ñ

M11 – Seguretat Informàtica – UF2

Pràctica 3 – EINES PALIATIVES

Nil Massó

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

Table of Contents

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

• A l'hora d'avaluar i qualificar el treball es tindran en compte els aspectes estètics, de correctesa lingüística (sintàctica i ortogràfica) a més del que s'hagi comentat al cicle formatiu sobre la redacció de documentació tècnica i manuals.

• El mòdul professional pertany a uns estudis orientats al món laboral, cosa que fa que un cop complerts els requisits mínims la nota resultant serà condicionada per la quantitat i qualitat del treball individual realitzat per cada alumne.

• **Recordeu crear una portada i un índex.**

Pràctica 2 – Eines pal·liatives

Fes els exercicis següents. Contesteu directament sota dels enunciats. Poseu-hi captures de pantalla si ho considereu necessari.

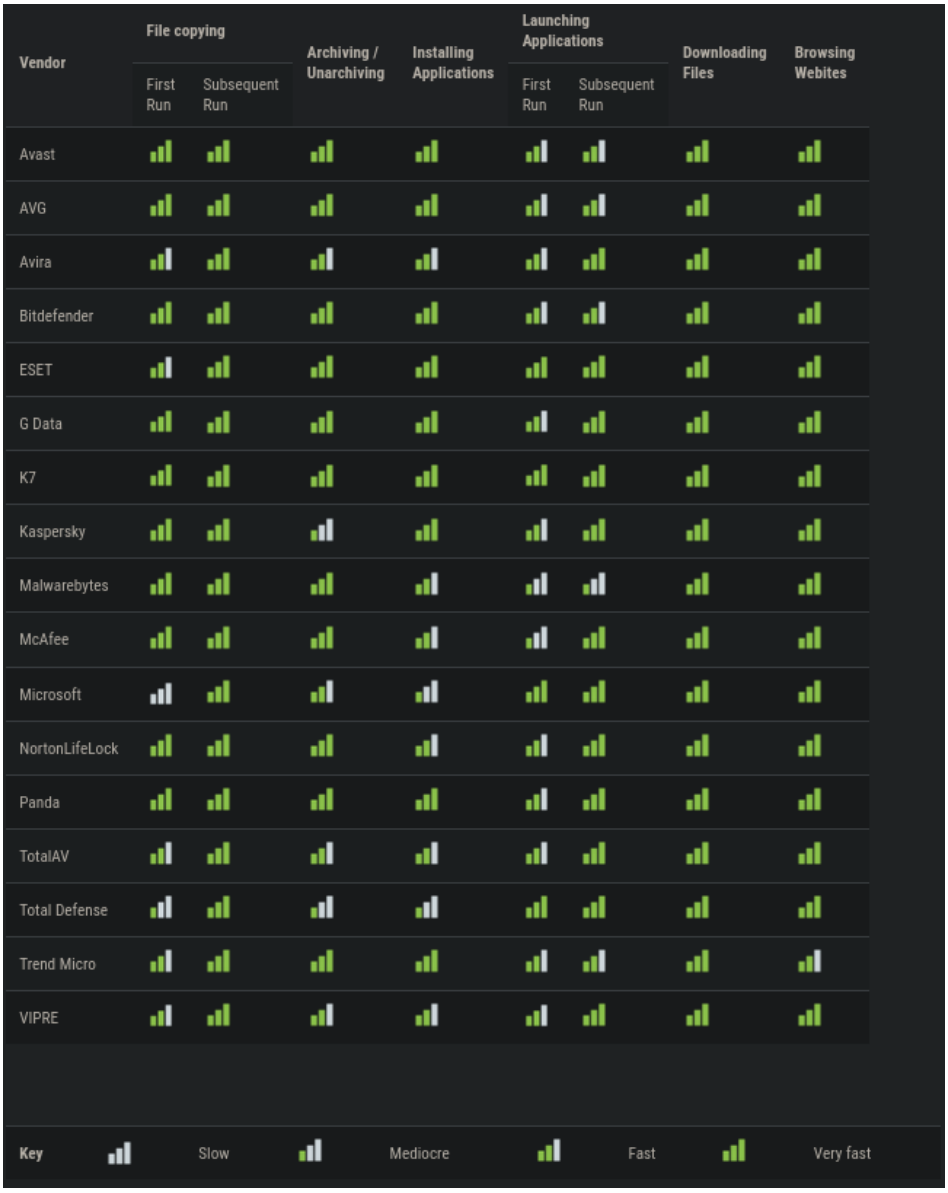
Recordeu a citar TOTES les fonts utilitzades

