

ÍNDICE

PREFACIO	XIX
CAPÍTULO 1. INTRODUCCIÓN A LA SEGURIDAD EN DOCKER	1
Introducción a los contenedores Docker.....	1
Comparativa Máquina Virtual vs Contenedor	3
Docker Engine	5
Arquitectura Docker Engine.....	7
Aislamiento de Docker	8
Seguridad del kernel.....	8
Principios de la seguridad en Docker.....	9
Seguridad flexible	9
Limitar recursos y la exposición de información.....	9
Filtrado del tráfico	9

Namespaces (espacios de nombres).....	10
Grupos de control (cgroups)	11
El daemon Docker y comandos docker	13
Capacidades (Linux capabilities)	16
Uso de capabilities de control de red	24
Listado de capacidades.....	25
Deshabilitar el ping de un contenedor	25
Contenedores privilegiados	26
Vectores de ataque en Docker	29
Seguridad intrínseca del kernel.....	29
El daemon Docker	29
Problemas en la configuración del contenedor	30
CAPÍTULO 2. SEGURIDAD EN CONTENEDORES E IMÁGENES DOCKER	31
Conceptos de imagen y contenedor.....	31
Capas en Docker	33
DockerFile.....	34
La instrucción FROM	36
La instrucción RUN.....	36
Tratamiento de la caché en Docker	37
Las instrucciones CMD y Entrypoint.....	40
Construir nuestra aplicación con NodeJS.....	41
Reducir el tamaño de la imagen con multistage	42

Reducir el tamaño de la imagen con Alpine Linux y Distroless	43
Optimizando el dockerfile y buenas prácticas	47
Inspección de contenedores	49
Buscar y ejecutar una imagen Docker	52
Ingeniería inversa de un dockerfile	54
Visualización de dependencias entre capas	56
Docker Content Trust	58
Mecanismo de firma de imágenes	60
Procedencia de la imagen	61
Descarga segura en dockerfile	62
Notary como herramienta para administrar imágenes.....	64
Distribución de imágenes en Docker Hub	65
Docker Registry	66
Comprobar imágenes actualizadas.....	72
Docker Hub vs Docker Engine.....	74
Construcción de imágenes de forma automatizada	76
Superficie de ataque del daemon docker	81
Mejores prácticas de seguridad	82
Deshabilitar los permisos de SETUID	84
Mínimos privilegios e imágenes de solo lectura	85
Actualizar el Kernel del Docker host	87
Limitar llamadas del sistema.....	87

Privilegios de Docker	87
Verificar las imágenes	88
Conectando contenedores usando Docker Compose.....	88
Casos de uso de Docker compose	89
Instalación y comandos de Docker compose	90
Servicios en Docker compose	94
Configurar variables de entorno en Docker compose.....	96
Variables de entorno y paso de parámetros	96
Exposición de puertos y comunicación de contenedores.....	98
Usar puertos para conectar el contenedor con el host.....	100
Mapeo de puertos en servidor nginx	101
Ejemplos prácticos de exposición de puertos	103
Control de recursos en contenedores Docker	106
Configurar el recurso compartido de CPU	107
Limitar el número de núcleos de un contenedor	109
Establecer límite de memoria	111
Ejemplos prácticos con contenedores Python.....	113
Ejecutando un servidor web con python	113
Ejecutando un contenedor de Python interactivo	114
Ejecutando comandos con Python memcached	117
Inyectando procesos en contenedores con el comando Docker exec	120
Eliminar contenedores	122

Eliminar contenedores en ejecución.....	122
Eliminar contenedores detenidos.....	122
CAPÍTULO 3. SEGURIDAD EN EL DOCKER HOST	123
Introducción	123
Securizando el Docker Daemon.....	123
Securizando el kernel de Linux	124
SELinux	125
Apparmor y Seccomp	126
Instalar apparmor en distribuciones ubuntu	128
Práctica con apparmor.....	130
Perfil docker-default de apparmor	130
Ejecutar contenedor sin perfil apparmor.....	131
Defensa en profundidad	132
Ejecutar contenedor con perfil seccomp	133
Escalado de privilegios en el socket de Docker	135
Reducir la superficie de ataque del contenedor.....	139
Docker Bench Security.....	140
Ejemplos de ejecución con Docker Bench Security.....	147
Código fuente de Docker Bench Security.....	151
Actuary como herramienta de auditoría	155
Lynis.....	156
Auditando el Docker host con Lynis.....	157

Auditando un Dockerfile	162
Código fuente de lynis	163
Dockscan como herramienta de análisis de contenedores	165
Docker Explorer	169
Alternativa al comando Docker History.....	171
CAPÍTULO 4. SEGURIDAD EN IMÁGENES DOCKER	173
Introducción	173
Docker Security Scanning	173
Arquitectura de Docker Security Scanning.....	174
El proceso de escaneo de seguridad en Docker.....	175
Docker y vulnerabilidades CVE.....	177
El ciclo de vida del software con Docker	181
Herramientas de integración continua (CI)	181
Jenkins	182
Travis CI.....	184
Flujo de integración continua con Docker	185
Herramientas open source para análisis de vulnerabilidades	188
CoreOS Clair Scanner	188
Base de datos Clair CVE	189
Repositorios github y enlaces coreos clair.....	196
Repositorio de imágenes Quay.io	196
Registrarse en quay.io	197

Subir una imagen al repositorio de quay.io.....	199
Crear un repositorio en quay.io.....	200
Crear un repositorio en línea de comandos	200
Descargar una imagen de quay.io	201
Etiquetar el contenedor a una imagen.....	201
Trabajando con etiquetas de un repositorio	201
Escaneo de seguridad.....	203
Habilitar content trust.....	206
Anchore y Anchore Navigator	207
Instalar y ejecutar Anchore	210
Ejecutar Anchore con docker compose.....	214
Analizando las imágenes con anchore-cli.....	215
Consultas en imágenes con Anchore.....	215
Anchore como escáner de vulnerabilidades.....	218
Integración de Jenkins con Anchore.....	219
Anchore Navigator	220
Dagda	223
Owasp Dependency Check.....	227
Microscanner.....	231
Soluciones comerciales	233
Tenable.io Container Security.....	233
Twistlock	237

Protección en tiempo de ejecución	239
Gestión de vulnerabilidades	239
Integración continua	239
Imágenes de confianza	240
Recursos y artículos twistlock.....	240
Black Duck.....	240
Aquasec.....	242
NeuVector	243
Seguridad inteligente en contenedores	245
StaxRox	247
Sysdig Secure	248
Interfaces de usuario para administrar Docker	249
Gestionar vulnerabilidades en imágenes Docker	254
CAPÍTULO 5. MONITORIZACIÓN EN CONTENEDORES DOCKER	257
Introducción a la monitorización en Docker.....	257
Visualización de registros de logs	258
Estadísticas en contenedores	261
Obtener métricas mediante docker inspect	264
Eventos en contenedores docker	264
Monitorizar el rendimiento en contenedores docker	266
cAdvisor	266
Prometheus	269

Dive.....	273
Sysdig falco como herramienta de monitorización	276
Monitorización por comportamiento	277
Ejemplo de monitorización en contenedores	278
Lanzar Sysdig como contenedor	280
Lista de eventos y formato de salida	284
Filtros Sysdig	286
Uso de CPU por contenedor	287
Procesos y uso de CPU de contenedores en ejecución	288
Listar el tráfico de red por contenedor.....	288
Procesos en ejecución de tráfico de red.....	289
Conexiones de red.....	289
Procesos que hacen más uso de e/s.....	289
Monitorizar las solicitudes http de los contenedores	290
Reconstruir el archivo /etc/hosts utilizado por apache.....	290
Obtener los archivos abiertos por apache en /var/www	291
Tráfico entre dos contenedores	291
Filtrar consultas mysql.....	291
Analizar la actividad de mysql y apache	291
Csysdig como herramienta para analizar las llamadas al sistema.....	292
Explorando espectogramas.....	293
Sysdig falco como herramienta de detección de intrusos	294

Instalar Sysdig falco de forma manual	294
Fichero de configuración falco.yaml	295
Definición de reglas	297
Identificar comportamiento anómalo.....	299
Contenedor nginx ejecutando Shell interactivo.....	300
Proceso no autorizado ejecutándose dentro de un contenedor	302
Escribir en un directorio que no forme parte de un volumen de datos.....	304
Puntos de montaje en contenedores.....	306
Explorando el cliente Docker de Python.....	308
CAPÍTULO 6. SEGURIDAD EN VOLÚMENES DOCKER	313
Introducción a los volúmenes de datos.....	313
Montar un directorio de host como un volumen de datos	315
Montar un contenedor de volumen de datos	316
Exponer puntos de montaje	316
Contenedores de datos	317
CAPÍTULO 7. GESTIONAR LA SEGURIDAD DE CLAVES SECRETAS	321
Introducción	321
Estrategias para gestionar claves secretas	321
Guardar secretos en la imagen	321
Pasando secretos en variables de entorno	322
Pasando secretos en volúmenes de datos	322
Uso de soluciones con almacenamiento clave-valor.....	323

KeyWhiz	323
Componentes KeyWhiz	324
Infraestructura clave pública en KeyWhiz	324
Vault.....	325
Características de Vault	326
Instalar e iniciar el servidor de Vault.....	327
Almacenar y leer secretos en el servidor de Vault.....	330
Backends secretos	332
Montar un backend	332
Backend AWS.....	333
Configurar el servicio de AWS.....	335
Creando un rol en AWS.....	335
Generando el secreto en AWS	337
Backends de autenticación	338
Políticas en Vault	340
Escribir políticas en Vault.....	341
Probar políticas en Vault.....	342
Gestión de secretos en Docker Swarm.....	343
CAPÍTULO 8. NETWORKING Y TIPOS DE REDES DE CONTENEDORES	347
Introducción al networking en Docker	347
Configurar el reenvío de puertos entre el contenedor y el host	349
Tipos de red en Docker.....	351

None	352
Modo Bridge	353
Modo Host	357
Desactivar/activar la comunicación entre contenedores	360
Enlazando contenedores dentro del mismo docker host con --link	361
Mapeo de un puerto desde contenedores vinculados	363
Cillium como herramienta de conectividad de red	364
Introducción a Cillium	364
Linux Kernel BPF.....	365
Instalar Cillium	366
Instalación con Docker Compose	366
Instalación con Vagrant	367
Crear una red Docker con Cillium	369
CAPÍTULO 9. AUDITORÍAS, IMÁGENES VULNERABLES Y ANÁLISIS DE MALWARE	373
Auditoría y análisis de vulnerabilidades en imágenes Docker	373
Ciclo de vida de los contenedores	374
Análisis de imágenes vulnerables del Docker Hub	375
Clasificación de vulnerabilidades de seguridad.....	376
Evaluación de repositorios oficiales en Docker Hub	377
Evaluación de repositorios generales en Docker Hub.....	380
Vulners para obtener detalles de CVE	381

Amenazas en contenedores	384
Explotaciones del kernel	384
Ataques de denegación de servicio(DoS).....	384
Imágenes troyanizadas	384
Ejemplos de ataques en contenedores.....	384
Dirtycow exploit (cve-2016-5195)	389
Vulnerabilidad jack in the box (cve-2018-8115)	393
Paquetes más vulnerables.....	395
Imágenes vulnerables en Docker Hub	396
Análisis de malware en virus total.....	397
Ejecución de aplicaciones de análisis de malware como contenedores Docker	400
Proyecto REMnux	400
Pwnbox como contenedor Docker para ingeniería inversa y reversing	403
Docker IDA	405
CAPÍTULO 10. OTRAS PLATAFORMAS DE CONTENEDORES.....	407
CoreOS y Rocket	407
Herramientas de orquestación.....	408
Docker Swarm.....	409
Kubernetes.....	410
Seguridad en Kubernetes.....	413
Vulnerabilidades en Kubernetes	414

Mesos y Marathon	415
Ventajas de usar Docker	416
Probar Docker de forma online	417
Repositorios de github	418
Conclusiones.....	419
CAPÍTULO 11. CUESTIONARIOS	421
Cuestionario básico	421
Cuestionario de evaluación	423
CAPÍTULO 12. GLOSARIO DE TÉRMINOS	425
ÍNDICE ANALÍTICO	431