**Analiza Wybranych Podatności**

**CVE-2016-5195**

**Autor:** Szymon Litwicki

**Nr albumu:** 264036

**Nr zespołu:** 2

**CVE-2016-5195**

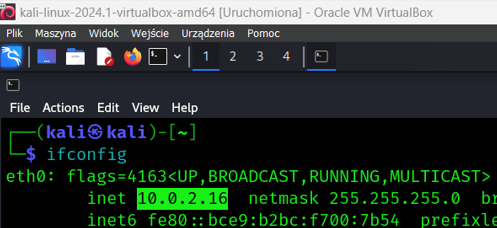
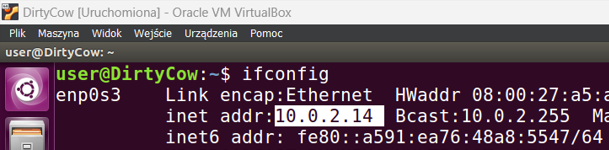
**Wstęp**

**CVE-2016-5195** to podatność znana również pod nazwą **"Dirty COW"**. Jest to podatność znaleziona w jądrze systemu **Linux** i została ona opublikowana w październiku **2016 roku**. Nazwa "Dirty COW" jest akronimem od **"Dirty Copy On Write"**, odnoszącym się do ataku wykorzystującego operację „kopiowania na zapis” (Copy-On-Write) w systemie plików, by uzyskać uprawnienia **roota**. Ta podatność wykorzystuje mechanizm kontroli dostępu do pamięci w systemie Linux, który umożliwiał złośliwemu użytkownikowi uzyskanie nielimitowanego dostępu do plików systemowych. Atak działał na zasadzie wywołanie błędnej operacji **odczytu/zapisu** na pliku pamięci mapowanej do użytkownika w jądrze Linux, a następnie **nadpisania** odpowiadającego mu pliku pamięci w jądrze. Dzięki temu atakujący może zmienić dowolny plik w pamięci jądra, nawet jeśli był on tylko do odczytu. Przez to możliwe stało się wykonanie kodu z uprawnieniami roota na zainfekowanym systemie. CVE-2016-5195 była obecna w jądrach Linux od wersji **2.6.22** (wydanej w lipcu **2007** roku) do wersji **4.8.3** (wydanej w październiku **2016** roku), kiedy to została ujawniona publicznie.

**Przygotowanie do analizy**

Sprawdzenie działania tej podatności nastąpiło na dwóch maszynach wirtualnych:

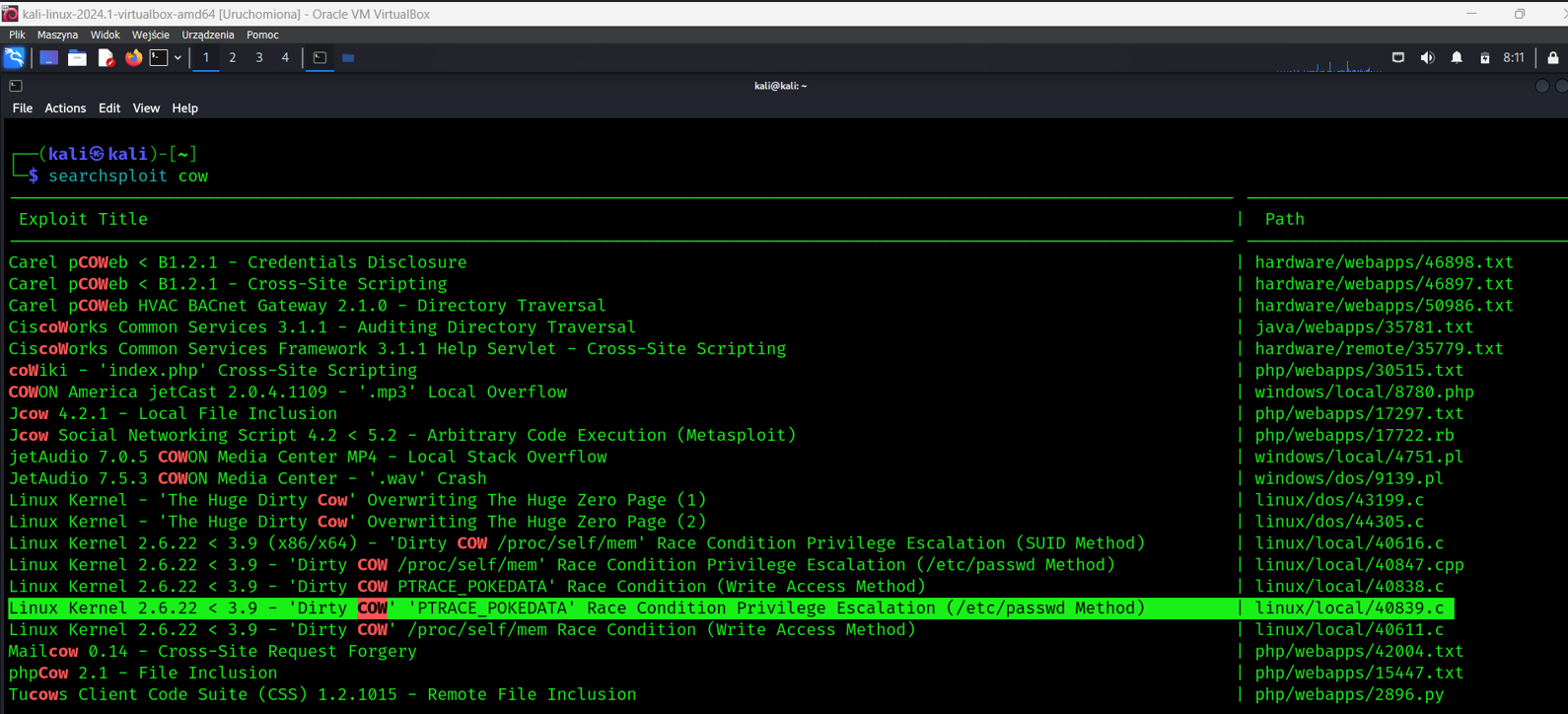
* Kali Linux 2024.1 (maszyna atakująca)
* Ubuntu 16.04.7 LTS „Dirty Cow” (ofiara ataku)

