MATRIZ DE ESTADO DE SEGURIDAD

(Alejandro Corletti – acorletti@hotmail.com**)**

Madrid, marzo de 2004.

RESUMEN: El presente trabajo, es simplemente una propuesta a analizar, con pocos parámetros a tener en cuenta para poder evaluar el estado de seguridad de un sistema y realizar el seguimiento del mismo tratando de minimizar las subjetividades y fuertemente basado en herramientas de detección de vulnerabilidades e intrusiones. Como todo trabajo "Libre" de Internet, es susceptible a todas las mejoras que puedan surgir (que seguramente serán muchas) y que permitan mejorar el mismo.

DESARROLLO

Desde hace tiempo que existen en Internet, numerosos métodos para poder evaluar el estado de seguridad en que se encuentra un sistema informático, entendiéndose por sistema informático, el conjunto de componentes que hacen posible la sistematización a través de computadoras del trabajo de una organización, es decir: Servidores, hosts, bases de datos, componentes de red, etc.

Basado en la experiencia de trabajo cotidiano, se llegó a la conclusión que es imprescindible poder obtener valores, que permitan evaluar el nivel alcanzado en seguridad en un momento dado, como así también realizar las comparativas correspondientes para poder determinar si se ha mejorado o empeorado a lo largo del tiempo y corroborar o no, que las medidas que se adoptan son las adecuadas. Este detalle es de particular interés tanto para los administradores de sistemas como para los directivos, pues permite generar informes periódicos que justifiquen el trabajo y las inversiones realizadas demostrando el destino final de los mismos.

Luego de analizar y poner en práctica muchos de ellos, se ha llegado a la conclusión que presentan casi todos una serie de factores que hacen poco útil su empleo, algunos de ellos son:

- Subjetividad en la asignación de valores.
- Complejidad en su confección y cálculo.
- Dificultad en su mantenimiento y actualización.
- Generación de alta resistencia al cambio para los administradores.
- Falta de integración con herramientas de detección de eventos reales.

Buscando alguna forma práctica de llevar a cabo esta actividad, que se considera fundamental, se planteó definir inicialmente los conceptos que pueden hacer que esta tarea llegue a buen puerto, para luego avanzar a su desarrollo. Bajo esta idea, se propuso lo siguiente:

- Solo lo simple promete éxito.
- Eliminar toda subjetividad.
- Poder obtener índices de seguimiento y evolución.

Bajo estos conceptos rectores, se trató de acotar el problema a lo siguiente:

- El sistema debe estar organizado por zonas de seguridad, respetando rigurosamente la colocación de cada elemento en su zona, acorde al impacto que este puede ocasionar en el sistema, valorado por la criticidad de la información que controla.
- Se debe conocer claramente sus límites y puntos de acceso.
- Se deben integrar las herramientas de detección y escucha con esta tarea.
- Se supone que se mantienen actualizados todos los plugins necesarios para estar al día con detección de eventos y vulnerabilidades en las herramientas a emplear.
- Se centra la atención exclusivamente en servidores y elementos de red, dejándose a un lado los hosts cliente.
- Se tendrá en cuenta para su bastionado y calificación todo servidor y elemento de red, es decir Servidores de todo tipo, FWs, Routers, NIDS y HIDS, Puntos de acceso, etc. De aquí en más denominado "Elemento"

Para pasar al desarrollo, se definieron los siguientes conceptos:

Zonas:

Si bien se pueden diferenciar algunas otras, en este caso se limitarán a las tres siguientes:

a. **Internet:** En esta zona se encontrará todo elemento que puede ser accedido por cualquier usuario de Internet. Cabe aclarar, que en otro estudio que es motivo de mi tesis, esta zona suelo dividirla en dos (Internet y lo que denominé "Customnet"). La última de ellas, me pareció adecuado tratarla por separado en un estudio profundo, pues la característica que la diferencia es la posibilidad del usuario de interactuar con cierta libertad sobre un servidor en esa zona, como por ejemplo, disponer de un espacio de disco duro, personalizar páginas web, etc. Estas características generan algunos puntos débiles que no existen en el caso de un servidor que sólo permite realizar "consultas pasivas", por así llamarlas, es más ya hay disponibles servidores que operan sobre CDs, sin la necesidad de disco duro. No cabe duda que este último caso es de muy difícil alteración, no sucediendo lo mismo sobre un servidor que me permite acceder a su disco y realizar operaciones sobre el mismo. En resumen esta zona, puede ser subdividida por razones de seguridad, y a ambas podrá acceder un usuario totalmente desconocido desde Internet, pero cada una de ellas deberá ser tratada de forma diferente por parte del administrador de seguridad. En este trabajo, por razones de simplificar el ambiente de trabajo, no se subdividirá, pero puede hacerse sin ningún problema

b. **Intranet:** A esta zona sólo accederán usuarios de la empresa. Se pueden considerar también aquí a los partners y clientes, si los mismos están debidamente autenticados y registrados. Si no se los desea incluir aquí, al igual que en el punto anterior, se puede ampliar este trabajo con otra zona más denominada comúnmente "Extranet" y realizar el tratamiento de la misma, bajo esta metodología. A los efectos de acotar el problema, en este trabajo no se dividirá esta zona, pero se puede realizar sin mayores inconvenientes.

c. **Core:** Como su palabra lo dice, es el corazón de la empresa. Esta zona debe ser tratada con especial atención y claramente diferenciada de Intranet. En esta zona sólo accederán ciertos usuarios de la Empresa y con los máximos controles de seguridad. Se encuentran aquí las bases de datos de facturación, personal, I+D, etc.

Una vez definidas y acotadas estas tres zonas, se especifican los parámetros con los que se va a confeccionar la matriz.

Cada parámetro es tenido en cuenta desde dos posibilidades de ocurrencia:

- Por equipo: Afecta únicamente a ese elemento.
- Por Zona: Afecta a todos los componentes de la zona.

1. Detección de vulnerabilidades (Por equipo):

Este parámetro se obtiene a partir de herramientas de detección de vulnerabilidades como pueden ser Nessus, Nikto, ISS, etc. Se debe tener el rango de direcciones a escanear, y se obtendrá un informe de cada una de ellas. El grado de certeza de la información recabada, dependerá del empleo de las mismas. Se aplica a cada equipo, sin tener en cuenta la zona en que está emplazado.
Sobre los valores obtenidos, se deben acotar a tres niveles, que en general suelen ser: Alto, Medio y Bajo.

Aquí se tienen en cuenta dos factores:

- Cantidad de equipos vulnerables:
- Cantidad de vulnerabilidades:

CONSIDERACIONES:

- (Hipótesis 1) Factor entre cantidad de elementos/ Cantidad de elementos vulnerables: Inicialmente se planteó esta relación como detalle a tener en cuenta, es decir, si una empresa tiene mil equipos y sólo 10 vulnerables, ¿su situación es mejor que otra que tiene 20 equipos de los cuales 10 son vulnerables?, pareciera que sí, pero si una vez más se deja de lado las subjetividades, la realidad es que cualquiera de esos 10 equipos vulnerables, se puede explotar en ambas empresas y el daño potencial a ocasionar es igualmente probable para las dos. Por lo tanto, este valor se descarta y se considera igual que la empresa tenga 1000 elementos que 4.

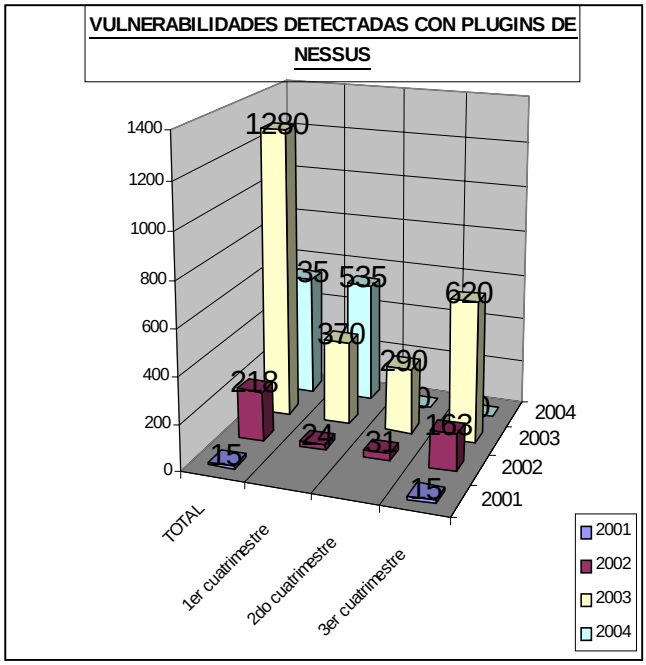
- (Hipótesis 2) Cantidad de vulnerabilidades: En este punto se debe centrar el análisis únicamente en los elementos vulnerables del sistema (independientemente de cuántos posea o se escaneen). El planteo aquí es el siguiente: ¿Cómo considerar la cantidad de vulnerabilidades?, ¿Es lo mismo tener 3 elementos vulnerabilidades que 100?. ¿Es lo mismo tener 10 altas y 100 bajas , que al revés? Aquí el enfoque varía del anterior, pues si bien evidentemente no es lo mismo, debe haber un límite en el cual, dado un cierto número de vulnerabilidades acordes a su peso, el resultado final no debería variar demasiado, pues ya se ha superado un cierto umbral de “Inaceptabilidad”, y en la práctica, daría casi igual tener 30 vulnerabilidades altas que 40 o casi 100 o 2000, etc, pues en esa situación el sistema es lo que se podría denominar “Un desastre”. En esta apreciación se desearía alcanzar un crecimiento logarítmico, bajo el cual se genere una alta pendiente inicial y alcanzado un cierto valor, la misma se haga menos pronunciada, pues se encuentra en una situación en la cual si bien sigue aumentando el valor, la situación es tan mala como en el valor anterior.

- (Hipótesis 3) Índice de vulnerabilidad: Considerando la hipótesis anterior, ¿Deben crecer iguales las curvas de vulnerabilidades Altas, Medias y Bajas?, en este punto aparece naturalmente la respuesta, pues no es lo mismo tener 10 vulnerabilidades altas y 2 bajas que al revés. Por lo tanto se deberían describir tres curvas cuyo crecimiento sea mucho más pronunciado en el caso de las vulnerabilidades Altas, sensiblemente menor en las medias y muy poco significativo en las Bajas.

- (Hipótesis 4): Envejecimiento: Se trata aquí de tener en cuenta que a medida que pasa el tiempo, surgen nuevas vulnerabilidades, y lo que hoy no se medía, mañana sí. Por lo tanto, si no se realiza una detección de vulnerabilidades actualizada, existen muchas probabilidades que el elemento posea una o varias nuevas. Este valor de envejecimiento es un índice que incrementa día a día el puntaje obtenido desde la fecha del último scan de vulnerabilidades de cada equipo.
  Para el análisis de esta hipótesis se tomó como referencia la herramienta NESSUS y se evaluó la evolución de los plugins a lo largo de estos cuatro últimos años. En la lista de plugins se tuvo en cuenta la fecha de modificación de los mismos y no la de creación, pues los mismos, muchas veces son actualizados cuando se descubre una nueva vulnerabilidad, y pudieron haber sido creados mucho tiempo antes, es decir que si una "Vulnerabilidad evoluciona", interesa saber que si es modificado el correspondiente plugin, su envejecimiento fue solucionado.

  A fines de febrero de 2004, Nessus posee 2048 plugins. A continuación se representa la plantilla y la gráfica correspondiente a su clasificación cuatrimestral desde diciembre del año 2001:

MES	2001	2002	2003	2004
Ene		0	105	456
Feb		2	62	79
Mar		15	91	0
Abr		7	112	0
May		3	64	0
Jun		1	158	0
Jul		3	45	0
Ago		24	23	0
Sep		58	180	0
Oct		2	153	0
Nov		16	62	0
Dic	15	87	225	0
TOTAL	**15**	**218**	**1280**	**535**
1er cuatrimestre		24	370	535
2do cuatrimestre		31	290	0
3er cuatrimestre	15	163	620	0



Se puede apreciar la evolución de vulnerabilidades sufrida desde fines de 2001 y el notable incremento de las mismas en cada cuatrimestre. El detalle más representativo es que en los dos primeros meses de este año (535 modificaciones de plugins), el valor se encuentra casi llegando al mismo del último cuatrimestre de 2003 (620).
Para no complicar el cálculo del envejecimiento, se limitará a adoptar un valor que se aprecia más que representativo, el cual será 600 modificaciones de vulnerabilidades en

un cuatrimestre (este número podrá ser ajustado a medida que se posean las estadísticas de los meses sucesivos).
Si se adopta este valor, implica que en 120 días aparecen 600 vulnerabilidades nuevas que detecta Nessus, es decir **5 por día**.
Para resumir este concepto, lo que se trata de explicar es que si no se realizan escaneos de vulnerabilidades a la propia red muy periódicamente, existirá la probabilidad de que cada día, cualquiera de los equipos, posea 5 vulnerabilidades nuevas Y NADIE LO SEPA, excepto alguien de afuera del sistema, que **sí** haya actualizado sus herramientas de búsqueda de vulnerabilidades, y en ese preciso instante detectará que existe un agujero de seguridad en ese sistema (y reitero: EL ADMINISTRADOR NO SE ENTERÓ AUN). Por lo tanto se adoptará no arbitrariamente, sino basado en una estadística, este valor de envejecimiento de **5 nuevas vulnerabilidades diarias**.

El parámetro que se adopta como valor de envejecimiento es **0,2 puntos** por cada día que pasa, es decir que cada 5 días que no se ejecute el scan de vulnerabilidades, incrementará en 1 punto el valor de ese equipo. Este valor se calcula automáticamente, en este ejemplo se emplea la función AHORA() de Excel, a la que se le resta la fecha en la que se pasó el scan y da como resultado los días que han pasado, ese valor se multiplica por 0,2 y resulta el número que representa al envejecimiento.

- (Hipótesis 5): Popularidad: Este parámetro se obtiene a partir de la cantidad de ataques totales que recibe un elemento dado por período de tiempo. La idea está fundamentada en la aparición de vulnerabilidades nuevas y la probabilidad de ser descubiertas en un determinado elemento, es decir, si se descubre una vulnerabilidad que aplica a un equipo que recibe 20 ataques por día, frente a otro que recibe 1000, el tiempo que tardaría un intruso en descubrirlo, debería ser menor en el último. El número que se obtenga aquí multiplica directamente al elemento, por lo tanto, si el mismo es muy popular, deberá hacerse un gran esfuerzo por bastionarlo, para poder obtener un valor final aceptable, y por el contrario si su popularidad es baja, el resultado final no será tan importante. Este valor se creyó conveniente tratarlo en forma porcentual, es decir de la totalidad de ataques que se recibe en una zona determinada, cuántos se corresponden con el equipo dado.

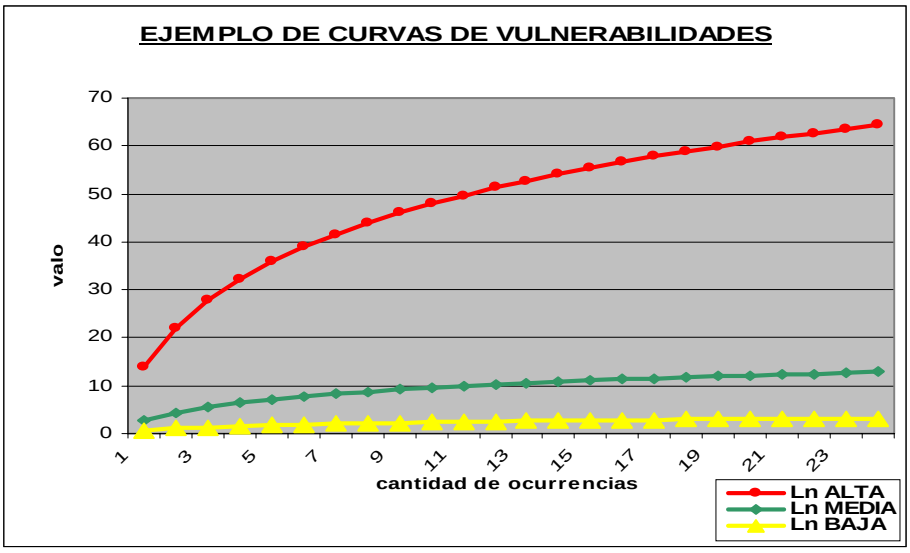
  Es decir: si en Internet se tienen 5 equipos, y se reciben 10.000 ataques distribuidos de la siguiente forma:
  - Equipo A = 5.000 ataques,
  - Equipos B y C = 2.000 ataques
  - Equipo D =800
  - Equipo E = 200

  La distribución sería:
  - Equipo A = 5.000/10.000 = 0,5
  - Equipos B y C = 2.000/10.000 = 0,2
  - Equipo D =800/10.000 = 0,08
  - Equipo E = 200 = 0,02

  A continuación se presentan distintas opciones de referencia sobre algunos posibles porcentajes. La elección del mismo queda al criterio del lector, se puede optar por el empleo de las magnitudes logarítmicas (para hacer más suave este parámetro) o en forma lineal. En este texto se aplicará la multiplicación por el valor dado en la cuarta columna { Ln(porcentaje+2) }, por ser el que más se ajusta a la red con la que se trabajó.

Porcentaje	LN(Porcentaje+1)	LN(Porcentaje+1,5)	LN(Porcentaje+2)	LN(Porcentaje+5)
0,001	0,0009995	0,4061316	0,6936471	1,6096379
0,01	0,0099503	0,4121097	0,6981347	1,6114359
0,1	0,0953102	0,4700036	0,7419373	1,6292405
0,2	0,1823216	0,5306283	0,7884574	1,6486586
0,5	0,4054651	0,6931472	0,9162907	1,7047481
0,8	0,5877867	0,8329091	1,0296194	1,7578579
1	0,6931472	0,9162907	1,0986123	1,7917595

A continuación se presenta un ejemplo de cómo serían las tres curvas para diferentes ocurrencias de vulnerabilidades y sus tablas de valores:



Vulner.	Ln ALTA	Ln MEDIA	Ln BAJA
1	13,86294361	2,772588722	0,69314718
2	21,97224577	4,394449155	1,09861229
3	27,72588722	5,545177444	1,38629436
4	32,18875825	6,43775165	1,60943791
5	35,83518938	7,167037877	1,79175947
6	38,91820298	7,783640596	1,94591015
7	41,58883083	8,317766167	2,07944154
8	43,94449155	8,788898309	2,19722458
9	46,05170186	9,210340372	2,30258509
10	47,95790546	9,591581091	2,39789527
11	49,698133	9,939626599	2,48490665
12	51,29898715	10,25979743	2,56494936
13	52,78114659	10,55622932	2,63905733
14	54,16100402	10,8322008	2,7080502
15	55,45177444	11,09035489	2,77258872
16	56,66426688	11,33285338	2,83321334
17	57,80743516	11,56148703	2,89037176
18	58,88877958	11,77775592	2,94443898
19	59,91464547	11,98292909	2,99573227
20	60,89044875	12,17808975	3,04452244
21	61,82084907	12,36416981	3,09104245
22	62,70988432	12,54197686	3,13549422
23	63,56107661	12,71221532	3,17805383
24	64,3775165	12,8755033	3,21887582

a. Valor vulnerabilidad alta = **ln** (Cantidad Ocurrencias altas +1) ***20**

b. Valor vulnerabilidad media = **ln** (Cantidad Ocurrencias medias + 1) ***** **4**

c. Valor vulnerabilidad baja: = **ln** (Cantidad Ocurrencias bajas+1)

Valor promedio = (a + b + c) * envejecimiento * popularidad

(el límite de lo que se aprecia aceptable por equipo es <**3**, un valor mayor debería ser solucionado, se corresponde con una vulnerabilidad media y una baja)

Se presenta a continuación una plantilla con ejemplos de distintas ocurrencias de vulnerabilidades:

			envejecimiento en días - popularidad porcentual (Ej:10-0,1 = 10 días - 0,1 popularidad)											
	Ejemplos de vulnerabilidades	**suma**	**10-0,01**	**10-0,1**	**10-0,5**	**10-0,8**	**20-0,01**	**20-0,1**	**20-0,5**	**20-0,8**	**50-0,01**	**50-0,1**	**50-0,5**	**50-0,8**
suma: valor de vulnerabilidades ya aplicados los logaritmos naturales (en este ejemplo se puede interpretar como un equipo con todas esas vulnerabilidades o varios equipos con su sumatoria de vulnerabilidades, para el ejemplo la idea es la misma	1Vuln. Baja	1	1,39627	1,4839	1,8326	2,0592	2,79254	2,9677	3,6652	4,1185	6,98135	7,4194	9,1629	10,296
	4 Vuln. Baja	2	2,79254	2,9677	3,6652	4,1185	5,58508	5,9355	7,3303	8,237	13,9627	14,839	18,326	20,592
	2 Vuln. Baja y 2 Vuln. Media - o 100 Vuln. Baja	5	6,98135	7,4194	9,1629	10,296	13,9627	14,839	18,326	20,592	34,9067	37,097	45,815	51,481
	5 Vuln. Baja y 2 Vuln. Media	8	11,1702	11,871	14,661	16,474	22,3403	23,742	29,321	32,948	55,8508	59,355	73,303	82,37
	7 Vuln. Baja y 4 Vuln. Media	10	13,9627	14,839	18,326	20,592	27,9254	29,677	36,652	41,185	69,8135	74,194	91,629	102,96
	4 Vuln. Baja y 1 Vuln. Alta	15	20,944	22,258	27,489	30,889	41,8881	44,516	54,977	61,777	104,72	111,29	137,44	154,44
	4 Vuln. Media y 1 Vuln. Alta	20	27,9254	29,677	36,652	41,185	55,8508	59,355	73,303	82,37	139,627	148,39	183,26	205,92
	2 Vuln. Baja y 5 Vuln. Media y 2 Vuln. Alta	30	41,8881	44,516	54,977	61,777	83,7762	89,032	109,95	123,55	209,44	222,58	274,89	308,89
	2 Vuln. Baja y 5 Vuln. Media y 4 Vuln. Alta	40	55,8508	59,355	73,303	82,37	111,702	118,71	146,61	164,74	279,254	296,77	366,52	411,85
	10 Vuln. Baja y 8 Vuln. Media y 6 Vuln. Alta	50	69,8135	74,194	91,629	102,96	139,627	148,39	183,26	205,92	349,067	370,97	458,15	514,81
	10 Vuln. Baja y 9 Vuln. Media y 10 Vuln. Alta	60	83,7762	89,032	109,95	123,55	167,552	178,06	219,91	247,11	418,881	445,16	549,77	617,77
	100 Vuln. Baja y 22 Vuln. Media y 22 Vuln. Alta	80	111,702	118,71	146,61	164,74	223,403	237,42	293,21	329,48	558,508	593,55	733,03	823,7
	100 Vuln. Baja y 60 Vuln. Media y 50 Vuln. Alta	100	139,627	148,39	183,26	205,92	279,254	296,77	366,52	411,85	698,135	741,94	916,29	1029,6
	1000 Vuln. Baja y 1000 Vuln. Media y 1000 Vuln. Alta	170	237,366	252,26	311,54	350,07	474,732	504,52	623,08	700,14	1186,83	1261,3	1557,7	1750,4

INACEPTABLE		Valor promedio = (a + b + c) * envejecimiento * popularidad
CRITICO		lo que es igual a : Valor promedio = suma * [días *0,2] * [Ln(porcentaje+2)]
PELIGRO		
MALO		
REGULAR		

La idea de la plantilla anterior es poseer una referencia de las diferentes zonas de peligro sobre las que debería mantenerse el sistema, por supuesto que puede mejorarse y/o adaptarse a cada sistema en particular, pero la intención de la misma es solamente servir de guía y permitir llevar adelante acciones de mantenimiento y mejora del estado de seguridad de la red.

Se reitera una vez más lo planteado en la hipótesis 1, respecto a la cantidad de equipos que se posean, pues se hace hincapié en que una red que llegue a una zona “amarilla” ya está en una situación irregular independientemente de la cantidad de equipos que posea, pues es vulnerable a varios tipos de ataques.

2. Bastionado (Por equipo):

Este valor se obtiene con herramientas que permitan cuantificar el nivel de robustez que posee un elemento, algunas de ellas son CISscan (para Unix) y MSBN (Para Windows). Cualquiera que se emplee da como resultado un informe aclaratorio y una calificación. Lo más significativo para esta matriz es la calificación, la cual es creciente, es decir que cuanto más sea el nivel de bastionado, mayor será al valor y viceversa.
El valor dado por las diferentes herramientas de bastionado no tiene por qué responder a la misma escala, por lo tanto para poder acotar el mismo independientemente del rango que emplee la herramienta se empleará la siguiente fórmula:

$$\text{Valor final} = [1 - (\text{NOTA} / \text{Máximo valor escala})] * 20$$

Con esto se obtiene un valor final acotado entre cero y 20 que se corresponde al porcentaje de peso que tiene ese valor dentro de la calificación de la herramienta que se emplee para medir el nivel de bastionado, siendo el valor "cero" el mejor nivel de bastionado y "veinte" el peor, por esta razón se resta a uno en la fórmula, pues interesa trabajar con valores similares a los tratados en el punto uno, es decir que cuanto mayor sea el resultado, peor será el nivel de seguridad (este principio se mantendrá durante todo este trabajo).

En este parámetro se aplican también las hipótesis 4 y 5 (Envejecimiento y popularidad) del punto anterior, es decir, a medida que va pasando el tiempo desde la última evaluación de bastionado, este parámetro se degrada, pues día a día aparecen nuevas vulnerabilidades y las herramientas de evaluación las van incorporando, pero si no se aplican las herramientas, no se obtiene el valor actual correspondiente. La única salvedad aquí es que se ha **detectado en la práctica** que el valor del envejecimiento no debe ser tratado de igual forma que con los detectores de vulnerabilidades, por dos características diferenciativas entre ambos:

- Las herramientas de evaluación de bastionado no son tan dinámicas como los detectores de vulnerabilidades (es decir que no sufren 600 actualizaciones cuatrimestrales).
- En la mayoría de los casos, solucionar temas de bastionado no es una tarea trivial ni automática, pues requiere muchas horas hombre y un importante grado de riesgo, pues a veces puede peligrar la estabilidad de los sistemas a bastionar.

Por estas dos razones, el multiplicador de envejecimiento de este parámetro se **adopta en 0,1** (a diferencia de 0,2 del punto 1. Vulnerabilidades), por lo tanto "envejece" en el doble de tiempo que el punto anterior

La popularidad afecta también directamente este valor y de igual forma que lo tratado en el punto 1.

Como se puede apreciar, los puntos 1 y 2 están íntimamente relacionados, pues ajustando el Bastionado se reducen las vulnerabilidades y a medida que aparecen nuevas vulnerabilidades, frecuentemente estas se solucionan aplicando nuevas medidas de bastionado. Lo importante en el tratamiento de ambos por separado es que permiten mantener "vivo" el estado del sistema y estar bien al tanto de la situación, cada vez que se realiza cualquier acción sobre uno de ellos, por esta razón es que se consideró fundamental su división en dos apartados.

Se presenta a continuación una tabla a título de ejemplo de distintos valores de bastionado y los resultados a medida que envejece:

		envejecimiento en días - popularidad porcentual (Ej:10-0,1 = 10 días - 0,1 popularidad)											
Valor	**Val*20**	**10-0,01**	**10-0,1**	**10-0,5**	**10-0,8**	**20-0,01**	**20-0,1**	**20-0,5**	**20-0,8**	**50-0,01**	**50-0,1**	**50-0,5**	**50-0,8**
0,1	2	1,40	1,48	1,83	2,06	2,79	2,97	3,67	4,12	6,98	7,42	9,16	10,30
0,2	4	2,79	2,97	3,67	4,12	5,59	5,94	7,33	8,24	13,96	14,84	18,33	20,59
0,5	10	6,98	7,42	9,16	10,30	13,96	14,84	18,33	20,59	34,91	37,10	45,81	51,48
0,8	16	11,17	11,87	14,66	16,47	22,34	23,74	29,32	32,95	55,85	59,35	73,30	82,37
1	20	13,96	14,84	18,33	20,59	27,93	29,68	36,65	41,18	69,81	74,19	91,63	102,96
2	40	27,93	29,68	36,65	41,18	55,85	59,35	73,30	82,37	139,63	148,39	183,26	205,92
3	60	41,89	44,52	54,98	61,78	83,78	89,03	109,95	123,55	209,44	222,58	274,89	308,89
5	100	69,81	74,19	91,63	102,96	139,63	148,39	183,26	205,92	349,07	370,97	458,15	514,81
8	160	111,70	118,71	146,61	164,74	223,40	237,42	293,21	329,48	558,51	593,55	733,03	823,70
10	200	139,63	148,39	183,26	205,92	279,25	296,77	366,52	411,85	698,13	741,94	916,29	1029,62
15	300	209,44	222,58	274,89	308,89	418,88	445,16	549,77	617,77	1047,20	1112,91	1374,44	1544,43
20	400	279,25	296,77	366,52	411,85	558,51	593,55	733,03	823,70	1396,27	1483,87	1832,58	2059,24
25	500	349,07	370,97	458,15	514,81	698,13	741,94	916,29	1029,62	1745,34	1854,84	2290,73	2574,05
30	600	418,88	445,16	549,77	617,77	837,76	890,32	1099,55	1235,54	2094,40	2225,81	2748,87	3088,86

Valor promedio = (a + b + c) * envejecimiento * popularidad

lo que es igual a : Valor promedio = suma * [días *0,2] * [Ln(porcentaje+2)]

VALOR ORIGIN.	VAL *20	Concepto
0,2	4	MUY BIEN
0,3	6	BIEN
0,4	8	REGULAR
0,5	10	LIMITE
0,6	12	MAL
0,7	14	CORREGIR
0,8 a 1	16 a 20	INACEPTABLE

INACEPTABLE	
CRITICO	
PELIGRO	
MALO	
REGULAR	

Como se puede apreciar en la tabla, existen zonas cuyos valores pueden servir, inicialmente como alarma y al superara estos, ya debería comenzar a tomarse acciones correctivas. Al final de la tabla, se incluye también los límites de valores que se han adoptado como criterio en estos parámetros.

3. Impacto (Por zona):

Este valor se podría analizar en cada elemento, pero a los efectos de simplificar el cálculo, se aplica directamente a cada zona. Se ha tomado esta decisión en virtud de contemplar que la distribución de elementos es acorde al primer principio rector aclarado al inicio de este documento. Es decir, el primer paso para iniciar el cálculo de esta matriz, es colocar cada elemento en su zona correspondiente, pues no puede caber duda acerca de la ubicación de cada uno. Una vez definidas las ubicaciones, se calculan todos los parámetros y la suma de los valores dados, se los multiplica por el impacto de cada zona.

Los valores a aplicar son:

a. Internet: 1
b. Intranet: 3
c. Core: 7

4. Ataques (Por zona):

Los conceptos de este parámetro son muy similares a los de detección de vulnerabilidades (parámetro 1). Existen dos diferencias importantes:

- Se aplica por zona.
- Cada zona presenta diferentes tipologías de ataques: Esto sucede por las diferentes "Barreras" colocadas en cada zona y, por esta razón también, la ocurrencia de ataques más sofisticados a medida que se avanza hacia el interior del sistema.

Los ataques se detectan con herramientas de detección de intrusiones, en este caso sólo se contemplan los de red, es decir los NIDS, sin considerar los de hosts (HIDS).

En general todos ellos dividen el grado de peligrosidad de los ataques en tres tipos:

a. prioridad alta:
b. prioridad media:
c. prioridad baja:

En este punto, nuevamente interesa trabajar con porcentajes, es decir si se tienen en cuenta el 100 % de los ataques (independientemente de la cantidad), ¿cuántos fueron altos, medios y bajos?. Esta decisión se adoptó en virtud que la cantidad de ataques no es un parámetro controlable por el administrador. Lo que se trata aquí es el hecho de poder ejercer cierto control sobre la peligrosidad de los mismos, es decir, un administrador puede adoptar medidas para minimizar los de prioridad alta o media, pero en general, es no puede reducir escaneos de puertos en la frontera de la red o el intento de empleo de un determinado exploit sobre un servidor que tiene abierto un puerto determinado, podrá bastionar el servidor, pero no hacer que desde el exterior no intenten aprovecharse de él. Si bien existen mil ejemplos y casos en los que sí se puede operar, se creyó más oportuno trabajar con porcentajes, para que esto dé como resultado el tomar medidas tendientes a minimizar los ataques de máximas prioridades, con lo cual, este parámetro se reduce considerablemente.
Las fórmulas a aplicar son:

a. Valor prioridad alta = porcentaje ocurrencias altas *** 200**

b. Valor prioridad media = porcentaje ocurrencias medias *** 40**

c. Valor prioridad baja: = porcentaje ocurrencias bajas * **10**

Valor final = a + b + c

En este parámetro se obtendrá un valor menor o igual que 200 y mayor o igual a cero, y se puede apreciar que tratando de minimizar los ataques de prioridad alta es donde realmente impacta en este valor final. Se adoptaron estos valores para guardar cierta relación respecto a los puntos tratados anteriormente, cuyo valor central de "peligro", oscila entorno al número 100. El valor final de ataques **se sumará** al valor final de cada zona.

5. Métodos y controles de acceso (Por zona)

Este parámetro se contempla por zona, pero se apreció conveniente obtener el promedio de la misma, es decir, a cada elemento se le colocará la puntuación acorde a los valores que se detallan

a continuación y luego una vez que se han completado todos los elementos de cada zona, se obtendrá la media de cada una de ellas, acorde a la siguiente fórmula:

Promedio Zona = [(**Σ** cada_valor_individual) / cantidad_elementos] + **1**

Como se puede apreciar este valor estará acotado entre "uno" y "seis", en el cálculo final se ponderará la zona en que esté ubicado. Este parámetro se ha pensado teniendo en cuenta que al ubicar elementos en zonas más críticas (Ej: core), sea necesario el adoptar medidas más importantes de control de accesos, pues caso contrario, disparará valores muy altos, por lo tanto es un valor que potencia mucho el resultado final sobre todo en las zonas de mayor impacto.

El promedio de Zona, se multiplicará directamente con todo el valor obtenido en cada una de ellas.

a. Nada: 5
b. Autenticación: 4
c. Autenticación y control de acceso: 3
d. Autenticación Fuerte: 2
e. Autenticación Fuerte y control de acceso: 1
f. Autenticación Fuerte, control de acceso y canal seguro: 0

6. **Otros parámetros:** A cada uno de estos parámetros se le asignará un valor entre "cero" y "cien". Ya que la subjetividad no puede ser dejada totalmente de lado, se trató en este punto de separar del resto de la matriz a todos los aspectos que de alguna forma no pueden ser taxativamente cuantificados, pero para poder controlar el límite de los mismos, se coloca esta escala (0 a 100), la cual sin lugar a dudas dependerá del criterio y la buena fe de quien la estime.

   a. Política de seguridad: El concepto aquí pasa por determinar el estado en que se encuentra la misma, los aspectos más importantes a considerar para asignar este valor son:

      - Actualización de la misma.
      - Análisis de riesgo.
      - Identificación de recursos.
      - Identificación de actividades (Accesos, DOS, desbloqueos, modificación de información, etc).
      - Autorización de uso de recursos.
      - Uso correcto de recursos.
      - Autorización de crear usuarios, accesos, permisos, etc.
      - Privilegios.
      - Responsabilidades de cada miembro del sistema.
      - Tratamiento de información sensible.
      - Proceder ante violaciones del plan y ante incidentes.
      - Política de difusión del plan.
      - Puntos de acceso.
      - Configuración de sistemas y equipos.
      - Tipos de servicios.
      - Protocolos y puertos.
      - Cuentas y contraseñas.

- Fronteras y puertas traseras.
- Seguridad física.
- Monitorización del sistema.
- Educación de usuarios y administradores.
- Procedimientos.

b. Reglas en Firewalls: La idea aquí es llevar un serio control sobre la configuración de estos elementos. El concepto básico es el bien conocido límite entre un FW "ajustado" o "amplio", es decir que sus reglas realmente se restringen a lo verdaderamente necesario, o si son generosas en cuanto a lo que dejan pasar. Este es un tema muy común y conocido para quienes tienen FWs muy dinámicos en cuanto al empleo de sus reglas y deben modificarlas con gran frecuencia. Suele suceder en muchos casos que se van abriendo reglas, que luego quedan sin ser vueltas a una situación normal, y a medida que va pasando el tiempo, existen muchas puertas abiertas, que en realidad no se sabe para quien son. El otro caso que suele ocurrir es que en vez de tomarse el trabajo de analizar en detalle la conexión, se abre el puerto "in" y "out" por las dudas, y sin siquiera acotarlo a un rango específico de direcciones origen y destino, es decir que se trata de una regla bastante "amplia".
Este parámetro, si bien es muy subjetivo, si se es consciente de la importancia del mismo (pues es el verdadero portero que tenemos en nuestro sistema) se puede parametrizar muy bien, y si se toma como punto de partida un valor bien alto, da como consecuencia la obligación de trabajar en serio sobre este aspecto para poder disminuir su valor. Se recomienda muy especialmente darle una gran importancia a este apartado, y tomarse el trabajo de profundizar seriamente con cada una de las reglas de cada FW, pues es una de las mejores medidas que se pueden tomar en seguridad.

c. Nivel de integración entre detector de vulnerabilidades y detector de intrusiones:

Al trabajar con ambas herramientas se empieza a hacer evidente que existen muchas vulnerabilidades que reconoce uno y que el NIDS no las marca como alarmas (o eventos). Para aclarar bien este punto se ejemplificará el caso de emplear Nessus y Snort (existe un artículo que se ha publicado anteriormente de esta actividad que se denomina ***"METODOLOGIA: GENERACION DE ATAQUES / DETECCIÓN CON NIDS (Nivel de Inmadurez de los NIDS {segunda parte})"***). Cuando se lanza un scan con Nessus, se pone de manifiesto que aparecen detectadas algunas vulnerabilidades, y si se estaba capturando en ese momento con Snort, no existe una relación uno a uno entre los eventos que marca uno y el otro. En el artículo anteriormente mencionado, se tomó el trabajo de aislar en laboratorio ambas herramientas, identificar cada uno de los plugins con los que Nessus atacaba y daba como resultado la detección de una vulnerabilidad y luego lanzarlos uno a uno, verificando la detección o no por parte de Nessus, los resultados fueron bastante interesantes, pero en definitiva, lo que interesa es el trabajo final que DEBE HACERSE; una vez que se identificó una vulnerabilidad de la red y se evidenció que Snort no es capaz de detectarla SÍ o SÍ, se debe generar la regla correspondiente en las local.rules de Snort, para que en caso de producirse este ataque, entonces se pueda estar tranquilo que Snort lo detectará, pues sino, se sabe que existe una vulnerabilidad en la propia red y encima se es consciente que no hay capacidad de detectarla, lo cual no es una buena situación de seguridad.

