Sistema de ciberdefensa dinámica basada en algoritmos evolutivos para la prevención de ataques informáticos

Autor: *Ernesto Serrano Collado*
Tutor: *Juan Julián Merelo Guervós*

Granada, 23 de Septiembre de 2019

Hola!

Me llamo Ernesto Serrano

- Rompiendo cosas desde 1983
- Desarrollador principal del *Stevie Wonder Simulator* para Android
- *DevOps Tech Lead* en **OpenExO**

1.

Introducción

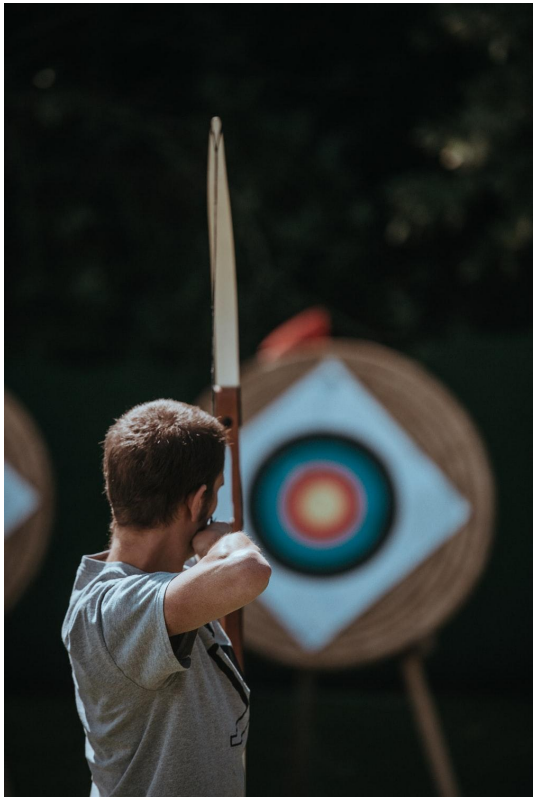
Conceptos principales en los que se basa este proyecto

El arte de la guerra está basado en el engaño

(Sun Tzu)

