PROYECTO: ARTÍCULO DE REVISIÓN SOBRE EL LAB DE SEGURIDAD SOBRE FEDORA 33

ESTUDIANTE

JUANA VALENTINA MENDOZA SANTAMARÍA

PRESENTADO A

JENNIFER ELIANA CORREA USSA

REDES
UNIVERSIDAD SANTO TOMÁS
SECCIONAL TUNJA
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA DE SISTEMAS

TUNJA, MAYO 28 DE 2020

Tabla de Contenido

1. INTRODUCCIÓN

El pasado 27 de Octubre fue lanzada la última versión de Fedora que corresponde a la 33. Donde algunas de las novedades más relevantes son el uso del editor de texto GNU Nano, un sistema de archivos BTRFS y agregar un proceso de SID en segundo plano.

Fedora ofrece varias versiones para ambientes de escritorio, servidor, cloud y para internet de las cosas (IoT).

Fedora Labs es una selección depurada de paquetes de software de propósito específico y contenido, depurado y mantenido por los miembros de la comunidad de Fedora. Estos pueden ser instalados como versiones completas autónomas de Fedora o como complementos a instalaciones de Fedora existentes. Los siguientes laboratorios están disponibles:

- **Astronomy**: para explorar el espacio exterior.
- **Comp Neuro**: un conjunto muy completo de herramientas de modelado computacional de código abierto y libre, para la neurociencia.
- **Design sute**: diseño visual, producción multimedia y suite de publicación de herramientas creativas libres y de código abierto.
- **Games:** una perfecta colección y exhibición de los mejores juegos disponibles en Fedora.
- **Jam:** para entusiastas del audio y de la música que quieran crear, editar y producir audio y música en linux.
- **Python classroom:** un laboratorio para enseñar el lenguaje de programación de python para los estudiantes.
- **Security lab:** un entorno de pruebas seguro para trabajar en auditoría de seguridad, análisis forense, sistemas de rescate y enseñanza de metodologías de prueba de seguridad.
- **Robotics suite:** una amplia variedad de paquetes de software de robótica libres y de código abierto para principiantes y expertos en robótica.
- **Scientific:** un conjunto de herramientas numéricas y científicas de código abierto utilizadas en investigación.

Fedora Spin son entornos de escritorio de Fedora. El entorno por defecto es GNOME. Están disponibles los siguientes:

- **KDE plasma desktop:** un escritorio completo y moderno.
- **XFCE desktop:** un escritorio completo y muy bien integrado.

- **LXQT desktop:** es un escritorio ligero y bien integrado.
- **Mate-compiz desktop:** es un escritorio con un gestor de ventanas 3D.
- **Cinnamon desktop:** es un escritorio moderno con la experiencia tradicional de GNOME.
- **LXDE desktop:** es un escritorio ligero, rápido y que consume pocos recursos.
- **SOAS desktop (Sugar on a Stick):** es un escritorio para educación.
-

El presente proyecto se enfocará en la revisión sobre los spins del laboratorio de seguridad de Fedora 33.

2. FEDORA SECURITY LAB

La Edición del laboratorio de seguridad de Fedora ofrece un entorno de prueba seguro para trabajar en auditorías de seguridad, forenses, rescate de sistemas, y enseñanza de diferentes metodologías para verificar la seguridad en universidades, o en otras organizaciones.

Esta edición es mantenida por una comunidad de evaluadores de seguridad y desarrolladores. Viene con el sencillo y rápido entorno de Escritorio Xfce y con un menú personalizado que permite tener todos los instrumentos indispensables para seguir una ruta de prueba para verificaciones de seguridad o para rescatar a un sistema corrupto. La imagen viva se ha diseñado para hacer posible la instalación de software mientras se ejecuta, y si se usa desde una memoria USB creada con el Creador LiveUSB mediante la herramienta de recubrimiento, podrá instalar, actualizar el software y grabar los resultados de las pruebas en forma permanente.

Dentro de las aplicaciones destacadas de este lab tenemos:

- **Etherape:** es un monitor gráfico de red para Unix modelado con base en etherman. Muestra la actividad de la red de forma gráfica [Ghe01].
- **Ettercap:** es una suite comprensiva para ataques humanos en el medio [Ett01].
- **Medusa:** tiene como objetivo ser un atacante rápido de fuerza bruta, de computación paralela masiva y modular [Foo01].
- **Nmap:** es una herramienta gratuita y de código abierto para descubrir redes y realizar auditorias de seguridad [Lyo01].
- **Scap-workbench:** es un Scanner SCAP (Security Content Automation Protocol), utilidad gráfica que ofrece una forma fácil de ejecutar tareas comunes del protocolo SCAP. Esta utilidad permite a los usuarios ejecutar rastreos de configuración y vulnerabilidades en un sistema local simple o retomo, ejecutando la remediación del sistema de acuerdo con el archivo XCCDF (Formato de Descripción de lista de Verificación de Configuración Entendible) o SDS (Flujo de Datos Fuente) [Red01].
- **Skipfish:** es una herramienta activa de reconocimiento de seguridad de aplicaciones Web [Ski01].
- **SQLninja:** herramienta para probar vulnerabilidades de inyección de SQL en aplicaciones Web que use Microsoft SQL Server en la capa de acceso de datos [ICE01].
- **WireShark:** es un analizador de tráfico en la red [Com01].
- **Yersinia:** es una herramienta de red diseñada para tomar ventaja sobre los diversos protocolos de red [Tom01].

3. PRINCIPALES DISTRIBUCIONES DE LINUX DESTINADAS A LA SEGURIDAD

3.1 KaliLinux

Fue creada por Offensive Security. Está basada en Debian, es una distro que integra cuentos de herramientas de auditorias de seguridad. Se utiliza para test de penetración análisis forense y auditorías de seguridad. Existen versiones para plataformas de 32 y 64 bits y para procesadores ARM [Wil01].

3.2 Parrot Security OS

Parrot Security OS o ParrotSec se basa en Debian y fue creada por FrozenBox. Utiliza un entorno de escritorio MATE y un gestor de pantallas LightDM para hacerla más ligera. Incluye herramientas de seguridad (penetración, forense y auditorias). Está disponible para ediciones de 32 y 64 bits en su edición estándar. También tiene una edición completa y una edición en la nube [Par01].

3.3 Xiaopan OS

Es una distribución ligera basada en Tiny Core, se especializa en un nicho muy concreto de la seguridad, la auditoría de redes inalámbricas. Está pensada como tanto a principiantes como profesionales y tiene herramientas para realizar test, como Infaltor, AirCrack-NG, Minidwep GTK, Wifite, etc, puede auditar redes WIFI (protocolos WPA, WPA2, WEP) y soporte a la mayoría de tarjetas de red [Xia01].

3.4 WifiSlax

Es una distro española muy famosa, orientada a las redes Wifi, basada en Slax, absorbió gran parte de las herramientas y funcionalidades de BackTrack [Seg01].

3.5 BackBox

Es una distribución italiana basada en Ubuntu, por tanto hereda su sencillez de uso y sus virtudes. Integra Window Manager Xfce para ser más ligera y rápida sin olvidar la integración de un buen kit de herramientas para hacking genérico (pentesting, auditorías, forense) [Bac01].

3.6 Samurai Web Testing Framework

Es un Live de una distro Linux que viene comprimido tiene herramientas de código abierto y otro tipo de herramientas libres para seguridad web que incorpora. Aunque no es tan genérica, sí que es una buena opción para la seguridad web, ya que integra tools como BeEf, w3af, burp, AJAXShell, etc [Sam01].

3.7 Santoku Linux

Esta nueva distribución se centra en auditorías y pentesting para dispositivos móviles y análisis forense digital. Incluye SDKs, drivers, GUI framework preconfigurado (PyGTK), sistemas de autodetección y setup de nuevos dispositivos móviles conectados, herramientas para análisis forense de imágenes de NAND flash, tarjetas de memoria SD, RAM, firmware flashing para ROMs de diferentes fabricantes, scripts muy útiles, aplicaciones de análisis de malware en sistemas iOS y Android, etc [San01].

3.8 BlackArch

BlackArch, como su propio nombre indica, está basada en la fantástica distribución Arch Linux. Tiene un enorme repositorio con unos 1500 paquetes correspondientes a herramientas para pentesting, análisis forense y auditorías de seguridad en general [Bla01].

4. EJECUCIÓN DE FEDORA 33 SECURITY LAB

Al menos que se disponga de una máquina dedicada para el análisis forense dentro de la organización, que se pueda anonimizar y que arriesgue su integridad en las pruebas forenses, se recomienda ejecutar en vivo desde un medio óptico o USB la imagen de Fedora 33 Security Lab, de lo contrario se instala este sistema operativo en la máquina aislada.

Primero se debe de lanzar Fedora 33 como imagen viva, posteriormente, se abrirá la terminal y se digitará el comando **sudo dnf update**.

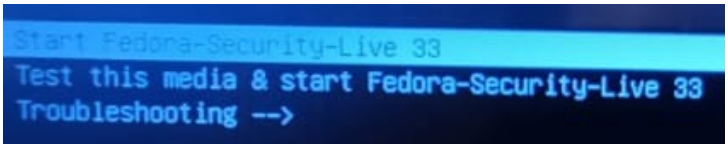


Figure 1: Start Fedora-Security-Live 33

Tener en cuenta que cuando es una imagen viva las instalaciones, las actualizaciones y los archivos que se creen, se crean en memoria RAM, lo que significa que se perderán una vez se apague el computador.

Las aplicaciones del laboratorio de seguridad se clasifican en análisis de código, forense, detección de intrusos, estadísticas de red, herramientas de contraseñas, reconocimiento, VoIP (voz sobre IP), pruebas de aplicaciones web, e inalámbricas

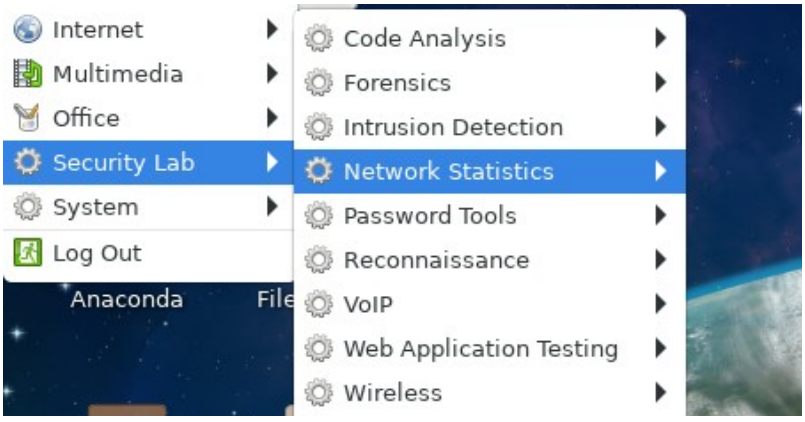


Figure 2: Las aplicaciones del laboratorio

5. PRUEBAS FORENSES

5.1 Diagnóstico de red

Para conocer la anatomía y la estructura de la red se probarán las siguientes herramientas del Lab:

5.1.1 Etherape

Primero se descargará la aplicación etherape digitando el siguiente comando: **sudo dnf install etherape**.

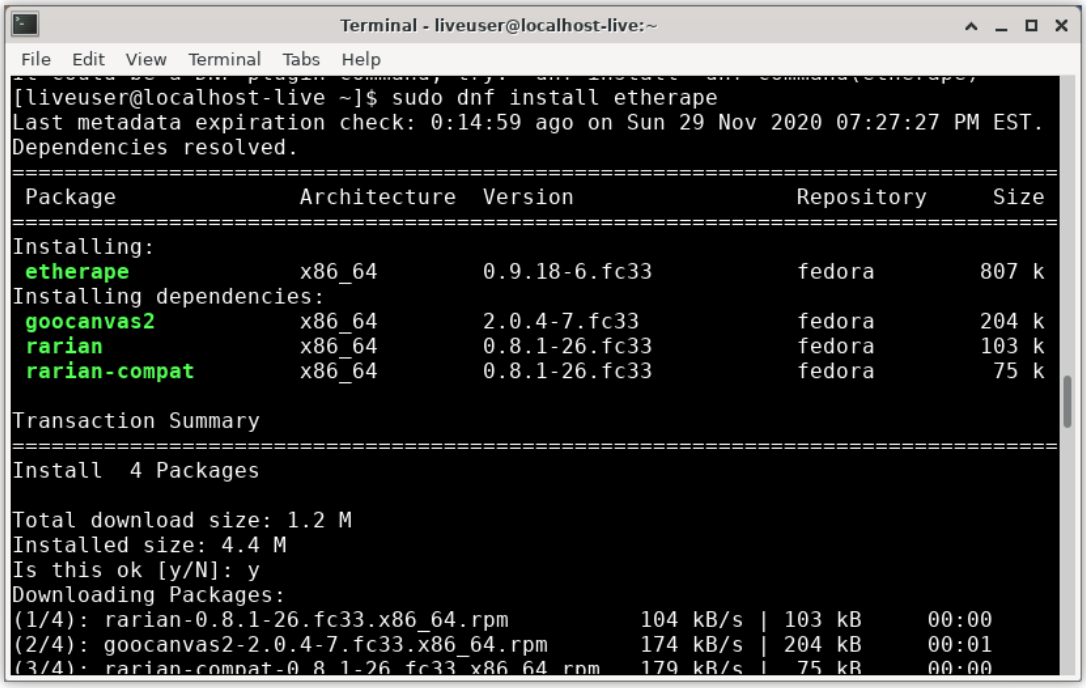


Figure 3: Install Etherape

Para poder ejecutar la aplicación se digita el comando: **sudo etherape.**

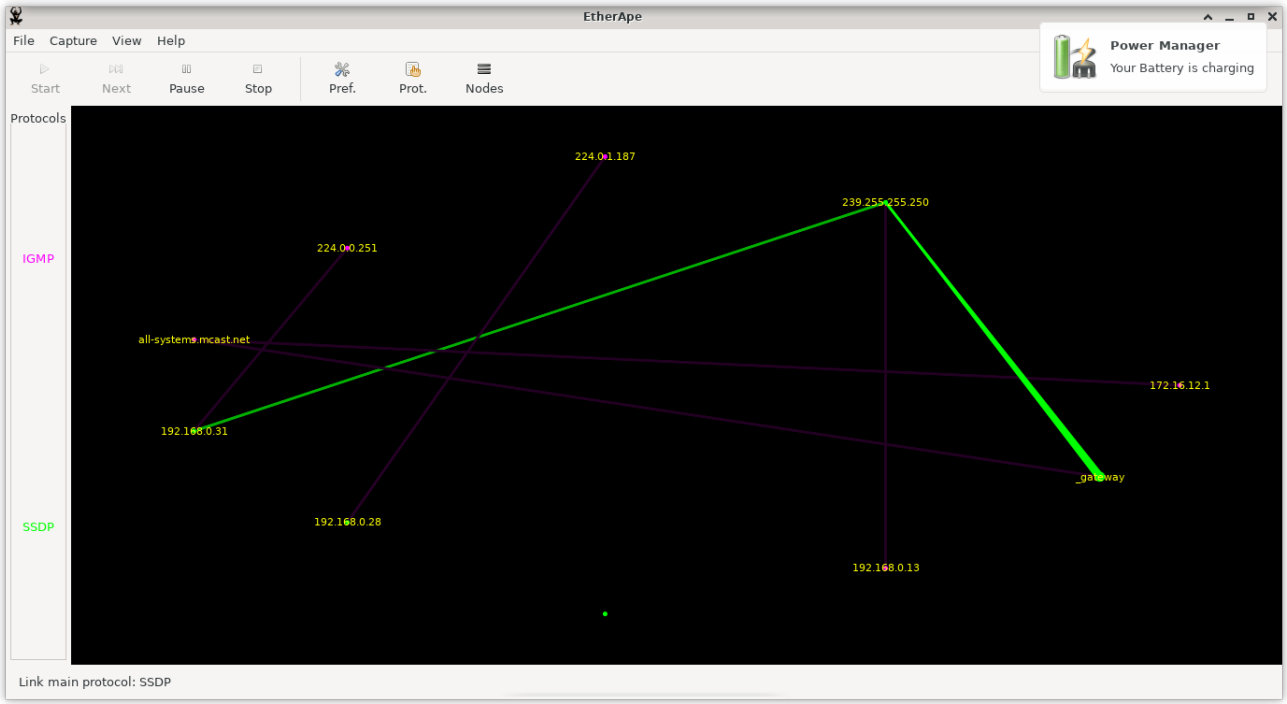


Figure 4: Etherape

Ahora se realiza un ping al servidor web de la Universidad Santoto Tomás Tunja. Nos responde que su dirección IP es 181.49.105.138. De manera que, ahora se identifica la dirección IP en el mapa.

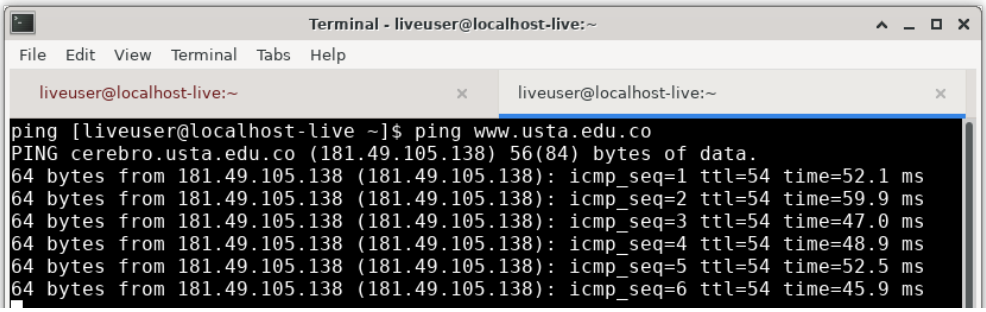


Figure 5: Ping al servidor web de la USTA

Abrimos la página de la Universidad para verificar que nodos externos utiliza en el diseño de su página, así como su proveedor de internet.

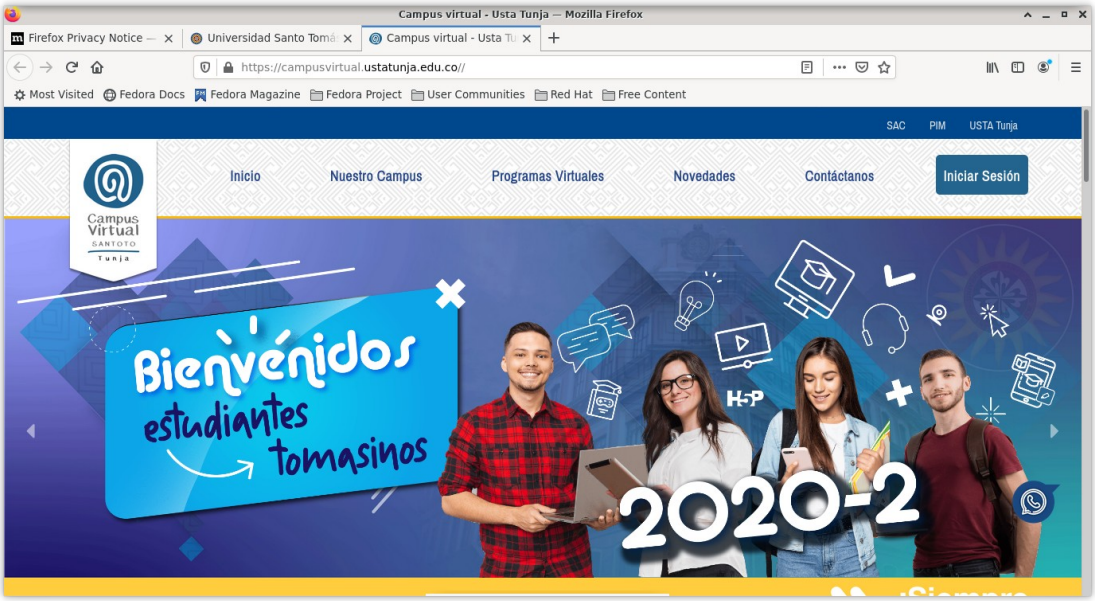


Figure 6: Página de la USTA

Volvemos a ejecutar Etherape:

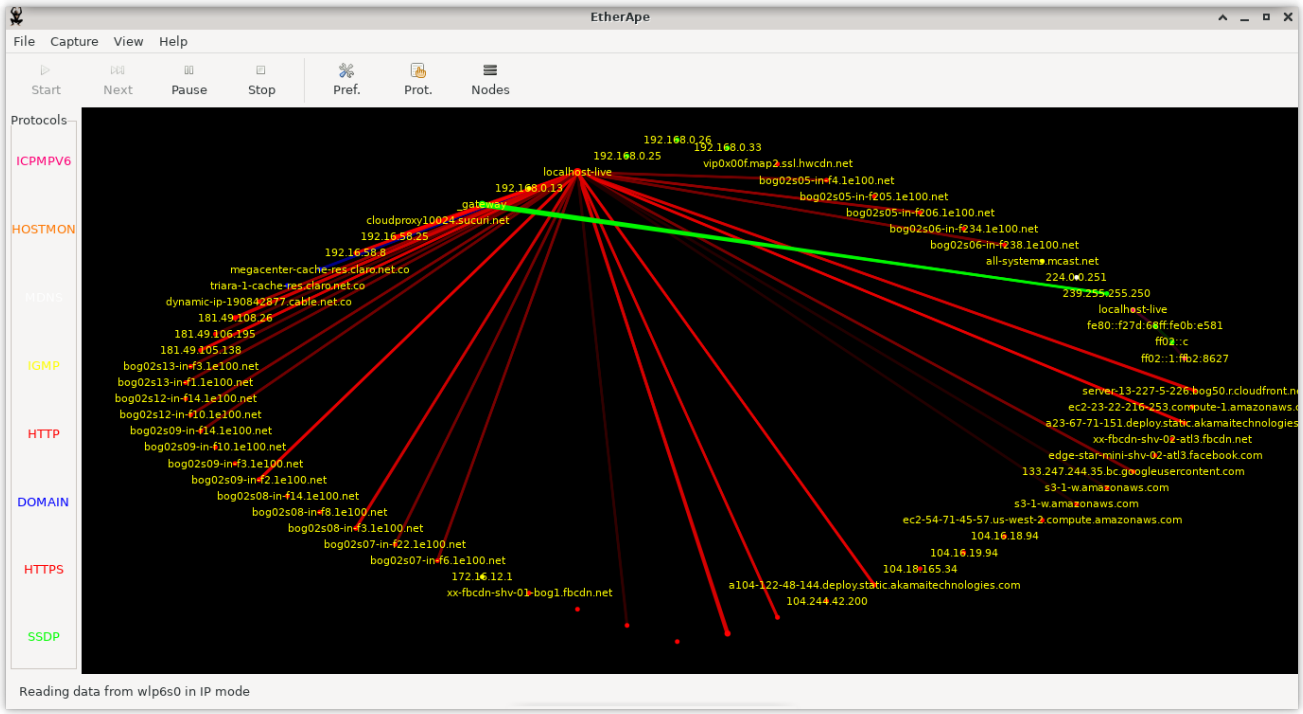


Figure 7: Nodos de la página de la USTA

Se puede apreciar que en el cargue de la página de la universidad, a su vez se consultan muchos nodos externos, por ejemplo Facebook, Cloudfront, Amazon, etc. Esto se debe a que la página de inicio tiene muchos servicios, en especial visuales, estos sacrifica el rendimiento de carga de la página. Podemos detectar también que el proveedor de internet de la universidad es Claro, que aparece en la parte superior izquierda de la captura de pantalla (megacenter-claro).

Ahora analicemos las estadísticas de algunos nodos al rededor del servidor de la página Web de la universidad.

