Open Source Defensive Security - The Trinity of Tactics for Defenders.

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

Our high-tech workshop has a unique “protection vs attack” formula. It means that most of the security issues and use-cases we are talking about will be detected and effectively protected by the use of a suitable techniques & approach, sophisticated open source software and recommended secure configuration. We do focus on delivering a defensive content, but we understand that for being good in defense you have to understand also the opposite, offensive side. That way we are providing a kind of knowledge-mix in those fields using Open Source software.

Except for basic Linux skills and TCP/IP knowledge, most of the lab exercises require of the student at least basic understanding of what attacker’s techniques are and this is what we

are delivering too. We strongly believe that only a mix of broad, systematic Defensive and Offensive Security knowledge can guarantee secure solutions and environments. As Sun Tzu said: "Know your enemy and know yourself and you can fight a hundred battles without disaster."

KEY LEARNING OBJECTIVES → just a few examples of laboratory use-cases:

- Web Application Firewall & hardened HTTP Reverse Proxy configuration vs OWASP * and other offensive techniques
- User space and kernel space hardening vs exploitation techniques showing misconfigurations and diving into vulnerabilities details from the last past years (glibc, sudo, netlink, pp-key, waitid, PERF_EVENTS, ptrace/sysret, memppodiper, semtex, sendpage, chroot() escape, dirty_cow, many more)
- Seccomp/capabilities/namespaces vs exploits
- SELinux vs exploits (Redis Command Execution, Venom vs sVirt, Apache)
- Docker Security vs escaping techniques
- Volatility Framework vs Linux rootkits
- Linux Users Isolation and accountability, including root
- Secure SSH relays and importance of low level privileges rule
- Linux Domain Controller - centralized HBAC and sudo rules
- Sysdig / stap for detecting deviations in syscall's behavior of daemons and services
- Network packet filtering including TOR, ipsets, IP reputation, port knocking
- Network honeypots vs scanning tools and detection techniques
- PCAP analysis and Deep Packet Inspection vs malware
- Sandboxing for malware detection and deep analysis (cuckoo, yara)
- and many more

Through hands-on lab this training delivers you a bigger picture of what you really need to care about when thinking initially or improving lately your overall IT environment or Red and Blue team skills. All the above training description is based on pure hands-on where student will run every single action or chained scenarios in 'protection vs attack' formula on his own in dedicated virtual-lab network.

WHO SHOULD ATTEND:

- Linux Administrators / System Engineers & Architects
- Penetration testers / Security Engineers
- IT Security Professionals / Experts / Consultants
- Network / Web Application Firewall Administrators
- Blue Team members

PREREQUISITE KNOWLEDGE:

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

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 mind suitable for your IT Security job positions
- Created by enthusiasts and professionals for professionals with enthusiasm

FULL AGENDA:

1. Threats are everywhere - introduction to technical Open Source Defensive Security program.
2. Web application security -> hardened Reverse Proxy -> modsecurity vs HTTP security issues:
    a. Analysis and practical use of exploits for popular web applications: Jenkins, Magento, Zimbra, PHPnuke, Joomla, Drupal, PHPmyadmin, OScommerce, Wordpress, dotProject and others

    b. Authorization and authentication: CAS SSO, OAuth, SAML (ipsilon), Federation, Basic / Digest Auth, SSL authentication, LDAP authorization, SAML based - mod_auth_mellon, Kerberos based - mod_auth_kerb, Login-form based - mod_intercept_form_submit, mod_lookup_identity, mod_pubcookie

    c. HTTPS – how to achieve a verify a A+ status?:

i. Attacks:
    - Heartbleed
    - Breach
    - Drown
    - Beast
    - Poodle
    - MiTM: sslstrip, bettercap, arpspoof

ii. How to configure mutual SSL between reverse proxy and application servers?

d. 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, Sub-Resource Integrity, Per-page sub-origins, Content Security Policy (CSP), HSTS, SOP / Cross Origin Resource Sharing (CORS), HPKP, PFS

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

f. HTTP header anomalies
g. Virtual patching
h. Full HTTP auditing
i. LUA/OpenResty support
j. Sensor approach - OWASP Appsensor
k. Web application security using Modsecurity - creating dedicated WAF rules against misconfigurations, vulnerabilities and attacks:
    i. *Injections
    ii. Null bytes
    iii. Path/directory traversal
    iv. LFI/RFI->Command Execution
    v. Cross Site Scripting (XSS) vs CSP
    vi. Cross Site Request Forgery (CSRF)
    vii. HTTP Parameter Pollution (HPP)
    viii. Open Redirect
    ix. Insecure Direct Object Reference vs HMAC
    x. Forceful Browsing
    xi. CSWSH - Cross Site Websocket Hijacking
    xii. Session Security
    xiii. Brute force
    xiv. Slow DOS
    xv. GEO restrictions
    xvi. Error handling
    xvii. Leakage detection
    xviii. Secure file upload
    xix. Secure log out / forgot password form
    xx. Web honeypots

xxi. Bot/scan protection
xxii. AV protection
xxiii. PHP Security
xxiv. Tomcat Security
xxv. Tools:
- Sqlmap, sqlninja
- Xsser
- Dominator
- XXEinjector
- Skipfish
- ZAP / Burp
- Wafdetect
- Joomscan, wpscan, drupwn
- Dirbuster, dirb
- Nikto
- JSDetox
- Brakeman
- And others

xxvi. Commercial & cloud WAF

3. Hardened Linux vs exploits/rootkits:
   a. Discretionary Access Control (DAC) vs Mandatory Access Control (MAC)
   b. Grsecurity / PAX
   c. SELinux / Multi Category Security / sVirt
   d. Apparmor, Tomoyo, Smack, RSBAC
   e. SSP, NX, PIE, RELRO, ASLR vs attacks
   f. Linux Containers - Docker security vs escaping
   g. LKM-off / yama-ptrace / sysctl enforcing options
   h. Linux capabilities vs SUID attacks.
   i. System call restriction - seccomp-BPF.
   j. Integrity checking - IMA/EVM
   k. Package mgmt security and CVE tracking
   l. Debuggers and profilers - gdb / strace / ldd / valgrind /yara
   m. Chroot/jail/pivot_root vs escaping
   n. Behavioral analysis - systemtap / LTTng / sysdig / eBPF
   o. Memory forensics - Volatility Framework vs malware
   p. PAM / 2FA / sudo_pair
   q. System update vs reboot
   r. Local and external enumeration + *privchecks + security auditing
   s. System Auditing, integrating & accounting:
      i. *syslog
      ii. Auditd
      iii. OSSEC / Samhain / aide
      iv. SIEM: Splunk / (H)ELK / OSSIM / osquery

4. Network security:

a. Vulnerability scanning:
    i. Nmap NSE
    ii. Seccubus
    iii. OpenVAS
b. Metasploit / Meterpreter / Veil
c. Linux Domain Controller - IdM / HBAC / SUDO / PKI
d. SFTP/SCP - Secure SSH Relay + SSH tips and tricks
e. Restricted shells/commands vs escaping
f. NFS (In)Security
g. Postgres / MySQL Database Hardening
h. DNSSEC
i. Email Security
j. DOS / scanning / brute-force / port-knocking protection techniques
k. Advanced network firewall: iptables/nftables/ebtables
l. Network honeypots.
m. Network traffic analysis - wireshark, scapy / tcpdump / tcpreplay
n. Suricata / Bro IDS vs known malware and attacks:
    i. Metasploit,
    ii. Pass The Hash
    iii. Heartbleed
    iv. Shellshock and many others
o. Security by obscurity

5. Attack, detection and protection - Vulnhub VM challenge.
6. Summary: offense vs defense.

TIME DURATION:

- 3 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 trainings:

    - Post Exploitation Adversary Simulations - Network Data Exfiltration Techniques
    - Open Source Defensive Security (OSDS)
    - ModSecurity → Web Application Firewall vs attacks
    - FreeIPA → Centralised Identity Management System for Linux Environment (Linux Domain Controller)
    - SELinux - Creating and managing of SELinux policies
    - Advanced RHEL/Centos Defensive Security & Hardening

- 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, HITB, 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
- Biatel

CONTACT:

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