

Ψηφιακά Πειστήρια

1^η Εβδομαδιαία εργασία

Ομάδα 0:

Χρήστος Αργυρόπουλος

Φίλιππος Δουραχαλής

Γεράσιμος Λαπάκης

Βασίλης Μπότσος

A. IPTABLES

- a) Οι εντολές που εκτελέσαμε ήταν οι ακόλουθες:

sudo iptables --policy INPUT DROP

Η παράμετρος --policy καθορίζει την default πολιτική της αλυσίδας κανόνων INPUT, που χρησιμοποιείται για τον έλεγχο εισερχόμενων πακέτων.

Θέλουμε το σύστημα να απορρίπτει όλη την εισερχόμενη κίνηση (DROP), πλην εκείνης που θα εμπίπτει στους κανόνες που ορίζουμε στην συνέχεια.

sudo iptables -A INPUT -p icmp -j ACCEPT

Ορίζουμε ότι τα εισερχόμενα πακέτα θα αντιπαραβάλλονται με τους κανόνες της αλυσίδας INPUT και επιτρέπουμε να περνάνε (-j ACCEPT) μόνο πακέτα του πρωτοκόλλου ICMP

sudo iptables --policy OUTPUT DROP

Αντίστοιχα με πριν, ορίζουμε την default πολιτική χειρισμού πακέτων της αλυσίδας OUTPUT, που χρησιμοποιείται για τον έλεγχο εξερχόμενης κίνησης, σε DROP ώστε να απαγορεύσουμε όλα τα εξερχόμενα πακέτα πλην αυτών που θα συμφωνούν με τους κανόνες που θα θέσουμε.

sudo iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

Προσθέτουμε έναν νέο κανόνα στην αλυσίδα OUTPUT με τον οποίο επιτρέπουμε να περνάνε μόνον πακέτα TCP με θύρα πηγής 80, που χρησιμοποιείται τυπικά από το HTTP.

sudo iptables -A INPUT -p tcp --dport 25 -j LOG --log-prefix 'Incoming connection TCP 25'

Ο κανόνας επιτρέπει εισερχόμενα TCP πακέτα που έχουν ως θύρα προορισμού την 25. Ως ενέργεια για τα πακέτα που ταιριάζουν με αυτόν βάζουμε LOG, που σημαίνει ότι καταγράφεται το πακέτο με το μήνυμα που δίνουμε στο --log-prefix αλλά συνεχίζει να συγκρίνεται με τους υπόλοιπους κανόνες της αλυσίδας.

Συνολικά οι παραπάνω κανόνες φαίνονται στην συνέχεια:

```

philip@philip-VirtualBox:~$ sudo iptables --policy INPUT DROP
[sudo] password for philip:
philip@philip-VirtualBox:~$ sudo iptables -A INPUT -p icmp -j ACCEPT
philip@philip-VirtualBox:~$ sudo iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
philip@philip-VirtualBox:~$ sudo iptables --policy OUTPUT DROP
philip@philip-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 25 -j LOG --log-prefix 'Incoming connection TCP port 25'

```

Εκτελούμε την εντολή “**iptables -L**” και επαληθεύουμε ότι οι κανόνες πέρασαν στις αντίστοιχες αλυσίδες.

```

philip@philip-VirtualBox:~$ sudo iptables -L
[sudo] password for philip:
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT icmp -- anywhere anywhere
LOG tcp -- anywhere anywhere tcp dpt:smtp LOG level warning prefix "Incoming connection TCP port 25"

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy DROP)
target prot opt source destination
ACCEPT tcp -- anywhere anywhere tcp spt:http

```

- b) Εκτελούμε επιπλέον τις εντολές που φαίνονται παρακάτω για να προσθέσουμε τους κανόνες στις αλυσίδες.
- Σημειώνεται ότι οι κανόνες προστίθενται στην αρχή κάθε αλυσίδας. Ο λόγος που γίνεται αυτό είναι διότι κάθε πακέτο (εισερχόμενο ή εξερχόμενο) συγκρίνεται με τη σειρά με κάθε κανόνα στην αντίστοιχη αλυσίδα έως ότου να ταιριάξει με έναν που ορίζει ως ενέργεια την αποδοχή (ACCEPT) ή την απόρριψή του (DROP/REJECT). Σε εκείνο το σημείο το πακέτο χειρίζεται κατάλληλα και το ταίριασμα τερματίζεται. Επομένως ένα πακέτο με διεύθυνση πηγής ή προορισμού 192.168.1.2 θα περάσει αμέσως, ενώ κάποιο από μια άλλη διεύθυνση θα συνεχίσει να συγκρίνεται για να εξεταστεί αν ταιριάζει με κάποιον από τους κανόνες του προηγούμενου ερωτήματος.

sudo iptables -I INPUT -s 192.168.1.2 -j ACCEPT &&

sudo iptables -I INPUT -s 192.168.1.2 -j LOG --log-prefix 'SECURITY'

Οι δύο προηγούμενες εντολές προσθέτουν τους δύο κανόνες στην αρχή της αλυσίδας INPUT (με τον δεύτερο κανόνα να εισάγεται στην πρώτη θέση). Ορίζουμε αρχικά να καταγράφονται (LOG) όλα τα εισερχόμενα πακέτα με διεύθυνση πηγής αυτή του δεύτερου VM με το μήνυμα “SECURITY”. Εφόσον η ενέργεια LOG δεν προκαλεί τον τερματισμό του ταίριασματος του πακέτου, αυτό θα ταιριάξει και με τον δεύτερο κανόνα, ο οποίος επιτρέπει όλα τα πακέτα με την συγκεκριμένη source IP.

sudo iptables -I OUTPUT -d 192.168.1.2 -j ACCEPT &&

sudo iptables -I OUTPUT -d 192.168.1.2 -j LOG --log-prefix 'SECURITY'

Αντίστοιχα με προηγούμενως, ορίζουμε τους συγκεκριμένους κανόνες οι οποίοι θα καταγράψουν και στη συνέχεια θα επιτρέψουν την διέλευση εξερχόμενων πακέτων με διεύθυνση προορισμού αυτή του δεύτερου VM.

```

philip@philip-VirtualBox:~$ sudo iptables -I INPUT -s 192.168.1.2 -j ACCEPT
philip@philip-VirtualBox:~$ sudo iptables -I INPUT -s 192.168.1.2 -j LOG --log-prefix 'SECURITY'
philip@philip-VirtualBox:~$ sudo iptables -I OUTPUT -d 192.168.1.2 -j ACCEPT
philip@philip-VirtualBox:~$ sudo iptables -I OUTPUT -d 192.168.1.2 -j LOG --log-prefix 'SECURITY'

```

Επαληθεύουμε ξανά ότι όλοι οι κανόνες έχουν περάσει στις αντίστοιχες αλυσίδες.

```

philip@philip-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination            LOG level warning prefix "SECURITY"
ACCEPT     all  --  192.168.1.2            anywhere
ACCEPT     icmp --  192.168.1.2            anywhere
LOG         tcp  --  anywhere              anywhere               tcp dpt:smtp LOG level warning prefix "Incoming connection TCP port "

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy DROP)
target     prot opt source                destination            LOG level warning prefix "SECURITY"
ACCEPT     all  --  anywhere              192.168.1.2
ACCEPT     tcp  --  anywhere              192.168.1.2            tcp spt:http

```

Τα iptables by default δεν αποθηκεύουν τους κανόνες που προσθέτουμε. Προκειμένου να μην χαθούν οι κανόνες έπειτα από ένα restart και να μην χρειαστεί να τους ξαναγράψουμε, μπορούμε να δημιουργήσουμε ένα αρχείο όπου θα αποθηκεύονται και να το χρησιμοποιούμε όποτε χρειάζεται.

Αρχικά δημιουργούμε ένα καινούργιο αρχείο όπου θα αποθηκεύονται οι κανόνες μας

“sudo touch /etc/iptables/rules.v4”

Αφού γράψουμε όλους τους παραπάνω κανόνες, τους αποθηκεύουμε με την εντολή

“sudo sh -c iptables-save > /etc/iptables/rules.v4”

Σε κάθε επακόλουθη εκτέλεση μπορούμε να επαναφέρουμε τους κανόνες με την εντολή

“sudo iptables-restore < /etc/iptables/rules.v4”

B. Snort

Για την συγκεκριμένη άσκηση εγκαταστήσαμε το Snort σε ένα VM με λειτουργικό CentOS 7.

Με την εγκατάστασή του Snort, δημιουργείται το ακόλουθο startup script που μας επιτρέπει να τρέχουμε το Snort ως υπηρεσία του Linux κατά την εκκίνηση:

“/etc/rc.d/init.d/snortd”

Ενεργοποιούμε την υπηρεσία με την εντολή:

“systemctl enable snortd.service”

```
[root@localhost ~]# systemctl enable snortd.service
```

Έπειτα παρατηρούμε ότι η υπηρεσία είναι ενεργή ακόμα και μετά από ένα reboot του συστήματος.

```

[root@localhost ~]# systemctl status snortd.service
■ snortd.service - SYSV: snort is a lightweight network intrusion detection tool that currently detects more than 1100 host and network vulnerabilities, portscans, backdoors, and more.
   Loaded: loaded (/etc/rc.d/init.d/snortd; bad; vendor preset: disabled)
   Active: active (exited) since Sat 2022-05-21 00:29:18 EEST; 2h 19min ago
     Docs: man:systemd-sysv-generator(8)

May 21 00:29:18 localhost.localdomain snort[1224]: Autodetect ports (PAF)
May 21 00:29:18 localhost.localdomain snort[1224]: SMB: None
May 21 00:29:18 localhost.localdomain snort[1224]: TCP: 1025-65535
May 21 00:29:18 localhost.localdomain snort[1224]: UDP: 1025-65535
May 21 00:29:18 localhost.localdomain snort[1224]: RPC over HTTP server: 1025-65535
May 21 00:29:18 localhost.localdomain snortd[1201]: Starting snort: Spawning daemon child...
May 21 00:29:18 localhost.localdomain snortd[1201]: My daemon child 1427 lives...
May 21 00:29:18 localhost.localdomain snortd[1201]: Daemon parent exiting (0)
May 21 00:29:18 localhost.localdomain snortd[1201]: [ OK ]
May 21 00:29:18 localhost.localdomain systemd[1]: Started SYSV: snort is a lightweight network ....
Hint: Some lines were ellipsized, use -l to show in full.

```

Στη συνέχεια βρίσκουμε την IP διεύθυνση του μηχανήματός μας με την εντολή **“ifconfig”** και θέτουμε την σταθερά HOME_NET του configuration αρχείου του Snort να δείχνει σε αυτήν. Αυτό είναι χρήσιμο ώστε να μην χρειάζεται να την προσδιορίζουμε ρητά κάθε φορά που θέλουμε να την χρησιμοποιήσουμε στους κανόνες.

```
[root@localhost ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.103 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::22ed:f9b3:6135:da26 prefixlen 64 scopeid 0x20<link>
    inet6 fdfd:3427:2509:0:4d8b:3d7f:7b26:4305 prefixlen 64 scopeid 0x0<global>
    inet6 2a02:2149:8b93:d00:3108:d4be:9c58:1d41 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:de:99:ee txqueuelen 1000 (Ethernet)
    RX packets 14521 bytes 2071473 (1.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 474 bytes 37378 (36.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 48 bytes 4276 (4.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 48 bytes 4276 (4.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Τροποποιούμε το αρχείο παραμετροποίησης με την εντολή :

“sudo nano /etc/snort/snort.conf”

```
[root@localhost ~]# sudo nano /etc/snort/snort.conf

#####
# Step #1: Set the network variables. For more information, see README.variables
#####

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.103

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
```

Τέλος γράφουμε τους κανόνες στο αρχείο **“/etc/snort/rules/local.rules”**. Οι κανόνες αυτοί φαίνονται στην παρακάτω εικόνα.

```
[root@localhost ~]# sudo nano /etc/snort/rules
GNU nano 2.3.1 File: /etc/snort/rules/local.rules

alert icmp any any -> $HOME_NET any (msg:"Ping scan detected"; sid:100001; rev:1;)
alert tcp any any -> $HOME_NET any (flags:S; msg:"TCP scan detected"; sid:100002; rev:1;)
alert tcp any any -> $HOME_NET any (flags:AR; msg:"Potential TCP scan detected - [RST, ACK] received"; sid:100003; rev:1;)
alert tcp any any -> $HOME_NET any (flags:F; msg:"FIN scan detected"; sid:100004; rev:1;)
alert tcp any any -> $HOME_NET any (flags:0; msg:"NULL scan detected"; sid:100005; rev:1;)
alert tcp any any -> $HOME_NET [21,23,2323] (msg:"FTP/Telnet scan detected"; sid:100006; rev:1;)
alert tcp any any -> $HOME_NET [53,137,139] (msg:"DNS/Netbios scan detected"; sid:100007; rev:1;)
alert udp any any -> $HOME_NET [137,138] (msg:"Netbios UDP scan detected"; sid:100008; rev:1;)
alert tcp any any -> $HOME_NET [$HTTP_PORTS,443] (msg:"HTTP/HTTPS scan detected"; sid:100009; rev:1;)

alert tcp any any -> $HOME_NET [6000:6063,1521,1830,1433,1434,5432,3306] (msg:"Detected scan against X11, Oracle DB, MySQL, PostgreSQL or SQL Server"; sid:100010; rev:1;)
alert udp any any -> $HOME_NET 69 (msg:"tFTP scan detected"; sid:100011; rev:1;)
```

Τέλος, επαληθεύουμε ότι το configuration και οι κανόνες είναι σωστά τρέχοντας την εντολή: **“sudo snort -T -c /etc/snort/snort.conf”**

```

Rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!

[ Port Based Pattern Matching Memory ]
[ Number of patterns truncated to 20 bytes: 0 ]

--== Initialization Complete ==--

_ _ _ _ _
o" )~
_ _ _ _ _
    -> Snort! <*-
    Version 2.9.7.5 GRE (Build 262)
    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.
    Using libpcap version 1.5.3
    Using PCRE version: 8.32 2012-11-30
    Using ZLIB version: 1.2.7

    Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
    Preprocessor Object: SF_SSH Version 1.1 <Build 3>
    Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
    Preprocessor Object: SF_SIP Version 1.1 <Build 1>
    Preprocessor Object: SF_SDF Version 1.1 <Build 1>
    Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
    Preprocessor Object: SF_POP Version 1.0 <Build 1>
    Preprocessor Object: SF_MQDBUS Version 1.1 <Build 1>
    Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
    Preprocessor Object: SF_GTP Version 1.1 <Build 1>
    Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
    Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
    Preprocessor Object: SF_DNS Version 1.1 <Build 4>
    Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
    Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>

Snort successfully validated the configuration!
Snort exiting

```

Από ένα διαφορετικό μηχάνημα τρέχουμε διαφορετικά nmap scans και καταγράφουμε τα alerts που εγείρει το snort. Τα διάφορα αποτελέσματα φαίνονται παρακάτω (για λόγους αναγνωσιμότητας κάποιες εικόνες δεν περιέχουν όλες τις γραμμές του output, αλλά αυτές που επιδεικνύουν την καταγραφή των αντίστοιχων scans).

```

04/21-18:44:37.439085  [**] [1:100001:1] Ping scan detected [**] [Priority: 0] {ICMP} 192.168.1.165
-> 192.168.1.103

```

Εικόνα 1 nmap -sn 192.168.56.103

```

04/21-18:54:47.641692  [**] [1:100006:1] FTP/Telnet scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52110 -> 192.168.1.103:2323
04/21-18:54:47.641692  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52110 -> 192.168.1.103:2323
04/21-18:54:47.642703  [**] [1:100006:1] FTP/Telnet scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52111 -> 192.168.1.103:23
04/21-18:54:47.642703  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52111 -> 192.168.1.103:23
04/21-18:54:47.643704  [**] [1:100006:1] FTP/Telnet scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52112 -> 192.168.1.103:21
04/21-18:54:47.643704  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52112 -> 192.168.1.103:21
04/21-18:54:53.638364  [**] [1:100006:1] FTP/Telnet scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52100 -> 192.168.1.103:23
04/21-18:54:53.638364  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52100 -> 192.168.1.103:23
04/21-18:54:53.639451  [**] [1:100006:1] FTP/Telnet scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52109 -> 192.168.1.103:2323
04/21-18:54:53.639451  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52109 -> 192.168.1.103:2323
04/21-18:54:53.650150  [**] [1:100006:1] FTP/Telnet scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52107 -> 192.168.1.103:21
04/21-18:54:53.650150  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52107 -> 192.168.1.103:21
04/21-18:54:55.641095  [**] [1:100006:1] FTP/Telnet scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52110 -> 192.168.1.103:2323
04/21-18:54:55.641095  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52110 -> 192.168.1.103:2323
04/21-18:54:55.642692  [**] [1:100006:1] FTP/Telnet scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52111 -> 192.168.1.103:23
04/21-18:54:55.642692  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52111 -> 192.168.1.103:23
04/21-18:54:55.643678  [**] [1:100006:1] FTP/Telnet scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52112 -> 192.168.1.103:21
04/21-18:54:55.643678  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52112 -> 192.168.1.103:21

```

Εικόνα 2 nmap -Pn -p 21,23,2323 192.168.1.103

```

^[[04/21-18:57:43.804960  [**] [1:100007:1] DNS/Netbios scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52120 -> 192.168.1.103:53
04/21-18:57:43.804960  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52120 -> 192.168.1.103:53
04/21-18:57:43.805071  [**] [1:100007:1] DNS/Netbios scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52121 -> 192.168.1.103:139
04/21-18:57:43.805071  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52121 -> 192.168.1.103:139
04/21-18:57:43.805193  [**] [1:100007:1] DNS/Netbios scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52122 -> 192.168.1.103:137
04/21-18:57:43.805193  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52122 -> 192.168.1.103:137
04/21-18:57:44.805745  [**] [1:100007:1] DNS/Netbios scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52122 -> 192.168.1.103:137
04/21-18:57:44.805745  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52122 -> 192.168.1.103:137
04/21-18:57:44.806761  [**] [1:100007:1] DNS/Netbios scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52120 -> 192.168.1.103:53
04/21-18:57:44.806761  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52120 -> 192.168.1.103:53
04/21-18:57:44.806782  [**] [1:100007:1] DNS/Netbios scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52121 -> 192.168.1.103:139
04/21-18:57:44.806782  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52121 -> 192.168.1.103:139
04/21-18:57:45.808199  [**] [1:100007:1] DNS/Netbios scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52123 -> 192.168.1.103:137
04/21-18:57:45.808199  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52123 -> 192.168.1.103:137
04/21-18:57:45.808325  [**] [1:100007:1] DNS/Netbios scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52124 -> 192.168.1.103:139
04/21-18:57:45.808325  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52124 -> 192.168.1.103:139
04/21-18:57:45.808525  [**] [1:100007:1] DNS/Netbios scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52125 -> 192.168.1.103:53
04/21-18:57:45.808525  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52125 -> 192.168.1.103:53

```

Εικόνα 3 nmap -Pn -p 53,137,139 192.168.1.103


```

^[[A^[[A04/21-18:58:50.024423  [**] [1:100008:1] Netbios UDP scan detected [**] [Priority: 0] {UDP} 192.168.1.165:54479 -> 192.168.1.103:137
04/21-18:58:50.024463  [**] [1:100008:1] Netbios UDP scan detected [**] [Priority: 0] {UDP} 192.168.1.165:54479 -> 192.168.1.103:138
04/21-18:58:52.033285  [**] [1:100008:1] Netbios UDP scan detected [**] [Priority: 0] {UDP} 192.168.1.165:54480 -> 192.168.1.103:138
04/21-18:58:52.033322  [**] [1:100008:1] Netbios UDP scan detected [**] [Priority: 0] {UDP} 192.168.1.165:54480 -> 192.168.1.103:137

```

Εικόνα 4 nmap -Pn -sU -p 137,138 192.168.1.103

```

04/21-19:00:06.755150  [**] [1:100009:1] HTTP/HTTPS scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52149 -> 192.168.1.103:8080
04/21-19:00:06.755150  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52149 -> 192.168.1.103:8080
04/21-19:00:06.756092  [**] [1:100009:1] HTTP/HTTPS scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52147 -> 192.168.1.103:80
04/21-19:00:06.756092  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52147 -> 192.168.1.103:80
04/21-19:00:06.757707  [**] [1:100009:1] HTTP/HTTPS scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52148 -> 192.168.1.103:443
04/21-19:00:06.757707  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52148 -> 192.168.1.103:443
04/21-19:00:07.256727  [**] [1:100009:1] HTTP/HTTPS scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52147 -> 192.168.1.103:80
04/21-19:00:07.256727  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52147 -> 192.168.1.103:80
04/21-19:00:07.259284  [**] [1:100009:1] HTTP/HTTPS scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52148 -> 192.168.1.103:443
04/21-19:00:07.259284  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52148 -> 192.168.1.103:443
04/21-19:00:07.757406  [**] [1:100009:1] HTTP/HTTPS scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52147 -> 192.168.1.103:80
04/21-19:00:07.757406  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52147 -> 192.168.1.103:80
04/21-19:00:07.758137  [**] [1:100009:1] HTTP/HTTPS scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52150 -> 192.168.1.103:8080
04/21-19:00:07.758137  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52150 -> 192.168.1.103:8080
04/21-19:00:07.758304  [**] [1:100009:1] HTTP/HTTPS scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52151 -> 192.168.1.103:443
04/21-19:00:07.758304  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52151 -> 192.168.1.103:443
04/21-19:00:07.759511  [**] [1:100009:1] HTTP/HTTPS scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52148 -> 192.168.1.103:443
04/21-19:00:07.759511  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52148 -> 192.168.1.103:443

```

Εικόνα 5 nmap -Pn -p 80,8080,443 192.168.1.103

```

04/21-19:02:18.555259  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52
170 -> 192.168.1.103:6013
04/21-19:02:18.556208  [**] [1:1000010:1] Detected scan against X11, Oracle DB, MySQL, PostgreSQL or
SQL Server [**] [Priority: 0] {TCP} 192.168.1.165:52174 -> 192.168.1.103:6004
04/21-19:02:18.556208  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52
174 -> 192.168.1.103:6004
04/21-19:02:18.558106  [**] [1:1000010:1] Detected scan against X11, Oracle DB, MySQL, PostgreSQL or
SQL Server [**] [Priority: 0] {TCP} 192.168.1.165:52180 -> 192.168.1.103:6012
04/21-19:02:18.558106  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52
180 -> 192.168.1.103:6012
04/21-19:02:18.559126  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52
176 -> 192.168.1.103:1334
04/21-19:02:18.559601  [**] [1:1000010:1] Detected scan against X11, Oracle DB, MySQL, PostgreSQL or
SQL Server [**] [Priority: 0] {TCP} 192.168.1.165:52178 -> 192.168.1.103:6010
04/21-19:02:18.559601  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52
178 -> 192.168.1.103:6010
04/21-19:02:18.570984  [**] [1:1000010:1] Detected scan against X11, Oracle DB, MySQL, PostgreSQL or
SQL Server [**] [Priority: 0] {TCP} 192.168.1.165:52184 -> 192.168.1.103:6054
04/21-19:02:18.570984  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52
184 -> 192.168.1.103:6054
04/21-19:02:18.571533  [**] [1:1000010:1] Detected scan against X11, Oracle DB, MySQL, PostgreSQL or
SQL Server [**] [Priority: 0] {TCP} 192.168.1.165:52166 -> 192.168.1.103:1433
04/21-19:02:18.571533  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52
166 -> 192.168.1.103:1433
04/21-19:02:18.571554  [**] [1:1000010:1] Detected scan against X11, Oracle DB, MySQL, PostgreSQL or
SQL Server [**] [Priority: 0] {TCP} 192.168.1.165:52172 -> 192.168.1.103:6045
04/21-19:02:18.571554  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52
172 -> 192.168.1.103:6045
04/21-19:02:18.571559  [**] [1:1000010:1] Detected scan against X11, Oracle DB, MySQL, PostgreSQL or
SQL Server [**] [Priority: 0] {TCP} 192.168.1.165:52182 -> 192.168.1.103:6022
04/21-19:02:18.571559  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52
182 -> 192.168.1.103:6022
04/21-19:02:18.571926  [**] [1:1000010:1] Detected scan against X11, Oracle DB, MySQL, PostgreSQL or
SQL Server [**] [Priority: 0] {TCP} 192.168.1.165:52168 -> 192.168.1.103:6031
04/21-19:02:18.571926  [**] [1:100002:1] TCP scan detected [**] [Priority: 0] {TCP} 192.168.1.165:52
168 -> 192.168.1.103:6031

```

Εικόνα 6 nmap -Pn -p 6000-6063,5432,3306,1433,1434,1521,1830 192.168.1.103

```

04/21-19:04:44.550461  [**] [1:1000011:1] tFTP scan detected [**] [Priority: 0] {UDP} 192.168.1.165:
49917 -> 192.168.1.103:69
04/21-19:04:45.550748  [**] [1:1000011:1] tFTP scan detected [**] [Priority: 0] {UDP} 192.168.1.165:
49918 -> 192.168.1.103:69

```

Εικόνα 7 nmap -Pn -sU -p 69 192.168.1.103


Γ. Splunk

Παρουσίαση Splunk

Το Splunk είναι ένα σύστημα SIEM (Security Information & Event Management) με τη δυνατότητα να συλλέγει και να αναλύει logs σε πραγματικό χρόνο. Αποτελείται από τρία (3) μέρη, τον Forwarder, τον Indexer και το Search Head. Ο Forwarder εγκαθίσταται στα endpoints που θέλουμε να παρακολουθήσουμε (πχ servers) και συλλέγει δεδομένα τα οποία προωθεί στο "κέντρο ελέγχου" του Splunk. Εκεί βρίσκονται ο Indexer, ο οποίος επεξεργάζεται και να κανονικοποιεί τα δεδομένα που λαμβάνει από τον Forwarder, και το Search Head, το οποίο χρησιμοποιεί την Splunk Search Processing Language και επικοινωνεί με το Indexer για να κάνει αναζήτηση πάνω στα logs.

Εγκατάσταση Splunk & Διασύνδεση με Snort

Αρχικά φτιάχνουμε λογαριασμό στην ιστοσελίδα του splunk και κατεβάζουμε τα κατάλληλα packages για το λειτουργικό μας (εν προκειμένω Kali). Ταυτόχρονα εγκαθιστούμε το εξής app στο Splunk:

 **Snort Alert for Splunk** Install

This app provides field extractions for Snort alert logs (fast and full) as well as dashboards, saved searches, reports, event types, tags and event search interfaces.

While this app is not formally supported, the developer can be reached at gfransen@splunk.com OR in splunk-usergroups slack, @Guillaume Pierre Fransen. Responses are made on a best effort basis. Feedback is always welcome and appreciated!

[Less](#)

Category: [IT Operations, Utilities](#) | Author: [Splunk Works](#) | Downloads: 1801 | Released: 9 months ago | Last Updated: 5 months ago | [View on Splunkbase](#)

Στη συνέχεια, εγκαθιστούμε και δημιουργούμε account για το splunk:

- `mv ~/Downloads/splunk-9.0.4.1-419ad9369127-linux-2.6-amd64.deb /opt/`
- `sudo apt install /opt/splunk-9.0.4.1-419ad9369127-linux-2.6-amd64.deb`
- `sudo /opt/splunk/bin/splunk start --accept-license`

Παραμετροποιούμε το splunk μέσω του browser και ορίζουμε την θύρα που συλλέγουμε τα logs (έστω την θύρα 9997):

- Επισκεπτόμαστε το <https://localhost:8000>
- Εκτελούμε την εξής ενέργεια: Settings > Forwarding and Receiving > New Receiving Port > 9997


splunk>enterprise 1 3 Messages Settings Activity Help

Receive data New Receiving Port

[Forwarding and receiving](#) > Receive data

Successfully saved "9997".

Showing 1-1 of 1 item



Listen on this port	Status	Acti
9997	Enabled Disable	Del

Εγκαθιστούμε και δημιουργούμε account για το splunk forwarder:

- `mv ~/Downloads/splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb /opt/`
- `sudo apt install /opt/splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb`
- `sudo /opt/splunkforwarder/bin/splunk start --accept-license`

Παραμετροποιούμε το splunk forwarder ορίζοντας τον προορισμό που στέλνει τα logs, τον φάκελο από τον οποίο τα συλλέγει και τις ιδιότητες αυτών (εν προκειμένω το splunk βρίσκεται στο ίδιο μηχάνημα με τον forwarder):

- `sudo /opt/splunkforwarder/bin/splunk add forward-server 127.0.0.1:9997`
- `sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/snort` (εν προκειμένω την τοποθεσία αποθήκευσης των logs του snort)
- `sudo nano /opt/splunkforwarder/etc/apps/search/local/inputs.conf` όπως φαίνεται στο μεθεπόμενο screenshot
- `sudo /opt/splunkforwarder/bin/splunk restart`

```
chrisargy@PenTestVM: /opt/splunkforwarder/etc/system/local
File Actions Edit View Help
GNU nano 7.2 /opt/splunkforwarder/etc/system/local/outputs.conf
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 127.0.0.1:9997

[tcpout-server://127.0.0.1:9997]

chrisargy@PenTestVM: /opt/splunkforwarder/etc/apps/search
File Actions Edit View Help
/opt/splunkforwarder/etc/apps/search/local/inputs.conf
[splunktcp://9997]
connection_host = 127.0.0.1
[monitor:///var/log/snort]
disabled = false
index = main
source_type = snort_alert_full
source = snort
```

Διασύνδεση Splunk με Office 365 & Gsuite

Για τη διασύνδεση με Office 365 και Gsuite απαιτούνται τα δύο παρακάτω apps του Splunk:

Splunk Add-on for Microsoft Office 365

Install

The Splunk Add-on for Microsoft Office 365 allows a Splunk software administrator to pull service status, service messages, and management activity logs from the Office 365 Management API. You can collect:

- * Audit logs for Azure Active Directory, Sharepoint Online, and Exchange Online, supported by the Office 365 Management API.
- * Historical and current service status, and service messages for the corresponding Microsoft Office 365 Management API.
- * Data Loss Prevention on Microsoft Office 365 Management API.

After the Splunk platform indexes the events, you can then directly analyze the data or use it as a contextual data feed to correlate with other data in the Splunk platform

[Less](#)

Category: [IT Operations](#) | Author: [Splunk Inc.](#) | Downloads: 68362 | Released: 4 months ago | Last Updated: 4 months ago | [View on Splunkbase](#)

Gmail Audit

Install

This app provides three main functions for organisations using Google GSuite and Gmail:

- Enable auditing on Gmail inboxes of users in the G Suite Directory and configure email audit events to go to the specified audit recipient inbox
- Retrieve audited emails (headers only) from the audit recipient inbox
- Retrieve the G Suite Directory listing of users and their attributes

Category: [IT Operations](#), [Security](#), [Fraud & Compliance](#) | Author: [Nick von Korff](#) | Downloads: 1285 | Released: 2 years ago | Last Updated: 5 months ago | [View on Splunkbase](#)

Δ. GRR

Η εγκατάσταση του GRR server πραγματοποιήθηκε σε ένα VM με λειτουργικό Linux Mint 21 (Ubuntu 22.04). Ως βάση δεδομένων χρησιμοποιείται η MySQL, η οποία έχει ρυθμιστεί

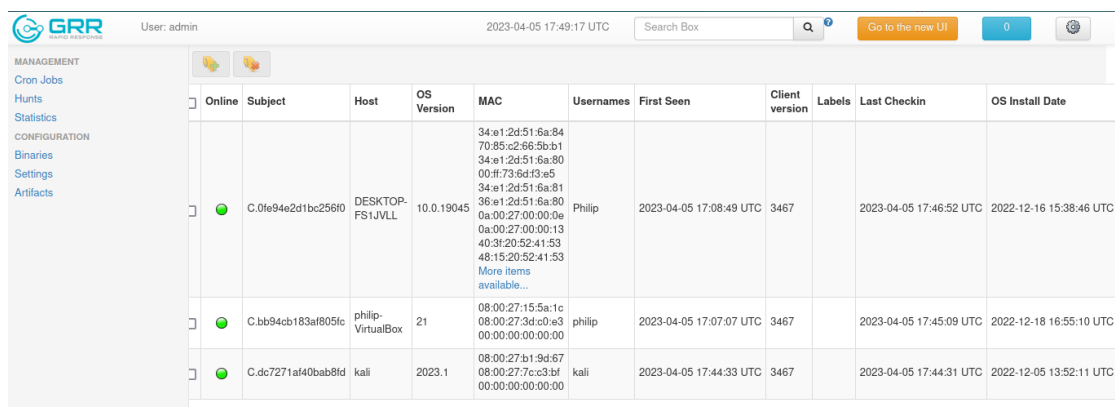
όπως ορίζεται στο documentation¹. Για την παραμετροποίηση του server δίνονται οι ακόλουθες ρυθμίσεις, όπου 192.168.56.105 είναι η διεύθυνση του μηχανήματός μας και 3306 η θύρα στην οποία ακούει η MySQL:

```
AdminUI.port: 8000
AdminUI.url: http://192.168.56.105:8000
Blobstore.implementation: DbBlobStore

Client.fleetspeak_enabled: true
Client.server_urls:
- http://192.168.56.105:8080/
ClientBuilder.fleetspeak_bundled: true
Database.implementation: MySQLDB
FleetspeakFrontend Context:
  Server.fleetspeak_message_listen_address: localhost:11111
Frontend.bind port: 8080