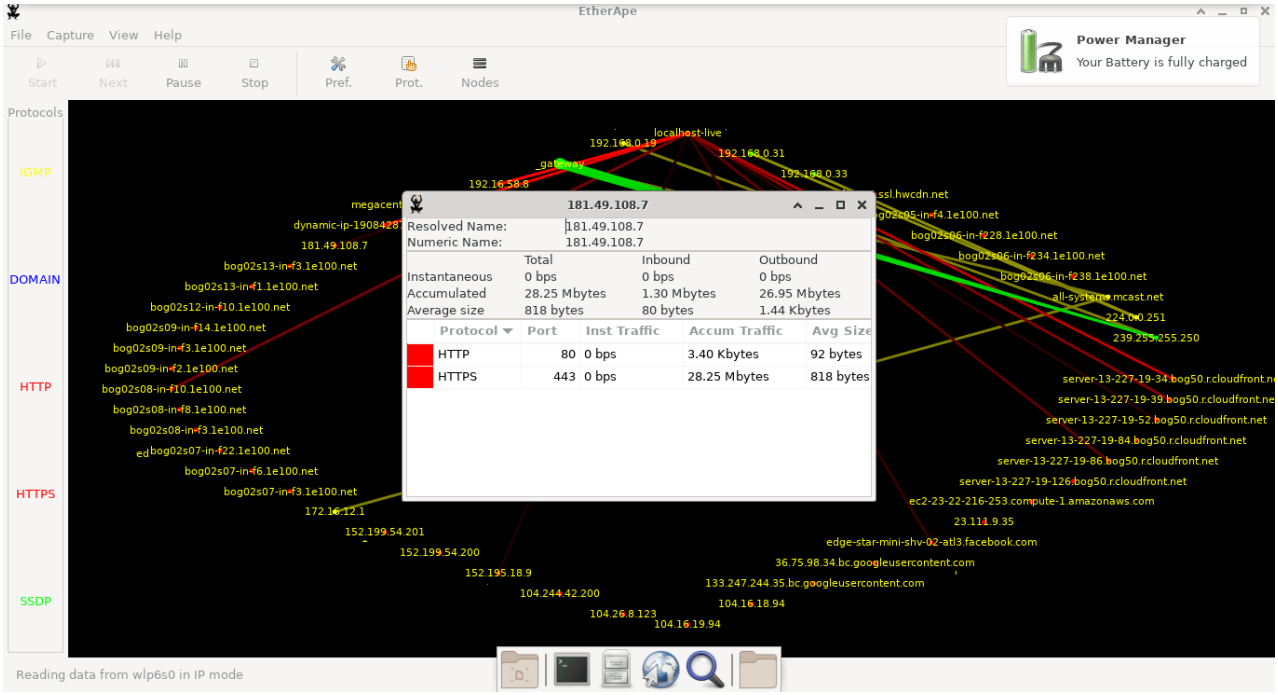


Figure 8: Estadísticas de algunos nodos

Podemos ver que en una ráfaga de cargue, utilizando los protocolos HTTP y HTTPS hubo transferencias de 818 bytes en promedio por ráfaga. Dejamos ejecutando a Etherape por un tiempo aproximado de 5 minutos, solamente abriendo la página inicial del campus virtual y el trafico se acumuló a 28.25 Megabytes. En tan corto tiempo, el trafico de red se contabiliza en Megabytes y puede ser una fuerte carga para la red y los servidores de la universidad para tener estas tasas por solo una conexión. Además hay que tener en cuenta que el ejercicio que se hizo unicamente consistió en abrir la página principal del portal de la Universidad en Tunja y la página principal del campus virtual en Tunja.

Se recomienda que el equipo de trabajo del departamento de TIC se reúna con el equipo de trabajo de diseño Web de la página y evalúen estas métricas y puedan llegar a tomar decisiones que no sacrifiquen el diseño de la página Web ni tampoco su desempeño.

5.1.2 Ettercap

Es otra herramienta de diagnóstico de red. Para ejecutarla digitamos el comando: **sudo ettercap -G.**

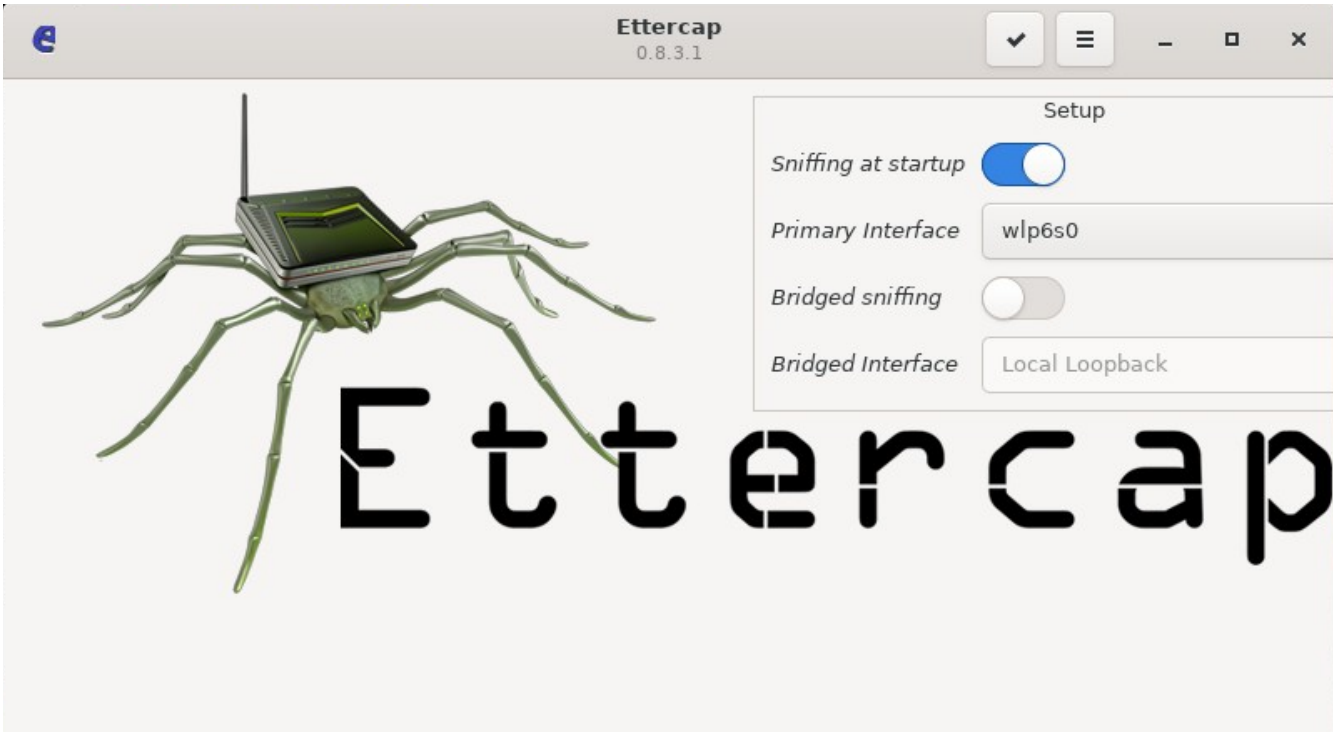


Figure 9: Herramienta Ettercap

De una forma sencilla, podemos conocer la información de los computadores que pertenecen a la red local, sencillamente haciendo clic sobre el botón de host, después de haber ejecutado el test (sniffing) haciendo clic en el botón play. En este corto diagnóstico que se interrumpió al minuto de ejecución se encontraron once máquinas, de las cuales me brindan información de su dirección física (MAC address) y su dirección de red (IP address). Estas máquinas corresponde a computadores encendidos, celulares, cámaras de vigilancia y el router de la red.

Por la secuencia de las direcciones IP, podemos detectar que la red está configurada con un servidor de DHCP (protocolo de configuración dinámica de host), es decir, el router tiene un servidor que asigna de forma automática las direcciones IP del los computadores que se van conectando a él.

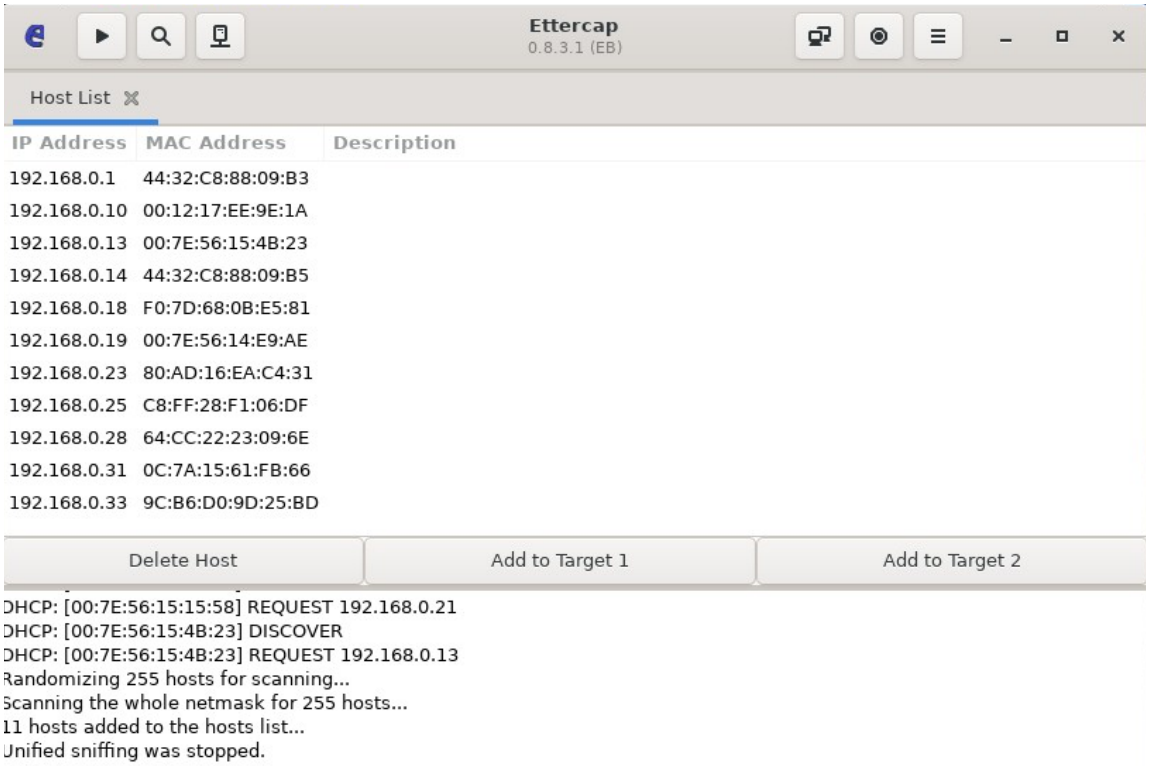


Figure 10: Información de los computadores que pertenecen a la red local

Se buscaron aleatoriamente 254 hosts porque el direccionamiento de esta red es de clase C (192.168.0.xx), en el campo de xx solo permitirá desde el 1 hasta el 254.

