# Podatność CVE-2019-0708

CVE-2019-0708, znana również jako "BlueKeep", to krytyczna luka w zabezpieczeniach zdalnego pulpitu (RDP) ujawniona w maju 2019 roku. Umożliwia ona zdalne wykonanie kodu na podatnych systemach, co oznacza, że ​​atakujący może przejąć pełną kontrolę nad zainfekowanym komputerem.

Szczegóły techniczne:

* Wektor ataku: Zdalne wykonanie kodu
* Dotknięte oprogramowanie: systemy operacyjne
  + Windows XP
  + Windows Server 2003
  + Windows 7
  + Windows Server 2008
  + Windows Server 2012
  + Windows 8.1 Windows Server 2012 R2
  + Windows 10 (wersje przed 17 maja 2019 r.)
* Opis: Luka wynika z błędu w sposobie, w jaki RDP przetwarza pewne pakiety sieciowe. Osoby atakujące mogą wykorzystać tę lukę do uruchomienia dowolnego kodu na podatnym systemie bez uwierzytelniania.

Skutki:

* Zdalne przejęcie systemu: Osoby atakujące mogą przejąć pełną kontrolę nad podatnym systemem.
* Kradzież danych: Osoby atakujące mogą ukraść poufne dane, takie jak hasła i dane finansowe.
* Szkodliwe oprogramowanie: Osoby atakujące mogą zainstalować szkodliwe oprogramowanie na podatnym systemie.

Rozwiązanie:

* Instalacja patchy udostępnionych przez Microsoft

## Detekcja podatności

Do sprawdzenia czy dany system jest podatny na ten exploit użyjemy narzędzia metasploit. W konsoli metasploit wyszukujemy exploitów dotyczących bluekeep.

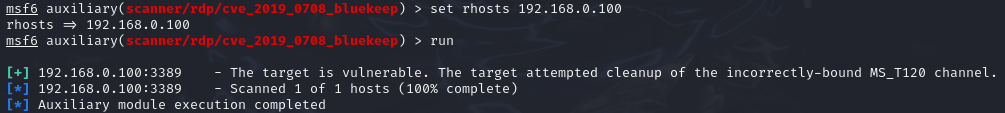
Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Następnie wybieramy moduł typu auxiliary, moduły tego typu dotyczą sprawdzania podatności.



Po wybraniu modułu możemy ustawić adres ip urządzenia które będziemy sprawdzać, a następnie poprzez użycie polecenia run przeprowadzamy test podatności.



Jak widać na screenie powyżej Sprawdzany przez nas system jest podatny na exploit bluekeep.

## Symulacja ataku

Do przeprowadzenia ataku użyjemy narzędzia Metasploit. W konsoli wyszukujemy frazy bluekeep.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Tym razem wybieramy moduł z numerem 1



Możemy zauważyć, że exploit jest ustawione standardowo do przeprowadzenia ataku który ma na celu ustanowienie połączenia reverse TCP. Listę wszystkich możliwych payloadów możemy sprawdzić przy pomocy polecenia show payloads, w tym przypadku otrzymujemy listę 73 możliwych payloadów do wyboru.

Następnym krokiem jest wybranie typu naszego celu przy pomocy polecenia show targets, z powodu że działamy na maszynach wirtualnych przy pomocy VirtualBox wybieramy opcję numer 2 przy pomocy polecenia set target 2

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Ustawiamy również adres IP komputera który będziemy atakować.



Po ustawieniu wszystkich wartości możemy przejść do wykonywania ataku.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

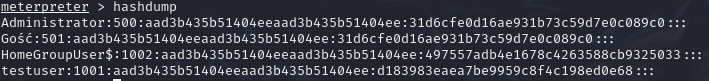
Z tego poziomu mamy już pełny dostęp do zaatakowanego systemu

Obraz zawierający tekst, zrzut ekranu, menu, Czcionka

Opis wygenerowany automatycznie

Przykładowe zastosowanie

Odczytanie haseł użytkowników, aby to wykonać możemy użyć polecenia hashdump które zwróci nam hash hasła wszystkich użytkowników w systemie



Aby odczytać hasła możemy użyć narzędzia kiwi które najpierw należy załadować

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Po załadowaniu kiwi możemy użyć polecenia creds\_all które zwróci nam hasła użytkowników którzy są aktualnie aktywni w systemie, czyli można się na nie zalogować.

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie