Skanowanie sieci

Skanowanie sieci jest ważnym aspektem bezpieczeństwa sieci. Pozwala to na gromadzenie i analizę rzeczywistej informacji o topologii sieci i aktywnych usługach w swoich sieciach. Teoretyczna wiedza o swojej sieci i informacja rzeczywista mogą się różnić z następnych powodów:

- Słaba praca działów IT.
- Słaba współpraca działów IT i działu Bezpieczeństwa informacji (BI) firmy.
- Uruchomienie innymi jednostkami firmy sprzętu i oprogramowania bez uwzględnienia i informowania działów IT i BI.
- Wynik udanego ataku na infrastrukturę firmy. (Obecność nielegalnych hostów i usług)

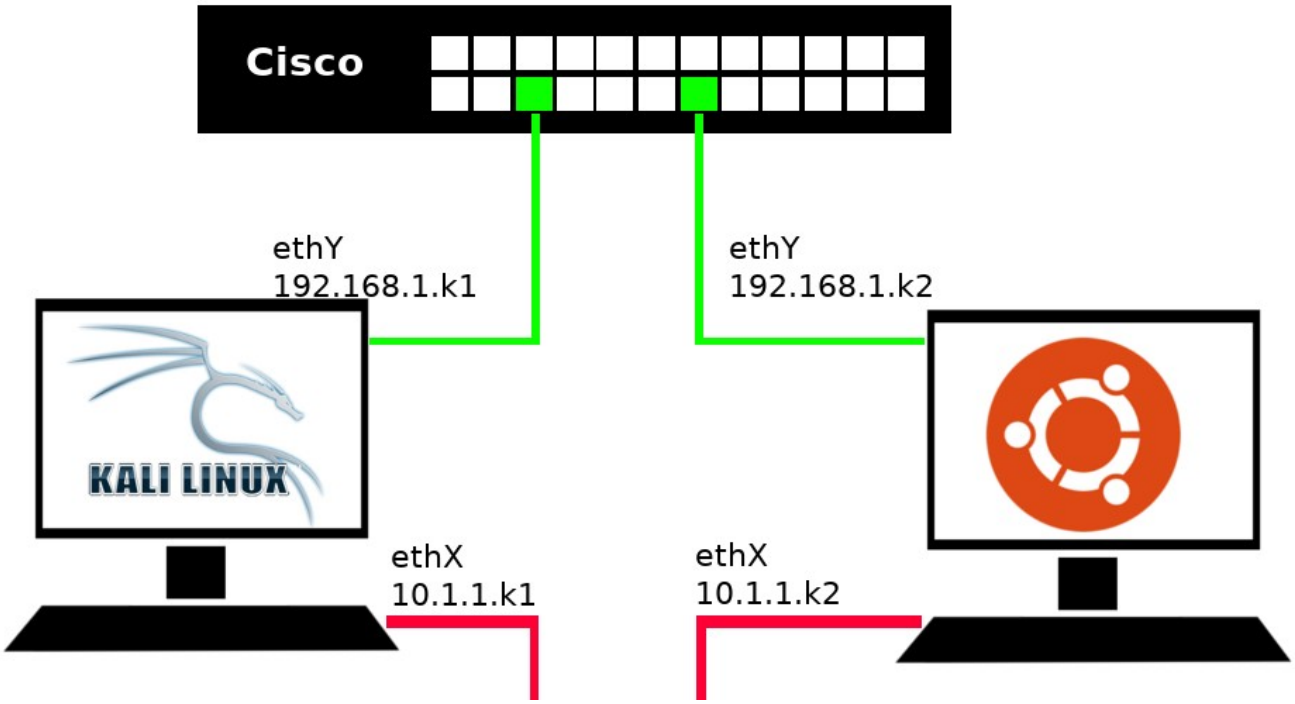
Skanowanie może być aktywnym (opiera się na schemat „moje pytanie”→ „odpowiedź na moje pytanie”→ „analiza odpowiedzi”) i pasywnym (opiera się na schemat „obce pytanie”→ „odpowiedź na obce pytanie”→ „analiza odpowiedzi”), które jest gromadzeniem ruchu sieciowego i jego analizą. Zaletą pasywnego skanowania jest niewidoczność dla innych węzłów w sieci i unikanie obciążenia sieci ruchem skanerów.

Celem pracy jest - nauczyć się:

- Korzystać z niespecjalizowanego dla tych celów oprogramowania (telnet, netcat) dla aktywnego skanowania sieci .
- Korzystać z skanerów sieci i skanerów podatności (nmap, ZenMap, Sparta) dla aktywnego skanowania sieci .
- Pasywnemu skanowaniu sieci (Wireshark, Xplico).

0. Stanowisko laboratoryjne

Pierwszym krokiem będzie budowanie stanowiska laboratoryjnego (Rys.1).



Rys.1.

Stanowisko składa się z:

- Komputera k1 pod zarządzaniem Kali Live OS.
- Komputera k2 pod zarządzaniem Ubuntu Live OS
- Przełącznika sieciowego Cisco

Komputer k1 i k2 mają być połączone do sieci dwoma interfejsami: ethX oraz ethY.

Interfejs ethX już jest połączony do sieci laboratorium 204 i ma adres 10.1.1.k/16, brama domyślna poprzez 10.1.0.1.

Połącz inny dostępny interfejs sieciowy (nazwany na rysunku „ethY") do przełącznika Cisco. Ustaw adres IP: 192.168.1.k/24

Sprawdź łączność do komputera sąsiada za pomocą polecenia PING na adres 192.168.1.k.

Zainstaluj na k1 pakiet ***xplico***.

Zainstaluj na k2 pakiety:

- ***apache2***
- ***ssh***
- ***samba***
- ***vsftpd***
- ***freeradius***

D0
Zademonstruj łączność z sąsiadem poprzez przełącznik Cisco.

1. Wykorzystanie do skanowania sieci ogólnodostępnych narzędzi.

Old School

Warto wiedzieć, że dla skanowania sieci mogą być stosowane nie tylko specjalizowane oprogramowania, ale i różne narzędzia sieciowe. Można korzystać z nich jeżeli w aktualnej chwili nie mamy dostępu do skanerów lub nie mamy możliwości instalacji skanerów.

Takie metody często są wykorzystywane hakerami po uzyskaniu dostępu do systemu, w którym administrator ograniczył dostęp użytkowników lokalnych do sieciowych skanerów.

Wykorzystanie **telnet** dla skanowania otwartych portów.

```
telnet  $IP_adres  $numer_portu
```

Za pomocą polecenia **telnet** połącz komputer k1 z portem 22 na adresie 192.168.1.k2.
Za pomocą polecenia **telnet** połącz komputer k1 z portem 20 na adresie 192.168.1.k2.
Jak reaguje telnet na otwarty port?

Wykorzystanie **netcat** dla skanowania otwartych portów.

```
nc  <kluczy>  $IP_adres  $numer_portu
```

Za pomocą polecenia **nc** połącz komputer k1 z portem 1 na adresie 192.168.1.k2. (klucz **-vn**)
Za pomocą polecenia **nc** połącz komputer k1 z portem 20 na adresie 192.168.1.k2. (klucz **-vn**)
Za pomocą polecenia **nc** połącz komputer k1 z portem 22 na adresie 192.168.1.k2. (klucz **-vn**)

Jak reaguje netcat na otwarty port?

Skanowanie wielu portów oprogramowaniem **netcat**:

```
nc  -vnz  $IP_adres  $od_numeru_portu-$do_numeru_portu
```

Za pomocą kluczy **-vnz** (skanowanie bez nawiązywania połączenia) zeskanuj porty od 1 do 1024 na adresie 192.168.1.k2.

Zahamuj działanie serwera Apache2 oraz SSH na k2.

```
service $nazwa_usługi stop
```

Za pomocą kluczy **-vnz** (skanowanie bez nawiązywania połączenia) ponownie zeskanuj porty od 1 do 1024 na adresie 192.168.1.k2. Jak zmieniła się sytuacja?

Uruchom z powrotem serwery Apache2 oraz SSH na k2.

```
service $nazwa_usługi start
```

Jest możliwość wykorzystania tych narzędzi w nietrywialny sposób dla skanowania i wykrycia hostów w sieci (na przykład jeżeli administrator ograniczył dostęp do programu PING).

Uruchom poniżej podany kod w terminalu k1:

```
i=1; while((i<=20)); do nc -vn -w1 192.168.1.$i 1; ((i++)); done
```

Ten kod (kod bash + netcat) faktycznie zeskanuje adresy od 192.168.1.1 do 192.168.1.20 na obecność hostów. W jaki sposób możemy wykryć w odpowiedzi komputera ip-adresy obecnych w sieci hostów?

D1
Zademonstruj na k1 stosowanie netcat dla wykrycia hostów w sieci 192.168.1.1-192.168.1.32. Który ip-adres jest obecny?
Zademonstruj na k1 wykorzystanie netcat dla skanowania portów k2 od 1 do 1024.

2. Wykorzystanie Nmap do skanowania sieci.

```
nmap <kluczy> $ip_adres
```

Uruchom na k2 w terminalu kod:

```
nc -l 8888 &
```

Skorzystaj na k1 Nmap dla skanowania k2.
Jaka jest różnica w porównaniu do wyników polecenia "nc -vnz 192.168.1.$k2 1-1024" ?
W jaki sposób możemy uzyskać taki sam wynik za pomocą "nc -vnz"?

D2
Zademonstruj wykrycie otwartego portu 8888 za pomocą skanowania poleceniem "nc -vnz..."

Wyświetlenie szczegółowej informacji o skanowaniu: klucz **-v**.
Wyświetlić powód na podstawie którego Nmap podejmuje decyzje o stan portu: klucz **--reason**.

Skanowanie wybranych pojedynczych portów:

```
nmap   -p  $numer_portu   $ip_adres
```

Skanowanie wielu wybranych portów:

```
nmap   -p  $numer_portu,$numer_portu,$numer_portu,$numer_portu   $ip_adres
nmap   -p  $od_numeru_portu-$do_numeru_portu   $ip_adres
```

Zeskanuj port 80 na k2.
Zeskanuj porty 21, 22, 53, 80, 443 na k2.
Zeskanuj porty od 1 do 53 na k2.

Wykryć protokoły które obsługuje host: (uwaga metoda jest długotrwała ~4-8 minut)

```
nmap   -sO  $ip_adres
```

Wykryć wersję OS na hostie:

```
nmap   -O  $ip_adres
```

Czasem informacja nie jest szczegółowa, co z kolei nie pozwala wykryć dystrybucję OS.
Można wykryć szczegóły w wersjach serwisów.

Wykryć wersji uruchomionych serwisów:

```
nmap   -sV  $ip_adres
```

D3
Jednym poleceniem Nmap uzyskuj informację która pozwala wyjaśnić:

- **które porty są otwarte na k2,**
- **na podstawie czego Nmap podejmuję decyzje o stan portu 53 na k2,**
- **który system operacyjny jest uruchomiony na k2,**
- **która to jest dystrybucja?**

3. Skanowanie portów UDP

Bardzo często porty UDP są ignorowane pod czas skanowania sieci z powodu wysokiej czasochłonności skanowania. Nie jest to dobrą praktyką. W taki sposób można pozostawić uruchomionymi podatne usługi, które mogą zostać atakowane przez hakera.

Dla skanowania portów UDP Nmap ma być uruchomiony z kluczem **-sU**.

Zeskanuj porty UDP od 1800 do 1820 na k2.
Które porty są otwarte?

D4
Zademonstruj na k1 wykrycie Nmapem portów działającego na k2 serwera freeradius.

Skanowanie wielu adresów.

```
nmap   $ip_adres   $ip_adres   $ip_adres   $ip_adres
nmap   192.168.10.1,2,3,4,5
```

Skanowanie obszaru ip-adresów/sieci.

```
nmap   $od_ip_adresu-$do_ip_adresu
nmap   $ip_adresy_sieci/$prefix_sieci
nmap   192.168.10.*
```

Wykrywać obecne hosty:

```
nmap -sn   $ip_adresy_sieci/$prefix_sieci
```

Nie skanować adresy:

```
nmap   $ip_adresy_sieci/$prefix_sieci   --exclude   $ip_adres_który_mamy_unikać
```

4. ZenMap

ZenMap jest GUI dla programu Nmap. Oczywiście, że nie jest on na tyle elastyczny i składanie niestandardowych poleceń często prowadzi do błędów. Jednak jest dobrym narzędziem dla wizualizacji i systematyzacji wykrytej informacji, co z kolei jest bardzo przydatnym dla skanowania dużej i skomplikowanej infrastruktury.

Uruchom na k1 ZenMap.

Ustaw jako target sieć ***192.168.1.0/24***, profile: „***ping scan***”.
Uruchom skanowanie.

Ustaw jako target sieć ***10.1.1.0/24***, profile: „***ping scan***”.
Uruchom skanowanie.
Ustaw jako target ip-adres ***192.168.1.k2***, profile: „***Intense scan, all TCP ports***”.

Uruchom skanowanie.

Ustaw jako target „***myslitski.edu.pl***”, profile: „***Quick traceroute***”.
Uruchom skanowanie.

Zobacz w jaki sposób ZenMap prezentuje wyniki skanowania.
Informacja o hostach.
Informacja o usługach.
Topologia sieci.

