Technology & Security Risk Services

Ataques a políticas de seguridad según contexto

ERNST & YOUNG

Quality In Everything We Do

Índice

Políticas de Seguridad

A la hora de crear sistemas centralizados de gestión y control TI, la definición de procedimientos y normativas para homogeneizar criterios es uno de los primeros pasos a realizar. Tener un sistema a la hora de decidir que nombres emplear es lo que entendemos durante esta charla como “política de seguridad”.

1. Políticas y procedimientos nominales:

- Nombres de usuario

- Nombres DNS

2. Políticas de contraseñas:

- Prefijos, sufijos

- Tamaño de palabra y charset

Pruebas de seguridad

- Búsqueda de cgi en servidores web
- Búsqueda de equipos en red o dns
- Abuso de argumentos en cgi
- Búsqueda de Usuarios y contraseñas
- …

```
ilo@aramis:/mnt/share/Large Wordlist Collection$ du -h .
80K     ./password collection list for emule packs rar zip torrent passwort sammlung liste
64K     ./UserName_WordList
19M     ./Wordlist For Bruteforce Attack
17M     ./1600000 W0rter
4,3M    ./Bigdict - Big Wordlist Password
16M     ./Brute Force - Wordlist multilang
16M     ./English Dictionary Wordlist (1.4 Million Words)
7,2M    ./English -Wordlist
76M     ./Hacker Wordlist
94M     ./Hacker Wordlist Dictionary Over 8.5 Million Different Multilanguage Words By Netzwerg
120M    ./Md5 Wordlist Hack
64M     ./REFERENCES - wordlist-english-&-german-dictionary-big
120M    ./Wordlist_2_by_King_Passy
4,6M    ./Wordlist 521000 Passwords Usados Comunmente En Argentina Ht Passwd Txt
9,8M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/mwords
688K    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/english
3,0M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/mpos
5,8M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/mlang
8,2M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/mpron
176K    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/swedish
2,6M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/mhyph
9,8M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/moby/mwords
3,0M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/moby/mpos
5,8M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/moby/mlang
8,2M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/moby/mpron
2,6M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/moby/mhyph
26M     ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/moby/mthes
5,2M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/moby/mshak
60M     ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/moby
26M     ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/mthes
304K    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/italian
960K    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par/german
197M    ./Wordlist Dico For Bruteforce Full Language And Names Brute Force Word List Compil0 Par
750M    .
```

Problemas comunes

- Diccionarios:
  - Antiguos, no mantenidos
  - Desordenados
  - Categorías no útiles
  - Idioma
  - Tamaño
- Catálogos genéricos: temáticas desvinculadas
- Falta de herramientas
- Disponibilidad: Tiempo y recursos

Alternativa: John the ripper

- Manipulación de diccionario (rules)
  - Aceptar o rechazar origen y resultado
  - Control de caracteres:
    - Posición
    - Clases
    - Conversión, reemplazo
  - Capitalización (May. Min.)
  - Control de longitud
  - Control gramático: pluralizar, conjugación
- Uso específico en password cracking

Soluciones

- Catálogos contextuales
- Algoritmos predictivos

Catálogos contextuales

- Diccionarios pequeños
  - Generación instantánea
  - Categorización
- Contexto es utilizado para
  - Generación
  - Ponderación por catálogo
  - Idioma
- No se consideran Éxito y fracaso

Catálogos cortos y más precisos basados en contextos definidos

Algoritmos activos: adaptativos y predictivos

- Análisis estadístico.
- El contexto es utilizado para
  - Ponderación por palabra
- No se consideran Éxito y fracaso

Catálogos ordenados por probabilidad

Sistemas dinámicos

- Generación y ordenación de catálogos
- Mayor probabilidad de acierto
- Menor tiempo de prueba

Catálogos basados en contexto y ordenados por probabilidad

Catálogos

- No existe desviación gramatical
  - Solo palabras relacionadas
  - No existen signos de puntuación

- Catálogo contextual:
  - Catálogos específicos según categoría
  - Catálogos generales

Catálogos contextuales

- Conceptuación de términos
- Categorización de orígenes
- Puntuación y relativización
- Generación de árboles ponderados
- Generación de términos relacionados

Consideraciones

- Del término a la categoría y viceversa
- Traducción
  - Gramática (sustantivos)
  - Genero y Número
  - Acrónimos
  - Dialectos, expresiones hechas
- Desambiguación
  - Diferentes significados = diferentes árboles
- Desviación
  - Traducción y desambiguación, género y número

