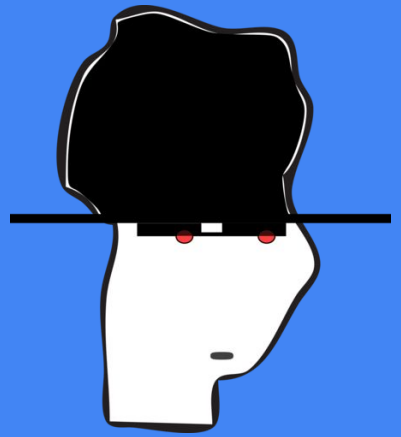
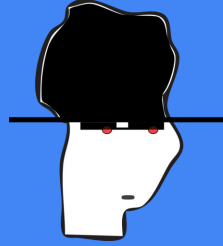
Pentesting

Seguridad Ofensiva



Introducción a las pruebas de intrusión

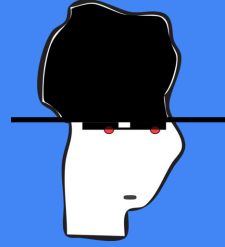


Definición
Llamaremos Pentest / Test de intrusión al proceso llevado a cabo dentro de la vida de un sistema, en el cual se procede a planificar, analizar y verificar distintas características involucradas con la seguridad del mismo.

Objetivos
Todo esto con el objetivo de analizar el nivel de seguridad y la exposición de los sistemas ante posibles ataques. (Encontrar y corregir vulnerabilidades)

Propiedades de interés:
Integridad, confidencialidad, disponibilidad, control, etc.

Potencial Caso… medianamente moderno



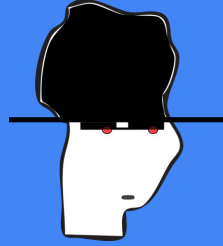
```
$ sudo apt-get update
$ sudo apt-get install docker-ce docker-ce-cli containerd.io
```

```
sudo usermod -aG docker your-user
```

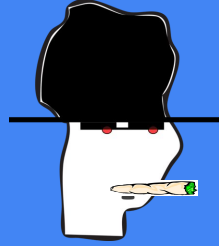
```
joe@zoidberg:~/Seg$ docker run -v /:/hostOS -it chrisfosterelli/rootplease

You should now have a root shell on the host OS
Press Ctrl-D to exit the docker instance / shell
# 
```

Mitigaciones



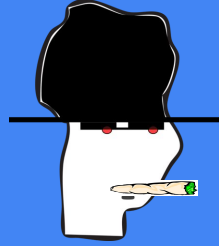
Mitigaciones de seguridad (scanning)



¿Como nos/los prevenimos?

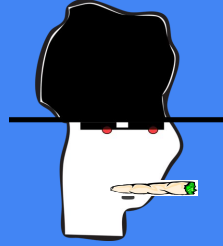
- Tuning & Hardening configurations
- Firewalls (iptables, ufw, pfsense, wafs… a lot)
- Honeypots (Tripwire, ManTrap)
- IDS (scanlogd, psad, suricata, sagan?)
- IPS (portsentry, snort, EndPoint Protection)

Hardening



- A nivel Sistema Operativo. (15 steps)
- A nivel físico (example)
- A nivel motor web. (nginx,).
- A nivel cloud (US Sec Baseline)
- A nivel de permisos de acceso (ej)
- etc

