INSE6120 - Project

### **Sub-groups:**

- Attack Group: Maliheh Goliforoushani, Armin Mansouri,Nazanin Nasserifar

- Development Group:

—

### **Useful Materials:**

If you are not familiar with Docker and Containers, there is a useful course in Udemy:

[Docker for the Absolute Beginner - Hands On - DevOps](https://concordia.udemy.com/course/learn-docker/)

<https://www.youtube.com/watch?v=_jKNnHROiC0>

—-

### **Meetings:**

—-

Attacks:

A good place to start:

[Docker Hacking | Hacker101](https://www.hacker101.com/sessions/docker_hacking)

| No. | Link | Student | Checked |
| --- | --- | --- | --- |
| 1 | CVE-2022-0847:DIRTY PIPE | afshin |  |
| 2 | CVE-2014- 6271:Shell Shock | Maliheh Goliforoushani |  |
| 3 | Docker - - privileged flag | Maliheh Goliforoushani |  |
| 4 | 1. Docker attack surface  2. Exploiting vulnerable images -implemented by Arash  <https://www.youtube.com/watch?v=U0T1i4u_L1A>  <https://snyk.io/blog/hacking-docker-containers-by-exploiting-base-image-vulnerabilities/>  <https://www.youtube.com/watch?v=pRBj2dm4CDU> | ARASH |  |
| 5 | 4. Container escape using docker.sock | ARASH |  |
| 6 | [Proof of Concept: Manually Escaping Privileged Docker Containers Without Exploiting Vulnerabilities](https://www.youtube.com/watch?v=8gDP3nJMlJI) |  |  |
| 7 | [How I Hacked Play-with-Docker and Remotely Ran Code on the Host](https://www.cyberark.com/resources/threat-research-blog/how-i-hacked-play-with-docker-and-remotely-ran-code-on-the-host) |  |  |
| 8 | [How to escape docker container?](https://www.youtube.com/watch?v=_dhONyAk4es) | Maliheh Goliforoushani |  |
| 9 | [Malicious Container Escape Exploit (CVE-2019-5736) PoC Demo](https://www.youtube.com/watch?v=gjvsbcAlQl8) | Armin Mansouri |  |
| 10 | [Dirty COW - (CVE-2016-5195) - Docker Container Escape](https://blog.paranoidsoftware.com/dirty-cow-cve-2016-5195-docker-container-escape/) | Nazanin Nasserifar |  |
| 11 | [Exploiting Gitlab 11.4.7 & Escaping a Privileged Docker Container - Ready on HackTheBox](https://www.youtube.com/watch?v=LuXBtPztA5I) | Amir |  |
| 12 | [Vulnerability Exploitation In Docker Container Environments](https://www.youtube.com/watch?v=77-jaeUKH7c) | Amir |  |
| 13 | [Docker Vulnerability Let Attacker To Take Complete Control Over Host](https://gbhackers.com/docker-vulnerability/) | Ali Hasheminezhad |  |
| 14 | [Container Security](https://devopedia.org/container-security) | Ali Hasheminezhad |  |
| 15 | [Mitigating High Severity RunC Vulnerability (CVE-2019-5736)](https://blog.aquasec.com/runc-vulnerability-cve-2019-5736) | Armin Mansouri |  |
| 16 | [Escape from a Docker container: Explanation of the last patched vulnerability on docker < 18.09.2 (CVE-2019-5736) - EvaBssi](https://evabssi.com/en/escape-from-a-docker-container-explanation-of-the-last-patched-vulnerability-on-docker-18-09-2-cve-2019-5736/) | Armin Mansouri |  |
| 17 | [Four Features of Containers that Help Docker Security | Sysdig](https://sysdig.com/blog/docker-security-landscape/) |  |  |
| 18 | [Dirty COW - (CVE-2016-5195) - Docker Container Escape](https://blog.paranoidsoftware.com/dirty-cow-cve-2016-5195-docker-container-escape/) | Hadi |  |
| 19 | [Attacking & Auditing Docker Containers Using Open Source tools](https://youtu.be/ru7GicI5iyI) | Amir |  |
| 20 | [CVE-2019-5736: runC Container Breakout](https://utku.eu/cve-2019-5736-runc-container-breakout/)  <https://github.com/twistlock/RunC-CVE-2019-5736> | Armin Mansouri |  |
| 21 | <https://www.blackhat.com/docs/us-17/thursday/us-17-Cherny-Well-That-Escalated-Quickly-How-Abusing-The-Docker-API-Led-To-Remote-Code-Execution-Same-Origin-Bypass-And-Persistence_wp.pdf> | Nazanin Nasserifar |  |
| 22 | https://www.bmc.com/blogs/docker-security-best-practices/ | Hadi |  |
| 23 | Docker bench security. It examines the containers and score them based on their security.  Our aim is to increase the Score values using the information and warning section, thus making our container deployments more secure. | Maliheh Goliforoushani |  |
| 24 | Trivy tool to scan the vulnerabilities in the image | Hadi |  |
| 25 | Trivy tool to scan the vulnerabilities in the image | Hadi |  |
| 26 | <https://www.youtube.com/watch?v=6xMGsdD-ArI> Zero logon exploitation script  <https://github.com/risksense/zerologon>  <https://www.cvedetails.com/cve/CVE-2020-35195/> |  |  |
| 27 | APPARMOR and SElinux for preventing containers |  |  |
| 28 | CVE 2020 11492  <https://www.pentestpartners.com/security-blog/docker-desktop-for-windows-privesc-cve-2020-11492/>  <https://github.com/joshfinley/CVE-2020-11492#readme>  <https://www.youtube.com/watch?v=VYQm5L9zmTk>  <https://nvd.nist.gov/vuln/detail/CVE-2020-11492> | Nazanin |  |
| 29 | Privilege escalation using volume mounts |  |  |
| 30 | Writing to Kernel space from a container |  |  |
| 31 | CVE-2022-0185 |  |  |
| 32 | https://blog.aquasec.com/cve-2020-15257-containerd-shim-api-vulnerability |  |  |
| 33 | docker socket exploit |  |  |
| 34 | cve-2019-14271 docker |  |  |

**References:**

1. <https://www.cncf.io/wp-content/uploads/2020/11/CNCF_Survey_Report_2020.pdf>
2. <https://en.wikipedia.org/wiki/LXC>
3. <https://linuxcontainers.org/lxd/introduction/>
4. <https://github.com/lxc/lxcfs>
5. <https://en.wikipedia.org/wiki/Docker_(software)>
6. <https://nvd.nist.gov/vuln/detail/CVE-2016-5195>
7. <https://docs.docker.com/storage/storagedriver/>
8. <https://blog.paranoidsoftware.com/dirty-cow-cve-2016-5195-docker-container-escape/>
9. <https://github.com/hedeesaa/dirty-cow-poc.git>
10. <https://github.com/scotty-c/dirty-cow-poc>
11. <https://blog.aquasec.com/dirty-cow-vulnerability-impact-on-containers>
12. <https://twitter.com/_fel1x/status/1151487051986087936?s=20&t=5HlPP3vfnDPUMb-YB8oJMw>
13. <https://www.docker.com/blog/what-is-containerd-runtime/>
14. <https://www.kernel.org/doc/Documentation/cgroup-v1/cgroups.txt>
15. <https://blog.trailofbits.com/2019/07/19/understanding-docker-container-escapes/>
16. <https://www.youtube.com/watch?v=U0T1i4u_L1A>
17. <https://nvd.nist.gov/vuln/detail/cve-2014-6271>
18. <https://hub.docker.com/>
19. <https://betterprogramming.pub/about-var-run-docker-sock-3bfd276e12fd/>
20. <https://traefik.io/>
21. <https://www.portainer.io/>
22. <https://elastest.io/>
23. <https://docs.gitlab.com/ee/ci/docker/using_docker_build.html/>
24. <https://ubuntu.com/server/docs/security-apparmor>
25. <https://linux-audit.com/linux-capabilities-101/>
26. Lin, Xin, et al. "A measurement study on linux container security: Attacks and countermeasures." *Proceedings of the 34th Annual Computer Security Applications Conference*. 2018.
27. <https://vickieli.dev/system%20security/escape-docker/>
28. <https://www.nginx.com/blog/what-are-namespaces-cgroups-how-do-they-work/>
29. <https://www.youtube.com/watch?v=mQkVB6KMHCg&list=RDCMUC0ZTPkdxlAKf-V33tqXwi3Q&start_radio=1>
30. <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/resource_management_guide/ch01>
31. <https://dockerlabs.collabnix.com/advanced/security/cgroups/>
32. <https://github.com/docker/docker-bench-security>
33. <https://docs.chef.io/inspec/>
34. <https://docs.docker.com/engine/security/userns-remap/>
35. <https://github.com/anchore/grype>
36. [https://www.cloudsavvyit.com/14929/how-to-find-vulnerabilities-in-containers-and-files-with-grype](https://www.cloudsavvyit.com/14929/how-to-find-vulnerabilities-in-containers-and-files-with-grype/)/
37. <https://man7.org/linux/man-pages/man7/capabilities.7.html>
38. <https://www.youtube.com/watch?v=CQLtT_qeB40&list=RDCMUC0ZTPkdxlAKf-V33tqXwi3Q&index=2>