

SZKOLENIE DWUDNIOWE — DZIEŃ 1 z 2



Cyberbezpieczeństwo w praktyce

CompTIA Security+ SY0-701 z laboratoriami CertMaster Labs

28.09.2026

07:00–15:00

Zdalnie (MS Teams)

Poziom średniozaawansowany

6 laboratoriów

8 godzin dydaktycznych · 6 modułów · zestaw laboratoriów oraz ćwiczeń praktycznych · pre-test i post-test · zaświadczenie i certyfikat

Agenda Dnia 1 — 13 pozycji harmonogramu BUR

OTWARCIE

Godziny zgodne z kartą usługi nr 2026/09/04/204299/3790068. Blok = zajęcia merytoryczne, LAB = laboratorium CertMaster Labs.

07:00–07:45 · Otwarcie, pre-test, krajobraz zagrożeń, taksonomia ataków, APT, ransomware

Blok 1

07:45–08:30 · LAB 4.1.1 Password Security

Laboratorium

08:30–08:45 · Przerwa

08:45–09:30 · Kryptografia i PKI: AES-256, RSA, ECDH, TLS 1.3, X.509, PFS, post-quantum

Blok 2

09:30–10:15 · LAB 3.1.1 Storage Encryption

Laboratorium

10:15–10:30 · Przerwa

10:30–11:15 · Bezpieczeństwo sieci: rozpoznanie, nmap, MitM, ARP Spoofing, DDoS, model OSI

Blok 3

11:15–12:00 · LAB 2.1.1 Finding Open Ports

Laboratorium

12:00–12:30 · Przerwa obiadowa

12:30–13:00 · Bezpieczeństwo aplikacji webowych: OWASP Top 10, SQLi, XSS, CSRF

Blok 4

13:00–13:30 · LAB 8.1.1 SQL Injection

Laboratorium

13:30–14:15 · Zapory sieciowe i segmentacja + LAB 9.2.1 Firewall

Blok 5

14:15–15:00 · Zarządzanie podatnościami CVE/CVSS/EPSS + LAB 8.3.1 + podsumowanie

Blok 6

Efekty uczenia się i sposób ich weryfikacji

Zapiseane zgodnie ze standardem karty usługi w Bazie Usług Rozwojowych — to jest kontrakt na dzisiejsze dwa dni.

Zagrożenia i malware

identyfikujecie Państwo aktualne zagrożenia oraz klasyfikujecie typy ataków sieciowych i złośliwego oprogramowania. Weryfikacja: test teoretyczny generowany automatycznie.

Kryptografia

opisujecie Państwo zasady działania mechanizmów kryptograficznych (szyfrowanie symetryczne, asymetryczne, funkcje skrótu, PKI) stosowanych do ochrony danych i komunikacji.

Bezpieczeństwo sieci

konfigurujecie i testujecie Państwo kontrole bezpieczeństwa sieci: reguły zapory, segmentację VLAN, monitorowanie ruchu — weryfikacja przez obserwację w środowisku CertMaster Labs.

IAM

zarządzacie Państwo tożsamością i dostępem z zastosowaniem polityk haseł, MFA i uprawnień opartych na rolach (RBAC) — ćwiczone w laboratorium 4.1.1.

Zarządzanie podatnościami

wykonujecie Państwo skanowanie podatności i interpretujecie wyniki (CVSS, CVE) w celu identyfikacji luk w infrastrukturze.

Walidacja: post-test 30 pytań wielokrotnego wyboru w dniu 2, próg zaliczenia 70% (21/30 pkt), wynik generowany automatycznie i rozdzielony od procesu kształcenia.

Jak pracujemy — CertMaster Labs i materiały

Sześć laboratoriów dzisiaj, sześć jutro — każde wykonywane na osobnym, izolowanym środowisku w przeglądarce.

Platforma CertMaster Labs

- **12 laboratoriów** wybranych spośród 37 dostępnych w kursie CompTIA Security+ SY0-701, po 6 na każdy dzień.
- **Dostęp przez przeglądarkę** — Chrome, Edge lub Firefox w aktualnej wersji, bez instalacji dodatkowego oprogramowania.
- **Środowisko izolowane** dla każdego uczestnika — działania jednej osoby nie wpływają na środowisko innych.
- **Automatyczna walidacja kroków** w większości laboratoriów — platforma sama potwierdza poprawność wykonanego zadania.
- **Czas na laboratorium: 30 minut** — jeśli ktoś nie zdąży, wraca do niego po szkoleniu, dostęp pozostaje aktywny.

Materiały dla uczestników

- **Prezentacje slajdów (PDF)** z dnia 1 i dnia 2 — materiał do powrotu po szkoleniu.
- **Arkusz ćwiczeń** — gap analysis, rejestr ryzyk, wzór procedury IR do samodzielnego wypełnienia.
- **Mapa certyfikacji CompTIA** i ścieżek kariery — omówimy szczegółowo w bloku końcowym dnia 2.
- **Zaświadczenie / certyfikat** ukończenia szkolenia, warunek: obecność min. 80% zajęć.
- **Lista zasobów** do dalszej nauki: CERT Polska, NIST, ENISA, sekurak.pl.

Pre-test wiedzy wyjściowej

10 pytań, 8 minut. Wynik zna tylko uczestnik i prowadzący — to punkt odniesienia, nie ocena.

1

Które z poniższych NIE jest elementem triady CIA?

a) Poufność b) Integralność c) Autoryzacja d) Dostępność

2

Jaki tryb pracy AES zapewnia jednocześnie poufność i integralność?

a) ECB b) CBC c) GCM d) CTR

3

Który protokół jest aktualnym standardem TLS?

a) TLS 1.0 b) TLS 1.1 c) TLS 1.2 d) TLS 1.3

4

Co oznacza skrót CVSS?

System oceny liczbowej krytyczności podatności — Common Vulnerability Scoring System

5

Czym różni się IDS od IPS?

IDS wykrywa i alarmuje, IPS wykrywa i aktywnie blokuje ruch

6

Ile faz obejmuje cykl reagowania na incydent wg NIST SP 800-61?

Sześć: przygotowanie, detekcja, powstrzymanie, eliminacja, odzyskanie, wnioski

7

Co to jest Zero Trust?

Model bezpieczeństwa zakładający brak domyślnego zaufania — weryfikacja każdego żądania niezależnie od lokalizacji

8

Ile godzin ma podmiot kluczowy na wczesne ostrzeżenie CSIRT wg UoKSC?

24 godziny od wykrycia incydentu poważnego

9

Co oznacza RTO w kontekście BCP/DR?

Recovery Time Objective — maksymalny akceptowalny czas przywrócenia usługi

10

Jaka jest różnica między CVE a CVSS?

CVE identyfikuje konkretną podatność, CVSS ocenia jej krytyczność liczbowo

CompTIA Security+ SY0-701 — struktura egzaminu

Pięć domen wiedzy, 90 pytań, 90 minut, próg zdawalności 750/900. Cały dzisiejszy i jutrzejszy program mapuje się na te domeny.

1. General Security Concepts (12%)

podstawowe pojęcia bezpieczeństwa: triada CIA, kontrole, zarządzanie zmianą, kryptografia podstawowa. Pokrywamy w Bloku 1 i 2 dzisiaj.

2. Threats, Vulnerabilities & Mitigations (22%)

największa domena: aktorzy zagrożeń, malware, ataki sieciowe i aplikacyjne, zarządzanie podatnościami. Pokrywamy w blokach 1, 3, 4, 6 dzisiaj.

3. Security Architecture (18%)

architektura sieci, Zero Trust, segmentacja, bezpieczeństwo chmury. Pokrywamy w Bloku 5 dzisiaj i w kontekście IAM jutro.

4. Security Operations (28%)

największa domena łącznie: monitoring, SIEM, reagowanie na incydenty, hardening, IAM. To główny temat jutrzejszego dnia.

5. Security Program Management & Oversight (20%)

zarządzanie ryzykiem, zgodność regulacyjna (NIS2, UoKSC, CRA), audyt, BCP/DR. Domena kończąca jutrzejszy dzień.

Dla zdających egzamin: SY0-701 zastąpił SY0-601 w listopadzie 2023 r. — kluczowe zmiany to większy nacisk na chmurę, Zero Trust i automatyzację (SOAR), mniejszy na klasyczne PKI.

Kluczowe pojęcia — wspólny słownik na dziś

Sześć terminów, które mylą się najczęściej, a które będą wracać przez cały dzień.

Zagrożenie (threat)

potencjalna przyczyna niepożądanego incydentu, np. grupa ransomware, błąd operatora, awaria sprzętu. Zagrożenie istnieje niezależnie od tego, czy mamy podatność.

Podatność (vulnerability)

słabość w systemie, procesie lub kontroli, którą zagrożenie może wykorzystać — np. niezaktualizowany serwer, brak MFA, source code z błędem walidacji danych wejściowych.

Ryzyko (risk)

ilożyny prawdopodobieństwa wystąpienia zdarzenia i skutku, jaki wywoła. Ryzyko = zagrożenie działające na podatność, ważone wpływem na biznes.

Podatność do wykorzystania: exploit

konkretny kod, technika lub sekwencja kroków, która faktycznie wykorzystuje podatność. Exploit różni się od podatności jak klucz różni się od zamka.

