PIWIK PRO

Wstęp do cyberbezpieczeństwa na podstawie certyfikacji CompTIA Security+

Plan prezentacji

1. Co to i po co to komu?
   - Ogólnie o certyfikacie
   - Dla kogo on jest?

2. Podstawy bezpieczeństwa - zakres certyfikatu
   - Podział dziedziny według CompTIA
   - Przykładowe zagadnienia z każdej dziedziny
   - Przykładowe pytania

3. Informacje praktyczne - jak się przygotować żeby zdać?
   - Jak, gdzie i za ile?
   - Materiały do nauki
   - Protipy do zdania

Co to i po co to komu?

CompTIA Security+

- Entry-level certyfikat z bardzo szeroko rozumianego cyberbezpieczeństwa
- Vendor-neutral certification
- Ostatni z podstawowej ścieżki certyfikacyjnej CompTIA
- Bardzo szeroki zakres materiału teoretycznego
- Nacisk na stronę praktyczną

Dla kogo?

- Dla osób na stanowiskach technologicznych i około technologicznych (np dla managerów)
- Dla ludzi z technicznym doświadczeniem ok. 2 lat (niewymagane)
- Dla kogoś, kto chciałby pracować w (amerykańskim) rządzie lub wojsku - ISO 17024, US DoD 8140/8570.01-M, ANSI
- Dla osoby, która chciałaby spojrzeć na cyberbezpieczeństwo organizacji w możliwie jak najszerszy sposób
- Nie dla Hacker-Mana

Podstawy bezpieczeństwa - zakres certyfikatu

Attacks, Threats, and Vulnerabilities

1. Social engineering
2. Rodzaje ataków i jak je rozpoznać
3. Podatności i typy ataków na aplikacjach
4. Podatności i typy ataków sieciowych
5. Podmioty, wektory i źródła informacji wywiadowczych.
6. Możliwe luki i słabości różnych środowisk
7. Ocena bezpieczeństwa środowiska
8. Testy penetracyjne

Przykładowe pytanie:

While conducting a penetration test of an organization's web applications, you attempt to insert the following script into the search form on the company's web site:

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

<script>alert("This site is vulnerable to an attack!")</script>

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Then, you clicked the search button, and a pop-up box appears on your screen showing the following text, "This site is vulnerable to an attack!" Based on this response, what vulnerability have you uncovered in the web application?

C. XSS

Architecture and Design

1. Bezpieczeństwo firmy
2. Wirtualizacja i Cloudy
3. Automatyzacja, DevOps
4. Autentykacja i autoryzacja
5. Zapewnianie ciągłości działania
6. Systemy wbudowane i specjalistyczne
7. Fizyczne zabezpieczenia
8. Podstawy kryptografii

Przykładowe pytanie:

You are helping to set up a backup plan for your organization. The current plan states that all of the organization's servers must have a daily backup conducted. These backups are then saved to a local NAS device. You have been asked to recommend a method to ensure the backups will work when needed for restoration. Which of the following should you recommend?

Attempt to restore to a test server from one of the backup files to verify them.

Implementation

1. Protokoły
2. Zabezpieczanie hostów i aplikacji
3. Projektowanie bezpiecznych sieci
4. Bezpieczeństwo sieci bezprzewodowych
5. Bezpieczeństwo urządzeń mobilnych
6. Bezpieczeństwo rozwiązań chmurowych
7. Zarządzanie kontami użytkowników
8. Wdrażanie autoryzacji i autentykacji
9. PKI

Przykładowe pytanie:

Which of the following does a User Agent request a resource from when conducting a SAML transaction?

D. Service provider (SP)

Operations and Incident Response

1. Narzędzia i aplikacje
2. Polityki, procesy i procedury (Incident Response)
3. Logi i inne źródła danych
4. Podatności i typy ataków sieciowych
5. Techniki zabezpieczenia środowiska
6. Digital forensic (techniki kryminalistyczne)

You have run a vulnerability scan and received the following output:

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

CVE-2011-3389

QID 42366 - SSLv3.0/TLSv1.0 Protocol weak CBC mode Server side vulnerability

Check with: openssl s_client -connect login.diontraining.com:443 - tls -cipher "AES:CAMELLISA:SEED:3DES:DES"

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Which of the following categories should this be classified as?

B. Web application cryptography vulnerability

Governance, Risk, and Compliance

1. Rodzaje kontroli
2. Regulacje, akty prawne i standardy
3. Polityki i procedury jako sposób zapewnienia bezpieczeństwa organizacji
4. Zarządzanie ryzykiem
5. Prywatne i wrażliwe dane

Przykładowe pytanie:

MyCompany has performed an assessment as part of their disaster recovery planning. The assessment found that the organization's RAID takes, on average, about 8 hours to repair when two drives within the RAID fail. Which of the following metrics would best represent this time period?

D. MTTR

Informacje praktyczne - jak się przygotować żeby zdać?

Jak, gdzie i za ile?

1

Na oficjalnej stronie CompTIA trzeba kupić voucher. Koszt waha się w granicach 330€ (~1500 pln)

2

Są dwie opcje zdawania, oba przez PearsonVUE:

- Stacjonarnie
- Online

3

Czas trwania: 90 minut plus 45 za bycie z nieanglojęzycznego kraju

4

Trzeba zdobyć przynajmniej 750/900 pkt. ~ zazwyczaj jest około 85 pytań, wszystkie wielokrotnego wyboru + symulacje

Certyfikat jest ważny przez 3 lata - żeby go przedłużyć trzeba, zrobić kolejne (wyższe) certyfikaty, publikować materiały, zdobywać doświadczenie zawodowe lub przejść przez kurs oferowany przez CompTIA.

Polecane materiały

1. Przede wszystkim dobry kurs na udemy ~ ja korzystałem z DionTrening zarówno kursu w postaci filmików jak i jego testów
2. Oficjalna książka - strasznie dużo materiału, oraz wysoka cena. Dobra do “doczytywania” trudniejszych konceptów.
3. Inna książka w bardzo wygodnej elektronicznej formie, z wyszukiwarką, przykładowymi pytaniami i dwoma całymi testami - bardzo polecam. Wystarczy trail albo taniutka subskrybcja żeby mieć dostęp.
4. Dużo przykładowych testów:
   - Przykładowy test z samego CompTIA (króciutka wersja próbna ale moim zdaniem warto)
   - Exam dumpy dostępne w internecie (aczkolwiek jest to nielegalne)
   - Nie kupujcie żadnych rzeczy droższych niż ~10$ - prawdopodobnie to ściema

Protips

- Bardzo dużo skrótów, akronimów oraz portów/protokołów do nauczenia się. Polecam zrobić sobie fiszki (np. w Anki)
- Zacząć na egzaminie od pytań wielokrotnego wyboru, czasu jest dużo więc spokojnie się zdąży zrobić wszystko.
- Jeszcze raz: przerobić dużo testów żeby wiedzieć czego się nie wie.
- Uczyć się codziennie i systematycznie :)
- Na sam egzamin wziąć dzień wolny i wyprosić wszystkich z domu w przypadku opcji online (dowolny głos będzie podstawą do anulowania egzaminu)

Mój pierwszy cert: