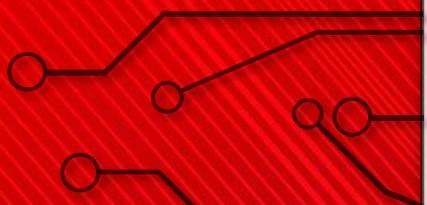


KURS PENTESTERA 22/23

MAN IN THE MIDDLE

ERNEST ŁATOSZYŃSKI



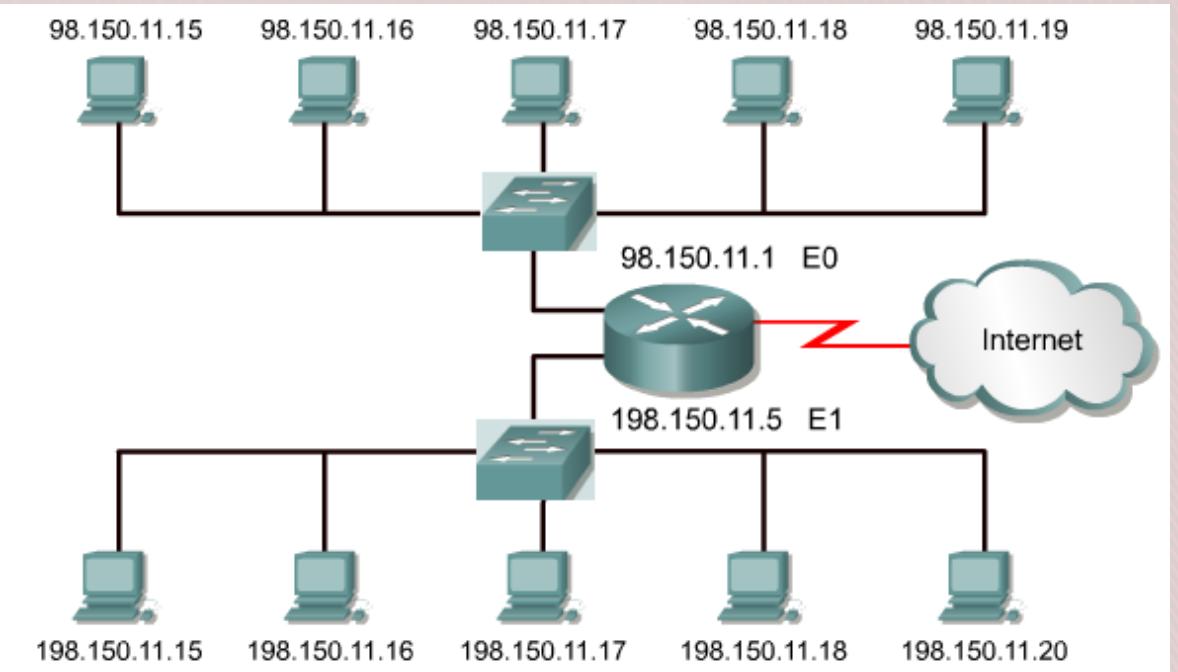
JAKIE ASPEKTY PORUSZYMY NA DZISIEJSZYCH ZAJĘCIACH

1. Czym jest Sieć komputerowa – Przypomnienie
2. Protokół ARP – co to jest, schemat działania
3. Protokół DNS – co to jest, schemat działania
4. Protokół DHCP – co to jest, schemat działania
5. Ataki MITM – rodzaje, przykłady, narzędzia
6. SSLStrip – co to jest

SIEĆ KOMPUTEROWA

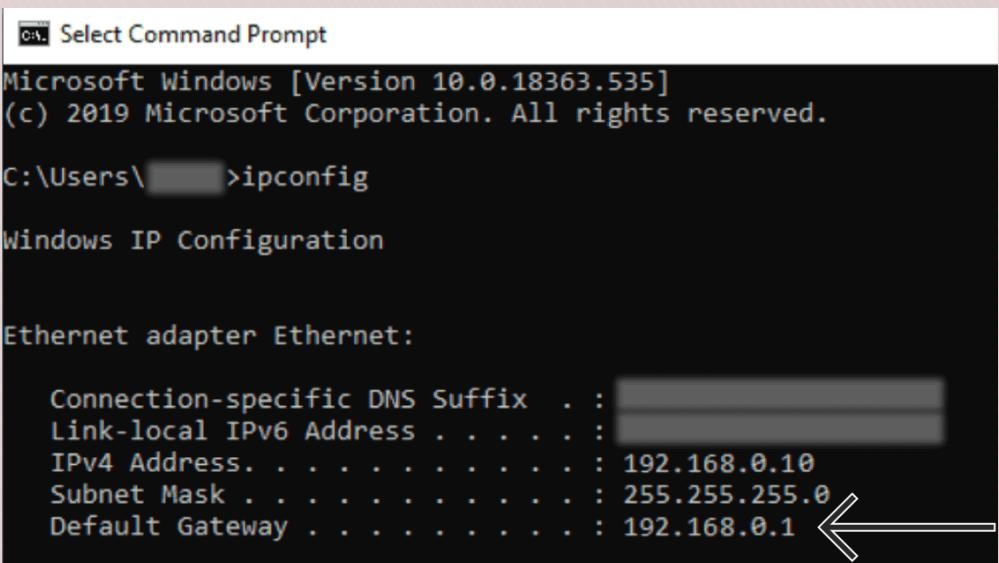
Sieć Komputerowa to zbiór komputerów i innych urządzeń sieciowych, które są połączone ze sobą za pomocą kabli lub bezprzewodowo, w celu wymiany danych i informacji.

Mogą być one różnych rozmiarów, od małych sieci lokalnych (LAN) połączonych ze sobą w jednym budynku, do ogromnych sieci rozległych (WAN) łączących komputery na całym świecie.



SIEĆ KOMPUTEROWA

Brama Domyślna (Default Gateway) to urządzenie sieciowe, które jest ustawione jako punkt końcowy dla ruchu sieciowego w danej sieci lokalnej (LAN). Służy do przekazywania pakietów danych pomiędzy urządzeniami w sieci LAN, a sieciami zewnętrznymi (na przykład Internet). Brama domyślna jest zazwyczaj ustawiona jako adres IP routera lub innego urządzenia sieciowego, które jest podłączone do sieci LAN i ma dostęp do Internetu.



```
CH Select Command Prompt
Microsoft Windows [Version 10.0.18363.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\ [REDACTED] >ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : [REDACTED]
Link-local IPv6 Address . . . . . : [REDACTED]
IPv4 Address . . . . . : 192.168.0.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1 ←
```

PROTOKÓŁ ARP

ARP (Address Resolution Protocol) to protokół sieciowy, który służy do przypisywania adresów IP do adresów **MAC** (Media Access Control) w sieci lokalnej.