Exercici 1: Tests antivirus (1,5 punts)

Hi ha moltes maneres i eines d'analitzar els sistemes informàtics en busca de malware. Per a poder triar la que millor s'ajusti a les nostres necessitats, hem de saber quines són les seves condicions de funcionament. Per això, cal consultar informació sobre tipus de tests, com afecten als nostres equips i quina efectivitat tenen. No totes les eines funcionen igual contra els diferents tipus de malware. Per a conèixer una mica aquests tipus de tests, entreu a https://www.av-comparatives.org/test-methods/ i escolliu 2 tipus de tests diferents. Adjunteu el link que l'explica, i feu vosaltres (amb les vostres paraules) un resum del que hi trobeu (en què es basen el tests, proves fetes, algun exemple i valoració de software avaluat, etc).

Performance test: Per mesurar l'imapcte que tenen els softwares antivirus en les tasques diaries. Per fer-ho s'agafa una maquina sense el software instalat i se li realitzen tasques com , llençar aplicacions, intsalarles, copiar arxius i archivarlos etcetera; es mesura el temps promig que es tarda a realitzar aquetes tasques i després es mesura el que es tarda a fer exactament les mateixes tasques però amb el software antivirus instalat i en execució, d'aquesta manera s'aconsegueix veure l'impacte real que te en la productivitat del dia a dia.

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			



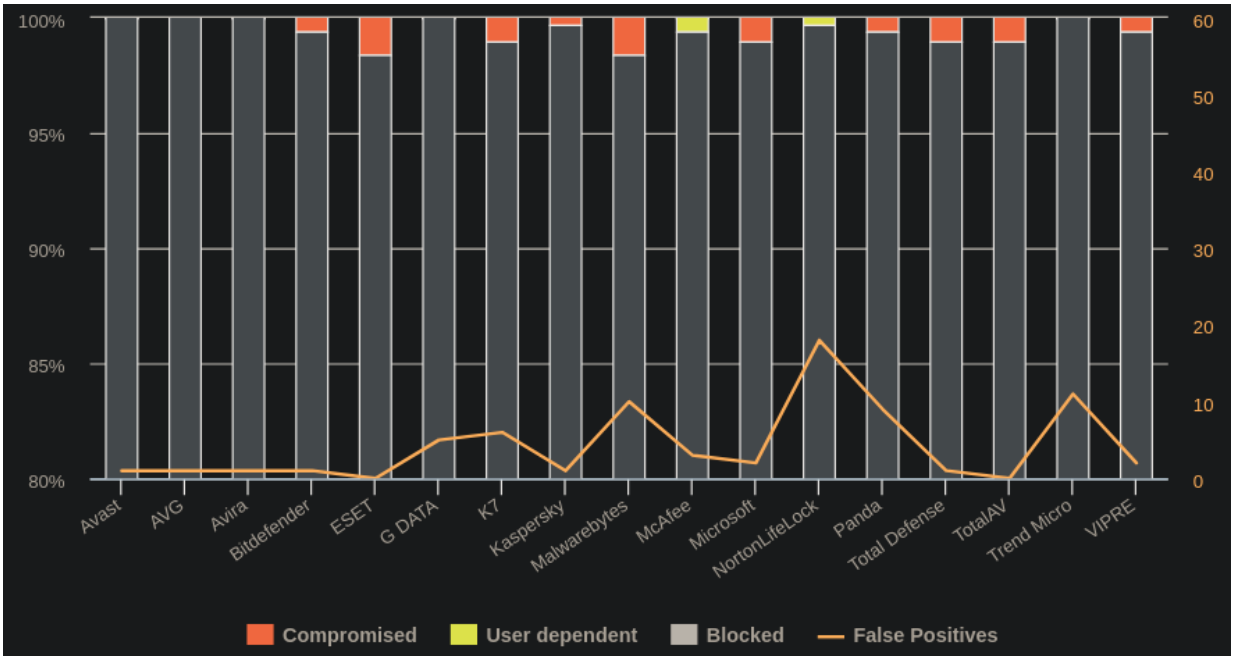
Exemple de comparativa de performance.

