REPUBLIQUE TUNISIENNE
Ministère de l'Enseignement Supérieur et de la Recherche
Scientifique Université de Carthage

Institut National des Sciences Appliquées et de Technologie

Compte Rendu d'examen de TP:

Spécialité : Réseaux informatiques et télécommunications

Examen de TP : Evaluation d'une activité malicieuse associée à une attaque par NSM

Présenté par

Eya

Ben Youssef

RT5/1

1. Informations générales (3 points)

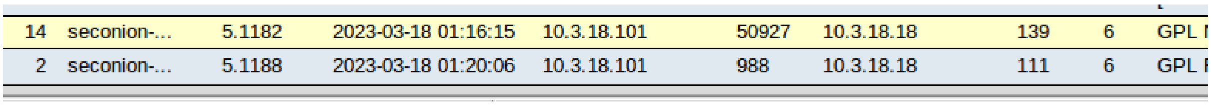
Fenêtre temporelle de l’attaque :

Identifier la date et l’heure du début et de la fin des événements malveillants.

2023-03-18 01:16:15

2023-03-18 01:20:06

⇒Attaque courte (~4 minutes), typique d’une tentative automatisée.

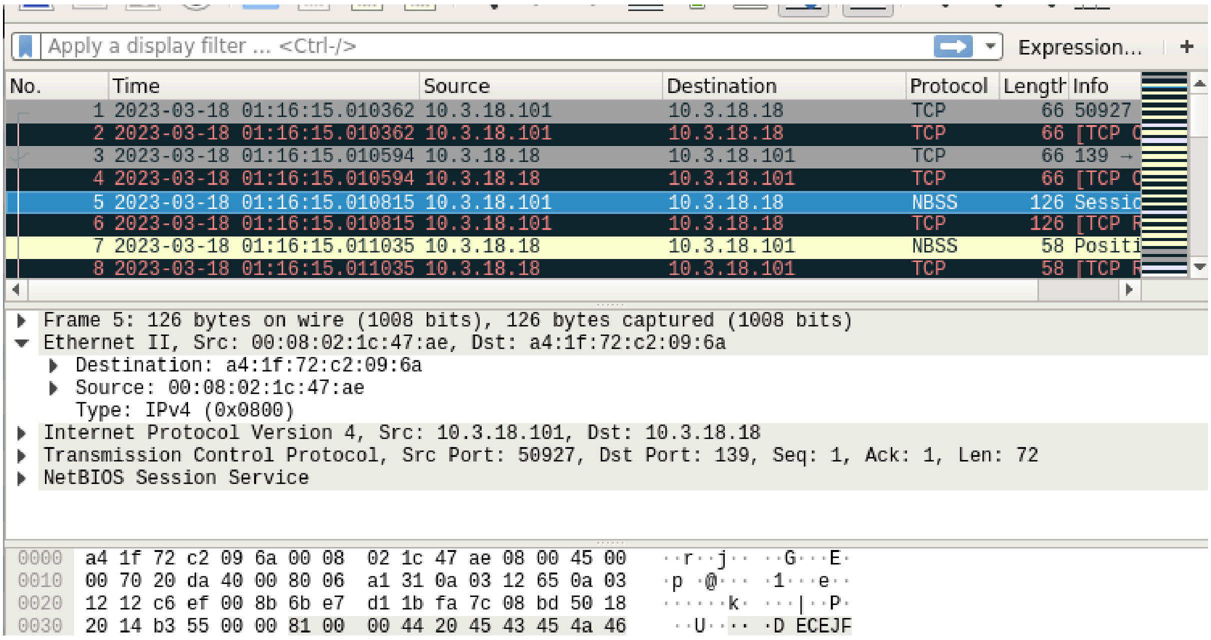


14	seconion-...	5.1182	2023-03-18 01:16:15	10.3.18.101	50927	10.3.18.18	139	6	GPL
2	seconion-...	5.1188	2023-03-18 01:20:06	10.3.18.101	988	10.3.18.18	111	6	GPL

Pour la machine victime, Identifier :

