CONTAINER SECURITY – OVERVIEW PT.1

JOAS ANTONIO
https://www.linkedin.com/in/joas-antonio-dos-santos

CONTAINERS CONCEPT

- https://www.docker.com/resources/what-container
- https://www.netapp.com/devops-solutions/what-are-containers/
- https://www.ibm.com/cloud/learn/containers
- https://www.redhat.com/pt-br/topics/containers/containers-vs-vms
- https://www.burwood.com/blog-archive/containerization-vs-virtualization#:~:text=Virtualization%20enables%20you%20to%20run,single%20virtual%20machine%20or%20server.
- https://www.ibm.com/cloud/blog/containers-vs-vms
- https://docs.microsoft.com/pt-br/virtualization/windowscontainers/about/containers-vs-vm
- https://www.backblaze.com/blog/vm-vs-containers/
- https://www.youtube.com/watch?v=cjXI-yxqGTI
- https://www.youtube.com/watch?v=LZ2Uw228fhk
- https://www.youtube.com/watch?v=1WnDHitznGY
- https://devopscon.io/blog/docker/docker-vs-virtual-machine-where-are-the-differences/

CONTAINERS CGROUP AND NAMESPACE

- https://www.nginx.com/blog/what-are-namespaces-cgroups-how-do-they-work/
- https://opensource.com/article/19/10/namespaces-and-containers-linux
- https://www.redhat.com/sysadmin/building-container-namespaces
- https://en.wikipedia.org/wiki/Linux_namespaces
- https://www.youtube.com/watch?v=sK5i-N34im8
- https://www.youtube.com/watch?v=-YnMr1lj4Z8
- https://www.youtube.com/watch?v=0kJPa-1FuoI
- https://docs.docker.com/get-started/overview/

CONTAINERS COMMANDS

- https://docs.docker.com/engine/reference/commandline/container/
- https://docs.docker.com/engine/reference/commandline/docker/
- https://kubernetes.io/docs/tasks/inject-data-application/define-command-argument-container/
- https://towardsdatascience.com/15-docker-commands-you-should-know-970ea5203421
- https://www.testcontainers.org/features/commands/
- https://www.section.io/engineering-education/managing-docker-containers-using-command-line-interface/
- https://kubernetes.io/pt-br/docs/reference/kubectl/cheatsheet/
- https://kubernetes.io/docs/tasks/access-application-cluster/list-all-running-container-images/

CONTAINERS SECURITY

- https://github.com/gunjan5/container-security
- https://github.com/OWASP/Docker-Security
- https://github.com/sysdiglabs/kube-psp-advisor
- https://github.com/Vinum-Security/kubernetes-security-checklist
- https://github.com/ellerbrock/docker-security-images
- https://github.com/Metarget/awesome-cloud-native-security
- https://github.com/kai5263499/awesome-container-security
- https://github.com/gunjan5/container-security
- https://github.com/OWASP/Docker-Security
- https://github.com/sysdiglabs/kube-psp-advisor
- https://github.com/Vinum-Security/kubernetes-security-checklist
- https://github.com/quay/container-security-operator

CONTAINERS SECURITY 2

- https://github.com/ellerbrock/docker-security-images
- https://github.com/Metarget/awesome-cloud-native-security
- https://github.com/kai5263499/awesome-container-security
- https://github.com/OWASP/Container-Security-Verification-Standard
- https://github.com/krol3/container-security-checklist
- https://github.com/myugan/awesome-docker-security

THREAT MODEL

- https://cloudsecdocs.com/container_security/theory/threats/docker_threat_model/
- https://securityintelligence.com/articles/threat-modeling-container-environment/
- https://www.oreilly.com/library/view/container-security/9781492056690/ch01.html
- https://medium.com/csg-govtech/container-infrastructure-threat-modelling-8fa7315d861d
- https://github.com/kata-containers/documentation/blob/master/design/threat-model/threat-model.md
- https://owasp.org/www-chapter-belgium/assets/2018/2018-09-07/Dirk_Wetter_-_Docker_Security_Brussels.pdf
- https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/guidance-on-kubernetes-threat-modeling

DOCKER ATTACK

- https://attack.mitre.org/matrices/enterprise/containers/
- https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html
- https://venturebeat.com/2021/06/28/aqua-security-50-of-new-docker-instances-attacked-within-56-minutes/
- https://www.net4all.ch/en/publications/docker-and-security-attacks-in-the-docker-environment/
- https://beaglesecurity.com/blog/article/docker-container-security.html
- https://www.trendmicro.com/en_us/research/21/b/threat-actors-now-target-docker-via-container-escape-features.html
- https://sysdig.com/blog/7-docker-security-vulnerabilities/
- https://morphuslabs.com/attacking-docker-environments-a703fcad2a39
- https://medium.com/geekculture/security-analysis-of-docker-containers-a686cebf6405

CONTAINER PENTEST TOOLS

- https://github.com/vchinnipilli/kubestriker
- https://github.com/Metarget/metarget
- https://github.com/Metarget/k0otkit
- https://github.com/grantseltzer/karn
- https://github.com/madhuakula/kubernetes-goat
- https://github.com/anchore/ci-tools
- https://github.com/0xN3utr0n/Kanis
- https://github.com/brant-ruan/awesome-container-escape
- https://github.com/CanonicalLtd/canonical-kubernetes-third-party-integrations

CONTAINER PENTEST TOOLS 2

- https://github.com/topics/container-security
- https://github.com/sysdiglabs/secure-image-scanning
- https://github.com/null-open-security-community/nullCloudSecurity
- https://github.com/devopstoday11/sigrun
- https://github.com/sysdiglabs/security-playground
- https://github.com/aquasecurity/trivy
- https://github.com/enaqx/awesome-pentest

IMAGE BASED ATTACK

- https://blog.aquasec.com/malicious-container-image-docker-container-host
- https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/malicious-docker-hub-container-images-cryptocurrency-mining
- https://snyk.io/blog/hacking-docker-containers-by-exploiting-base-image-vulnerabilities/
- https://thenewstack.io/repository-attacks-continue-with-backdoored-docker-images/
- https://www.sdxcentral.com/articles/news/aqua-attacks-container-image-based-malware-in-sandbox/2020/04/
- https://github.com/OWASP/Docker-Security/blob/main/001%20-%20Threats.md

DOCKER PRIVILEGE ESCALATION

- https://gtfobins.github.io/gtfobins/docker/
- https://book.hacktricks.xyz/linux-unix/privilege-escalation/docker-breakout
- https://github.com/KrustyHack/docker-privilege-escalation
- https://www.hackingarticles.in/docker-privilege-escalation/
- https://www.youtube.com/watch?v=MnUtHSpcdLQ
- https://www.youtube.com/watch?v=pRBj2dm4CDU
- https://www.youtube.com/watch?v=m8_bgwDKEKM
- https://portswigger.net/daily-swig/container-security-privilege-escalation-bug-patched-in-docker-engine
- https://keiran.scot/privilege-escallation-with-docker-56dc682a6e17
- https://blog.creekorful.org/2020/08/docker-privilege-escalation/

AQUA SECURITY CONTAINER SECURITY

- https://www.microfocus.com/media/flyer/detect_and_prevent_container_based_threats_with_arcsight_and_aqua_container_security_platform_flyer.pdf
- https://cdn2.hubspot.net/hubfs/1665891/Assets/Aqua%20Illustrated%20Guide%20to%20Container%20Security.pdf
- https://f.hubspotusercontent40.net/hubfs/1665891/Cloud%20Native%20Security%20Threat%20Report%2009-2020/Aqua_Security_Cloud_Native_Security_Threat_Report_2020.pdf
- https://www.happiestminds.com/wp-content/uploads/2020/05/Container-Security-powered-by-DevSecOps_V2.pdf
- https://media.bitpipe.com/io_14x/io_148034/item_1967657/A%20Framework%20DevSecOps%20Guide%20Making%20It%20Happen.pdf
- https://cdn2.hubspot.net/hubfs/1665891/Aqua%20NIST%20Guide.pdf
- https://wenovate.de/wp-content/uploads/2020/03/Aqua-Booklet_11-19-PRINT.pdf
- https://github.com/aquasecurity
- https://info.aquasec.com/hubfs/Assets/DevOps.com%20-%20Container%20Security%20Challenges.pdf
- https://d1.awsstatic.com/Marketplace/solutions-center/downloads/Aqua-Daatasheet.pdf
- https://f.hubspotusercontent40.net/hubfs/1665891/Assets/Solution_Sheets_and_Datasheets/Aqua%20Solution%20Sheet%20.pdf
- https://2020.forum-fic.com/Data/DO/tgBloc/16011/fr/params/file/FT19-AQUASECURITY.pdf
- https://securosis.com/assets/library/reports/Securosis_BuildingContainerSecProgram_2018.pdf

AWESOME CONTAINER SECURITY

- https://github.com/Friz-zy/awesome-linux-containers
- https://github.com/veggiemonk/awesome-docker
- https://github.com/pditommaso/awesome-containers
- https://github.com/tomhuang12/awesome-k8s-resources
- https://github.com/borntorock/awesome-containers