Logging.domain: localhost
Monitoring.alert_email: grr-monitoring@localhost
Monitoring.emergency_access_email: grr-emergency@localhost
Mysql.database: grr
Mysql.database_name: grr
Mysql.database_password: 
Mysql.database_username: grr
Mysql.host: localhost
Mysql.password: 
Mysql.port: 3306
Mysql.username: grr
```

Έχοντας ενεργοποιήσει την υπηρεσία του server, μπορούμε να συνδεθούμε στο admin panel στην διεύθυνση 192.168.56.105:8000 και να κατεβάσουμε τα binaries τα οποία μεταφέρουμε στα μηχανήματα των clients για να τους αρχικοποιήσουμε. Για τους σκοπούς της εργασίας εκκινούμε έναν client σε Windows 10, έναν σε Linux Kali και έναν στο ίδιο μηχανήμα που έχουμε και τον server. Μόλις οι υπηρεσίες των clients ξεκινήσουν, εμφανίζονται στο πάνελ:



Online	Subject	Host	OS Version	MAC	Username	First Seen	Client version	Labels	Last Checkin	OS Install Date
<input type="checkbox"/>				34:e1:2d:51:6a:84 70:85:c2:66:5b:b1 34:e1:2d:51:6a:80 00:ff:73:6d:f3:e5 34:e1:2d:51:6a:81 36:e1:2d:51:6a:80 0a:00:27:00:00:0a 0a:00:27:00:00:13 40:3f:20:52:41:53 48:15:20:52:41:53 More items available...	Philip	2023-04-05 17:08:49 UTC	3467		2023-04-05 17:46:52 UTC	2022-12-16 15:38:46 UTC
<input type="checkbox"/>	C.0fe94e2d1bc256f0	DESKTOP-FS1JVLL	10.0.19045	08:00:27:15:5a:1c 08:00:27:3d:c0:e3 00:00:00:00:00:00	philip	2023-04-05 17:07:07 UTC	3467		2023-04-05 17:45:09 UTC	2022-12-18 16:55:10 UTC
<input type="checkbox"/>	C.bb94cb183af805fc	philip-VirtualBox	21	08:00:27:b1:9d:67 08:00:27:7c:c3:bf 00:00:00:00:00:00	kali	2023-04-05 17:44:33 UTC	3467		2023-04-05 17:44:31 UTC	2022-12-05 13:52:11 UTC

Εικόνα 8 GRR's connected clients screen

Kali investigation:

¹ <https://grr-doc.readthedocs.io/en/latest/installing-grr-server/from-release-deb.html>

Επιλέγοντας αρχικά το kali, μπορούμε αρχικά να δούμε κάποιες βασικές πληροφορίες σχετικά με αυτόν, όπως το όνομά του, τους χρήστες, την διεύθυνση MAC κτλ.

The screenshot shows the GRR web interface with the 'Host Information' tab selected for a Kali Linux client. The interface includes a sidebar with navigation options like 'Start new flows', 'Browse Virtual Filesystem', and 'Advanced'. The main content area displays client details in three panels: OS information, Timestamps, and Interfaces.

OS			
Linux - Kali GNU/Linux 2023.1			
Last Local Clock			
2023-04-18 17:47:45 UTC			
GRR Client Version			
3467			
Architecture			
x86_64			
Kernel			
6.1.0-kali5-amd64			
Memory Size			
3.8GiB			
Labels			
No labels assigned.			
Users			
... (kali)			

Timestamps			
OS installation time			
2022-12-05 13:52:11 UTC 134 days ago			
First seen			
2023-04-18 17:47:57 UTC 3 minutes ago			
Last booted			
-			
Last seen			
2023-04-18 17:47:56 UTC 3 minutes ago			

Interfaces			
IF Name	Mac Address	Addresses	
eth0	08:00:27:f3:7f:12	192.168.56.103	fe80:0000:0000:0000:c907:0cdf:c73d:367
eth1	08:00:27:7c:c3:bf	10.00.03.15	fe80:0000:0000:0000:4905:82f8:6f67:55e
lo	00:00:00:00:00:00	127.00.00.01	0000:0000:0000:0000:0000:0000:0000:0000

Εικόνα 9 Kali Linux client information

Επιλέγοντας το tab “start new flow” στα αριστερά, μπορούμε να υποβάλλουμε εργασίες στον client ώστε να μας επιστρέψει πληροφορίες από τις οποίες μπορούμε να εξάγουμε πειστήρια. Μερικά από τα flows περιλαμβάνουν:

- **Interrogate**, το οποίο τρέχει by default ανά τακτά χρονικά διαστήματα για να παρέχει βασικές πληροφορίες για τον client.
- **Client File Finder**, το οποίο μας επιστρέφει μια λίστα με όλα τα αρχεία στα directories του client που προσδιορίζουμε, τα οποία επίσης μπορούμε να κατεβάσουμε
- **Process Dump**, που μας επιστρέφει ένα dump της μνήμης για τις διεργασίες που δίνουμε σαν είσοδο
- **Nestat**, που επιστρέφει πληροφορίες δικτύου του client, όπως διαθέσιμες διεπαφές, τις διευθύνσεις τους, το δίκτυο στο οποίο ανήκουν κτλ.

Ξεκινάμε τρέχοντας ένα **Client File Finder Flow** για τα directories “/home/kali/Downloads/”, “/home/kali/Documents/”, “/bin/” και “/opt/”, προσδιορίζοντας ως ACTION το “HASH”, το οποίο σημαίνει ότι μαζί με την λίστα των αρχείων θα μας επιστραφούν και τα hashes τους. Αυτό είναι χρήσιμο όταν χρειάζεται να αναζητήσουμε πειστήρια μεταξύ των προσωπικών αρχείων του χρήστη (π.χ. αρχεία που έχει κατεβάσει ή έχει δημιουργήσει) και των προγραμμάτων που μπορεί να έχει εγκαταστήσει στον υπολογιστή του (τυπικά βρίσκονται στα directories /bin/ και /opt/). Με τον υπολογισμό του hash εξασφαλίζουμε την ακεραιότητα των ψηφιακών πειστηρίων, τα οποία μπορούμε στη συνέχεια να κατεβάσουμε στον server για περαιτέρω ανάλυση.

Administrative

- Interrogate
- KeepAlive
- OnlineNotification

Browser

- Browser History

Checks

- Run Checks

Collectors

FileTypes

Filesystem

- Client Side File Finder
- Collect large file
- File Finder
- GetMBR
- ListVolumeShadowCopies

Memory

Network

Processes

Registry

Paths +

×

/bin/*

×

/opt/*

×

%%users.homedir%%/Documents/*

×

%%users.homedir%%/Downloads/*

Pathtype

OS (default) ▾

Conditions +

Action

Action

Hash ▾

Advanced ▾

Max size

500000000

ClientFileFinder

A client side file finder flow.

Εικόνα 10 GRR new flow selection and customization

Flow Information	Requests	Results	Log	API
<div><div><div>Name</div><div>ClientFileFinder</div></div><div><div>Flow ID</div><div>263894848219EEFC</div></div><div><div>Creator</div><div>admin</div></div><div><div>Start Time</div><div>2023-04-18 20:29:52 UTC</div></div><div><div>Last Active</div><div>2023-04-18 20:30:24 UTC</div></div><div><div>State</div><div>TERMINATED</div></div></div>				
<div>Arguments<div><div>Paths</div><div><div>/bin/*</div><div>/opt/*</div><div>%%users.homedir%%/Documents/*</div><div>%%users.homedir%%/Downloads/*</div></div></div><div><div>Action</div><div><div>Action</div><div>Hash</div><div>Collect extended attributes</div><div>false</div></div></div></div>				
<div>Runner Arguments<div><div>Notify at Completion</div><div>true</div></div><div><div>Client id</div><div>C.71693ea92c8d2db5 ⓘ</div></div><div><div>Flow name</div><div>ClientFileFinder</div></div></div>				
<div>Context<div><div>Client resources</div><div><div>Cpu usage</div><div>Network bytes sent</div><div>848767</div></div></div><div><div>Create time</div><div>2023-04-18 20:29:52 UTC</div></div><div><div>Creator</div><div>admin</div></div><div><div>Current state</div><div>End</div></div><div><div>Network bytes sent</div><div>848767</div></div><div><div>Next outbound id</div><div>2</div></div><div><div>Outstanding requests</div><div>0</div></div><div><div>Session id</div><div>aff4:/C.71693ea92c8d2db5/263894848219EEFC</div></div><div><div>State</div><div>TERMINATED</div></div></div>				
<div>State Data<div><div><div>_result_metadata</div><div>Num results per type</div><div>Tag</div><div>Count</div><div>3202</div></div><div><div>Is metadata set</div><div>true</div></div><div><div>files_found</div><div>3202</div></div></div></div>				

Εικόνα 11 Client File Finder flow information

3202 entries

Value			
Payload	Stat entry	Aff4path	aff4:/C.71693ea92c8d2db5/fs/os/bin/i686-w64-mingw32-ar
		St mode	-rwxr-xr-x
		St ino	4617456
		St dev	2049
		St nlink	1
		St uid	0
		St gid	0
		St size	1132824
