Politechnika Wrocławska

SPRAWOZDANIE Z ZAJĘĆ LABORATORYJNYCH
CYBERBEZPIECZEŃSTWO

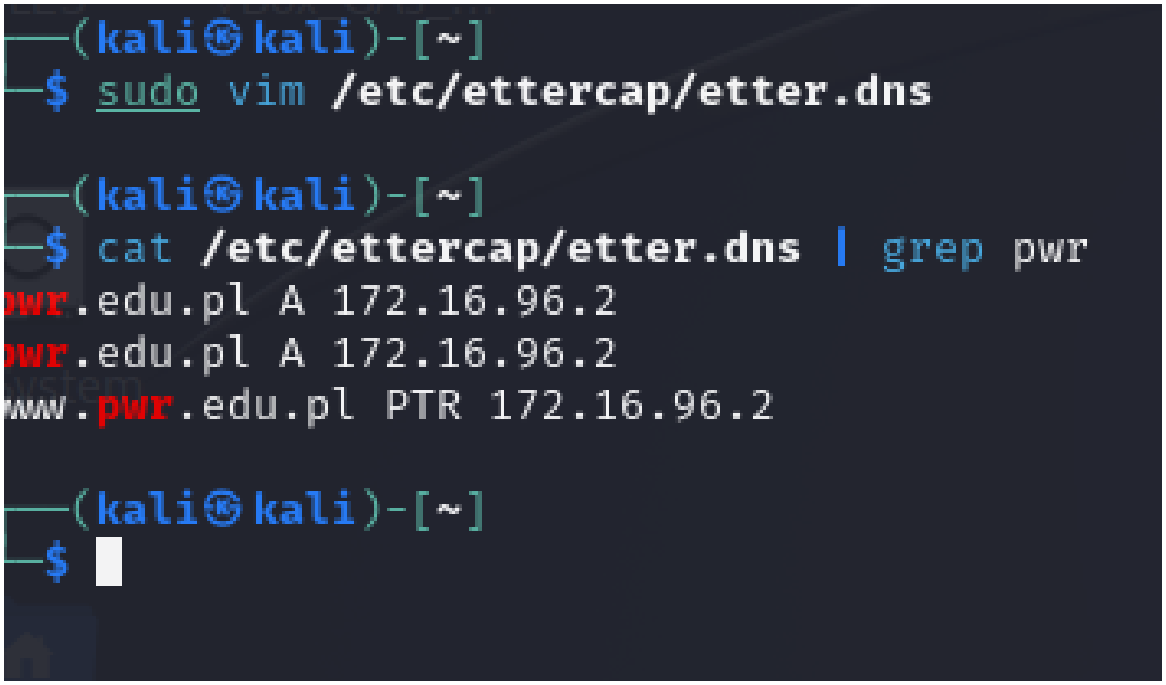
Lab 08
Ataki na komunikację

Tomasz Mroczko, 266604

