NASZE PODEJŚCIE DO EDUKACJI CYBERBEZPIECZEŃSTWA:

Programy warsztatów i zaawansowanych szkoleń technicznych w Defensive Security przygotowaliśmy bazując na podejściu “ochrona przeciwko atakowi”, które z powodzeniem pozwolą osiągnąć silniejsze poziomy obrony oraz skuteczniejsze wykrywanie incydentów w rozbudowanych środowiskach IT. Przekazywana wiedza praktyczna pozwala lepiej zrozumieć podejście współczesnych przeciwników, ich styl myślenia ofensywnego, techniki i oraz używane narzędzia. Wszystkie z oferowanych programów szkoleniowych posiadają unikalną formułę "ochrona przeciwko atakowi". Oznacza to, że podczas ćwiczeń laboratoryjnych większość problemów związanych z bezpieczeństwem, czyli omawianych przypadków ataków i nadużyć zostanie wykryta i skutecznie zabezpieczona za pomocą odpowiednich technik, podejść, zaawansowanych narzędzi oraz zalecanych konfiguracji utwardzających.

W Defensive Security skupiamy się na dostarczaniu treści dt. ochrony i utwardzania, lecz jesteśmy świadomi, że poznanie ofensywnej strony jest w tym przypadku równie istotne. W ten sposób zapewniamy pewnego rodzaju mieszankę wiedzy z bezpieczeństwa sieci, systemu operacyjnego oraz aplikacji webowych pod kątem zaawansowanego ataku i ochrony wykorzystując do tego celu wyłącznie wyselekcjonowane oprogramowanie Open Source.

Sun Tzu powiedział: "Jeśli poznasz siebie i swego wroga, przetrwasz pomyślnie sto bitew." i jest to podejście, które stosujemy podczas budowania i dostarczania warsztatów technicznych od wielu lat.

DOŚWIADCZENIE:

a. Leszek Miś – główny trener w Defensive Security posiadający autoryzowane certyfikacje, wśród których wymienić należy:
   - Offensive Security Certified Professional (OSCP)
   - Red Hat Certified Architect (RHCA)
   - Red Hat Certified Security Specialist (RHCSS)
   - Red Hat Certified Data Center Specialist (RHCDS)
   - Red Hat Certified Virtualization Administrator (RHCVA)

- Red Hat Certified Engineer (RHCE)
- Red Hat Certified Instructor (RHCI)
- Comptia Security+
- Splunk Certified Architect

b. Kompetencje:
   - W latach 2015-2018 pracował w amerykańskim start-upie Collective Sense jako VP, Head of Cybersecurity, gdzie zajmował się głównie badaniami nad bezpieczeństwem sieci, analizą kampanii APT, wykrywaniem anomalii oraz analizą behawioralną środowiska sieciowego, analizą biznesową i strategiczną firmy, a także wdrażaniem nowych funkcjonalności technicznych do produktu z zakresu bezpieczeństwa sieci, systemu operacyjnego oraz aplikacji webowych.
   - Ponad 15 lat doświadczenia z zakresu technologicznego bezpieczeństwa IT i zarządzania systemami Linux.
   - Uznany ekspert korporacyjnych rozwiązań Open Source.
   - 11 lat doświadczenia w nauczaniu i przekazywaniu wiedzy technicznej (ilość przeszkolonych osób: 600+, średnia ocena pracy trenera w skali 1-5: 4.9).
   - Nadzoruje projekty i rozwija ofertę IT Security.
   - Specjalizuje się w Network Security oraz w defensywnym podejściu do bezpieczeństwa systemu Linux oraz platform webowych. Pasjonat OSINT.
   - Znany i ceniony trener i egzaminator Red Hat w Polsce. Prowadził szkolenia i egzaminy ze ścieżki Red Hat Certified Architect / RHCSS / RHCE.
   - Autor wielu warsztatów z zakresu IT Security (Open Source Defensive Security, Modsecurity, FreeIPA, SELinux, Linux Hardening).
   - Prelegent na wielu konferencjach: Brucon BE, Flocon US, Hack In The Box Dubai, OWASP Appsec US, Confidence, PLNOG, NGSec, Sysday, Open Source Day, Confitura, Red Hat Roadshow, OWASP Poland Chapter, ISSA Infotrams.
   - Zrzeszony członek ISSA Polska oraz OWASP Poland.
   - Profil LinkedIN: https://www.linkedin.com/in/crony/