		St atime	2023-03-07 18:03:46 UTC
		St mtime	2023-02-25 19:49:36 UTC
		St ctime	2023-03-07 18:04:58 UTC
		St blocks	2216
		St blksize	4096
		St rdev	0
		St flags osx	
		St flags linux	-----g--
	Hash entry	Pathspec	Pathtype OS Path /bin/i686-w64-mingw32-ar Path options CASE_LITERAL
		Sha256	09d5143864bd2f595f7abf487f1e291166e14689e7f2460f1b02e5a8071a8f5a
		Sha1	8bfe1d4b480877b3cc785419939076eab8327260
		Md5	df1e9760f994aece91b58b1b7d9c5d5e
		Num bytes	1132824
Payload type	FileFinderResult		
Timestamp	2023-04-18 20:30:24 UTC		

Εικόνα 12 File Finder partial results

Τα directories που διέτρεξε το flow μαζί με τα περιεχόμενά τους προστίθενται στο tab “Browse Virtual FileSystem” το οποίο μπορούμε να χρησιμοποιήσουμε για να εξερευνήσουμε το Filesystem του client. Επιλέγοντας ένα οποιοδήποτε αρχείο μπορούμε να πατήσουμε το κουμπί “collect from client” για να το κατεβάσουμε και να προβάλουμε τα περιεχόμενά του. Με αυτόν τον τρόπο μπορούμε να εντοπίσουμε πιθανώς κακόβουλα αρχεία και να συλλέξουμε πληροφορίες που θα μας βοηθήσουν να αντιμετωπίσουμε το περιστατικό, όπως για παράδειγμα το είδος του περιστατικού, την έκτασή του, τον αντίκτυπό του κ.α.

Icon	Name	st_size	st_mtime	st_ctime	GRR Snapshot
	1password2john	11547	2022-11-09 16:13:36 UTC	2022-12-05 13:52:49 UTC	2023-04-18 20:30:15 UTC
	2to3-2.7	96	2022-08-01 06:23:55 UTC	2022-12-05 13:53:09 UTC	2023-04-18 20:30:15 UTC
	7z	39	2020-08-15 08:26:14 UTC	2022-12-05 13:53:09 UTC	2023-04-18 20:30:15 UTC
	7z2john	86945	2022-11-09 16:13:36 UTC	2022-12-05 13:52:49 UTC	2023-04-18 20:30:15 UTC
	7za	40	2020-08-15 08:26:14 UTC	2022-12-05 13:53:09 UTC	2023-04-18 20:30:15 UTC
	7zr	40	2020-08-15 08:26:14 UTC	2022-12-05 13:53:09 UTC	2023-04-18 20:30:15 UTC
	DPAPImk2john	26132	2022-11-09 16:13:36 UTC	2022-12-05 13:52:49 UTC	2023-04-18 20:30:15 UTC

Εικόνα 13 Client Filesystem navigation

fs > os > home > kali > Downloads

Icon	Name	st_size	st_mtime	st_ctime
	DirBusterReport-10.129.33.248-80-simple.txt	361	2023-04-14 19:42:30 UTC	2023-04-14 19:42:30 UTC
	DirBusterReport-10.129.33.248-80.txt	826	2023-04-14 19:42:30 UTC	2023-04-14 19:42:30 UTC
	LinEnum.sh	655718	2023-04-15 10:40:38 UTC	2023-04-15 15:12:41 UTC
	Metasploitable Scan_j0e9s.nessus	1806573	2023-04-02 13:31:07 UTC	2023-04-02 13:31:08 UTC
	academy-regular.ovpn	9324	2023-04-14 17:23:19 UTC	2023-04-14 17:24:32 UTC
	failedlogins.log	996	2023-04-15 13:11:50 UTC	2023-04-15 13:11:50 UTC
	grr_3.4.6.7_amd64.deb	20856334	2023-04-18 17:47:13 UTC	2023-04-18 17:47:28 UTC

monitor.sh

Stats Download TextView HexView

Hash

Sha256	03c21e81a0e5d16ec31812de146943ace8a60449bc28b62d9f699b708b16ada1
Sha1	d885934a01a8316ca060711f53775b2cde1e4c66
Md5	8534799cd212d65c692f4eeca76776e6
Num bytes	4015

Last Collected
2023-04-18 22:01:36 UTC

Download

Download (4015 bytes)

Εικόνα 14 Files downloaded in the server can be viewed separately

Ένα ακόμη χρήσιμο flow που τρέχουμε είναι το **Process Dump**, το οποίο μας επιτρέπει να λάβουμε ένα στιγμιότυπο της μνήμης ορισμένων διεργασιών που εκτελούνται.

Επιλέγουμε τα process IDs 583 (Nessus service) και 1008 (ssh-agent). Ένα τμήμα των αποτελεσμάτων φαίνονται παρακάτω:

Flow Information		Requests	Results	Log	API	
Name Flow ID Creator Start Time Last Active State	DumpProcessMemory 35F3E2A8BF8BAF63 admin 2023-04-18 21:29:47 UTC 2023-04-18 21:30:12 UTC TERMINATED					
	Arguments	Pids	1008 583			
		Ignore grr process	true			
		Dump all processes	false			
		Size limit	0			
		Chunk size	104857600			
Skip special regions		false				
Skip mapped files		true				
Skip shared regions		false				
Skip executable regions		false				
Skip readonly regions		false				
Runner Arguments	Notify at Completion	true				
	Client id	C:71693ea92c8d2db5 ⓘ				
	Flow name	DumpProcessMemory				
Context	Client resources	Cpu usage	1037152			
		Network bytes sent				
	Create time	2023-04-18 21:29:47 UTC				
	Creator	admin				

Εικόνα 15 Process Dump flow information

17 entries

Filter

Value		
	Process	<div> <div>Pid</div> <div>1008</div> </div> <div> <div>Ppid</div> <div>907</div> </div> <div> <div>Name</div> <div>ssh-agent</div> </div> <div> <div>Exe</div> <div>/usr/bin/ssh-agent</div> </div> <div> <div>Cmdline</div> <div>x-session-manager</div> </div> <div> <div>Ctime</div> <div>1681831841580000</div> </div> <div> <div>Real uid</div> <div>1000</div> </div> <div> <div>Effective uid</div> <div>1000</div> </div> <div> <div>Saved uid</div> <div>1000</div> </div> <div> <div>Real gid</div> <div>1000</div> </div> <div> <div>Effective gid</div> <div>1000</div> </div> <div> <div>Saved gid</div> <div>108</div> </div> <div> <div>Username</div> <div>kali</div> </div> <div> <div>Terminal</div> <div>None</div> </div> <div> <div>Status</div> <div>sleeping</div> </div> <div> <div>Nice</div> <div>0</div> </div> <div> <div>Cwd</div> <div>/</div> </div> <div> <div>Num threads</div> <div>1</div> </div> <div> <div>User cpu time</div> <div>0.11999999731779099</div> </div> <div> <div>System cpu time</div> <div>0</div> </div> <div> <div>Rss size</div> <div>40960</div> </div> <div> <div>Vms size</div> <div>8097792</div> </div> <div> <div>Memory percent</div> <div>0.000964407654479146</div> </div>
		<div> <div>Dump time us</div> <div>22979</div> </div>
	Memory regions	<div> <div>Start</div> <div>94386606497792</div> </div> <div> <div>Size</div> <div>8192</div> </div> <div> <div>File</div> <div> <div>Pathtype</div> <div>TMPFILE</div> <div>Path</div> <div>/var/tmp/grr/tmpea4u12co/ssh-agent_1008_55d81826e000_55d818270000.tmp</div> <div>Path options</div> <div>CASE_LITERAL</div> </div> </div> <div> <div>Is executable</div> <div>false</div> </div> <div> <div>Is writable</div> <div>true</div> </div> <div> <div>Is readable</div> <div>true</div> </div> <div> <div>Dumped size</div> <div>8192</div> </div> <div> <div>Start</div> <div>94386620407808</div> </div> <div> <div>Size</div> <div>397312</div> </div> <div> <div>File</div> <div> <div>Pathtype</div> <div>TMPFILE</div> <div>Path</div> <div>/var/tmp/grr/tmpea4u12co/ssh-agent_1008_55d818b2000_55d819013000.tmp</div> <div>Path options</div> <div>CASE_LITERAL</div> </div> </div> <div> <div>Is executable</div> <div>false</div> </div> <div> <div>Is writable</div> <div>true</div> </div> <div> <div>Is readable</div> <div>true</div> </div> <div> <div>Dumped size</div> <div>397312</div> </div> <div> <div>Start</div> <div>140615167717376</div> </div> <div> <div>Size</div> <div>53248</div> </div> <div> <div>File</div> <div> <div>Pathtype</div> <div>TMPFILE</div> <div>Path</div> <div>/var/tmp/grr/tmpea4u12co/ssh-agent_1008_7fe3851f3000_7fe385200000.tmp</div> <div>Path options</div> <div>CASE_LITERAL</div> </div> </div> <div> <div>Is executable</div> <div>false</div> </div> <div> <div>Is writable</div> <div>true</div> </div> <div> <div>Is readable</div> <div>true</div> </div> <div> <div>Dumped size</div> <div>53248</div> </div> <div> <div>Start</div> <div>140615172481024</div> </div> <div> <div>Size</div> <div>12288</div> </div>
