Education & Services Portfolio

OUR APPROACH TO CYBERSECURITY EDUCATION:

At Defensive Security we have developed training programs with a focus on blue vs red team actions that gives you the best opportunity to make stronger defensive layers inside your IT environment. Conversely, it will help you to better understand the mind and approach of modern adversaries, their style of offensive thinking, techniques and of course tools in current use.

All of our high-tech training programs have a unique “protection vs attack” formula. This means that during lab exercises most of the security issues, use-cases and attack examples we talk about will be detected and effectively protected by using suitable techniques, approaches, sophisticated open source tools and recommended secure configurations. We focus on delivering a defensive content, but on the other hand, we understand that for being good in a defensive scope you have to understand the other side too, the offensive side. In that way, we provide a kind of knowledge-mix in these fields using Open Source software only.

As Sun Tzu said: "Know your enemy and know yourself (and your tools!) and you can fight a hundred battles without disaster."

SERVICE & CONSULTING AREAS:

We understand that the best training programs are based on a true experience from real production environments and use-cases. This is the main reason why we still actively participate in security projects. With over 13 years being inside the 'battle' in the IT security world supporting the largest companies and institutions, it has given us a great opportunity to deliver to you the highest quality of IT security services.

- Threat Hunting & OSINT activities
- Automated Network Data Exfiltration
- Penetration testing, security audits & forensics

- Hardening of Linux/Cloud Environments
- Evaluation of AI/ML/NG Security products

TRAINING PORTFOLIO:

- Open Source Defensive Security → The Trinity of Tactics for Defenders.
- Post Exploitation Adversary Simulations → Network Data Exfiltration Techniques.
- SELinux → Development & Administration of Mandatory Access Control Policy.
- Advanced RHEL/CentOS Defensive Security & Hardening.
- ModSecurity → Development and Management of Web Application Firewall rules.
- FreeIPA → Identity Management for Linux Domain Environments & Trusts.
- CISSP Exam Preparation Course

Through our hands-on labs, these training programs deliver you a bigger picture of what you really need to care about when thinking initially or later improving your overall IT security environment, operations or Red and Blue team skills. All these training descriptions are based on pure hands-on experiences where students will run every single action or chained scenarios in a 'protection vs attack' formula on his own in a dedicated virtual-lab network.

TRUE VALUES:

- Realistic 100% pure lab-oriented offensive and defensive security use cases
- Minimum theory, maximum hands-on with high level of expertise
- Effective and appropriate techniques and actions you can replay in your organization
- A lot of accumulated knowledge in one place with a focus on high priority elements
- Extending knowledge, skill sets and the mind suitable for your IT Security job positions
- Created by enthusiasts and professionals for professionals with enthusiasm

---

TARGET GROUPS:

- IT Security Professionals, Experts & Consultants
- Blue, Red & Purple Team members
- DevOps and DevSecOps Team members
- Penetration testers & Security Engineers
- Linux Experts & Administrators
- Incident Response Team members
- System Engineers & Architects
- Network & Web Application Firewall Administrators

- Open Source Security Enthusiasts

REVIEWS:

- “Excellent content, great stuff and awesome knowledge from the trainer.”
- “Excellent balance between breadth and depth of contents, great materials.”
- “Awesome 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!”
- “If you need to get deep and broad knowledge in the scope of Defensive Security using Open Source software then don't hesitate and just grab for it - definitely worth to attend and meet Leszek in person and his experience.”

DELIVERY OPTIONS:

- Public training:
    - Poland, Warsaw or Cracow
    - Germany, Berlin
    - UK, London
    - Belgium, Brussels

- Onsite training:
    - at your location, in your office

- Virtual training, live:
    - we use dedicated video conferencing technology

TRAINING CATALOG:

Open Source Defensive Security → The Trinity of Tactics for Defenders:

- Short description:
  - Advanced IT Security workshop dedicated to IT professionals in mind who need to close the gaps within Web, Linux & Network Security knowledge (A Trinity of Tactics). Very extensive and up to date training content with a focus especially on blue vs red team actions & tactics gives you the best opportunity to make stronger defensive layers inside your network infrastructures and Linux / Web application instances. Delivering real-world scenarios in our hands-on labs provide you with the very practical knowledge that is needed for expanding your Open Source Security skills: the defensive and offensive as well.