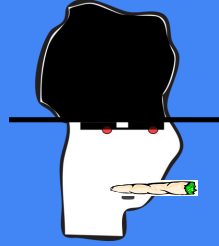
Firewalls



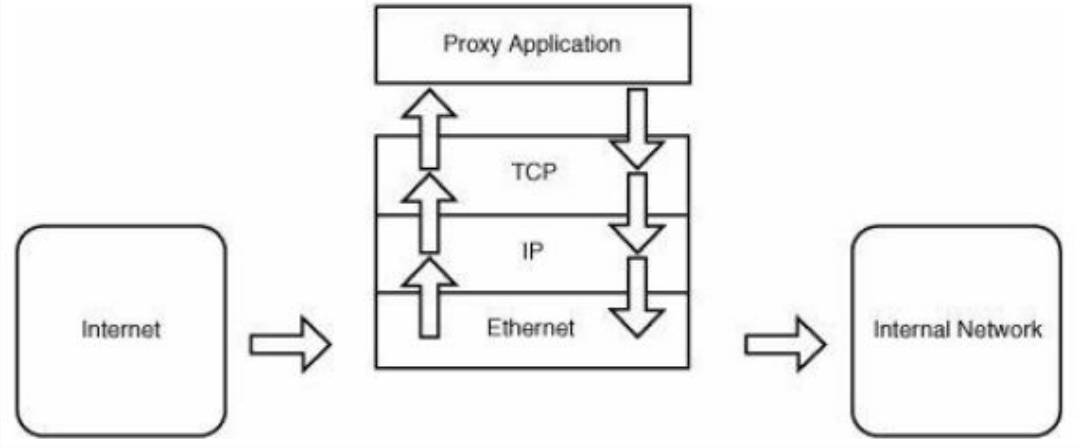
- El propósito básico de un firewall es servir como un punto de comunicación “obligatorio” entre dos conjuntos de computadoras en red.
- Los administradores de red pueden definir una política de seguridad de firewall que se aplica a todo el tráfico que intenta pasar por ese punto de estrangulamiento.

1. Host 1.2.3.4 can talk to 5.5.5.5.
2. The user Jim on the host 1.2.3.10 can talk to 5.5.5.6.
3. Any host can connect to host 5.5.5.4 over TCP port 80.
4. Hosts on the 5.5.5.0/24 network can talk to any host.
5. UDP packets from host 1.2.3.15 source port 53 can go to host 5.5.5.5 port 53.
6. All other traffic is denied.

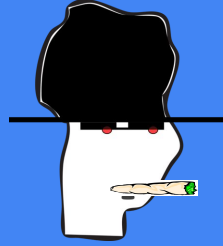
Firewalls



- Un servidor firewall para incrementar la seguridad utiliza la pila TCP / IP completa de la máquina del servidor de seguridad como parte de la cadena de procesamiento.



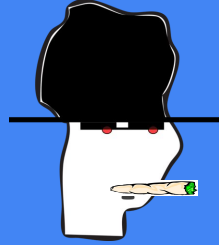
WAF (ejemplo)

