FreeIPA → Identity Management for Linux Domain Environments & Trusts

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:

- *FreeIPA → Identity Management for Linux Domain Environments & Trust* is a dedicated training which helps you understand the basics and deploy later very expanded Linux Domain Environments within your private or cloud infrastructure. During hands-on labs we will cover in details every important aspect and functionality of FreeIPA. Except simple things like user or password management we will talk about big installations and advanced integrations with Active Directory or other Unix systems like AIX, Solaris or HP-UX. We will go through not so simple PKI features, critical network services integration like VPN or Proxy. We will deep dive into replication process and issues, Single-Sign On and 2FA setups. There are also lab sessions related to hardening and security testing of FreeIPA instances. Distributed SUDO and Host-Based Access Control rules for your desktops, servers and critical applications allow you to build controlled, secured and accountable environment and this training shows you all of that. As a bonus we will show you how to use user's LDAP attributes for achieving hidden network data exfiltration across isolated network segments, LDAP denial of service, anonymous BINDs and of course how to protect your installation against above threats.

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

- Deploy and manage FreeIPA master/replica clustered servers
- Enroll Linux client machines and integrate other Unix systems like AIX, Solaris or HP-UX
- Create and manage user and service identities
- Define HBAC access policies
- Configure and integrate critical network services into FreeIPA authentication and authorization capabilities
- Manage advanced PKI infrastructure
- Setup multi-factor authentication and run SSO and trusts
- Protect and harden domain environment instances

WHO SHOULD ATTEND:

- IT Consultants and Solution Integrators
- DevOps and DevSecOps Engineers
- Linux and Network Engineers
- System Administrators

PREREQUISITE KNOWLEDGE:

- An intermediate level of command line syntax experience using Linux and Windows
- Fundament knowledge of TCP/IP network protocols
- Understanding needs and modern architecture of corporate networks

---

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 to domain environments.

2. Installing and configuring FreeIPA server.
3. Installing and enrolling client machines.
4. SSSD and PAM configuration.
5. User, group and role management.
6. SSO kerberos-based authentication and authorization:
    a. SSH
    b. HTTP
    c. NFS
    d. Samba
    e. Squid
    f. Radius
    g. VPN

7. 2FA, one-time password and smart card authentication.
8. DNS configuration and management.
9. HBAC - Host Based Access Control.
10. Distributed SUDO rules management.
11. SSH pubkey configuration.
12. SELinux user mapping.
13. Public Key Infrastructure - Certificate Management.
14. FreeIPA replication.
15. FreeIPA in the cloud.
16. Active Directory Trust Integration.
17. FreeBSD, Solaris, AIX and HP-UX Integration.
18. FreeIPA hardening and vulnerability scanning.
19. Backup and restore.
20. FreeIPA tips and tricks.
21. Summary and final lab.

TIME DURATION:

- 2 days of 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 83 10 18
- Website: https://www.defensive-security.com