5.2 Detección de contraseñas

Fedora Security Lab dispone de varias herramientas para intentar adivinar contraseñas configuradas en diferentes sistemas. Vamos a considerar a Crunch, Hydra, y Medusa.

Existen varios métodos para detectar la contraseña de un usuario en un sistema, por ejemplo, la fuerza bruta que consiste en un algoritmo que calcula las posibles combinaciones de una contraseña, teniendo en cuenta su longitud (cantidad de caracteres), el conjunto de caracteres (alfabéticos, numéricos, especiales); y después intenta ingresar al sistema con cada una de estas combinaciones. Es una técnica muy demorada y dependiendo de la configuración de la contraseña y del poder del cómputo, puede tardar años o inclusive décadas en descifrar la contraseña. Otra técnica es el diccionario de contraseñas, este diccionario es un archivo que contiene las contraseñas más comunes o posibles de utilizar, este algoritmo es más rápido que el de fuerza bruta, pero la predicción de la contraseña depende de que tan común es. La última técnica, que es la más utilizada en la actualidad es la ingeniería social, no se trata de un algoritmo computacional, es descifrar la contraseña teniendo en cuenta el perfil de quien la configuró. Esto requiere, conocer a la persona, su fecha o lugar de nacimiento, sus hobbies, sus películas o series favoritas, el nombre de sus parientes, amigos o compañeros de trabajo, etc. En realidad, es aplicar técnicas sicológicas y- sociológicas alrededor de la persona. Obtener esta información depende de la creatividad del hacker, por ejemplo, citar a la victima, a reuniones sociales para extraer la información, hurgar en la basura de su trabajo o casa, visitar las redes sociales de la victima, o una herramienta muy utilizada actualmente, que es el fishing. El fishing se puede lograr, entre otras, enviando un correo fachada a la victima, por ejemplo, utilizando los logos y creando una página falsa de la entidad bancaria de la victima. Sin saberlo, de forma ingenua se invita a la victima que visite esta página Web falsa, o que descargue un archivo malicioso, o que se habilite un software licenciado (crack). Una vez el usuario haya caído en la trampa se puede capturar la información sensible de seguridad.

Para este laboratorio vamos a utilizar herramientas de la primera y segunda categoría: fuerza bruta y diccionario de contraseñas.

5.2.1 Crunch

Fedora Security Labs dispone de una biblioteca que contiene un conjunto de herramientas forenses, de acuerdo con los parámetros del CERT (equipo de respuesta ante emergencias informáticas), denominado cert-forensics-tools. El repositorio de herramientas forenses de Linux CERT, suministra muchos paquetes útiles para adquisición cyber-forense. No es un repositorio aislado sino que es una

extensión de sistemas soportados. Las herramientas pueden ser instaladas como se necesiten o todas a la vez utilizando el metapaquete cert-forensics-tools. Actualmente, Fedora y CentOS/RHEL suministran este repositorio. Procederemos a instalar el repositorio, primero descargamos el repositorio.

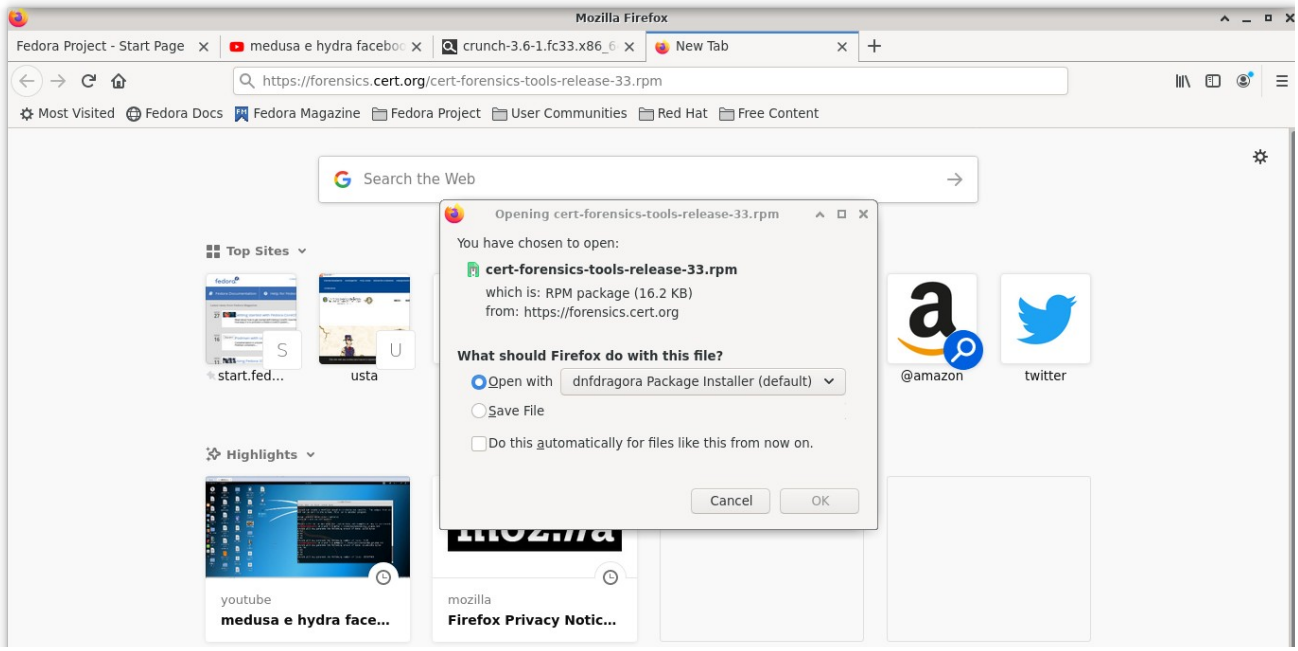


Figure 11: Descargar el repositorio

Una vez descargado el repositorio procederemos a instalar a Crunch:

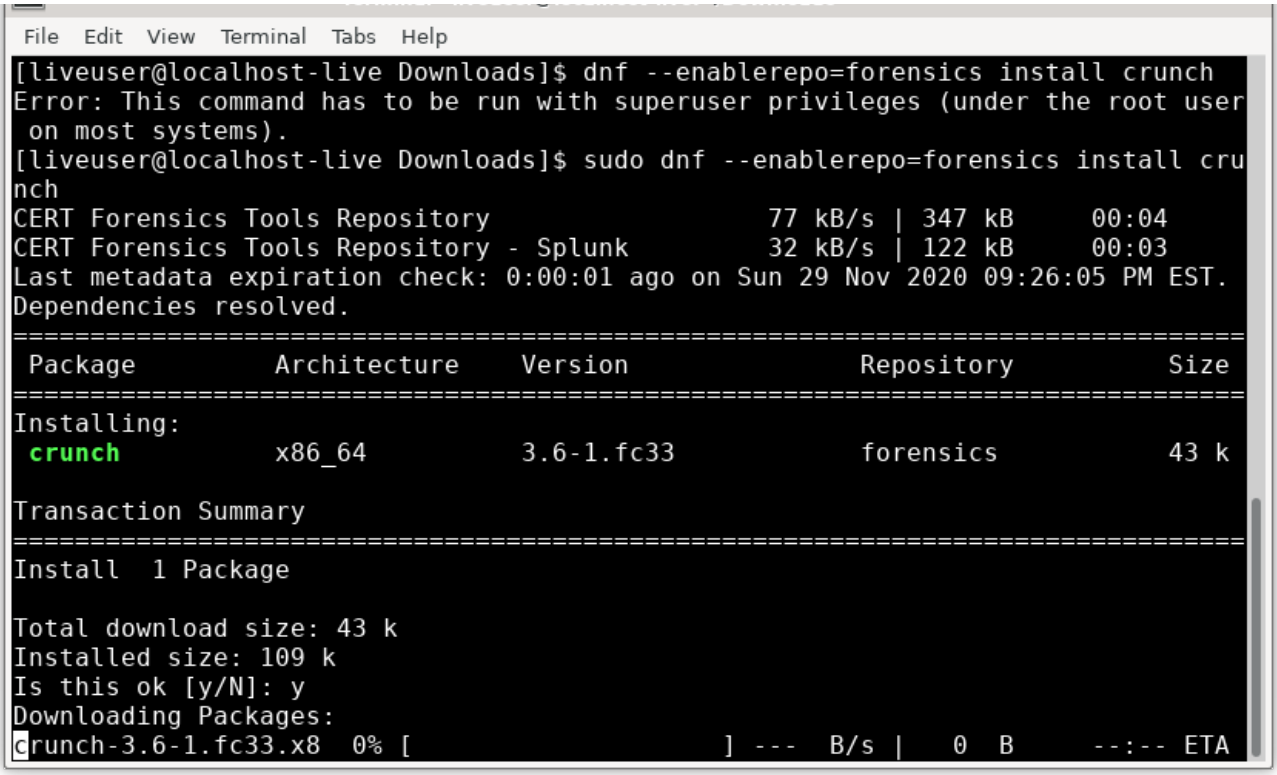


Figure 12: Instalar Crunch

Con Crunch[1] podemos crear diccionarios con todas las combinaciones posibles, de acuerdo con la configuración de la contraseña, para posteriormente, mediante otra herramienta, como es el caso de Hydra y Medusa, poder hacer ataques de fuerza bruta. Por ejemplo, podemos utilizar el comando: **crunch 5 5 aw72! > passwords.txt**.