Przykładowe Komendy Win\Linux:

- **arp -a** -> wyświetla tablice arp
- **arp -d** -> czyści tablicę arp

```
C:\> Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.18362.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>arp -a

Interface: 192.168.8.129 --- 0x7
 Internet Address      Physical Address      Type
 192.168.8.1           a4-9b-4f-1b-d0-8f  dynamic
 192.168.8.105          70-54-b4-11-af-da  dynamic
 192.168.8.133          70-77-81-37-34-77  dynamic
 192.168.8.255          ff-ff-ff-ff-ff-ff  static
 224.0.0.22              01-00-5e-00-00-16  static
 224.0.0.251             01-00-5e-00-00-fb  static
 224.0.0.252             01-00-5e-00-00-fc  static
 239.255.255.250         01-00-5e-7f-ff-fa  static

Interface: 192.168.56.1 --- 0x14
 Internet Address      Physical Address      Type
 192.168.56.255         ff-ff-ff-ff-ff-ff  static
 224.0.0.22              01-00-5e-00-00-16  static
 224.0.0.251             01-00-5e-00-00-fb  static
 224.0.0.252             01-00-5e-00-00-fc  static
 239.255.255.250         01-00-5e-7f-ff-fa  static

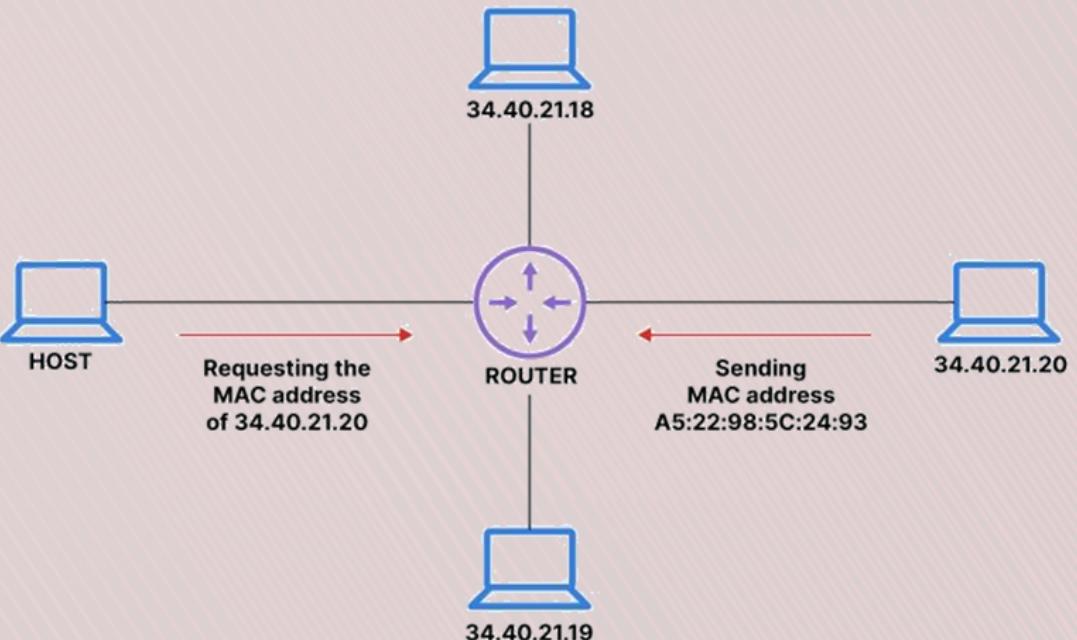
C:\WINDOWS\system32>arp -d
C:\WINDOWS\system32>arp -a

Interface: 192.168.8.129 --- 0x7
 Internet Address      Physical Address      Type
 224.0.0.22              01-00-5e-00-00-16  static

Interface: 192.168.56.1 --- 0x14
 Internet Address      Physical Address      Type
 224.0.0.22              01-00-5e-00-00-16  static
 239.255.255.250         01-00-5e-7f-ff-fa  static
```

PROTOKÓŁ ARP - PRZYKŁAD

Gdy komputer A chce wysłać do komputera B pakiet danych, najpierw musi **uzyskać adres MAC komputera B**. Aby to zrobić, wysyła on do sieci specjalne żądanie **ARP request**, zawierające adres IP komputera B. Każde urządzenie w sieci lokalnej otrzymuje to **zapytanie** i sprawdza czy **posiada podany adres IP**. Jeśli tak, to odpowiada **zwrotnym komunikatem ARP** zawierającym swój **adres MAC**. Komputer A otrzymuje tę odpowiedź i może wysłać pakiet danych z docelowym adresem MAC komputera B.



PROTOKÓŁ DNS

Protokół DNS (Domain Name System) to system nazw domen, który służy do mapowania nazw domen na adresy IP. Pozwala użytkownikom na korzystanie z nazw domen zamiast z trudnych do zapamiętania adresów IP w przeglądarce internetowej lub innym oprogramowaniu sieciowym.

Przykładowe komendy Windows:

ipconfig /flushdns - czyści pamięć podręczną DNS na komputerze, co może być przydatne w przypadku problemów z dostępem do niektórych stron internetowych

ipconfig /displaydns - wyświetla wszystkie rekordy DNS zapisane w pamięci podręcznej komputera

Przykładowe komendy Linux:

dig i **nslookup** - umożliwiają sprawdzenie informacji DNS dla określonej nazwy domeny lub adresu IP

```
C:\Users\Khan>ipconfig /displaydns

Windows IP Configuration

play.google.com
-----
Record Name . . . . .: play.google.com
Record Type . . . . .: 1
Time To Live . . . . .: 125
Data Length . . . . .: 4
Section . . . . . . .: Answer
A (Host) Record . . . .: 172.217.19.14

www.youtube.com
-----
Record Name . . . . .: www.youtube.com
Record Type . . . . .: 5
Time To Live . . . . .: 187
Data Length . . . . .: 8
Section . . . . . . .: Answer
CNAME Record . . . .: youtube-ui.l.google.com
```

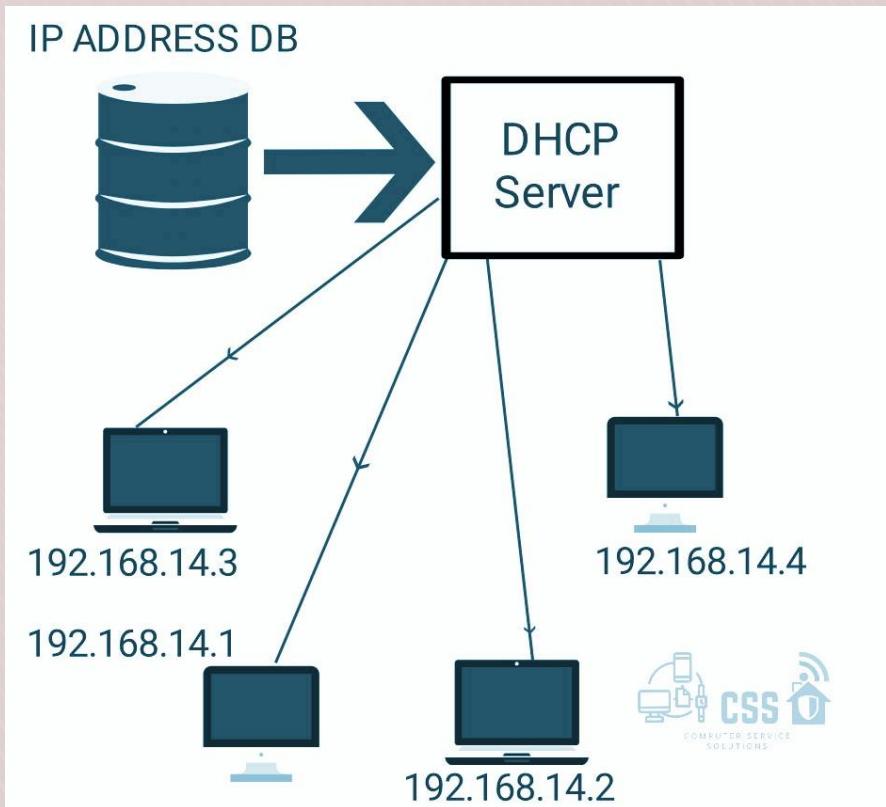
```
dave@howtogeek:~$ dig howtogeek.com +nocomments

; <>> DiG 9.11.3-1ubuntu1.11-Ubuntu <>> howtogeek.com +nocomments
;; global options: +cmd
;howtogeek.com.          IN      A
howtogeek.com.        3403    IN      A      151.101.194.217
howtogeek.com.        3403    IN      A      151.101.130.217
howtogeek.com.        3403    IN      A      151.101.66.217
howtogeek.com.        3403    IN      A      151.101.2.217
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Mar 22 07:47:05 EDT 2020
;; MSG SIZE  rcvd: 106
```