Real-World Protection: Aquest es centra en avaluar la efectivitat dels antivirus testats davant les amenaçes que es poden trobar els usuaris durant el seu dia a dia a internet.

Per a fer el test s'excuta el link amb el software malicios a la maquina amb l'antivirus i es mira si: esl bloqueja, el descarrega per en executar el bloqueja, o si requereix input de l'usuari podent també comprometre el siestema. Es deixa temps per veure el resulats obtinguts, tant del malware com de l'antivirus, i es mira si el sistema ha estat compromes o no.

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

Exemple de resultats



Exercici 2: Spybot – Search & Destroy (1,5 punts)

Descarrega i instal·la **«Spybot – Search & Destroy»** i busca informació sobre perquè serveix aquest programa anti-malware. **(0,5 punts)**

Es un programa de codi tancat per de us privat gratuït que es destina a la protecció i eliminació de spyware, adware i malware. Es capaç de buscar i eliminar problemes amb cookies de seguiment, registre de Windows , segrestadors de navegadors i un llarg etcètera. Fins i tot degut a que alguns programes deixen de funcionar si l'spyare o adware que contenen s'elimina el que fan les noves versions del programa enlloc de eliminar-lo, es emplenar els arxius que utilitza amb codi que no aporta res però que fa que el software segueixi poguent funcionar sense el adware.

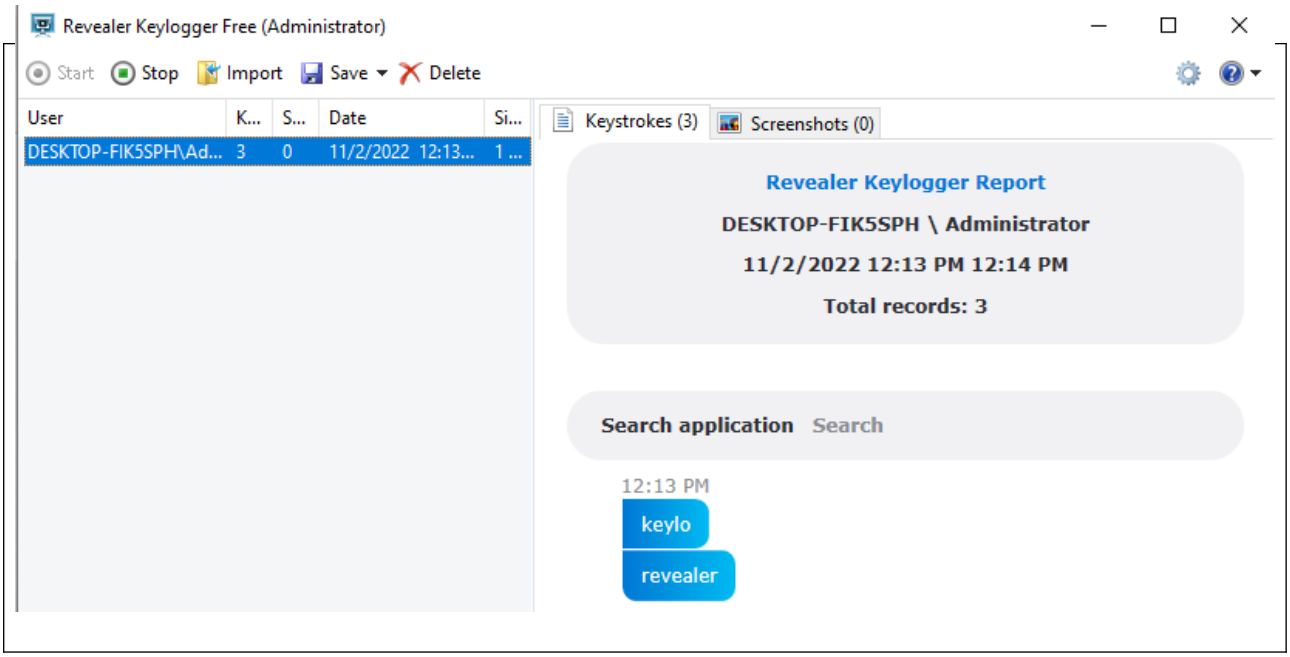
Comenta per a que es fa servir el fitxer hosts dels sistemes operatius Windows i Linux. Obre el fitxer hosts del teu Sistema Operatiu mitjançant el teu editor favorit i no el tanquis. **(0,5 punts)**