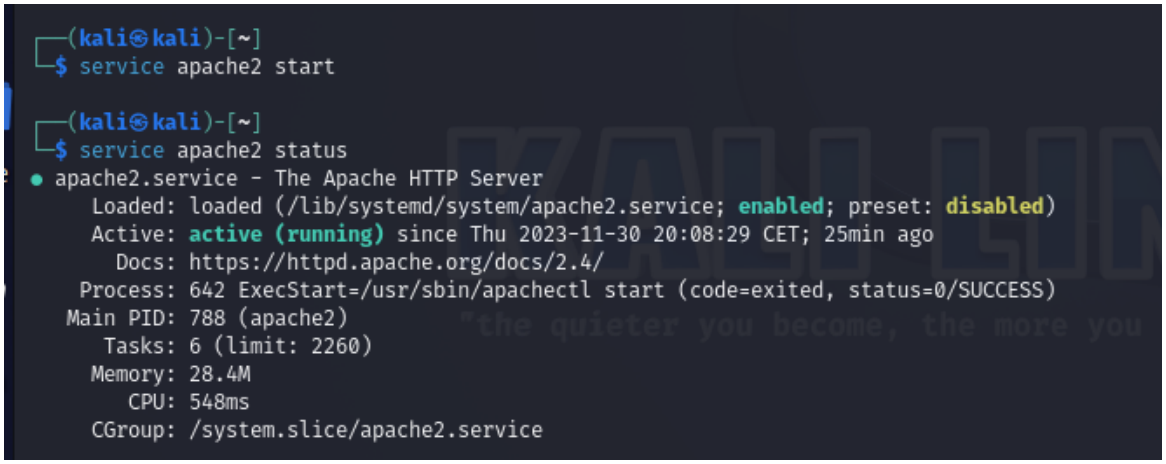
December 1, 2023

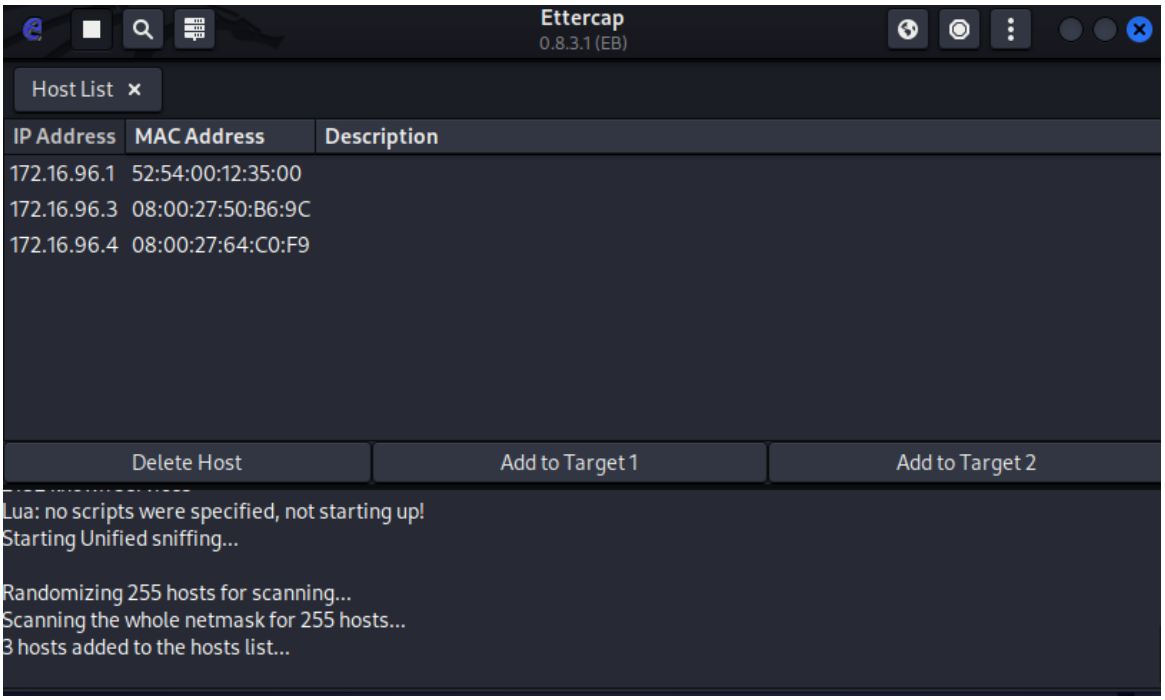
1 Kroki ataku

Zlokalizowanie i zmodyfikowanie pliku etter.dns na VM Kali

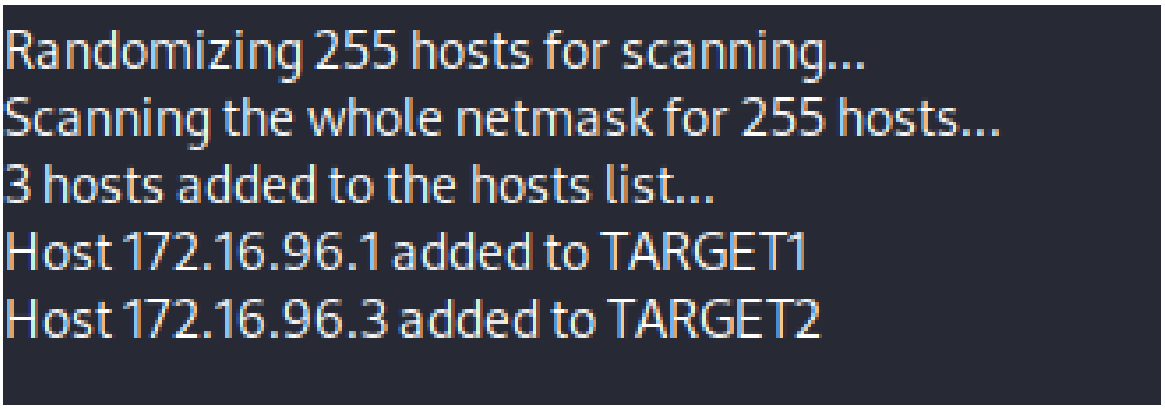


