sedian

Seguridad Digital
de Andalucía

Técnicas de equipo Blue Team para realizar pruebas defensivas en una red y evitar ataques cibernéticos

Enrique Palacios Sánchez

Junta de Andalucía

¿Qué es un equipo Blue Team?

- Un equipo Blue Team está formado por profesionales de la seguridad que tienen una visión de la organización desde dentro hacia fuera. Su tarea es proteger los dispositivos críticos de la misma contra cualquier tipo de amenaza.

- Conocen los objetivos de negocio y de la estrategia de seguridad de la organización. Por lo tanto, su tarea es fortalecer los muros del castillo para que ningún intruso pueda comprometer las defensas.

Funciones de un equipo Blue Team

Las funciones del equipo azul son las siguientes:

- Recopila datos y documenta exactamente lo que hay que proteger y realiza una evaluación de riesgos.
- A continuación, refuerzan el acceso al sistema de muchas maneras, entre ellas, introduciendo políticas más estrictas en materia de contraseñas y educando al personal para que comprenda y se ajuste a los procedimientos de seguridad.
- A menudo se establecen instrumentos de vigilancia que permiten registrar la información relativa al acceso a los sistemas y comprobar si hay actividades inusuales.

Funciones de un equipo Blue Team

- Un equipo Blue Team tienen que establecer medidas de seguridad en torno a los dispositivos clave de una organización. Para ello, diseñan un plan defensivo identificando los dispositivos críticos, documentando la importancia de estos equipos para el negocio y el impacto que tendrá la ausencia de los mismos.

- A continuación, realizan evaluaciones de riesgo identificando las amenazas contra cada dispositivo y las debilidades que pueden explotar.

Herramientas de utilizan

- Según la ENS en su documento CCN-STIC-818 el listado de herramientas que podemos utilizar serían las siguientes:

Tipo de herramienta	Herramienta orientativa	Fabricante	Plataforma	Licenciamiento
Control y calidad en el desarrollo	Subversion	Apache Software Foundation	Multiplataforma	Gratuita
	Git	Software Freedom Conservancy, Inc. (Software libre)	Multiplataforma	Gratuita
	Rational ClearCase	IBM	Multiplataforma	Comercial
	Jenkins	Jenkins CI	Multiplataforma	Gratuita
Auditoría de código	Sonar	SonarSource	Multiplataforma	Gratuita
	Checkstyle	Software libre	Multiplataforma	Gratuita
	FindBugs	University of Maryland	Multiplataforma	Gratuita
Análisis y/o limpieza de metadatos	Libextractor	Gnu.org	Multiplataforma	Gratuita
	Doc Scrubber	Brightfort	Windows	Gratuita
	MetaStripper	PhotoThumb.com	Windows	Gratuita
	OOMetaExtractor	Informática64	Windows	Gratuita
	FOCA	Informática64	Windows	Gratuita y Comercial
	Metaviewer	Pinpoint Laboratories	Windows	Gratuita
	BatchPurifier	Digital Confidence	Windows	Comercial
Detección y prevención de intrusiones (HIDS)	OSSEC	Trend Micro, Inc.	Multiplataforma	Gratuita
	Tripwire	Tripwire, Inc.	Multiplataforma	Comercial
Limpieza de metadatos	MetaShield Protector	Informática64	Windows	Comercial
	MailValve GX	Digital Confidence	Windows	Comercial
	Metadact-e	Litéra	Windows	Comercial

Herramientas de utilizan

Tipo de herramienta	Herramienta orientativa	Fabricante	Plataforma	Licenciamiento
Cifrado	TrueCrypt	TrueCrypt Foundation	Multiplataforma	Gratuita
	GnuPG[2]	Free Software Foundation, Inc.	Multiplataforma	Gratuita
Captura, monitorización y análisis de tráfico	Snort	Sourcefire, Inc.	Multiplataforma	Gratuita
	Wireshark	Wireshark Foundation	Multiplataforma	Gratuita
Monitorización y análisis de logs	OSSIM	AlienVault	Linux	Gratuita y Comercial
	Bitacora	S21Sec	Linux	Comercial
	LogICA	Grupo ICA	Linux	Comercial
	iView	Cyberoam	Multiplataforma	Gratuita
	ArcSight	HP	Multiplataforma	Comercial
	NetIQ	Novell	Máquina virtual	Comercial
	QRadar	IBM	Appliance	Comercial
	NitroSecurity	McAfee	Appliance	Comercial
	LogLogic	LogLogic Inc.	Máquina virtual	Comercial
	Splunk	Splunk Inc.	Multiplataforma	Comercial
Análisis de código dañino	IOC Finder	Mandiant	Windows	Gratuita
	IOC Editor	Mandiant	Windows	Gratuita
	Redline	Mandiant	Windows	Gratuita
	IDA	Hex-Rays	Multiplataforma	Gratuita y Comercial
	OllyDbg	Oleh Yuschuk	Windows	Gratuita
	HijackThis	Trend Micro	Windows	Gratuita
	IceSword	pjf	Windows	Gratuita
	GMER	GMER	Windows	Gratuita
	Process Monitor	Microsoft (Sysinternals)	Windows	Gratuita
Gestión de incidencias	GLPI	Asociación Indepnet	Multiplataforma	Gratuita
	MantisBT	MantisBT Group	Multiplataforma	Gratuita