PRAWDZIWE WARTOŚCI:

- Realistyczne, w 100% laboratoryjne, ofensywne i defensywne przypadki
- Minimalna ilość teorii, maksymalna ilość ćwiczeń praktycznych
- Skuteczne i odpowiednie techniki i taktyki, które możesz powtórzyć w swojej organizacji

- Mnóstwo wiedzy zgromadzonej w jednym miejscu, ze szczególnym uwzględnieniem obszarów krytycznych
- Poszerzanie świadomości i umiejętności z zakresu bezpieczeństwa sieci pod kątem eksfiltracji oraz działań posteksploitacyjnych
- Program stworzony przez profesjonalistów i entuzjastów dla profesjonalistów z entuzjazmem

---

OPINIE:

- "Doskonałe treści, świetne przypadki i niesamowicie obszerna wiedza trenera."
- "Doskonała równowaga między szerokością i głębokością treści, doskonałe materiały".
- "Extra szkolenie, wiele się nauczyłem! Miło było Cię poznać."
- "Bardzo dobry kurs, instruktor był bardzo kompetentny i odpowiedział na wszystkie nasze pytania. Kurs przekroczył moje oczekiwania, świetna robota! "
- "Jeśli chcesz zdobyć głęboką i szeroką wiedzę z zakresu defensywnego bezpieczeństwa przy pomocy oprogramowania Open Source, nie zwlekaj - zdecydowanie warto przyjechać, poznać Leszka osobiście oraz jego doświadczenie."
- “Chciałem aby mój zespół doświadczył czegoś nowego, innego... Chciałem, żeby analitycy SOC w praktyczny sposób poznali wyszukane sposoby na omijanie zabezpieczeń i eksfiltrację danych i żeby nauczyli się je wykrywać oraz poznali techniki atakujących, którzy mogli już przełamać zabezpieczenia i działają w środku. I wtedy pojawił się Leszek. Przez trzy dni warsztatów nie potrzebowaliśmy ani jednej kawy! Leszek podzielił się z nami ogromną wiedzą w bardzo przystępny sposób. Materiały, laby, scenariusze - wszystko przygotowane i działające. Dziękuję Leszek Miś! Polecam!!!”
- “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 very advanced topics. We have gained many use cases that we will certainly use in practice. Thanks once again and respect"

KLIENCI:

- PZU
- ING Tech
- PGNiG
- Integrated Solutions
- Warta
- Orange Polska (CERT)
- AXA
- Europejski Organ Nadzoru Globalnego Systemu Nawigacji Satelitarnej

- 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

O WARSZTACIE:

“In & Out - Detection of Network Exfiltration and Post-Exploitation Techniques - BLUE EDITION" to zaawansowany warsztat stworzony w celu zaprezentowania uczestnikom:

- sposobów wykrywania technik i narzędzi służących do eksfiltracji i wykradania danych z uwzględnieniem mapowania zdarzeń do uznanych metodologii
- zrozumienia taktyk i zachowań przeciwnika po uzyskaniu dostępu do sieci pod kątem generowanych artefaktów sieciowych, zdarzeń systemowych oraz logów
- możliwości wykorzystania narzędzi Open Source z rodziny IDS / IPS / WAF w walce z działaniami intruzów oraz ich integracji z narzędziami analitycznymi
- mechanizmów i sposobów detekcji tunelowania protokołów, ukrywania i generowania złośliwych zdarzeń sieciowych
- istotności korelacji zdarzeń z uwzględnieniem kontekstu celem zmniejszenia ilości występujących false positive-ów
- technik weryfikacji produktów i dostawców usług z obszaru IT Security

