Entraînement

*****

Conseils et astuces en forensics

12/07/2022

\E

ANSSI

whoami

- \E :)
- Epreuves sur le FCSC :
  - 2021 : Ordiphone 1 & 2, Malware 1, 2 & 3 et Sacré jeton, toujours le token pour rire
  - 2022 : C-3PO, R2-D2, R5-D4

Disclaimer

Ce que n'est pas cette présentation :

- Une formation SANS
- Une présentation très technique

Objectif :

- Partager des conseils et astuces en forensics

Plan

- Analyse mémoire
- Récupération de fichiers
- Divers

Analyse mémoire

- Plusieurs types d'images :

Analyse mémoire

- Plusieurs types d'images :
  - Crashdumps (C:\Windows\memory.dmp, C:\Windows\Minidump.dump) : peuvent être analysés avec WinDBG

Analyse mémoire

- Plusieurs types d'images :
  - Crashdumps (C:\Windows\memory.dmp, C:\Windows\Minidump.dump) : peuvent être analysés avec WinDBG
  - Hibernation file (C:\hiberfile.sys)

Hibernation file

- Crée quand une machine est mise en hibernation
- Conversion parfois nécessaire :
  - Hibr2bin :
    - https://github.com/comaeio/Hibr2Bin, ancienne version compilée : https://github.com/Crypt2Shell/Comae-Toolkit
  - Hibernation Recon :
    - https://arsenalrecon.com/downloads/

Analyse mémoire

- Plusieurs types d'images :
  - Crashdumps (C:\Windows\memory.dmp, C:\Windows\Minidump.dump) : peuvent être analysés avec WinDBG
  - Hibernation file (C:\hiberfile.sys)
  - VirtualBox Snapshots

VirtualBox Snapshots

- Fichiers au format .sav crées quand une VM est suspendue ou qu'un instantané d'une VM est créée

```
$ hd bin.sav | head -n 2
00000000  7f 56 69 72 74 75 61 6c  42 6f 78 20 53 61 76 65  |.VirtualBox Save|
00000010  64 53 74 61 74 65 20 56  32 2e 30 0a 00 00 00 00  |dState V2.0.....|
```

- Détails sur le format : https://parsiya.net/blog/2018-01-29-virtualbox-live-state-file-format/
- ASIS Quals 2014 : http://blog.rentjong.net/2014/05/asis-quals-2014-forensic-300.html
- Bitsctf 2017 : https://ox002147.gitlab.io/writeup-bitsctf-for60.html
- Samsung CTF 2021: https://github.com/SSTF-Office/SamsungCTF/blob/main/2021_Hackers_Playground/Remains/exploit/writeup.md


AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Démo

Analyse mémoire

- Plusieurs types d'images :
  - Crashdumps (C:\Windows\memory.dmp, C:\Windows\Minidump.dump) : peuvent être analysés avec WinDBG
  - Hibernation file (C:\hiberfile.sys)
  - VirtualBox Snapshots
  - VirtualBox Core Dump ("dumpvmcore")

Analyse mémoire

- Plusieurs types d'images :
  - Crashdumps (C:\Windows\memory.dmp, C:\Windows\Minidump.dump) : peuvent être analysés avec WinDBG
  - Hibernation file (C:\hiberfile.sys)
  - VirtualBox Snapshots
  - VirtualBox Core Dump ("dumpvmcore")
  - VMWare Snapshots

VMWare Snapshots

- Différents fichiers

Applicable VMWare File Types

File	Usage	Description
.vmx	vmname.vmx	Virtual machine configuration file
.vmxf	vmname.vmxf	Additional virtual machine configuration files
.nvram	vmname.nvram or nvram	Virtual machine BIOS or EFI configuration
.vmsd	vmname.vmsd	Virtual machine snapshots
.vmsn	vmname.vmsn	Virtual machine snapshot data file
.vswp	vmname.vswp	Virtual machine swap file
.vmss	**vmname.vmss**	Virtual machine suspend file
.vmem	**vmware.vmem**	Virtual Machine volatile memory file