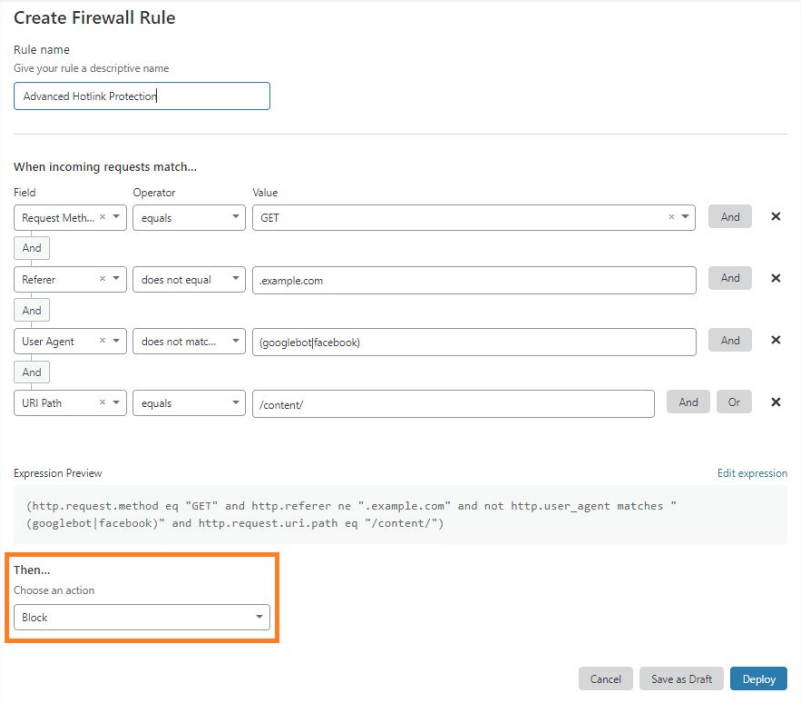


Son aplicaciones web que permiten registrar, establecer reglas y analizar las peticiones entrantes.
Basado en el comportamiento de las peticiones analizadas, permiten tomar acciones como:

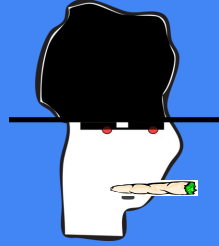
- log
- allow
- block
- challenge (captcha)
- challenge (js)

WAF (ejemplo)




Create Firewall Rule
Rule name
Give your rule a descriptive name
Advanced Hotlink Protection
When incoming requests match...
Field
Operator
Value
Request Meth...
equals
GET
And
Referer
does not equal
.example.com
User Agent
does not matc...
(googlebot|facebook)
URI Path
equals
/content/
Or
Expression Preview
Edit expression
(http.request.method eq "GET" and http.referer ne ".example.com" and not http.user_agent matches "(googlebot|facebook)" and http.request.uri.path eq "/content/")
Then...
Choose an action
Block
Cancel
Save as Draft
Deploy

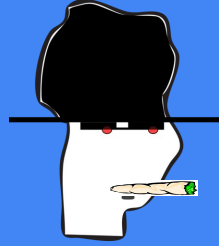
WAF (ejemplo)



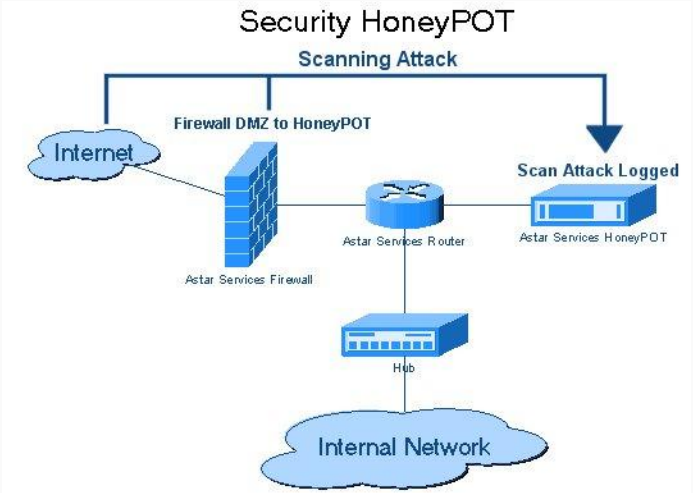
Date	Action taken	Country	IP address	Service
06 Oct, 2020 13:40:22	Block	Argentina	[redacted]8	WAF

Ray ID	5de0d2e24f9808e5	**Service**	WAF
Method	GET	**Rule ID**	100173
HTTP Version	HTTP/2	**Rule message**	XSS, HTML Injection - Script Tag
Host	[redacted]w.for[redacted]com	**Rule group**	Cloudflare Specials
Path	/search_data.json	**Action taken**	Block
Query string	?q=%253Cscript%253Ealert(1)%253C%2Fscript%253E&search_mode=autocomplete&size=3	**Bot score**	74
		Bot source	Machine Learning
User agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:80.0) Gecko/20100101 Firefox/80.0		Export event JSON
IP address	[redacted]3		
ASN	AS10318 Telecom Argentina S.A.		
Country	Argentina		

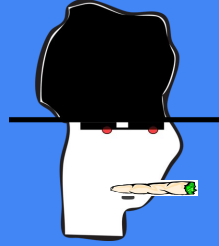
HoneyPots



- Son servidores aislados que recopilan información sobre atacantes e intrusos del sistema(Fuertemente monitoreados).
- Aprenden como estos intentan obtener acceso en nuestros sistemas. Reúnen información a nivel forense.