PROTOKÓŁ DHCP

Protokół DHCP (Dynamic Host Configuration Protocol) to sieciowy protokół, który umożliwia automatyczne przydzielanie adresów IP dla urządzeń w sieci LAN. Dzięki temu użytkownik nie musi tego ustawiać ręcznie osobno. Protokół DHCP działa poprzez wymianę specjalnych wiadomości pomiędzy urządzeniami w sieci:

1. Klient chcący się połączyć z serwerem wysyła do sieci lokalnej pakiety rozgłoszeniowe zaadresowane do wszystkich odbiorców. Procedura ta nosi nazwę **DHCP DISCOVER** – odkrywanie DHCP
 - 1.1. Urządzenie wysyła specjalną wiadomość o nazwie "żądanie" (ang. request) do serwera DHCP w sieci LAN
2. Serwer DHCP odpowiada wysyłając do urządzenia wiadomość o nazwie "oferta" (ang. offer), w której znajdują się informacje o adresie IP oraz innych ustawieniach sieciowych, które są dostępne dla tego urządzenia
3. Urządzenie akceptuje ofertę, wysyłając do serwera DHCP wiadomość o nazwie "potwierdzenie" (ang. acknowledgement)
4. Serwer DHCP przydziela adres IP i inne ustawienia sieciowe urządzeniu i wysyła do niego wiadomość o nazwie "przydzielanie" (ang. assignment)

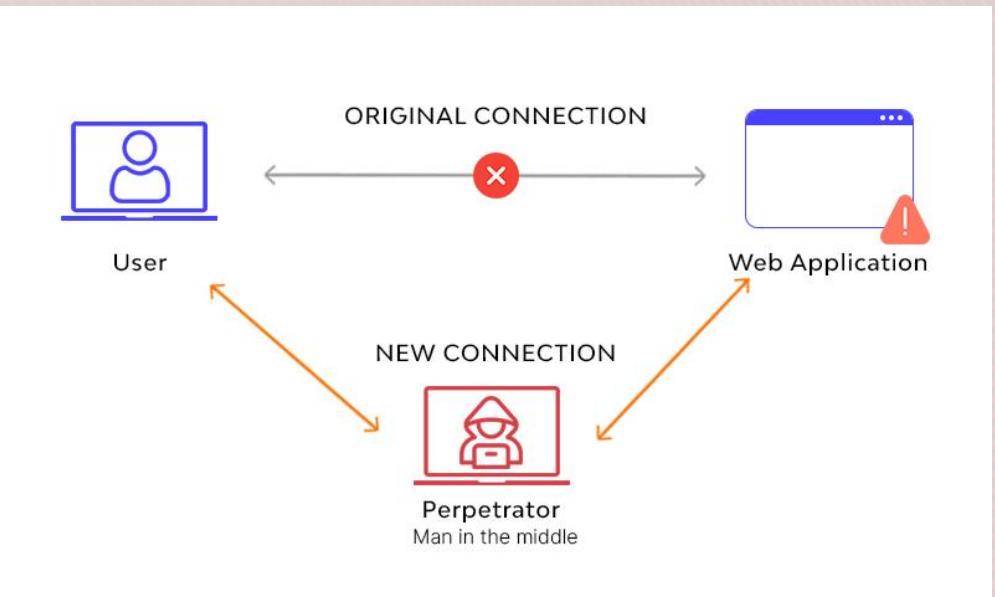


ATAKI MITM

Atak MITM (ang. Man-in-the-Middle) to rodzaj ataku, w którym atakujący wchodzi w pośrednią rolę między dwoma stronami, które wymieniają się informacjami. Atakujący może w ten sposób przechwytywać, modyfikować lub przekazywać fałszywe informacje, a także ukrywać swoją obecność przed obiema stronami.

Ataki MITM są szczególnie niebezpieczne, ponieważ obie strony mogą myśleć, że komunikują się bezpośrednio ze sobą, podczas gdy atakujący może czytać i modyfikować ich komunikaty.

Mogą być one przeprowadzane za pomocą różnych technik, takich jak podmiana adresu IP, przekierowywanie ruchu przez fałszywe punkty dostępowe lub wykorzystywanie luk w zabezpieczeniach sieci.



ATAKI MITM - PRZYKŁADY

ARP
Spoofing

DNS
Spoofing

DHCP
Spoofing

Evil Twin

BGP
Hijacking



NARZĘDZIA WYKORZYSTYWANE DO ATAŁÓW MITM

- Ettercap

Hosts list...

IP Address	MAC Address
10.157.6.1	00:10:DB:6C:4E:B8
10.157.6.40	00:30:48:43:2D:08
10.157.6.131	00:0C:29:E1:81:6E
10.157.6.139	00:0C:29:31:F3:09
10.157.6.140	00:0C:29:81:60:5B
10.157.6.151	00:0C:29:7E:3F:F8
10.157.6.152	00:0C:29:23:D7:38
10.157.6.231	00:0C:29:8D:3D:CC
10.157.6.233	00:0D:93:9C:7C:CE

- Bettercap

v1.1.0

```
[I] Targeting the whole subnet 192.168.1.0..192.168.1.255 ...
[I] Network discovery thread started.
[I] Searching for alive targets ...
[I] Getting gateway 192.168.1.254 MAC address ...
[I] Collected 4 total targets.
[I] 192.168.1.65 : 9c:d3:6d:9e:38:d4 ( Netgear, )
[I] 192.168.1.109 : e4:ce:8f:56:34:4f ( Apple )
[I] 192.168.1.129 : e8:94:f6:1f:65:86 ( Tp-link Technologies Co. )
[I] 192.168.1.253 : 2:24:17:d2:c1:91
```

- Dsniff

```
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
-----
08/15/17 06:43:20 tcp 192.168.179.147.1083 -> 192.187.120.114.21 (ftp)
USER anonymous
PASS IEUser@

-----
08/15/17 06:43:25 tcp 192.168.179.147.1084 -> 192.187.120.114.21 (ftp)
USER anonymous
PASS IEUser@

-----
08/15/17 06:43:39 tcp 192.168.179.147.1085 -> 192.187.120.114.21 (ftp)
USER yeahhub
PASS yeahhub123
```

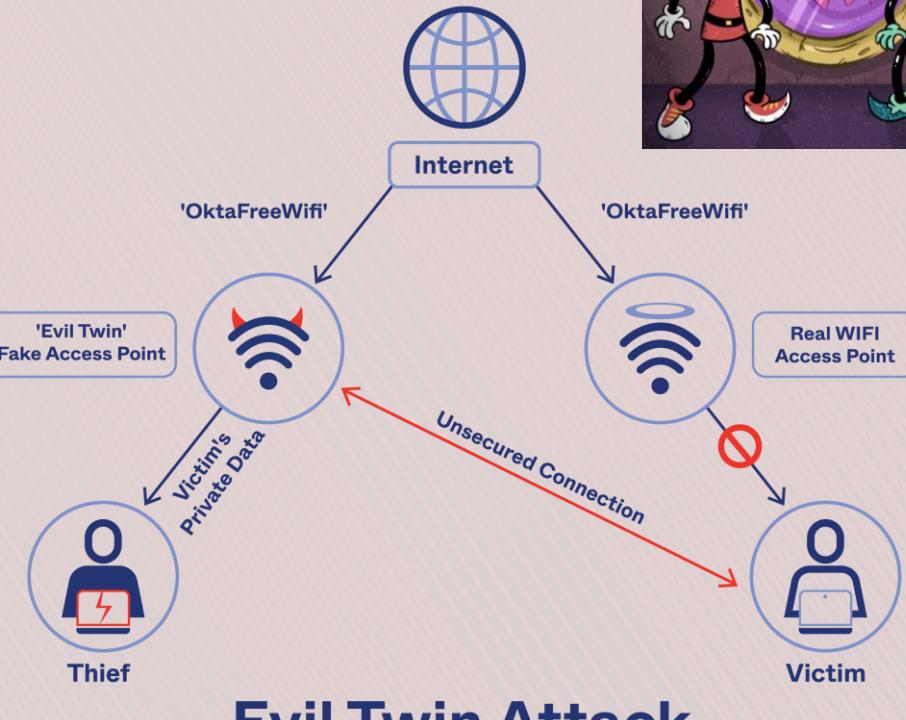
MITM – EVIL TWIN

Evil Twin Attack („Zły Bliźniak”) to rodzaj ataku MITM, w którym atakujący tworzy fałszywą sieć Wi-Fi o takiej samej nazwie jak oryginalna sieć, aby uwierzytelnić użytkowników i przechwycić ich dane.

Atakujący w ten sposób może uzyskać dostęp do danych użytkowników, takich jak hasła, dane osobowe czy informacje finansowe. Atakujący może również wykorzystać fałszywą sieć Wi-Fi do przekierowania ruchu internetowego przez własne serwery i w ten sposób uzyskać dostęp do treści, do których normalnie nie miałby dostępu.

Aby zapobiec takim atakom:

- Najlepiej unikać połączeń z publicznymi sieciami WiFi
- Wyłączyć automatyczne łączenie z WiFi (urządzenie łączy się za pośrednictwem SSID WiFi, co oznacza że nie potrafi odróżnić poprawnych od złych sieci bliźniaczych)
- Używać szyfrowania np za pomocą VPN.



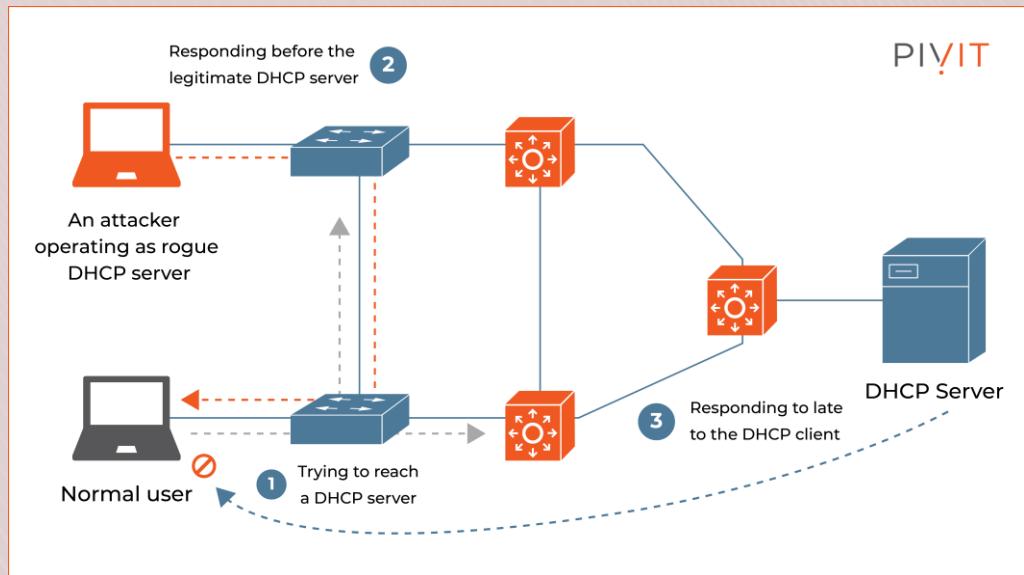
MITM – DHCP SPOOFING

DHCP Spoofing, to rodzaj ataku, w którym atakujący wysyła fałszywe odpowiedzi protokołu DHCP do sieci, oszukując urządzenia, że otrzymują prawidłowe przypisanie adresu IP od serwera DHCP.

Celem ataku jest wyczerpanie puli dostępnych adresów IP w sieci, co powoduje, że prawidłowe urządzenia nie mogą się połączyć. Może też być używany do przekierowywania ruchu do złośliwych serwerów lub stron internetowych, umożliwiając przechwytywanie wrażliwych danych lub zainfekowanie urządzeń malware'm.

Aby zapobiec takim atakom:

- Poprawie ustawień firewalla i IDSy oraz dodatkowo używać szyfrowania
- Regularne aktualizowanie oprogramowania i firmware, aby zapewnić ochronę urządzeń przed znymi lukami bezpieczeństwa



MITM – DNS SPOOFING

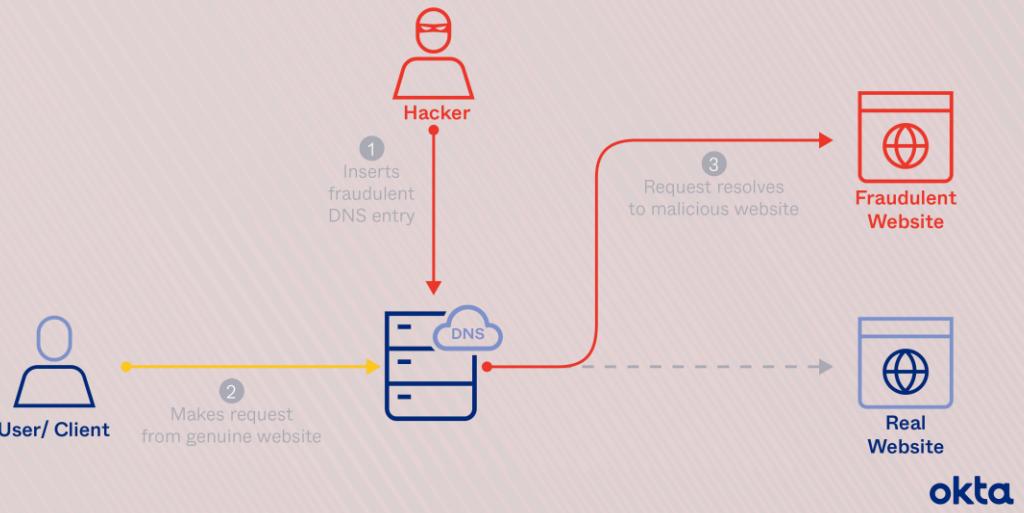
DNS **Spoofing**, to rodzaj ataku, w którym atakujący manipuluje rekordami DNS danej domeny, przekierowując ruch przeznaczony dla prawdziwej strony internetowej na złośliwą stronę. Umożliwia to przechwycenie wrażliwych danych, takich jak dane logowania lub informacje finansowe, lub nawet na dystrybucję malware nieświadomym użytkownikom.