		<div> <div>File</div> <div> <div>Pathtype</div> <div>TMPFILE</div> <div>Path</div> <div>/var/tmp/grr/tmpea4u12co/ssh-agent_1008_7fe38567e000_7fe385681000.tmp</div> <div>Path options</div> <div>CASE_LITERAL</div> </div> </div> <div> <div>Is executable</div> <div>false</div> </div> <div> <div>Is writable</div> <div>true</div> </div> <div> <div>Is readable</div> <div>true</div> </div> <div> <div>Dumped size</div> <div>12288</div> </div> <div> <div>Start</div> <div>140615173689344</div> </div> <div> <div>Size</div> <div>12288</div> </div>
		<div> <div>File</div> <div> <div>Pathtype</div> <div>TMPFILE</div> <div>Path</div> <div>/var/tmp/grr/tmpea4u12co/ssh-agent_1008_7fe3857a5000_7fe3857a8000.tmp</div> <div>Path options</div> <div>CASE_LITERAL</div> </div> </div> <div> <div>Is executable</div> <div>false</div> </div> <div> <div>Is writable</div> <div>true</div> </div> <div> <div>Is readable</div> <div>true</div> </div> <div> <div>Dumped size</div> <div>12288</div> </div> <div> <div>Start</div> <div>140615173791744</div> </div> <div> <div>Size</div> <div>8192</div> </div>
		<div> <div>File</div> <div> <div>Pathtype</div> <div>TMPFILE</div> <div>Path</div> <div>/var/tmp/grr/tmpea4u12co/ssh-agent_1008_7fe3857be000_7fe3857c0000.tmp</div> <div>Path options</div> <div>CASE_LITERAL</div> </div> </div> <div> <div>Is executable</div> <div>false</div> </div> <div> <div>Is writable</div> <div>true</div> </div> <div> <div>Is readable</div> <div>true</div> </div> <div> <div>Dumped size</div> <div>8192</div> </div> <div> <div>Start</div> <div>140726255140864</div> </div> <div> <div>Size</div> <div>135168</div> </div>
		<div> <div>File</div> <div> <div>Pathtype</div> <div>TMPFILE</div> <div>Path</div> <div>/var/tmp/grr/tmpea4u12co/ssh-agent_1008_7fd6272c000_7fd6274d000.tmp</div> </div> </div>

Εικόνα 16 Process Dump partial results

Κατόπιν, μπορούμε να κατεβάσουμε το dump της μνήμης στον server προκειμένου να αναλύσουμε τα περιεχόμενά της

Τέλος εκτελούμε ένα **netstat flow** το οποίο μας επιστρέφει πληροφορίες σχετικά με τις ενεργές διεπαφές δικτύου και τις ανοικτές θύρες του μηχανήματος καθώς και τις υπηρεσίες που ακούνε σε αυτές. Αυτό είναι χρήσιμο σε περίπτωση που θα θέλαμε για παράδειγμα να αναζητήσουμε ύποπτες διεργασίες που ακούνε για συνδέσεις στο δίκτυο, γεγονός που θα μπορούσε να σηματοδοτεί την ύπαρξη malware στο μηχάνημα το οποίο συνδέεται πίσω στον επιτιθέμενο ή περιμένει μια σύνδεση από αυτόν. Μερικά από τα αποτελέσματα φαίνονται στη συνέχεια:

Payload	Family	INET	
	Type	SOCK_DGRAM	
	Local address	Ip	192.168.56.103
		Port	68
	Remote address	Ip	192.168.56.100
		Port	67
	State	NONE	
Pid	537		
Process name	NetworkManager		
Payload type	NetworkConnection		
Timestamp	2023-04-18 18:01:46 UTC		
Payload	Family	INET	
	Type	SOCK_DGRAM	
	Local address	Ip	10.0.3.15
		Port	68
	Remote address	Ip	10.0.3.2
		Port	67
	State	NONE	
Pid	537		
Process name	NetworkManager		
Payload type	NetworkConnection		
Timestamp	2023-04-18 18:01:46 UTC		
	Family	INET6	
	Type	SOCK_STREAM	

Payload	Local address	Ip	::
		Port	8834
	State	LISTEN	
	Pid	588	
	Process name	nessusd	
Payload type	NetworkConnection		
Timestamp	2023-04-18 18:01:46 UTC		

Payload	Family	INET	
	Type	SOCK_STREAM	
	Local address	Ip	0.0.0.0
		Port	8834
	State	LISTEN	
	Pid	588	
	Process name	nessusd	
Payload type	NetworkConnection		
Timestamp	2023-04-18 18:01:46 UTC		

Payload	Family	INET	
	Type	SOCK_STREAM	
	Local address	Ip	127.0.0.1
		Port	53752
	Remote address	Ip	127.0.0.1
		Port	9392
	State	ESTABLISHED	
	Pid	1144	
Process name	firefox-esr		
Payload type	NetworkConnection		
Timestamp	2023-04-18 18:01:46 UTC		

Payload	Family	INET	
	Type	SOCK_STREAM	
	Local address	Ip	127.0.0.1
		Port	53720
	Remote address	Ip	127.0.0.1
		Port	9392
	State	ESTABLISHED	
	Pid	1144	
Process name	firefox-esr		
Payload type	NetworkConnection		
Timestamp	2023-04-18 18:01:46 UTC		

Payload	Family	INET	
	Type	SOCK_STREAM	
	Local address	Ip	127.0.0.1
		Port	5432
	State	LISTEN	
	Pid	4024	
	Process name	postgres	
Payload type	NetworkConnection		
Timestamp	2023-04-18 18:01:46 UTC		

Payload	Family	INET6	
	Type	SOCK_STREAM	
	Local address	Ip	::1
		Port	5432
	State	LISTEN	
	Pid	4024	
	Process name	postgres	
Payload type	NetworkConnection		
Timestamp	2023-04-18 18:01:46 UTC		

Εικόνα 17 Netstat flow results

Windows investigation:

Επιλέγοντας τον Windows client, όπως και προηγουμένως μας εμφανίζονται αρχικά κάποιες βασικές πληροφορίες για το μηχάνημα:

The screenshot shows the GRR interface for a Windows client. The sidebar on the left contains navigation links: Host Information, Hunt, Statistics, Configuration, Binaries, Settings, and Artifacts. The main content area is titled 'DESKTOP-FS1JVLL' and displays various system details. The 'OS' section shows 'Windows 10 10.0.22621'. The 'Last Local Clock' is '2023-04-19 08:05:55 UTC'. The 'GRR Client Version' is '3467'. The 'Architecture' is 'AMD64'. The 'Kernel' is '10.0.22621'. The 'Memory Size' is '15.3GB'. The 'Labels' section indicates 'No labels assigned'. The 'Users' section lists several users, including 'MSSQL\$SQLSERVER\$', 'MSSQL\$SQLSERVER\$', 'MSSQL\$SQLSERVER\$', 'MSSQL\$SQLSERVER\$', and 'MSSQL\$SQLSERVER\$'. The 'Timestamps' section shows 'OS installation time' as '2022-10-06 11:38:39 UTC' (194 days ago), 'First seen' as '2023-04-18 17:49:56 UTC' (14 hours ago), 'Last booted' as '2023-04-19 07:28:05 UTC' (47 minutes ago), and 'Last seen' as '2023-04-19 08:05:58 UTC' (9 minutes ago). The 'Interfaces' section lists network adapters and their MAC addresses, including 'Bluetooth Device (Personal Area Network)', 'Kaspersky VPN', 'Microsoft Kernel Debug Network Adapter', 'Microsoft Wi-Fi Direct Virtual Adapter', and 'Microsoft Wi-Fi Direct Virtual Adapter'.

Εικόνα 18 Windows Client info

Επιπλέον των ανωτέρω flows, για τον συγκεκριμένο client, το GRR μας επιτρέπει να λάβουμε πληροφορίες για το Registry του μηχανήματος. Εκτελώντας το flow “**Registry Finder**” μπορούμε να προσδιορίσουμε directories του registry τα οποία θα επιστρέψει ο client για ανάλυση, όπως φαίνεται παρακάτω.

Flow Information

Requests

Results

Log

API

Name

Flow ID

Creator

Start Time

Last Active

State

RegistryFinder

81F3B61BB8D227CD

admin

2023-04-19 09:19:12 UTC

2023-04-19 09:19:25 UTC

TERMINATED

Arguments

Keys paths

HKEY_LOCAL_MACHINE

HKEY_CURRENT_CONFIG

HKEY_USERS/%%users.sid%%/Software/Microsoft/Windows/CurrentVersion/Run/*

Runner Arguments

Notify at Completion

Client id

Flow name

true

C.aac9f378a1e00145

RegistryFinder

Context

Client resources

Create time

Creator

Current state

Network bytes sent

Next outbound id

Outstanding requests

Session id

State

Cpu usage

Network bytes sent

2023-04-19 09:19:12 UTC

admin

End

6450

2

0

aff4:/C.aac9f378a1e00145/81F3B61BB8D227CD

TERMINATED

6450

State Data

_result_metadata

Num results per type

Tag

Count

Is metadata set

Type

FileFinderResult

20

true

Εικόνα 19 Registry Info Flow information

20 entries

Value			
Payload	Stat entry	Aff4path	aff4:/C.aac9f378a1e00145/registry/HKEY_LOCAL_MACHINE
		St mode	d-----
		St size	0
		St mtime	2023-04-19 08:39:06 UTC
		Registry type	REG_NONE
		Pathspec	Pathtype REGISTRY Path /HKEY_LOCAL_MACHINE Path options CASE_LITERAL