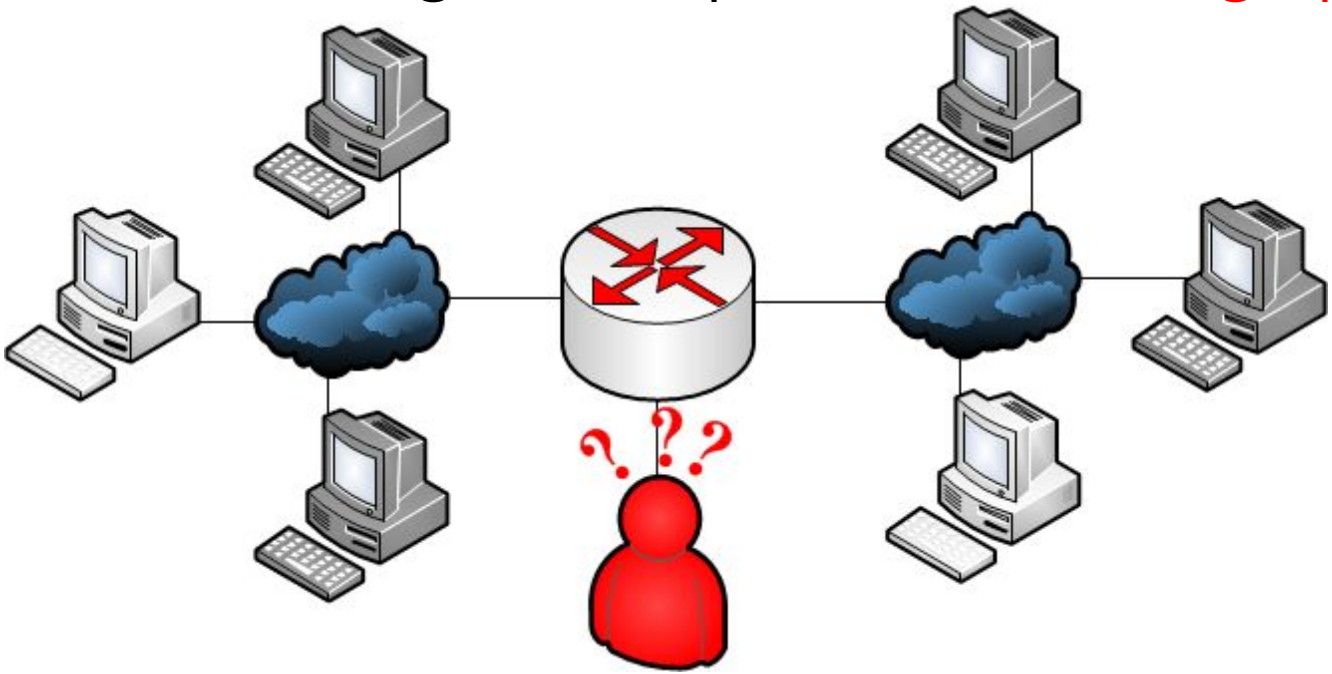
Moving Target Defense

Defensa por objetivo móvil



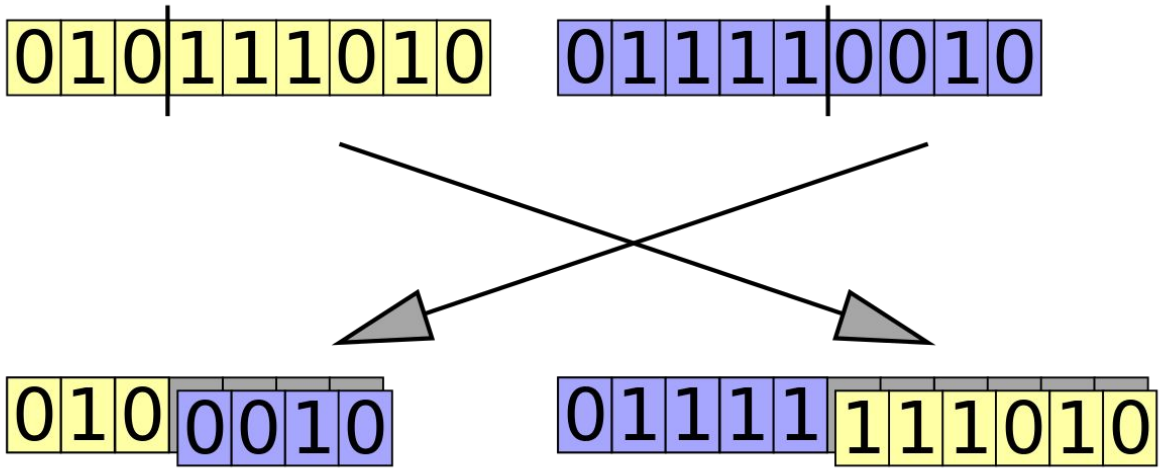
Moving Target Defense

Cambio de configuración para evitar el fingerprinting



Moving Target Defense

Configuración mediante un algoritmo genético



2.

Objetivos

Lo que deseamos alcanzar con este proyecto

Objetivos

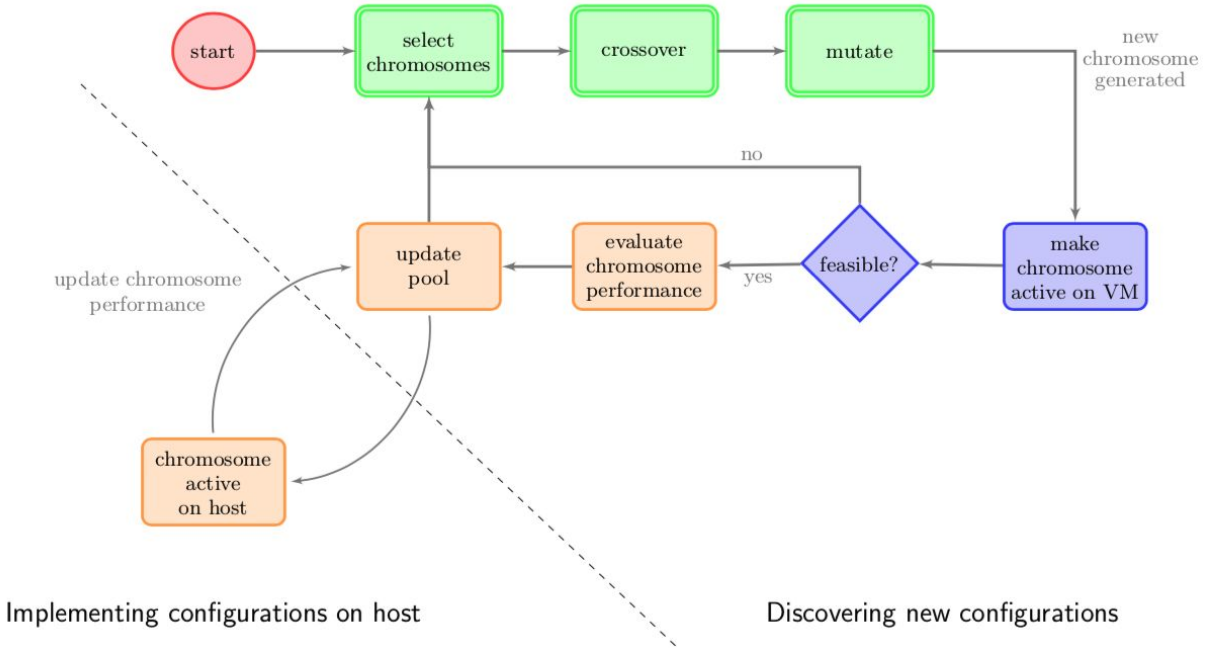
- **OBJ-1.** Prevenir ataques informáticos usando la técnica del **objetivo móvil**
- **OBJ-2.** Generar las configuraciones necesarias mediante **algoritmos genéticos**.