Es un mini arxiu de dns que fa la resolució de noms a ips en el propi dispositiuCrea una còpia del teu fitxer hosts. Després des de l'Spybot selecciona la funció de «Associated Tasks -> Immunization» i comprova que succeeix en el fitxer hosts del teu Sistema Operatiu. Per a què ho fa? De què ens protegeix? **(0,5 punts)**
Emplena l'arxiu amb gran quantitat de hosts coneguts que contenen programes maliciosos i els redirigeix cap a localhost de tal manera que queden inaccessibles
Enllaç: https://www.fosshub.com/Spybot-Search-and-Destroy.html

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

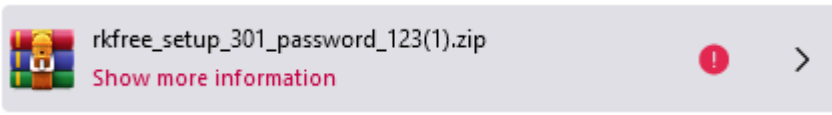
Exercici 3: Key Loggers (1,5 punts)

Instal·la el programa **Revealer Keylogger** en una màquina virtual de Windows i comprova el seu funcionament. Es pot tornar invisible per tal que no la pugui veure l'usuari però en la versió de pagament. Adjunta alguna captura de pantalla mostrant el seu funcionament. **(1 punts)**

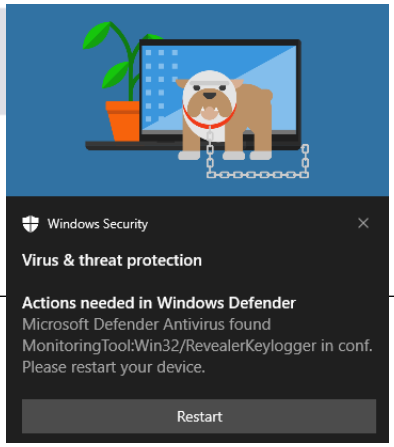


Comprova si un antimalware o antispyware detecta el keylogger i el deshabilita. Adjunta alguna captura de pantalla amb el resultat **(0,5 punts)**

Firefox el detecta com a virus



I Windows defender també



Enllaç: https://www.logixoft.com/index

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

Exercici 4: Antivirus ClamAV (2,5 punts)

ClamAV és un antivirus molt popular sobretot en sistemes Linux com a solució opensource. Així doncs és una solució antivirus que suporta múltiples formats (documents, executables, arxius), utilitza característiques d'escaneig multi-thread i té un sistema d'actualitzacions de signatures que normalment s'executa 3 o 4 cops al dia com a mínim, i sol estar molt a la última del que hi ha per la xarxa. Es sol utilitzar molt sovint en solucions d'escaneig en plataformes de serveis online, o serveis FTP o sobretot, en serveis de correu electrònic, ja sigui de forma individual o amb plataformes de content filter com per exemple Amavis. Es pot configurar per funcionar com a procés sota demanda o com a daemon. Per a la realització d'aquest exercici podeu fer servir per exemple una ubuntu Desktop 18.04.5. Cal que:

- **Instal·leu Clamav via apt-get.** Adjunteu captura de la comanda i les 3-4 línies següents que us generi. Quan acabi, mostreu la versió amb clamscan –version **(0,25 punts)**

```
root@nil-Standard-PC-i440FX-PIIX-1996:~# apt install clamav -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  clamav-base clamav-freshclam libclamav9 libcurl4 libllvm3.9 libmspack0
  libtfm1
```

Amb la comanda donada no apareix, he utilitzar clamscan -V

```
root@nil-Standard-PC-i440FX-PIIX-1996:~# clamscan -V
ClamAV 0.103.6
```

- Caldrà que poseu el sistema de firmes al dia, busqueu com fer-ho i adjunteu la captura de la comanda i el resultat: **(0,5 punts)**

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

- Per treballar amb el sistema, farem ús de la eina clamscan. Executeu clamscan --help per a més informació però Internet està ple d'exemples com el que farem a continuació i evidentment els podeu consultar (però citant les fonts).

- Cal que feu un escaneig recursiu de **/home**. **Si no arribeu a un mínim de 50 fitxers escanejats**, **cal canviar-ho i fer-ho a /etc** o **/** sencera. Adjunteu la captura de la comanda i el resultat obtingut. **(0,5 punts)**

- Ara aneu a /tmp i creeu la carpeta activitat3. Ens interessa demostrar que ClamAV funciona però NO ho fareu amb cap arxiu maliciós de veritat. Busqueu informació sobre el test EICAR, feu una explicació curta de què és, com es fa servir, etc i feu la demostració dins de /tmp/activitat3. Adjunteu la captura del resultat de l'escaneig (normal, només recursiu) de tot el /tmp i expliqueu com ho heu fet per generar la prova EICAR. **(0,75 punts)**

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

- Ara busqueu com cal fer-ho perquè ClamAV **a part de detectar el virus, també l'elimini**. Feu-ho sobre **/tmp** i adjunteu les captures de 2 execucions seguides. A la primera us hauria de trobar el virus i eliminar-lo i per tant a la segona ja no us l'hauria de trobar. Adjunteu també una captura de **ls –l /tmp/activitat3** per demostrar-ho. **(0,5 punts)**

Exercici 5: Filtres antispam (2 punts)

Per solucionar el tema de l'spam una de les tècniques més freqüentment aplicades i efectives són els filtres bayesians. **Busqueu informació sobre què són, en què es basen, des de quan s'utilitzen, i tot allò que creieu interessant. (1 punts)**

Es un filtre que es remonta a la dècada de 19990, el qual mitjançant una formula matemàtica avalua la probabilitat de que siguis spam segons les paraules que conte i que prèviament se li ha ensenyat que solen estar a correus spam.

Per altra banda, un dels softwares antispam més efectius és **SpamAssassin**. Busqueu informació sobre ell, sobretot del seu funcionament per classificar l'spam i les seves característiques, i també sobre **les tècniques que utilitza per determinar si un correu és SPAM o no**. Utilitzen **bayesians**? **(1 punts)**

SpamAssassin és un programa que analitza els correus electrònics entrants i els classifica com a SPAM o no. Per aquesta classificació utilitza un sistema de

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

bayesians, així com també un sistema per analitzar els headers, blocklists de DNS, i filtres col·laboratius

Enllaç: https://spamassassin.apache.org/

Exercici 6: Actualitzacions (1 punt)

Instal·la una aplicació antiga de WinRAR (o equivalent) a una màquina virtual. Executa la següent comanda des del powershell i indica la versió de WinRAR instal·lada: **(0,25 punts)**

Get-ItemProperty Selec-ob HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Format-Table -AutoSize*

Per a que serveix l'aplicació **Software Update Monitor**? **(0,5 punts)**

Per actualitzar software de l'ordinador, sobretot per a aquells que no porten un autoactualitzador.

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

Instal·la el programa Software Update Monitor i comprova que detecta les actualitzacions pendents del WinRAR. Mostra'n una imatge **(0,25 punts)**

Enllaç: https://www.kcsoftwares.com/?sumo

https://winrar.uptodown.com/windows/versions