|  |
| --- |
| Politechnika Wrocławska, Informatyka Stosowana |
| Wykorzystanie podatności |
| Cyberbezpieczeństwo, Laboratorium nr.12 - raport |

|  |
| --- |
| Autor: Aleksander Stepaniuk  Nr. Indeksu: 272644 |

**4. Pytania**

**Pytanie 1;**

Reverse shell to technika ataku pozwalająca przejąć kontrolę nad zainfekowanym systemem. Polega na tym, że zainfekowany system nawiązuje połączenie z serwerem atakującego otwierając zdalny dostęp do swojej powłoki shell. W przeciwieństwie do standardowego shella, gdzie atakujący łączy się z ofiarą, tutaj to ofiara inicjuje połączenie wychodzące co pomaga ominąć zapory i inne mechanizmy zabezpieczające. Wykorzystuje się to do przesłania szkodliwego oprogramowania na maszynę ofiary.

**Pytanie 2;**

Nadanie odpowiednich uprawnień użytkownikom jest kluczowe dla bezpieczeństwa, ponieważ minimalizujemy wtedy szkody jakie zostaną wyrządzone jeśli usługa zostanie przejęta – potencjalny napastnik będzie miał dostęp tylko do zasobów, do których ma uprawnienia dane konto (konta z niskimi uprawnieniami nie mają dostępu do wrażliwych plików i konfiguracji systemu). Dodatkowo kiedy każda usługa działa w swoim środowisku z minimalnymi uprawnieniami, zapobiegamy wtedy eskalacji uprawnień i dalszej propagacji ataku.

Warto trzymać się zasady najmniejszych uprawnień (PoLP) - każdy użytkownik lub proces ma dostęp tylko do tych zasobów, które są niezbędne do ich działania. Przykładowo jeśli serwer WWW działa na koncie bez uprawnień administracyjnych, atakujący, który wykorzysta lukę w oprogramowaniu, nie będzie mógł przejąć kontroli nad całym systemem.

**5. Zadania**

**Zadanie 0;**

Adresy IP maszyn:

**Metasploitable**: 172.16.96.5

**Kali linux**: 172.16.96.8

**Adres sieci:** 172.16.96.0/24

**Zadanie 1;**

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, menu, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka, menu

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

**Zadanie 2;**

Usługa vsftd w wersji 2.3.4. posiada podatność CVE-2011-2523, gdzie po zalogowaniu się do serwera dowolnym loginem zakończonym na „:)” i dowolnym hasłem otwiera się port 6200.

**Zadania 3-7;**

Pierwsze skanowanie portu 6200 - closed

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, Czcionka, zrzut ekranu, design

Opis wygenerowany automatycznie

Ponowne skanowanie portu 6200 – port zmienił stan z closed na open

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Teraz po wpisaniu komendy whoami; widzimy że wyświetla się root.

Obraz zawierający tekst, zrzut ekranu, Czcionka, design

Opis wygenerowany automatycznie

**Zadania 8-21;**

Usługa distccd to serwer pozwalający na kompilowanie kodu napisanego w C lub C++ na kilku komputerach w sieci. Domyślnie ta usługa jest uruchomiona na porcie 3632.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, menu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka, oprogramowanie

Opis wygenerowany automatycznie



Wykorzystamy podatność o identyfikatorze CVE-2009-1185, która pozwala na uzyskanie prawa administratora (roota) poprzez zainfekowany plik, który uruchomi konkretny port na maszynie.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Uruchamiamy usługę Apache2 w Kali oraz kopiujemy ówcześnie pobrany zainfekowany plik do /var/www/html/

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, Czcionka, zrzut ekranu, design

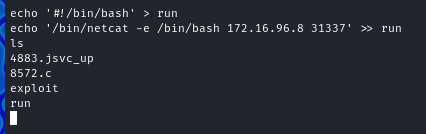
Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Widzimy że Pid tego procesu wynosi 2618.

Tworzymy plik run:



Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie

I uruchamiamy exploit:



Atak zakończył się pomyślnie – mamy uprawnienia roota na maszynie ofiary.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie