**Pytania nasze**

**Bezpieczeństwo systemów internetowych i baz danych (semestr letni 2023/24)**

**1. Na czym polega spoofing? Wymień rodzaje spoofingu.**

Spoofing (maskarada) – podanie się za kogoś innego, niż jest się w rzeczywistości. System na podstawie informacji podawanych przez atakującego rozpoznaje go jako uprawniony użytkownik.

Rodzaje**:** IP spoofing – polega na podmianie adresu IP na fałszywy, w celu potwierdzenia swojej tożsamości dla określonych usług.

ARP spoofing – rozsyłany jest odpowiedni pakiet ARP, który zawiera fałszywe dane MAC. Efektem jest przechowywanie danych przez komputer o fałszywym adresie MAC.

E-mail spoofing – zmieniane są nagłówki e-maili, aby wyglądały na wysyłane z zaufanego adresu e-mail

**2.Czym jest ransomware?**

Ransomware to złośliwe oprogramowanie, które szyfruje dane ofiary, a następnie umieszcza informacje co musi zrobić użytkownik by odzyskać te dane. Zazwyczaj atakowanym pokazuje się komunikat z żądaniem okupu.

**3.Scharakteryzuj schemat kryptograficzny z użyciem klucza symetrycznego.**

Szyfrowanie symetryczne oparte jest na wykorzystywaniu pojedynczego klucza tajnego do szyfrowania i deszyfracji. Jest to parametr wejściowy określający szczegóły działania algorytmu szyfrującego niezależny od samego algorytmu ani od tekstu jawnego.

Algorytm szyfrujący musi być na tyle solidny, by znający go intruz, dysponujący dodatkowo zestawem szyfrogramów, nie był w stanie odtworzyć tekstu jawnego bez znajomości użytego klucza.

W tej grupie plasują się zarówno proste algorytmy np. szyfr Cezara, jak i nowoczesne algorytmy w postaci AES i różnych odmian DES.

**4. Jak działa uwierzytelnianie dwuskładnikowe?**

Uwierzytelnianie dwuskładnikowe wprowadza dodatkowe zabezpieczenie do istniejącego już sposobu uwierzytelniania.

Polega to na uwierzytelnianiu w dwóch etapach: w pierwszym podajemy zazwyczaj swój login i hasło, natomiast w kroku drugim dodawany jest drugi materialny składnik uwierzytelniania: token sprzętowy.

Token istnieje tylko w jednym konkretnym egzemplarzu i nie może zostać zduplikowany – dostęp do niego wiąże się z jawną kradzieżą lub fizycznym dostępem co może zostać zauważone (cecha „coś co posiadasz”).

Żeby użyć tokenu niezbędne jest posiadanie hasła, zatem samo posiadanie tokenu nie jest przydatne (cecha „coś co wiesz”).

Uwierzytelnianie dwuskładnikowe występuje w wielu obecnie wykorzystywanych usługach:

- Systemy bankowe: podczas wypłaty gotówki z bankomatu oprócz karty (cecha „coś co posiadasz”) niezbędne jest podanie kodu PIN (cecha „coś co wiesz”).

- Wiele usług internetowych, np. logowanie do konta pocztowego Gmail: po podaniu loginu i hasła (cecha „coś co wiesz”) użytkownik musi podać kod uwierzytelniający SMS z telefonu, którego numer został podany podczas rejestracji (cecha „coś co posiadasz”) .

**5. Czym jest dowód z wiedzą zerową? Podaj przykład.**

Dowód z wiedzą zerową jest procedurą kryptograficzną, w której jedna z komunikujących się stron potrafi udowodnić, że posiada tajną informację nie ujawniając jej treści.

Użytkownik A wchodzi do labiryntu i na rozwidleniu wybiera jedną z dróg

Użytkownik B wchodzi do labiryntu, zatrzymuje się w punkcie kontrolnym na rozwidleniu dróg

Użytkownik B rzuca monetą (losowo wybiera drogę)

Użytkownik A musi teraz wyjść z wybranej przez Użytkownika B ścieżki niezależnie którą ścieżką wszedł na początku.

Aby upewnić się że użytkownik A na prawdę zna sposób przejścia labiryntu cała procedura jest powtarzana n-razy. Przy wystarczająco dużej liczbie prób, szansa na to, że użytkownik A zawsze będzie potrafił poprawnie wyjść bez naprawdę znajomości labiryntu, jest bliska zeru.

Losowy rzut monetą i poprawne wyjście użytkownika A za każdym razem powoduje że nie może być to tylko kwestia szczęścia, a Użytkownik A zna tajną informację.

**6.Statystyczna analiza zachowania w systemach IDPS.**

Systemy IDPS ukierunkowane są na wykrycie potencjalnego ataku (pasywny system IDS) i zapobiegnięcie jego skutkom (reaktywny system IPS). Dodatkowo zapisywane są informacje o ataku w dzienniku zdarzeń oraz generowany jest alert o wystąpieniu zagrożenia.