Incydent (incident)

zdarzenie, w którym zagrożenie faktycznie zmaterializowało się i naruszyło poufność, integralność lub dostępność aktywa.

Pytanie egzaminacyjne (typowy wzorec): „Nieaktualizowany serwer WWW to...” — poprawna odpowiedź: podatność. Sam fakt istnienia luki to nie ryzyko ani nie incydent, dopóki ktoś jej nie wykorzysta.

Aktorzy zagrożeń — kto atakuje i dlaczego

Motywacja i poziom zaawansowania określają, jakich technik i jakiej obrony potrzeba.

1

Nation-state / APT (Advanced Persistent Threat)

Grupy sponsorowane przez państwa. Wysokie zasoby, długi horyzont czasowy (miesiące–lata), cel: szpiegostwo, sabotaż infrastruktury krytycznej. Przykłady technik: zero-day, supply chain.

2

Zorganizowana cyberprzestępczość

Motywacja finansowa. Ransomware-as-a-Service, handel danymi, oszustwa BEC (Business Email Compromise). Wysoki poziom profesjonalizacji, własne „help desk” dla ofiar.

3

Hacktywiści

Motywacja ideologiczna/polityczna. DDoS, defacement stron, wycieki danych w celu nagłośnienia sprawy. Zwykle niższy poziom techniczny niż APT.

4

Insiderzy (zagrożenie wewnętrzne)

Pracownicy lub kontraktorzy — złośliwi (sabotaż, kradzież danych przy odejściu) lub niezamierzeni (błąd, kliknięcie w phishing). Statystycznie odpowiadają za istotną część incydentów.

5

Script kiddies

Niski poziom umiejętności, wykorzystują gotowe narzędzia i exploity bez pełnego rozumienia mechanizmu. Motywacja: rozgłos, ciekawość, wandalizm.

6

Ryzyko łańcucha dostaw (supply chain)

Atak nie na cel bezpośrednio, lecz przez zaufanego dostawcę oprogramowania lub usług — np. atak na aktualizację, którą instalują wszyscy klienci dostawcy.

Inżynieria społeczna — atak na człowieka, nie na system

Statystycznie najskuteczniejszy wektor wejścia — omija najdroższe nawet zabezpieczenia techniczne.

Techniki oparte na komunikacji

- **Phishing** — masowy, niespersonalizowany e-mail podszywający się pod zaufaną instytucję, nakłaniający do kliknięcia linku lub podania danych.
- **Spear phishing** — phishing spersonalizowany, skierowany do konkretnej osoby lub grupy, z wykorzystaniem informacji zebranych wcześniej (OSINT).
- **Whaling** — spear phishing celujący wyłącznie w kadrę kierowniczą (C-level) — stawka i wiarygodność ataku są najwyższe.
- **Vishing i smishing** — ten sam mechanizm socjotechniczny, przeniesiony na rozmowę telefoniczną (voice) oraz wiadomość SMS (SMS phishing).
- **Pretexting** — atakujący buduje fałszywy, wiarygodny scenariusz (np. „dzwonię z działu IT”), aby uzyskać zaufanie i informacje.

Techniki fizyczne i mechanizmy wpływu

- **Tailgating / piggybacking** — wejście za uprawnioną osobą przez zabezpieczone drzwi bez własnej autoryzacji — różnica: piggybacking zakłada świadomą zgodę osoby wpuszczającej.
- **Shoulder surfing** — podglądanie hasła, PIN-u lub poufnych danych na ekranie zza pleców ofiary — w miejscach publicznych i open space.
- **Dumpster diving** — przeszukiwanie odpadów firmy w poszukiwaniu wydruków, nośników danych czy dokumentów zawierających informacje wrażliwe.
- **Mechanizmy wpływu (Cialdini)** — autorytet, pilność/presja czasu, niedobór, wzajemność, sympatia, dowód społeczny — te same dźwignie psychologiczne stoją za każdą skuteczną kampanią socjotechniczną.

Cyber Kill Chain i MITRE ATT&CK — anatomia ataku

Dwa uzupełniające się modele opisujące etapy i techniki realnego ataku.

Cyber Kill Chain (Lockheed Martin)

siedem liniowych etapów: rekonesans, uzbrojenie, dostarczenie, eksploatacja, instalacja, dowodzenie i kontrola (C2), działania na celu.

Logika modelu

przerwanie ataku na dowolnym wcześniejszym etapie jest tańsze i skuteczniejsze niż reagowanie na etapie ostatnim, gdy dane już wypłynęły.

MITRE ATT&CK

macierz taktyk i technik (nie liniowa, lecz siatka) oparta na realnie obserwowanych atakach — obecny standard branżowy do opisu zachowań przeciwnika.

Taktyki ATT&CK (przykłady)

Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Lateral Movement, Exfiltration, Impact.

Zastosowanie praktyczne

zespoły SOC mapują alerty na konkretne techniki ATT&CK (np. T1566 Phishing), co ujednolica komunikację i pozwala mierzyć pokrycie obrony.

Dla egzaminu: SY0-701 oczekuje rozpoznania etapów Kill Chain i ogólnej koncepcji ATT&CK jako frameworku opisu technik przeciwnika, nie pamięciowej znajomości numerów technik.

Taksonomia złośliwego oprogramowania

Klasyfikacja wg mechanizmu działania — kluczowa dla egzaminu i dla doboru środków zaradczych.

- 1 Wirus (virus)**
Wymaga nosiciela (pliku wykonywalnego) i działania użytkownika (uruchomienie), by się rozprzestrzeniać. Replikuje się, dołączając kod do innych plików.
- 2 Robak (worm)**
Samodzielnie replikuje się przez sieć, bez działania użytkownika i bez potrzeby nosiciela — wykorzystuje podatności usług sieciowych.
- 3 Trojan**
Maskuje się jako legalne oprogramowanie. Nie replikuje się samodzielnie — polega na tym, że użytkownik sam go zainstaluje.
- 4 Rootkit**
Ukrywa obecność złośliwego oprogramowania na poziomie systemu operacyjnego lub jądra — modyfikuje mechanizmy, które miałyby go wykryć.
- 5 Spyware / Keylogger**
Zbiera informacje o użytkowniku bez jego wiedzy: naciśnięcia klawiszy, historię przeglądania, dane logowania.
- 6 Botnet**
Sieć zainfekowanych urządzeń (bot = zombie) sterowana centralnie przez atakującego przez kanał C2 — wykorzystywana m.in. do DDoS i rozsyłania spamu.

Ransomware — ewolucja czterech generacji

Od prostego szyfrowania do modelu przestępczości zorganizowanej jako usługi (RaaS).

1. generacja — proste szyfrowanie:

atakujący szyfruje pliki lokalnie i żąda okupu za klucz deszyfrujący. Ochrona: kopia zapasowa wystarcza do pełnego odzyskania.

2. generacja — szyfrowanie sieciowe:

ransomware rozprzestrzenia się w sieci wewnętrznej (podobnie jak robak), szyfrując udziały sieciowe i serwery, nie tylko stację roboczą.

3. generacja — podwójne wymuszenie (double extortion):

przed zaszyfrowaniem dane są eksfiltrowane. Nawet działający backup nie chroni przed groźbą publikacji skradzionych danych.

4. generacja — potrójne/poczwórne wymuszenie i RaaS:

dochodzi DDoS na infrastrukturę ofiary, kontakt z klientami/partnerami ofiary, a samo oprogramowanie działa w modelu Ransomware-as-a-Service z podziałem zysków.

Wniosek praktyczny: backup chroni wyłącznie przed generacją pierwszą i drugą. Przeciwko podwójnemu wymuszeniu potrzebna jest prewencja (segmentacja, EDR, MFA) — o tym w blokach 5 i 6 dzisiaj.

LAB 4.1.1 Password Security

LAB 4.1.1

Password Security

Konfiguracja polityki haseł, wymuszenie złożoności hasła oraz test odporności na ataki słownikowe w środowisku symulowanym.

Czas: 30 min (07:45–08:30)

Domena SY0-701: Domena 2 — Threats, Vulnerabilities & Mitigations (uwierzytelnianie i ataki na hasła)

Kroki laboratorium

1. Zaloguj się do przypisanego środowiska CertMaster Labs, moduł 4.1.1.
2. Skonfiguruj politykę haseł: minimalna długość, złożoność (wielkie/małe litery, cyfry, znaki specjalne), historia haseł.
3. Przetestuj utworzenie hasła niespełniającego polityki i zaobserwuj reakcję systemu.
4. Uruchom symulowany atak słownikowy na konto testowe ze słabym hasłem.
5. Porównaj czas łamania hasła słabego i hasła zgodnego z polityką.
6. Zapisz wnioski do arkusza ćwiczeń — użyjemy ich w debriefie.

Na co zwrócić uwagę

- **Długość ważniejsza niż złożoność** — hasło 16-znakowe ze słownika fraz jest odporniejsze na brute-force niż 8-znakowe z myślnikami i cyframi.
- **Ataki słownikowe vs brute-force** — słownikowy testuje znane hasła/frazy, brute-force wszystkie kombinacje — czas łamania rośnie wykładniczo z długością.
- **Polityka nie zastępuje MFA** — nawet silne hasło można wykraść phishingiem; druga warstwa uwierzytelniania pozostaje niezbędna.

