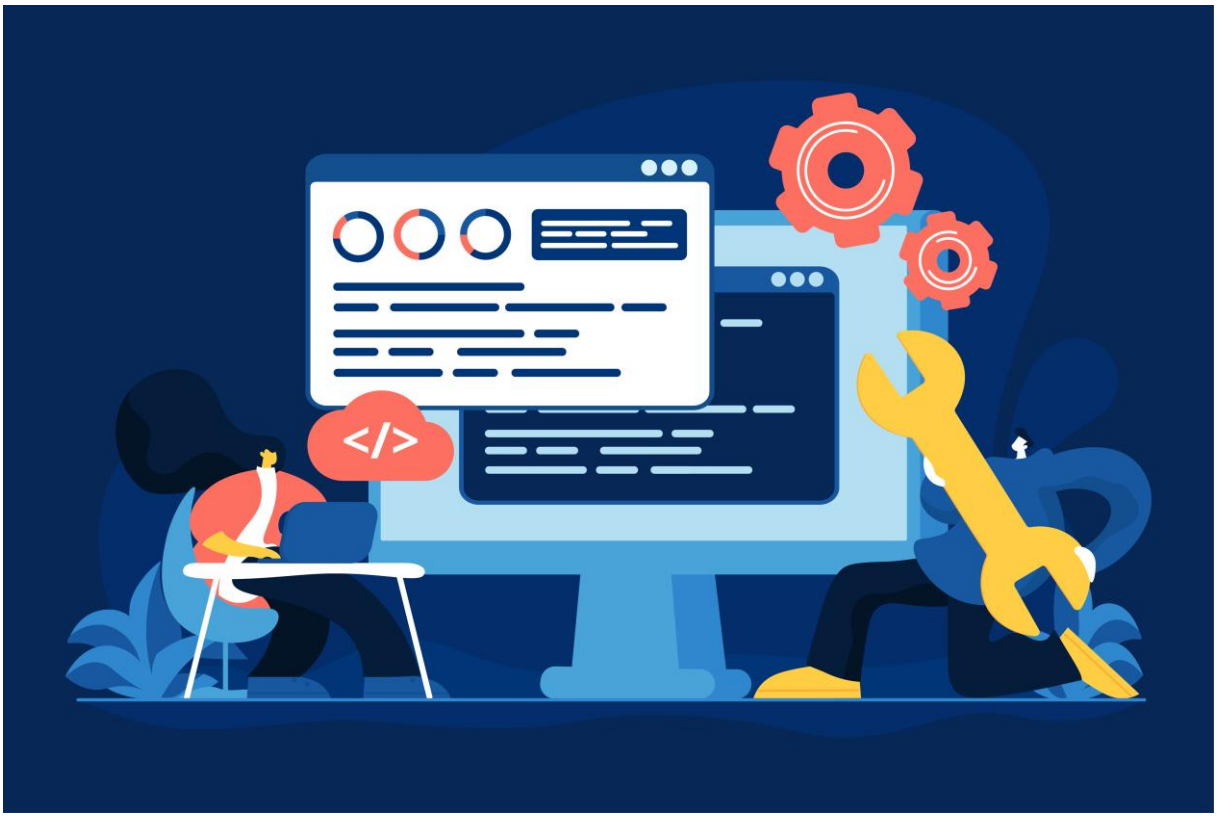

Podstawy Incident Response

LEKCJA 1 – „Coś tu nie gra… czyli wykrycie i triage”

1 | Cele lekcji

Uczeń:

1. potrafi wykryć niepokojący ruch sieciowy i wskazać możliwe źródło;
2. analizuje podstawowe dane (adresy IP, tablica ARP, ścieżka pakietu);
3. wie, jak sporządzić notatkę z pierwszej obserwacji (data, host, objawy).

2 | Czas trwania

45 min

3 | Potrzebne materiały

- Komputer z Win 10/11 lub Linux (admin).
- nmap, **Wireshark**, curl zainstalowane.
- Dostęp do sieci szkolnej (wydzielona podsieć ćwiczeniowa).
- Wydrukowany *Incident Response Cheat-sheet* (ścieżka, polecenia, miejsce na notatki).
- Ekran / tablica.

4 | Przebieg zajęć

Czas	Etap	Co robi nauczyciel	Co robią uczniowie
3'	**Hook**	Pokazuje wykres NOC: nagły skok ruchu z IP 192.168.0.23. Pytanie: „Jak dowiedzieć się, co to za host?”	Propozycje narzędzi.
7'	**Identyfikacja hosta**	Demonstruje ipconfig na własnym PC → różnica między	Sprawdzają IP swoich stacji.

		lokalnym IP a podejrzanym.	
5'	**Żywy/zombie?**	ping 192.168.0.23 – brak odpowiedzi. Wyjaśnia, że ping może być blokowany.	Notują obserwację.
8'	**Mapa sąsiedztwa**	arp -a, krótko o MAC. Następnie nmap -sn 192.168.0.0/24 (szybkie host discovery).	Odszukują 192.168.0.23 na liście (host odpowiada, ale ICMP filtruje).
7'	**Trasa i usługa**	tracert 192.168.0.23 (1 hop = host lokalny). curl -I http://192.168.0.23 → 200 OK, Server: nginx.	Wnioskują, że stoi serwer www.
10'	**Wireshark live**	Krótki capture, filtr ip.addr == 192.168.0.23. Pokazuje setki żądań GET do dziwnych domen.	Liczą, ile domen w 30 s.
5'	**Podsumowanie/triage note**	Na tablicy wzór notatki: *kto*, *co*, *kiedy*, *jak wykryto*.	Wypełniają cheat-sheet dla incydentu.

