601785.601…	10.0.1.5	10.0.0.11	TCP	66 56390 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
663…	601785.600…	10.0.1.5	10.0.0.11	TCP	66 56389 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
663…	601785.360…	10.0.1.5	10.0.0.11	TCP	66 56388 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Figure 11 - Port 80 accessible

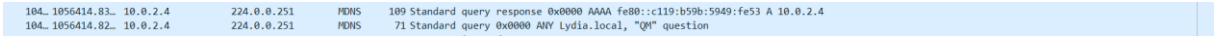
Filtre : 10.0.2.3



589…	516461.238…	10.0.2.3	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
589…	516461.001…	10.0.2.3	224.0.0.251	MDNS	109 Standard query response 0x0000 AAAA fe80::b287:c747:b6fb:4dc A 10.0.2.3
589…	516460.997…	10.0.2.3	224.0.0.251	MDNS	71 Standard query 0x0000 ANY DoLly.local, "QM" question
589…	516459.514…	10.0.2.3	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
589…	516438.213…	10.0.2.3	10.0.3.255	BROWS…	248 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
589…	516425.717…	10.0.2.3	224.0.0.251	MDNS	282 Standard query response 0x0000 PTR, cache flush DoLly.local PTR, cache flush DoLly.local A, cache flush 10.0.2.3 AAAA, cache flush fe80…
589…	516420.594…	10.0.2.3	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
589…	516419.592…	10.0.2.3	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
589…	516418.585…	10.0.2.3	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
589…	516417.574…	10.0.2.3	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
589…	516378.209…	10.0.2.3	10.0.3.255	BROWS…	248 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
589…	516361.702…	10.0.2.3	224.0.0.251	MDNS	282 Standard query response 0x0000 PTR, cache flush DoLly.local PTR, cache flush DoLly.local A, cache flush 10.0.2.3 AAAA, cache flush fe80…
588…	516329.699…	10.0.2.3	224.0.0.251	MDNS	305 Standard query response 0x0000 PTR, cache flush DoLly.local PTR, cache flush DoLly.local A, cache flush 10.0.2.3 AAAA, cache flush fe80…
587…	516318.219…	10.0.2.3	10.0.3.255	BROWS…	243 Local Master Announcement DOLLY, Workstation, Server, NT Workstation, Potential Browser, Master Browser
587…	516318.205…	10.0.2.3	10.0.3.255	BROWS…	248 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
587…	516318.205…	10.0.2.3	10.0.3.255	BROWS…	218 Request Announcement DOLLY
587…	516318.205…	10.0.2.3	10.0.3.255	BROWS…	218 Request Announcement DOLLY
587…	516317.698…	10.0.2.3	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
587…	516317.451…	10.0.2.3	10.0.3.255	NBNS	110 Registration NB <01><02>__MSBROWSE__<02><01>
587…	516316.695…	10.0.2.3	10.0.3.255	NBNS	110 Registration NB <01><02>__MSBROWSE__<02><01>
587…	516315.938…	10.0.2.3	10.0.3.255	NBNS	110 Registration NB <01><02>__MSBROWSE__<02><01>
587…	516315.184…	10.0.2.3	10.0.3.255	NBNS	110 Registration NB <01><02>__MSBROWSE__<02><01>
587…	516314.692…	10.0.2.3	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
587…	516314.430…	10.0.2.3	10.0.3.255	NBNS	110 Registration NB WORKGROUP<1d>
587…	516313.690…	10.0.2.3	224.0.0.251	MDNS	305 Standard query response 0x0000 PTR, cache flush DoLly.local PTR, cache flush DoLly.local A, cache flush 10.0.2.3 AAAA, cache flush fe80…
587…	516313.674…	10.0.2.3	10.0.3.255	NBNS	110 Registration NB WORKGROUP<1d>
587…	516312.919…	10.0.2.3	10.0.3.255	NBNS	110 Registration NB WORKGROUP<1d>
587…	516312.166…	10.0.2.3	10.0.3.255	NBNS	110 Registration NB WORKGROUP<1d>
587…	516311.684…	10.0.2.3	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
587…	516311.427…	10.0.2.3	224.0.0.251	MDNS	81 Standard query 0x0202 PTR 4.2.0.10.in-addr.arpa, "QM" question
587…	516311.165…	10.0.2.3	10.0.3.255	BROWS…	230 Browser Election Request
586…	516310.160…	10.0.2.3	10.0.3.255	BROWS…	230 Browser Election Request
586…	516309.148…	10.0.2.3	10.0.3.255	BROWS…	230 Browser Election Request
586…	516308.667…	10.0.2.3	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
586…	516308.137…	10.0.2.3	10.0.3.255	BROWS…	230 Browser Election Request