Podstawowym celem warsztatu jest osiągnięcie lepszej detekcji działań “po ataku” oraz skuteczniejszej obsługi i zrozumienia incydentów pozwalając tym samym na zmniejszenie ilości występujących false positive-ów w środowisku SOC. Poszczególne przypadki laboratoryjne zostaną wspólnie uruchomione i szczegółowo przeanalizowane pod kątem występujących artefaktów, a modularna postać laboratoryjna pozwoli na ich późniejsze wykorzystanie oraz kombinację z uwzględnieniem własnych, skomplikowanych taktyk,

technik i procedur (TTP).

Poszczególne artefakty działań typu “RED” zostaną powiązane, odpowiednio scharakteryzowane, otagowane i pogrupowane z uwzględnieniem poziomu krytyczności, mapowania do ATT&CK Framework oraz łańcuchowania zdarzeń i dowodów składających się na dany incydent bezpieczeństwa.

Elementem integralnym warsztatu będzie quiz DFIR składający się z przedstawienia rzeczywistych przypadków podejrzanych działań w postaci artefaktów offline.
Zadaniem uczestników będzie wspólne wypracowanie teorii mającej na celu zdiagnozowanie opisywanego przypadku w formacie true / false positive. Każdy z przypadków zostanie przeanalizowany pod kątem wszystkich możliwie występujących cech szczególnych.

Cały powyższy opis szkolenia opiera się na czysto praktycznym laboratorium, w którym student samodzielnie wykona każdą akcję lub powiązane scenariusze w dedykowanej sieci laboratorium wirtualnego. Ta klasa skupia się na architekturze x86 / x64, sieciach IPv4 / IPv6 oraz docelowych środowiskach Linux i Windows.

W zakresie IDS / IPS / Data Leakage Protection i lepszego zrozumienia aktualnego stanu twojej pozycji bezpieczeństwa sieci, doświadczenie szkoleniowe pomoże ci zrozumieć ryzyko, zidentyfikować martwe punkty bezpieczeństwa sieci i nieodkryte przestrzenie infrastruktury poprzez symulację i wykrywanie działań prawdziwego cyber-przeciwnika.

Uzyskaj pewność, że bezpieczeństwo Twojej sieci naprawdę działa!

Proponowany warsztat w wersji defensywnej jest naturalną kontynuacją części pierwszej → ofensywnej (RED). Na dzień dzisiejszy oferta Defensive Security uwzględnia zatem dwuetapową ścieżkę warsztatową dt. symulacji i wykrywania działań z zakresu "po uzyskaniu dostępu do sieci korporacyjnej" oraz technik i detekcji eksfiltracji sieciowych.

Wysoce techniczne treści i tylko praktyczne podejście gwarantuje, że wykorzystanie przekazanej wiedzy i technologii w rzeczywistych środowiskach produkcyjnych będzie łatwe, płynne i powtarzalne.

FULL AGENDA:

1. Introduction → PCAP Exfiltration CTF-style challenge.
2. One more time → MITRE Attack Framework → detection map based on 5 examples of chained attack scenarios.

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

4. Collecting, analyzing and correlating data from different data sources using:
    a. Splunk
    b. Elastic Stack
    c. Wazuh
    d. Graylog
    e. Netflow
    f. Auditd / go-audit
    g. eBPF
    h. OSquery

5. Windows Sysinternals Suite:
    a. Sysmon:
        i. Process execution events
        ii. Network connection events
        iii. Image load events
        iv. Named pipe events
        v. WMI events
        vi. PSexec events

    b. Process Explorer
    c. Process Monitor
    d. Autoruns
    e. Evidence traces of file download and execution:
        i. cmd.exe
        ii. HTA
        iii. JS
        iv. VBS
        v. WSF
        vi. JSE
        vii. CSharp
        viii. certutil
        ix. Powershell
        x. Bitsadmin
        xi. Shellcode injection techniques
        xii. WebDAV / SMB / NFS share mapping

6. Low level Linux security tracing and profiling for critical services:
    a. eBPF
    b. sysdig

7. Detection of unusual log patterns and 0-day exploitation attempts using source code analysis of your critical network service.