Po podstawowym skonfigurowaniu tych maszyn, należało zapewnić łączność między nimi, czyli umieścić je w jednej sieci NAT. Adresy IP maszyn potwier dzają poniższe zrzuty ekranu.

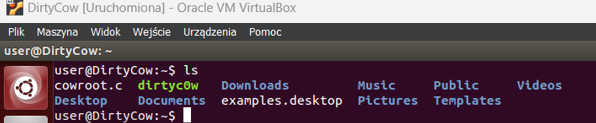
Rysunek 2 Adres IP maszyny ofiary Ubuntu

Rysunek 1 Adres IP maszyny atakującego Kali Linux

Kolejnym etapem procesu, było umieszczenie złośliwego skryptu na maszynie ofiary, po jego wcześniejszym znalezieniu, a jest on dostępny do wykorzystania w standardowej instalacji Kali Linux. Warto tutaj zaznaczyć, że do wykonania tego exploitu potrzebny jest dostęp do danego systemu, w tym przypadku na konto User na podatnej maszynie. User nie ma uprawnień roota, a ich zdobycie jest celem tego exploitu – dostęp do systemu ofiary jest innym problemem, który tutaj w ramach prezentacji samej podatności CVE-2016-5195 został rozwiązany zwykłym połączeniem SSH, czyli w założeniu, że atakujący zna hasło użytkownika user.



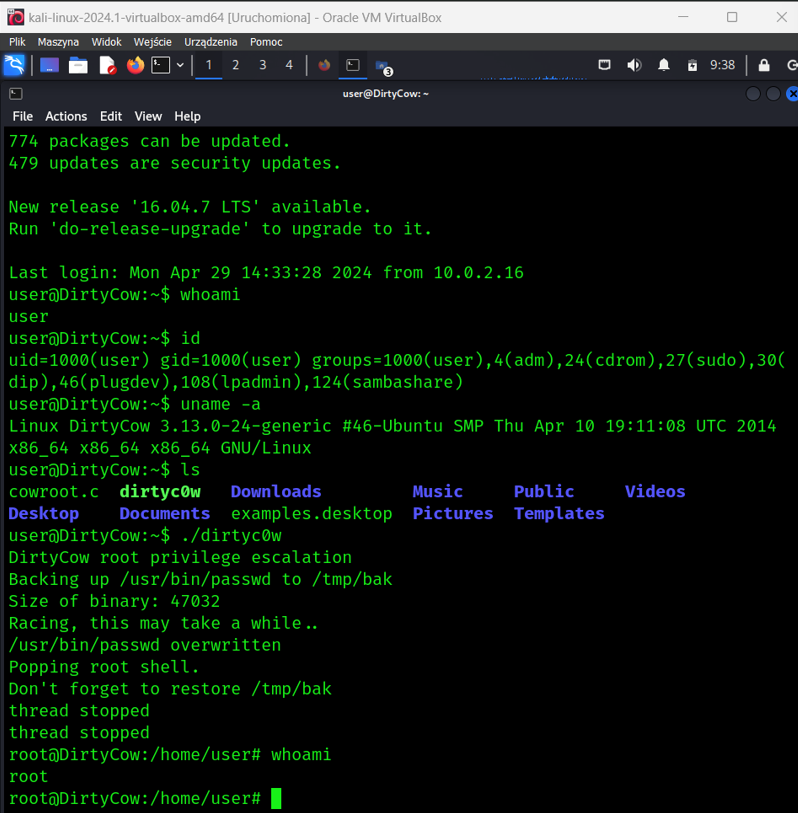
Rysunek 3 Expolity powiązane z Dirty COW znalezione w searchsploit



Rysunek 4 Potwierdzenie umieszczenia złośliwego skryptu w systemie ofiary

**Wykorzystanie podatności**

Po umieszczeniu w systemie ofiary złośliwego skryptu wydano komendę **whoami**, która jako wynik działania zwróciła wartość user. Po wykonaniu złośliwego skryptu ta sama komenda zwróciła wartość root, co potwierdza sukces w wykonaniu ataku. Zdobyto uprawnienia użytkownika root nie znając jego hasła, a będąc jedynie zalogowanym na konto zwykłego użytkownika (poprzez ssh z maszyny atakującego).



Rysunek 5 Wykonanie złośliwego skryptu i zdobycie uprawnień roota

**Podsumowanie**

Analizowana podatność CVE-2016-5195 okazała się być krytyczna. Była ona spowodowana przez błędy w oprogramowaniu i w celu ochrony przed jej wykorzystaniem należy dbać o aktualność używanych rozwiązań i instalowanie poprawek bezpieczeństwa.