Herramientas de utilizan

Tipo de herramienta	Herramienta orientativa	Fabricante	Plataforma	Licenciamiento
	OTRS Help Desk	OTRS Inc.	Multiplataforma	Gratuita
	Redmine	Jean-Philippe Lang	Multiplataforma	Gratuita
	Request Tracker	Best Practical Solutions LLC.	Linux	Gratuita
	Request Tracker for Incident Response	Best Practical Solutions LLC.	Linux	Gratuita
	Jira	Atlassian	Multiplataforma	Comercial

Herramientas que utilizan

Otras herramientas que se utilizan:

- Nmap, que permite recopilación de información y búsqueda de vulnerabilidades de equipos en red, a través de los puertos y servicios disponibles.
- Metasploit, que proporciona información sobre vulnerabilidades, o exploits, y permite hacer pruebas de explotación usando payloads o código de explotación.
- OpenVAS, que se utiliza para la evaluación de vulnerabilidades a través de red, utilizando diferentes herramientas integradas.
- ExploitDB, que consiste en un directorio web de vulnerabilidades publicadas por diferentes hackers, y los exploits asociados a estas.
- CVE, que es un listado de vulnerabilidades y exposiciones comunes de seguridad informática que se encuentra publicado en la web.

Tipos de medidas de seguridad

Las medidas de seguridad que se pueden utilizar por parte de un equipo Blue Team son:

- Realizar auditorías del DNS (servidor de nombres de dominio) para prevenir ataques de phishing, evitar problemas de DNS caducados, evitar el tiempo de inactividad por la eliminación de registros del DNS y prevenir/reducir los ataques al DNS y a la web.
- Realizar análisis de los certificados digitales para rastrear la actividad de los usuarios e identificar cualquier firma conocida que pueda indicar una violación de la seguridad.
- Instalar software de seguridad en dispositivos como computadoras, portátiles y smartphones.
- Garantizar que los controles de acceso al cortafuegos estén correctamente configurados y que el software antivirus se mantenga actualizado.

Tipos de medidas de seguridad

- Desplegar software IDS e IPS como control de seguridad de detección y prevención.
- Implementar soluciones SIEM para registrar y controlar la actividad de la red.
- Analizar los registros y la memoria para recoger la actividad inusual en el sistema e identificar y localizar un ataque.
- Segmentar las redes y asegurarse de que están configuradas correctamente.
- Usar regularmente software de exploración de vulnerabilidades.
- Asegurar los sistemas mediante el uso de software antivirus o antimalware.
- Integrar la seguridad en los procesos.

Evaluaciones de riesgo

- Al evaluar los riesgos y priorizarlos, el equipo azul desarrolla un plan de acción para implementar controles que pueden reducir el impacto o la probabilidad de que las amenazas se materialicen contra los dispositivos de nuestra red.

- La participación del personal directivo es importante en esta etapa, ya que sólo él puede decidir aceptar un riesgo o aplicar controles de mitigación contra el mismo. La selección de los controles suele basarse en un análisis de costos y beneficios para garantizar que los controles de seguridad aporten el máximo valor a la empresa.

Evaluaciones de riesgo

- Por ejemplo, un equipo azul puede identificar que la red de la empresa es vulnerable a un ataque de DDoS (denegación de servicio distribuido). Este ataque reduce la disponibilidad de la red para los usuarios legítimos al enviar solicitudes de tráfico incompletas a un servidor. Cada una de estas solicitudes requiere recursos para realizar una acción, por lo que el ataque paraliza gravemente la red.

- El equipo calcula entonces la pérdida en caso de que se produzca la amenaza. Basándose en el análisis de costo-beneficio y alineándose con los objetivos de negocio, un equipo azul consideraría la instalación de un sistema de detección y prevención de intrusos para minimizar el riesgo de ataques DDoS.

Comprobaciones periódicas

A menudo se establecen instrumentos de vigilancia que permiten registrar la información relativa al acceso a los sistemas y comprobar si hay actividades inusuales. Los equipos azules realizarán comprobaciones periódicas del sistema que pueden ser las siguientes:

- Auditorías del sistema de nombres de dominio (DNS).
- Exploraciones de vulnerabilidades de la red interna o externa.
- Captura de paquetes de tráfico de la red para su análisis.

Herramientas de Seguridad
DEMOSTRACIONES

sedian Seguridad Digital de Andalucía