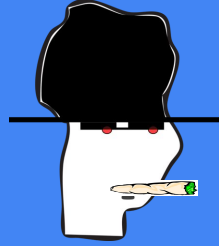
IDS & IPS

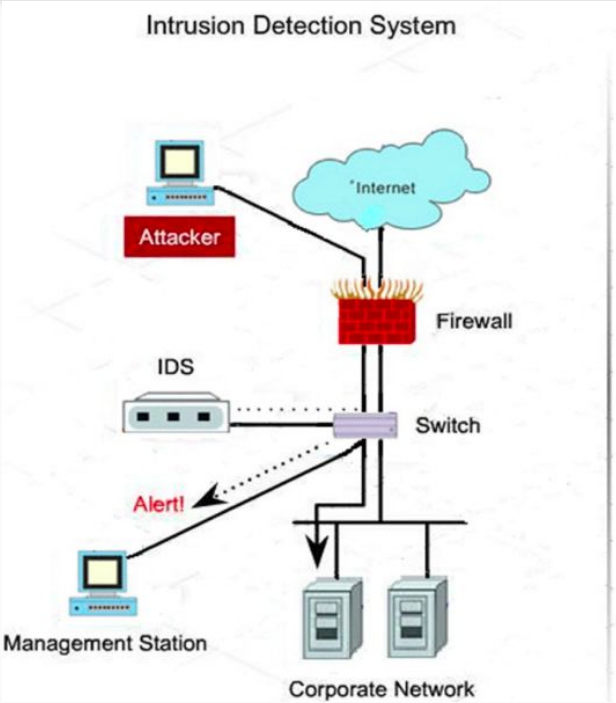


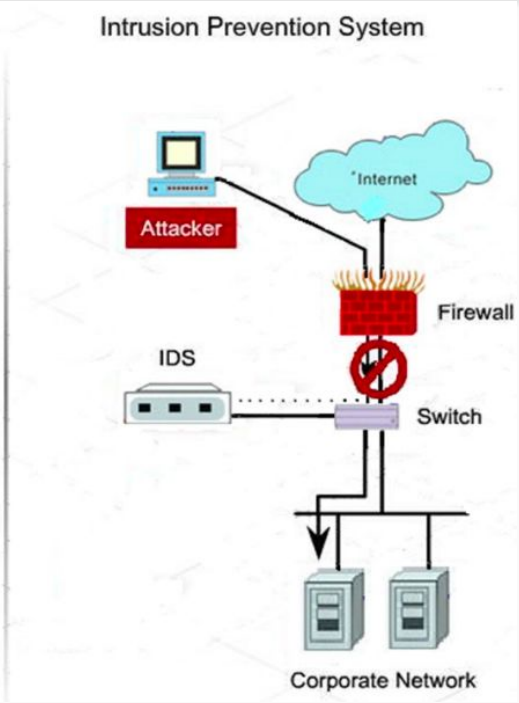
Es software (o hardware) que monitorea la red y/o los sistemas en busca de anomalías en los sistemas y en la política de de seguridad de una red reportando todo lo necesario. En el caso de los IPS, tienen el poder de tomar acciones en consecuencia, poner filtros, reglas de ruteo, etc.

Cons: Usan recursos, la efectividad se reduce con el ruido, falsas alarmas, paquetes encriptados.

