Wednesday, May 6, 2015

Resumen Criptografia

Posibles noticias de actualidad

-Hackeo a Sony (Esta wea sale si o si lo posteo 3 veces) :

Como lo dice la maxima informática que el eslabón mas débil es el usuario. Usando la táctica de suplantación de identidad Pishing, para obtener datos de las víctimas haciéndose pasar por una entidad confiable.

En este caso un Pishing al Apple ID, que fue enviado a diversos administradores de Sony.

El ataque se realizo de la siguiente forma :

- Los administradores de Sony recibieron un correo electrónico de verificación de Apple ID muy convincente.
- Al introducir su contraseña los enviaba a otro link señalando que su contraseña era errónea.
- Ya con la información, la analizaban y conectaban con perfiles de LinkedIn de los usuarios, obteniendo mas datos pudiendo ingresar al sistema e infectarlo con un malware.
- Cabe destacar que esto también se debió a que lo usuarios poseían la misma contraseña para distintos servicios.

NSA propone llave que abra todos los dispositivos :

- Desde la aparición de los cifrados por defecto de Android 5.0 e iOS 8, la NSA desea evitar este escollo de seguridad para acceder, lo que genera que exista la posibilidad de otros posibles atacantes.
- Propone dos llaves una a nivel usuario y una compartida para que los organismos de seguridad que tengan acceso.(Fabricante , gobierno)

-**DoS a Apple** :

- Se descubrió que los dispositivos Apple al estar cerca de un router en particular se generaba una denegación de servicio (DoS).
- Ocurre debido a que generando un certificado SSL y generaba un fallo, con esto se caían las aplicaciones que usan protocolo SSL.

-**Password Alert Google**:

- Herramienta de google para prevenir pishing.

-**Pishing en chile :**

- Usaban pishing con un correo de verificación del numero de teléfono de gmail, luego los enviaba a un portal idéntico a gmail y obtenían los datos de usuario y contraseña.
- Dentro del correo usaban suplantación de identidad para pedir dinero.

-**Hackeo de Uber:**

-Se uso un ataque por fuerza bruta, que usaba como diccionario una base de datos que circula por el mercado negro con un registro de los nombres de usuarios y contraseñas mas comunes.

Google Hacks

Preguntas a realizar:

- ¿Cómo se llama lo que estoy buscando?
- ¿Dónde estará almacenado?
- ¿Qué extensión tendrá?
- ¿Cuándo se publicó?
- ¿Tendrá relación con algún software?

Sentencia	Valor(Hexadecimal)
Espacio	%20 (Tambien puede ser _ o dejar todo junto HolaMundo)
:	%30
"	%22
“="	%3D
/	%2f

Busquedas clásicas

- Index Of / : entrega un directorio donde están alojados los archivos de un dominio
- SW : rutas por defecto de wordpress para acceder a sus archivos CMS (fotos, archivos php, etc)
- PHP Bulletin Board : entrega un directorio erróneo pero dentro del error nos entrega la version de apache que puede servir para un ataque en base a la información de su siguiente actualización .

- Belarc: permite administrar y obtener los Key de cada SW en la maquina , todo esto online.
- As_qdr y Qrd Upagrade: permite buscar por meses y por días, minutos y segundos respectivamente
- Start : indica el numero de paginas desde donde se quiere buscar.
- Exploit Database : buscar alguna sentencia que nos permita ingresar al phpMyAdmin y utilizar algún ataque para acceder.

ISO/IEC

ISO: organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

La finalidad principal de las normas ISO es orientar, coordinar, simplificar y unificar los usos para conseguir menores costes y efectividad.

No todas las empresas lo adoptan como sistema de seguridad, su motivación es el certificado que entrega ventajas competitivas.

IEC: es la organización global líder en la preparación y publicación de estándares y normas internacionales en las áreas eléctricas y electrónicas.

Certificación ISO/IEC 27001: Permite gestionar y proteger sus valiosos activos de información.

Define los requisitos de un SGSI(Servicio de gestión de la seguridad de la información).

Entrega confianza a los clientes.

SGSI (Sistema de gestión de seguridad de la información):

La seguridad de la información según SGSI consiste en la preservación de su confidencialidad, integración y disponibilidad.