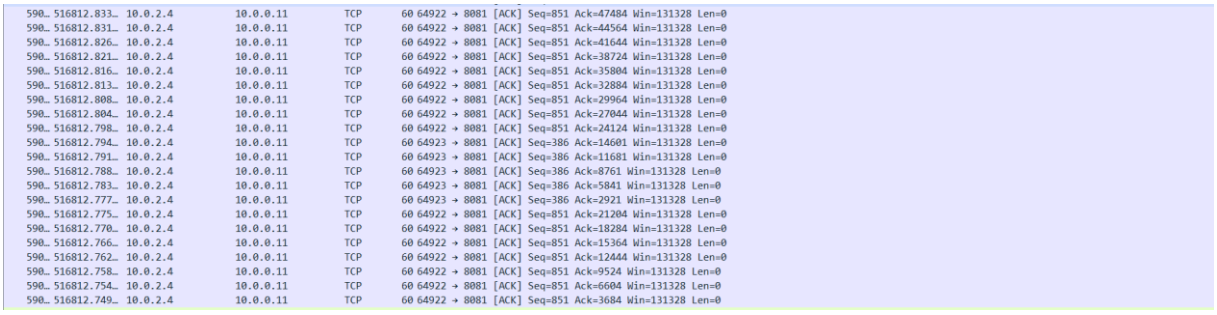
Figure 12 - "Dolly", il s'agit d'une IP de l'équipe attaquante

Filtre : 10.0.2.4



104…	1056414.83…	10.0.2.4	224.0.0.251	MDNS	109 Standard query response 0x0000 AAAA fe80::c119:b59b:5949:fe53 A 10.0.2.4
104…	1056414.82…	10.0.2.4	224.0.0.251	MDNS	71 Standard query 0x0000 ANY Lydia.local, "QM" question

Figure 13 - "Lydia", il s'agit également d'une IP de l'équipe attaquante



590…	516812.833…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=47484 Win=131328 Len=0
590…	516812.831…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=44564 Win=131328 Len=0
590…	516812.826…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=41644 Win=131328 Len=0
590…	516812.821…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=38724 Win=131328 Len=0
590…	516812.816…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=35804 Win=131328 Len=0
590…	516812.813…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=32884 Win=131328 Len=0
590…	516812.808…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=29964 Win=131328 Len=0
590…	516812.804…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=27044 Win=131328 Len=0
590…	516812.798…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=24124 Win=131328 Len=0
590…	516812.794…	10.0.2.4	10.0.0.11	TCP	60 64923 → 8081 [ACK] Seq=386 Ack=14601 Win=131328 Len=0
590…	516812.791…	10.0.2.4	10.0.0.11	TCP	60 64923 → 8081 [ACK] Seq=386 Ack=11681 Win=131328 Len=0
590…	516812.788…	10.0.2.4	10.0.0.11	TCP	60 64923 → 8081 [ACK] Seq=386 Ack=8761 Win=131328 Len=0
590…	516812.783…	10.0.2.4	10.0.0.11	TCP	60 64923 → 8081 [ACK] Seq=386 Ack=5841 Win=131328 Len=0
590…	516812.777…	10.0.2.4	10.0.0.11	TCP	60 64923 → 8081 [ACK] Seq=386 Ack=2921 Win=131328 Len=0
590…	516812.775…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=21204 Win=131328 Len=0
590…	516812.770…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=18284 Win=131328 Len=0
590…	516812.766…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=15364 Win=131328 Len=0
590…	516812.762…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=12444 Win=131328 Len=0
590…	516812.758…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=9524 Win=131328 Len=0
590…	516812.754…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=6604 Win=131328 Len=0
590…	516812.749…	10.0.2.4	10.0.0.11	TCP	60 64922 → 8081 [ACK] Seq=851 Ack=3684 Win=131328 Len=0

Figure 14 - Découverte de la BDD (port 8081)