DNS spoofing polega na oszukaniu serwera DNS, że fałszywy rekord DNS jest prawdziwy. Opiera się to wszystko na wykorzystaniu luki w zabezpieczeniach serwera DNS. Gdy użytkownik wpisuje nazwę domeny, serwer DNS szuka odpowiadającego adresu IP i kieruje przeglądarkę użytkownika na odpowiednią stronę internetową.

Jeśli nie zostało zaimplementowane sprawdzanie wiarygodności źródła odpowiedzi DNS (na przykład korzystając z DNSSEC), to serwer zapisze w pamięci sperekonowany przez atakującego rekord i udostępni go, kierując użytkownika na złośliwą stronę internetową, zamiast tej prawidłowej.

Aby zapobiec takim atakom po stronie klienta:

- Poprawie ustawień firewalla i IDSy oraz dodatkowo używać szyfrowania
- Regularne aktualizowanie oprogramowania i firmware



MITM – SSL STRIPPING

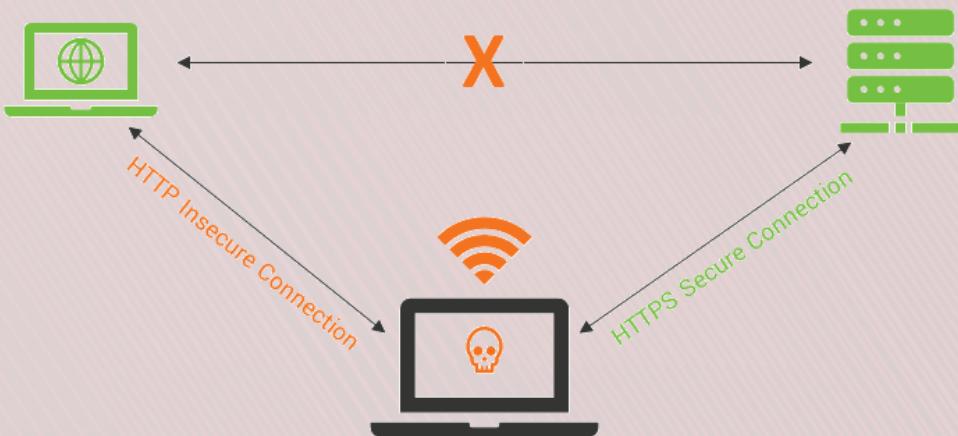
SSL Stripping, to rodzaj ataku, w którym atakujący próbuje wykorzystać luki w bezpieczeństwie sieci, aby przechwycić ruch sieciowy i zdjąć warstwę bezpieczeństwa z szyfrowanego połączenia SSL/TLS.

Podczas ataku atakujący udaje pośrednika pomiędzy użytkownikiem a stroną internetową i próbuje przekierować ruch sieciowy przez niezabezpieczone połaczenie HTTP zamiast przez szyfrowane połaczenie HTTPS. Dzięki temu atakujący może przechwycić wrażliwe dane, które są przesyłane między użytkownikiem, a stroną internetową.

Aby zapobiec takim atakom:

- Stosowanie protokołu HTTPS dla wszystkich stron internetowych, które przetwarzają wrażliwe dane
- Regularne aktualizowanie oprogramowania i firmware

How an SSL Stripping Attack Works



Zaawansowane

Zawsze używaj bezpiecznych połączeń

Uaktualnij elementy nawigacyjne do protokołu HTTPS i wyświetlaj ostrzeżenia przed wczytaniem stron, które go nie obsługują



Użyj bezpiecznego serwera DNS

Określa, jak nawiązywać połączenia ze stronami przez zabezpieczone połączenie



Korzystając z obecnego dostawcy usługi

Bezpieczny DNS może nie być dostępny przez cały czas

Za pomocą Niestandardowe ▾

MITM – ARP SPOOFING

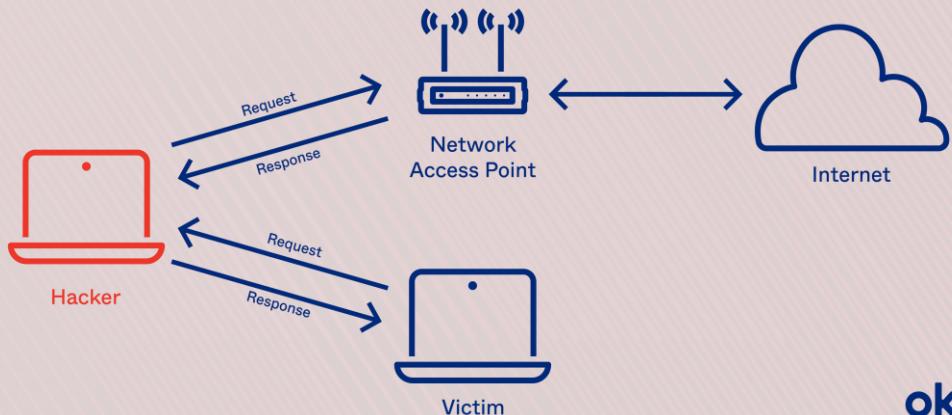
ARP **Spoofing**, to rodzaj ataku, w którym atakujący manipuluje tablicami ARP, aby przekierować ruch sieciowy na swoje urządzenie.

Podczas ataku ARP spoofing atakujący wysyła fałszywe odpowiedzi ARP do urządzeń w sieci, podając swój adres MAC jako adres MAC urządzenia docelowego. Dzięki temu wszystkie pakiety przesyłane do urządzenia docelowego są faktycznie przekierowywane do atakującego, pozwalając mu przechwytywać ruch sieciowy lub wprowadzać zmiany w przesyłanych danych.

Aby zapobiec takim atakom:

- Poprawie ustawień firewalla i IDSy oraz dodatkowo używać szyfrowania
- Regularne aktualizowanie oprogramowania i firmware, aby zapewnić ochronę urządzeń przed znanimi lukami bezpieczeństwa

ARP Poisoning/Spoofing



okta

MITM – ARP SPOOFING - PRZYKŁAD

```
Windows Command Prompt  
Microsoft Windows [Version 10.0.17763.737]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Users\user>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::d0fc:bf97:54a:d6ba%13  
IPv4 Address . . . . . : 192.168.1.19  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.254  
  
Ethernet adapter Npcap Loopback Adapter:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::f950:9fc0:64e1  
Autoconfiguration IPv4 Address. . : 169.254.79.7  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . :
```

```
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:7f:71:3a  
          inet addr:192.168.1.10 Bcast:192.168.1.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe7f:713a/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:4423 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:619 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:371905 (363.1 KB) TX bytes:814816 (795.7 KB)  
          Base address:0xd010 Memory:f0000000-f0020000  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING MTU:16436 Metric:1  
          RX packets:335 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:335 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:123489 (120.5 KB) TX bytes:123489 (120.5 KB)
```