Start apache2 oraz ettercap

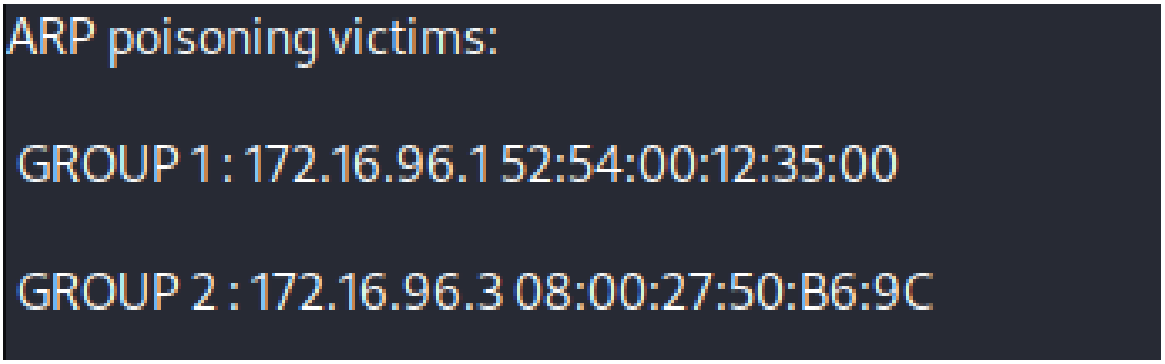




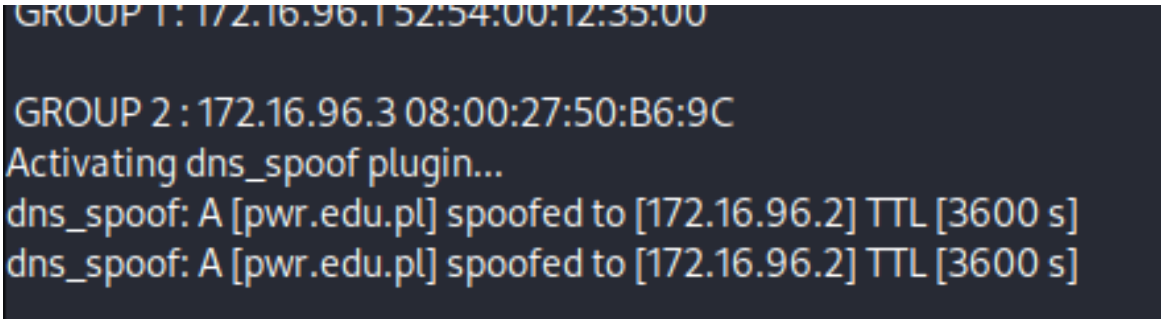
Dodanie bramy domyślnej oraz VM Ubuntu jako cele ataku