- Time duration:
  - 3 days (9:00am - 5:00pm)

- Agenda:
  - Web application security → hardened Reverse Proxy → modsecurity WAF vs HTTP security issues & attacks:
    - OSINT your org!
    - Analysis and practical use of exploits for popular web applications and bug bounty reports
    - Authorization and authentication
    - HTTPS – how to achieve a verify a A+ status?
    - Security headers and cookies
    - HTTP header anomalies
    - Full HTTP auditing
    - LUA/OpenResty support
    - Sensor approach - OWASP Appsensor
    - Web application security using Modsecurity - creating dedicated WAF rules against misconfigurations, vulnerabilities and attacks based on OWASP Top 10 and much more
    - Virtual patching
    - Web honeypots
    - Commercial & cloud WAF

  - Hardened Linux vs attacks, exploits and rootkits:
    - DAC vs MAC
    - Grsecurity / PAX vs kernel exploits
    - SELinux / Multi Category Security / sVirt
    - Apparmor, Tomoyo, Smack, RSBAC
    - SSP, NX, PIE, RELRO, ASLR vs attacks
    - Linux Containers - Docker security vs escaping
    - LKM-off / YAMA / enforcing
    - Linux capabilities vs SUID
    - System call restriction - seccomp
    - Integrity checking - IMA/EVM
    - Package security and CVE tracking

        - Debuggers and profilers - gdb / strace / ldd / Valgrind / yara
        - Chroot/jail/pivot_root vs escaping
        - Behavioral analysis - systemtap / LTTng / sysdig
        - Memory forensics - Volatility Framework vs Linux rootkits
        - PAM / 2FA / sudo_pair
        - System update vs reboot
        - Local and external enumeration + *priv checks + security auditing
        - System Auditing, integrating & accounting

    - Network Security vs attacker:
        - Vulnerability management & vulnerability scanning - understand the attacker's mind
        - Basics of Metasploit / Meterpreter / Veil
        - Basics of Linux Domain Controller - IdM / HBAC / SUDO / PKI
        - SFTP/SCP - Secure SSH Relay + SSH tips and tricks
        - Restricted shells/commands vs escaping
        - NFS (In)Security
        - Postgres / MySQL Database Hardening
        - DNS & Email Security
        - DOS / scanning / brute-force / port-knocking protection techniques
        - Advanced network firewall: iptables/nftables/ebtables
        - Network honeypots
        - Network traffic analysis - wireshark, scapy / tcpdump / tcpreplay
        - Suricata / Bro IDS vs known malware, exfiltration techniques and network attacks
        - Attack, detection and protection - Vulnhub VM challenge.

- Who should attend:
    - Linux Administrators / System Engineers & Architects
    - DevOps / DevSecOps Engineers
    - Penetration testers / Security Engineers
    - IT Security Professionals / Experts / Consultants
    - Network / Web Application Firewall Administrators
    - Blue Team members

- Training details:
    - https://defensive-security.com

SELinux - Development & Administration of Mandatory Access Control Policy.

- Short description:
    - This training is dedicated for students who want to learn in detail how SELinux really works internally, how to manage the existing policy and how to create their 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 in battle with modern exploitation techniques.

- Time duration:
  - 2 days (9:00am - 5:00pm)

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

  - 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.

  - 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

  - Analysis of targeted SELinux policy:
    - Source code analysis of RHEL / CentOS and Tresys Reference Policy
    - Types and modes
    - Filesystem locations

  - SELinux module development and compilation:
    - Syntax of m4 language
    - Classes oraz objects
    - Interfaces and macros
    - Aliases, types and attributes
    - Boolean variables definition
    - Compilation modes

  - Access Vector Cache.
  - Tools used to create and modify SELinux policy.
  - Creating SELinux users and roles.
  - Using SELinux for hardening Docker containers and cloud environments.
  - SELinux against exploits → real security use-cases.
  - SELinux tips and tricks.
  - Final project.

- Who should attend:
  - Linux Engineers
  - System Architects
  - DevOps and DevSecOps team members
  - Security Engineers

- Training details:
  - https://defensive-security.com

Post Exploitation Adversary Simulations - Network Data Exfiltration Techniques.

- Short description:
  - This training class has been designed to present students with modern and emerging tools and techniques available for network data exfiltration, testing and bypassing DLP/IDS/IPS/FW systems, protocol tunneling, hiding, pivoting and generating malicious network events. This highly technical content and only a hands-on practical approach guarantees that the usage of this transferred knowledge & technologies in real production environments will be easy, smooth and repeatable. Using an available set of tools, the student will play one by one with well-prepared exfiltration, pivoting and tunneling use-cases to generate the true network symptoms of a modern attacker's behavior. Great content for SIEM / SOC team validation.

- Time duration:
  - 3 days (9:00am - 5:00pm)

- Agenda:
  - Introduction:
    - ATT&CK Framework API.
    - Caldera
    - MAEC
    - TTP, Kill chain & defense in depth
  - Modern RAT's implementation and popular APT&C2 malware communication design → real use cases
  - TCP/UDP bind and reverse shells.
  - Bypassing, exfiltration, tunneling, pivoting, proxying and C2 techniques.
  - Cloud-based exfiltration and C2 channels.
  - Windows & Powershell exfiltration tools.
  - Just a Browser Exfiltration.
  - Hoping from air-gapped networks.
  - USB attacks and network exfiltration combo.
  - The art of data hiding → steganography examples.
  - Signature-based event analytics, rule bypassing & malicious network traffic generation.
  - Adversary simulation moves, actions, tools & automated platforms.
  - Summary → recommended defensive/protection tactics, tools and platforms.

- Who should attend:
  - Red and Blue team members
  - Security / Data Analytics
  - CIRT / Incident Response Specialists
  - Network Security Engineers
  - SOC members and SIEM Engineers
  - AI / Machine Learning Developers
  - Chief Security Officers and IT Security Directors

- Training details:
  - https://defensive-security.com

Advanced RHEL/CentOS Defensive Security & Hardening:

- Short description:
  - *Advanced RHEL/CentOS Defensive Security & Hardening* is a dedicated training about how we can protect and attack a 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 the fun. During dedicated labs, you will find out how to use different offensive and defensive tools, scripts, services and techniques to better understand how an attacker thinks and what are the most important actions of this modern adversary. Additionally, you will explore how to design secure, hardened systems and 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 an OS. This training is intended to increase skills needed to ensure data integrity on a critical system for organizations with the highest security standards. The discussed methods of automation will support the process of achieving compliance.

- Time duration:
  - 2 days (9:00am - 5:00pm)

- Agenda:
  - Introduction:
    - Defense in depth.
    - DevSecOps methodology.
    - Threat hunting.
  - Discretionary Access Control (DAC) vs Mandatory Access Control (MAC) → typical attack vectors against Linux OS, application and network services.
  - Secure file system design, attributes, flags, ACL and encryption.
  - Package management security and CVE tracking.
  - SSP, NX, PIE, RELRO, ASLR, LD_PRELOAD vs attacks.
  - The importance of SELinux:
    - Targeted policy vs exploits
    - Multi Category Security (MCS)
    - Rule Based Access Control
    - sVirt
  - Linux capabilities vs SUID attacks.
  - System call restriction - seccomp-BPF vs exploits.
  - Linux Containers - Docker security vs escaping.
  - Chroot / jail / nsjail vs escaping.
  - LKM-off / ptrace-yama / and other sysctl enforcing options.
  - Debuggers and profilers - gdb / strace / ltrace / ldd / yara.
  - Behavioral analysis and hacker’s fishing - systemtap / eBPF / sysdig.
  - Integrity checking - IMA/EVM.
  - Grub and secure boot configuration.
  - System update vs reboot.
  - Linux Domain Controller: HBAC / SUDO / RBAC.
  - PAM configuration: 2FA / sudo_pair / time-based access.
  - Secure SSH / SCP / SFTP + tips and tricks.

    - Advanced network firewall: iptables / nftables / ebtables.
    - Local and external security enumeration and reconnaissance tactics.
    - Linux visibility, auditing & accounting:
        - auditd
        - syslog
        - OSSEC
        - osquery

    - Linux Memory forensics - Volatility Framework vs malware.
    - Automation of STIG Hardening standard for RHEL/CentOS by using:
        - Ansible roles
        - Puppet manifests
        - Chef cookbooks

    - Summary and final lab.

- Who should attend:
    - Linux Administrators & Engineers from banks and financial organizations
    - DevOps / Sysops team members
    - System Architects
    - IT Security Experts and Consultants

- Training details:
    - https://defensive-security.com

FreeIPA - Identity Management for Linux Domain Environments & Trusts:

- Short 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 for 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 delve deeply 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 environments and this training will show 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 the above threats.

- Time duration:
    - 2 days (9:00am - 5:00pm)

- Agenda:
    - Introduction to domain environments.
    - Installing and configuring FreeIPA server.
    - Installing and enrolling client machines.
    - SSSD and PAM configuration.
    - User, group and role management.
    - SSO kerberos-based authentication, authorization and integration:
        - SSH
        - HTTP
        - NFS
        - Samba
        - Squid
        - Radius
        - VPN
    - 2FA, one-time password and smart card authentication.
    - DNS configuration and management.
    - HBAC - Host Based Access Control.
    - Distributed SUDO rules management.
    - SSH pubkey configuration.
    - SELinux user mapping.
    - Public Key Infrastructure - Certificate Management.
    - FreeIPA replication.
    - FreeIPA in the cloud.
    - Active Directory Trust Integration.
    - FreeBSD, Solaris, AIX and HP-UX Integration.
    - FreeIPA hardening and vulnerability scanning.
    - FreeIPA tips and tricks.
    - Summary and final lab.

- Who should attend:
    - IT Consultants and Solution Integrators
    - DevOps and DevSecOps Engineers
    - Linux and Network Engineers
    - System Administrators

- Training details:
    - https://defensive-security.com

ModSecurity → Development and Management of Web Application Firewall rules:

- Short description:
    - *ModSecurity - Development and Management of Web Application Firewall rules* is a dedicated training which helps you understand the basics and deploy later complex web application firewall rules and hardened configuration against modern flaws in your web application infrastructure. During hands-on labs we will cover in detail every

important aspect and functionality of ModSecurity vs current attacker's techniques, vulnerabilities and server misconfigurations. Various examples such as Command Execution, SSRF, SQL Injection or Cross Site Scripting are just a few of the most commonly used bugs. There are dozens of types of susceptibility. The most dangerous, however, are the so-called hybrid-attacks which are chained attacks consisting of misconfiguration or vulnerabilities in many different layers - and we want to focus on that! Within the labs we will examine features that lie in the open design of ModSecurity project: configuration, rule syntax, logs, tuning and troubleshooting. In addition to that, we will build our own dedicated rules and create virtual patches. There are also abs from other areas of application (in)security: web-based honeypots in central Reverse Proxy architecture, secure HTTP headers, Appsensor approach, Content Security Policy, HMAC, SRI, upload security, Tomcat / PHP / DB hardening and many more. The whole web application security material is preserved in a "protection vs. attack" model.

- Time duration:
  - 2 days (9:00am - 5:00pm)

- Agenda:
  - Threats are everywhere → short introduction to Web Application Security.
  - Analysis and practical use of exploits for popular web applications: Jenkins, Magento, Zimbra, PHPnuke, Joomla, Drupal, PHPmyadmin, OScommerce, Wordpress, dotProject, Bug Bounty writeups and others.

  - Hardened Apache/Nginx configuration:
    - Modules in use, path / HTTP method restrictions and file system security.
    - Secure HTTPS - how to achieve and verify a A+ status?
    - Mutual and authenticated SSL between reverse proxy and backend servers
    - Kerberos and LDAP for your web-based Single Sign On setup
    - Security headers: Content Security Policy, Cross Origin Resource Sharing / Same Origin Policy, X-Frame-Options, X-Content-Type-Options, X-XSS-Protection, Fetch API, Service Workers, SRI, Per-page sub-origins, HSTS, HPKP, PFS.

    - Cookies: Secure, Httponly, Domain, Path, Same_site, Clear Site Data Feature Policy, First-party cookies

    - HTTP header anomalies and full HTTP auditing.
    - LUA support for Apache/Nginx.
    - ModSecurity syntax, scoring, collections and logs.
    - Deep dive into OWASP CRS and tuning.
    - Sensor approach - OWASP Appsensor within ModSecurity.
    - ModSecurity rules against server misconfigurations, vulnerabilities and attacks:
      - *Injections
      - Null bytes
      - Path/directory traversal
      - LFI/RFI->Command Execution
      - Cross Site Scripting (XSS) vs CSP
      - Cross Site Request Forgery (CSRF)
      - Server Side Request Forgery (SSRF)

- HTTP Parameter Pollution (HPP)
- Open Redirect
- Insecure Direct Object Reference vs HMAC
- Forceful Browsing vs HMAC
- CSWSH - Cross Site Websocket Hijacking
- Session Security
- Brute force
- Slow DOS
- GEO restrictions
- Central Error handling
- Leakage detection
- Secure file upload
- Secure log out / forgot password form
- Web honeypots
- Bot/scan protection
- AV protection
- PHP and Tomcat Security
- MySQL / PGSQL Hardening vs data exfiltration
- Tools in use:
    - Sqlmap, sqlninja
    - Xsser
    - Dominator
    - XXEinjector
    - Skipfish
    - ZAP / Burp
    - Wafdetect
    - Joomscan, wpscan, drupwn
    - Dirbuster, dirb
    - Nikto
    - JSDetox
    - Brakeman
    - Browser plugins and others

- Central logging and hunting with ELK.
- Commercial & cloud WAF.

- Who should attend:
    - IT Consultants and Solution Integrators
    - Web Server Administrators and Hosting Providers
    - Web Application Firewall Experts
    - Linux Experts and System Engineers
    - Network Security Engineers
    - Penetration Testers
    - IT Consultants
    - SOC members

- Training details:
    - https://defensive-security.com

TRAINER:

- Leszek Miś is the Founder of Defensive Security, Principal Trainer & IT Security Architect. Recently he was a VP, Head of Cyber Security in Collective Sense - a Machine Learning Network Security Startup from the U.S. where he was responsible for product security research, strategy, business analysis & technical feature implementation and recommendation. He has over 13 years of experience in the IT security market supporting the world's largest customers in terms of exfiltration simulations and penetration tests, infrastructure hardening and general Open Source and IT Security consultancy services. In addition, he has 11 years of experience in teaching and transferring a deep technical knowledge and his own experience. He has trained 600+ students with the highest rank. He is an IT Security Architect with offensive love and a recognized expert in the enterprise OSS market.

- As a speaker, trainer or just a participant he has attended many conferences such as Brucon, OWASP Appsec USA, FloCon, SuriCon, HITB, AlligatorCon, Semafor, Exatel Security Days, Confidence, PLNOG, NGSEC, Open Source Day, SysDay, Confitura, Red Hat Roadshow, OWASP Chapter Poland, ISSA, InfoTrams.

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

CUSTOMERS:

- PGNiG, Stack Overflow, DailyMotion, 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, Biatel S.A.

CONTACT:

- Email: info@defensive-security.com / lm@defensive-security.com
- Mobile: +48 791 611 309 (Poland) / +48 791 831 018 (Poland)
- Website: https://www.defensive-security.com