PDCA:

- PLAN : establecer SGSI
- DO : implementar y utilizar SGSI
- CHECK : Revisar SGSI
- ACT: Mantener SGSI

NCh-ISO 27001:2 : identico a SGSI, pero permite implementar controles de seguridad propios

OSSTMM

Test de seguridad que es :

- Cuantificable, en cuanto a seguridad de :
  - Información
  - Procesos
  - Tecnologias de internet
  - Comunicaciones
  - Inalámbrica
  - Fisica
- Consistente y que se pueda repetir
- Basado en el merito del testeador y analista, no marcas comerciales
- Exhaustivo
- Concordante con leyes individuales y locales, respetando el derecho a la privacidad.
- Valido mas allá del periodo actual.

Metodologia de intrusion

- Recopilación de la información
  - GoDaddy(Herramienta para obtener información de dominios)
  - Whois (Herramienta para obtener información de dominios)
- Mapeo de red
- Identificación de vulnerabilidades
- Acceso
- Escala de privilegios
- Enumeración adicional de sistemas
- Compromiso de ubicaciones y usuarios remotos

Buscar información de un objetivo

- Elegir empresa
- Encontrar maquinas y servicios
- Buscar usuarios
- Buscar backdoors

Passwords

Fuerza Bruta: forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

Para resolver ejercicios de duración de contraseña debemos saber dos datos:

- Pass/Seg que genero
- Numero de caracteres que dispongo

Entropía : Cantidad de variación de caracteres.

Se calcula H = L log2 W, donde W es la base utilizada y L largo del string.

Mnemotecnia : procedimiento de asociación mental para facilitar el recuerdo de algo (¿Pregunta secreta?)

CONTRASEÑA SEGURA ES AQUELLA QUE POSEE NUMEROS LETRAS Y CARACTERES ESPECIALES.

ATAQUES

THC-HYDRA: Intenta crackear por fuerza bruta gran cantidad de protocolos.(TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MYSQL, REXEC,RSH, RLOGIN, CVS, SNMP, SMTP-AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, LDAP2, LDAP3, Postgres, Teamspeak, Cisco auth, Cisco enable, AFP, LDAP2, Cisco AAA)

Jhon The Ripper : programa de criptografía de fuerza bruta, es capaz de romper algoritmos cifrados o en hash.

HashCat: recuperación de contraseña a partir del hash de cada una de ellas

Blind SQLi = es una técnica de ataque que utiliza la inyección SQL. Se evidencia cuando en una página web, por una falla de seguridad, no se muestran mensajes de error al no producirse resultados correctos ante una consulta a la base de datos,

mostrándose siempre el mismo contenido (es decir, solo hay respuesta si el resultado es correcto).

Problemas Touch: manchas en la clave de desbloqueo pueden evidenciar nuestra contraseña.

Pishing : Suplantación de identidad para obtener información de la víctima.

Webs chilenas

Metodo para recuperar contraseña:

- Enviando al correo
- Respondiendo la pregunta secreta
- Conociendo datos privados

Metodo de entrega de contraseña:

- Sigue siendo la misma
- Se cambia por una generada aleatoriamente

Cifrado Clásico

Definiciones:

- Texto claro: mensaje que se puede leer
- Cifrado: acción de poner ilegible el texto claro
- Texto cifrado: mensaje que ha sido cifrado
- Criptografía: ciencia que estudia algoritmos de cifrado
- Criptoanálisis: ciencia que intenta romper cifrado(Descubrir texto claro).
    - El criptoanalista conoce el algoritmo y su implementación
    - Lo unico secreto es la llave.
    - No se puede depender del desconocimiento del algoritmo.

Metodos de cifrado :

1. Atbash: codificación del alfabeto hebreo, consiste en usar el simétrico del alfabeto. También llamado método del espejo.
2. Cesar: Cifrado por desplazamiento, se selecciona un numero a correr en el abecedario para cifrar el código

3. Vignere: Se crea una matriz del abecedario, existe una llave que determina el cambio de cada letra respectivamente, si la llave es mas corta que el string se repite desde la primera letra de la llave.
4. Rail Fence : desorden de los caracteres, muy vulnerable.
5. Anagrama: palabras formadas a partir de otra original
6. Mors: lenguaje de sordos.