DESGRANGES Thomas
FALIGOT Clémence
NGUYEN Frédéric
SUBTS Yann

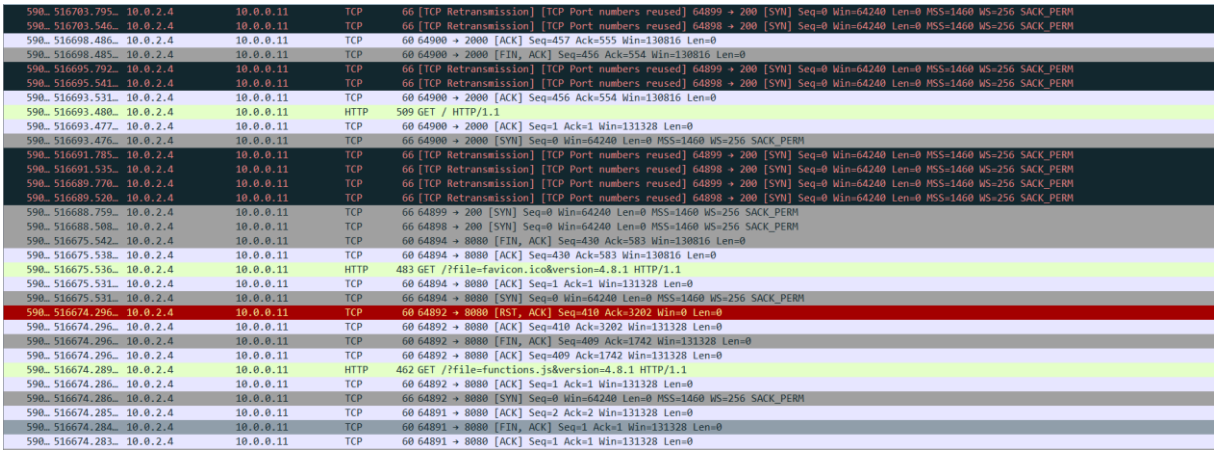


Figure 15 - Tentatives sur plusieurs ports, requêtes HTTP, découverte de la BDD

Sur l'ensemble des captures Wireshark, nous remarquons des requêtes http sur notre application, mais également sur le panneau d'administration de la BDD, ainsi que la découverte de nos bases de données par l'équipe qui réalisait l'attaque.

Pour pallier ce problème, nous pourrions mieux configurer notre pare-feu, afin de limiter l'accès au panneau d'administration des BDD aux personnes concernées.

Proxmox VE

Syslog

Proxmox VE utilise Syslog pour collecter, stocker et gérer les journaux système, ce qui permet alors de suivre l'état et les performances du cluster de virtualisation. Les informations recueillies via Syslog peuvent inclure des données sur les erreurs, les avertissements, les événements importants et d'autres informations de diagnostic. Il est également possible de configurer Proxmox VE pour envoyer les journaux Syslog vers des emplacements distants ou pour les stocker localement.

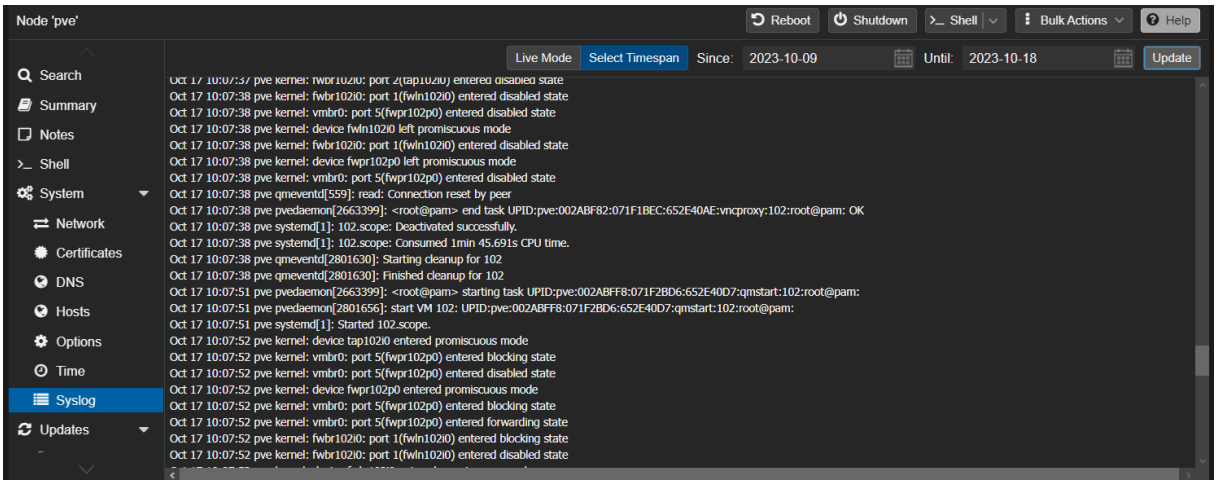


Figure 16 - Outil Syslog sur Proxmox

Ainsi, nous avons pu observer les différentes tentatives d'intrusion sur le serveur Proxmox.

```
Oct 11 15:05:55 pve sshd[1633273]: Invalid user admin from 10.0.1.3 port 52251
Oct 11 15:07:24 pve sshd[1633273]: fatal: Timeout before authentication for 10.0.1.3 port 52251
```