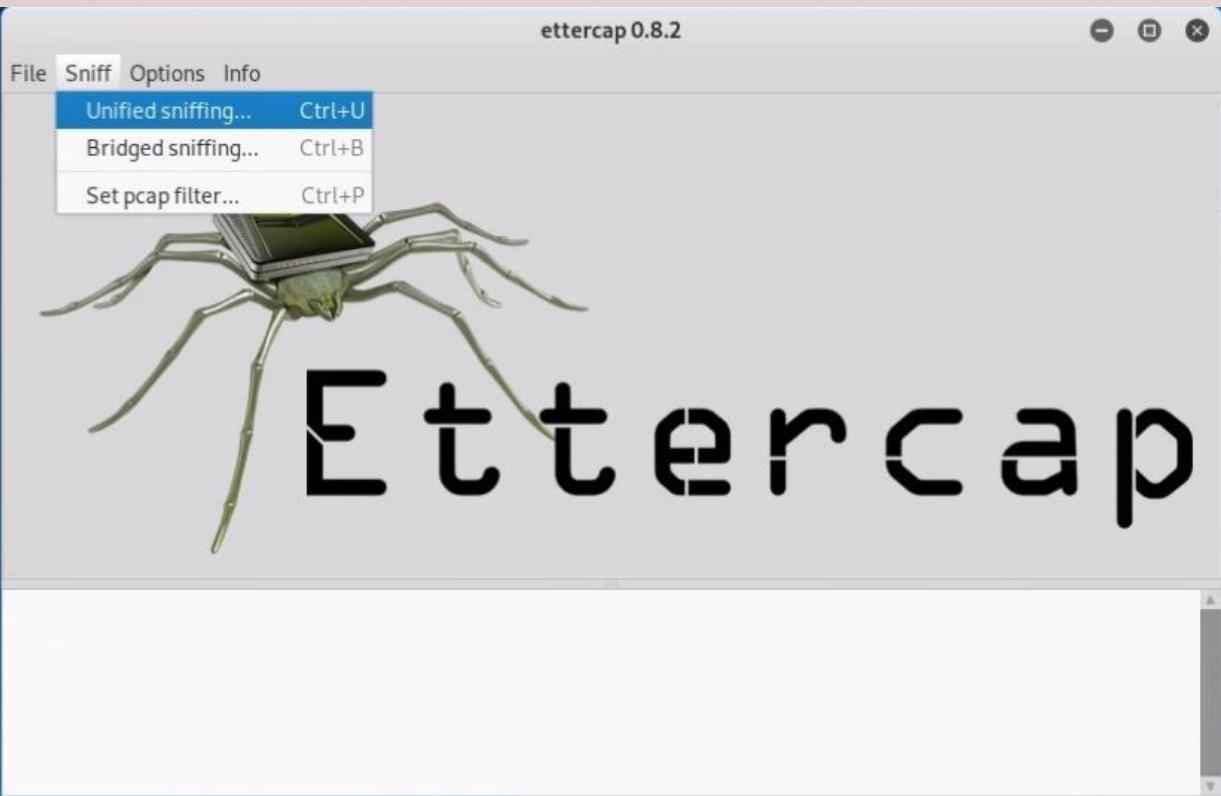


MITM – ARP SPOOFING - PRZYKŁAD

The image shows a Kali Linux desktop environment. In the top-left corner, there is a terminal window titled "root@kali: ~" with the command "ettercap -G" entered and the output "ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team" displayed. To the right of the terminal is the Ettercap graphical user interface window, titled "ettercap 0.8.2". The window features a logo of a spider with a circuit board body and the word "Ettercap" in large, bold, black letters. The Ettercap interface has a menu bar with "File", "Sniff", "Options", and "Info".



MITM – ARP SPOOFING - PRZYKŁAD



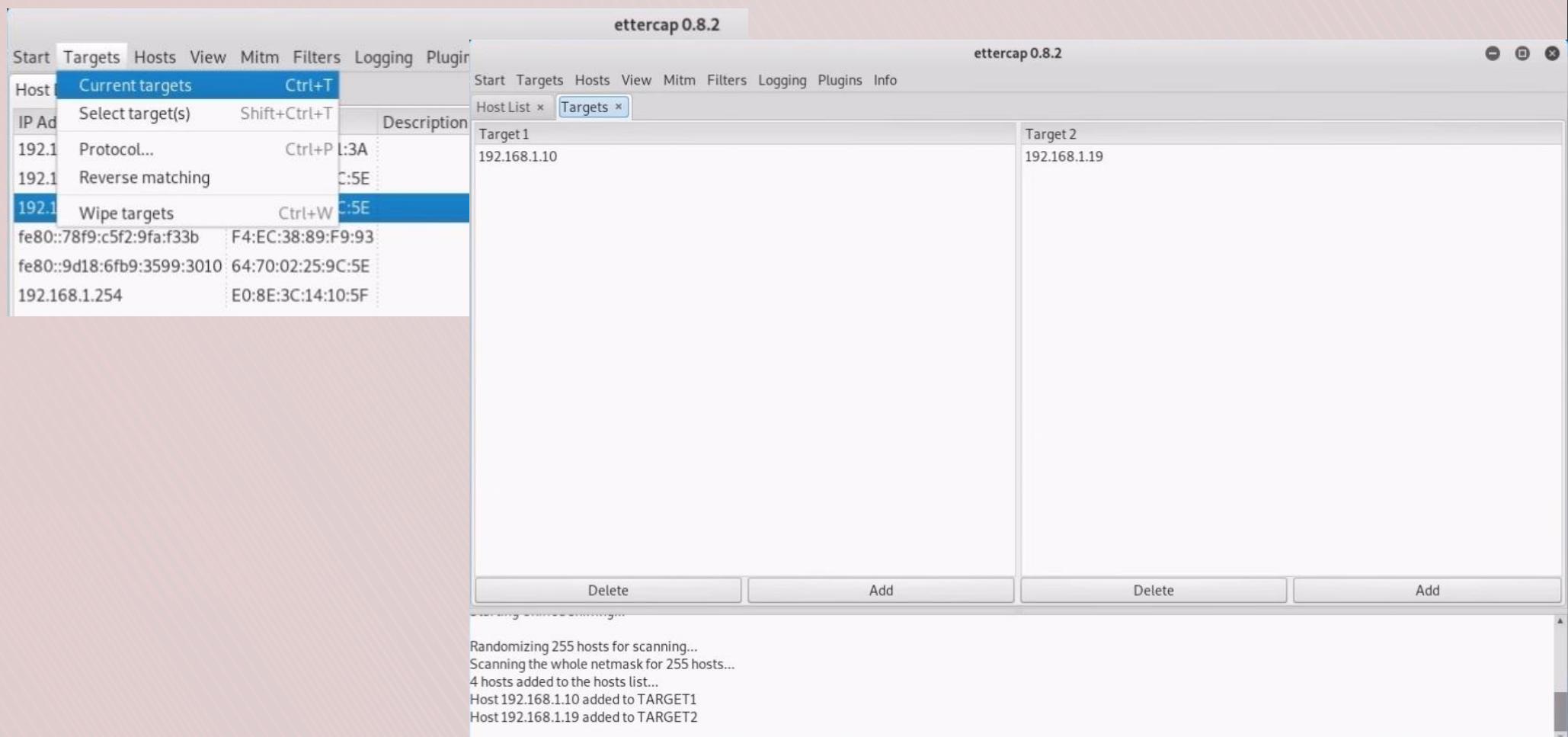
MITM – ARP SPOOFING - PRZYKŁAD

The screenshot shows a network penetration testing interface with the following components:

- Host List (Main Window):** Displays a table of discovered hosts with IP Address, MAC Address, and Description columns. The table includes:

IP Address	MAC Address	Description
192.168.1.10	08:00:27:7F:71:3A	
192.168.1.12	64:70:02:25:9C:5E	
192.168.1.19	64:70:02:25:9C:5E	
fe80::78f9:c5f2:9fa:f33b	F4:EC:38:89:F9:93	
fe80::9d18:6fb9:3599:3010	64:70:02:25:9C:5E	
192.168.1.254	E0:8E:3C:14:10:5F	
- Host List (Sub-Menu):** A context menu for host 192.168.1.10 with options: Add to Target 1, Add to Target 2, and Delete host.
- Host List (Sub-Menu):** A context menu for host 192.168.1.19 with options: Add to Target 1, Add to Target 2, and Delete host.
- Buttons:** Delete Host, Add to Target 1, Add to Target 2.
- Logs:** Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...