Adresse IP : 10.3.18.101

Adresse MAC: 00:08:02:1c:47:ae

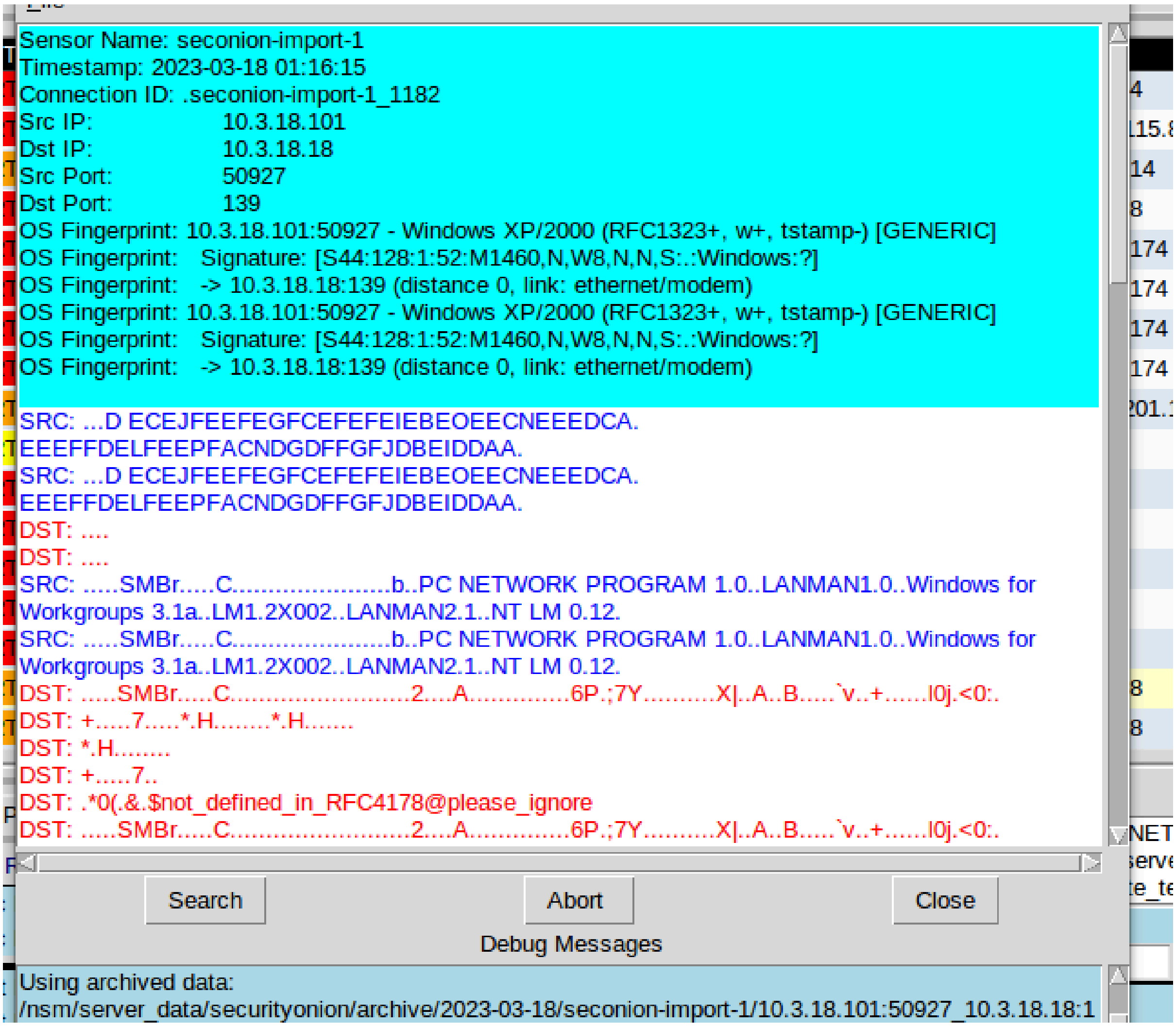


```
No.   Time                        Source          Destination     Protocol Length Info
    1 2023-03-18 01:16:15.010362 10.3.18.101     10.3.18.18      TCP        66 50927
    2 2023-03-18 01:16:15.010362 10.3.18.101     10.3.18.18      TCP        66 [TCP C
    3 2023-03-18 01:16:15.010594 10.3.18.18      10.3.18.101     TCP        66 139 →
    4 2023-03-18 01:16:15.010594 10.3.18.18      10.3.18.101     TCP        66 [TCP C
    5 2023-03-18 01:16:15.010815 10.3.18.101     10.3.18.18      NBSS      126 Sessic
    6 2023-03-18 01:16:15.010815 10.3.18.101     10.3.18.18      TCP       126 [TCP R
    7 2023-03-18 01:16:15.011035 10.3.18.18      10.3.18.101     NBSS       58 Positi
    8 2023-03-18 01:16:15.011035 10.3.18.18      10.3.18.101     TCP        58 [TCP R
```

```
▸ Frame 5: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
▾ Ethernet II, Src: 00:08:02:1c:47:ae, Dst: a4:1f:72:c2:09:6a
   ▸ Destination: a4:1f:72:c2:09:6a
   ▸ Source: 00:08:02:1c:47:ae
     Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.3.18.101, Dst: 10.3.18.18
▸ Transmission Control Protocol, Src Port: 50927, Dst Port: 139, Seq: 1, Ack: 1, Len: 72
▸ NetBIOS Session Service
```

```
0000  a4 1f 72 c2 09 6a 00 08  02 1c 47 ae 08 00 45 00   ··r··j··  ··G···E·
0010  00 70 20 da 40 00 80 06  a1 31 0a 03 12 65 0a 03   ·p ·@···  ·1···e··
0020  12 12 c6 ef 00 8b 6b e7  d1 1b fa 7c 08 bd 50 18   ······k·  ···|··P·
0030  20 14 b3 55 00 00 81 00  00 44 20 45 43 45 4a 46    ··U····  ·D ECEJF
```