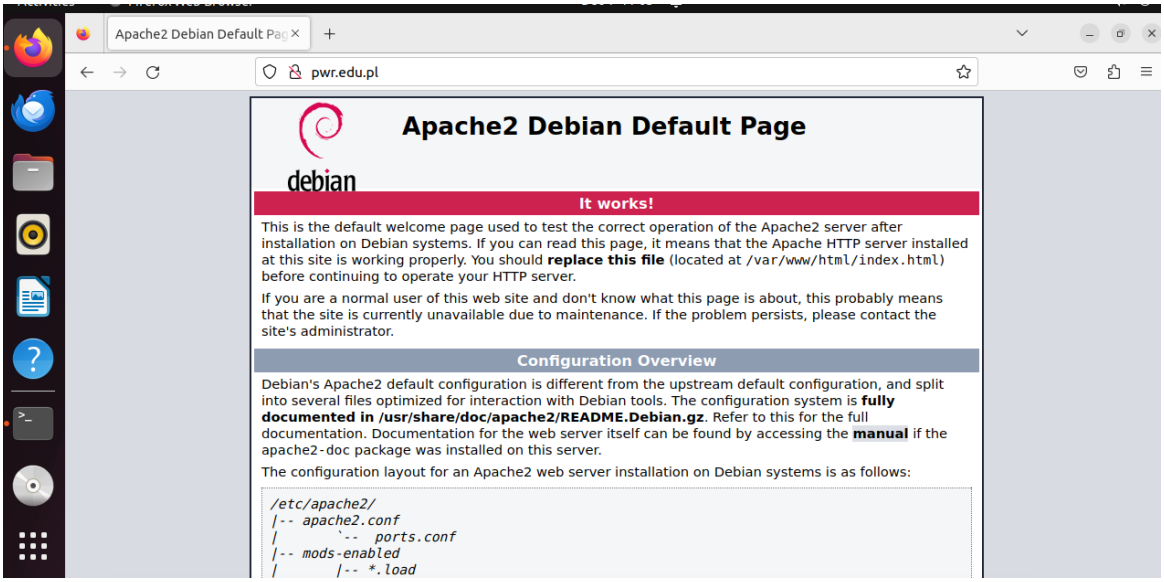
Rozpoczęcie ARP Poisoning



Próba otwarcia "pwr.edu.pl" z widoku VM Kali

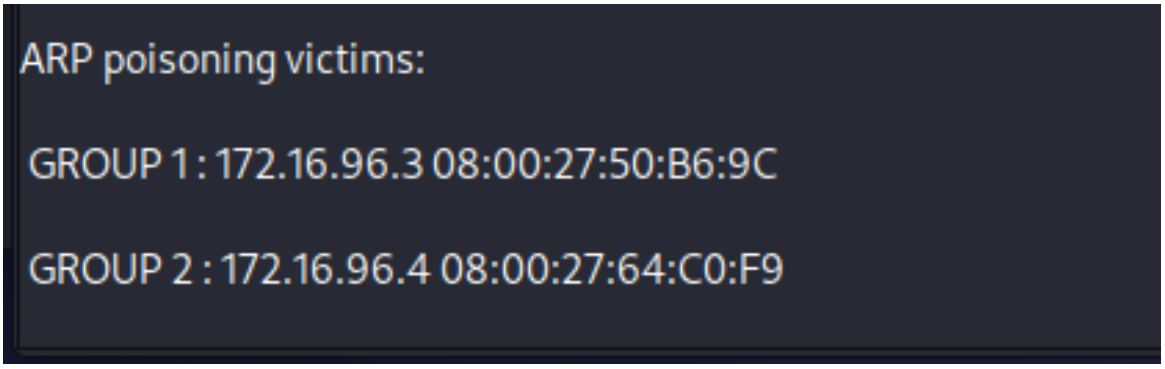


Próba otwarcia "pwr.edu.pl" z widoku klienta (VM Ubuntu)