Ejemplos

- Venus y Júpiter
- Kyrgyzstan y Kashgar
- Legolas y Aragorn

Ejemplo

- **Venus** puede referirse a:
  - **Venus**, el segundo planeta más cercano al sol
  - **Venus (mitología)**,Diosa romana representativa del amor
  - **Venus Swimwear**, Marca comercial de ropa de mujer
  - **Símbolo Venus (♀),** referído a femenino
  - Nombre común de la droga: **2C-B**
  - **Venus Bucureşti**, equipo de futbol rumano
  - **Venus Williams**, Jugadora de tenis
  - Alias de Angelica Costello, actriz porno
  - **Venus**, Florida, pueblo de estados unidos
  - **Venus**, Texas, pueblo de estados unidos
  - **Venus**, Romania, resort situado en Rumanía
  - **Venus** (genus), a genus of clams in the bivalve mollusc family Veneridae
  - **VENUS** (Victoria Experimental Network Under the Sea), observatorio oceanografico cerca de Victoria, B.C., Canada
  - **Venus** Atrapamoscas (*Dionaea muscipula*), planta carnivora
  - **Venus** (TMNT), hermana de las tortujas ninja (aparición esporádica …

Ejemplo

- **Jupiter** puede referirse a:

  - **Jupiter** es el quinto planeta más cercano al sol
  - **Jupiter** (mitología), Principal dios romano
  - **Jupiter**, Florida, un pueblo en in Palm Beach County, Florida, Estados unidos
  - **Jupiter**, Romania, resort de verano en el mar negro
  - HMS **Jupiter**, naves de la armada "British Royal Navy"
  - **Jupiter** (tugboat), a historic tugboat preserved in Philadelphia, Pennsylvania
  - PGM-19 Jupiter Nombre de un misil
  - **Jupiter-C**, Nombre de un cohete
  - Operation **Jupiter**, Diferentes estrategias militares durante la segunda guerra mundial:
  - La Simfonia No. 41 de Mozart
  - **Jupiter**(album), Disco del grupo "Cave In"
  - Linea de equipos sintetizadores de la marca Roland:
    - Roland **Jupiter** -4
    - Roland **Jupiter** -6
    - Roland **Jupiter** -8
  - **Jupiter** Disco 1 de "Stadium Arcadium" de Red Hot Chili Peppers
  - **Jupiter** (compañia), estudio de desarrollo de hardware y software de videjuegos japonea
  - **Jupiter** JVM, nombre de una maquina virtual de Java
  - Sailor **Jupiter**, AKA Makoto Kino, personaje de *Sailor Moon*
  - Nombres de libros, grupos de música, etc...

Conceptuar términos (I)

- Manzana (Apple):
  - Fruta
  - Marca comercial
  - Espacio geográfico comprendido entre cuatro calles.
  - Color
- Palabras relacionadas con Manzana (fruta)
  - Zumo, semilla, flor
- Palabras dentro de la categoría frutas:
  - Pera, melocotón, cereza

Conceptuar términos (II)

- dos (two):
  - Número cardinal
  - Acrónimo de Denial of Service

Palabras relacionadas con dos (número):

  - Par, mitad, doble..

- Palabras dentro de la categoría Números
  - Uno, dos, tres

Conceptuar términos (III)

- Género y número:
  - Palabras relacionadas con “fruta”
  - Palabras relacionadas con “frutas”
  - Palabras relacionadas con “fruto”

  - Palabras relacionadas con “el señor de los anillos”

Traducciones (I)

- **Luna**:
  - Nombre própio de la luna de la tierra
  - Cuerpo espacial orbital: satélite
  - Los **Luna** familia de infanzones aragoneses, un miembro fue Benedicto XIII, llamado el **Papa Luna**
  - **Tristán de Luna** (¿ ? , España) - México, 1573), explorador y conquistador español
  - **Bigas Luna** (Barcelona, 1946), director y guionista de cine español.
  - **Luna Lovegood**, personaje ficticio de la serie Harry Potter
  - **Luna** es un municipio en Aragón (España)
  - **Río Luna** es un río de la provincia de León
  - **Isla de la Luna** es una isla situada en el lago Titicaca, Bolivia
  - **Luna (arquitectura)** es un patio interior. Se encuentra muy a menudo en palacios renacentistas aragoneses
  - **Luna StarCraft Map**, mapa para el juego StarCraft
  - …
- **Moon**:
  - Nombre propio de la luna de la tierra
  - Cuerpo espacial orbital
  - To ***Moon***, exponerse a la luz de la luna
  - The ***Moon***, carta del tarot
  - Elizabeth ***Moon***, novelista
  - Keith ***Moon***, batería del grupo The Who
  - Sailor ***Moon***, personaje de ficción y serie manga
  - *The Dark Side of the **Moon***, album por Pink Floyd
  - …

Traducciones (II)

Los álbumes de Astérix están llenos de guiños hechos a un público francés o al menos francófono. Esto se refleja sobre todo en los nombres de los personajes, que invariablemente juegan con la fonética francesa y pierden gran parte de su gancho en las traducciones.