Système d’exploitation détecté: Windows XP / Windows 2000



```
Sensor Name: seconion-import-1
Timestamp: 2023-03-18 01:16:15
Connection ID: .seconion-import-1_1182
Src IP:           10.3.18.101
Dst IP:           10.3.18.18
Src Port:         50927
Dst Port:         139
OS Fingerprint: 10.3.18.101:50927 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [S44:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 10.3.18.18:139 (distance 0, link: ethernet/modem)
OS Fingerprint: 10.3.18.101:50927 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [S44:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 10.3.18.18:139 (distance 0, link: ethernet/modem)

SRC: ...D ECEJFEEFEGFCEFEFEIEBEOEECNEEEDCA.
EEEFFDELFEEPFACNDGDFFGFJDBEIDDAA.
SRC: ...D ECEJFEEFEGFCEFEFEIEBEOEECNEEEDCA.
EEEFFDELFEEPFACNDGDFFGFJDBEIDDAA.
DST: ....
DST: ....
SRC: .....SMBr.....C.....................b..PC NETWORK PROGRAM 1.0..LANMAN1.0..Windows for
Workgroups 3.1a..LM1.2X002..LANMAN2.1..NT LM 0.12.
SRC: .....SMBr.....C.....................b..PC NETWORK PROGRAM 1.0..LANMAN1.0..Windows for
Workgroups 3.1a..LM1.2X002..LANMAN2.1..NT LM 0.12.
DST: .....SMBr.....C........................2....A..............6P.;7Y..........X|..A..B.....`v..+......l0j.<0:.
DST: +.....7.....*.H........*.H.......
DST: *.H........
DST: +.....7..
DST: .*0(.&.$not_defined_in_RFC4178@please_ignore
DST: .....SMBr.....C........................2....A..............6P.;7Y..........X|..A..B.....`v..+......l0j.<0:.
```

```
Using archived data:
/nsm/server_data/securityonion/archive/2023-03-18/seconion-import-1/10.3.18.101:50927_10.3.18.18:1
```

Applications clientes utilisées (navigateur, ..):
Port 139 → SMB

Port 111 → RPC

Protocoles : TCP / SMB

Aucun navigateur web détecté

Aucun trafic HTTP/HTTPS observé

2. Analyse SGUIL / Alertes SNORT (3 points)

Alertes totales : 2 (2023-03-18 01:16:15 – 01:20:06)

Alertes & sévérité :

- 5.1182 : SMB IPC$ access → Low/Medium

- 5.1188 : RPC portmap NFS → Low/Medium

IP impliquées : Src 10.3.18.101 → Dst 10.3.18.18

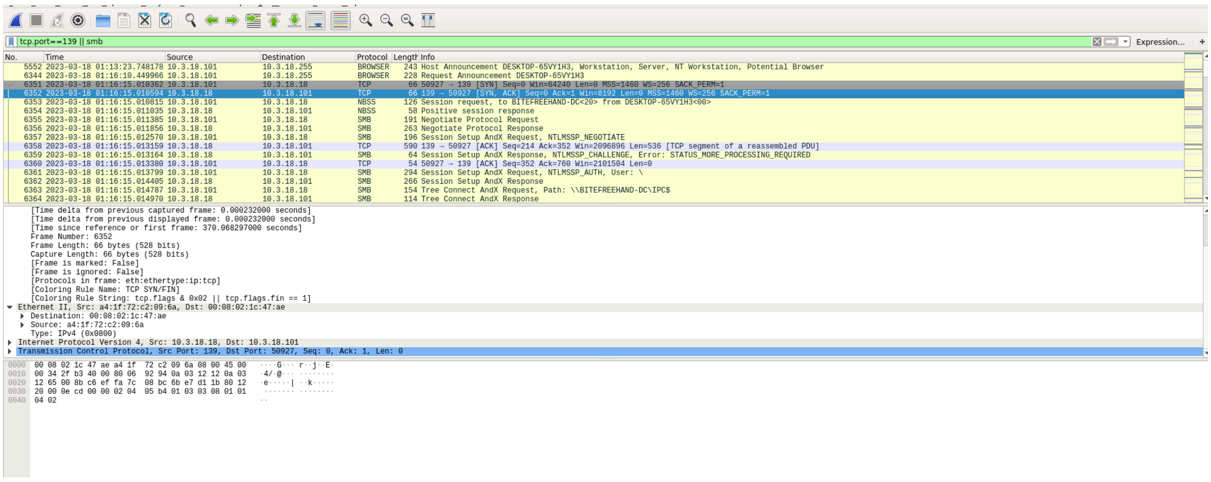
Domaines / URL / URI : Aucun

Observations : SMB/RPC Windows internes, non chiffrés, possibles transferts fichiers / mouvement latéral