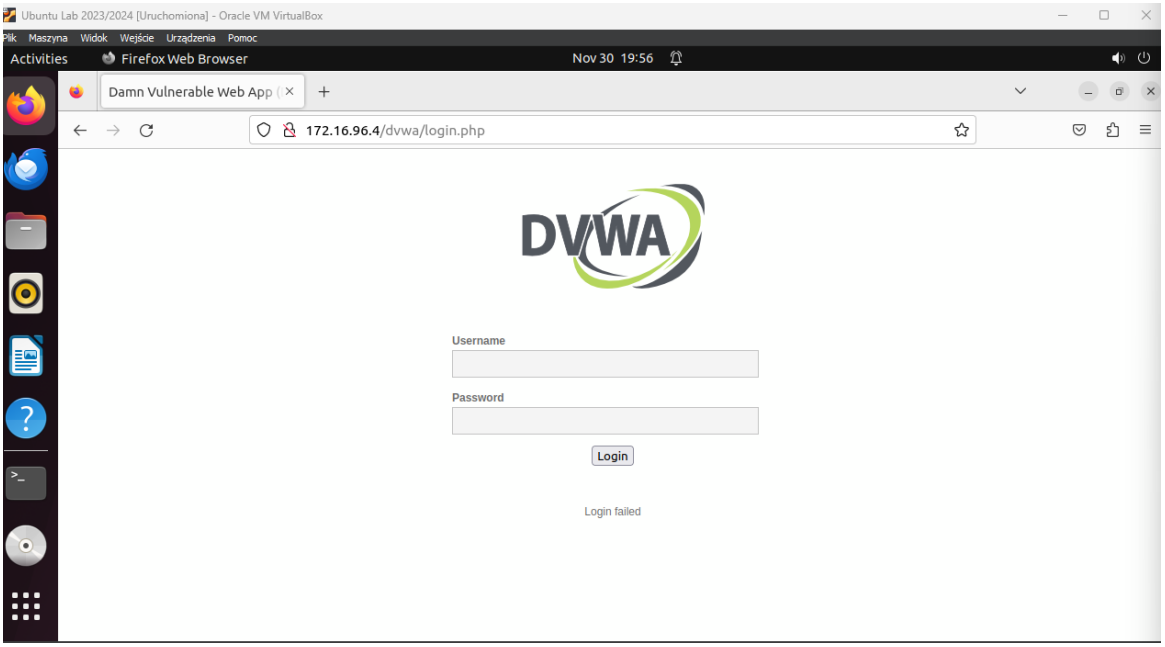


W

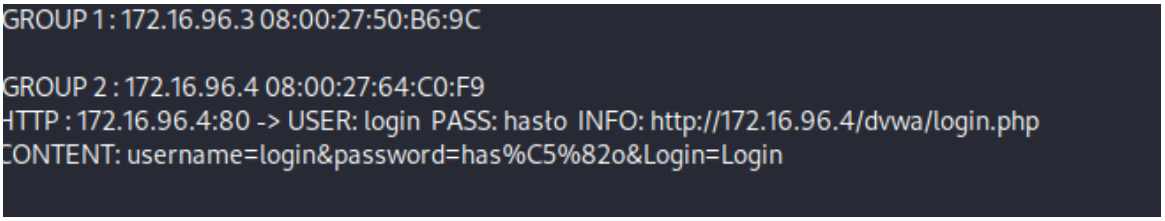
Dodanie VM Ubuntu i Metasploitable jako cele ataku i rozpoczęcie



Strona po wejścu na adres ip metasploitable/dvwa



Przechwycenie loginu i hasła próby logowania z Ubuntu na dvwa



2 Pytania

Pytanie I

Jaka jest różnica między aktywnymi i pasywnymi atakami MitM?

- Ataki pasywne:
  Podczas ataków pasywnych atakujący głównie podsłuchuje i monitoruje przesył danych. Celem takich ataków jest zazwyczaj odkrycie treści komunikatu, a atakujący nie ingeruje w przechwycone dane. Najczęściej mają one na celu przechwycenie poufnych informacji, takich jak hasła, numery kart lub poufne dane biznesowe. Są trudniejsze do wykrycia niż ataki aktywne ze względu na brak ingerencji w przesyłane dane.
- Ataki aktywne:
  Ataki aktywne obejmują bezpośrednią ingerencje w komunikację pomiędzy stronami. Dane zostają zmodyfikowane lub zfałszowane. Przykładem takiego ataku jest używany w ćwiczeniu *DNS spoofing*, podczas którego atakujący fałszuje odpowiedzi DNS w celu przekierowania celu ataku na inne strony.

Pytanie II

Jak zabezpieczyć swoją sieć przed atakami zatruwania ARP?

Można statycznie ustalić wszystkie wpisy ARP dla ważnych urządzeń sieci. To bardzo efektywne, ponieważ atakujący nie będzie w stanie nadpisać takich adresów. Jednak w przypadku zmian w obrębie sieci uciążliwe staje się utrzymanie tablic ARP. Wiele switchy posiada funkcje mające na celu zwiększenie bezpieczeństwa przeciwko ARP poisoning. Jedną z nich jest DAI(Dynamic ARP Inpection).

Szyfrowanie nie zabezpiecza przed ARP, może jednak złagodzić szkody. Przechwytujący dane może przechwycić ruch, ale pozostanie mu bardzo trudne zadanie rozszyfrowania informacji.

Kontrolowanie fizycznego dostępu do sieci może utrudnić możliwość ataku. Komunikaty ARP nie wychodzą poza lokalną sięć, więc atakujący musi mieć fizyczny dostęp do sieci lub jednego z urządzeń w niej.

Pytanie III

> *Dlaczego ważne jest, aby używać rozszerzeń DNSSEC w celu zapobiegania atakom polegającym na fałszowaniu DNS*

DNS w podstawowej wersji nie zawiera mechanizmów bezpieczeństwa. Nie daje możliwości uwierzytelniania odpowiedzi, co zwiększa podatnosć na fałszowanie DNS. DNSSEC(Domain Name System Security Extensions) to rozbudowanie protokołu DNS, wzmacniające bezpieczeństwo. Opiera się na kryptografii klucza publiczngo, certyfikatach i podpisach cyfrowych. Daje to możliwość werfyfikacji pochodzenia odpowiedzi, co zapobiega fałszowaniu odpowiedzi.

Pytanie IV

> *Co to jest tryb monitorowania i jak można go używać do podsłuchiwania komunikacji sieciowej?*

Podczas trybu monitorowania karta sieciowa nasłuchuje całego ruchu sieciowego, który przez nią przechodzi, bez ingerencji w dane. Dzięki temu, korzystający z takiej karty, z pomocą odpowiedniego oprogramowania mieć wgląd w pakiety przechodzące przez daną sieć. Często używa się go do analizy diagnostyki sieci. Osoba korzystająca może jednak wykorzystać to do posłuchiwania komunikacji. Daje to wgląd w zawartość ramek oraz wiele informacji w danej sieci. Atakujący może podjąć próbę zdobycia pożądanych informacji, a jeśli sieć nie jest dobrze zabezpieczona - przechwycić je.