Base: cambiar de base permite ofuscar código.

1. Base 64: [A-Z][a-z][0-9][+/] Método para codificar binario dentro de los textos. A continuación una transformación.
    - Texto claro : Man, Texto cifrado = TWFu
    - Man codificado en ASCII corresponde a 77, 97 y 110
    - Pasando a binario queda 01001101, 01100001, 01101110
    - Se toman 6 bits ya que 2^6 es 64 valores distintos
    - 010011 | 010110 | 000101 | 101110
    - Quedando 19 , 22 , 5, 46
    - ahora en ASCII => T W F u
    - Para cuando no son múltiplos exactos se usa = de relleno h-> aA==

Otros mecanismos de seguridad:

1. One time pad (Digipass) : 100% seguro si se usa una sola vez y se compone de números aleatorios no predecibles.

    1.1 eToken Pass

    1.2 TAN (Transaction autenication number)

2. Tarjetas de coordenadas

3.Google authenticator : clave secreta base32, tiene una duración de 30 seg.

4. SMS = ingresar código enviado a celular por SMS.

5. Dual pin Protection : contraseñas asociadas a una pareja de usuarios.

6. Genoma humano : ADN estructura lineal que constituye nuestro genoma, es único.No existe mucha tecnología de identificación para este método

7.Maquinas Cifradoras :

- 2 rotores
- Periodos 676 (26x26)
- Tres rotores
- Periodo 17.576(26x26x26)
- Llave : alambrado del rotor
- Llave : posición inicial de los rotores

8. **Enigma**

Características:

1. 7 transformaciones (3 de ida,3 de vuelta y el reflector)
2. Reflector hace que enigma sea reciproco
3. Nunca un caracter de entrada queda igual al carácter de salida (A entrada nunca retorna A de salida)
4. Facilita criptoanális

Procedimiento:

1. Se debe elegir una posición inicial de los rotores
2. Esta posición se envía al receptor antes del mensaje para que pueda descifrarlo, permitiendo una posición distinta para cada mensaje.
3. Se envía posición inicial en claro mas la llave de mensaje cifrada 2 veces
4. La redundancia facilito el criptoanalisis.

Automatización

1. Para el 31 de cada mes poner los rotores 1,5,3 de izq a der
2. Posición inicial de rotores : 06(F), 20(T), 24(X)
3. Conectar el patch panel : U-A, P-F, R-Q, N-I, E-Y,B-G,H-L,T-X,Z-J

Errores de usuarios:

1. Encabezados predecibles “mein fuehrer!..”….
2. La misma llave mucho tiempo
3. Mensajes enviados todos los días a la misma hora y mismo encabezado

Funcionamiento :

1. Presionar una tecla
2. Pasa por el patch panel cambiando a otra letra
3. Llega a los rotores, al reflector y se devuelve por los rotores.
4. Pasa por el patch panel de nuevo
5. Se prende luz con la letra cifrada

Cifrado Simétrico

Cifrado de flujo:

Usar llave de flujo XOR

Texto claro	1001011
Llave de flujo	0101101
Texto cifrado	1100110
Llave de flujo	0101101
Texto claro	1001011

- Desventajas conociendo 2 datos se obtiene el tercero, llave o texto claro
- Es muy rápido

Cifrador de bloque:

- Se cifra un bloque de datos y una llave de cifrado de tamaño fijo
- El primero fue Lucifer
- Es una transformación simple, no necesariamente reversible
- Cada paso es round, mientras mas tenga mas seguro es.

Red de Feistel :

1. Se selecciona 1 cadena de 64 o 128 bits y se divide en 2 iguales A y B.
2. Se toma una función F y una llave K y se aplica solo a una cadena A o B
3. La cadena obtenida se cambia por la que no se realizan operaciones y se siguen haciendo rondas

DES

Lucifer fue el primer algoritmo de encriptacion que cumpla con todas las características solicitadas por la NSA .

La NSA cambio la llave de 112 a 56 bits.