Lo que se trata entonces en este parámetro es de ser conscientes de la situación de correspondencia que existe entre las "n" vulnerabilidades que detecta Nessus y las "m" alarmas que genera Snort (o el conjunto de herramientas que se esté empleando). El valor final a colocar aquí es bastante preciso si se hizo bien el trabajo (y es muy aconsejable

hacerlo), en la medida que no se domine este tema pasa a ser más subjetivo, y si esta es la situación, se debería colocar un valor alto, pues realmente se está mal posicionado y esto obligará a profundizar en el tema.

d. Empleo de Backups:
En este punto nuevamente aparece la subjetividad, pues no se puede se muy matemático en su asignación, pero los aspectos a tener en cuenta son:
- Política de Backups.
- Empleo de Backups.
- Tipos de medios empleados.
- Almacenamiento de los mismos (locales y remotos).
- Metodologías de recuperación de información.
- Prácticas de recuperación de información.
- Nivel de redundancia en los medios de backup.
- Solidez de la infraestructura de almacenamiento (Clusters, arrays de discos, etc.).

e. Administración y control de Logs:

Los logs son los verdaderos repositorios e informantes de todo lo que está sucediendo en un sistema.
En la inmensa mayoría de los sistemas, suelen ser tomados como una medida preventiva de última prioridad, es decir que se analizan los mismos cuando ya no hay otra solución. La realidad es que los mismos deben ser DEFINIDOS – OPTIMIZADOS y MANTENIDOS.

Lo que se trata de decir aquí, es que son tan importantes que no pueden ser tomados como "default", sino que debe planificarse bien:

- "Qué" se debe guardar
- "Cómo" se debe guardar
- "Dónde" se debe guardar
- "Cuándo se deben borrar"
- "De qué manera emplearlos".

Una vez definidos, comienza la etapa de OPTIMIZACIÓN de los mismos, pues empiezan a llenarse los discos de grandes volúmenes de información y "El bosque tapa al árbol", por lo tanto se difunden los eventos verdaderamente importantes en un "bosque" de trivialidades.

La etapa final de estos eventos es mantenerlos adecuadamente, para que permitan ser empleados con el fin que se los definió.

Sin entrar en detalle sobre este tema, lo que se trata de recalcar aquí, es que este aspecto es importante, y no debe ser dejado de lado. Si es un tema que se encuentra relegado en el sistema, nuevamente la mejor opción es asignarle un valor alto, para crear la obligación de mejorarlo.

f. Seguridad física:

La seguridad física es uno de los puntos más débiles que se pueden observar en los sistemas, por lo tanto se trata también en esta matriz. Los aspectos a considerar son:

- Procedimientos de acceso a zonas críticas.
- Plan de distribución de elementos.
- Políticas de control de accesos.
- Empleo de medidas de protección física (llaves, sensores, alarmas, rondines, luces, etc).
- Planos actualizados de cableados, antenas, enlaces, etc.
- Personal de seguridad física.
- Empleo de carteles identificativos de cada zona.
- Seguridad en "horas grises".
- Clasificación de niveles de acceso.
- Monitorización de actividades y horarios.

g. Preparación de incidentes:

Un lema importante a destacar aquí es ***"tranquilidad ante la adversidad***".

Si no se prevé con anticipación las posibles reacciones que pueden ocasionar ciertos eventos o acciones, es mucho más difícil hacerlo durante un momento de confusión, alarma o crisis. Por esta causa es que se realizan simulacros, entrenamientos o prácticas en situaciones adversas en la mayoría de las actividades que desarrollan su labor bajo situaciones especiales (bomberos, policías, militares, personal adiestrado para catástrofes, etc). En el caso de un sistema, sucede igual, toda situación que haya estado prevista, planificada y ensayada tiene muchas mayores probabilidades de éxito que si no se ha hecho.
Los aspectos a considerar en este punto son:

- Pasos a seguir ante incidentes
- Pasos a seguir para la recolección de información para análisis forensic
- Aspectos que se deben analizar para la recolección de información para análisis forensic
- Metodología para instruir y actualizar al personal abocado al tratamiento de incidentes (Políticas, Procedimientos, Planes).
- Simulación de Incidentes
- Preparación para análisis forensic
- Políticas y procedimientos para análisis forensic
- Cadena (árbol) de llamadas
- Cadena (árbol) de escalada
- Inventarios de HW
- Planos de Red
- Formularios de reportes, planillas e informes
- Métodos de comunicación
- Formación de personal en Procedimientos Operativos Normales (PON)
- Herramientas disponibles (Inventario de las mismas, Secuencia de empleo, Manuales de empleo, Ubicación, Responsables).
- Procedimientos de logs (Metodología, envíos, túneles, seguridad, centralización, normalización, resguardo, consulta o visualización).
- Procedimientos de tiempo (Metodología, empleo de protocolo NTP, sincronización, monitoreo).
- Procedimientos de resguardo de información general
- Políticas de privacidad de la información
- Laboratorio de Forensic

h. Procedimientos:

Es muy interesante el hecho de tomarse el trabajo de documentar todas las actividades que se realizan con cierta rutina. El detalle particular que esto supone es "la no imprescindibilidad" de las personas. Desde el punto de vista de seguridad, se están produciendo con más frecuencia de la deseada, hechos generados por personal que tenía cierto control de los sistemas y que se sintió herido por alguna causa en particular (desde su ego, pasando por el factor económico hasta un despido, etc). En ejemplos como estos, y en muchos otros más, no se puede permitir la dependencia de una persona para el funcionamiento del sistema. La mejor forma de llevar adelante cualquiera de estas situaciones es a través de procedimientos claros y entendibles, que permitan rápidamente solucionar este tipo de hechos. Sin el menor lugar a dudas esta es una tarea que afecta directamente a la seguridad, por lo tanto se incluye también aquí, para que se valore el nivel alcanzado en este tipo de procedimientos. Algunos ejemplos son:

Para instalación de elementos.
Test de procedimientos.
Procedimiento de Actividades agendadas.
Procedimientos ante incidentes.
Procedimientos post incidentes.
Procedimientos para evaluación de vulnerabilidades.
Procedimientos de autenticación y control de accesos.
Procedimientos de backup y restauración.
Procedimientos de bastionado.
Procedimientos de puesta en servicio.
Procedimientos para la administración de nombres y direcciones.
Procedimientos para la administración de cuentas.
Procedimientos para la administración de contraseñas y claves.

7. RESULTADO FINAL:

El resultado de todos estos parámetros queda reflejado en una base de datos muy simple (o en su defecto a través de plantillas), que deben permitir realizar cuatro consultas.

- Internet.
- Intranet.
- Core.
- FINAL.

Las tres primeras son iguales y responden al mismo formato. La única diferencia entre ellas es el multiplicador de zona, llamado IMPACTO y tratado en el punto 3.