D5
Zademonstruj listę wykrytych hostów na których zostały wykryte usługi ssh.
Zademonstruj listę wszystkich wykrytych usług.
Zademonstruj topologię sieci.

5. Sparta

Uwaga! Sparta nie jest skanerem sieci. Sparta jest skanerem podatności. Faktycznie jest GUI, które zarządza innymi skanerami i automatyzuje wykrycie hostów, skanowanie portów, wykrycie wersji usługi, skanowanie podatności wykrytych usług, brute-force loginów i haseł, i t.d.

Uruchom Sparta na k1.

Dodaj sieć ***192.168.1.0/24*** dla skanowania.
Zobacz ile informacji Sparta wykrywa w tamtej sieci.

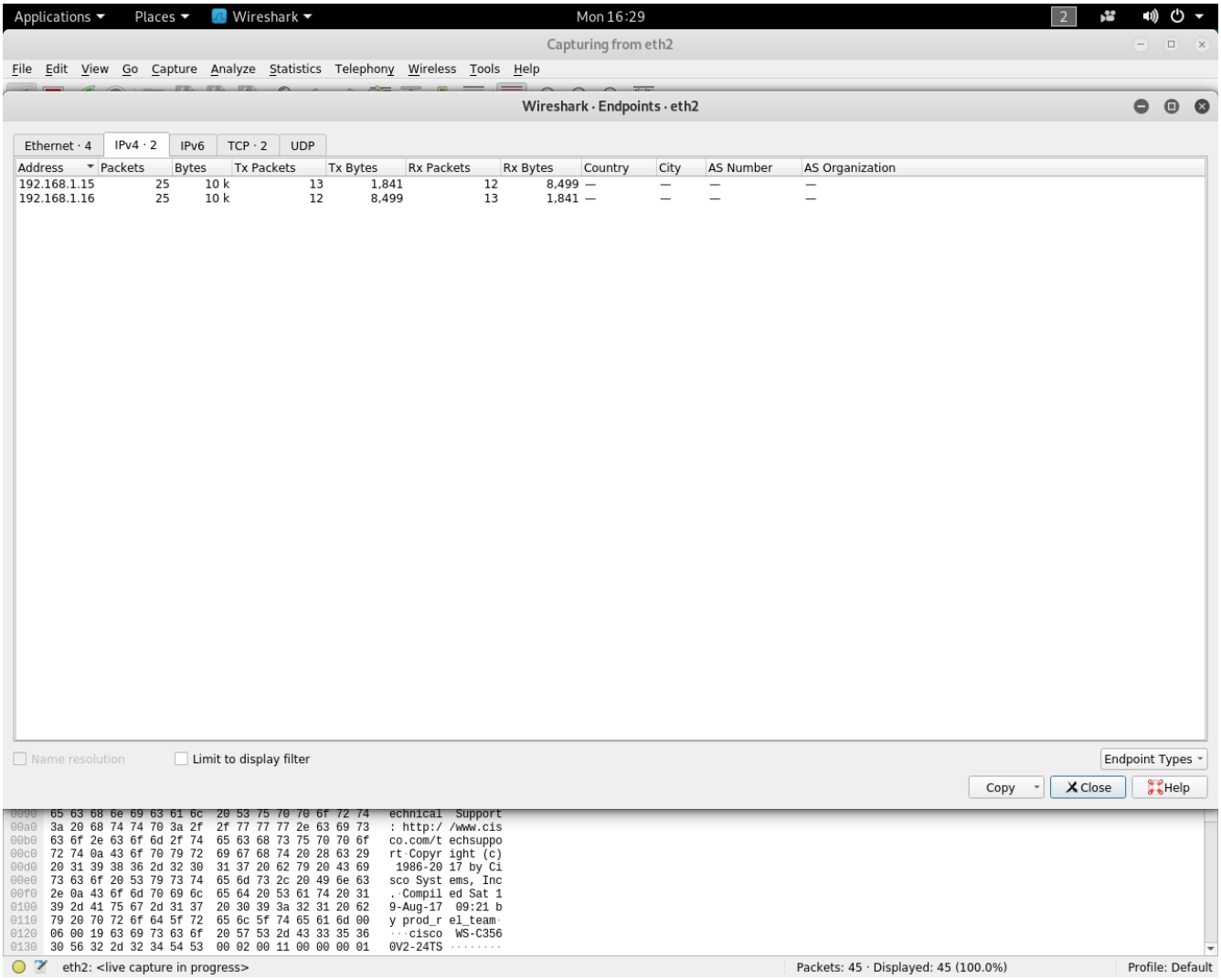
Uwaga: skaner nikto na porcie 80 będzie działał bardzo długo, z tego powodu po 5 minutach pracy przerwij jego działanie i zademonstruj wyniki.