.vmss, .vmsn, .vmem
: https://flings.vmware.com/vmss2core

Permet de convertir un snapshot VMWare dans un format utilisable par Volatility (lire le manuel pour les options)

Analyse mémoire

- Plusieurs types d'images :
  - Crashdumps (C:\Windows\memory.dmp, C:\Windows\Minidump.dump) : peuvent être analysés avec WinDBG
  - Hibernation file (C:\hiberfile.sys)
  - VirtualBox Snapshots
  - VirtualBox Core Dump ("dumpvmcore")
  - VMWare Snapshots
  - Linux, Android, MacOS

Analyse mémoire

- Plusieurs types d'images :
  - Crashdumps (C:\Windows\memory.dmp, C:\Windows\Minidump.dump) : peuvent être analysés avec WinDBG
  - Hibernation file (C:\hiberfile.sys)
  - VirtualBox Snapshots
  - VirtualBox Core Dump ("dumpvmcore")
  - VMWare Snapshots
  - Linux, Android, MacOS
- Profils

Profils

- Faire un profil :
  - Windows : volatility -f dump.bin imageinfo
  - Linux/Android :
    - strings dump.bin | grep -i 'Linux version' | uniq doit matcher le uname -a
    - https://andreafortuna.org/2019/08/22/how-to-generate-a-volatility-profile-for-a-linux-system/
    - https://gabrio-tognozzi.medium.com/lime-on-android-avds-for-volatility-analysis-a3d2d89a9dd0
  - MacOS : vol -f dump.bin mac_get_profile

- Tips pour une analyse avec un profil :
  - Sauvegarder les résultats de chaque commande
  - Utiliser le cache : --cache
  - Commencer par un cmdscan/consoles/pstree ou linux_bash/linux_pstree/linux_psaux
  - https://www.echotrail.io/
  - Utiliser linux_recover_filesystem
  - Plugins supplémentaires : https://github.com/volatilityfoundation/community

~~Profils~~

- Quand ne pas faire de profil :
  - Si il s'agit d'un OS propriétaire
  - Si c'est *overkill*

- La plupart des challenges de CTF peuvent se faire sans profil


AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Démo

Profils

- Carving de fichiers avec des motifs connus :
  - Clés SSH
  - auth.log ("sshd]:")
  - Images
  - Strings particulières

  "grep –ai <motif> dump.bin -C 20"

  strings –t d dump.bin > strings_1.txt, strings –t d –e l dump.bin > strings_2.txt, etc.
- Carving "manuel" du .bash_history :

  - grep –ai "/home/" dump.bin : <username>
  - grep –ai "<username>@" dump.bin : <hostname>
  - grep –ai "<username>@<hostname>:" dump.bin : .bash_history.

  ou

  - grep –a "]0;" dump.bin
  - grep -a "\[00m:" dump.bin
  - grep -a "\[01;32m" dump.bin
  - grep -a "\[01;34m" dump.bin

~~Profils~~

- Carving de clés avec aeskeyfind et rsakeyfind :
  - Clés SSH
  - Conteneur LUKS
  - Truecrypt
  - Clés FDE sur des vieux Android
  - Bitlocker
  - Clés WPA :)

- https://github.com/congwang/rsakeyfind
- https://github.com/makomk/aeskeyfind

~~Profils~~

- Carving massif https://github.com/simsong/bulk_extractor : souvent, l'output contient beaucoup de fichiers
- Utile pour les recherches Google et le browsing Web
- Autre utilité en CTF : reconstitution d'un PCAP, peut être un *quick win*

- Alternative : https://github.com/sevagas/swap_digger en spécifiant /dev/tmp en rootfs

~~Profils~~

Carving d'images dans la mémoire :