3. Analyse Wireshark (3 points)

1/ Alerte 5.1182 – SMB IPC$

filtre tcp



```
tcp.port==139 || smb

No.   Time                        Source        Destination   Protocol Length Info
 5552 2023-03-18 01:13:23.748178 10.3.18.101   10.3.18.255   BROWSER   243 Host Announcement DESKTOP-65VY1H3, Workstation, Server, NT Workstation, Potential Browser
 6344 2023-03-18 01:16:10.449966 10.3.18.101   10.3.18.255   BROWSER   228 Request Announcement DESKTOP-65VY1H3
 6351 2023-03-18 01:16:15.010362 10.3.18.101   10.3.18.18    TCP        66 50927 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 6352 2023-03-18 01:16:15.010594 10.3.18.18    10.3.18.101   TCP        66 139 → 50927 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 6353 2023-03-18 01:16:15.010815 10.3.18.101   10.3.18.18    NBSS      126 Session request, to BITEFREEHAND-DC<20> from DESKTOP-65VY1H3<00>
 6354 2023-03-18 01:16:15.011035 10.3.18.18    10.3.18.101   NBSS       58 Positive session response
 6355 2023-03-18 01:16:15.011385 10.3.18.101   10.3.18.18    SMB       191 Negotiate Protocol Request
 6356 2023-03-18 01:16:15.011856 10.3.18.18    10.3.18.101   SMB       263 Negotiate Protocol Response
 6357 2023-03-18 01:16:15.012570 10.3.18.101   10.3.18.18    SMB       196 Session Setup AndX Request, NTLMSSP_NEGOTIATE
 6358 2023-03-18 01:16:15.013159 10.3.18.18    10.3.18.101   TCP       590 139 → 50927 [ACK] Seq=214 Ack=352 Win=2096896 Len=536 [TCP segment of a reassembled PDU]
 6359 2023-03-18 01:16:15.013164 10.3.18.18    10.3.18.101   SMB        64 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
 6360 2023-03-18 01:16:15.013380 10.3.18.101   10.3.18.18    TCP        54 50927 → 139 [ACK] Seq=352 Ack=760 Win=2101504 Len=0
 6361 2023-03-18 01:16:15.013799 10.3.18.101   10.3.18.18    SMB       294 Session Setup AndX Request, NTLMSSP_AUTH, User: \
 6362 2023-03-18 01:16:15.014405 10.3.18.18    10.3.18.101   SMB       266 Session Setup AndX Response
 6363 2023-03-18 01:16:15.014787 10.3.18.101   10.3.18.18    SMB       154 Tree Connect AndX Request, Path: \\BITEFREEHAND-DC\IPC$
 6364 2023-03-18 01:16:15.014970 10.3.18.18    10.3.18.101   SMB       114 Tree Connect AndX Response

    [Time delta from previous captured frame: 0.000232000 seconds]
    [Time delta from previous displayed frame: 0.000232000 seconds]
    [Time since reference or first frame: 370.068297000 seconds]
    Frame Number: 6352
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP SYN/FIN]
    [Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
▾ Ethernet II, Src: a4:1f:72:c2:09:6a, Dst: 00:08:02:1c:47:ae
  ▸ Destination: 00:08:02:1c:47:ae
  ▸ Source: a4:1f:72:c2:09:6a
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.3.18.18, Dst: 10.3.18.101
▸ Transmission Control Protocol, Src Port: 139, Dst Port: 50927, Seq: 0, Ack: 1, Len: 0

0000  00 08 02 1c 47 ae a4 1f  72 c2 09 6a 08 00 45 00   ····G··· r··j··E·
0010  00 34 2f b3 40 00 80 06  92 94 0a 03 12 12 0a 03   ·4/·@··· ········
0020  12 65 00 8b c6 ef fa 7c  08 bc 6b e7 d1 1b 80 12   ·e·····| ··k·····
0030  20 00 0e cd 00 00 02 04  05 b4 01 03 03 08 01 01    ······· ········
0040  04 02                                               ··
```

Protocole : TCP

Type de paquet : SYN-ACK

Port source : 139 (SMB)

Port destination : 50927 (port client)

