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 13 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, Flocon, 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."

KLIENCI:

- 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

O WARSZTACIE:

"The Post Exploitation Adversary Simulations - Network Data Exfiltration Techniques" to zaawansowany warsztat stworzony w celu zaprezentowania uczestnikom:

- aktualnych technik i narzędzi służących do eksfiltracji i wykradania danych oraz taktyki działań atakujących “po ataku”
- testowania i omijania systemów DLP / IDS / IPS / FW
- tunelowania protokołów, ukrywania i generowanie złośliwych zdarzeń sieciowych.
- sposobów walidacji skuteczności rozwiązań SIEM oraz środowisk SOC.

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 "Defence 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 clone, armor and phish popular websites
- 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:
    a. ATT&CK Framework API.
    b. Caldera.
    c. MAEC.
    d. TTP, Kill chain & Defense in depth.
    e. The importance of:
        i. network traffic baseline profiling
        ii. memory forensics
        iii. real threat simulations != penetration tests
        iv. log correlation

2. Modern RAT's implementation and popular APT&C2 malware communication design - real use cases:
    a. The review of the latest APT campaigns
    b. Multi-Staging
    c. Network Link chaining
    d. Hiding
    e. Data Obfuscation
    f. Transfer/protocol limits
    g. Timing channels / scheduled jobs / packet dripping

3. TCP/UDP bind and reverse shells:
    a. Meterpreter + Veil Framework:
        i. bypassing payloads
        ii. common and exotic ports
        iii. routing, pivoting & port forwarding

    b. CLI tips & tricks:
        i. netcat / nc / cryptocat / telnet / socat / curl / wget / xxd / rsync
        ii. /dev/tcp
        iii. PTY
        iv. PHP / Perl / Python / Ruby / Java / ASP shellz

    c. TCP/UDP raw socket tunnels

d. Generate your own network shellcode & analyze the Exploit-db Shellcode Archive

4. General bypassing, exfiltration, tunneling, pivoting, proxying and C2 techniques:
    a. ICMP
    b. DNS:
        i. Authoritative vs recursive
        ii. CDN theory & domain fronting
        iii. Fast-flux domains
        iv. Dictionary and random characters DGA
        v. DNS proxy
        vi. DNS anomalies

    c. HTTP/S & web application exploitation techniques combo:
        i. HTTP 404
        ii. HTTP headers:
            1. Etag
            2. Cookies
            3. User-agent
            4. Accept
            5. If-None-match
        iii. GET/POST
        iv. Website cloning and armoring
        v. WebDAV
        vi. Websockets
        vii. Certificate exfiltration & TLS/SSL anomalies
        viii. *Injections + exfiltration
        ix. HTTP redirects
        x. Webshells
        xi. HTTP anomalies

    d. WMI / PS-remote
    e. Proxy / Socks
    f. SSH / SFTP / SCP
    g. LDAP
    h. FTP / TFTP
    i. SMB / NFS
    j. RDP
    k. Anonymizers:
        i. VPN
        ii. TOR
        iii. Open Proxy

    l. POP3 / SMTP / IMAP

m. VOIP
n. P2P
o. IRC
p. IPv6
q. + chaining of aboves and many more.

5. Cloud-based exfiltration and C2 channels:
    a. Twitter
    b. Pastebin
    c. Github
    d. Slack
    e. Youtube
    f. Office 365
    g. Gmail / Google Docs
    h. AWS / Google Cloud
    i. Skype
    j. Dropbox
    k. Soundcloud
    l. Tumblr

6. Windows & Powershell exfiltration tools:
    a. AD / LDAP properties
    b. Empire

7. Just a Browser Exfiltration:
    a. audio/video exfil
    b. keylogging

8. Hoping from air-gapped networks.
9. USB attacks and network exfiltration combo.
10. The art of data hiding → steganography examples:
    a. Binary
    b. WAV
    c. Image
    d. VOIP
    e. Routing Protocol
    f. Screen

11. Signature-based event analytics, rule bypassing & malicious network traffic generation:
    a. Suricata ET / VRT rules vs attacker → the syntax rules of the rules
    b. Bro IDS log “features” for deep low-level network baselining
    c. Threat Intelligence feeds, lists and 3rd party APIs:
        i. IP reputation lists

ii. Malware feeds
iii. Phishing feeds
iv. C2 lists
v. Open Proxy lists
vi. Tor exit-nodes
vii. Censys / VT / Passive Total
viii. Shodan

d. Replaying and analysing malicious PCAP files.

12. Adversary simulation moves, actions, tools & automated platforms:
    a. In&Out Simulated Network Exfiltration Platform
    b. APT simulator
    c. Dumpster Fire
    d. Firebolt
    e. Flightsim
    f. Armoring:
        i. Nmap NSE scripts
        ii. MiTM/Spoofing/TCP flooding
        iii. Port Knocking
        iv. Brute force
        v. DHCP starvation
        vi. Info disclosure on SMB/CIFS shares

13. Summary → recommended defensive/protection tactics, tools and platforms.

SŁOWA KLUCZOWE:

- impacket, pyexfil, scapy, metasploit/meterpreter, Veil Framework, 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, SELKS, Security Onion, wondjina, trevor C2, sharpSocks, WSC2, sqlmap, BeeF Framework, twittor, torify, TheFatRat, cloakify, WMIsploit, certreq, SSH, ngrep, nping, iptables, Merlin, udp2raw, Volatility Framework, SILK, nfdump, NativePayload_IP6DNS, dnsmasq, thc-flood, knockd, dnstwist, yersinia, DNSexfiltrator, SMBmap, testssl, firebolt, dumpster fire, APT simulator, cuckoo, moloch, icmptunnel, transmission, openvswitch, ngrok i inne

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 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.
    - Post Exploitation Adversary Simulations → Network Data Exfiltration Techniques.
    - 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: info@defensive-security.com
- Tel: +48 791 611 309 / +48 791 83 10 18
- Strona www: https://www.defensive-security.com