Debrief — polityki haseł wg NIST SP 800-63B

Aktualne wytyczne odwracają część wieloletnich, powszechnie stosowanych praktyk.

Długość ponad złożoność

NIST rekomenduje minimum 8 znaków dla kont użytkowników (najlepiej 15+), bez wymuszania konkretnych klas znaków — długa fraza bywa skuteczniejsza niż krótkie hasło ze znakami specjalnymi.

Rezygnacja z okresowej wymiany haseł

wymuszanie zmiany hasła co 30/60/90 dni bez powodu prowadzi do słabszych haseł (wzorce typu Hasło1, Hasło2...). Zmiana tylko przy podejrzeniu kompromitacji.

Sprawdzanie względem list wyciekłych haseł

nowe hasło powinno być porównywane z bazami znanych, skompromitowanych haseł (np. Have I Been Pwned), a nie tylko z regułami składniowymi.

Menedżery haseł

rekomendowane jako standard — pozwalają na unikalne, długie hasła dla każdego serwisu bez obciążania pamięci użytkownika.

MFA jako uzupełnienie, nie substytut

hasło pozostaje jednym z czynników uwierzytelniania („coś, co wiesz”), ale nie jedynym — do pełnej architektury MFA wrócimy w Dniu 2.

Kryptografia — cele i podstawowe pojęcia

BLOK 2

Blok 2 (08:45–10:15): kryptografia i PKI — najbardziej egzaminacyjnie wymagający temat dzisiejszego dnia.

Poufność (confidentiality)

tylko uprawnione strony mogą odczytać dane. Realizowana przez szyfrowanie.

Integralność (integrity)

dane nie zostały zmienione w sposób nieautoryzowany. Realizowana przez funkcje skrótu i podpisy cyfrowe.

Autentyczność (authenticity)

potwierdzenie, że dane pochodzą od zadeklarowanego nadawcy. Realizowana przez podpisy cyfrowe i certyfikaty.

Niezaprzeczalność (non-repudiation)

nadawca nie może zaprzeczyć, że wysłał daną wiadomość — kluczowe w kontekście prawnym (np. podpis elektroniczny).

Dwa fundamentalne rodzaje szyfrowania

symetryczne (jeden wspólny klucz) i asymetryczne (para kluczy: publiczny i prywatny) — różne zastosowania, różna wydajność.

Dlaczego to ważne: kryptografia nie jest jednym mechanizmem — to zestaw narzędzi, z których każde realizuje inny cel. Dobór złego narzędzia do celu to częsty błąd projektowy.

Szyfrowanie symetryczne: AES-256 i tryby działania

Advanced Encryption Standard — de facto światowy standard szyfrowania symetrycznego od 2001 roku.

AES-256

szyfr blokowy z kluczem 256-bitowym, operuje na blokach danych po 128 bitów. Standard NIST FIPS 197, uznawany za odporny na ataki brute-force przy obecnej mocy obliczeniowej.

Tryb ECB (Electronic Codebook)

najprostszy, ale wadliwy: identyczne bloki danych wejściowych dają identyczne bloki zaszyfrowane — ujawnia wzorce. Unikać w praktyce.

Tryb CBC (Cipher Block Chaining)

każdy blok jest XOR-owany z poprzednim blokiem zaszyfrowanym przed szyfrowaniem — eliminuje wzorce ECB, ale nie zapewnia integralności.

Tryb GCM (Galois/Counter Mode)

tryb uwierzytelnionego szyfrowania (AEAD) — zapewnia jednocześnie poufność i integralność/autentyczność. Standard w TLS 1.3.

Tryb CTR (Counter Mode)

zamienia szyfr blokowy w strumieniowy, umożliwia przetwarzanie równoległe — podstawa dla GCM (CTR + uwierzytelnianie).

Pytanie z pre-testu: GCM zapewnia poufność i integralność jednocześnie (AEAD) — to odpowiedź c) z pytania 2 na początku dnia. CBC daje tylko poufność.

Funkcje skrótu: SHA-256, SHA-3, HMAC

Jednokierunkowe funkcje matematyczne — fundament weryfikacji integralności i przechowywania haseł.

Funkcja skrótu (hash)

przekształca dane dowolnej długości w skrót o stałej długości. Jednokierunkowa (nieodwracalna) i deterministyczna — te same dane zawsze dają ten sam skrót.

SHA-256

część rodziny SHA-2, skrót 256-bitowy. Powszechny standard: certyfikaty TLS, blockchain, weryfikacja plików.

SHA-3

nowsza rodzina (2015), inna konstrukcja matematyczna (Keccak) niż SHA-2 — dodatkowa różnorodność na wypadek przyszłego złamania SHA-2.

MD5 i SHA-1

przestarzałe, obie mają udowodnione kolizje (dwa różne pliki dające ten sam skrót). Nie stosować do celów bezpieczeństwa.

Salt (sól)

losowy ciąg dodawany do hasła przed haszowaniem, unikalny dla każdego użytkownika — chroni przed atakami rainbow table.

HMAC

Hash-based Message Authentication Code — funkcja skrótu połączona z kluczem tajnym, weryfikuje jednocześnie integralność i autentyczność nadawcy.

Szyfrowanie asymetryczne: RSA

Para kluczy — publiczny i prywatny — rozwiązuje problem bezpiecznej dystrybucji klucza.

Zasada działania

dwa matematycznie powiązane klucze: publiczny (do udostępniania) i prywatny (trzymany w tajemnicy). Co zaszyfrowane jednym, można odszyfrować tylko drugim.

Podstawa matematyczna

trudność faktoryzacji bardzo dużych liczb będących iloczynem dwóch liczb pierwszych — obliczeniowo praktycznie niewykonalna dla dużych kluczy klasycznymi komputerami.

Typowa długość klucza

2048 lub 4096 bitów. Znacznie dłuższa niż w AES, bo mechanizm łamania jest inny (faktoryzacja, nie brute-force) — nie da się bezpośrednio porównywać długości kluczy między RSA a AES.

Dwa zastosowania

1) szyfrowanie: nadawca szyfruje kluczem publicznym odbiorcy, tylko odbiorca (z kluczem prywatnym) odczyta; 2) podpis cyfrowy: nadawca podpisuje kluczem prywatnym, każdy (z kluczem publicznym) zweryfikuje autentyczność.

Wada praktyczna

znacznie wolniejszy obliczeniowo niż AES — dlatego w praktyce (np. TLS) RSA/ECDH służy tylko do wymiany klucza symetrycznego, a nie do szyfrowania całej transmisji.

Krzywe eliptyczne: ECDH, ECDSA, Curve25519

Nowsza matematyka kryptografii asymetrycznej — te same funkcje co RSA, znacznie krótsze klucze.

Kryptografia krzywych eliptycznych (ECC)

oparta na problemie logarytmu dyskretnego na krzywej eliptycznej, nie na faktoryzacji jak RSA — pozwala na dużo krótsze klucze przy tym samym poziomie bezpieczeństwa.

Porównanie długości kluczy

klucz ECC 256-bitowy daje bezpieczeństwo porównywalne z kluczem RSA 3072-bitowym — mniejsze obciążenie obliczeniowe i sieciowe.

ECDH (Elliptic Curve Diffie-Hellman)

protokół uzgadniania wspólnego klucza symetrycznego między dwiema stronami bez jego bezpośredniej transmisji — podstawa wymiany klucza w TLS 1.3.

ECDSA

wariant podpisu cyfrowego oparty na krzywych eliptycznych, odpowiednik podpisu RSA, ale wydajniejszy.

Curve25519

konkretna, nowoczesna krzywa eliptyczna zaprojektowana pod kątem wydajności i odporności na błędy implementacyjne — stosowana m.in. w Signal, WireGuard, SSH.

Dla egzaminu: wystarczy rozpoznać ECC/ECDH/ECDSA jako nowszą, wydajniejszą alternatywę dla RSA o tym samym poziomie bezpieczeństwa przy krótszych kluczach — nie wymaga się znajomości matematyki krzywych.

PKI: certyfikaty X.509 i łańcuch zaufania

Infrastruktura klucza publicznego — jak przeglądarka wie, że klucz publiczny faktycznie należy do banku, a nie do atakującego.

Problem, który rozwiązuje PKI

kryptografia asymetryczna gwarantuje, że dane odszyfruje tylko posiadacz klucza prywatnego, ale nie gwarantuje, że klucz publiczny faktycznie należy do tego, za kogo się podaje.

Certyfikat X.509

elektroniczny dokument wiążący klucz publiczny z tożsamością (nazwa domeny, organizacja), podpisany cyfrowo przez zaufaną trzecią stronę.

Urząd certyfikacji (CA)

zaufana instytucja (np. DigiCert, Let's Encrypt), która weryfikuje tożsamość wnioskodawcy i podpisuje jego certyfikat swoim kluczem prywatnym.

Łańcuch zaufania

certyfikat serwera podpisany przez CA pośredni, ten podpisany przez CA root. System operacyjny/przeglądarka ma wbudowaną listę zaufanych certyfikatów root.

Self-signed certificate

certyfikat podpisany samym sobą, bez CA — brak zewnętrznej weryfikacji tożsamości, używany tylko wewnętrznie/testowo, przeglądarka pokazuje ostrzeżenie.