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

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. Intelligent HTTP C2 Redirection
    k. Port knocking
    l. Domain fronting
    m. ngrok
    n. SSH Tunneling and pivoting
    o. RDP Tunneling and pivoting / RDP Inception
    p. Egress testing and common network traffic on non-standard ports

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. Detection of brute-force attacks → use cases:
    a. SQL
    b. AD
    c. SSH
    d. Web Apps

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

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

14. Describing relevant log events in generic and open signature → Sigma rules:
    a. Application
    b. APT
    c. Linux
    d. Network

e. Proxy
f. Web
g. Windows

CZAS TRWANIA:

- 3 dni bardzo intensywnego warsztatu technicznego (9:00-17:00)

GRUPY DOCELOWE:

- Specjaliści ds. bezpieczeństwa IT, eksperci i konsultanci
- Członkowie zespołów Blue, Red i Purple
- Inżynierowie SIEM oraz analitycy bezpieczeństwa
- Inżynierowie oraz specjaliści ds. testowania bezpieczeństwa
- Członkowie zespołów ds. reagowania na incydenty bezpieczeństwa
- Inżynierowie systemowi oraz architekci IT
- Entuzjaści bezpieczeństwa oraz świata oprogramowania Open Source

---

WYMAGANIA SW / HW:

- Minimum 30 GB dostępnej przestrzeni na dysku
- Minimum 8 GB of RAM
- Najnowsza wersja oprogramowania VirtualBox
- Pełne uprawnienia do systemu operacyjnego na laptopie

SŁOWA KLUCZOWE:

- Empire Framework, Metasploit Framework, Volatility Framework, yara, ssdeep, osquery, Graylog, Wazuh / OSSEC, ngrok, ELK, Splunk, Sigma, hydra, SysInternals, PowerSploit, PowerView, DOSFuscation, ntlmrelayx, Bloodhound, goDoH, ssh, BRO IDS, Suricata, sysdig, eBPF, auditd, OpenVswitch, dnscat2, tcpreplay, wireshark, tcpdump, nmap, WMImplant, Invoke-PipeShell, SharpSploit, Sharpshooter, plink, dsquery, adexplorer, PIngCastle, ngrep, print.exe, Shellter i wiele innych.

INNE USŁUGI I PROJEKTY:

Oprócz świadczenia usług edukacyjnych pod kątem bezpieczeństwa IT służymy pomocą przy:

- planowaniu, budowaniu oraz walidacji skuteczności działania środowisk typu Security Operation Center (SOC) ze szczególnym uwzględnieniem przeprowadzania symulacji działań atakujących polegających na wykradaniu/wycieku krytycznych danych poprzez infrastrukturę sieciową (tzw. Network Data Exfiltration).
- wykonywaniu testów penetracyjnych infrastruktury, aplikacji webowych oraz audytów bezpieczeństwa
- zabezpieczaniu systemów, usług i aplikacji webowych/internetowych bazując na oprogramowaniu typu Web Application Firewall z uwzględnieniem procesu tzw. wirtualnego patchowania.
- przeprowadzaniu zaawansowanych szkoleń technicznych z zakresu bezpieczeństwa systemów informatycznych, w szczególności polecamy dedykowane warsztaty techniczne:
    - Open Source Defensive Security → The Trinity of Tactics for Defenders.
    - In & Out → Network Data Exfiltration Techniques [RED EDITION]
    - The Art of Modern Deception Techniques for Blue Teams.
    - 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.

KONTAKT:

- Email: leszek.mis@defensive-security.com / info@defensive-security.com
- Tel: +48 791 611 309 / +48 791 83 10 18
- Strona www: https://www.defensive-security.com