D6
Zademonstruj wyniki działania Sparta

6. WireShark

Gromadzenie ruchu sieciowego pozwala na wykrycie hostów i usług działających w sieci bez aktywnego skanowania za pomocą analizy tego ruchu.

Uruchom na k2 WireShark na interfejsie sieciowym ethY.
Wykonaj polecenie ping z komputera k2 na k1 (interfejsy ethY).
Zobacz statystykę połączeń końcowych w WireShark (przykład na Rys. 2)



Rys. 2.

Uruchom WireShark na interfejsie ethX.

D7

Zaprezentuj wyniki działania WireShark po kilku minutach monitoringu sieci laboratorium 204 (które hosty są aktywnymi w sieci?).

7. Xplico

Uwaga! Xplico nie jest skanerem sieci i nie jest sniferem sieciowym. Xplico jest rozwiązaniem informatyki śledczej dla analizy gromadzonego ruchu sieciowego. Tak czy inaczej ma możliwość pracy nie tylko ze zawczasu gromadzonymi próbkami ruchu, ale również jest zdolny do analizy ruchu na bieżąco.

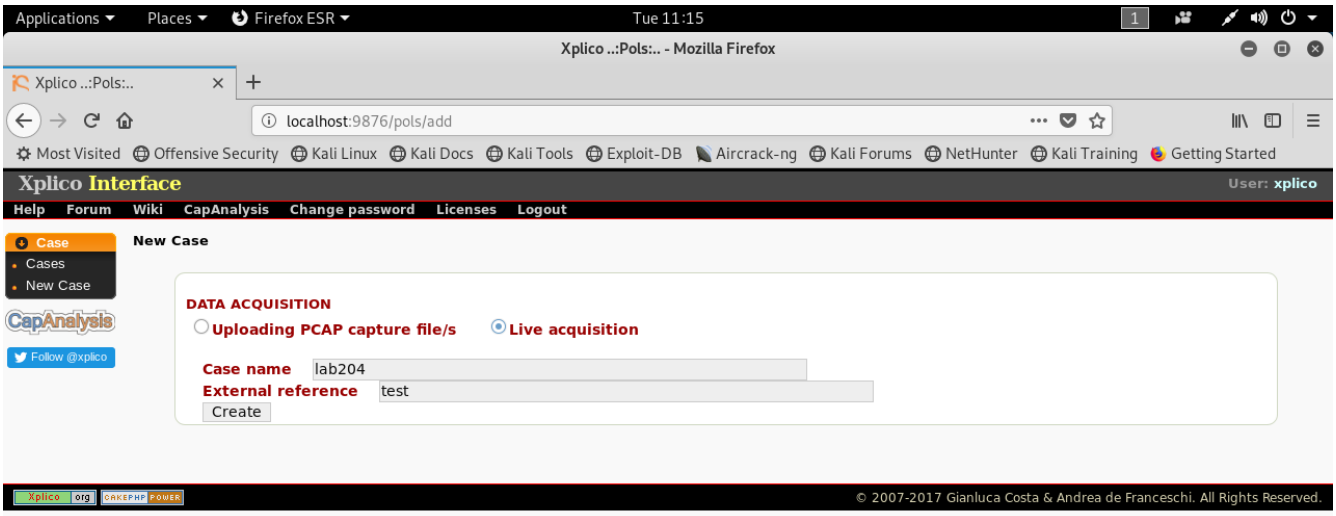
Uruchom na k2 serwer ***apache2***.

Uruchom na k2 serwer ***xplico***.

Uruchom przeglądarkę internetową i przejdź na URL: ***http://localhost:9876/***

Zaloguj się w Xplico:
login: „***xplico***”, hasło: „***xplico***”

Załóż nowe postępowanie „***New Case***”. Wybierz tryb „Na żywo” (***Live acquisition***). Rys. 3.



Rys. 3.

Załóż nową sesją „***New Session***”.
Uruchom sesję na interfejsie ethX.

D8
Zaprezentuj wyniki działania Xplico po kilku minutach monitoringu sieci laboratorium 204. (które hosty są aktywne w sieci?).

Koszty zadań:

Zadanie.	**Koszt**	**Całka**
D0	**0**	**0**
D1	**1**	**1**
D2	**0.5**	**1.5**
D3	**1**	**2.5**
D4	**0.5**	**3**
D5	**0.5**	**3.5**
D6	**0.5**	**4**
D7	**0.5**	**4.5**
D8	**0.5**	**5**