		Registry data	
Payload type	FileFinderResult		
Timestamp	2023-04-19 09:19:25 UTC		
Payload	Stat entry	Aff4path	aff4:/C.aac9f378a1e00145/registry/HKEY_CURRENT_CONFIG
		St mode	d-----
		St size	0
		St mtime	2022-10-06 12:35:00 UTC
		Registry type	REG_NONE
		Pathspec	Pathtype REGISTRY Path /HKEY_CURRENT_CONFIG Path options CASE_LITERAL
		Registry data	
Payload type	FileFinderResult		
Timestamp	2023-04-19 09:19:25 UTC		
Payload	Stat entry	Aff4path	aff4:/C.aac9f378a1e00145/registry/HKEY_USERS/S-1-5-21-2771329061-3625613965-3786517578-1002/Software/Microsoft/Windows/CurrentVersion/Run/HPSEU_Host_Launcher
		St mode	-----
		St size	46
		Registry type	REG_SZ
		Pathspec	Pathtype REGISTRY Path /HKEY_USERS/S-1-5-21-2771329061-3625613965-3786517578-1002/Software/Microsoft/Windows/CurrentVersion/Run/HPSEU_Host_Launcher Path options CASE_LITERAL
		Registry data	C:\System.sav\util\HPSEU\HpseuHostLauncher.exe
Payload type	FileFinderResult		
Timestamp	2023-04-19 09:19:25 UTC		
Payload	Stat entry	Aff4path	aff4:/C.aac9f378a1e00145/registry/HKEY_USERS/S-1-5-21-2771329061-3625613965-3786517578-1002/Software/Microsoft/Windows/CurrentVersion/Run/Steam
		St mode	-----
		St size	48
		Registry type	REG_SZ
		Pathspec	Pathtype REGISTRY Path /HKEY_USERS/S-1-5-21-2771329061-3625613965-3786517578-1002/Software/Microsoft/Windows/CurrentVersion/Run/Steam Path options CASE_LITERAL
		Registry data	"C:\Program Files (x86)\Steam\steam.exe" -silent
Payload type	FileFinderResult		
Timestamp	2023-04-19 09:19:25 UTC		
Payload	Stat entry	Aff4path	aff4:/C.aac9f378a1e00145/registry/HKEY_USERS/S-1-5-80-684135558-66954648-645343295-865517114-2956913369/Software/Microsoft/Windows/CurrentVersion/Run/OneDriveSetup
		St mode	-----
		St size	51
		Registry type	REG_SZ
		Pathspec	Pathtype REGISTRY Path /HKEY_USERS/S-1-5-80-684135558-66954648-645343295-865517114-2956913369/Software/Microsoft/Windows/CurrentVersion/Run/OneDriveSetup Path options CASE_LITERAL
		Registry data	C:\Windows\System32\OneDriveSetup.exe /thfirstsetup
Payload type	FileFinderResult		
Timestamp	2023-04-19 09:19:25 UTC		
Payload	Stat entry	Aff4path	aff4:/C.aac9f378a1e00145/registry/HKEY_USERS/S-1-5-80-684135558-66954648-645343295-865517114-2956913369/Software/Microsoft/Windows/CurrentVersion/Run/HPSEU_Host_Launcher
		St mode	-----
		St size	46
		Registry type	REG_SZ
		Pathspec	Pathtype REGISTRY Path /HKEY_USERS/S-1-5-80-684135558-66954648-645343295-865517114-2956913369/Software/Microsoft/Windows/CurrentVersion/Run/HPSEU_Host_Launcher Path options CASE_LITERAL
		Registry data	C:\System.sav\util\HPSEU\HpseuHostLauncher.exe
Payload type	FileFinderResult		
Timestamp	2023-04-19 09:19:25 UTC		

Εικόνα 20 Registry Info partial flow results

Μέσω του flow “CollectRunKeyBinaries” μπορούμε να λάβουμε τις εγκατεστημένες εφαρμογές στο μηχάνημα του χρήστη.

3B6B5F9B91E30F26

CollectRunKeyBinaries

2023-04-19 11:59:07 UTC

2023-04-19 11:59:31 UTC

admin

Flow Information

Requests

Results

Log

API

Name

Flow ID

Creator

Start Time

Last Active

State

CollectRunKeyBinaries

3B6B5F9B91E30F26

admin

2023-04-19 11:59:07 UTC

2023-04-19 11:59:31 UTC

TERMINATED

Arguments

Runner Arguments

Notify at Completion

true

Client id

C.aac9f378a1e00145

Flow name

CollectRunKeyBinaries

Context

Client resources

Cpu usage

Network bytes sent

41956

Create time

2023-04-19 11:59:07 UTC

Creator

admin

Current state

End

Network bytes sent

41956

Next outbound id

3

Outstanding requests

0

Session id

aff4/C.aac9f378a1e00145/3B6B5F9B91E30F26

State

TERMINATED

State Data

_result_metadata

Num results per type

Type

StatEntry

tag

Count

16

Is metadata set

true

Εικόνα 21 RunKeyBinaries flow information

State	Path	Flow Name	Creation Time	Last Active	Creator
3B6B5F9B91E30F26	CollectRunKeyBinaries	2023-04-19 11:59:07 UTC	2023-04-19 11:59:31 UTC	admin	
Value					
Payload	Aff4path	aff4:/C.aac9f378a1e00145/fs/ntfs/\\?Volume{7dd08dd4-57ee-41f4-9d05-9d03a2468204}/Users/Philip/AppData/Local/Microsoft/OneDrive/OneDrive.exe			
	St mode	-rwxrwxrwx			
	St size	2631048			
	St atime	2023-04-19 11:54:52 UTC			
	St mtime	2023-04-14 20:59:41 UTC			
	St ctime	2023-04-14 20:59:41 UTC			
	Pathtype	OS			
	Path	\\?Volume{7dd08dd4-57ee-41f4-9d05-9d03a2468204}			
	Mount point	C:			
	Pathspec	Pathtype NTFS Path /Users/Philip/AppData/Local/Microsoft/OneDrive/OneDrive.exe Path options CASE_LITERAL Inode 5066549580811948			
	St btime	2022-04-12 15:18:26 UTC			
Payload type	StatEntry				
Timestamp	2023-04-19 11:59:31 UTC				
Payload	Aff4path	aff4:/C.aac9f378a1e00145/fs/ntfs/\\?Volume{7dd08dd4-57ee-41f4-9d05-9d03a2468204}/Users/Philip/AppData/Local/Microsoft/Teams/Update.exe			
	St mode	-rwxrwxrwx			
	St size	2587368			
	St atime	2023-04-19 11:22:38 UTC			
	St mtime	2023-03-28 09:09:43 UTC			
	St ctime	2023-03-28 09:09:43 UTC			
	Pathtype	OS			
	Path	\\?Volume{7dd08dd4-57ee-41f4-9d05-9d03a2468204}			
	Mount point	C:			
	Pathspec	Pathtype NTFS Path /Users/Philip/AppData/Local/Microsoft/Teams/Update.exe Path options CASE_LITERAL Inode 281474977026330			
	St btime	2022-03-17 16:29:00 UTC			
Payload type	StatEntry				
Timestamp	2023-04-19 11:59:31 UTC				
Payload	Aff4path	aff4:/C.aac9f378a1e00145/fs/ntfs/\\?Volume{7dd08dd4-57ee-41f4-9d05-9d03a2468204}/Program Files (x86)/Unified Remote 3/RemoteServerWin.exe			
	St mode	-rwxrwxrwx			
	St size	3245752			
	St atime	2023-04-19 11:22:25 UTC			
	St mtime	2021-11-22 13:30:00 UTC			
	St ctime	2022-07-03 10:08:25 UTC			
	Pathtype	OS			
	Path	\\?Volume{7dd08dd4-57ee-41f4-9d05-9d03a2468204}			
	Mount point	C:			
	Pathspec	Pathtype NTFS Path /Program Files (x86)/Unified Remote 3/RemoteServerWin.exe Path options CASE_LITERAL Inode 2251799814518373			
	St btime	2022-07-03 10:08:25 UTC			
Payload type	StatEntry				
Timestamp	2023-04-19 11:59:31 UTC				

Εικόνα 22 RunKeyBinaries partial results

Όπως και προηγουμένως εκτελούμε επίσης τα flows “Client File Finder”, “Netstat”, τα αποτελέσματα των οποίων φαίνονται στην συνέχεια. Και πάλι, μόλις τρέξουν τα παραπάνω flows μπορούμε να προβάλλουμε το Filesystem του client, το οποίο έχει εμπλουτιστεί με τους φακέλους και τα αρχεία που διέτρεξαν τα flows.

State

Path

Flow Name

Creation Time

✓

BE9846ED67141820

ClientFileFinder

2023-04-19 09:20:36 UTC

Name

Flow ID

Creator

Start Time

Last Active

State

ClientFileFinder

BE9846ED67141820

admin

2023-04-19 09:20:36 UTC

2023-04-19 09:20:41 UTC

TERMINATED

Arguments

Paths

C:/Program Files/*

%%users.homedir%%/Downloads/*

Action

STAT

Action

Stat

Collect extended attributes

false

Runner Arguments

Notify at Completion

true

Client id

C.aac9f378a1e00145

?

Flow name

ClientFileFinder

Context

Client resources

Cpu usage

Network bytes sent

23959

Create time

2023-04-19 09:20:36 UTC

Creator

admin

Current state

End

Network bytes sent

23959

Next outbound id

2

Outstanding requests

0

Session id

aff4:/C.aac9f378a1e00145/BE9846ED67141820

State

TERMINATED

State Data

_result_metadata

Num results per type

Tag

Count

Is metadata set

Type

FileFinderResult

119

true

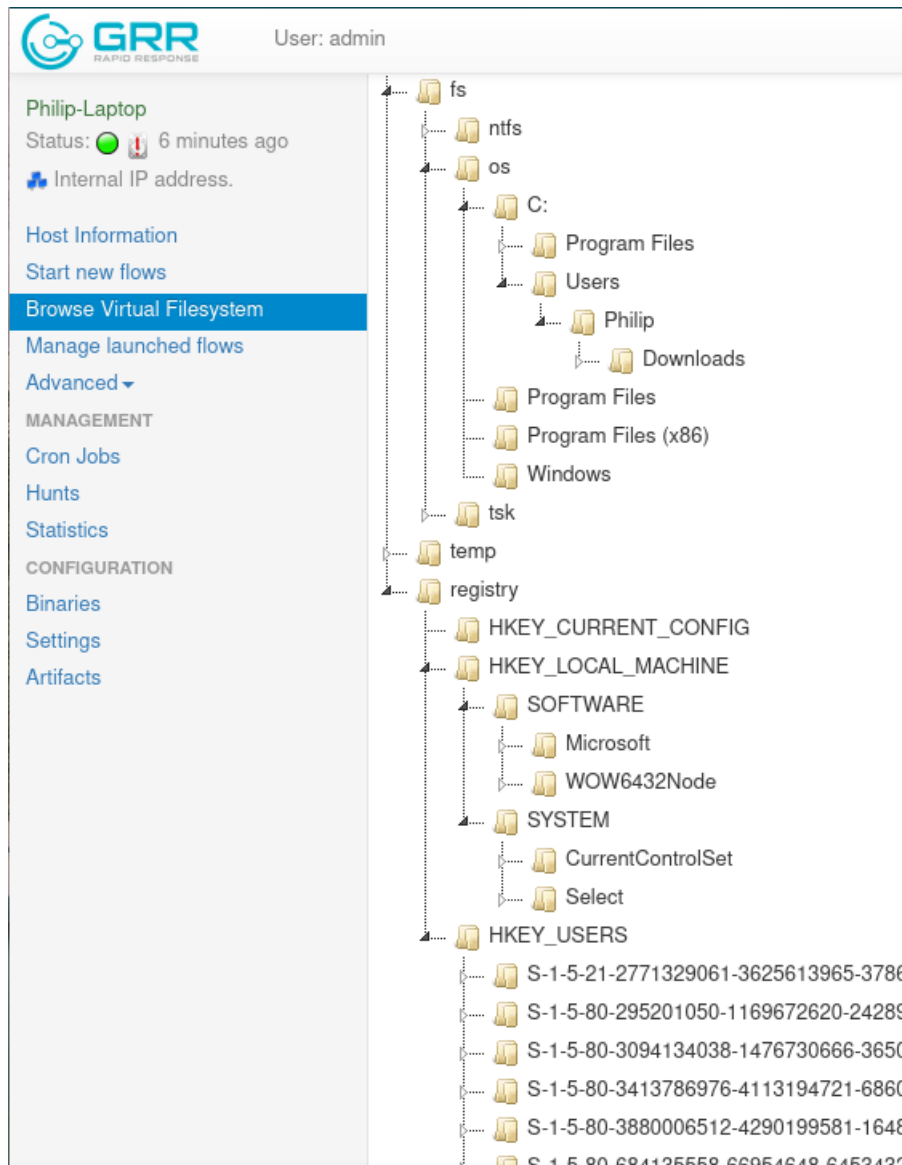
