LINUX PRIVILEGE ESCALATION BOOTCAMP

These video recordings are from our live online bootcamp

Session I

The following topics are covered in Session I

- Linux Concepts
    - Linux Users and Groups
    - Linux File Permissions
    - Interactive programs
        - Text Editor
        - Terminal based Browsers
    - Popular Linux Utilities
- Misconfigured SUID
- Misconfigured SUDO
- Misconfigured File Permissions

2:49:53

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

- Permissions Matter! (https://attackdefense.com/challengedetails?cid=75)
- Exploiting Setuid Programs (https://attackdefense.com/challengedetails?cid=73)
- Editing Gone Wrong (https://attackdefense.com/challengedetails?cid=80)

Session II

The following topics are covered in Session II

- Cron Job
    - Crontab File formats

        - Understanding the Load Order
        - Creating a shared library
- Leveraging Cron Jobs
    - Unix Wildcards gone wild
    - World writable scripts
    - World readable cron error messages
    - Symlinks and PATH-based misconfigurations.
- Vulnerable Application and Services
- Web to Root
- App to Root
- Shared Library Injection

2:56:31

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

- Cron Jobs Gone Wild! (https://attackdefense.com/challengedetails?cid=74)
- The Golden Logs (https://attackdefense.com/challengedetails?cid=81)
- Cron Jobs Gone Wild II (https://attackdefense.com/challengedetails?cid=77)
- Symlinks Get Me Worried! (https://attackdefense.com/challengedetails?cid=91)
- Not all PATHs are Secure (https://attackdefense.com/challengedetails?cid=92)
- Fallen Guardian (https://attackdefense.com/challengedetails?cid=699)
- Liberator Database (https://attackdefense.com/challengedetails?cid=698)
- Leveraging Message Transfer Agent (https://attackdefense.com/challengedetails?cid=1340)
- Leveraging X Windows System (https://attackdefense.com/challengedetails?cid=700)
- Shared Server (https://attackdefense.com/challengedetails?cid=87)
- CMS Admin to Root II (https://attackdefense.com/challengedetails?cid=86)
- Library Chaos (https://attackdefense.com/challengedetails?cid=90)
- Library Chaos II (https://attackdefense.com/challengedetails?cid=98)
- Load Order Matters (https://attackdefense.com/challengedetails?cid=88)

Session III

The following topics are covered in Session III

- Restricted Shells
- Chroot Jail
- Namespaces and Cgroups
- Introduction to Docker
- Compromising Docker Host via an exposed TCP socket

2:49:36

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

- Restricted Shell (https://attackdefense.com/challengedetails?cid=97)
- Chroot Jail I (https://attackdefense.com/challengedetails?cid=1306)
- Cgroups and Namespaces (https://attackdefense.com/challengedetails?cid=2274)
- Docker Basics (https://attackdefense.com/challengedetails?cid=1342)
- Exposed Docker Socket (https://attackdefense.com/challengedetails?cid=1194)

Session IV

The following topics are covered in Session IV

- Compromising Docker Host via mounted docker socket
- Breaking out of containers via management tools
- Sharing namespaces in docker
- Introduction to Linux Capabilities
    - History
    - Process and file capabilities
    - Linux Capabilities Sets
    - Identifying capabilities provided to binaries and running process
    - Managing capabilities
- Breaking out of privileged container
- Capability based container breakouts
    - CAP_DAC_READ_SEARCH
    - CAP_SYS_MODULE
    - CAP_SYS_ADMIN
    - CAP_SYS_PTRACE
- Abusing Linux Capabilities on Linux utilities and interpreters.
    - CAP_DAC_READ_SEARCH
    - CAP_SYS_MODULE
    - CAP_SYS_ADMIN
    - CAP_SYS_PTRACE

3:35:58

- Mounted Docker Socket (https://attackdefense.com/challengedetails?cid=1195)
- Weakest Link (https://attackdefense.com/challengedetails?cid=1415)
- Shared Network Namespace (https://attackdefense.com/challengedetails?cid=1460)
- 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)
- The Basics: CAP_NET_RAW (https://attackdefense.com/challengedetails?cid=1346)
- The Basics: CAP_DAC_READ_SEARCH (https://attackdefense.com/challengedetails?cid=1343)
- The Basics: CAP_SYS_MODULE (https://attackdefense.com/challengedetails?cid=1344)
- The Basics: CAP_SYS_MODULE II (https://attackdefense.com/challengedetails?cid=1345)
- The Basics: CAP_SYS_ADMIN (https://attackdefense.com/challengedetails?cid=1376)
- The Basics: CAP_SYS_PTRACE (https://attackdefense.com/challengedetails?cid=1412)