CONTAINER SECURITY BOOTCAMP

These video recordings are from our live online bootcamp

Session I

The following topics are covered

- Introduction to Containers
- Container vs VM
- Docker Basic Commands
- Microservice and Multi-Container Setups
- Groups, Namespaces in detail
- Creating Container using Linux Kernel features

2:33:22

List of labs covered during the session (and homework):

- Docker Basics Lab (https://attackdefense.com/challengedetails?cid=1342)
- Multi Container Setups (https://attackdefense.com/challengedetails?cid=2271)
- Containerd Basics Lab (https://attackdefense.com/challengedetails?cid=1450)
- Containers With Runc (https://attackdefense.com/challengedetails?cid=1462)
- Cgroups and Namespaces (https://attackdefense.com/challengedetails?cid=2274)
- Chroot Jail I (https://attackdefense.com/challengedetails?cid=1306)
- Attacking Microservice Containers I (https://attackdefense.com/challengedetails?cid=1029)
- Attacking Microservice Containers II (https://attackdefense.com/challengedetails?cid=1030)
- Attacking Microservice Containers III (https://attackdefense.com/challengedetails?cid=1031)

Session II

- Docker Socket Misconfigurations
- Excessive Privileges
- Special scenarios
- Linux Capabilities
- Shared Namespaces

2:23:09

List of labs covered during the session (and homework):

- Linux Capabilities I (https://attackdefense.com/challengedetails?cid=1822)
- Linux Capabilities II (https://attackdefense.com/challengedetails?cid=1823)
- Linux Capabilities III (https://attackdefense.com/challengedetails?cid=1824)
- Linux Capabilities IV (https://attackdefense.com/challengedetails?cid=1825)
- The Basics: CAP_SYS_MODULE (https://attackdefense.com/challengedetails?cid=1344)
- The Basics: CAP_NET_RAW (https://attackdefense.com/challengedetails?cid=1346)
- The Basics: CAP_SYS_PTRACE (https://attackdefense.com/challengedetails?cid=1412)
- Mounted Docker Socket (https://attackdefense.com/challengedetails?cid=1195)
- Privileged Container (https://attackdefense.com/challengedetails?cid=1196)
- Privileged Container II (https://attackdefense.com/challengedetails?cid=1197)
- Process Injection (https://attackdefense.com/challengedetails?cid=1198)
- Abusing SYS_MODULE Capability (https://attackdefense.com/challengedetails?cid=1199)
- Abusing DAC_READ_SEARCH Capability (https://attackdefense.com/challengedetails?cid=1458)
- Shared Network Namespace (https://attackdefense.com/challengedetails?cid=1460)
- Abusing DAC_OVERRIDE Capability (https://attackdefense.com/challengedetails?cid=1459)

Session III

The following topics are covered

- Privilege Escalation by abusing
  - Docker socket/group
  - Containerd/runc components
  - Fake image and insecure registry
- Docker Host Takeover by abusing management tool
- Discovering vulnerable Docker hosts
- Stealing confidential data by using
  - Backdoored image

2:21:07

List of labs covered during the session (and homework):

- Misconfigured Docker Socket (https://attackdefense.com/challengedetails?cid=1194)
- Weakest Link (https://attackdefense.com/challengedetails?cid=1415)
- Weakest Link II (https://attackdefense.com/challengedetails?cid=1417)
- Leveraging Containerd (https://attackdefense.com/challengedetails?cid=1452)
- Low-Level Container Runtime (https://attackdefense.com/challengedetails?cid=1453)
- Leveraging Containerd II (https://attackdefense.com/challengedetails?cid=1457)
- Abusing Group Membership (https://attackdefense.com/challengedetails?cid=1251)
- Exploiting Remote Docker Host (https://attackdefense.com/challengedetails?cid=2307)
- Flag File Forensic Recovery I (https://attackdefense.com/challengedetails?cid=1036)
- Flag File Forensic Recovery II (https://attackdefense.com/challengedetails?cid=1037)
- System Backdoor (https://attackdefense.com/challengedetails?cid=1454)
- Malicious Binary (https://attackdefense.com/challengedetails?cid=1455)
- Credential Recovery (https://attackdefense.com/challengedetails?cid=1456)
- Hidden Directory (https://attackdefense.com/challengedetails?cid=1032)
- Insecure Secret Keys (https://attackdefense.com/challengedetails?cid=1033)
- Embedded Credentials (https://attackdefense.com/challengedetails?cid=1034)
- Misconfigured Server (https://attackdefense.com/challengedetails?cid=1035)
- Insecure Docker Registry I (https://attackdefense.com/challengedetails?cid=1024)
- Insecure Docker Registry II (https://attackdefense.com/challengedetails?cid=1025)
- Protected Docker Registry I (https://attackdefense.com/challengedetails?cid=1026)
- Insecure Docker Registry III (https://attackdefense.com/challengedetails?cid=1027)
- Insecure Docker Registry IV (https://attackdefense.com/challengedetails?cid=1028)
- Corrupting Source Image (https://attackdefense.com/challengedetails?cid=1573)
- Corrupting Source Image II (https://attackdefense.com/challengedetails?cid=1574)
- Corrupting Source Image III (https://attackdefense.com/challengedetails?cid=1587)

Session IV

The following topics are covered

- Auditing Docker host and containers
- Enabling Authentication on TCP Socket
- Image Vulnerability scanning
- Enabling Authentication and TLS on Docker Registry
- Namespace remapping and its benefits
- Singing Docker images
- Dockerfile Linting

2:27:28

List of labs covered during the session (and homework):

- Securely Accessing Remote Docker Host (https://attackdefense.com/challengedetails?cid=2308)
- User Namespace Remapping (https://attackdefense.com/challengedetails?cid=2309)
- Securing Private Docker Registry (https://attackdefense.com/challengedetails?cid=2310)
- Dockerfile Linter (https://attackdefense.com/challengedetails?cid=2161)
- Dockerfilelint (https://attackdefense.com/challengedetails?cid=2161)
- Dockerlint (https://attackdefense.com/challengedetails?cid=2163)
- Hadolint (https://attackdefense.com/challengedetails?cid=2164)
- Portainer (https://attackdefense.com/challengedetails?cid=1414)
- Dive (https://attackdefense.com/challengedetails?cid=1416)
- Docker Bench Security (https://attackdefense.com/challengedetails?cid=1607)
- Dockscan (https://attackdefense.com/challengedetails?cid=1608)
- Amicontained (https://attackdefense.com/challengedetails?cid=1609)
- Clair (https://attackdefense.com/challengedetails?cid=1620)
- Falco (https://attackdefense.com/challengedetails?cid=1621)

Earn Completion Certification

The completion certification for the Container Security: Beginner Edition Bootcamp can be earned by solving the challenges listed here:
https://attackdefense.com/badgedetails?id=cert-container-security-beginner