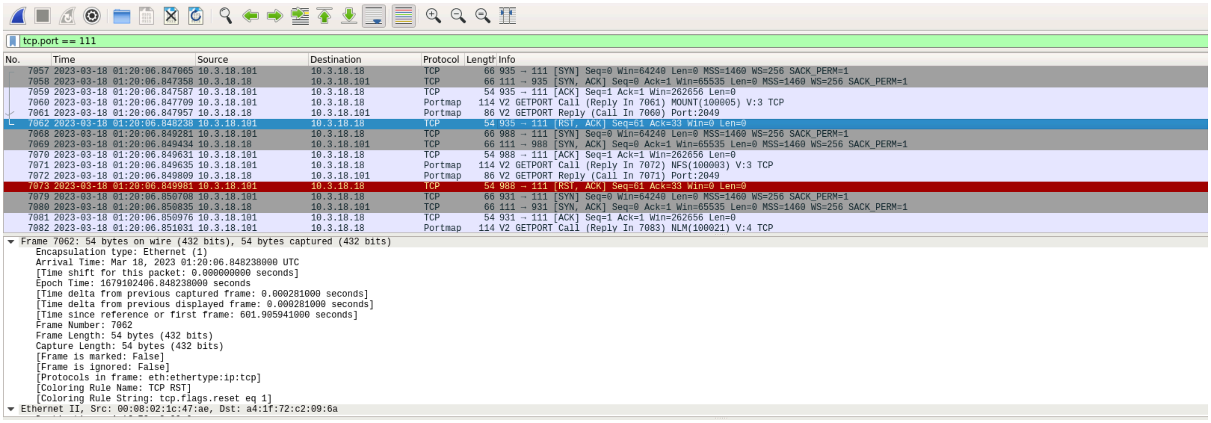
IP source : 10.3.18.18

IP destination : 10.3.18.101

Date/Heure : 2023-03-18 01:16:15

2/ alert 2

filtre tcp.port == 111



tcp.port == 111

```
No.   Time                       Source        Destination   Protocol Length Info
 7057 2023-03-18 01:20:06.847065 10.3.18.101   10.3.18.18    TCP       66 935 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 7058 2023-03-18 01:20:06.847358 10.3.18.18    10.3.18.101   TCP       66 111 → 935 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 7059 2023-03-18 01:20:06.847587 10.3.18.101   10.3.18.18    TCP       54 935 → 111 [ACK] Seq=1 Ack=1 Win=262656 Len=0
 7060 2023-03-18 01:20:06.847709 10.3.18.101   10.3.18.18    Portmap  114 V2 GETPORT Call (Reply In 7061) MOUNT(100005) V:3 TCP
 7061 2023-03-18 01:20:06.847957 10.3.18.18    10.3.18.101   Portmap   86 V2 GETPORT Reply (Call In 7060) Port:2049
 7062 2023-03-18 01:20:06.848238 10.3.18.101   10.3.18.18    TCP       54 935 → 111 [RST, ACK] Seq=61 Ack=33 Win=0 Len=0
 7068 2023-03-18 01:20:06.849281 10.3.18.101   10.3.18.18    TCP       66 988 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 7069 2023-03-18 01:20:06.849434 10.3.18.18    10.3.18.101   TCP       66 111 → 988 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 7070 2023-03-18 01:20:06.849631 10.3.18.101   10.3.18.18    TCP       54 988 → 111 [ACK] Seq=1 Ack=1 Win=262656 Len=0
 7071 2023-03-18 01:20:06.849635 10.3.18.101   10.3.18.18    Portmap  114 V2 GETPORT Call (Reply In 7072) NFS(100003) V:3 TCP
 7072 2023-03-18 01:20:06.849809 10.3.18.18    10.3.18.101   Portmap   86 V2 GETPORT Reply (Call In 7071) Port:2049
 7073 2023-03-18 01:20:06.849981 10.3.18.101   10.3.18.18    TCP       54 988 → 111 [RST, ACK] Seq=61 Ack=33 Win=0 Len=0
 7079 2023-03-18 01:20:06.850708 10.3.18.101   10.3.18.18    TCP       66 931 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 7080 2023-03-18 01:20:06.850835 10.3.18.18    10.3.18.101   TCP       66 111 → 931 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 7081 2023-03-18 01:20:06.850976 10.3.18.101   10.3.18.18    TCP       54 931 → 111 [ACK] Seq=1 Ack=1 Win=262656 Len=0
 7082 2023-03-18 01:20:06.851031 10.3.18.101   10.3.18.18    Portmap  114 V2 GETPORT Call (Reply In 7083) NLM(100021) V:4 TCP
```

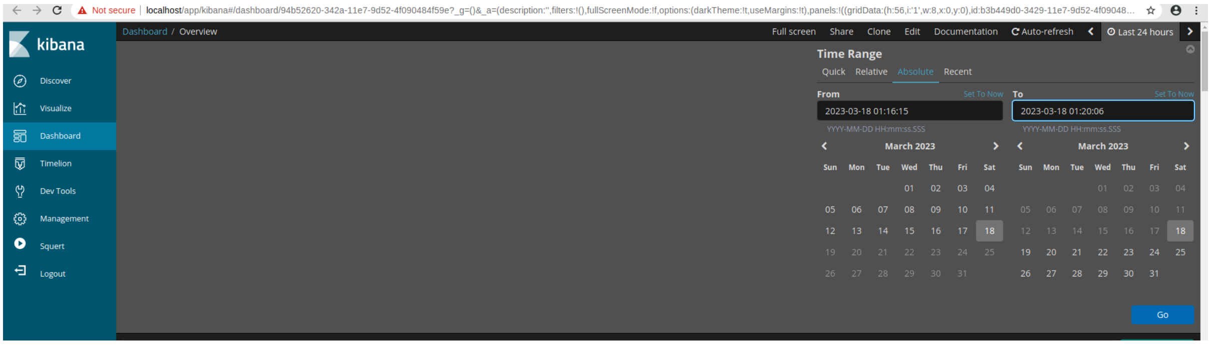
```
▼ Frame 7062: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 18, 2023 01:20:06.848238000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1679102406.848238000 seconds
    [Time delta from previous captured frame: 0.000281000 seconds]
    [Time delta from previous displayed frame: 0.000281000 seconds]
    [Time since reference or first frame: 601.905941000 seconds]
    Frame Number: 7062
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP RST]
    [Coloring Rule String: tcp.flags.reset eq 1]
▼ Ethernet II, Src: 00:08:02:1c:47:ae, Dst: a4:1f:72:c2:09:6a
```