Praktyczny przykład: kłódka w przeglądarce nie oznacza „strona bezpieczna” — oznacza tylko „transmisja zaszyfrowana i tożsamość zweryfikowana przez CA”. Strona phishingowa też może mieć ważny certyfikat.

Unieważnianie certyfikatów: CRL i OCSP

Co się dzieje, gdy klucz prywatny wycieknie zanim certyfikat wygaśnie naturalnie.

Problem

certyfikat jest ważny przez określony czas (zwykle do 398 dni w publicznym WWW), ale klucz prywatny może wyciec wcześniej — potrzebny mechanizm natychmiastowego unieważnienia.

CRL (Certificate Revocation List)

lista unieważnionych certyfikatów publikowana okresowo przez CA. Wada: rośnie w czasie, klient musi ją pobrać w całości, opóźnienie aktualizacji.

OCSP (Online Certificate Status Protocol)

zapytanie w czasie rzeczywistym do CA o status pojedynczego certyfikatu — szybsze niż CRL, ale ujawnia CA, jakie strony odwiedza klient (kwestia prywatności).

OCSP Stapling

serwer sam dołącza (staple) aktualną odpowiedź OCSP do handshake TLS — eliminuje problem prywatności i przyspiesza połączenie.

Dla egzaminu: różnica CRL vs OCSP to klasyczne pytanie porównawcze — CRL = lista pobierana okresowo, OCSP = zapytanie w czasie rzeczywistym o jeden certyfikat.

TLS 1.3: handshake i Perfect Forward Secrecy

Aktualny standard szyfrowania komunikacji internetowej — łączy wszystkie omówione dotąd mechanizmy w jeden protokół.

TLS 1.3 (2018)

aktualna wersja protokołu Transport Layer Security. Usunął przestarzałe, słabe algorytmy dozwolone jeszcze w TLS 1.2 (m.in. RC4, statyczny RSA key exchange, SHA-1).

Handshake

proces uzgodnienia parametrów połączenia: wymiana kluczy przez ECDHE, weryfikacja certyfikatu serwera, uzgodnienie klucza sesji symetrycznego (AES-GCM).

Skrócony handshake (1-RTT, a nawet 0-RTT)

TLS 1.3 redukuje liczbę „podróż w obie strony” potrzebnych do nawiązania połączenia względem TLS 1.2 — szybsze ładowanie stron.

Perfect Forward Secrecy (PFS)

każda sesja używa unikalnego, tymczasowego klucza (dzięki ECDHE) — przechwycenie klucza prywatnego serwera dziś NIE pozwala odszyfrować nagranych wcześniej ruchów.

Dlaczego PFS jest krytyczny

bez PFS atakujący mógł nagrywać zaszyfrowany ruch latami, a po wykradzeniu klucza prywatnego serwera odszyfrować całą historię naraz.

Egzaminacyjny skrót: TLS 1.3 = ECDHE (wymiana klucza) + AES-GCM (szyfrowanie danych) + PFS (unikalny klucz per sesja) + krótszy handshake.

HSTS i bezpieczne nagłówki HTTP

Nagłówki, które wzmacniają bezpieczeństwo komunikacji webowej ponad samo TLS.

HSTS (HTTP Strict Transport Security)

- **Problem, który rozwiązuje:** użytkownik wpisujący adres bez `https://` jest podatny na atak downgrade — przekierowanie na złośliwą wersję `http` przed przekierowaniem na `https`.
- **Mechanizm:** serwer wysyła nagłówek `Strict-Transport-Security`, informujący przeglądarkę, by przez określony czas ZAWSZE łączyła się wyłącznie przez `HTTPS`, bez wyjątku.
- **HSTS Preload List:** lista domen wbudowana fabrycznie w przeglądarki — eliminuje nawet pierwsze połączenie przez `HTTP`.

Inne istotne nagłówki bezpieczeństwa

- **Content-Security-Policy (CSP):** ogranicza, z jakich źródeł przeglądarka może ładować skrypty/style — kluczowa obrona przed XSS (wrócimy w bloku 4).
- **X-Frame-Options:** zapobiega osadzeniu strony w ramce (`iframe`) innej witryny — obrona przed clickjackingiem.
- **X-Content-Type-Options: nosniff:** zapobiega interpretowaniu pliku niezgodnie z deklarowanym typem MIME.

Kryptografia postkwantowa: zagrożenie „Q-Day”

Dlaczego komputery kwantowe zmuszają branżę do zmiany fundamentów kryptografii asymetrycznej.

Zagrożenie

algorytm Shora, uruchomiony na wystarczająco potężnym komputerze kwantowym, potrafiłby efektywnie rozwiązać problem faktoryzacji (RSA) i logarytmu dyskretnego (ECC) — złamałby całą dzisiejszą kryptografię asymetryczną.

„Q-Day”

umowna nazwa hipotetycznego momentu, w którym komputery kwantowe osiągną moc wystarczającą do złamania RSA-2048/ECC w praktyce. Data niepewna, szacunki wahają się między dekadą a kilkoma dekadami.

„Harvest now, decrypt later”

realne ryzyko już dziś: przeciwnicy (szczególnie nation-state) nagrywają zaszyfrowany ruch teraz, licząc na odszyfrowanie go po zbudowaniu komputera kwantowego.

NIST PQC Standards (2024)

NIST ustandaryzował pierwsze algorytmy postkwantowe: ML-KEM (dawniej CRYSTALS-Kyber) do wymiany klucza, ML-DSA (CRYSTALS-Dilithium) do podpisów cyfrowych — oparte na innych problemach matematycznych, odpornych na algorytm Shora.

AES pozostaje względnie bezpieczny

algorytm Grovera (kwantowy) tylko obniża efektywną siłę AES o połowę — AES-256 pozostaje wystarczająco silny nawet w erze postkwantowej.

LAB 3.1.1 Storage Encryption

LAB 3.1.1

Storage Encryption

Szyfrowanie dysków i folderów w symulowanym środowisku oraz weryfikacja integralności zaszyfrowanych danych.

Czas: 30 min (09:30–10:15)

Domena SY0-701: Domena 1 — General Security Concepts (kryptografia stosowana, szyfrowanie danych w spoczynku)

Kroki laboratorium

1. Zaloguj się do modułu 3.1.1 w CertMaster Labs.
2. Zidentyfikuj dysk/wolumin do zaszyfrowania w symulowanym środowisku.
3. Skonfiguruj szyfrowanie pełnego dysku (Full Disk Encryption) i zapisz klucz odzyskiwania.
4. Zaszyfruj wybrany folder z danymi wrażliwymi metodą szyfrowania na poziomie plików.
5. Zweryfikuj integralność danych po zaszyfrowaniu — porównaj skrót pliku przed i po operacji.
6. Przetestuj próbę dostępu do zaszyfrowanych danych bez klucza — zaobserwuj efekt.

Kontekst: dane w spoczynku vs w transporcie

- **Dane w spoczynku (at rest)** — FDE (BitLocker na Windows, LUKS na Linux, FileVault na macOS) chroni dane, gdy nośnik jest fizycznie skradziony lub dostęp uzyskano offline.
- **Dane w transporcie (in transit)** — chronione przez TLS, o którym mówiliśmy przed przerwą — inny mechanizm, inny cel, oba potrzebne równolegle.
- **Zarządzanie kluczem odzyskiwania** — utrata klucza FDE = utrata danych bezpowrotnie. Klucz odzyskiwania musi być przechowywany osobno (np. Active Directory, sejf), nigdy na tym samym dysku.

Debrief: szyfrowanie danych w spoczynku w praktyce

BitLocker, LUKS i FileVault — trzy implementacje tego samego problemu na trzech systemach operacyjnych.

BitLocker (Windows)

wbudowane w Windows Pro/Enterprise, wykorzystuje moduł TPM (Trusted Platform Module) do bezpiecznego przechowywania klucza szyfrującego powiązanego ze sprzętem.

LUKS (Linux Unified Key Setup)

standard szyfrowania dysków w Linuksie, niezależny od dystrybucji, obsługuje wiele metod odblokowania (hasło, keyfile, TPM).

FileVault (macOS)

natywne szyfrowanie pełnego dysku Apple, również zintegrowane ze sprzętowym modułem bezpieczeństwa (Secure Enclave w nowszych Mac).

TPM (Trusted Platform Module)

dedykowany układ sprzętowy przechowujący klucze kryptograficzne w sposób odporny na wyjęcie dysku i próbę odczytu na innym urządzeniu.

Ograniczenie FDE

chroni dane TYLKO gdy urządzenie jest wyłączone/zablokowane. Po zalogowaniu system deszyfruje dane w locie — FDE nie chroni przed malware działającym na uruchomionym systemie.

Model OSI jako mapa powierzchni ataku

BLOK 3

Blok 3 (10:45–12:15): bezpieczeństwo sieci. Każda z siedmiu warstw OSI to inna kategoria ataku i inna obrona.

Warstwa 1–2 (Fizyczna, łączy danych)

ataki: podsłuch fizyczny, ARP Spoofing, MAC flooding. Obrona: port security, 802.1X.

Warstwa 3 (Sieciowa)

ataki: IP Spoofing, routing attacks. Obrona: ACL, filtrowanie na routerach, RPF (Reverse Path Forwarding).

Warstwa 4 (Transportowa)

ataki: SYN Flood, port scanning. Obrona: firewall stanowy, SYN cookies, rate limiting.