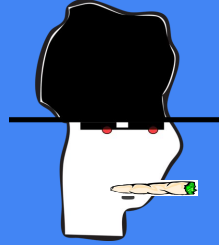
IDS & IPS




Intrusion Detection System
Internet
Attacker
Firewall
IDS
Switch
Alert!
Management Station
Corporate Network


Intrusion Prevention System
Internet
Attacker
Firewall
IDS
Switch
Corporate Network

IDS & IPS

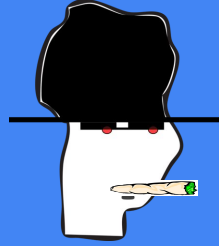


Es software (o hardware) que monitorea la red y/o los sistemas en busca de anomalías en los sistemas y en la política de de seguridad de una red reportando todo lo necesario. En el caso de los IPS, tienen el poder de tomar acciones en consecuencia, poner filtros, reglas de ruteo, etc.

```
:Oct  4 12:08:25  scanlogd: 71.6.167.124 to 143.0.100.198 ports 4321, 9051, 143, 1
:Oct  4 13:21:19  scanlogd: More possible port scans follow
:Oct  1 20:47:39  scanlogd: 195.54.167.89:42624 to 143.0.100.198 ports 376, 358, 3
:Oct  1 21:25:09  scanlogd: 80.82.78.20:58300 to 143.0.100.198 ports 11076, 11094,
:Oct  1 21:27:12  scanlogd: 194.26.25.126:45781 to 143.0.100.198 ports 40053, 5200
:Oct  1 22:04:06  scanlogd: 80.82.70.25:58894 to 143.0.100.198 ports 1927, 1972, 1

:Oct  1 22:28:52  scanlogd: 94.102.49.106:58879 to 143.0.100.198 ports 1681, 1698,
:Oct  1 22:40:00  scanlogd: More possible port scans follow
:Sep 29 08:19:51  scanlogd: 2.56.176.186 to 143.0.100.198 ports 1000, 2010, 8033,
:Sep 29 10:30:52  scanlogd: 2.56.176.186 to 143.0.100.198 ports 4444, 40098, 6160,
:Sep 29 12:04:33  scanlogd: 124.92.127.102:6000 to 143.0.100.198 ports 9433, 1500,
:Sep 29 12:47:05  scanlogd: 2.56.176.186 to 143.0.100.198 ports 3780, 30002, 1443,
:Sep 29 12:54:12  scanlogd: 3.80.166.95:54850 to 143.0.100.198 ports 50003, 92, 25
```

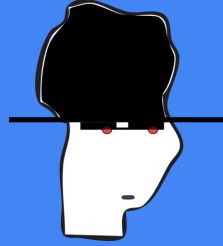
Mitigaciones para la explotación



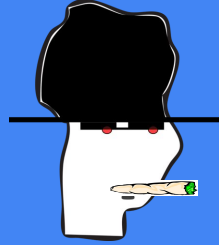
Corregir las vuln

Incorporar controles, políticas y pruebas de seguridad lo más temprano posible es la mejor prevención, pero no siempre es suficiente.

Cosas de Teams



Red Teams



El red teaming es el proceso de “emular” una amenaza del mundo real con la finalidad de **entrenar y medir** la efectividad de las **personas, procesos y tecnologías** utilizadas para defender su entorno

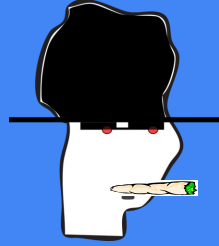
-

Joe Vest & James Tubberville

Red Team Development and Operations: A practical guide

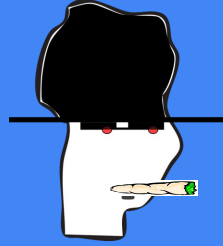
.

