SELinux - Development & Administration of Mandatory Access Control Policy.

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:

The "SELinux - Development and Administration of Mandatory Access Control Policy" is a training dedicated for students who want to learn in details how SELinux really works, how to manage the existing policy and how to create your own SELinux policy modules from scratch for unsecured local and network services. Together with participants we will go through attack vectors and malicious methods used by attackers directly in confrontation with SELinux. We focus a lot on detailed analysis of Linux security subsystems, hardening options and confinement of local and network services.

WHO SHOULD ATTEND:

- Linux Engineers
- System Architects
- DevOps and DevSecOps team members
- Security Engineers

PREREQUISITE KNOWLEDGE:

- An intermediate level of command line syntax experience using Linux
- Penetration testing experience performing enumeration, exploiting, and lateral movement is beneficial, but not required
- Basic programming skills is a plus, but not essential

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. Discretionary Access Control vs Mandatory Access Control → typical attack vectors against Linux OS, application and network services.

2. Analysis and practical use of Linux exploits and vulnerabilities:
    - invalid read, use-after-free, out-of-bound, stack and heap overflows, null pointer dereference, syscall hooking and more.

3. SELinux Architecture and capabilities:
    - Flask Model
    - Mandatory Access Control
    - Rule Based Access Control
    - Multi Level Security
    - Multi Category Security
    - domains and types, security context, domain and type transition
4. Analysis of targeted SELinux policy:
    - Source code analysis of RHEL / CentOS and Tresys Reference Policy
    - Types and modes
    - Filesystem locations

5. SELinux module development and compilation:
    - m4 syntax
    - classes oraz objects
    - interfaces and macros
    - aliases, types and attributes
    - boolean variables definition

    - compilation modes

6. Access Vector Cache.
7. Tools used to create and modify SELinux policy.
8. Creating SELinux users and roles.
9. Using SELinux for hardening Docker containers and cloud environments.
10. SELinux against exploits → real security use-cases
11. Tips and tricks.
12. Final project:
    - Creating a SELinux policy module for service daemon including: domain definition, file contexts, macros, transitions, boolean variables and more.

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)
- Website: https://www.defensive-security.com