3.

Antecedentes

Estado del arte previo sobre esta temática

Implementaciones teóricas



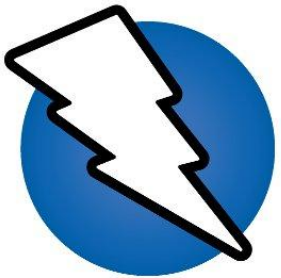
D. John, R. Smith, W. Turkett, D. Cañas & E. Fulp, **«Evolutionary Based Moving Target Cyber Defense»**, in *Proceedings of the Companion Publication of the 2014 Annual Conference on Genetic and Evolutionary Computation*

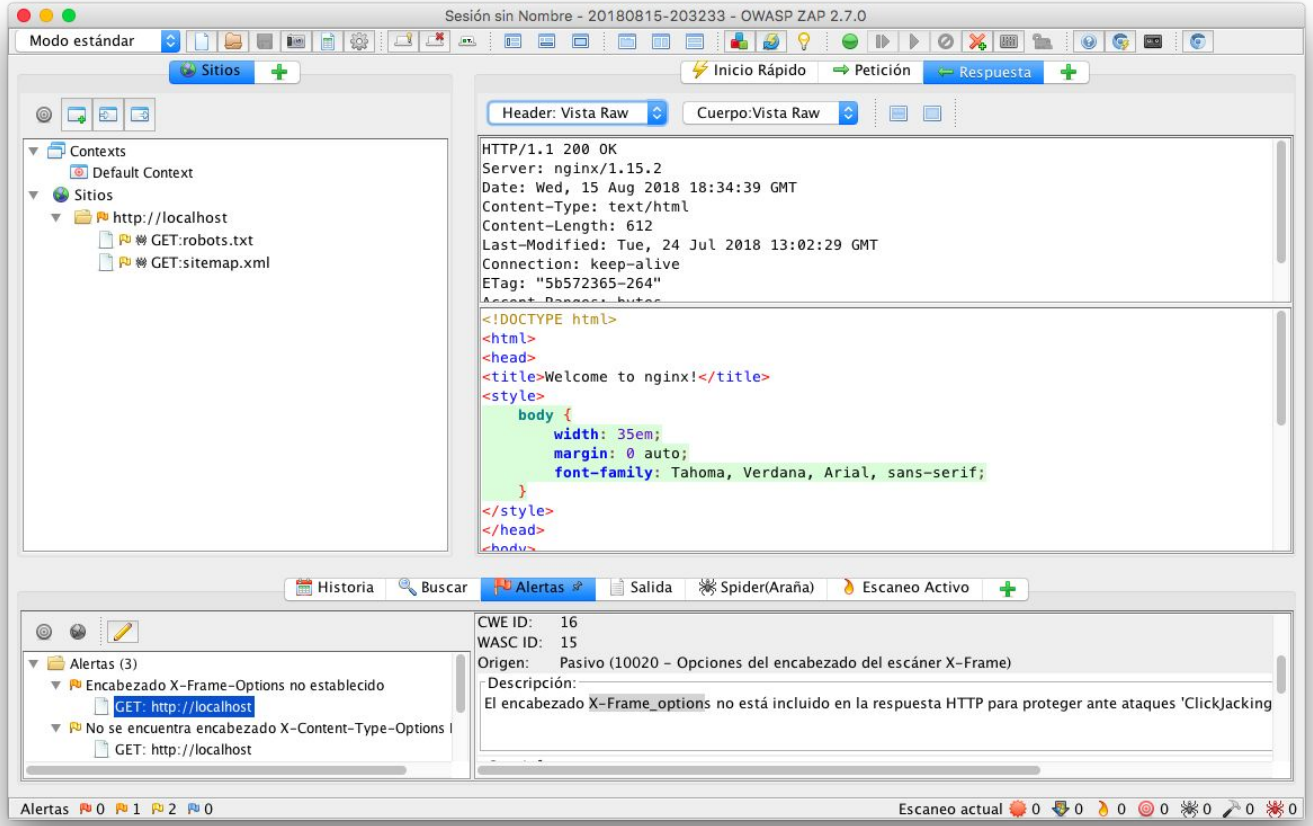
4.

