TRAINING OVERVIEW:

“In & Out - Detection of Network Exfiltration and Post-Exploitation Techniques - BLUE EDITION" is an advanced lab-based training created to present participants:

- Significance of security events correlation including context to reduce the number of false positives and better detection of adversary activities
- Advanced detection methods and techniques against exfiltration and lateral movement including event mapping, grouping and tagging
- Understand tactics and behaviours of the adversary after gaining initial access to the network (Linux/Windows)
- Detection methods of tunnelling, hiding, pivoting and custom, simulated malicious network events
- Capabilities of many popular Open Source tools and integration with 3rd party security (IDS/IPS/WAF/EDR) and analytics solutions against adversaries actions
- Verification methods and techniques for product and service providers from IT Security space → in terms of internal testing and PoC / PoV programs

The main goal of the workshop is to achieve better detection of post-exploitation activities and more effective incident handling, thus allowing to reduce the number of false positives in the SOC environment. Individual detection lab cases will be launched and analyzed together in details by finding new and using existing DFIR artifacts. A modular lab-oriented form of the training allows for a later use and combination within your own SOC infrastructure, expanding and delivering complex tactics, techniques and procedures (TTP).

Individual artifacts of "RED" actions will be linked, properly characterized, tagged and grouped taking into account the level of criticality, mapping to the MITRE ATT&CK Framework and chain-linking events/pieces of evidence that make up a given security incident.

The workshop is filled with substantive examples / contextual insertions from the community world of Threat hunting, Blue / Red, including the source of origin.

The entire training is based on a purely practical laboratory in which the student independently performs each action or related scenarios in a dedicated virtual laboratory network. This class focuses on x86 / x64 architecture, IPv4 / IPv6 networks and targets distributed Linux and Windows environments (AD 2016, 10, 7).

In terms of IDS / IPS / Data Leakage Protection and for a better understanding of the current status of your network security position, training experience will help you understand the risks, identify dead points of your network security and undiscovered infrastructure spaces by simulating and detecting the actions of a real cyber-threat actor.

The proposed training BLUE agenda - in the defensive edition - is a natural continuation of the first → offensive (RED) edition of the training. Highly technical content and only a practical approach guarantees that the use of the transferred knowledge and technologies in real production environments will be easy, smooth and repeatable.

Make sure your network's security really works!

SHARED LAB INFRASTRUCTURE:

- Build on top of powerful dedicated servers: Intel® Xeon® W-2145 Octa-Core Skylake W, 128GB RAM, SSD, 1 GBit/s port

- Training environment includes: AD Domain Controllers, Windows / Linux clients, vSPAN, vNetflow, IDS/IPS, log aggregators and collectors, system instrumentation, monitoring, and analytics solutions, Storage, Firewall, Proxy server, Jump host

- Software in use: Volatility Framework, yara, ssdeep, osquery, Graylog, Wazuh / OSSEC, docker, ngrok, ELK, Splunk, Sigma, hydra, kerbrute, SysInternals, PowerSploit, PowerView, DOSFuscation, ntlmrelayx, Bloodhound, goDoH, ssh, BRO IDS, Suricata, sysdig, eBPF, audit, OpenVswitch, dnscat2, tcpreplay, wireshark, tcpdump, nmap, Empire Framework, Metasploit Framework, WMImplant, syslog, Invoke-PipeShell, Sharpshooter, plink, dsquery, adexplorer, PIngCastle, ngrep, print.exe, Shellter and many others

---

IF YOU ARE LOOKING TO:

- Learn ways to improve your detection and event correlations skills across many different data sources

- Find the malicious activities and identify threats details on the network
- Prepare your SOC team for fast filtering out network noise and allow for better incident response handling
- Profile your critical OS and network segments in terms of ‘normal vs exotic’ behaviour
- Find out how DFIR / IR Open Source Software can support your SIEM infrastructure
- Learn current trends, techniques, and tools for network exfiltration and lateral movements
- Understand the value of DLP / IDS / IPS / FW / WAF / Memory Forensics against real adversary lab scenarios
- Understand values from an automated approach to simulating attackers and generating anomalies
- Identify blind spots in your network security posture
- Then this training is for you!

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

PREREQUISITE KNOWLEDGE:

- An intermediate level of command line syntax experience using Linux and Windows
- Fundamental knowledge of TCP/IP network protocols
- Penetration testing experience performing enumeration, exploiting, and lateral movement is beneficial, but not required
- Basic programming skills are a plus, but not essential

HARDWARE / SOFTWARE REQUIREMENTS:

- At least 40GB 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

WHAT WILL STUDENTS BE PROVIDED WITH:

- Access to a dedicated cloud-based environment.
- Dedicated VPS access per student.
- VM images.
- Slides in electronic format (PDF).
- Lab Instructions.
- Slack channel access.

AGENDA:

DAY 1:

1. The value behind Adversary Simulations.
2. Introduction to network events analysis → PCAP Exfiltration CTF-style challenge.
3. MITRE Attack Framework for APT detection.
4. Open Source Security Software for your Security Operation Center - introduction to cloud-based LAB environment and more
    a. ElastiFlow / ipt_netflow
    b. Open vSwitch
    c. Bro IDS / Suricata IDS
    d. Moloch
    e. Wazuh
    f. Graylog
    g. Auditd / go-audit
    h. eBPF
    i. OSquery / Kolide
    j. Volatility Framework
    k. Splunk / Elastic Stack / HELK / Mordor
    l. Sysmon:
        i. Process execution events
        ii. Network connection events
        iii. Image load events
        iv. Named pipe events
        v. WMI events
        vi. PSexec events
        vii. Process Explorer
        viii. Process Monitor
        ix. Autoruns

x. Evidence traces of file download and execution:
    1. cmd.exe
    2. HTA
    3. JS
    4. VBS
    5. WSF
    6. JSE
    7. CSharp
    8. certutil
    9. Powershell
    10. Bitsadmin
    11. WebDAV / SMB / NFS share mapping

m. MISP + theHive
n. Vagrant / Packer / Terraform

5. Network baseline profiling and hunting for malicious events:
    a. Playing with BRO IDS / Suricata IDS for anomaly detection → finding malicious artifacts at the network level:
    b. The importance of network baseline for high-risk environments
    c. Virtual SPAN / TAP and Netflow → OpenVswitch
    d. Feature definition and extraction
    e. Bro-cut syntax
    f. Bro Script Index
    g. Client/server Fingerprinting:
        i. JA3
        ii. HASSH
    h. Security feature extraction per many different network protocols

6. Finding malicious artifacts using yara and ssdeep:
    a. How yara works and why it could be your best friend
    b. Yarascan + Volatility Framework vs Linux rootkits
    c. Yara vs webshells

DAY 2:

7. Low-level analysis of chained Sigma rules + Sysmon for better lateral movement detection:
    a. Application
    b. APT
    c. Linux
    d. Network
    e. Proxy
    f. Web

g. Windows

8. Low-level Linux security tracing and profiling for critical services:
    a. eBPF
    b. sysdig
    c. systemtap

9. Detection and traces of network exfiltration techniques → use cases:
    a. ICMP
    b. TCP / UDP
    c. SSL / TLS
    d. DNS / DoH / DGA / anomalies
    e. HTTP / HTTP2 / QUIC
    f. LDAP Exfil
    g. Dropbox / Twitter / Gmail / Mozilla
    h. SMB bind named pipes
    i. Legitimate website covert channel
    j. Port knocking
    k. Domain fronting
    l. ngrok
    m. SSH Tunneling and pivoting
    n. RDP Tunneling and pivoting / RDP Inception
    o. Egress testing and common network traffic on non-standard ports

---

DAY 3:

10. Detection and traces of post-exploitation, lateral movements → use cases:
    a. AD Reconnaissance / AD Snapshot
    b. Bloodhound artifacts
    c. Golden Ticket
    d. Silver Ticket
    e. Kerberoasting
    f. RPC over TCP/IP
    g. DCsync / DCShadow
    h. Mimicatz agent/server
    i. Pass The Hash
    j. SMBexec
    k. Invoke-WMI
    l. Invoke-PSexec
    m. PSRemoting
    n. RDP wrapping
    o. Offensive Powershell:
        i. WMI multiple sessions
        ii. Remote network relaying

iii. Copy VSS
iv. Keylogging
v. LSA secrets extraction
vi. Sandbox / virtual environment detection
vii. UAC bypassing

p. Poisoning LLMNR, NBT-NS, MDNS, WPAD and WSUS
q. SMB ransomware detection.
r. Browser pivoting.

11. Windows Malware Persistence Methods:
    a. Service
    b. Winlogon registry entries
    c. Run / RunOnce
    d. Scheduled Tasks
    e. Startup Folder
    f. WMI
    g. DLL

12. Linux Malware Persistence Methods:
    a. Service
    b. Startup scripts
    c. SSH magic password
    d. Port knocking / iptables
    e. Kernel modules

13. Summary.

DURATION:

- 3 days of very intensive training

REVIEWS:

- “It's been a while since I was so excited (like during #LockedShield2018). Together with group of secfreaks we had an opportunity to bring into play intensive scenarios and step into adversaries' shoes. I don’t remember when I exfiltra… took away so much knowledge. Actually is better to simply turn off computers. But try harder.”

- “Thank You for the training. It was not only very informative but also eye opening. At first you start with thick book of well-prepared theory which you don’t have time to read because you are doing 25+ lab’s and get another 25 for homework.”

- “One of the best security exfiltration training so far! Lots of fun & learning! If you want to learn how hackers think and what kind of tooling they use - this is it!”

- “That was one of the most exciting Security trainings I have attended in the last few months. The scope of the training materials and Leszek’s approach are so great that I would like to spend more time to study the In & Out - Network Exfiltration Techniques.”

- “Lots of hands-on labs. The trainer was very helpful and knowledgeable.”

- “Thank you very much for delivering out a valuable workshop on data exfiltration techniques. The team is extremely impressed with the knowledge you present, as well as how easily you presented a very advanced topics. We have gained many useful cases that we will certainly use in practice. Thanks once again and respect!”

- “I wanted my team to experience something new, different ... I wanted SOC analysts to learn practical ways to bypass security and data exfiltration and learn to detect them and learn the techniques of attackers who could already break the security and work inside. And then Leszek appeared. We did not need a single coffee for three days! Leszek shared great knowledge with us in a very accessible way. Materials, pictures, scenarios - everything prepared and working. Thank you Leszek Miś! Highly recommend !!!”

- “Excellent content, great stuff and awesome knowledge from the trainer.”
- “Excellent balance between breadth and depth of contents, great materials.”
- “Awesome @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), Principal Trainer and Security Researcher with over 15 years of experience in Cyber Security and Open Source Security Solutions market. He went through the full path of the infosec carrier positions: from OSS researcher, Linux administrator and system developer, Solution Engineer, DevOps and CI, through penetration tester and security consultant delivering hardening services and training for the biggest players in the European market, to become finally an IT Security Architect / SOC Security Analyst with deep non-vendor focus on Network Security attack and detection. He’s got deep knowledge about finding blind spots and security gaps in corporate environments. Perfectly understands technology and business values from delivering structured, automated adversary simulation platform.

- Recognized speaker and trainer: BruCON 2017/2018, Black Hat USA 2019, OWASP Appsec US 2018, FloCon USA 2018, Hack In The Box Dubai / Amsterdam / Singapore / Abu Dhabi 2018/2019, 44CON UK 2019, Confidence PL, PLNOG, Open Source Day PL, Secure PL, Advanced Threat Summit PL

- Member of OWASP Poland Chapter.

- Author of many IT Security training:

    - Open Source Defensive Security → The Trinity of Tactics for Defenders
    - In & Out → Network Exfiltration and Post-Exploitation Techniques [RED EDITION]
    - In & Out → Detection of Network Exfiltration and Post-Exploitation Techniques [BLUE EDITION]
    - System Internals – Network, OS and Memory Forensics
    - 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

- Holds many certifications: OSCP, RHCA, RHCSS, Splunk Certified Architect.

- His areas of interest include network “features” extraction, OS internals and forensics. Constantly tries to figure out what the AI/ML Network Security vendors try to sell. In free time he likes to break into “IoT world” just for fun.

- Still learning hard every single day.

CONTACT:

- Email: info@defensive-security.com
- Mobile: 0048 791 611 309 (Poland) / 0048 791 83 10 18
- Website: https://www.defensive-security.com