Es el caso de **Idéfix** o **Ideafix**, por ejemplo, cuyo nombre francés coincide fonéticamente de forma exacta con *idée fixe* ("idea fija"), lo que no ocurre en su adaptación española, o el del bardo Assurancetourix (*assurance tous risques*, "seguro a todo riesgo"), que pierde sonoridad en su adaptación Seguroatodoriésguix y no se entiende en Asegurancéturix. Lo mismo ocurre con los nombres no galos:

- Romanos: Babaorum (*Baba au rhum*, "pastel borracho al ron"), en castellano Pastelalrum; Petibonum (*petit bonhomme*, "hombrecito" o "persona de a pie"), sin adaptar en castellano; Joligibus (*joli gibus*, "bonita chepa"), en castellano Caius Magníficus.
- Normandos: Grossebaf (*grosse baffe*, "gran bofetón").
- Vikingos: Zoodvinsen (*Zoo de Vincennes*, nombre del parque zoológico de París); Neuillisursen (Neuilly-Sur-Seine, Neuilly del Sena, una población francesa).

- Origen: wikipedia:

  http://es.wikipedia.org/wiki/Asterix

- Origen: asterisk, what's in a name:

  http://www.literarytranslation.com//workshops/asterix/translatingnames/

Algoritmos

Predictivos

- Plazo de predicción:
  - Corto
  - Medio
  - Largo
- Sistema de “scoring”
- “DataSet” muy amplio

Adaptativos

- ART (Adaptive Resonance Algorithm)
  - Basado en repetición.
- AMT (Adaptive Model Algorithm)
  - Basado en modelos estadísticos

Métodos predictivos

- Básicos:
  - Unigramas (frecuencia absoluta de palabras)
  - Mejorado: Bigramas, trigramas etc..
  - Requieren entrenamientos largos

- Categoriales
  - Reducen el entrenamiento
  - Predicción a corto plazo
  - Palabras relacionadas

AMT (Adaptive model algorithm)

- Usado principalmente para compresión
- Modelo estadístico
- “DataSet” dinámico
- Modelos definidos
- Según su uso, también puede considerarse predictivo

AMT

- Modelo **N** → muestra de longitud **N**

- Probabilidad del siguiente objeto en función de la muestra de modelo **N**

Promedio modelo 0

En todos los lenguajes existen algunos caracteres que aparecen con mayor frecuencia que otros (en español, por ejemplo, la letra *e* aparece con una frecuencia mucho mayor que la letra *x*). Si se analizan muchos textos escritos en un lenguaje determinado es posible obtener una tabla que indique la *frecuencia promedio* con la que aparece cada carácter en un texto cualquiera. La Tabla 2 muestra esas frecuencias (truncadas al tercer decimal) para el español.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
␣	A	B	C	D	E	F	G	H	I	J	K	L	M
0,16	0,098	0,01	0,043	0,048	0,108	0,006	0,01	0,003	0,065	0,003	0,000	0,05	0,02

15	16	17	18	19	20	21	22	23	24	25	26	27	28
N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0,056	0,001	0,08	0,022	0,004	0,058	0,067	0,04	0,03	0,006	0,000	0,001	0,009	0,002

Tabla 2: *Probabilidad de aparición de cada carácter en un texto en español*

Promedio modelo 1

- Por cada elemento del “CharSet” existe una tabla modelo.
- Si se diferencian minúsculas y mayúsculas, los cada carácter debería tratarse de forma independiente.

Promedio modelo N

- El tiempo para calcular los modelos no debería ser superior al empleado en la averiguación por fuerza bruta.

- Los recursos para soportar todos los modelos son excesivos

DAMT (Dynamic Adaptive Modeling Algorithm)

- Recalcula los modelos para cada nueva prueba (considera Éxito y fracaso).
- Modelos dinámicos de N a 0, donde N es la longitud de la palabra más larga del “DataSet”.
- No presenta desviaciones, si la palabra se puede componer utilizando varias palabras del diccionario el calculo sigue siendo válido.

Palabra: “root@loc”

- DataSet
  - Localhost
  - root@local
  - Test
  - Test2
  - otras
- Predicción:
  - root@loc -> -
  - oot@loc -> -
  - ot@loc -> -
  - t@loc -> -
  - @loc -> -
  - loc -> alhost
- root@localhost

¿Preguntas?

- Si quieres matar un gatito:
  - Inaki.LopezGalilea@es.ey.com
  - Daniel.CabezasMolina@es.ey.com