- Changer l'extension de l'image en .data
- Ouvrir l'image dans GIMP

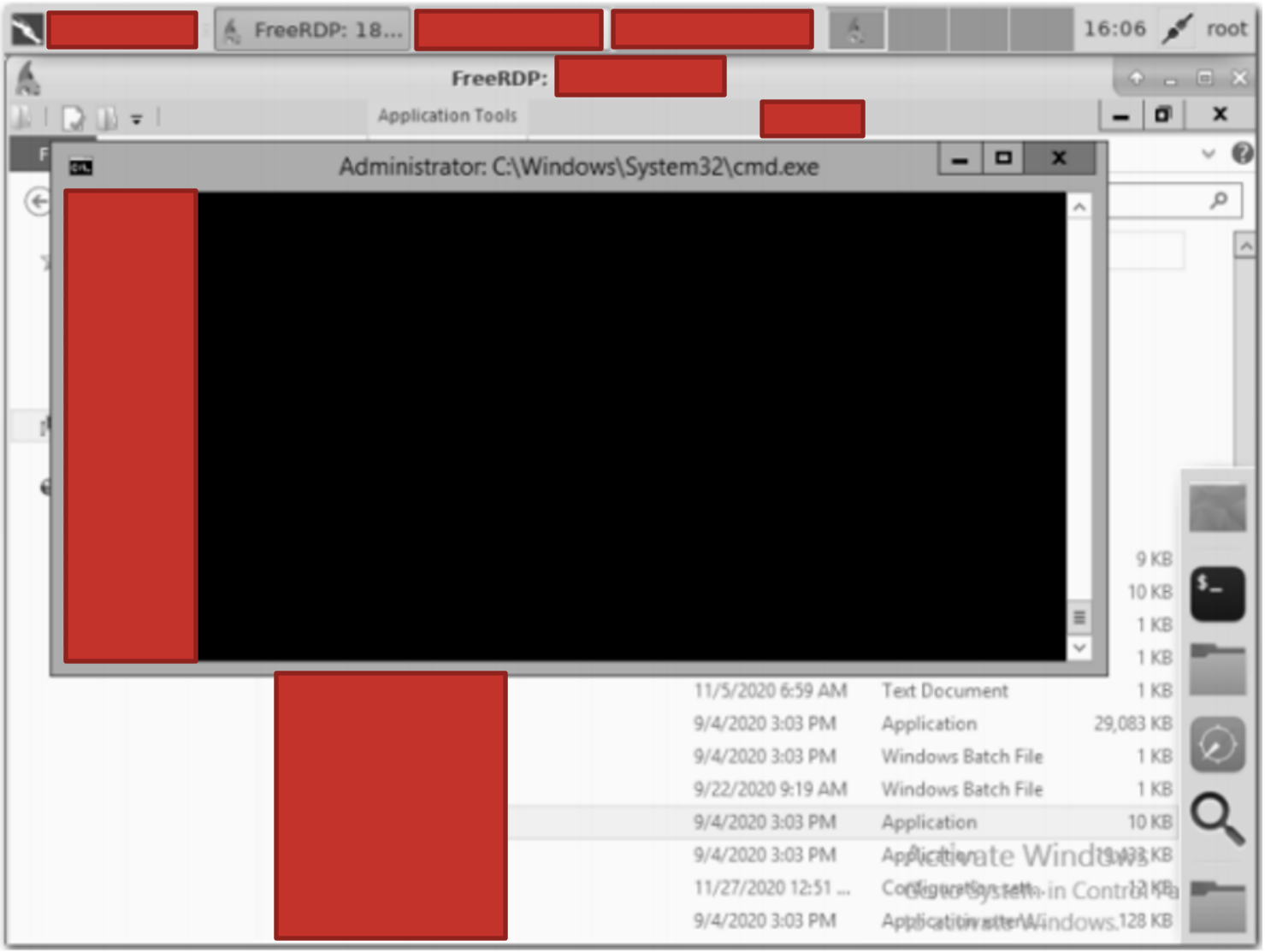
- Configurer la hauteur
- Faire varier la largeur (1920, 1024, 1568, 1457, 1280, 1200, 1067, 2162) et le décalage

- Mieux de targeter un processus en particulier (par exemple, mstsc.exe, mspaint.exe, etc.)

