In & Out - Network Exfiltration and Post-Exploitation Techniques.

SHORT TRAINING DESCRIPTION:

The In & Out - Network Exfiltration and Post-Exploitation Techniques [RED Edition] training class has been designed to present students modern and emerging TTPs available for network exfiltration and lateral movement phases. Highly technical content and only a hands-on practical approach guarantees that the usage of this transferred knowledge & tactics in real production environments will be easy, smooth and repeatable.

This 3 days, fast-track training course requires from students a fundamental knowledge of Linux and Windows internals, TCP/IP, strong focus and desire to learn.

WHO SHOULD TAKE THIS COURSE:

- Red and Blue team members
- SOC Analysts and SIEM Engineers
- Security / Data Analysts
- Pentesters and Risk Auditors
- CIRT / Incident Response Specialists
- Network Security Engineers
- AI / Machine Learning Security Developers
- Chief Security Officers and IT Security Directors

GOAL:

- “Gain more visibility and become confident that your SOC / network security really works!”

DIGGING DEEPER:

Through hands-on labs only, this training will deliver you a bigger picture of what you really need to care about when thinking initially or improving lately your Security Operation Center environment, Red and Blue team skills, your SIEM / data analytics deployments, your DLP / IDS / IPS installations or anomaly detection network security solutions.

Using available set of tools, the student will play one by one with well prepared lateral movement, exfiltration, pivoting and tunneling use-cases to generate the true network symptoms of modern adversary behavior.

Next to that, we will deep dive into the individual network protocols, services and post exploitation techniques commonly in use and discuss the detection points.

The workshop should perfectly power up your skills in field of adversary simulations and advanced threat detection.

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

- Simulate real adversaries in the network by using dedicated Open Source projects and techniques including LDAP as hidden storage, AD as C2, DCSync / DCShadow, Pass The Hash / The Ticket, remote creds dumping, registering a protocol handler remotely and many more.

- Bypass Linux and Windows local security restrictions and command line arguments detections by using obfuscation and Living Off The Land Binaries And Scripts

- Generate and run different, encrypted types of TCP/UDP reverse and bind shells across Windows and Linux systems, pivot to the next subnets, configure port forwarding & C2 proxying, change a transport on the fly and find what the network traffic artifacts of such actions are.

- Manually generate suspicious network events from Python, ex. establish a C2 connection by using QUIC, HTTP2, NTP and more.

- Simulate DNS DGA traffic, run a DNS tunnels and remote shells, exfiltrate and hide data transfer using DNS-over-HTTPS, deliver payload over AXFR or pwn the local Docker API over DNS Rebinding

- Setup a perfect implant jitter, connection time-outs and how to blend your C2 channel into the normal traffic

- Use different HTTP techniques, headers and methods for stealing the data with combination of web application injection techniques (OOB) + walk through the world of web shells

- Run, detect and understand a different TLS/SSL-based anomalies, exfiltration methods and hide behind chosen JA3 hash

- Create remote thread and deliver compressed and encrypted, in-memory offensive Powershell scripts during a post-exploitation stage for leaking the data and bypassing AV / EDR / AMSI

- Clone, armor and phish popular websites and use them for covert channel

- Create CDN domain fronting setup, punch holes in the NAT and run WAF filtering rules for C2 payload traffic

- Achieve a big file ICMP packet dripping covert channel and monitor ICMP traffic

- Bypass and pivot at scale by running internal HTTPS, WMI, Websockets, named pipes, WinRM and P2P covert channels

- Use a popular cloud-based services for C2 communication and data stealing, ex. Pastebin, Twitter, AWS, Dropbox, Google Drive.

- Run verification actions for IT security products and providers during PoC / PoV

- Discuss how Suricata IDS / Zeek IDS / Netflow / Sysmon / OSquery and Sigma rules can help you detect and correlate suspicious events

- And a combination of many more.

I guarantee, that your overall Linux, Windows and "feeling the network security" skills will also increase significantly.

HW / SW REQUIREMENTS:

- At least 30GB 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 STUDENTS ARE PROVIDED WITH:

- Slides in electronic format (PDF).
- Lab Instructions.
- VM images.
- Dedicated VPS access per student.

AGENDA - SHORTER VERSION:

1. Introduction to Adversary Simulations and Open Source Attack Emulation projects.
2. Modern RAT's implementation and popular APT/C2 malware communication design - the review of the latest APT campaigns mapped to MITRE ATT&CK Framework.
3. Not just the basics of TCP/UDP bind and reverse shells.
4. Covert channels and C2 techniques.
5. Lateral movement and Offensive Frameworks.
6. Cloud-based exfiltration techniques and C2 channels.
7. FW / WAF protection for your C2 infrastructure.
8. Signature-based event analytics, rule bypassing & malicious network traffic generation.
9. Summary → recommended defensive/protection tactics, tools and commercial platforms.

FULL AGENDA:

1. Introduction to Adversary Simulations and Open Source Attack Emulation projects:
    a. Atomic Red Team
    b. RTA
    c. APT simulator
    d. Dumpster Fire
    e. Firebolt
    f. Flightsim
    g. BYOB
    h. Metta
    i. Infection Monkey
    j. Caldera
    k. and more

2. Modern RAT's implementation and popular APT/C2 malware communication design - the review of the latest APT campaigns mapped to MITRE ATT&CK Framework and Sigma rules.