Metodología

Qué hemos utilizado para alcanzar los objetivos

Tecnologías utilizadas (I)



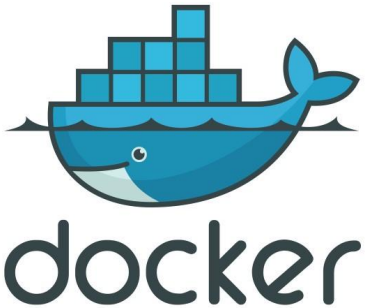

Sesión sin Nombre - 20180815-203233 - OWASP ZAP 2.7.0
Modo estándar
Sitios
Inicio Rápido
Petición
Respuesta
Header: Vista Raw
Cuerpo:Vista Raw
Contexts
Default Context
Sitios
http://localhost
GET:robots.txt
GET:sitemap.xml
HTTP/1.1 200 OK
Server: nginx/1.15.2
Date: Wed, 15 Aug 2018 18:34:39 GMT
Content-Type: text/html
Content-Length: 612
Last-Modified: Tue, 24 Jul 2018 13:02:29 GMT
Connection: keep-alive
ETag: "5b572365-264"
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
body {
width: 35em;
margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif;
}
</style>
</head>
Historia
Buscar
Alertas
Salida
Spider(Araña)
Escaneo Activo
Alertas (3)
Encabezado X-Frame-Options no establecido
GET: http://localhost
No se encuentra encabezado X-Content-Type-Options
GET: http://localhost
CWE ID: 16
WASC ID: 15
Origen: Pasivo (10020 - Opciones del encabezado del escáner X-Frame)
Descripción:
El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking
Alertas 0 1 2 0
Escaneo actual 0 0 0 0 0 0 0

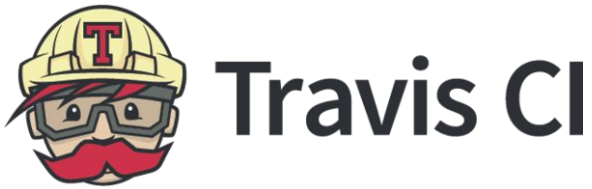
OWASP ZAP

Directivas de NGINX

Valores que modificaremos en la configuración

Id	STIG ID	Configuración Apache	Equivalente NGINX
0	V-13730	MaxClients	worker_connections
1	V-13726	KeepAliveTimeout	keepalive_timeout
2	V-13732	FollowSymLinks	disable_symlinks
3	V-13735	Indexes	autoindex
4	V-13724	Timeout	send_timeout
5	V-13738	LimitRequestFieldsize	large_client_header_buffers
6	V-13736	LimitRequestBody	client_max_body_size
7	V-6724	ServerTokens	server_tokens
8			gzip