5 | Pytania do dyskusji

1. Dlaczego host może nie odpowiadać na ping, a i tak działać?
2. Jak odróżnić normalny ruch HTTP od potencjalnego botnet-spamu?

6 | Ratunkowe wskazówki

- **Brak odpowiedzi narzędzia** → pokaż przygotowany screenshot.

- **Uczeń zadaje szczegół techniczny** → „Zapiszmy i sprawdźmy after-class – wrócimy do tego jutro.”

7 | Dodatkowe źródła

- „Wireshark Display Filters – Quick Reference” (pdf, 1 strona).
- nmap.org/book/usage – sekcja „Host Discovery”.

LEKCJA 2 – „Zabezpieczamy dowody i piszemy raport”

1 | Cele lekcji

Uczeń:

1. wykonuje obraz dysku i zrzut pamięci z zainfekowanego hosta;
2. wykorzystuje **Autopsy/WinHex** do znalezienia artefaktów (złośliwy plik, log);
3. przygotowuje zwięzły raport: opis incydentu, wnioski, rekomendacje.

2 | Czas trwania

45 min

3 | Potrzebne materiały

- Ten sam host-lab 192.168.0.23 lub gotowy obraz dysku .E01.
- **FTK Imager Lite**, dd, memdump/winpmem.
- **Autopsy** + próbka obrazu (jeśli czas nie pozwala na pełne kopiowanie na żywo).
- Szablon raportu (doc/pdf) – 1 strona z tabelami.

4 | Przebieg zajęć

Czas	Etap	Co robi nauczyciel	Aktywność uczniów
4'	**Przypomnienie**	Krótko streszcza ustalenia lekcji 1 – host 192.168.0.23 generuje dziwny ruch.	Otwierają wczorajsze notatki.
8'	**Obraz dysku**	Pokazuje dd if=/dev/sdb of=/mnt/usb/host23.img bs=4M status=progress **lub** kreator w FTK (E01 + hash MD5/SHA256). Wyjaśnia zasadę 1:1 i rolę sum.	Spisują komendę, notują hash.
6'	**Zrzut RAM**	Prezentuje tylko start komendy winpmem (Windows) / memdump (Linux) + dołączany symbolik. Podkreśla ulotność pamięci.	Zapisują lokalizację pliku .raw.
10'	**Autopsy – szybka ścieżka**	Ładuje wcześniej przygotowany kawałek obrazu (czas!). Wyszukuje plik /var/www/html/bot.php. Analiza timestampa = dzień incydentu.	Odszukują plik w drzewie, notują sha256.
7'	**Logi systemowe**	Otwiera fragment /var/log/nginx/access.log w **WinHex** lub tail. Wspólnie filtrują grep "POST /bot" – 1500 wpisów w godzinę.	Liczą liczbę wierszy, wpisują w raport.
5'	**Recovery i blokada**	Pokazuje prostą regułę firewall: iptables -A OUTPUT -d bad.dns.example -j DROP. Krótko o patchowaniu i CVE.	Proponują własne kroki (aktualizacja, zmiana haseł).

Czas	Etap	Co robi nauczyciel	Aktywność uczniów
5'	**Raport końcowy**	Na ekranie wzór raportu (sekcje: *Streszczenie, Linia czasu, Artefakty, Działania naprawcze*).	W parach uzupełniają szablon (bullet-points).

5 | Pytania do dyskusji

1. Jak hash potwierdza integralność obrazu?
2. Co zrobić, gdy malware ukrywa pliki jako „skasowane”?
3. Jak sprawdzić, czy incydent nie objął innych hostów?

6 | Ratunkowe wskazówki

Sytuacja	Szybka odpowiedź	Następny krok
Brak czasu na pełny dd	„Użyjmy przygotowanego mini-obrazu, proces wygląda identycznie – zaraz zobaczycie.”	Po lekcji kontynuuj kopiowanie w tle.
Uczeń chce „usunąć od razu bot.php”	„Najpierw dowody, potem kasowanie – to jak badanie miejsca zdarzenia.”	Po analizie pokaż bezpieczne usunięcie + patch.

7 | Dodatkowe źródła

- CERT Polska – „Podstawowe kroki IR” (pdf, 6 str.).
- DFIR Training – darmowe obrazy dysków do ćwiczeń (digitalcorpora.org).

📋 **Łącznik między lekcjami – jeśli odbywają się w różnych dniach**

- **Zadanie domowe (po lekcji 1):** Krótkie 3-zdaniowe streszczenie triage + lista narzędzi, których *nie* zdążyli użyć, a chcieliby.
- **Początek lekcji 2:** sprawdź te listy – wybierz 1 narzędzie klasy i pokaż je w 2 minuty (np. hping, netstat).