1 https://youtu.be/Pd2fTPZNCN0

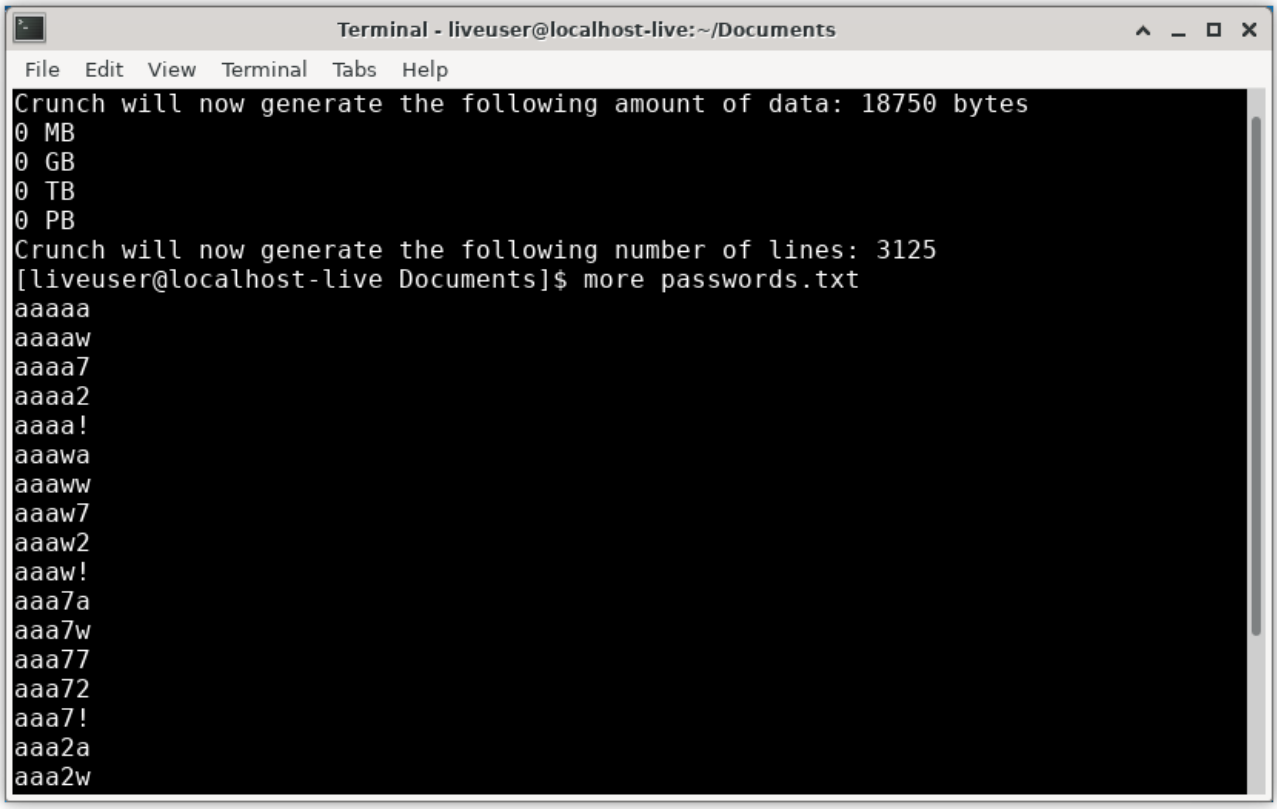


Figure 13: Creación del diccionario mediante el comando crunch

Como podemos ver en la figura anterior, creamos un archivo denominado passwords.txt que tiene todas las posibles combinaciones de los caracteres que se dieron como parámetro en el comando, es decir, los caracteres ‘a’, ‘w’, ‘7’, ‘2’, ‘!’, y la longitud de estas contraseñas son de cinco caracteres, ya que se dio como parámetro “5 5”, que significa mínimo cinco caracteres y máximo cinco caracteres.

5.2.2 Descargar un diccionario de contraseñas

Como vimos, el comando crunch creó un archivo de contraseñas con todas las combinaciones posibles, de acuerdo con los parámetros que se suministraron en el comando crunch. Este procedimiento no es tan efectivo, ya que consume muchos recursos computacionales y descifrar la contraseña podría tomar mucho tiempo o incluso nunca descifrarlo. Grupos de hackers y entusiastas por la seguridad computacional han creado y alimentado constantemente diccionarios de contraseñas más comunes utilizadas por las personas. En la figura siguiente, descargamos un diccionario de contraseñas de usuarios hispanohablantes:

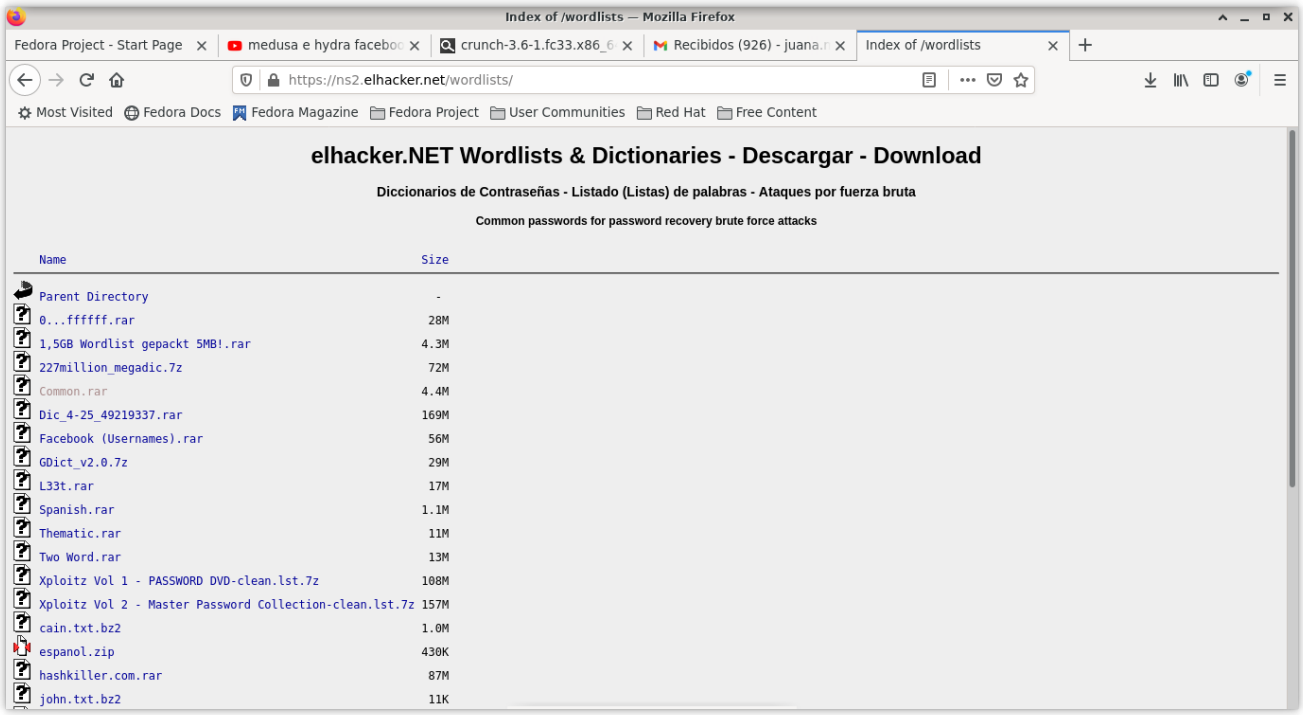


Figure 14: Diccionario de contraseñas hispanohablantes

De este repositorio de contraseñas descargamos el repositorio Common.dic.