Estos valores son:

Internet: 1
Intranet: 3
Core: 7

Los datos de cada consulta son:

- Una plantilla como la que se detalla a continuación por cada zona, donde deben figurar la totalidad de los elementos de esa zona:

Elemento	Popularidad	Detección de vulnerabilidades					bastionado			Ataques				Ctrl. Acc.	PUNTAJE FINAL DE ZONA
		fecha Scan	altas	medias	bajas	Valor FINAL	fecha Bast.	valor	Valor FINAL	%Bajo * 10	%medio * 40	%Alto * 200	SUMA Atqs		
Elemento A															
Elemento B															
Elemento C															
Elemento n															
Ejemplo:	0,1	hace 10 días		4	7	13,963	hace 10 días	2	13,96	5	16	20	41	4	275,69

- Una plantilla FINAL que constará de o siguiente:

PLANTILLA DE CÁLCULO FINAL	IMPACTO	VALOR TOTAL DE ZONA
Puntaje final INTERNET :	x 1	
Puntaje final INTRANET :	x 3	
Puntaje final CORE :	x 7	
Política de seguridad :		
Reglas en Firewalls :		
Nivel de integración Scan/NIDS :		
Empleo de Backups :		
Administración y control de Logs :		
Seguridad física :		
Preparación de incidentes :		
Procedimientos :		
VALOR FINAL :		

Las tres primeras filas son el resultado del "PUNTAJE FINAL DE ZONA" de cada una de las tres plantillas anteriores, multiplicadas por el IMPACTO de cada zona (1,3 ó 7).
Las ocho filas siguientes son el valor obtenido de cada uno de los "Otros parámetros" (tratados en el punto 6. De este documento).
El "VALOR FINAL", se obtendrá con la **suma** de las once filas.

A continuación se presenta un cuadro representativo de diferentes valores que se pueden obtener en cada zona, y los colores que se aplican a criterio de este trabajo. Estos colores y límites son los que se proponen aquí, pero seguramente pueden ser mejorados o ajustados a cualquier otra red. Solamente se proponen como parámetros a tener en cuenta inicialmente, luego cada administrador en particular podrá ir adaptando los mismos a sus sistemas o mejorar radicalmente la mecánica de obtención y los límites aquí propuestos.

Límites propuestos son:

color	Impacto = 1	Impacto = 3	Impacto = 7
blanco	<200	<601	< 1001
amarillo	201-400	601-900	1001-2000
verde	410-700	901-1500	2001-3000
naranja	701-1200	1501-2500	3001-4000
rojo	1201-2000	2501-3500	4001-5500
gris	>2000	>3501	>5500

Estos son los límites que se proponen (Como propuesta a mejorar).

Los criterios que se han tenido en cuenta para estos valores, se fundamentan en mantener la idea de los colores, es decir AUNQUE EL RESULTADO FINAL SEA UN VALOR BAJO, si cualquier parámetro llega a colores verde o naranja DEBE SER SOLUCIONADO, y por lo tanto deja de tener sentido el valor final. Esta decisión se adoptó para obligar a mantener un equilibrio en todos los parámetros e imposibilitar que se produzca un agujero de seguridad en cualquiera de ellos, pues si esto sucediera inmediatamente pasaría este parámetro a tomar un color inaceptable.

La plantilla de ejemplo es la siguiente:

Vulnerabil.	Basionado	Valor ataques = 20 / Valor ataques = 100 / Valor ataques = 200	ctrl Acc = 1 / ctrl Acc = 3 / ctrl Acc = 6	Impacto = 1	Impacto = 3	Impacto = 7
1,83	1,83	23,66	23,66	23,66	70,98	165,62
			70,98	70,98	212,94	496,86
			141,96	141,96	425,88	993,72
		103,66	103,66	103,66	310,98	725,62
			310,98	310,98	932,94	2176,86
			621,96	621,96	1865,88	4353,72
		203,66	203,66	203,66	610,98	1425,62
			610,98	610,98	1832,94	4276,86
			1221,96	1221,96	3665,88	8553,72
3,67	3,67	27,33	27,33	27,33	81,99	191,31
			81,99	81,99	245,97	573,93
			163,98	163,98	491,94	1147,86
		107,33	107,33	107,33	321,99	751,31
			321,99	321,99	965,97	2253,93
			643,98	643,98	1931,94	4507,86
		207,33	207,33	207,33	621,99	1451,31
			621,99	621,99	1865,97	4353,93
			1243,98	1243,98	3731,94	8707,86
14,66	14,66	49,32	49,32	49,32	147,96	345,24
			147,96	147,96	443,88	1035,72
			295,92	295,92	887,76	2071,44
		129,32	129,32	129,32	387,96	905,24
			387,96	387,96	1163,88	2715,72
			775,92	775,92	2327,76	5431,44
		229,32	229,32	229,32	687,96	1605,24
			687,96	687,96	2063,88	4815,72
			1375,92	1375,92	4127,76	9631,44
27,49	27,49	74,98	74,98	74,98	224,94	524,86
			224,94	224,94	674,82	1574,58
			449,88	449,88	1349,64	3149,16
		154,98	154,98	154,98	464,94	1084,86
			464,94	464,94	1394,82	3254,58
			929,88	929,88	2789,64	6509,16
		254,98	254,98	254,98	764,94	1784,86
			764,94	764,94	2294,82	5354,58
			1529,88	1529,88	4589,64	10709,16
1,83	30,89	52,72	52,72	52,72	158,17	369,06
			158,17	158,17	474,51	1107,18
			316,34	316,34	949,01	2214,37
		132,72	132,72	132,72	398,17	929,06
			398,17	398,17	1194,51	2787,18
			796,34	796,34	2389,01	5574,37
		232,72	232,72	232,72	698,17	1629,06
			698,17	698,17	2094,51	4887,18
			1396,34	1396,34	4189,01	9774,37

3,67	41,89	65,55	65,55	65,55	196,66	458,87
			196,66	196,66	589,98	1376,61
			393,32	393,32	1179,95	2753,23
		145,55	145,55	145,55	436,66	1018,87
			436,66	436,66	1309,98	3056,61
			873,32	873,32	2619,95	6113,23
		245,55	245,55	245,55	736,66	1718,87
			736,66	736,66	2209,98	5156,61
			1473,32	1473,32	4419,95	10313,23
14,66	14,66	49,32	49,32	49,32	147,96	345,24
			147,96	147,96	443,88	1035,72
			295,92	295,92	887,76	2071,44
		129,32	129,32	129,32	387,96	905,24
			387,96	387,96	1163,88	2715,72
			775,92	775,92	2327,76	5431,44
		229,32	229,32	229,32	687,96	1605,24
			687,96	687,96	2063,88	4815,72
			1375,92	1375,92	4127,76	9631,44
27,49	41,89	89,38	89,38	89,38	268,13	625,65
			268,13	268,13	804,40	1876,94
			536,27	536,27	1608,80	3753,88
		169,38	169,38	169,38	508,13	1185,65
			508,13	508,13	1524,40	3556,94
			1016,27	1016,27	3048,80	7113,88
		269,38	269,38	269,38	808,13	1885,65
			808,13	808,13	2424,40	5656,94
			1616,27	1616,27	4848,80	11313,88
30,89	30,89	81,78	81,78	81,78	245,34	572,46
			245,34	245,34	736,02	1717,38
			490,68	490,68	1472,04	3434,76
		161,78	161,78	161,78	485,34	1132,46
			485,34	485,34	1456,02	3397,38
			970,68	970,68	2912,04	6794,76
		261,78	261,78	261,78	785,34	1832,46
			785,34	785,34	2356,02	5497,38
			1570,68	1570,68	4712,04	10994,76
41,89	41,89	103,78	103,78	103,78	311,33	726,43
			311,33	311,33	933,98	2179,30
			622,66	622,66	1867,97	4358,59
		183,78	183,78	183,78	551,33	1286,43
			551,33	551,33	1653,98	3859,30
			1102,66	1102,66	3307,97	7718,59
		283,78	283,78	283,78	851,33	1986,43
			851,33	851,33	2553,98	5959,30
			1702,66	1702,66	5107,97	11918,59
54,98	54,98	129,96	129,96	129,96	389,88	909,72
			389,88	389,88	1169,64	2729,16
			779,76	779,76	2339,28	5458,32
		209,96	209,96	209,96	629,88	1469,72
			629,88	629,88	1889,64	4409,16
			1259,76	1259,76	3779,28	8818,32
		309,96	309,96	309,96	929,88	2169,72
			929,88	929,88	2789,64	6509,16
			1859,76	1859,76	5579,28	13018,32