Figure 17 - Tentative d'intrusion Proxmox le 11/10/2023 à 15:05

```
Oct 11 15:27:11 pve sshd[1636414]: Invalid user admin from 10.0.1.3 port 52887
Oct 11 15:27:14 pve sshd[1636414]: pam_unix(sshd:auth): check pass; user unknown
Oct 11 15:27:14 pve sshd[1636414]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 11 15:27:15 pve sshd[1636414]: Failed password for invalid user admin from 10.0.1.3 port 52887 ssh2
Oct 11 15:28:34 pve sshd[1636414]: Connection closed by invalid user admin 10.0.1.3 port 52887 [preauth]
Oct 11 15:43:07 pve sshd[1638731]: Invalid user admin from 10.0.1.3 port 53275
Oct 11 15:44:38 pve sshd[1638731]: Connection closed by invalid user admin 10.0.1.3 port 53275 [preauth]
```

Figure 18 - Tentative d'intrusion Proxmox le 11/10/2023 à 15:27

```
Oct 12 09:59:02 pve sshd[1793014]: Unable to negotiate with 10.0.1.3 port 58417: no matching host key type found. Their offer: ssh-rsa,ssh-dss [preauth]
Oct 12 09:59:58 pve sshd[1793154]: Unable to negotiate with 10.0.1.3 port 58434: no matching host key type found. Their offer: ssh-rsa,ssh-dss [preauth]
Oct 12 10:05:10 pve sshd[1793888]: Unable to negotiate with 10.0.1.3 port 58678: no matching host key type found. Their offer: ssh-rsa,ssh-dss [preauth]
Oct 12 10:05:16 pve sshd[1793896]: Unable to negotiate with 10.0.1.3 port 58681: no matching host key type found. Their offer: ssh-rsa,ssh-dss [preauth]
Oct 12 10:06:12 pve pvedaemon[615119]: authentication failure; rhost=::ffff:10.0.1.3 user=guest@pve msg=no such user ('guest@pve')
Oct 12 10:06:19 pve pvedaemon[613757]: authentication failure; rhost=::ffff:10.0.1.3 user=guest@pam msg=no such user ('guest@pam')
```

Figure 19 - Tentative d'intrusion Proxmox le 12/10/2023 à 09:59

```
Oct 12 10:18:33 pve sshd[1795813]: Unable to negotiate with 10.0.1.3 port 59038: no matching host key type found. Their offer: ssh-rsa,ssh-dss [preauth]
Oct 12 10:18:52 pve pvedaemon[617441]: authentication failure; rhost=::ffff:10.0.1.3 user=guest@pam msg=no such user ('guest@pam')
Oct 12 10:19:04 pve pvedaemon[613757]: authentication failure; rhost=::ffff:10.0.1.3 user=guest@pve msg=no such user ('guest@pve')
Oct 12 10:32:29 pve sshd[1797820]: Invalid user admin from 10.0.1.3 port 58462
Oct 12 10:34:29 pve sshd[1797820]: fatal: Timeout before authentication for 10.0.1.3 port 58462
```

Figure 20 - Tentative d'intrusion Proxmox le 12/10/2023 à 10:18

```
Oct 13 10:05:18 pve sshd[1996441]: Invalid user admin from 10.0.1.3 port 51409
Oct 13 10:05:24 pve sshd[1996441]: Connection closed by invalid user admin 10.0.1.3 port 51409 [preauth]
```

Figure 21 - Tentative d'intrusion Proxmox le 13/10/2023 à 10:05

```
Oct 13 10:23:32 pve sshd[1999060]: error: kex_exchange_identification: Connection closed by remote host
Oct 13 10:23:32 pve sshd[1999060]: Connection closed by 10.0.1.5 port 56421
Oct 13 10:39:52 pve sshd[2001401]: error: kex_exchange_identification: Connection closed by remote host
Oct 13 10:39:52 pve sshd[2001401]: Connection closed by 10.0.1.5 port 56537
```