Algoritmo

- Expansión : la mitad del bloque de 32 bits se expande a 48 bits mediante la permutación de expansión, duplicando algunos bits.
- Mezcla : El resultado se combina con una subclave utilizando una operación XOR. 16 subclaves se derivan de la clave inicial mediante la generación de subclaves.
- Sustitución: Tras mezclarlo con la subclave , es divido en 8 trozos de 6 bits antes de ser procesados por las S-cajas, o cajas de susticion. Cada una de las ocho S-cajas reemplaza sus seis bits de entrada con los cuatro de salida, de acuerdo con una transformación no lineal. Las S-cajas constituyen el nucleo de la seguridad de DES(sin ellas, el cifrado seria lineal y fácil de romper).

Sub Llaves

- Se seleccionan 56 bits de la clave de los 64 iniciales mediante la elección permutada, los ocho bits restantes pueden descartarse o útilizarse como bits de paridad
- Los 56 bits se dividen en 2 mitades de 28 bits a continuacion cada mitad
- En rondas sucesivas ambas se desplazan hacia la izquierda uno o dos bits y entonces se seleccionan 48 bits de subleva mediante la elección permitida 24 bits mitad izquierda y 24 a la derecha

DES no es mas seguro con mas de 16 round ni menos seguro con menos de 16 round.

Como romper DES

- Fuerza bruta : 2^56 intentos
- Criptoanalisis diferencial : 2^47
- Criptoanalisis lineal 2^43
- Las llaves de 56 bits no son seguras hoy

Donde se usa DES

- Cajeros automaticos
- Coneccin ethernet a corriente eléctrica

Blowfish:

- Alternativa a DES tiene un largo de llave de 448 bits
- Es codigo abierto

Cifrado Asimétrico

- Basa su dificultad en factorizar numero primos grandes
- Posee 2 llaves una publica y privada

Cifrador de la mochila:

- Sea el M = “HOLA”
- Sea n = {2,4,5,34}
- Transformamos en ASCII y luego a Binario Hola quedando H = 01001000, O = 01001111, L = 01001100, A = 01000001.
- Separamos por n (4 largo de hola) 0100 1000 0100 1111 0100 1100 0100 0001
- ahora reemplazamos y sumamos por la llave Cifrado = 4, 2, 4, (2+4+5+34), 4, (2+4), 4, 3. Cifrado final: 4, 2, 4, 45, 4, 6, 4, 34

Protocolo Diffie- Hellman :

Permite el intercambio secreto de claves entre 2 partes que no han tenido contacto previo, utilizando un canal inseguro y de manera anónimo.

Su seguridad radica en la extrema dificultad de calcular un logaritmo discreto.

Ejercicio : A y B acuerdan usar el numero primo p = 23 y base g= 5

1. A elige el numero secreto 6 y se lo envia a B, 5^6 mod 23=8
2. B elige el numero secreto 15 y lo envía a A, 5^15 mod 23 = 19
3. A calcula 19^6 mod 23 = 2
4. B calcula 8^15mod 23 = 2

Utilizar numeros grandes para evitar descifrado

RSA:

Se necesitan 2 numeros primos y usar (p-1)(q-1) y n que es el producto de los 2 numeros primos

1. Se tiene p= 3 q=11 y el mensaje a cifrar = 10010011011000110n= 3*11=33
2. (p-1)(q-1)=2*10=20
3. Escoger 2 primos menores a 20
4. e = 13 y d = 17 -> 13*21 = 221
5. calcular 221 mod = 1
6. dividimos el mensaje por la potencia menor a 33 -> 2^5
7. 10010 | 01101 | 10001 | 00010

8 . 18 | 13 | 17 | 2

9. c = 18^13 mod 33 = 24

10. c = 13^13 mod 33 = 19

11. c= 17^13 mod 33 = 29

12. c= 2^13 mod 33 = 8

13.texto cifrado 2419298

Descifrando:

1. m= 24 ^17 mod 33 = 18
2. m= 19^17 mod 33 = 13
3. m= 29^17 mod 33 = 17
4. m = 8^17 mod 33 = 2
5. Texto claro = 1813172