59,35	59,35	138,70	138,70	138,70	416,10	970,90
			416,10	416,10	1248,30	2912,70
			832,20	832,20	2496,60	5825,40
		218,70	218,70	218,70	656,10	1530,90
			656,10	656,10	1968,30	4592,70
			1312,20	1312,20	3936,60	9185,40
		318,70	318,70	318,70	956,10	2230,90
			956,10	956,10	2868,30	6692,70
			1912,20	1912,20	5736,60	13385,40
54,98	61,78	136,76	136,76	136,76	410,28	957,32
			410,28	410,28	1230,84	2871,96
			820,56	820,56	2461,68	5743,92
		216,76	216,76	216,76	650,28	1517,32
			650,28	650,28	1950,84	4551,96
			1300,56	1300,56	3901,68	9103,92
		316,76	316,76	316,76	950,28	2217,32
			950,28	950,28	2850,84	6651,96
			1900,56	1900,56	5701,68	13303,92
59,35	73,30	152,65	152,65	152,65	457,95	1068,55
			457,95	457,95	1373,85	3205,65
			915,90	915,90	2747,70	6411,30
		232,65	232,65	232,65	697,95	1628,55
			697,95	697,95	2093,85	4885,65
			1395,90	1395,90	4187,70	9771,30
		332,65	332,65	332,65	997,95	2328,55
			997,95	997,95	2993,85	6985,65
			1995,90	1995,90	5987,70	13971,30
61,78	61,78	143,56	143,56	143,56	430,68	1004,92
			430,68	430,68	1292,04	3014,76
			861,36	861,36	2584,08	6029,52
		223,56	223,56	223,56	670,68	1564,92
			670,68	670,68	2012,04	4694,76
			1341,36	1341,36	4024,08	9389,52
		323,56	323,56	323,56	970,68	2264,92
			970,68	970,68	2912,04	6794,76
			1941,36	1941,36	5824,08	13589,52
73,30	73,30	166,60	166,60	166,60	499,80	1166,20
			499,80	499,80	1499,40	3498,60
			999,60	999,60	2998,80	6997,20
		246,60	246,60	246,60	739,80	1726,20
			739,80	739,80	2219,40	5178,60
			1479,60	1479,60	4438,80	10357,20
		346,60	346,60	346,60	1039,80	2426,20
			1039,80	1039,80	3119,40	7278,60
			2079,60	2079,60	6238,80	14557,20
61,78	82,37	164,15	164,15	164,15	492,45	1149,05
			492,45	492,45	1477,35	3447,15
			984,90	984,90	2954,70	6894,30
		244,15	244,15	244,15	732,45	1709,05
			732,45	732,45	2197,35	5127,15
			1464,90	1464,90	4394,70	10254,30
		344,15	344,15	344,15	1032,45	2409,05
			1032,45	1032,45	3097,35	7227,15
			2064,90	2064,90	6194,70	14454,30

73,30	91,63	184,93	184,93	184,93	554,79	1294,51
			554,79	554,79	1664,37	3883,53
			1109,58	1109,58	3328,74	7767,06
		264,93	264,93	264,93	794,79	1854,51
			794,79	794,79	2384,37	5563,53
			1589,58	1589,58	4768,74	11127,06
		364,93	364,93	364,93	1094,79	2554,51
			1094,79	1094,79	3284,37	7663,53
			2189,58	2189,58	6568,74	15327,06
82,37	82,37	184,74	184,74	184,74	554,22	1293,18
			554,22	554,22	1662,66	3879,54
			1108,44	1108,44	3325,32	7759,08
		264,74	264,74	264,74	794,22	1853,18
			794,22	794,22	2382,66	5559,54
			1588,44	1588,44	4765,32	11119,08
		364,74	364,74	364,74	1094,22	2553,18
			1094,22	1094,22	3282,66	7659,54
			2188,44	2188,44	6565,32	15319,08
91,63	91,63	203,26	203,26	203,26	609,78	1422,82
			609,78	609,78	1829,34	4268,46
			1219,56	1219,56	3658,68	8536,92
		283,26	283,26	283,26	849,78	1982,82
			849,78	849,78	2549,34	5948,46
			1699,56	1699,56	5098,68	11896,92
		383,26	383,26	383,26	1149,78	2682,82
			1149,78	1149,78	3449,34	8048,46
			2299,56	2299,56	6898,68	16096,92
82,37	103,00	205,37	205,37	205,37	616,11	1437,59
			616,11	616,11	1848,33	4312,77
			1232,22	1232,22	3696,66	8625,54
		285,37	285,37	285,37	856,11	1997,59
			856,11	856,11	2568,33	5992,77
			1712,22	1712,22	5136,66	11985,54
		385,37	385,37	385,37	1156,11	2697,59
			1156,11	1156,11	3468,33	8092,77
			2312,22	2312,22	6936,66	16185,54
91,63	148,40	260,03	260,03	260,03	780,09	1820,21
			780,09	780,09	2340,27	5460,63
			1560,18	1560,18	4680,54	10921,26
		340,03	340,03	340,03	1020,09	2380,21
			1020,09	1020,09	3060,27	7140,63
			2040,18	2040,18	6120,54	14281,26
		440,03	440,03	440,03	1320,09	3080,21
			1320,09	1320,09	3960,27	9240,63
			2640,18	2640,18	7920,54	18481,26
103,00	222,60	345,60	345,60	345,60	1036,80	2419,20
			1036,80	1036,80	3110,40	7257,60
			2073,60	2073,60	6220,80	14515,20
		425,60	425,60	425,60	1276,80	2979,20
			1276,80	1276,80	3830,40	8937,60
			2553,60	2553,60	7660,80	17875,20
		525,60	525,60	525,60	1576,80	3679,20
			1576,80	1576,80	4730,40	11037,60
			3153,60	3153,60	9460,80	22075,20

148,40	308,00	476,40	476,40	476,40	1429,20	3334,80
			1429,20	1429,20	4287,60	10004,40
			2858,40	2858,40	8575,20	20008,80
		556,40	556,40	556,40	1669,20	3894,80
			1669,20	1669,20	5007,60	11684,40
			3338,40	3338,40	10015,20	23368,80
		656,40	656,40	656,40	1969,20	4594,80
			1969,20	1969,20	5907,60	13784,40
			3938,40	3938,40	11815,20	27568,80
222,60	103,00	345,60	345,60	345,60	1036,80	2419,20
			1036,80	1036,80	3110,40	7257,60
			2073,60	2073,60	6220,80	14515,20
		425,60	425,60	425,60	1276,80	2979,20
			1276,80	1276,80	3830,40	8937,60
			2553,60	2553,60	7660,80	17875,20
		525,60	525,60	525,60	1576,80	3679,20
			1576,80	1576,80	4730,40	11037,60
			3153,60	3153,60	9460,80	22075,20
308,00	148,40	476,40	476,40	476,40	1429,20	3334,80
			1429,20	1429,20	4287,60	10004,40
			2858,40	2858,40	8575,20	20008,80
		556,40	556,40	556,40	1669,20	3894,80
			1669,20	1669,20	5007,60	11684,40
			3338,40	3338,40	10015,20	23368,80
		656,40	656,40	656,40	1969,20	4594,80
			1969,20	1969,20	5907,60	13784,40
			3938,40	3938,40	11815,20	27568,80