Statystyczna analiza zachowania: na przestrzeni dłuższego okresu czasu kolekcjonuje się dane charakteryzujące zachowanie się legalnego użytkownika, po czym analizuje się zachowanie bieżące użytkownika względem zachowania zdefiniowanego według danych zebranych wcześniej.

**7.Systemy macierzowe RAID.**

System macierzowy RAID jest zbiorem dwóch lub więcej urządzeń dyskowych łączonych ze sobą w jedną logiczną strukturę, zapewniającym osiągi niedostępne dla pojedynczego urządzenia.

Systemy RAID stosowane są w celu:

zwiększenia odporności na awarie dysków twardych, zwiększenia wydajności takiego systemu, zwiększenia powierzchni dyskowej, która może być traktowana jako jedna całość, łatwość rozbudowy systemu

W systemach RAID zdefiniowano poziomy, które określają minimalną liczbę dysków, sposób ich połączenia oraz dostępną przestrzeń. Najpopularniejsze systemy RAID obecnie to:

RAID 0 (stripping) – polega na połączeniu dwóch lub więcej dysków, w taki sposób aby tworzyły one jedną przestrzeń logiczną

RAID 1 (mirroring) – polega na replikacji dwóch lub więcej dysków, w taki sposób, aby dane były dublowane na każdym z tych dysków

RAID 5 – na tym poziomie realizowany jest stripping bloków podobnie do poziomu RAID 0. Bity parzystości rozpraszane są pomiędzy dyski znajdujące się w macierzy. W razie awarii jednego z dysków odzyskanie danych następuje przy wykorzystaniu kodów korekcyjnych znajdujących się na pozostałych dyskach

**8.Ataki związane z wstrzykiwaniem kodu SQL/NoSQL w bazach danych.**

Ataki typu SQL Injection wykorzystują podatność aplikacji w przypadku, kiedy dane wprowadzane przez użytkownika nie są sprawdzane ani filtrowane przed wrzuceniem ich do zapytania SQL.

Sprytny napastnik może wykorzystać możliwość zagnieżdżenia SQL do stworzenia nowego zapytania i potencjalnego zmodyfikowania lub odczytania danych z BD.

Istotą tego typu ataku jest umiejętne skonstruowanie zapytania SQL.

Zapytaniem, które może bezpośrednio zmodyfikować dane w BD to zapytanie składające się z wielu zapytań: SELECT \* FROM users WHERE name = 'a';DROP TABLE users; SELECT \* FROM userinfo WHERE 't' = 't';

**9.Czym jest kryptoanaliza?**

Techniki wykorzystywane do uzyskania tekstu jawnego bez jakiejkolwiek wiedzy dotyczącej szczegółów szyfrowania określamy mianem kryptoanalizy – znanej jako „łamanie kodu”.

Kryptoanaliza bazuje na znajomości natury algorytmu szyfrującego i ewentualnie na pewnych ogólnych cechach tekstu jawnego i jest ukierunkowana na poznanie klucza lub jedynie samego tekstu jawnego.

Kryptoanalityk może wykorzystać różne informacje do złamania klucza. Im posiada ich więcej, tym ma łatwiejszą drogę do poznania klucza szyfrującego.

Podejście praktyczne (realne) dla bezpieczeństwa algorytmu szyfrującego musi spełniać jedno z poniższych kryteriów:

• koszt złamania szyfru jest większy niż wartość zaszyfrowanej informacji,

• czas potrzebny na złamanie szyfru przekracza okres użyteczności zaszyfrowanej informacji.

**10.Przedstaw błędy w uwierzytelnianiu użytkownika i zarządzaniu jego sesją przez aplikację**

Błędy związane z sesją polegają na niezgodnym z przeznaczeniem wykorzystaniem danych uwierzytelniających oraz wykorzystaniem błędów związanych z implementacją sesji.

Do tych błędów należą:

• Brak haszowania lub szyfrowania danych użytkownika.

• Wykorzystywanie haseł słownikowych (łatwe do odgadnięcia) lub nadpisane przez słabo zabezpieczone funkcje aplikacji

• Identyfikatory sesji ujawniane są w adresie URL.

• Identyfikatory sesji podatne są na atak typu Session Hijacking.

• Identyfikatory sesji nie wygasają.

• Brak unieważniania sesji lub tokenów użytkowników przy wylogowaniu.

• Identyfikatory sesji nie są zmieniane (rotate) po udanym zalogowaniu.

• Dane uwierzytelniające są przesyłanie nieszyfrowanymi połączeniami komunikacyjnymi.

• Wiązanie sesji z innym użytkownikiem w systemie