3. Not just the basics of TCP/UDP bind and reverse shells:
    a. Meterpreter + Veil Framework + Shellter + Sharpshooter + Empire:
        i. Generating staged / stageless exotic payloads
        ii. Powershell & cmd.exe obfuscation
        iii. Auditing and bypassing firewalls
        iv. Routing, relaying, pivoting & port forwarding
        v. and more

    b. CLI / LOLBAS tips & tricks:
        i. netcat / nc / cryptocat / telnet / socat / curl / wget / xxd / rsync
        ii. /dev/tcp & /dev/udp
        iii. installutil / regsvr32 / regsvcs / regasm / print / msbuild / installutil
        iv. PHP / Perl / Python / Ruby / JSP / ASP / LUA / awk shellz
        v. and more

    c. TCP/UDP raw socket tunnels.
    d. Establish your own C2 communication channels by using:
        i. Covenant
        ii. Koadic
        iii. PoshC2
        iv. Apfell
        v. Faction C2
        vi. C3
        vii. and more

4. Covert channels and C2 techniques:
    a. ICMP
    b. DNS:
        i. CDN theory, domain fronting and domain reputation
        ii. Fast-flux domains
        iii. Dictionary and random characters DGA
        iv. DNS proxy, DNS over HTTPS, DNS over TLS
        v. Payload delivery over AXFR
        vi. DNS Rebinding and other DNS anomalies

    c. HTTP/S & web application exploitation techniques combo:
        i. HTTP methods / headers / cookies / redirects / error codes
        ii. Chunked Transfer Encoding
        iii. Website cloning and armoring

        iv. WebDAV and Websockets C2
        v. Certificate exfiltration & TLS/SSL anomalies
        vi. *Injections + exfiltration → OOB
        vii. Webshell as SOCKS proxy
        viii. QUIC / HTTP2
        ix. HTTP anomalies

5. Lateral movement and Offensive Frameworks:
    a. AD as C2 / LDAP as hidden storage
    b. DCShadow / DCsync
    c. Golden / Silver Ticket
    d. Kerberoasting
    e. NTLM relaying and redirects
    f. UNC paths
    g. RDP tunneling
    h. Credential dumping at scale
    i. WMI / WinRM / PS-remote
    j. Storage protocols: FTP / TFTP / SMB / NFS / iSCSI
    k. Forward / Reverse / SOCKS Proxy
    l. SSH tunneling / SFTP / SCP
    m. VPN / TOR / Open Proxy
    n. POP3 / SMTP / IMAP
    o. + chaining of aboves and many more.

6. Cloud-based exfiltration techniques and C2 channels:
    a. Slack as C2
    b. SSH over Google Drive
    c. Pastebin as C2

7. FW / WAF protection for your C2 infrastructure
8. Signature-based event analytics, rule bypassing & malicious network traffic generation:
    a. Suricata ET / VRT rules vs attacker → the syntax of the rules
    b. Bro IDS log “features” for deep low-level network baselining and “weird” findings
    c. Threat Intelligence feeds, lists and 3rd party APIs:
        i. IP reputation lists
        ii. Malware / Phishing feeds
        iii. C2 / Open Proxy lists / TOR exit-nodes
        iv. Censys / VT / Passive Total / Shodan

9. Summary → recommended defensive/protection tactics, tools and commercial platforms:
    a. TTP, Kill chain & Defense and Offense in depth.

b. The importance of:
    i. Network traffic baseline profiling
    ii. Memory forensics
    iii. Important data sources and log correlation
    iv. Open Source Security Projects for SOC environment

TRAINING KEYWORDS:

- impacket, pyexfil, scapy, metasploit/meterpreter, Veil Framework, Sharpshooter, Shellter, proxychains, poshC2, dns2tcp, pupy, tcpreplay, suricata, bro IDS, sg1, nmap, DET, xfltreat, pytbull, wireshark, tcpdump, sysdig, hping, fruityC2, tuna, RATTE, Powersploit, PowerShell Empire, nishang, corkscrew, Egress-assess, pivoter, hydra, wondjina, Trevor C2, C3, Koadic, Apfell, sharpSocks, WSC2, google_socsk, sqlmap, BeeF Framework, twittor, torify, TheFatRat, cloakify, WMIsploit, certreq, SSH, ngrep, nping, iptables, Faction C2, Merlin, ThunderShell, udp2raw, Volatility Framework, SILK, EvilURL, Katoolin, PowerLessShell, reGeorg, rpivot, WSC2, NativePayload_IP6DNS, dnsmasq, thc-flood, knockd, dnstwist, yersinia, DNSexfiltrator, SMBmap, testssl, firebolt, dumpster fire, APT simulator, cuckoo, moloch, icmptunnel, Invoke-DOSfuscation, ChunkyTuna, transmission, openvswitch, ngrok and more.

REVIEWS:

- “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!”

- “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.”

- “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 DevOps, 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

- 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