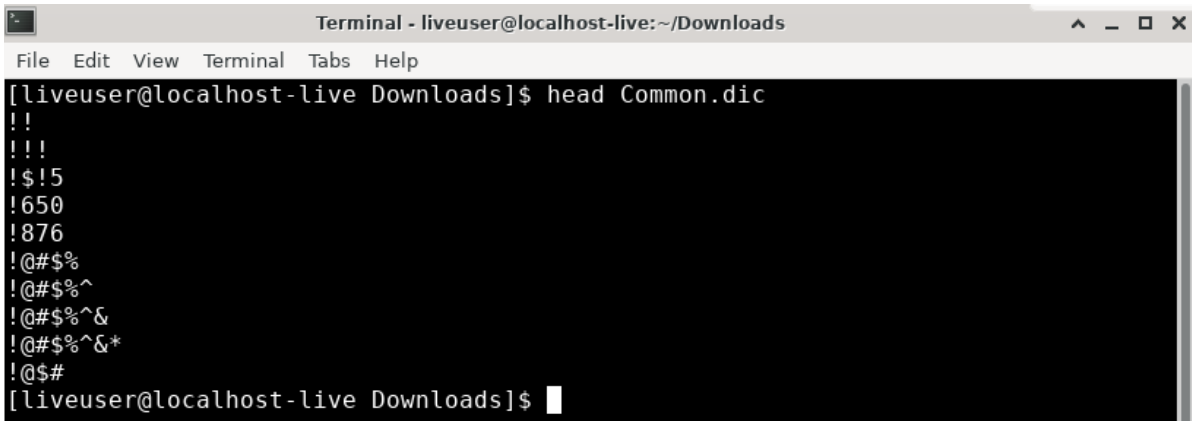
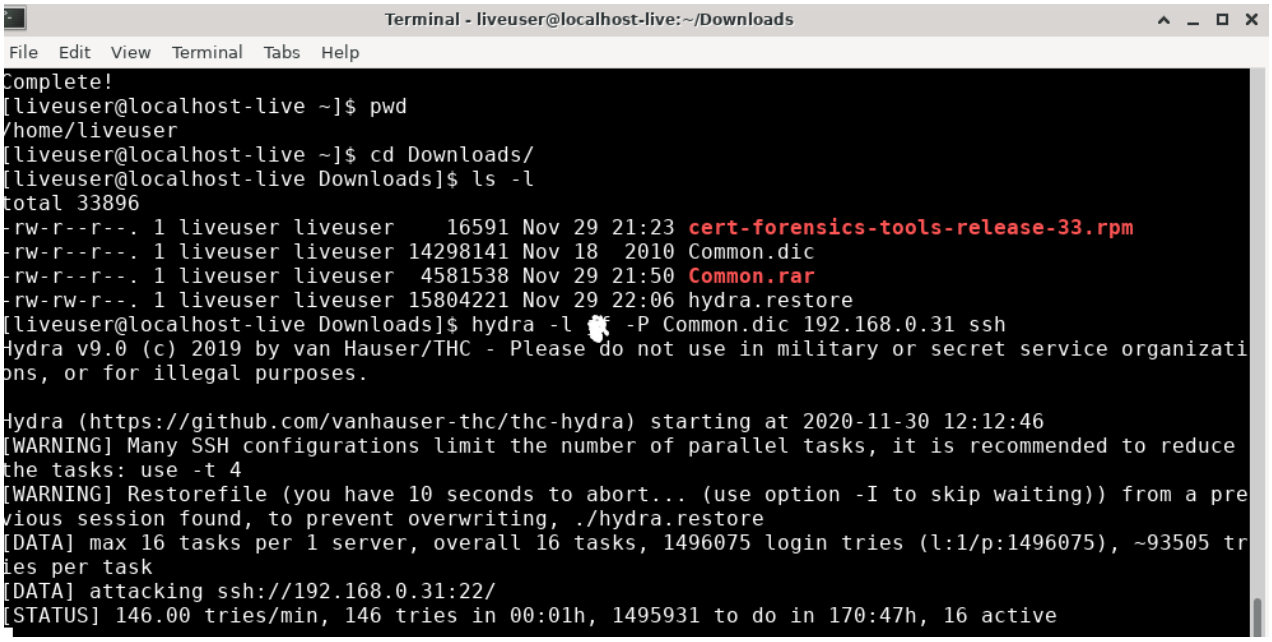


Figure 15: Descargar el repositorio Common.dic

5.2.3 Hydra

Con Hydra podemos hacer ataques secuenciales a sistemas, teniendo un diccionario de contraseñas, con el fin de descifrar la contraseña de un usuario determinado. Utilizamos el diccionario Common.dic que habíamos descargado anteriormente para descifrar la contraseña del sistema ssh de un determinado usuario. Por razones de seguridad ocultamos el usuario.



A pesar de disponer de este diccionario que contiene 1496075 contraseñas (se puede conocer con el comando: wc -l Common.dic), el comando Hydra nos dice que puede tomarse hasta 170:47 horas. Por tal razón, cancelamos el comando.

El comando ssh nos permite acceder a un sistema remoto. Por ejemplo:

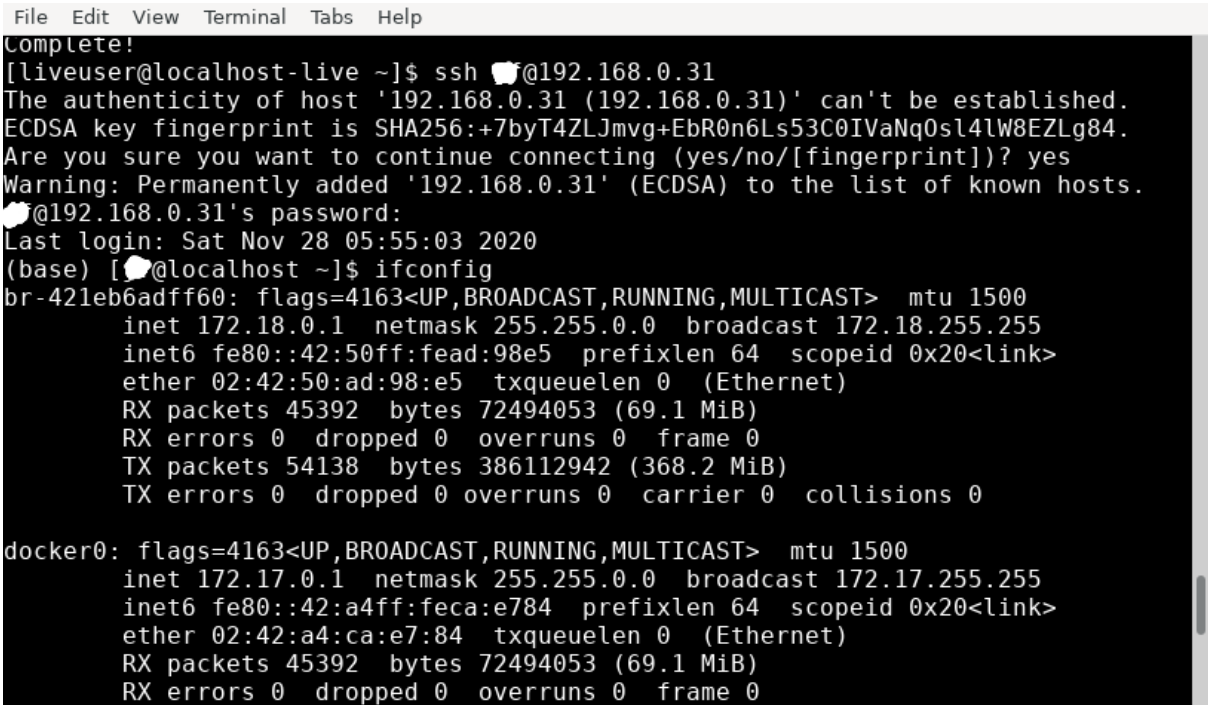


Figure 16: Acceder a un sistema remoto

Ahora intentemos descifrar una contraseña de email. El comando es muy similar al anterior, especificamos la cuenta de correo, el protocolo del correo (SMTP Simple Mail Transfer Protocol) y el puerto (en este caso, gmail utiliza el 465). Por lo tanto, el comando sería **hydra -S -l wc -l** juana.mendoza@usantoto.edu.co **-P Common.dic -s 465 smtp://smtp.gmail.com**.