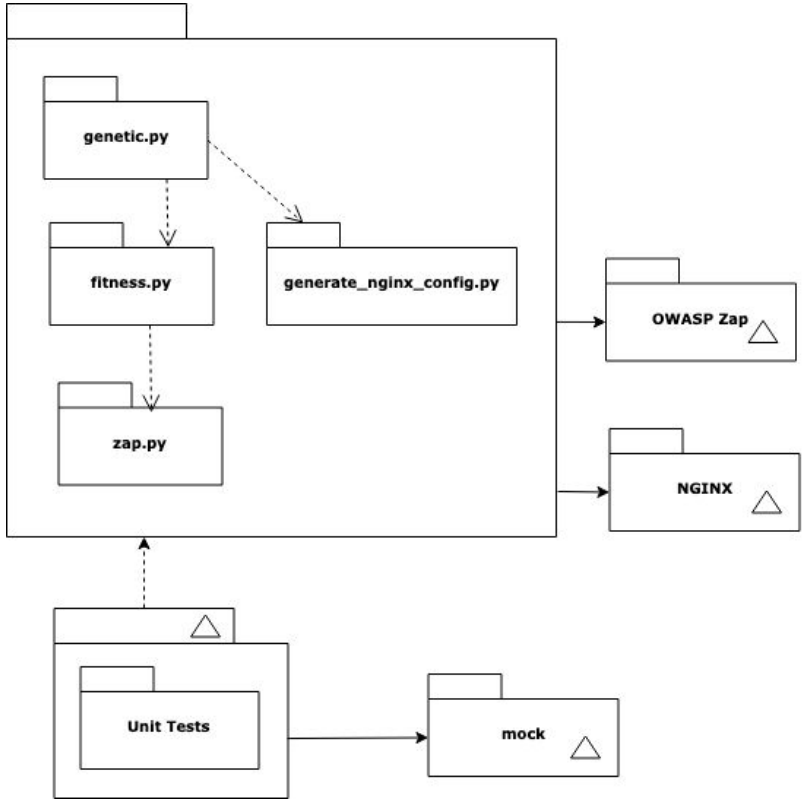




Tecnologías utilizadas (II)

Diagrama de paquetes

Cómo se interrelacionan los componentes de la aplicación



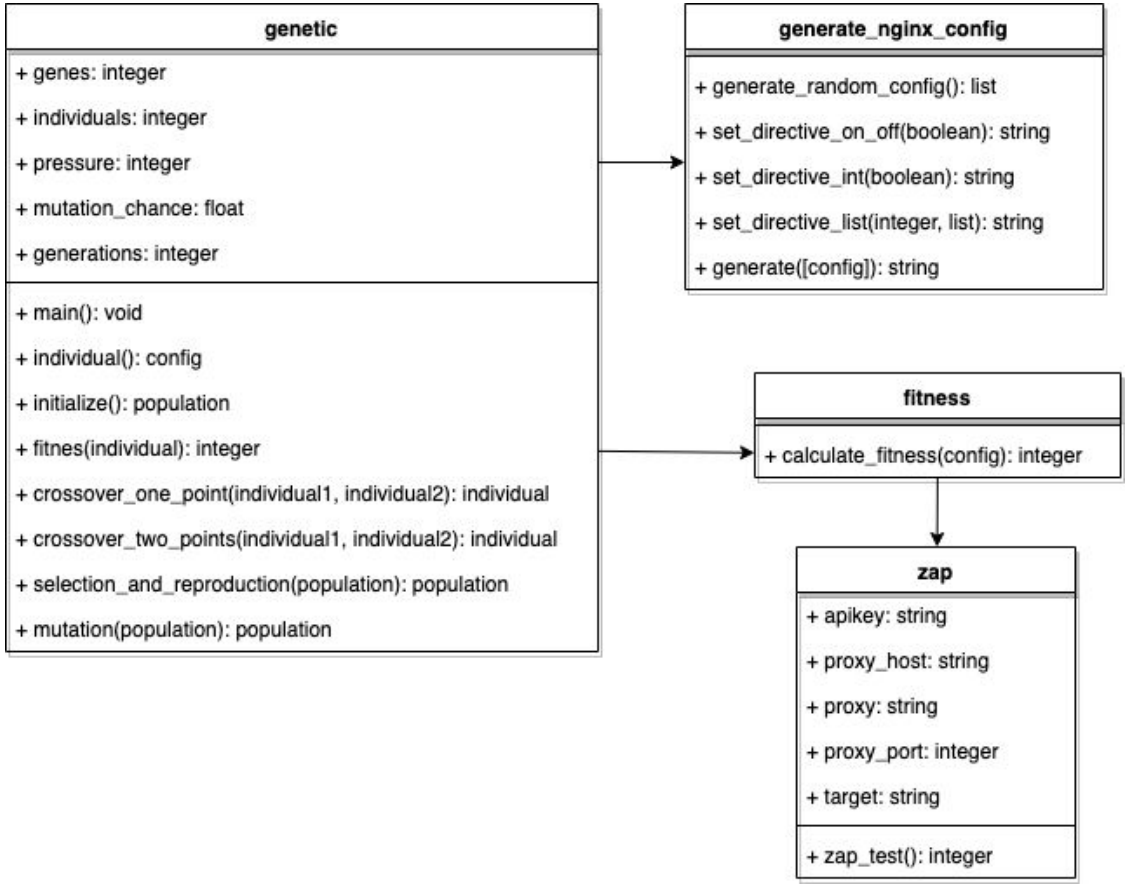
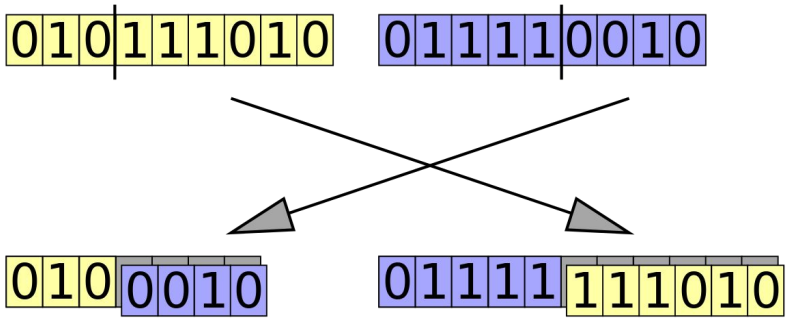