- **Filtre utilisé** : `tcp.port == 111`
- **Protocole** : RPC / Portmap
- **IP source** : 10.3.18.101
- **IP destination** : 10.3.18.18
- **Service ciblé** : NFS / MOUNT / NLM
- **Port retourné** : 2049
- **Date/Heure** : 2023-03-18 01:20:06

🔹 Indices suspects observés

- Requêtes **GETPORT RPC**
- Découverte de services internes
- Usage du **port 111**
- Communication suivie de **RST** (scan rapide)

4. Analyse Kibana (3 points)



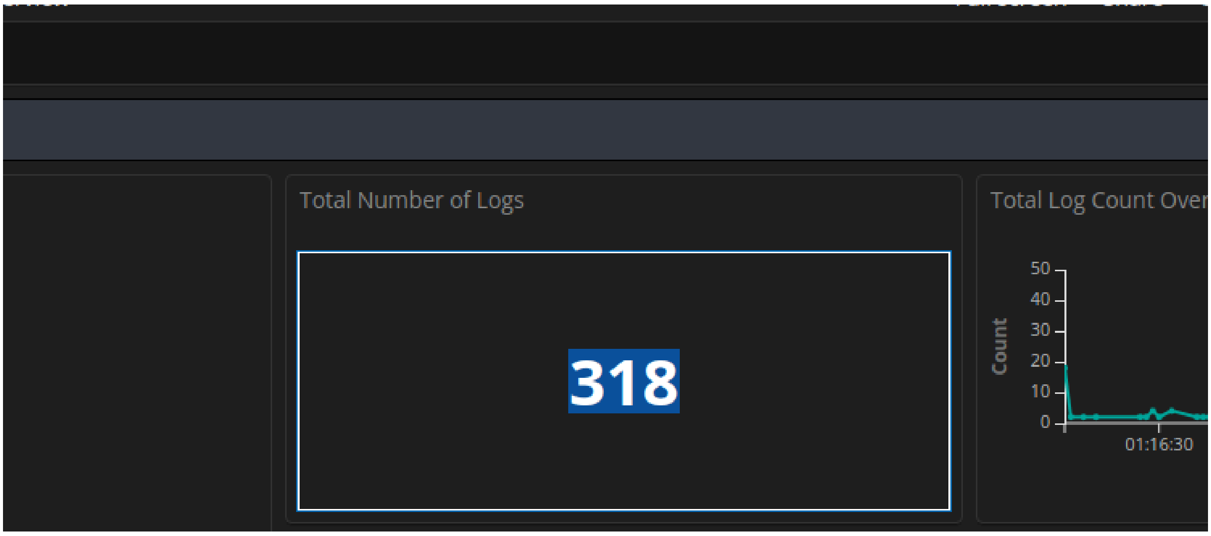
localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=()&_a=(description:'',filters:!(),fullScreenMode:!f,options:(darkTheme:!t,useMargins:!t),panels:!((gridData:(h:56,i:'1',w:8,x:0,y:0),id:b3b449d0-3429-11e7-9d52-4f09048…