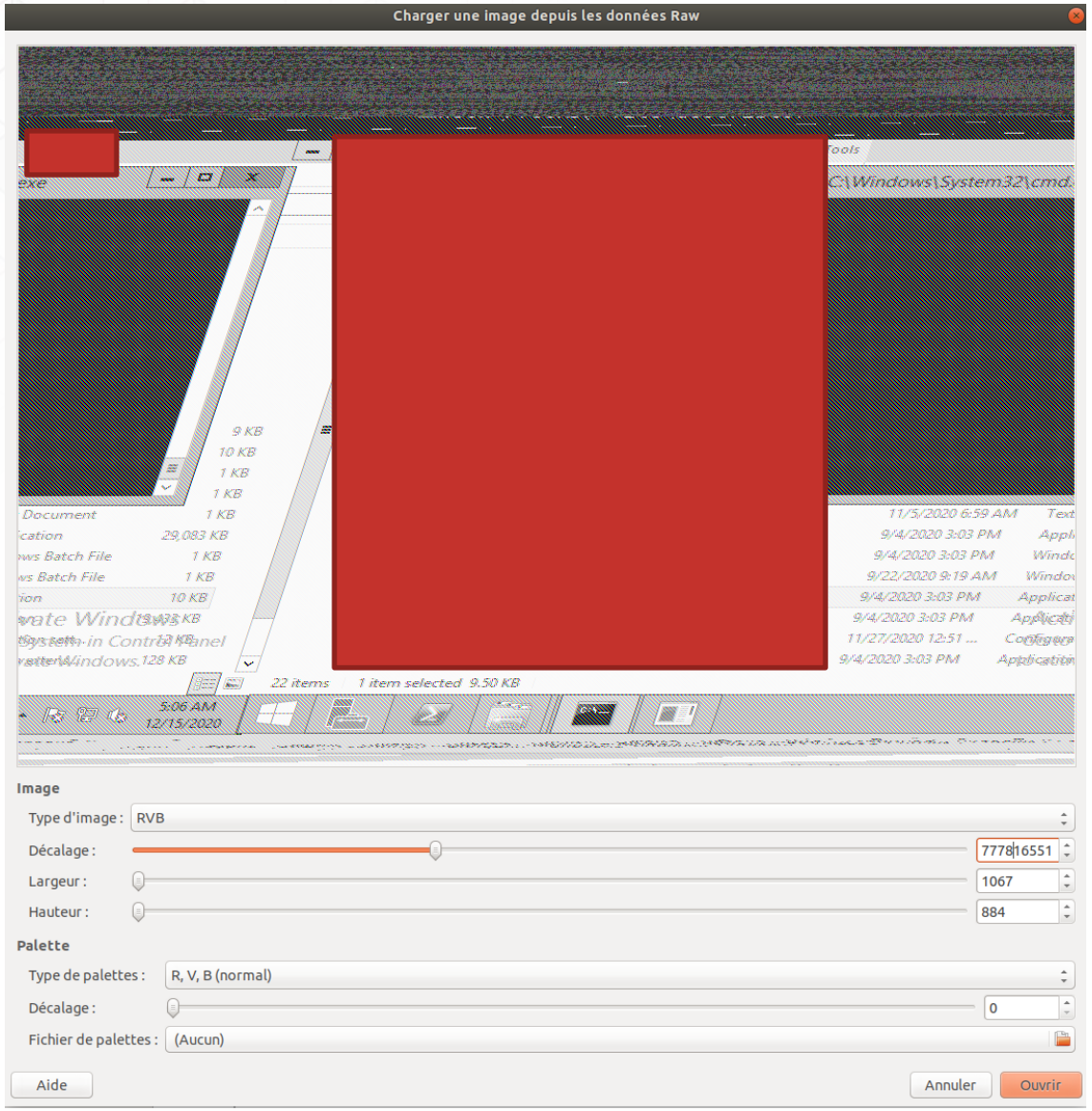
~~Profils~~


Charger une image depuis les données Raw
Untitled - Notepad
File Edit Format View Help
justCTF{7h3r3_15_n0_5uch_7h1n6_45_unh4ck4b13}
Windows (CRLF)
Ln 1, Col 46
190%
Image
Type d'image :
RVB
Décalage :
21467812
Largeur :
2162
Hauteur :
752
Palette
Type de palette :
R, V, B (normal)
Décalage :
0
Fichier de palettes :
(Aucun)
Aide
Annuler
Ouvrir

~~Profils~~


FreeRDP: 18...
16:06
root
FreeRDP:
Application Tools
Administrator: C:\Windows\System32\cmd.exe
9 KB
10 KB
1 KB
1 KB
11/5/2020 6:59 AM Text Document 1 KB
9/4/2020 3:03 PM Application 29,083 KB
9/4/2020 3:03 PM Windows Batch File 1 KB
9/22/2020 9:19 AM Windows Batch File 1 KB
9/4/2020 3:03 PM Application 10 KB
9/4/2020 3:03 PM Application
11/27/2020 12:51 ... Configuration settings
9/4/2020 3:03 PM Application 128 KB

~~Profils~~


Charger une image depuis les données Raw
Image
Type d'image : RVB
Décalage : 7778|16551
Largeur : 1067
Hauteur : 884
Palette
Type de palettes : R, V, B (normal)
Décalage : 0
Fichier de palettes : (Aucun)
Aide
Annuler
Ouvrir

~~Profils~~


AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Démo

Récupération de fichiers

On distingue :

- La récupération de fichiers dont l'entrée dans le système de fichiers est marquée pour suppression : le contenu du fichier existe encore, jusqu'à ce que l'entrée soit réutilisée et les blocs écrasés
- La récupération de fichiers en faisant du carving : recherche de motifs particuliers dans les entrées non allouées du disque

Récupération de fichiers

Récupération de fichiers :