Warstwa 7 (Aplikacji)

ataki: SQL Injection, XSS, atak na logikę aplikacji (omówimy szczegółowo w Bloku 4). Obrona: WAF, bezpieczne kodowanie, walidacja danych wejściowych.

Zasada praktyczna

im wyższa warstwa, tym trudniej ochronić się jednym uniwersalnym narzędziem — firewall sieciowy (warstwa 3–4) nie chroni przed SQL Injection (warstwa 7).

Dla egzaminu: pytania performance-based często podają symptom ataku i proszą o wskazanie warstwy OSI, na której należy zastosować środek zaradczy.

Rekonesans i footprinting: OSINT

Pierwszy etap każdego ataku (i każdego testu penetracyjnego) — zbieranie informacji o celu.

Rekonesans pasywny

zbieranie informacji bez bezpośredniej interakcji z celem: rejestry WHOIS, wpisy DNS, metadane dokumentów, portale społecznościowe, wycieki danych.

OSINT (Open Source Intelligence)

wywiad z ogólnodostępnych źródeł — LinkedIn (struktura organizacyjna, technologie w ogłoszeniach o pracę), Shodan (urządzenia podłączone do internetu), Google dorking.

Rekonesans aktywny

bezpośrednia interakcja z celem: skanowanie portów, banner grabbing, zapytania DNS o strefę — wyższe ryzyko wykrycia przez systemy monitorujące.

Footprinting

budowanie kompleksowego profilu organizacji: infrastruktura sieciowa, technologie, pracownicy, dostawcy — na tej podstawie planowany jest właściwy atak.

Implikacja obronna

organizacja powinna świadomie zarządzać swoim „śladem cyfrowym” — ograniczać publicznie dostępne metadane, szkolić pracowników w zakresie informacji publikowanych w mediach społecznościowych.

Praktyczny przykład: ogłoszenie o pracę „poszukujemy administratora z doświadczeniem w Exchange 2016 i Cisco ASA” to darmowy OSINT — ujawnia dokładny stack technologiczny atakującemu.

Skanowanie portów: nmap i typy skanów

Narzędzie, którego użyjemy za chwilę w laboratorium — zrozumienie mechaniki skanu jest kluczowe dla egzaminu.

nmap (Network Mapper)

najpowszechniejsze narzędzie do skanowania sieci i identyfikacji hostów, portów oraz usług — standard branżowy, darmowy i open-source.

TCP Connect scan

pełne nawiązanie połączenia TCP (trójstopniowy handshake) — najbardziej niezawodny, ale najłatwiejszy do wykrycia (widoczny w logach jako pełne połączenie).

SYN scan („half-open”)

wysyła tylko pakiet SYN, nie kończy handshake — szybszy i mniej widoczny w podstawowych logach, ale wciąż wykrywalny przez IDS/IPS.

UDP scan

wolniejszy i mniej niezawodny niż TCP (UDP jest bezpołączeniowy) — istotny, bo wiele usług (DNS, SNMP, NTP) działa na UDP.

Wykrywanie wersji usług (-sV)

identyfikuje nie tylko otwarty port, ale konkretną wersję oprogramowania nasłuchującego — kluczowe do dopasowania znanych podatności (CVE) do celu.

Zastosowanie dwustronne: nmap to narzędzie zarówno atakującego (rekonesans aktywny), jak i obrońcy (audyt własnej infrastruktury, wykrywanie nieautoryzowanych usług) — kontekst użycia decyduje o legalności.

Taksonomia ataków sieciowych

Mechanizm działania, nie tylko nazwa — dokładnie to, co sprawdza egzamin performance-based.

1

MitM — Man-in-the-Middle

Atakujący przechwytuje komunikację między dwiema stronami, które sądzą, że rozmawiają bezpośrednio ze sobą. Umożliwia podsłuch i modyfikację danych w locie.

2

ARP Spoofing

Atakujący wysyła fałszywe odpowiedzi ARP, kojarząc swój adres MAC z adresem IP innego urządzenia (np. bramy) w sieci lokalnej — klasyczna technika do przeprowadzenia MitM w LAN.

3

DNS Spoofing / Poisoning

Wstrzyknięcie fałszywych wpisów do cache serwera DNS lub odpowiedzi DNS — przekierowuje ofiarę na złośliwy adres IP mimo wpisania prawidłowej nazwy domeny.

4

On-path (dawniej: przechwytywanie sesji)

Atakujący fizycznie lub logicznie znajduje się na trasie komunikacji (np. złośliwy punkt WiFi) — nowsza terminologia CompTIA zastępująca starsze określenia.

5

Evil Twin

Fałszywy punkt dostępu WiFi podszywający się pod legalną sieć (np. "Hotel_WiFi_Free") — ofiary łączą się nieświadomie z siecią atakującego.

Bezpieczeństwo sieci bezprzewodowych

Od Evil Twin do standardu, który realnie chroni: WPA3 i uwierzytelnianie 802.1X.

WEP i WPA

przestarzałe, łamane w praktyce w minuty (WEP) lub podatne na atak słownikowy na handshake (WPA/WPA2-PSK ze słabym hasłem). Nie powinny występować w środowisku produkcyjnym.

WPA2 vs WPA3

WPA3 wprowadza SAE (Simultaneous Authentication of Equals) zamiast PSK — odporny na atak offline nawet przy słabszym hasle, oraz obowiązkowe szyfrowanie indywidualnych sesji (nawet w sieciach otwartych, Enhanced Open).

Tryb Personal (PSK) vs Enterprise (802.1X)

PSK to jedno współdzielone hasło dla wszystkich — brak indywidualnej rozliczalności. Enterprise wymaga uwierzytelnienia każdego użytkownika osobno przez serwer RADIUS.

EAP (Extensible Authentication Protocol)

rodzina protokołów uwierzytelniania używanych w trybie Enterprise — warianty EAP-TLS (certyfikaty, najsilniejszy) i PEAP (login/hasło w tunelu TLS) są najczęstsze w środowiskach korporacyjnych.

Rogue AP vs Evil Twin

Rogue AP to nieautoryzowany punkt dostępu podłączony przez pracownika (zwykle nieświadomie, dla wygody) do sieci firmowej. Evil Twin to celowo złośliwy AP podszywający się pod istniejącą sieć — różni je intencja i sposób podłączenia.

Rekomendacja praktyczna: sieć firmowa powinna działać w trybie WPA3-Enterprise z EAP-TLS, gościnna — w oddzielnym, odizolowanym VLAN-ie bez dostępu do zasobów wewnętrznych.

SYN Flood i DDoS

Ataki na dostępność — trzecią część triady CIA, obok poufności i integralności.

SYN Flood

atakujący wysyła masowo pakiety SYN bez dokończenia handshake TCP, wyczerpując tabelę połączeń oczekujących serwera. Obrona: SYN cookies, rate limiting.

DoS vs DDoS

DoS (Denial of Service) pochodzi z jednego źródła, łatwy do zablokowania (jeden adres IP). DDoS (Distributed) pochodzi z tysięcy/milionów źródeł jednocześnie, zwykle z botnetu.

Atak wolumetryczny

zalewa łącze internetowe ofiary surową ilością ruchu (np. UDP flood, DNS amplification) — cel: wyczerpać przepustowość, nie konkretny system.

Atak protokołowy

wykorzystuje słabości w implementacji protokołu (np. SYN Flood) — cel: wyczerpać zasoby konkretnego urządzenia (firewall, load balancer).

Atak aplikacyjny (warstwa 7)

imituje normalny ruch użytkownika, ale w dużej skali (np. powtarzane żądania do kosztownego zapytania bazodanowego) — najtrudniejszy do odróżnienia od ruchu legalnego.

Ochrona praktyczna: przeciwko DDoS wolumetrycznemu pojedyncza organizacja rzadko ma wystarczającą przepustowość — standardem jest usługa scrubbing (np. Cloudflare, AWS Shield) filtrująca ruch przed dotarciem do infrastruktury.

LAB 2.1.1 Finding Open Ports

LAB 2.1.1

Finding Open Ports

Skanowanie sieci, identyfikacja usług nasłuchujących na hostach, analiza wyników i przygotowanie raportu.

Czas: 30 min (11:30–12:15)

Domena SY0-701: Domena 2 — Threats, Vulnerabilities & Mitigations (rekonesans i skanowanie)

Kroki laboratorium

1. Zaloguj się do modułu 2.1.1 w CertMaster Labs.
2. Wykonaj podstawowy skan TCP Connect na przydzielony zakres adresów IP.
3. Powtórz skan z opcją wykrywania wersji usług (-sV).
4. Zidentyfikuj wszystkie otwarte porty i przypisane im usługi na każdym hoście.
5. Wskaż, które z wykrytych usług wyglądają na potencjalnie nadmiarowe lub ryzykowne (np. Telnet, FTP bez szyfrowania).
6. Przygotuj krótki raport: host, otwarte porty, usługa, wersja, rekomendacja.

Na co zwrócić uwagę

- **Zasada minimalnej powierzchni ataku** — każdy niepotrzebnie otwarty port to dodatkowy wektor ataku. Domyślna konfiguracja usług bywa nadmiarowa.
- **Protokoły bez szyfrowania** — Telnet (23), FTP (21), HTTP (80) bez wersji szyfrowanej — priorytet do migracji na SSH, SFTP, HTTPS.
- **Raport jako artefakt** — wynik skanowania bez interpretacji i rekomendacji to tylko dane. Wartość dodaje priorytetyzacja i kontekst biznesowy — dokładnie tak, jak w prawdziwym audycie.

Debrief: interpretacja wyników skanu w praktyce

Od surowej listy portów do raportu, który ktoś faktycznie wykorzysta.

Port otwarty ≠ podatność

otwarty port 443 z prawidłowo skonfigurowanym, aktualnym serwerem HTTPS nie jest sam w sobie problemem. Kontekst i konfiguracja usługi decydują o ryzyku.

False positive w skanowaniu

firewall może zwracać port jako "filtered" zamiast "closed", co bywa błędnie interpretowane jako otwarty — precyzja terminologii nmap ma znaczenie.

Priorytetyzacja wg ekspozycji

port otwarty na interfejsie publicznym (internet) jest znacznie krytyczniejszy niż ten sam port otwarty wyłącznie w sieci wewnętrznej za firewallem.

Regularne skanowanie jako proces

jednorazowy skan to zdjęcie momentu. Wartość operacyjną daje regularne, zaplanowane skanowanie i porównywanie wyników w czasie (drift detection).

OWASP Top 10 (2021) — przegląd

BLOK 4

Blok 4 (12:30–13:30): bezpieczeństwo aplikacji webowych. OWASP Top 10 to standardowy punkt odniesienia branży.

1

A01: Broken Access Control

Najczęstsza kategoria 2021 — użytkownik uzyskuje dostęp poza swoimi uprawnieniami.

2

A02: Cryptographic Failures

Słabe/brakujące szyfrowanie danych wrażliwych (dawniej "Sensitive Data Exposure").

3

A03: Injection

SQL Injection, command injection i pokrewne — omówimy szczegółowo za chwilę.

4

A04: Insecure Design

Nowa kategoria 2021 — problem architektoniczny, nie tylko błąd implementacji.

5

A05: Security Misconfiguration

Domyślne hasła, niepotrzebnie włączone funkcje, brak hardeningu.

6

A06: Vulnerable and Outdated Components

Biblioteki i zależności ze znanymi CVE — powiązane z SBOM, temat wróci przy CRA.

7

A07: Identification and Authentication Failures

Słabe uwierzytelnianie, brak MFA, zarządzanie sesją.

8

A10: Server-Side Request Forgery (SSRF)

Nowa kategoria 2021 — serwer zmuszony do wykonania żądania w imieniu atakującego.

SQL Injection: mechanika ataku

Jedna z najstarszych, wciąż powszechnie spotykanych i wciąż w pełni zapobiegalnych podatności.

Mechanizm

aplikacja buduje zapytanie SQL, wstawiając bezpośrednio dane od użytkownika do treści zapytania, bez odpowiedniego oczyszczenia — atakujący wstrzykuje własny kod SQL, zmieniając logikę zapytania.

Klasyczny przykład

pole logowania budujące zapytanie jako tekst: wpisanie w pole hasła frazy kończącej cudzysłów i dodającej warunek zawsze prawdziwy pozwala ominąć weryfikację hasła.

In-band SQLi

atakujący widzi wynik ataku bezpośrednio w odpowiedzi aplikacji (np. dodatkowe dane w widocznym komunikacie błędu).

Blind SQLi

aplikacja nie zwraca bezpośrednio danych, ale atakujący wnioskuje o prawdziwość warunków na podstawie zachowania aplikacji (różnica w czasie odpowiedzi, różne komunikaty).

Out-of-band SQLi

wynik ataku przesyłany innym kanałem niż odpowiedź HTTP, np. przez zapytanie DNS wygenerowane przez bazę danych — stosowane, gdy pozostałe metody są zablokowane.

Kluczowy środek zaradczy: zapytania parametryzowane (prepared statements) — dane od użytkownika NIGDY nie są wstawiane bezpośrednio do treści zapytania SQL. To rozwiązuje problem u źródła, nie tylko łagodzi objawy.

Cross-Site Scripting (XSS)

Wstrzyknięcie złośliwego kodu wykonywanego nie na serwerze, lecz w przeglądarce ofiary.

Mechanizm ogólny

aplikacja wyświetla dane pochodzące od użytkownika bez odpowiedniego oczyszczenia (encoding) — atakujący wstrzykuje kod JavaScript wykonywany w przeglądarce innej osoby (ofiary), nie atakującego.

Stored XSS

złośliwy skrypt jest trwale zapisany po stronie serwera (np. w komentarzu na forum) i wykonuje się u każdego, kto wyświetli tę stronę — najgroźniejszy wariant, największy zasięg.

Reflected XSS

złośliwy skrypt jest częścią ządania (np. parametru w URL) i „odbija się” bezpośrednio w odpowiedzi — wymaga, by ofiara kliknęła spreparowany link (element phishingu).

DOM-based XSS

podatność istnieje wyłącznie po stronie klienta, w kodzie JavaScript przetwarzającym dane w przeglądarce — serwer w ogóle nie widzi złośliwego ładunku.

Skutki

kradzież ciasteczek sesji (przejęcie konta), przekierowanie na stronę phishingową, modyfikacja treści widocznej dla ofiary, keylogging w przeglądarce.

Kluczowy środek zaradczy: output encoding (kodowanie danych przed wyświetleniem) + nagłówek Content-Security-Policy, o którym mówiliśmy przy HSTS — ogranicza, jakie skrypty w ogóle mogą się wykonać.

CSRF i Broken Access Control

Dwie kategorie ataków wykorzystujące zaufanie aplikacji do zalogowanej sesji lub żądania użytkownika.

CSRF (Cross-Site Request Forgery)

- **Mechanizm:** atakujący zmusza przeglądarkę zalogowanej ofiary do wysłania niechcianego żądania do aplikacji, w której ofiara ma aktywną sesję (np. przelew bankowy) — bez wiedzy ofiary.
- **Warunek ataku:** ofiara musi być jednocześnie zalogowana w atakowanej aplikacji i odwiedzić stronę kontrolowaną przez atakującego (np. przez link w mailu).
- **Obrona:** token CSRF unikalny dla każdej sesji/formularza, weryfikowany przez serwer przy każdym żądaniu modyfikującym dane.

Broken Access Control (OWASP A01)

- **Insecure Direct Object Reference (IDOR):** zmiana identyfikatora w URL (np. numeru zamówienia) ujawnia dane innego użytkownika bez weryfikacji uprawnień.
- **Eskalacja pozioma vs pionowa:** pozioma = dostęp do danych innego użytkownika tego samego poziomu; pionowa = zwykły użytkownik uzyskuje uprawnienia administratora.
- **Obrona:** weryfikacja uprawnień przy KAŻDYM żądaniu po stronie serwera — nigdy poleganie wyłącznie na ukryciu opcji w interfejsie (security through obscurity).

SDLC i DevSecOps

Bezpieczeństwo wbudowane w proces wytwarzania oprogramowania, nie doklejone na końcu.

SDLC (Software Development Lifecycle)

planowanie, projektowanie, implementacja, testowanie, wdrożenie, utrzymanie. Tradycyjnie bezpieczeństwo testowano dopiero na końcu (przed wdrożeniem).

Shift-left

przesunięcie testów bezpieczeństwa jak najwcześniej w cyklu — błąd znaleziony w fazie projektowania kosztuje ułamek tego, co ten sam błąd znaleziony po wdrożeniu produkcyjnym.

SAST (Static Application Security Testing)

analiza kodu źródłowego bez jego uruchamiania — wykrywa wzorce podatne na SQLi, XSS itd. już na etapie pisania kodu, zintegrowana z IDE/CI.

DAST (Dynamic Application Security Testing)

testowanie działającej aplikacji „z zewnątrz”, symulując realne ataki — wykrywa problemy, których SAST nie widzi (błędy konfiguracji środowiska uruchomieniowego).

SCA (Software Composition Analysis)

skanowanie bibliotek i zależności pod kątem znanych CVE — bezpośrednio odpowiada na kategorię A06 OWASP i wymogi SBOM z CRA (temat wróci jutro).

Rodzaje podatności — nie tylko aplikacja webowa

Egzamin SY0-701 wymaga rozróżnienia kategorii podatności poza samym kodem aplikacji.

1

Zero-day

Podatność nieznaną jeszcze producentowi — nie istnieje dla niej łatka w momencie wykorzystania. Najgroźniejsza kategoria, bo klasyczne łatanie nie pomaga.

2

Błędna konfiguracja (misconfiguration)

Najczęstsza realna przyczyna wycieków danych: domyślne hasła, publicznie dostępny zasobnik chmurowy, nadmiarowe uprawnienia — nie błąd w kodzie, lecz w ustawieniach.

3

Systemy przestarzałe / EOL (End-of-Life)

Oprogramowanie, dla którego producent zakończył wsparcie i przestał wydawać łatki bezpieczeństwa — podatność narasta z każdym dniem, nie da się jej „załatać”.

4

Race condition (warunek wyścigu)

Błąd wynikający z kolejności/czasu wykonania współbieżnych operacji — np. TOCTOU (Time-of-Check to Time-of-Use), gdy stan zasobu zmienia się między sprawdzeniem a użyciem.

5

Podatność łańcucha dostaw

Luka wprowadzona nie przez organizację, lecz przez jej dostawcę — bibliotekę, komponent sprzętowy, aktualizację. Wraca jutro przy CRA i wymogu SBOM.

LAB 8.1.1 SQL Injection

LAB 8.1.1

SQLi

Wykonanie ataku SQL Injection na podatną aplikację testową, analiza skutków oraz zastosowanie środków zaradczych.

Czas: 30 min (13:00–13:30)

Domena SY0-701: Domena 2 — Threats, Vulnerabilities & Mitigations (Injection, OWASP A03)

Kroki laboratorium

1. Zaloguj się do modułu 8.1.1 w CertMaster Labs.
2. Zapoznaj się z podatną aplikacją testową (prosty formularz logowania).
3. Wykonaj klasyczny atak obejścia logowania przez SQL Injection.
4. Zaobserwuj i zapisz, jaki dokładnie ciąg znaków zmienił logikę zapytania.
5. Przejrzyj kod źródłowy aplikacji i zidentyfikuj miejsce podatne na wstrzyknięcie.
6. Zastosuj poprawkę (zapytanie parametryzowane) i potwierdź, że atak przestaje działać.

Na co zwrócić uwagę

- **Ten sam atak, inna aplikacja** — mechanizm SQL Injection jest identyczny niezależnie od technologii (PHP, Java, .NET, Python) — różni się tylko dokładna składnia.
- **Poprawka nie jest kosmetyczna** — zapytanie parametryzowane eliminuje CAŁĄ klasę podatności, nie tylko konkretny przetestowany przypadek.
- **Powiązanie z Blokiem 6** — ta sama podatność zostałaby wykryta przez skaner podatności aplikacyjnych — wrócimy do tego przy zarządzaniu podatnościami.

Ewolucja zapór sieciowych

BLOK 5

Blok 5 (13:30–14:15): zapory sieciowe i segmentacja. Cztery generacje, coraz wyższa warstwa OSI inspekcji.

Packet Filter (generacja 1)

analizuje pojedyncze pakiety niezależnie od siebie: adres źródłowy/docelowy, port, protokół (warstwa 3–4 OSI). Brak pamięci o stanie połączenia.

Stateful Firewall (generacja 2)

śledzi stan każdego połączenia (tabela stanów) — rozumie, że pakiet odpowiedzi należy do już nawiązanego, legalnego połączenia. Standard od lat 90.

NGFW — Next-Generation Firewall (generacja 3)

dodaje inspekcję do warstwy 7 (aplikacji): rozpoznaje konkretną aplikację niezależnie od portu, integruje IPS, filtrowanie URL, czasem sandboxing.

WAF — Web Application Firewall (generacja wyspecjalizowana)

NGFW dedykowany wyłącznie ruchowi HTTP/HTTPS — rozumie strukturę żądań webowych, blokuje wzorce SQLi/XSS z Bloku 4 na poziomie sieci, jako dodatkowa warstwa obrony.

Zasada praktyczna: każda kolejna generacja NIE zastępuje poprzedniej warstwy ochrony — dobra architektura łączy stateful firewall na obwodzie sieci z NGFW/WAF bliżej aplikacji (defense in depth).

DMZ oraz architektura stref bezpieczeństwa

Jak fizycznie i logicznie oddzielić usługi publiczne od wewnętrznej sieci firmowej.

DMZ (strefa zdemilitaryzowana)

- **Cel:** umieszczenie usług dostępnych publicznie (serwer WWW, serwer poczty) w osobnej strefie sieciowej, oddzielonej od sieci wewnętrznej DWOMA zaporami.
- **Logika:** jeśli atakujący przejmie serwer w DMZ, wciąż musi pokonać drugą zaporę, żeby dostać się do wewnętrznej sieci firmowej z danymi wrażliwymi.
- **Typowa architektura:** Internet → firewall zewnętrzny → DMZ (serwery publiczne) → firewall wewnętrzny → sieć korporacyjna (LAN).

NAT (Network Address Translation)

- **Funkcja pierwotna:** oszczędność adresów IPv4 — wiele urządzeń wewnętrznych z prywatnymi adresami dzieli jeden publiczny adres IP.
- **Efekt uboczny bezpieczeństwa:** urządzenia wewnętrzne nie są bezpośrednio adresowalne z internetu — NAT działa jako naturalna, choć niepełna, bariera.
- **Zastrzeżenie:** NAT to NIE firewall — nie analizuje treści ruchu ani nie egzekwuje polityki bezpieczeństwa, tylko tłumaczy adresy.

Segmentacja VLAN i mikrosegmentacja

Dzielenie sieci na mniejsze, izolowane strefy — ograniczanie ruchu lateralnego atakującego po włamaniu.

VLAN (Virtual Local Area Network)

logiczny podział jednej fizycznej sieci na wiele odrębnych sieci logicznych, bez konieczności osobnego okablowania. Ruch między VLAN-ami wymaga przejścia przez router/firewall.

Typowa segmentacja korporacyjna

osobne VLAN-y dla: stacji roboczych pracowników, serwerów, urządzeń drukujących, gości (guest network), urządzeń IoT — każdy z inną polityką dostępu.

Dlaczego to działa obronnie

jeśli atakujący przejmie jedno urządzenie w VLAN-ie gości, nie ma bezpośredniego dostępu do VLAN-u z serwerami finansowymi — musi pokonać dodatkową kontrolę na granicy VLAN-ów.

Mikrosegmentacja

znacznie bardziej granularne podejście, typowe dla środowisk chmurowych i wirtualizowanych: polityka bezpieczeństwa definiowana per pojedyncze obciążenie (workload), nie per cała podsieć.

Ruch lateralny (lateral movement)

technika ataku z MITRE ATT&CK (poranny slajd), w której atakujący, po przejęciu jednego hosta, próbuje poruszać się dalej w głąb sieci. Segmentacja to bezpośrednia kontrola przeciwko tej technice.

Zero Trust — wprowadzenie

Fundamentalna zmiana filozofii: od „zaufaj, ale weryfikuj” do „nigdy nie ufaj, zawsze weryfikuj”. Pełne rozwinięcie jutro.

Model tradycyjny (perimeter security)

silna ochrona na granicy sieci (firewall obwodowy), ale domyślne zaufanie do wszystkiego „wewnątrz” — klasyczny zamek z fosą.

Problem modelu tradycyjnego

jeśli atakujący (lub złośliwy insider) znajdzie się „wewnątrz” — np. przez phishing albo VLAN gościnny — ma relatywnie swobodny ruch lateralny.

Zero Trust — zasada podstawowa

„never trust, always verify” — żadne żądanie nie jest domyślnie zaufane, niezależnie od tego, czy pochodzi z sieci wewnętrznej czy zewnętrznej.

Każde żądanie weryfikowane niezależnie

tożsamość, stan urządzenia (czy jest zainstalowane, czy ma aktywny antywirus), kontekst (lokalizacja, pora dnia) — przy KAŻDYM dostępie do zasobu, nie tylko przy logowaniu.

Rozwinięcie jutro

pełna architektura Zero Trust wg NIST SP 800-207, mikrosegmentacja jako element ZTA, ZTNA vs klasyczny VPN — Blok 8, Dzień 2.

Zapowiedź: Zero Trust to nie pojedynczy produkt do kupienia — to architektura i filozofia, budowana latami z wielu komponentów (IAM, MFA, mikrosegmentacja, monitoring). Jutro poświęcimy temu cały blok.

LAB 9.2.1 Firewall

LAB 9.2.1

Firewall

Konfiguracja reguł zapory sieciowej oraz testowanie ich skuteczności w symulowanym środowisku.

Czas: 30 min (w ramach bloku 13:30–14:15)
Domena SY0-701: Domena 3 — Security Architecture (kontrola sieciowa, segmentacja)

Kroki laboratorium

1. Zaloguj się do modułu 9.2.1 w CertMaster Labs.
2. Przeanalizuj domyślną (zbyt permissywną) konfigurację reguł zapory w środowisku testowym.
3. Skonfiguruj regułę blokującą ruch przychodzący na nieużywane porty.
4. Skonfiguruj regułę dopuszczającą ruch wyłącznie z zaufanej podsieci do usługi administracyjnej.
5. Przetestuj skuteczność reguł, próbując połączyć się z dozwolonego i niedozwolonego źródła.
6. Zweryfikuj kolejność reguł (order matters) — sprawdź efekt zamiany kolejności dwóch reguł.

Na co zwrócić uwagę

- **Domyślna polityka: deny-all** — dojrzała konfiguracja zaczyna od zablokowania wszystkiego i jawnie dopuszcza tylko to, co konieczne — nie odwrotnie.
- **Kolejność reguł ma znaczenie** — większość zapór przetwarza reguły sekwencyjnie, od góry — pierwsza pasująca reguła wygrywa, kolejne są ignorowane.
- **Zasada least privilege w sieci** — to samo pojęcie, które omawialiśmy przy IAM w efektach uczenia się, zastosowane do ruchu sieciowego, nie tylko uprawnień użytkownika.

Zarządzanie podatnościami: cykl VMP

BLOK 6

Blok 6 (14:15–15:00): zarządzanie podatnościami. Od jednorazowego skanu do systematycznego procesu.