Time Range

From: 2023-03-18 01:16:15

To: 2023-03-18 01:20:06

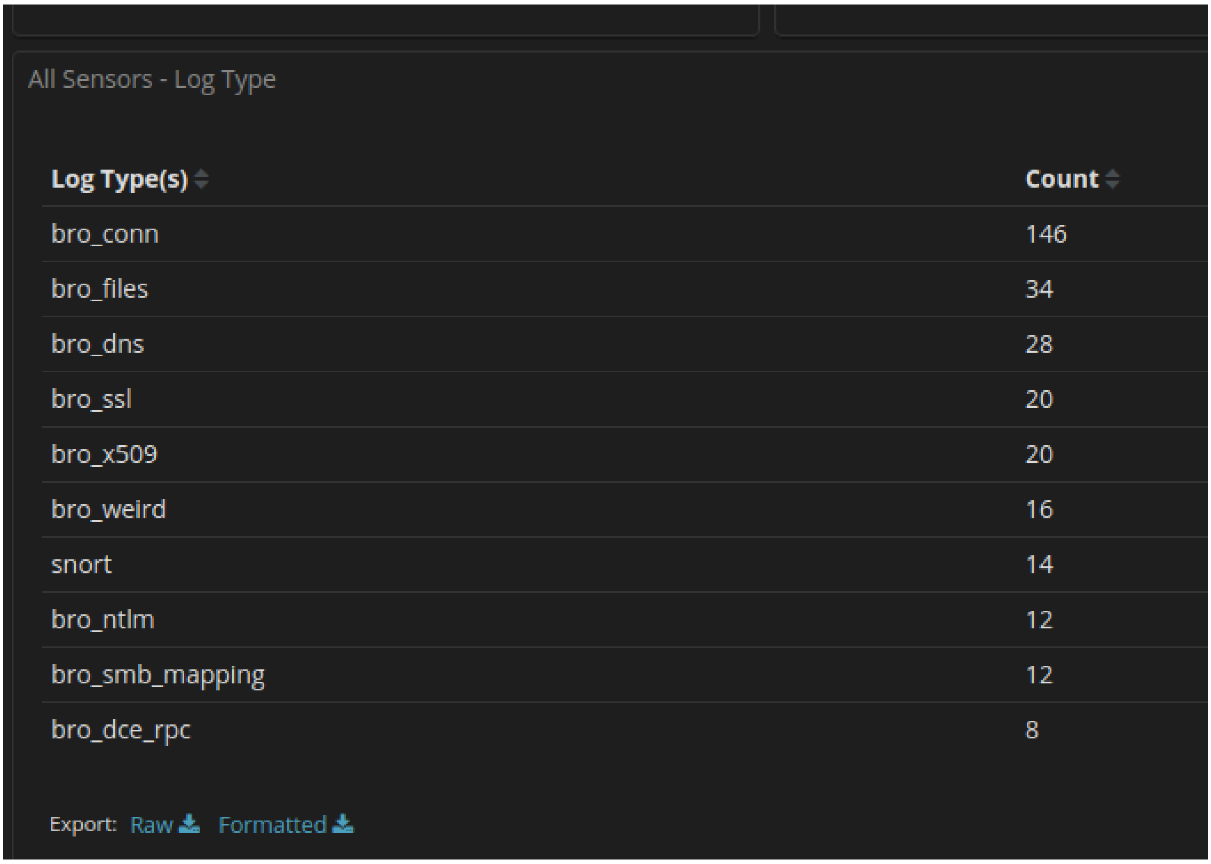
number of logs 318



Total Number of Logs

318

type of logs

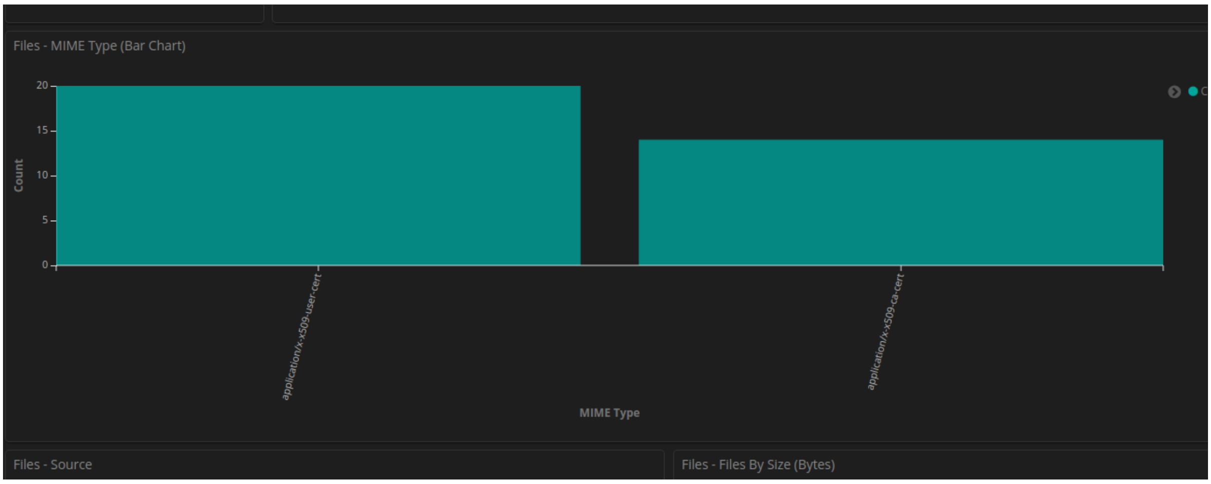


All Sensors - Log Type

Log Type(s)	Count
bro_conn	146
bro_files	34
bro_dns	28
bro_ssl	20
bro_x509	20
bro_weird	16
snort	14
bro_ntlm	12
bro_smb_mapping	12
bro_dce_rpc	8

