Advanced RHEL/CentOS Defensive Security & Hardening.

1. Training description.
2. Key learning objectives.
3. Who should attend.
4. Prerequisite knowledge.
5. HW / SW requirements.
6. Full agenda.
7. Time duration.
8. Training keywords.
9. Trainer Bio.
10. Customers.
11. Contact.

TRAINING DESCRIPTION:

Advanced RHEL/CentOS Defensive Security & Hardening is a dedicated training about how we can protect and attack Linux OS. Mandatory access control, sandboxing, root user limitation and low-level accountability, ACL, service isolation on different layers: seccomp, capabilities or SELinux are just the beginning of fun. During dedicated labs you will find how to use different offensive and defensive tools, scripts, services and techniques to understand better how attacker thinks and what are the most important actions of modern adversary. On the other hand you will explore also how to design secure, hardened systems, applications network services. Training content in formula “protection vs attack” will help you understand risks, identify network security blind spots and unexpected, uncovered spaces inside OS. This training is intended to increase skills needed to ensure data integrity on critical system for organizations with highest security standards. The discussed methods of automation will support the process of achieving compliance.

KEY LEARNING OBJECTIVES → We will explore in details how to:

- Prepare hardened OS configuration templates and automate deployment process
- Kernel and user space exploit techniques works and analyze critical CVE, bugs and misconfigurations from recent years
- Demonstrate that OS configuration meets security policy requirements

- Run local and network-based vulnerability scanning / CVE tracking
- Errata / security package management
- Configure Access Control Lists and special permissions, bits and secure flags
- Manage users and password policy
- Privileged and unprivileged access accounting / session recording
- Deploy basic Linux Domain Controller with SUDO / HBAC
- Understand system auditing and syscall behavioral profiling
- Manage and configure secure virtualization and Docker containers environment
- Configure and tweak targeted SELinux policy against latest exploits
- Understand different layers for user and service isolation
- Deploy advanced network firewall rules with anti-flooding capabilities
- Run memory acquisition and deliver memory forensics actions against Linux malware
- Compile code and run binaries in a hardened way vs local privilege escalation techniques

---

WHO SHOULD ATTEND:

- Linux Administrators & Engineers
- DevOps / Sysops team members
- System Architects
- IT Security Experts and Consultants

PREREQUISITE KNOWLEDGE:

- An intermediate knowledge about Linux OS
- An intermediate level of command line syntax experience using Linux
- Fundament knowledge of TCP/IP network protocols

HW / SW REQUIREMENTS:

- At least 20GB of free disk space
- At least 8GB of RAM
- Students should have the latest Virtualbox installed on their machine
- Full Admin access on your laptop

FULL AGENDA:

1. Introduction:
    a. Defense in depth.
    b. DevSecOps methodology.
    c. Threat hunting.

2. Discretionary Access Control (DAC) vs Mandatory Access Control (MAC).
3. Secure file system design, attributes, flags, ACL and FS encryption.
4. Package management security and CVE tracking.
5. SSP, NX, PIE, RELRO, ASLR, LD_PRELOAD vs attacks.
6. The importance of SELinux:
    a. Targeted policy vs exploits
    b. Multi Category Security (MCS)
    c. Rule Based Access Control
    d. sVirt

7. Linux capabilities vs SUID attacks.
8. System call restriction - seccomp-BPF vs exploits.
9. Linux Containers - Docker security vs escaping.
10. Chroot / jail / nsjail vs escaping.
11. LKM-off / ptrace-yama / and other sysctl enforcing options.
12. Debuggers and profilers - gdb / strace / ltrace / ldd / yara.
13. Behavioral analysis and hacker's fishing - systemtap / eBPF / sysdig.
14. Integrity checking - IMA/EVM.
15. Grub and secure boot configuration.
16. System update vs reboot.
17. Linux Domain Controller: HBAC / SUDO / RBAC.
18. PAM configuration: 2FA / sudo_pair / time-based access.
19. Secure SSH / SCP / SFTP + tips and tricks.
20. Advanced network firewall: iptables / nftables / ebtables.
21. Local and external security enumeration and reconnaissance tactics.
22. Linux visibility, auditing & accounting:
    a. auditd
    b. syslog
    c. OSSEC
    d. osquery

23. Memory forensics - Volatility Framework vs malware.
24. Automation of STIG Hardening standard by using:
    a. Ansible roles
    b. Puppet manifests
    c. Chef cookbooks

25. Summary and final lab.

TIME DURATION:

- 2 days of very intensive training (9:00-17:00)

REVIEWS:

- “Excellent content, great stuff and awesome knowledge from the trainer.”
- “Excellent balance between breadth and depth of contents, great materials.”
- “Awesome OSDS @brucon training, learned a lot! Was a pleasure to meet you.”
- “Very good course, the instructor was very knowledgeable and answered all our questions. Course exceeded my expectations, great job!”

TRAINER BIO:

- Leszek Miś is the Founder of Defensive Security (www.defensive-security.com) and VP, Head of Cyber Security in Collective Sense (www.collective-sense.com) where he is responsible for strategy, business analysis, and technical product security research & feature recommendations. He has over 13 years of experience in IT security market supporting the world’s largest customers in terms of exfiltration simulations and penetration tests, infrastructure hardening and general IT Security consultancy services. Next, to that, he has 10 years of experience in teaching and transferring a deep technical knowledge and his experience. He has trained 500+ students with the average evaluation on a 1-5 scale: 4.9. He is an IT Security Architect with offensive love and recognized expert in enterprise Open Source Security solutions market. Leszek provides network data exfiltration simulation services, web application & infrastructure penetration tests and OSINT. He specializes in low-level Linux/OS hardening and defensive security of web application platforms (ex. think about integration of WAF+BeeF!). He is also known and respected trainer/examiner of Red Hat solutions and author of many IT Security workshops:

    - Open Source Defensive Security (OSDS)
    - ModSecurity → Web Application Firewall rules vs attacks
    - FreeIPA → Centralised identity management system
    - SELinux - Creating and managing of SELinux policies
    - Advanced RHEL/Centos Defensive Security & Hardening

    - Post Exploitation Adversary Simulations - Network Data Exfiltration Techniques

- As a speaker, trainer or just a participant he attended many conferences like Brucon 2017/2018, OWASP Appsec USA, FloCon 2018("May the data stay with U!"), SuriCon 2017, HITBSecConf, AlligatorCon, Semafor, Exatel Security Days, Confidence 2016("Honey(pot) flavored hunt for cyber enemy), PLNOG 2016 ("Yoyo! It's us, packets! Catch us if you can"), NGSEC 2016 ("Many security layers for many defensive opportunities"), Open Source Day 2010/2011/2012/2013/2014, SysDay 2008 ("SELinux vs exploits"), Confitura 2014 ("Detection and elimination of threats in real time - OWASP Appsensor in action."), Red Hat Roadshow 2014, OWASP Chapter Poland 2015("Does your WAF can handle it?), ISSA, InfoTrams 2015, BIN Gigacon 2015("Mapping pen testers knowledge for the need to protect a critical IT infrastructure").

- The holder of many certificates:
    - Offensive Security Certified Professional (OSCP)
    - Red Hat Certified Architect (RHCA)
    - Red Hat Certified Security Specialist (RHCSS)
    - Splunk Certified Architect
    - Comptia Security+

CUSTOMERS:

- PGNiG
- Stack Overflow
- Daily Motion
- Alior Bank
- Ministry of Finance
- Millennium Bank
- Nazwa.pl
- Rekord Systemy Informatyczne
- IBS S.A.
- Cinkciarz.pl
- Rockwell Automation
- Esky.pl
- LPP S.A.
- ARiMR
- TUV
- Polkomtel

CONTACT:

- Email: info@defensive-security.com
- Mobile: 0048 791 611 309 (Poland) / 0048 791 611 309
- Website: https://www.defensive-security.com