- testdisk : https://www.cgsecurity.org/wiki/TestDisk_FR

Très complet et puissant

A utiliser systématiquement quand on possède une image disque / un device, avant de monter les partitions

Alternative pour le faire à la main : https://www.sleuthkit.org/sleuthkit/man/fls.html

Récupération de fichiers

Carving :

Beaucoup d'outils :

- Recuva
- binwalk
- Foremost
- PhotoRec
- bulk_extractor

Pour le faire à la main (rapidement) :

fdisk –l disk.raw : <block_size>

strings -t d disk.raw | grep <motif> : <offset>

dd if=disk.raw bs=<block_size> skip=<offset> count=<size> of=out

Récupération de fichiers

Carving, tout à la main :

- On cherche un fichier php, effacé de la partition /var d'un disque dont on a l'image. La partition /var commence à l'offset 1365588 dans le disque disque1.dd
- On dump les blocs non alloués : blkls –o 1365588 disque1.dd > blocs_non_alloues.raw
- On cherche la chaine "<?php" dans les blocs non alloués : strings –t d blocs_non_alloues.raw > blocs_non_alloues_offset.txt && grep "<?php" blocs_non_alloues_offset.txt. L'offset 193823148 match
- On convertit l'offset (en octets) en blocs : fsstat –o 1365588 disque1.dd | grep "Block Size". On obtient Block Size = 4096. On veut donc dumper le bloc 193823184/4096, c'est à dire le bloc 47320 dans les blocs non alloués
- On calcule le numéro du bloc dans la partition complète : blkcalc –o 1365588 –u 47320 disque1.dd. On obtient 110599
- On dump le bloc 110599 : blkcat –o 1365588 disque1.dd 110599 | hexdump –C | more
- Si le fichier fait n blocs : blkcat –o 1365588 disque1.dd 110599 n > fichier.php

Divers

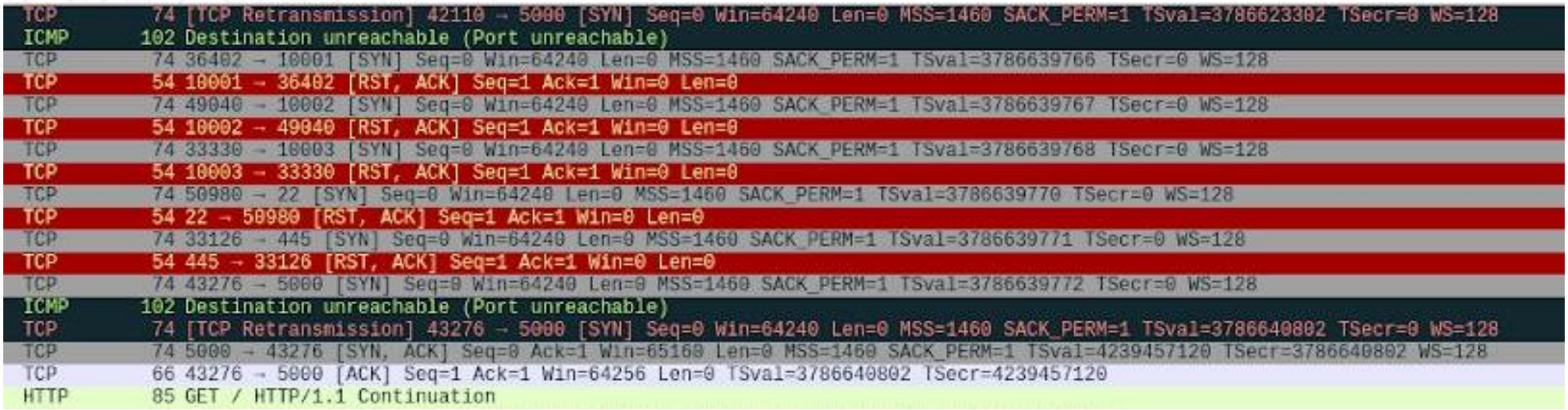
Pour la stégano :

- https://github.com/RickdeJager/stegseek : si steghide <= 0.5.1
- https://github.com/R4yGM/stegbrute : bruteforce en Rust
- https://stegonline.georgeom.net/upload + "CTF CheckList" : visualisation des bit-planes

Pour l'analyse réseau :

- Si peu de trafic : "Follow TCP Stream"
- Sinon, onglet "Statistics" -> "Conversation" -> "TCP" pour identifier une adresse IP malveillante
- Export HTTP objects
- Alternative à Wireshark pour du suivi de sessions VNC (par exemple) : https://github.com/brendangregg/Chaosreader. Nécessite de downgrader le fichier : editcap –F pcap cap.pcap old_format_cap.pcap && ./chaosreader -v old_format_cap.pcap

Divers


TCP 74 [TCP Retransmission] 42110 → 5000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3786623302 TSecr=0 WS=128
ICMP 102 Destination unreachable (Port unreachable)
TCP 74 36402 → 10001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3786639766 TSecr=0 WS=128
TCP 54 10001 → 36402 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP 74 49040 → 10002 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3786639767 TSecr=0 WS=128
TCP 54 10002 → 49040 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP 74 33330 → 10003 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3786639768 TSecr=0 WS=128
TCP 54 10003 → 33330 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP 74 50980 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3786639770 TSecr=0 WS=128
TCP 54 22 → 50980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP 74 33126 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3786639771 TSecr=0 WS=128
TCP 54 445 → 33126 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP 74 43276 → 5000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3786639772 TSecr=0 WS=128
ICMP 102 Destination unreachable (Port unreachable)
TCP 74 [TCP Retransmission] 43276 → 5000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3786640802 TSecr=0 WS=128
TCP 74 5000 → 43276 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=4239457120 TSecr=3786640802 WS=128
TCP 66 43276 → 5000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3786640802 TSecr=4239457120
HTTP 85 GET / HTTP/1.1 Continuation


AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

MERCI