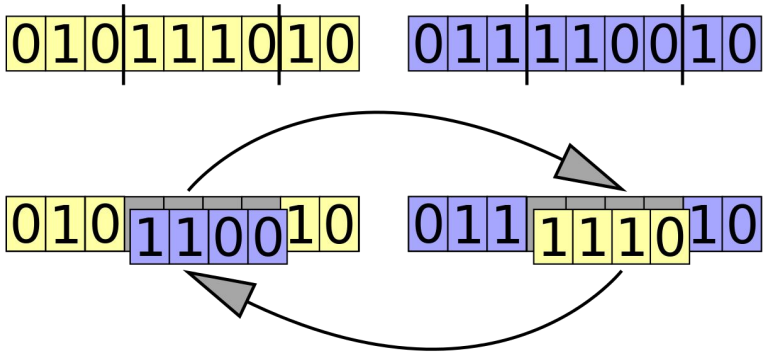
Diagrama de clases

Descripción detallada del programa

Funciones de cruzamiento

¿Cuál es más eficiente?





5.

Resultados

Resultados obtenidos

Población inicial de 10 individuos durante 5 generaciones

1	2	3	4	5	6	7	8	9	10	11	12	13
2008	57	1	1	0	1008	1736	1	0	2	3	0	0
2036	115	1	1	0	715	1646	0	0	0	3	0	2
806	10	0	0	1	763	1061	0	1	0	0	1	2
1184	19	0	0	0	687	1944	0	0	0	3	1	2
1244	100	0	0	1	1930	1088	0	0	0	1	0	2
1498	46	0	1	0	819	1391	0	0	1	1	0	2
2037	120	1	1	1	1137	1059	1	0	2	2	0	1
1171	118	0	0	1	1564	569	0	1	1	4	1	2
714	120	1	0	0	1282	1579	0	1	2	1	1	2
1710	87	0	0	0	654	529	0	0	2	1	1	2

Población final de 10 individuos durante 5 generaciones

1	2	3	4	5	6	7	8	9	10	11	12	13
714	120	0	0	0	687	1944	1	1	2	1	1	2
714	43	0	0	0	1282	1944	0	0	2	1	1	0
714	43	0	0	0	1282	1944	1	0	2	1	1	2
714	120	0	0	0	1282	1579	0	1	1	1	1	0
714	120	0	0	0	687	1579	1	1	2	1	1	2
714	120	0	0	0	1282	1579	0	1	2	1	1	0
714	120	0	0	0	687	1944	1	1	2	1	1	2
714	43	0	0	0	1282	1579	0	0	2	1	1	2
714	120	1	0	1	687	1944	1	0	2	1	1	2
714	120	0	0	0	1282	1579	0	1	2	1	1	2

6.

Conclusiones

Conclusiones sobre el proyecto

Conclusiones

- Se ha conseguido mejorar la seguridad.
- El algoritmo consigue generar y evolucionar configuraciones.
- El cruce en dos puntos es más eficiente.
- Un algoritmo genético quizá no sea lo más óptimo.
- Hay que balancear entre diversidad y seguridad.

¡Gracias!

¿Alguna pregunta?

Podéis encontrar el código en:

https://github.com/erseco/ugr_moving_target_defense