VMP (Vulnerability Management Process)

cykliczny proces, nie jednorazowe działanie: identyfikacja → priorytetyzacja → naprawa (remediation) → weryfikacja → powrót do identyfikacji.

CVE (Common Vulnerabilities and Exposures)

unikalny, publiczny identyfikator konkretnej, udokumentowanej podatności (format CVE-rok-numer) — wspólny język między producentami, badaczami i obrońcami.

NVD (National Vulnerability Database)

prowadzona przez amerykański NIST baza wzbogacająca wpisy CVE o ocenę CVSS, listę podatnych produktów i referencje.

Cykl życia podatności

odkrycie → (opcjonalnie) responsible disclosure do producenta → publikacja CVE → publikacja łatki przez producenta → wdrożenie łatki przez organizację. Każdy etap to okno ryzyka.

Powiązanie z dzisiejszym laboratorium 2.1.1

skan portów i wersji usług z bloku trzeciego to pierwszy krok VMP — identyfikacja. Dziś zamykamy pętlę: co robić z tą wiedzą dalej.

CVSS v4: metryki i interpretacja wyniku

Jak liczbowo ocenić krytyczność podatności, zamiast polegać na subiektywnej ocenie „to wygląda groźnie”.

CVSS (Common Vulnerability Scoring System)

standardowa metodologia oceny krytyczności podatności, wynik liczbowy od 0.0 do 10.0. Aktualna wersja: CVSS v4.0 (opublikowana 2023).

Grupa metryk bazowych (Base)

niezależne od czasu i środowiska: wektor ataku (sieć/lokalny), złożoność ataku, wymagane uprawnienia, wymagana interakcja użytkownika, wpływ na CIA.

Skala interpretacji

0.1–3.9 Niski · 4.0–6.9 Średni · 7.0–8.9 Wysoki · 9.0–10.0 Krytyczny.

Nowość w v4.0

dodano metryki Supplemental (dodatkowe, opcjonalne) i doprecyzowano ocenę wpływu na system podatny vs system kolejny (Vulnerable/Subsequent System) — istotne dla ataków łańcuchowych.

Kluczowe zastrzeżenie

sam wynik CVSS Base NIE mówi, czy dana podatność jest FAKTYCZNIE wykorzystywana w atakach na wolności (in the wild) — do tego potrzebny jest EPSS, o którym za chwilę.

Pytanie z pre-testu: CVSS to system oceny liczbowej krytyczności podatności — pytanie 4 z porannego pre-testu, dokładnie ten temat.

EPSS i CISA KEV: priorytetyzacja oparta na ryzyku

Odpowiedź na fundamentalne ograniczenie CVSS: co naprawdę naprawiać najpierw, mając ograniczony czas zespołu.

Problem praktyczny

w typowej organizacji rocznie ujawnianych jest dziesiątki tysięcy CVE. Nawet ograniczając się do „Krytycznych” wg CVSS, zostaje ich zbyt wiele, by załatać wszystkie natychmiast.

EPSS (Exploit Prediction Scoring System)

model statystyczny szacujący prawdopodobieństwo (0–100%), że dana podatność zostanie faktycznie wykorzystana w ataku w ciągu najbliższych 30 dni.

Różnica CVSS vs EPSS

CVSS = „jak groźna JEST ta podatność, gdyby ją wykorzystano” (teoria). EPSS = „jak prawdopodobne jest, że ZOSTANIE wykorzystana” (praktyka/statystyka).

CISA KEV (Known Exploited Vulnerabilities)

oficjalna lista podatności amerykańskiej agencji CISA, o których jest POTWIERDZONA wiedza, że są aktywnie wykorzystywane w rzeczywistych atakach — najwyższy priorytet praktyczny.

Praktyczna formuła priorytetyzacji

Krytyczność (CVSS) × Prawdopodobieństwo wykorzystania (EPSS) × Krytyczność aktywa dla biznesu = realny priorytet łatania, nie sam surowy wynik CVSS.

Zasada praktyczna: podatność na liście CISA KEV powinna mieć priorytet nad podatnością o wyższym CVSS, ale bez potwierdzonego wykorzystania w praktyce — realne zagrożenie bije teoretyczne.

LAB 8.3.1 Vulnerability Scans

LAB 8.3.1

Vulnerability Scans

Uruchomienie skanera podatności w środowisku symulowanym oraz analiza wygenerowanego raportu.

Czas: 30 min (w ramach bloku 14:15–15:00)
Domena SY0-701: Domena 2 — Threats, Vulnerabilities & Mitigations (zarządzanie podatnościami)

Kroki laboratorium

1. Zaloguj się do modułu 8.3.1 w CertMaster Labs.
2. Uruchom automatyczny skan podatności na przydzielonym środowisku testowym.
3. Przejrzyj wygenerowany raport: liczba znalezisk, rozkład wg poziomu krytyczności.
4. Wybierz trzy znaleziska o najwyższym CVSS i zidentyfikuj odpowiadające im CVE.
5. Zasymuluj priorytetyzację: dla każdego z trzech znalezisk oceń (na podstawie opisu) prawdopodobny EPSS.
6. Sformułuj rekomendację kolejności łatania dla zespołu IT — z uzasadnieniem.

Zamknięcie dnia 1 — od skanu do decyzji

- **To ostatnie laboratorium dnia** — domyka pełną pętlę: rekonesans (Blok 3) → identyfikacja podatności aplikacyjnej (Blok 4) → segmentacja jako kontrola (Blok 5) → priorytetyzacja naprawy (Blok 6).
- **Skaner to narzędzie, nie decyzja** — automatyczny raport dostarcza surowych danych; priorytetyzacja i decyzja biznesowa zawsze wymaga kontekstu, którego skaner nie zna.
- **Jutro:** od prewencji (dzisiejszy dzień) przechodzimy do detekcji i reakcji — monitoring, SIEM, reagowanie na incydenty.

Podsumowanie Dnia 1 — kluczowe wnioski

Sześć bloków, sześć laboratoriów, jedna spójna logika: prewencja na każdej warstwie modelu OSI.

Krajobraz zagrożeń

zrozumienie aktorów (od script kiddies po APT) i mechanizmów (malware, ransomware 4. generacji) jest punktem wyjścia dla każdej decyzji obronnej.

Kryptografia

symetryczna (AES-256/GCM) dla wydajności, asymetryczna (RSA/ECDH) dla bezpiecznej wymiany klucza i podpisu, PKI dla weryfikacji tożsamości, TLS 1.3 łączy wszystko z Perfect Forward Secrecy.

Bezpieczeństwo sieci

model OSI jako mapa ataku i obrony; nmap i skanowanie jako pierwszy krok zarówno ataku, jak i audytu.

Bezpieczeństwo aplikacji

OWASP Top 10 jako standard branżowy; SQLi i XSS jako klasyczne, wciąż aktualne wektory; shift-left/DevSecOps jako odpowiedź procesowa.

Architektura obronna

zapory (Packet Filter → NGFW), DMZ, segmentacja VLAN i mikrosegmentacja, Zero Trust jako kierunek rozwoju — wszystko realizujące defense in depth.

Mapowanie na SY0-701: dzisiejszy dzień pokrył istotną część Domeny 1 (General Security Concepts), Domeny 2 (Threats, Vulnerabilities & Mitigations) i Domeny 3 (Security Architecture).

Zapowiedź Dnia 2

Od prewencji do detekcji, reakcji i zgodności regulacyjnej — jutro 07:00, ta sama sala wirtualna.

Blok 7 — Monitoring i SIEM:

architektura monitorowania, źródła logów, reguły korelacji, alert fatigue. LAB 11.2.1 System Monitoring.

Blok 8 — IAM i Zero Trust:

pełne rozwinięcie RBAC, MFA/2FA, PAM oraz architektury Zero Trust wg NIST SP 800-207. LAB 12.1.1 IR Detection.

Bloki 9–11 — Forensics, reagowanie na malware, playbooki IR i SOAR:

LAB 12.3.1 Network Sniffers, LAB 13.1.1 Malware Response, LAB 14.1.1 Playbook.

Blok 12 — BCP/DR:

BIA, metryki MTD/RTO/RPO/WRT, reguła 3-2-1-1-0. LAB 7.1.1 Backups.

Blok 13 — NIS2/UoKSC/CRA dla specjalistów IT:

wymogi regulacyjne, mapa certyfikacji CompTIA, ścieżki kariery. Zamknięcie: post-test i wręczenie zaświadczeń.

Zadanie na wieczór (opcjonalne): w arkuszu ćwiczeń, który Państwo otrzymali, sekcja „Gap Analysis” — proszę zastanowić się, które z dzisiejszych sześciu obszarów są w Państwa organizacji najslabiej pokryte. Wrócimy do tego jutro w kontekście regulacyjnym.

ZAKOŃCZENIE DNIA 1

Pytania i odpowiedzi

Wracamy do pytań zaparkowanych w trakcie dnia oraz do tych, które pojawiły się przy ćwiczeniach.

✓ Konsultacja poszkoleniowa: 30 minut on-line w ciągu 30 dni – umów ją mailowo



Dziękuję za uwagę

ltmastery.com@gmail.com · Dostawca Usług w Bazie Usług Rozwojowych, ID 204299

Źródła: wykaz-ksc.gov.pl · gov.pl/cyber · cert.pl · enisa.europa.eu