Figure 22 - Tentative d'intrusion Proxmox le 13/10/2023 à 10:23

```
Oct 13 11:29:30 pve sshd[2008427]: error: kex_exchange_identification: Connection closed by remote host
Oct 13 11:29:30 pve sshd[2008427]: Connection closed by 10.0.1.5 port 56472
Oct 13 11:29:38 pve sshd[2008428]: error: kex_exchange_identification: Connection closed by remote host
Oct 13 11:29:38 pve sshd[2008428]: Connection closed by 10.0.1.5 port 56500
```

Figure 23 - Tentative d'intrusion Proxmox le 13/10/2023 à 11:29

```
Oct 16 11:37:14 pve IPCC.xs[2613004]: pam_unix(proxmox-ve-auth:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost=::ffff:10.0.2.4  user=root
```

Figure 24 - Tentative d'intrusion Proxmox le 16/10/2023 à 11:37

```
Oct 17 09:56:01 pve sshd[2799864]: Invalid user admin from 10.0.1.3 port 64965
Oct 17 09:56:01 pve sshd[2799864]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 09:56:01 pve sshd[2799864]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 17 09:56:02 pve sshd[2799864]: Failed password for invalid user admin from 10.0.1.3 port 64965 ssh2
Oct 17 09:56:03 pve sshd[2799864]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 09:56:05 pve sshd[2799864]: Failed password for invalid user admin from 10.0.1.3 port 64965 ssh2
Oct 17 09:56:05 pve sshd[2799864]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 09:56:07 pve sshd[2799864]: Failed password for invalid user admin from 10.0.1.3 port 64965 ssh2
Oct 17 09:56:08 pve sshd[2799864]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 09:56:09 pve sshd[2799864]: Failed password for invalid user admin from 10.0.1.3 port 64965 ssh2
Oct 17 09:56:10 pve sshd[2799864]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 09:56:12 pve sshd[2799864]: Failed password for invalid user admin from 10.0.1.3 port 64965 ssh2
Oct 17 09:56:12 pve sshd[2799864]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 09:56:14 pve sshd[2799864]: Failed password for invalid user admin from 10.0.1.3 port 64965 ssh2
Oct 17 09:56:14 pve sshd[2799864]: error: maximum authentication attempts exceeded for invalid user admin from 10.0.1.3 port 64965 ssh2 [preauth]
Oct 17 09:56:14 pve sshd[2799864]: Disconnecting invalid user admin 10.0.1.3 port 64965: Too many authentication failures [preauth]
Oct 17 09:56:14 pve sshd[2799864]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 17 09:56:14 pve sshd[2799864]: PAM service(sshd) ignoring max retries; 6 > 3
Oct 17 09:56:14 pve sshd[2799895]: Invalid user admin from 10.0.1.3 port 65072
Oct 17 09:56:14 pve sshd[2799895]: pam_unix(sshd:auth): check pass; user unknown
```

Figure 25 - Tentative d'intrusion Proxmox le 17/10/2023 à 09:56

```
Oct 17 09:56:14 pve sshd[2799895]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 09:56:14 pve sshd[2799895]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 17 09:56:14 pve sshd[2799894]: Invalid user admin from 10.0.1.3 port 65074
Oct 17 09:56:14 pve sshd[2799901]: Invalid user admin from 10.0.1.3 port 65081
Oct 17 09:56:14 pve sshd[2799894]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 09:56:14 pve sshd[2799894]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 17 09:56:14 pve sshd[2799901]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 09:56:14 pve sshd[2799901]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 17 09:56:14 pve sshd[2799896]: Invalid user admin from 10.0.1.3 port 65073
Oct 17 09:56:14 pve sshd[2799902]: Invalid user admin from 10.0.1.3 port 65080
Oct 17 09:56:14 pve sshd[2799902]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 09:56:14 pve sshd[2799902]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 17 09:56:14 pve sshd[2799896]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 09:56:14 pve sshd[2799896]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 17 09:56:14 pve sshd[2799898]: Invalid user admin from 10.0.1.3 port 65077
Oct 17 09:56:14 pve sshd[2799899]: Invalid user admin from 10.0.1.3 port 65075
Oct 17 09:56:14 pve sshd[2799903]: Invalid user admin from 10.0.1.3 port 65079
Oct 17 09:56:14 pve sshd[2799900]: Invalid user admin from 10.0.1.3 port 65078
Oct 17 09:56:14 pve sshd[2799897]: Invalid user admin from 10.0.1.3 port 65076
Oct 17 09:56:14 pve sshd[2799899]: pam_unix(sshd:auth): check pass; user unknown
```