Red Teams



Penetration Test	Ejercicio de red team
Esfuerzo especifico	Esfuerzos regulares, métodicos y repetibles
Acotado en tiempo	Mantenido en el tiempo
Usualmente realizado externamente (mirada independiente - poco conocimiento interno)	Puede ser realizado por personal interno (mayor conocimiento interno - Insider)
Alcance limitado	Alcance definido de acuerdo a las necesidades
Focalizado en el costo beneficio.	Focalizado en la mejora y la remediación.
Basado en la capacidad de explotación de vulnerabilidades	Basado en amenazas y TTPs

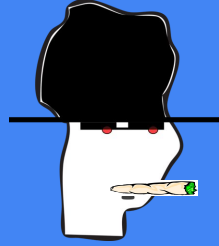
Red Teams



El enfoque RT modela y ejecuta escenarios que permitan evaluar:

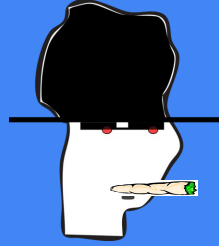
- Las técnicas de “**defensa**” con las que cuenta una entidad. (Firewalls, Antivirus, EDR, IDS/IPS, DLP, SIEM)
- El **monitoreo** con el que cuenta la compa~nia.
- Los mecanismos de **respuesta** a incidentes
- Capacidad de **recuperacion** frente a incidentes.
- Mejorar la eficiencia basada en los tiempos de deteccion (**ttd**) y de mitigacion (**ttm**)

Red Teams - fases



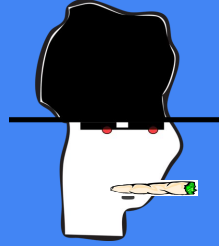
- Reconocimiento
- Compromiso
- Persistencia
- Command and Control
- Escalar privilegios
- Pivoting
- Reporte y limpieza

Blue Teams



- Equipos de seguridad defensiva
- Administradores de capas de seguridad
- Identificación de Intrusiones
- Ejecución de Respuesta a Incidentes
- Análisis de Malware
- Forensia Digital