Εικόνα 23 Client File Finder flow information

119 entries

Filter

Value			
Payload	Stat entry	Aff4path	aff4:/C:aac9f378a1e00145/fs/os/C:/Users/Philip/Downloads/Nessus_Metasploitable Scan_07cli.pdf
		St mode	-rw-rw-rw-
		St ino	7599824371926552
		St dev	3930354540
		St nlink	1
		St uid	0
		St gid	0
		St size	140840
		St atime	2023-04-16 15:52:18 UTC
		St mtime	2023-04-02 13:32:21 UTC
		St ctime	2023-04-16 15:52:17 UTC
		St flags osx	
		St flags linux	-----
		Pathspec	Pathtype OS
			Path C:/Users/Philip/Downloads/Nessus_Metasploitable Scan_07cli.pdf
			Path options CASE_LITERAL
Payload type		FileFinderResult	
Timestamp		2023-04-19 09:20:41 UTC	
Payload	Stat entry	Aff4path	aff4:/C:aac9f378a1e00145/fs/os/C:/Users/Philip/Downloads/Nessus_Metasploitable Scan_vlwx1j.pdf
		St mode	-rw-rw-rw-
		St ino	4222124651056398
		St dev	3930354540
		St nlink	1
		St uid	0
		St gid	0
		St size	1030012
		St atime	
		St mtime	
		St ctime	
		St flags osx	
		St flags linux	-----
		Pathspec	Pathtype OS
			Path C:/Users/Philip/Downloads/RACI MATRIX.xlsx
			Path options CASE_LITERAL
Payload type		FileFinderResult	
Timestamp		2023-04-19 09:20:41 UTC	
Payload	Stat entry	Aff4path	aff4:/C:aac9f378a1e00145/fs/os/C:/Users/Philip/Downloads/RACI MATRIX_BLANK.xlsx
		St mode	-rw-rw-rw-
		St ino	4785074604163915
		St dev	3930354540
		St nlink	1
		St uid	0
		St gid	0
		St size	9748
		St atime	2023-03-30 10:55:24 UTC
		St mtime	2023-03-03 09:14:23 UTC
		St ctime	
		St flags osx	
		St flags linux	
		Pathspec	Pathtype OS
			Path C:/Users/Philip/Downloads/RACI MATRIX.xlsx
			Path options CASE_LITERAL
Payload type		FileFinderResult	
Timestamp		2023-04-19 09:20:41 UTC	

Εικόνα 24 Client File Finder partial results (directories %homedir%/Downloads/, %homedir%/Documents/ and C:/Program Files/)



Εικόνα 25 Client Filesystem navigation after previous flows' execution

Flow Information

Requests

Results

Log

API

Name

Flow ID

Creator

Start Time

Last Active

State

Netstat

C5A3BF711A290979

admin

2023-04-19 09:19:23 UTC

2023-04-19 09:19:29 UTC

TERMINATED

Arguments

Runner Arguments

Notify at Completion

Client id

Flow name

true

C.aac9f378a1e00145

Netstat

Context

Client resources

Create time

Creator

Current state

Network bytes sent

Next outbound id

Outstanding requests

Session id

State

Cpu usage

2023-04-19 09:19:23 UTC

admin

End

27005

2

0

aff4:/C.aac9f378a1e00145/C5A3BF711A290979

TERMINATED

State Data

_result_metadata

conn_count

Num results per type tag

Is metadata set

Type Tag

Count

NetworkConnection

175

Εικόνα 26 Netstat flow information

175 entries

Value			
Payload	Family	INET6_WIN	
	Type	SOCK_STREAM	
	Local address	Ip	2a02:587:8194:9100:d00f:a874:64a5:3a69
		Port	62982
	Remote address	Ip	2a00:1450:4017:806::2004
		Port	443
	State	TIME_WAIT	
	Pid	0	
Process name	System Idle Process		
Payload type	NetworkConnection		
Timestamp	2023-04-19 09:19:29 UTC		
Payload	Family	INET	
	Type	SOCK_STREAM	
	Local address	Ip	192.168.1.10
		Port	139
	State	LISTEN	
	Pid	4	
	Process name	System	
	Payload type	NetworkConnection	
Timestamp	2023-04-19 09:19:29 UTC		
Payload	Family	INET	
	Type	SOCK_STREAM	
	Local address	Ip	127.0.0.1
		Port	49679
	State	LISTEN	
	Pid	5588	
	Process name	avp.exe	
	Payload type	NetworkConnection	
Timestamp	2023-04-19 09:19:29 UTC		
Payload	Family	INET	
	Type	SOCK_DGRAM	
	Local address	Ip	127.0.0.1
		Port	53658
	State	NONE	
	Pid	5652	
	Process name	svchost.exe	
	Payload type	NetworkConnection	
Timestamp	2023-04-19 09:19:29 UTC		
Payload	Family	INET	
	Type	SOCK_DGRAM	
	Local address	Ip	192.168.56.1
		Port	5353
	State	NONE	
	Pid	5784	
	Process name	nvcontainer.exe	

Εικόνα 27 Netstat partial results

Τέλος τρέχουμε το flow “List Processes”, το οποίο μας επιστρέφει μια λίστα με τα processes που εκτελούνται στο μηχάνημα του client μαζί με το path προς το εκτελέσιμο. Αυτό μπορεί να είναι αρκετά χρήσιμο στην αντιμετώπιση ενός περιστατικού καθώς υπάρχει η πιθανότητα κακόβουλα processes να εκτελούνται προσποιούμενα νόμιμα processes των Windows. Σε αυτή την περίπτωση, εξετάζοντας το ID, το parent ID και τη διαδρομή των

εκτελέσιμων αρχείων των διεργασιών μπορούμε να επαληθεύσουμε αν κάποια είναι κακόβουλη ή όχι.

Flow Information

RequestsResultsLogAPI

Name

Flow ID

Creator

Start Time

Last Active

State

ListProcesses09B3562E5B85AE00admin2023-04-19 09:19:18 UTC2023-04-19 09:19:29 UTCTERMINATED

Arguments

Runner Arguments

Notify at Completion

Client id

Flow name

true

C.aac9f378a1e00145

ListProcesses

Context

Client resources

Create time

Creator

Current state

Network bytes sent

Next outbound id

Outstanding requests

Session id

State

Cpu usage

2023-04-19 09:19:18 UTC

admin

End

115255

2

0

aff4:/C.aac9f378a1e00145/09B3562E5B85AE00

TERMINATED

State Data

_result_metadata

Num results per type

tag

Is metadata set

Type

Tag

Count

true

Process

261

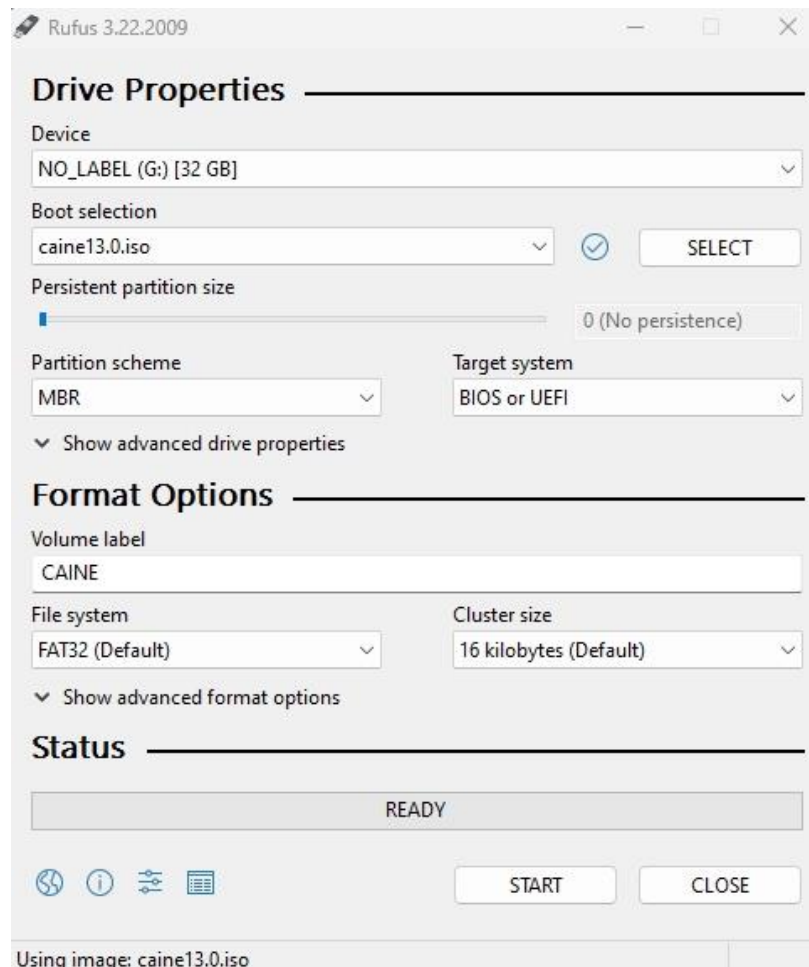
Εικόνα 28 List Processes flow information

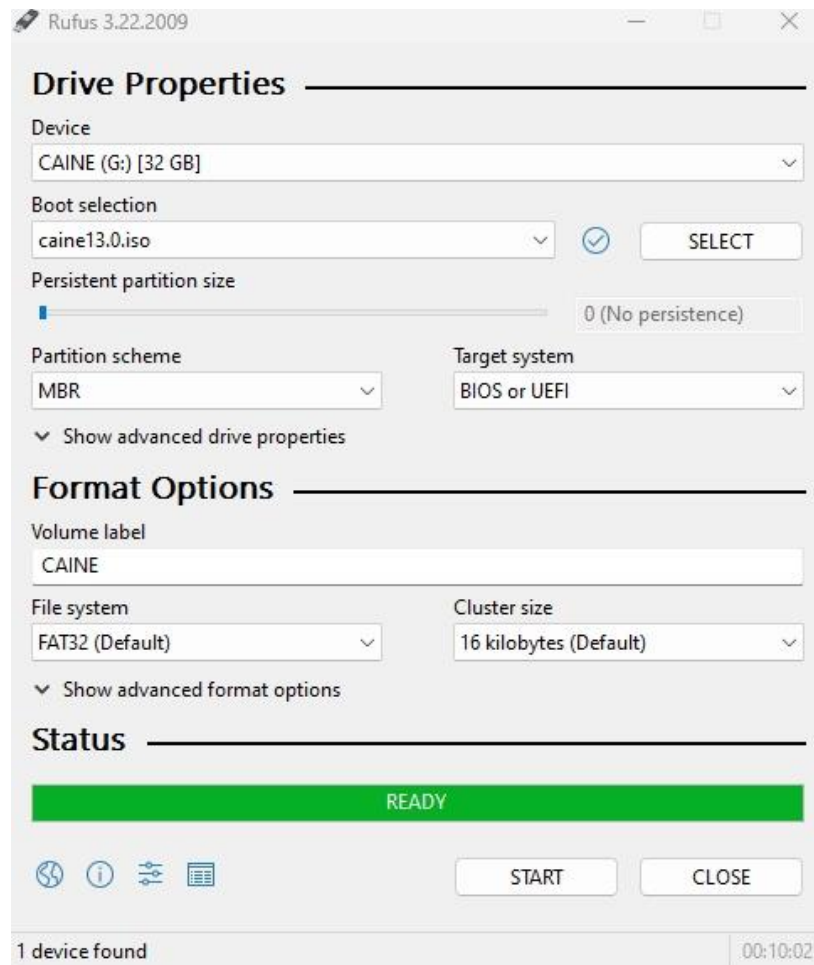
261 entries

Value		
Payload	Pid	216
	Ppid	4
	Name	Registry
	Exe	Registry
	Ctime	1681889285601253
	Username	NT AUTHORITY\SYSTEM
	Status	running
	Nice	32
	Num threads	4
	User cpu time	0
	System cpu time	0.765625
	Rss size	67764224
	Vms size	20090880
	Memory percent	0.411266565322876
Payload type	Process	
Timestamp	2023-04-19 09:19:29 UTC	
Payload	Pid	820
	Ppid	4
	Name	smss.exe
	Exe	C:\Windows\System32\smss.exe
	Cmdline	\SystemRoot\System32\smss.exe
	Ctime	1681889289369140
	Username	NT AUTHORITY\SYSTEM
	Status	running
	Nice	32
	Num threads	2
	User cpu time	0
	System cpu time	0
	Rss size	1134592
	Vms size	1175552
	Memory percent	0.006885930895805359
Payload type	Process	
Timestamp	2023-04-19 09:19:29 UTC	
Payload	Pid	1140
	Ppid	992
	Name	csrss.exe
	Exe	C:\Windows\System32\csrss.exe
	Cmdline	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
	Ctime	1681889294696224
	Username	NT AUTHORITY\SYSTEM
	Status	running
	Nice	32
	Num threads	14
	User cpu time	0.171875
	System cpu time	2.828125
	Rss size	5156864
	Vms size	2613248
	Memory percent	0.03129742667078972
Payload type	Process	

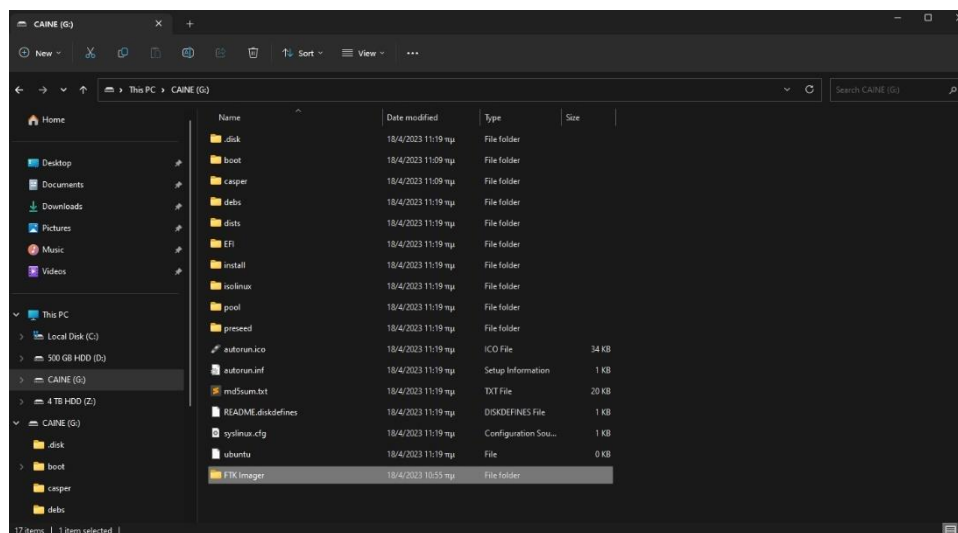
E. Caine

Για την εγκατάσταση του [Caine](#) χρησιμοποιήσαμε το [Rufus](#) για να γράψουμε το ISO του Caine σε ένα USB 32 GB. Χρησιμοποιήσαμε USB 32 GB ώστε να μπορέσουμε να αποθηκεύσουμε το αντίγραφο της μνήμης εκεί, καθώς συνήθως τα μεγέθη τους ξεπερνούν τα 16 GB, ενώ το Caine απαιτεί 4 GB αποθηκευτικού χώρου.

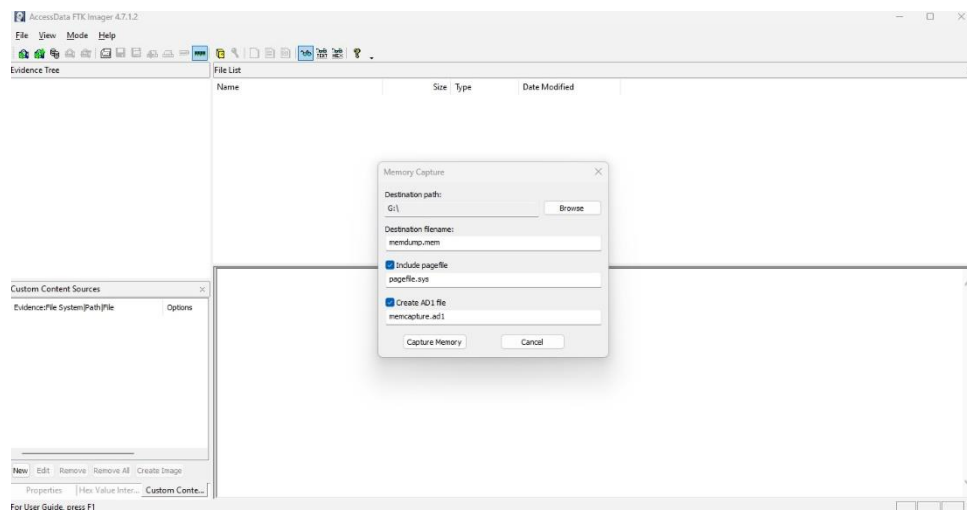
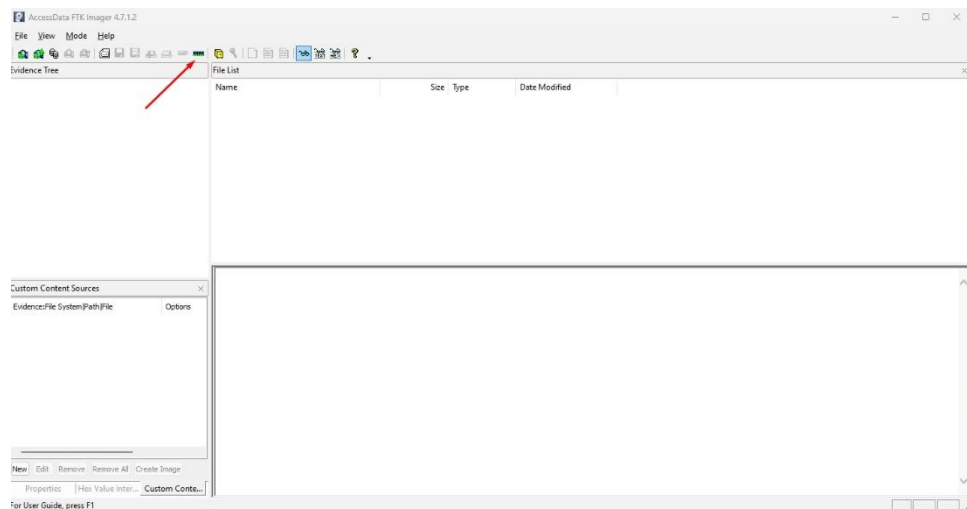




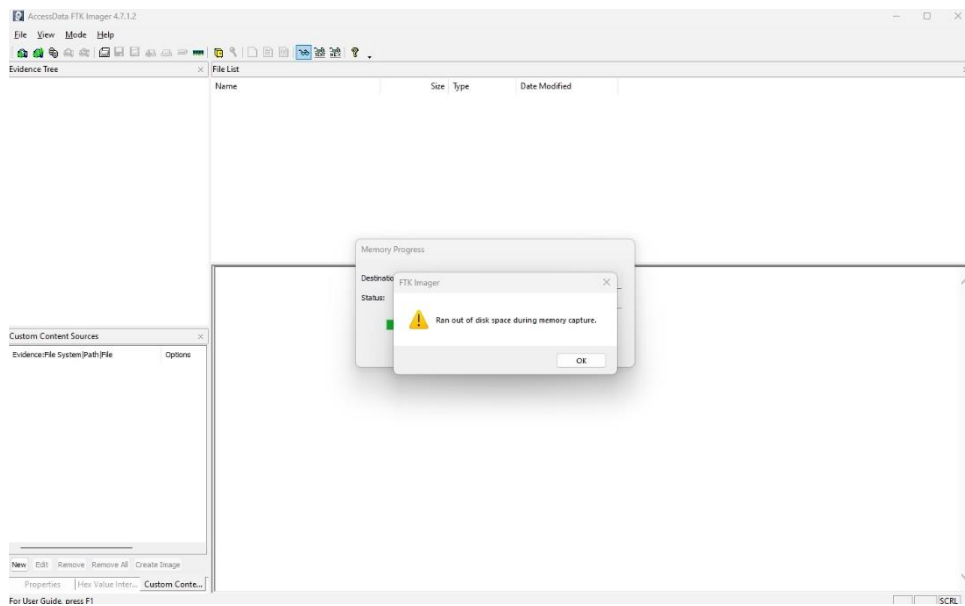
Έπειτα περάσαμε το [FTK Imager](#), σύμφωνα με τις οδηγίες της [Exterro](#).



Στην συνέχεια πήγαμε στον φάκελο του FTK Imager και τρέξαμε το executable για να πάρουμε το αντίγραφο της μνήμης.



Παρότι υπήρχε επαρκής αποθηκευτικός χώρος στο USB, το FTK Imager έδωσε μήνυμα ότι δεν υπάρχει αρκετός χώρος για να αποθηκευτεί το αντίγραφο μνήμης στο USB.



Για αυτόν το λόγο το αποθηκεύσαμε τοπικά στο υπολογιστή. Δυστυχώς δεν είχαμε στην διάθεσή μας USB 64 GB για να το δοκιμάσουμε.