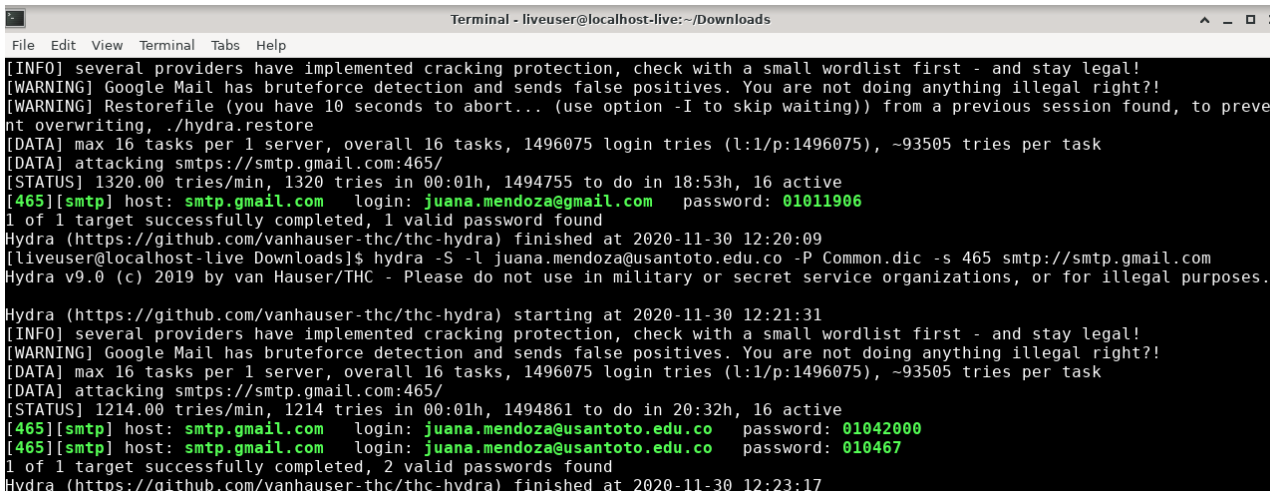


Figure 17: Descifrar contraseña

Como se puede apreciar en la anterior figura, el comando Hydra nos arrojo resultados, unas contraseñas. Pero nos advierte que Google Mail tiene un sistema de detección de fuerza bruta y envía falsos positivos. De hecho en esta figura, obtuvimos unas contraseñas (en color verde), pero estas contraseñas no son las reales. Podemos concluir que el sistema antifraude para la detección de contraseñas para Gmail está funcionando.

5.2.4 Medusa

Similar a Hydra, tenemos a Medusa, una herramienta creada principalmente para detectar contraseñas de sistemas Microsoft. La sitaxis es muy similar a la de Hydra:

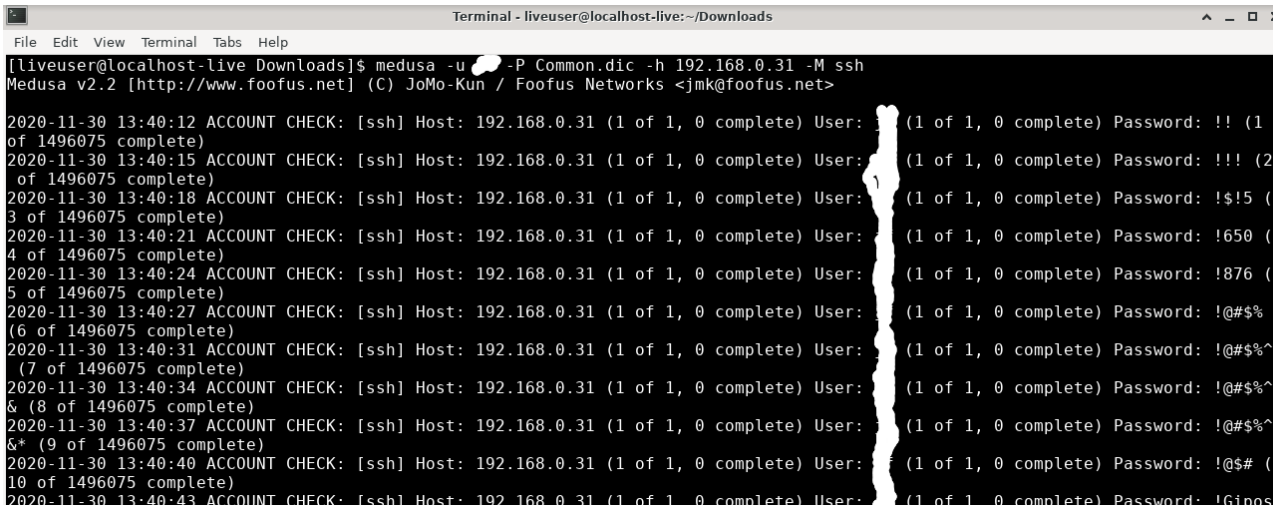


Figure 18: Medusa

La salida del comando es más didáctica, ya que nos muestra la hora del ataque, la contraseña utilizada y el avance de contraseñas probadas.

Como podemos concluir estas herramientas son poderosas, pero requieren de mucha paciencia, poder de cómputo. Asimismo, podemos detectar vulnerabilidad de los servidores destino del ataque. Por ejemplo, el servidor de Gmail tiene un algoritmo muy interesante para rechazar estos ataques creando falsas contraseñas (falsos positivos).

5. CONCLUSIONES

- Fedora Security Lab es probablemente una de las suits de seguridad más desconocidas para el público, otras distribuciones de Linux para seguridad son más populares, como es el caso de KaliLinux, pero Fedora Security Lab se puede emplear para tareas muy específicas y tiene el respaldo de la gran comunidad de Fedora y el apoyo económico de Red Hat.
- Fedora Security Lab es un laboratorio orientado al análisis forense y a las pruebas de penetración, conceptos claves para la cyberseguridad. La edición especial de Fedora 33 viene llena de utilidades muy prácticas, aplicaciones y programas que pueden utilizar ya sean profesionales o entusiastas en situaciones de prueba de penetración y análisis de seguridad, ya sea de redes o de sistemas.
- Ofrece herramientas para posibilitar el análisis forense informático basado en la metodología de recolectar, analizar y reportar, basados en los datos digitales de una forma legalmente admisible (lo que se conoce como hacking ético). La información se utilizar para detectar cosas y practicas que se están haciendo mal y para mejorar la detección y prevención del crimen informático.
- En las pruebas de penetración, más conocidas como pen-testing, nosotros determinamos la factibilidad de un conjunto particular de vectores de ataque e identificamos las vulnerabilidades de alto riesgo que resultan de la combinación de vulnerabilidades de bajo riesgo. Entonces, estas explotan en una secuencia particular. A esta metodología se le conoce como seguridad ofensiva.
- Al utilizar este laboratorio de seguridad, nosotros podemos estudiar la seguridad en nuestro computador, creando una cadena de ataque que pudiera potencialmente ocurrir en el mundo real.
- El laboratorio de seguridad de Fedora viene con aplicaciones que están agrupadas en categorías como análisis de código, forense, detección de intrusos, estadísticas de red, herramientas de contraseñas, reconocimiento, VoIP (voz sobre IP), pruebas de aplicaciones web, e inalámbricas.
- También se puede ampliar el repertorio de herramientas, simplemente instalando los paquetes con el comando **dnf**.
- Si queremos hacer pruebas desde nuestro computador, para no arriesgar su información y su integridad, es preferible ejecutar el laboratorio de seguridad de Fedora con un medio vivo, es decir, con medios ópticos o desde USB.

- El laboratorio de seguridad de Fedora fue creado por Fabian Affolter y Joerg Simon, ingenieros Seniors que tienen sus propias empresas de seguridad reconocidas mundialmente.

Referencias

Ghe01: Ghetta, Riccardo - Toledo, Juan, EtherApe a graphical network monitor, , etherape.sourceforge.io
Ett01: Ettercap Project, Ettercap, , ettercap-project.org
Foo01: Foofus Advanced Security Services, Medusa Parallel Network Login Auditor, , foofus.net/goons/jmk/medusa/medusa.html
Lyo01: Lyon, Gordon, NMAP.org, , nmap.org
Red01: Red Hat, Scap Workbench, , open-scap.org/tools/scap-workbench/
Ski01: , ,
ICE01: IceSurfer , SQLNinja, , sqlninja.sourceforge.net/
Com01: Combs, Gerald, WireShark, , wireshark.org
Tom01: Tomac, Yersinia, , github.com/tomac/yersinia
Wil01: Wilson, Ben - Boeving, Carsten, KaliLinux, , kali.org
Par01: Parrot Project, Parrot OS, , parrotsec.org
Xia01: Xiaopan Project, Xiaopan OS, , xiaopan.co
Seg01: Seguridad Wildless.net, Life WifiSlax, , wifislax.com
Bac01: BackBox, WHAT IS IT?, , https://www.backbox.org/
Sam01: Samurai Project, Samurai Web Testing Framework, 2016, http://www.samurai-wtf.org/
San01: Santoku, Santoku, , https://santoku-linux.com/
Bla01: L. Kayan, P. Freitas, A. Morozova, BlackArch Linux Penetration Testing Distribution, , https://blackarch.org/