Export: Raw Formatted

MIME type



Protocoles observés : TCP, SMB, RPC

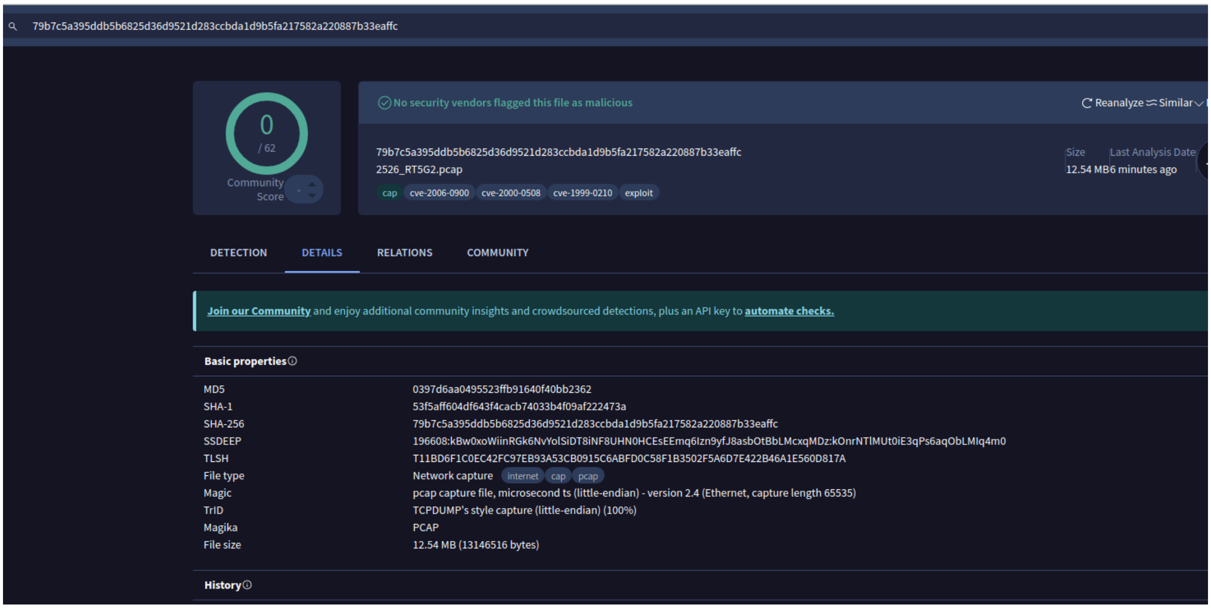
Ports utilisés : 139 (SMB), 111 (RPC), 2049 (NFS)

Connexions : internes Windows / LAN

Aucun téléchargement de fichiers exécutables ou archives détecté (pas de EXE/ZIP/DOC)

5. Analyse de malware (2 points)

avec VirusTotal



79b7c5a395ddb5b6825d36d9521d283ccbda1d9b5fa217582a220887b33eaffc

0 / 62 Community Score

No security vendors flagged this file as malicious

79b7c5a395ddb5b6825d36d9521d283ccbda1d9b5fa217582a220887b33eaffc
2526_RT5G2.pcap

cap cve-2006-0900 cve-2000-0508 cve-1999-0210 exploit

Size	Last Analysis Date
12.54 MB	6 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

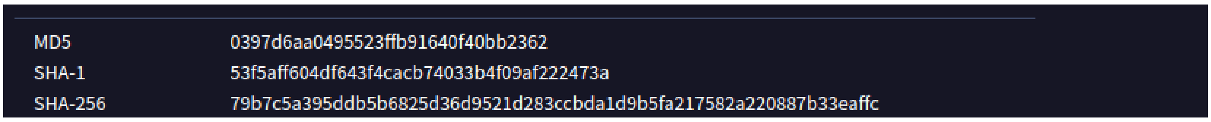
Basic properties

MD5	0397d6aa0495523ffb91640f40bb2362
SHA-1	53f5aff604df643f4cacb74033b4f09af222473a
SHA-256	79b7c5a395ddb5b6825d36d9521d283ccbda1d9b5fa217582a220887b33eaffc
SSDEEP	196608:kBw0xoWiinRGk6NvYolSiDT8iNF8UHN0HCEsEEmq6Izn9yfJ8asbOtBbLMcxqMDz:kOnrNTlMUt0iE3qPs6aqObLMIq4m0
TLSH	T11BD6F1C0EC42FC97EB93A53CB0915C6ABFD0C58F1B3502F5A6D7E422B46A1E560D817A
File type	Network capture internet cap pcap
Magic	pcap capture file, microsecond ts (little-endian) - version 2.4 (Ethernet, capture length 65535)
TrID	TCPDUMP's style capture (little-endian) (100%)
Magika	PCAP
File size	12.54 MB (13146516 bytes)

History

6. Liste des IoCs (2 points)

- **Hashes** :



```
MD5          0397d6aa0495523ffb91640f40bb2362
SHA-1        53f5aff604df643f4cacb74033b4f09af222473a
SHA-256      79b7c5a395ddb5b6825d36d9521d283ccbda1d9b5fa217582a220887b33eaffc
```

  - MD5 : 0397d6aa0495523ffb91640f40bb2362
  - SHA-1 : 53f5aff604df643f4cacb74033b4f09af222473a
  - SHA-256 : 79b7c5a395ddb5b6825d36d9521d283ccbda1d9b5fa217582a220887b33eaffc

- **IP** : 10.3.18.101 (victime), 10.3.18.18 (serveur interne)

9. Conclusion (1 point)

- Attaque courte (~4 min), automatisée
- Exploitation SMB/RPC interne pour reconnaissance et mouvement latéral
- Comportement typique de trojan/downloader
- Recommandations : patchs, segmentation réseau, surveillance IDS/IPS, détection Sigma/YARA