Penetration Testing and Docker Security

—

By Sristi Lakshmi Sravana Kumar
National Cybersecurity R&D Lab

Penetration Testing

- What is Penetration Testing?
- Why is Penetration Testing needed?
- How to do Penetration Testing?

What is Penetration Testing?

Limited Scope

Maximum of 1-2 Weeks

A localized and time-constrained attempt to breach the information security architecture using the attacker's techniques

Not a full security audit

http://www.fish2.com/security/admin-guide-to-cracking.html

Why is Penetration Testing needed?

- To improve information security awareness
- To assess risk
- To mitigate risk immediately
- To reinforce the Information Security process
- To assist in decision making processes

How to do Penetration Testing?

- Information Gathering
- Vulnerability Detection
- Exploitation
- Post-Exploitation
- Reporting, Cleanup

- Understanding of component relationships
- Target/Scope identification
- Infrastructure fingerprinting
- Sub-domain Enumeration

- Vulnerability scanners are valuable tools; because many pentests are performed within a shorter time window
- Manual scanning can be used to avoid detection and false positives

- Known/available exploit selection
- Exploit customization
- Exploit development
- Exploit testing
- Attack: target compromise

- Privilege Escalation
- Pivoting
- Lateral Movement
- Data-Exfiltration

Based on the scope of the testing

Tools for Penetration Testing and Vulnerability Assessment

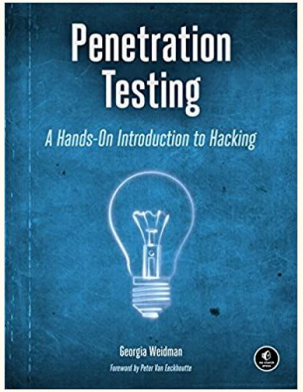
Docker Security

Common Techniques to Enchance Docker Security

1. Updating the Host machine and Docker with latest patches from known vulnerabilities
2. Do not expose the Docker daemon socket (even to the containers)
3. Configuring the Docker container to use an unprivileged user
4. Use static analysis tools
5. Set filesystem and volumes to read-only and Limit resources (memory, CPU, file descriptors, processes, restarts)
6. Lint the Dockerfile at build time

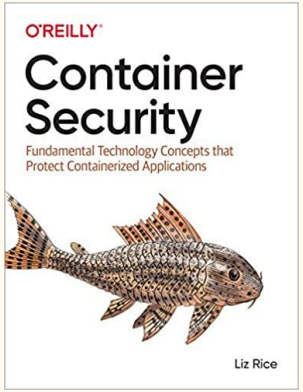
References

Penetration Testing



- https://www.amazon.com/Penetration-Testing-Hands-Introduction-Hacking/dp/1593275641
- http://www.pentest-standard.org/index.php/Main_Page
- https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

Docker Security



- https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html
- https://www.amazon.sg/Container-Security-Fundamental-Containerized-Applications/dp/1492056707