Figure 26 - Tentative d'intrusion Proxmox le 17/10/2023 à 09:56

```
Oct 17 09:56:32 pve sshd[2799897]: error: maximum authentication attempts exceeded for invalid user admin from 10.0.1.3 port 65076 ssh2 [preauth]
Oct 17 09:56:32 pve sshd[2799897]: Disconnecting invalid user admin 10.0.1.3 port 65076: Too many authentication failures [preauth]
Oct 17 09:56:32 pve sshd[2799897]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 17 09:56:32 pve sshd[2799897]: PAM service(sshd) ignoring max retries; 6 > 3
Oct 17 09:56:32 pve sshd[2799945]: Connection closed by invalid user admin 10.0.1.3 port 65186 [preauth]
Oct 17 09:56:32 pve sshd[2799938]: Connection closed by invalid user admin 10.0.1.3 port 65104 [preauth]
Oct 17 09:56:32 pve sshd[2799945]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 17 09:56:32 pve sshd[2799938]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 17 09:56:32 pve sshd[2799938]: PAM service(sshd) ignoring max retries; 5 > 3
Oct 17 09:56:32 pve sshd[2799937]: Connection closed by invalid user admin 10.0.1.3 port 65105 [preauth]
Oct 17 09:56:32 pve sshd[2799937]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.1.3
Oct 17 09:56:32 pve sshd[2799937]: PAM service(sshd) ignoring max retries; 5 > 3
Oct 17 09:56:32 pve sshd[2799966]: Connection closed by invalid user admin 10.0.1.3 port 65196 [preauth]
Oct 17 09:56:32 pve sshd[2799965]: Connection closed by invalid user admin 10.0.1.3 port 65197 [preauth]
```

Figure 27 - Tentative d'intrusion Proxmox le 17/10/2023 à 09:56

Suite à la découverte d'authentifications invalides, nous pouvons mettre en place des mesures d'amélioration comme :

- Configurer des alertes Syslog pour être averti en temps réel des tentatives d'authentification invalides. Cela permet de réagir rapidement en cas d'incident.
- Mettre en place des mécanismes de blocage automatique des adresses IP après un certain nombre de tentatives d'authentification infructueuses. Cela dissuade les attaquants en rendant difficile la poursuite des tentatives.

PfSense

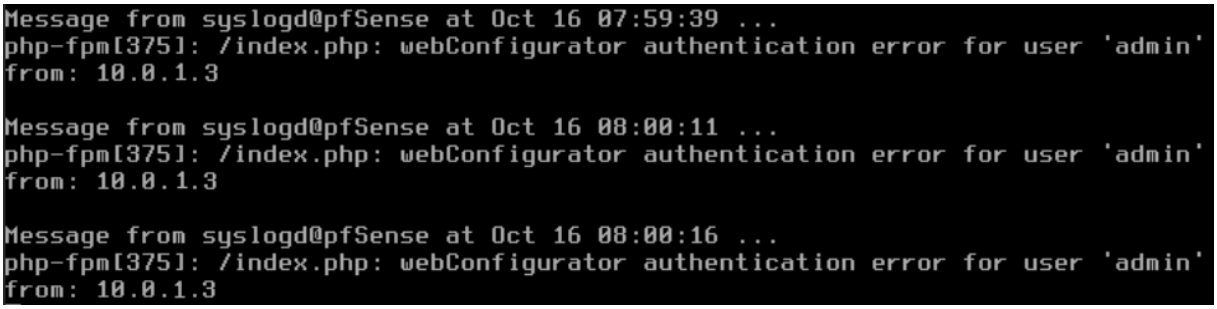


Figure 28 - Tentative de connexion à pfSense depuis le navigateur

Nous avons détecté des tentatives de connexion grâce à la console pfSense, nous avions également mis en place un mécanisme de blocage automatique des adresses IP après un certain nombre de tentatives infructueuses. C'est pour cela qu'il n'y en a que 3. Toutefois, nous pouvons améliorer la sécurité en limitant l'accès à pfSense uniquement aux personnes qui en ont besoin. Les règles de pare-feu doivent être correctement configurées pour ne permettre qu'aux adresses IP autorisées d'accéder à l'interface d'administration. Nous pouvons également configurer des alertes pour être averti en temps réel des tentatives de connexion infructueuses ou suspectes.