Blue Teams

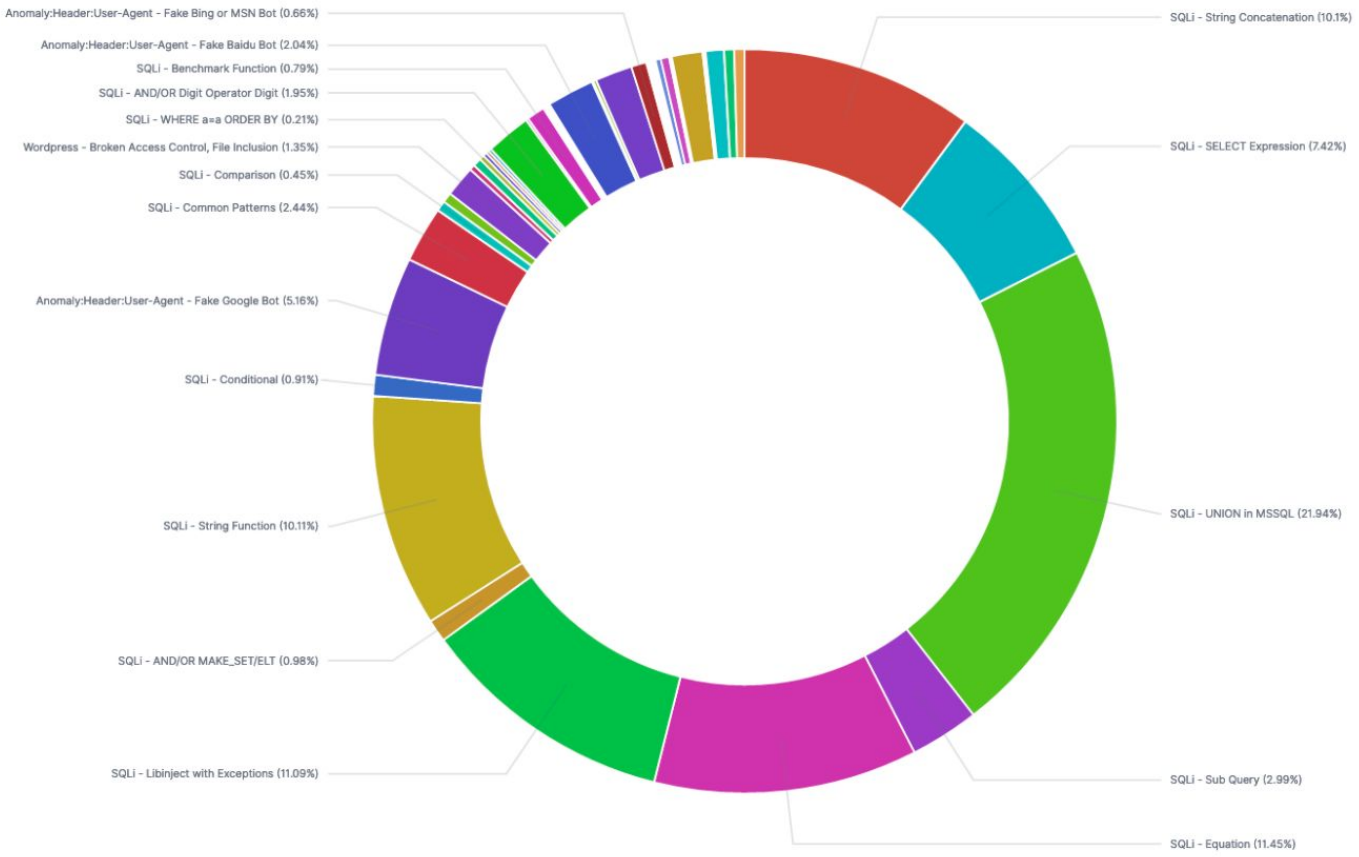


- Firewalls
- SIEM’s
- IDS/IPS
- Incident Response Tools

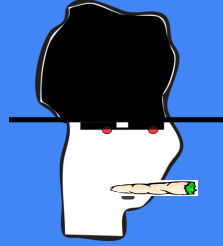
- Kibana
- Moloch
- Suricata
- Scanlogd
- PortSentry

https://www.blueteamvillage.org/meet-a-mentor/

FirewallMatchesActions: drop × ClientRequestHost is one of www.[redacted]om, imag[redacted]com × NOT WAFRuleMessage: × + Add filter



DevSecOps

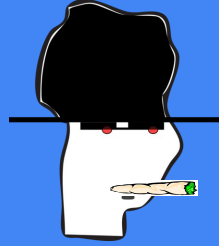


Implica pensar desde el principio en la seguridad de las aplicaciones y de la infraestructura.

También implica automatizar algunas puertas de seguridad para impedir que se ralentice el flujo de trabajo de DevOps.

El término DevSecOps no se refiere a un perímetro de seguridad que rodea las aplicaciones y los datos, sino a la seguridad integrada.

DevSecOps



Se recomienda mantener ciclos de desarrollo cortos y frecuentes, integrar medidas de seguridad con una interrupción mínima de las operaciones, mantenerse al día con las tecnologías innovadoras (como los contenedores y los microservicios) y, al mismo tiempo, fomentar una colaboración más estrecha entre los equipos que suelen estar aislados, lo cual es una tarea difícil para cualquier empresa.

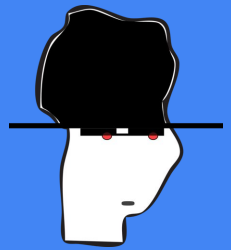
Purple Teams

Cuando los red teamers comparten y muestran a los blue teamers como evitar o burlar ciertos controles, y viceversa, ambos equipos incrementan su capacidad y son llamados purple teams.

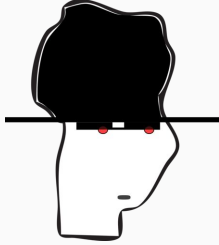
Este constante intercambio de conocimiento, incrementa la resiliencia de las aplicaciones

"Firewalls are barriers between 'us' and 'them' for arbitrary values of 'them'."

- Steve Bellovin -



Lo que estábamos esperando



X.X

xxxxxxx