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 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 (In & Out Series, Open Source Defensive Security, Modsecurity, FreeIPA, SELinux, Linux Hardening).
   - Prelegent na wielu konferencjach: 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
   - 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!!!”

KLIENCI:

- PZU
- ING Tech
- PGNiG
- Warta

- AXA
- Pekao
- AVIVA
- 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
- Integrated Solutions

O WARSZTACIE:

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

- sposobów walidacji skuteczności rozwiązań typu SIEM oraz środowisk SOC
- aktualnych trendów, technik i narzędzi służących do eksfiltracji i wykradania danych oraz taktyk i zachowań przeciwnika po uzyskaniu dostępu do sieci
- technik testowania i omijania systemów DLP / IDS / IPS / FW / WAF
- sposobów tunelowania protokołów, ukrywania i generowania złośliwych zdarzeń sieciowych.
- wartości ze zautomatyzowanego podejścia do symulacji działań atakujących
- technik weryfikacji produktów i dostawców usług bezpieczeństwa IT

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

Już podczas wprowadzenia omówimy najnowsze kampanie APT z wykorzystaniem próbek złośliwego oprogramowania, przeanalizujemy najciekawsze techniki komunikacji sieciowej C2, a wnioski i wyniki analizy zamapujemy bezpośrednio do narzędzia ATT&CK Framework, omówimy metodologię "Kill Chain" oraz zastosujemy strategię "Defense / Offense in depth".

Zwrócimy również uwagę na znaczenie wykonywania okresowej analizy pamięci RAM, wykorzystywania zautomatyzowanych systemów analizy złośliwego oprogramowania, a następnie przejdziemy do szczegółowego omawiania taktyk i sposobów symulacji prawdziwych zagrożeń, które to pozostają kluczowymi aspektami tego szkolenia.

Następnie zagłębimy się w poszczególne protokoły sieciowe, usługi i techniki powszechnie używane przez atakujących w sieciach korporacyjnych, zdefiniujemy oraz omówimy charakterystyczne cechy i artefakty służące lepszemu wykrywaniu incydentów bezpieczeństwa. Korzystając z dostępnego zestawu narzędzi (ponad 50 różnych narzędzi i frameworków), student uczestniczyć będzie w przygotowanych ćwiczeniach laboratoryjnych celem wygenerowania prawdziwych symptomów zachowania napastnika. Warsztat pozwoli na zwalidowanie skuteczności zespołu SOC, podniesienie poziomu wiedzy oraz świadomości, a także pozwoli na rozbudowanie widoczności funkcjonalnej systemów klasy SIEM.

KLUCZOWE CELE WARSZTATU → OMÓWIMY SZCZEGÓŁOWO:

- jak wygenerować różne typy połączeń sieciowych TCP/UDP bind / reverse shell w obrębie systemu Windows oraz Linux,
- w jaki sposób uzyskać dostęp do niedostępnych podsieci (pivoting), skonfigurować przekazywanie portów oraz środowiska Proxy w konfrontacji z dostępnymi artefaktami powyższych działań
- jak ręcznie wygenerować pojedyncze złośliwe pakiety sieciowe, np. celem wysycenia przestrzeni DHCP czy zalania pakietami krytycznej usługi sieciowej z poziomu środowiska scapy
- sposoby generowania własnych, szyfrowanych “raw” kanałów transmisji niewykrywalnych przez dostępne rozwiązania bezpieczeństwa
- jak zasymulować działanie złośliwego oprogramowania pod kątem ruchu DNS DGA, przetestujemy różne rodzaje tuneli i shelli w oparciu o protokół DNS, wykonamy wyciek danych oraz pokażemy w jaki sposób uzyskać darmowy dostęp do internetu w samolocie czy hotelu
- jak utworzyć środowisko typu “Domain Fronting”
- jak przesyłać dane pomiędzy systemami nieposiadającymi bezpośredniego połączenia, np. poprzez AD LDAP

- w jaki sposób wykorzystać protokół ICMP do ukrywania przesyłania danych oraz w jaki sposób wykrywać podobne przypadki
- w jaki sposób wykorzystać różne typy nagłówków oraz metody HTTP do wykradania danych w kombinacji z wykorzystaniem podatności i ataków typu “Injection” + analiza webshelli
- jak wykryć anomalie w ruchu TLS/SSL oraz techniki eksfiltracji na nich bazujące
- w jaki sposób uruchomić skrypty Powershell w procesie posteksploitacyjnym celem omijania zabezpieczeń typu AV/EDR
- platformy i podejścia wycieku danych korzystając z transmisji WMI, Websockets, VOIP czy P2P
- jak ukryć dane w pliku wykonywalnym, pliku WAV, obrazku oraz jak wykradać dane z systemów nie posiadających dostępu do internetu
- jak skonfigurować i podłączyć stacje robocze do sieci anonimizujących VPN, TOR, Open Proxy w konfrontacji z globalnymi listami reputacyjnymi, feedami oraz sygnaturami
- w jaki sposób skorzystać z publicznych platform chmurowych celem ustanowienia komunikacji C2: Pastebin, Twitter, AWS i inne
- przedstawimy sposoby ponownego uruchomienia pliku PCAP w kontekście analizy zachowania złośliwego oprogramowania
- omówimy składnię podejścia sygnaturowego z wykorzystaniem reguł przeznaczonych dla silnika Suricata, Bro IDS oraz określimy różnice pomiędzy nimi
- plus kombinacja powyższych i wiele więcej

Dzięki praktycznym ćwiczeniom eksfiltracyjnym warsztat ten pozwala uzyskać szerszy obraz tego, na co naprawdę trzeba zwracać uwagę myśląc początkowo lub udoskonalając środowisko SOC oraz umiejętności zespołu Red i Blue, samego wdrożenia i eksploatacji systemu SIEM, instalacji DLP / IDS / IPS lub rozwiązań bazujących na sztucznej inteligencji pod kątem wykrywania anomalii.

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 działań prawdziwego cyber-przeciwnika. Uzyskaj pewność, że bezpieczeństwo Twojej sieci naprawdę działa.

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

---

SŁOWA KLUCZOWE:

- 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.

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 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

---

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