MITM – ARP SPOOFING - PRZYKŁAD

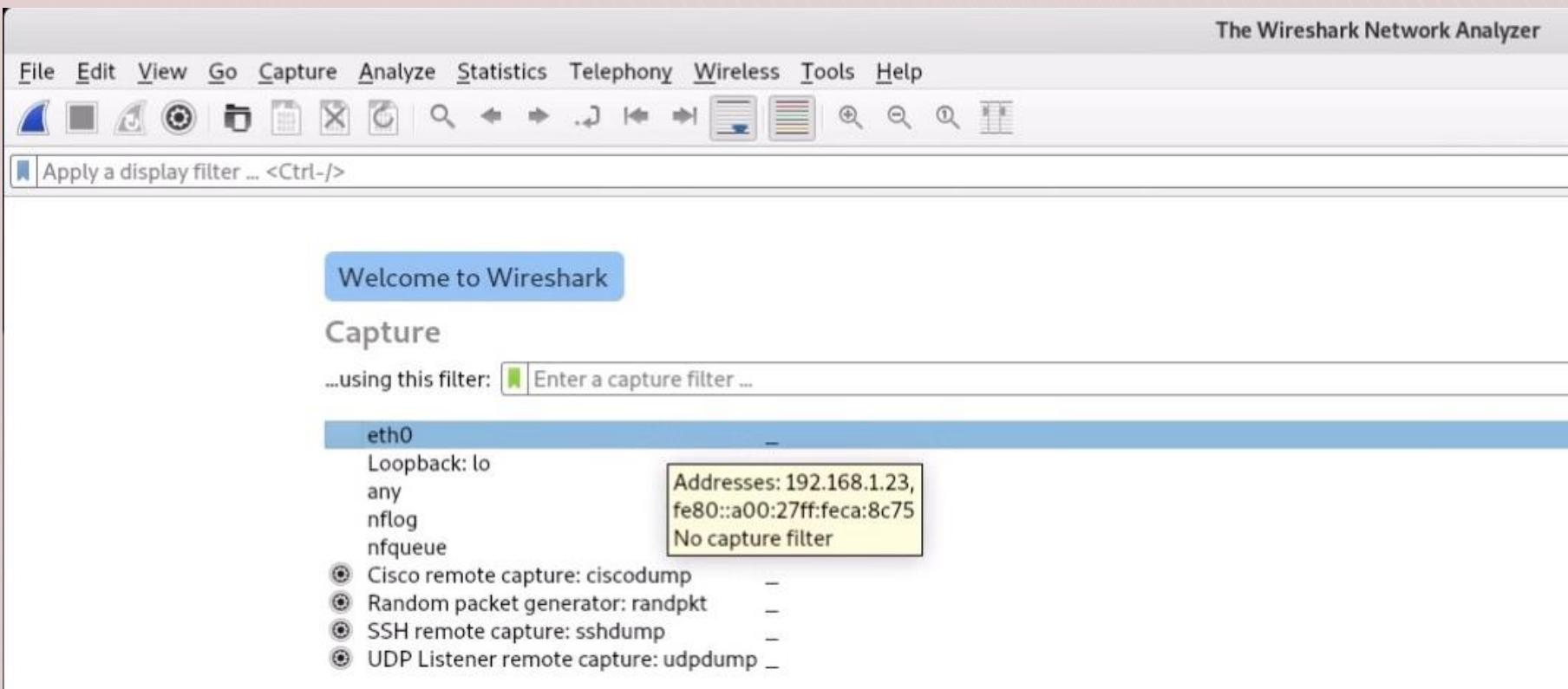


MITM – ARP SPOOFING - PRZYKŁAD

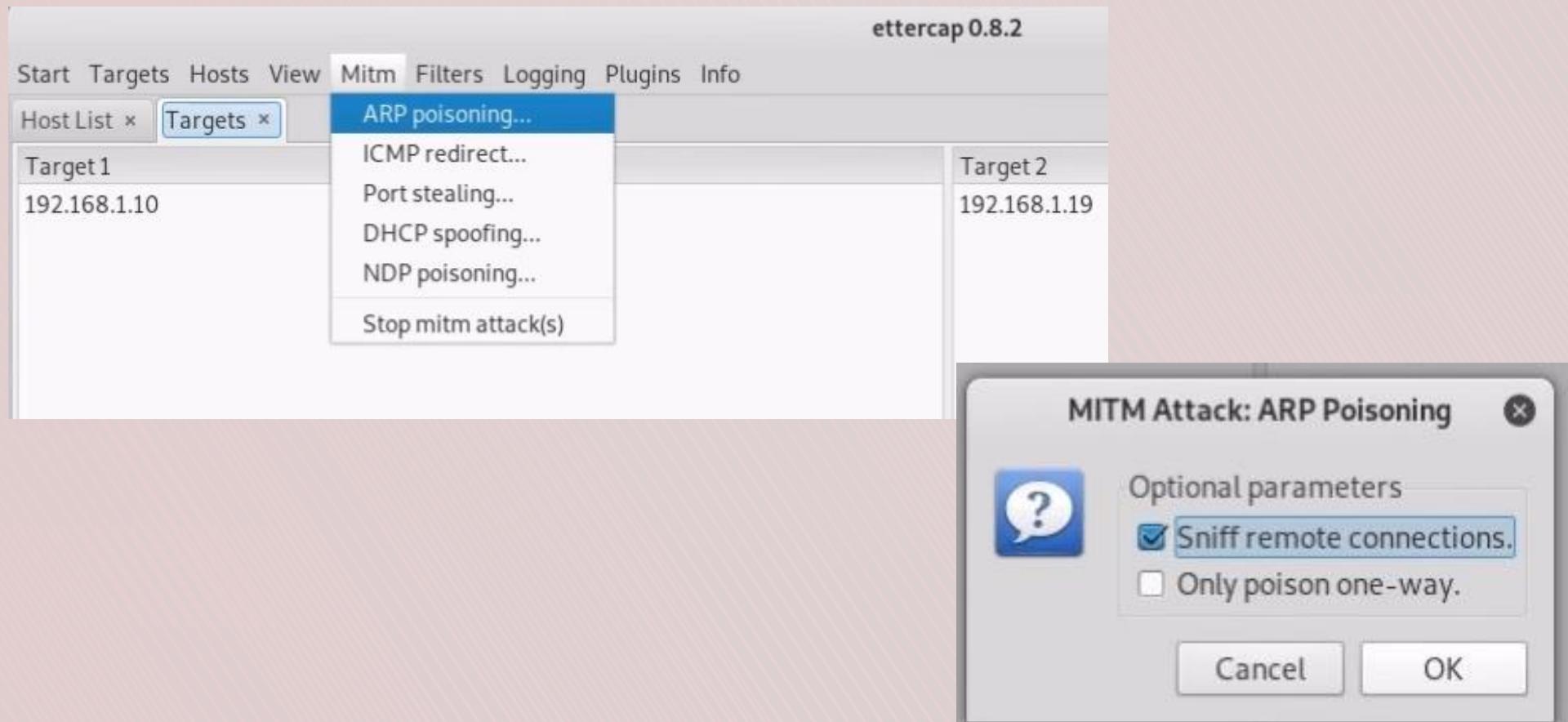
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# cat</proc/sys/net/ipv4/ip_forward
0
root@kali:~# echo 1>/proc/sys/net/ipv4/ip_forwardment Team
```



MITM – ARP SPOOFING - PRZYKŁAD



MITM – ARP SPOOFING - PRZYKŁAD



MITM – ARP SPOOFING - PRZYKŁAD

Capturing from eth0

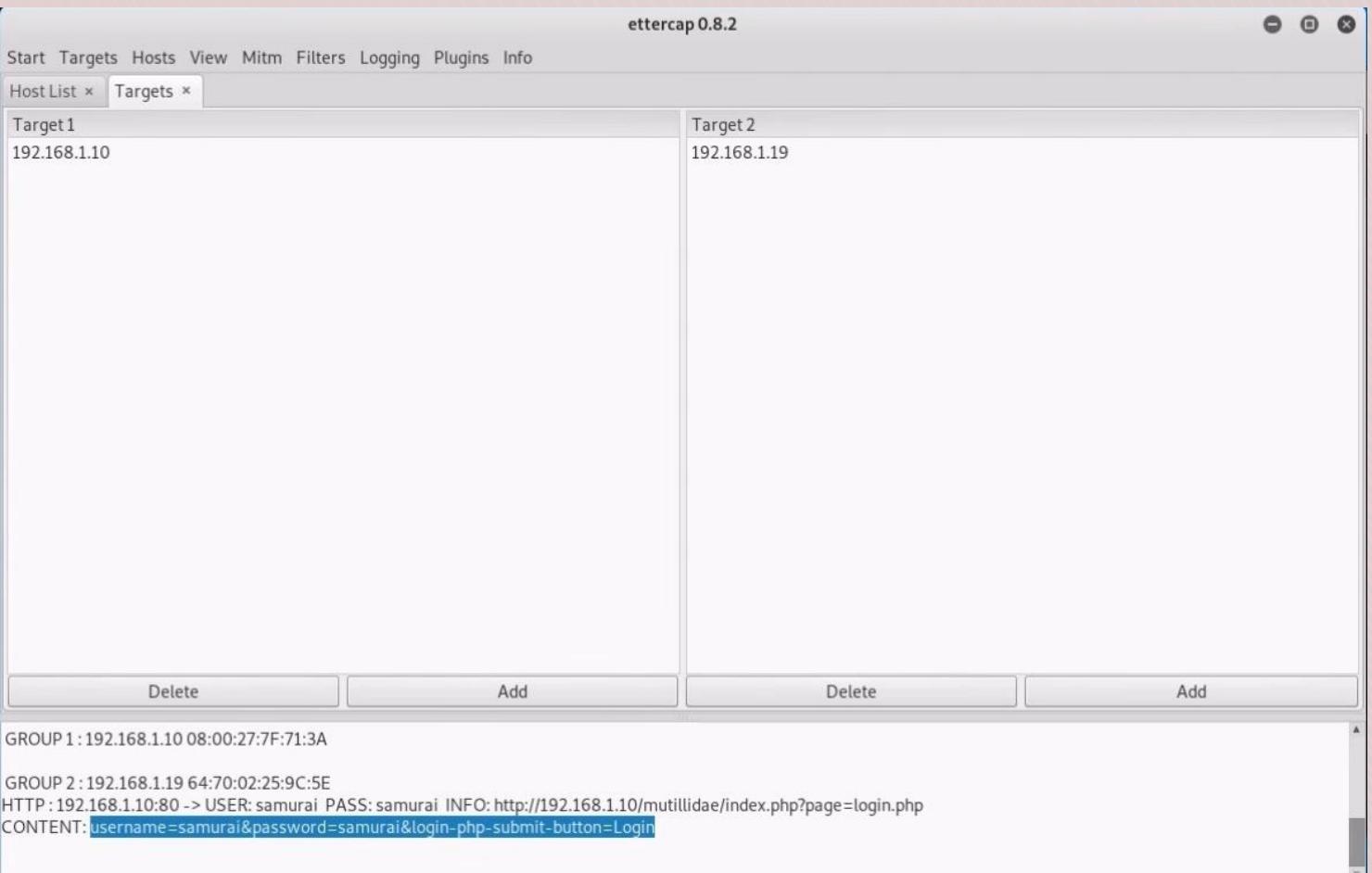
No.	Time	Source	Destination	Protocol	Length	Info
45	14.124078916	192.168.1.19	192.168.1.10	ICMP	42	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=127
46	14.126047890	192.168.1.10	192.168.1.19	ICMP	42	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=64
47	14.126170754	192.168.1.19	192.168.1.10	ICMP	42	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=128
48	15.135480086	PcsCompu_ca:8c:75	PcsCompu_7f:71:3a	ARP	42	192.168.1.19 is at 08:00:27:ca:8c:75
49	15.135593259	PcsCompu_ca:8c:75	Tp-LinkT_25:9c:5e	ARP	42	192.168.1.10 is at 08:00:27:ca:8c:75 (duplicate use of 192.168.1.19 detected!)
50	15.686165107	192.168.1.19	239.255.255.250	SSDP	180	M-SEARCH * HTTP/1.1
51	16.146343512	PcsCompu_ca:8c:75	PcsCompu_7f:71:3a	ARP	42	192.168.1.19 is at 08:00:27:ca:8c:75
52	16.146422174	PcsCompu_ca:8c:75	Tp-LinkT_25:9c:5e	ARP	42	192.168.1.10 is at 08:00:27:ca:8c:75 (duplicate use of 192.168.1.19 detected!)
53	17.156686698	PcsCompu_ca:8c:75	PcsCompu_7f:71:3a	ARP	42	192.168.1.19 is at 08:00:27:ca:8c:75
54	17.156757487	PcsCompu_ca:8c:75	Tp-LinkT_25:9c:5e	ARP	42	192.168.1.10 is at 08:00:27:ca:8c:75 (duplicate use of 192.168.1.19 detected!)
55	18.166962509	PcsCompu_ca:8c:75	PcsCompu_7f:71:3a	ARP	42	192.168.1.19 is at 08:00:27:ca:8c:75
56	18.167030591	PcsCompu_ca:8c:75	Tp-LinkT_25:9c:5e	ARP	42	192.168.1.10 is at 08:00:27:ca:8c:75 (duplicate use of 192.168.1.19 detected!)
57	18.655657060	192.168.1.19	239.255.255.250	SSDP	180	M-SEARCH * HTTP/1.1
58	19.249917530	PcsCompu_ca:8c:75	Tp-LinkT_25:9c:5e	ARP	42	Who has 192.168.1.19? Tell 192.168.1.23
59	19.249969308	PcsCompu_ca:8c:75	PcsCompu_7f:71:3a	ARP	42	Who has 192.168.1.10? Tell 192.168.1.23
60	19.250136300	PcsCompu_7f:71:3a	PcsCompu_ca:8c:75	ARP	60	192.168.1.10 is at 08:00:27:7f:71:3a
61	19.253381334	Tp-LinkT_25:9c:5e	PcsCompu_ca:8c:75	ARP	60	192.168.1.19 is at 64:70:02:25:9c:5e
62	21.727612312	192.168.1.19	239.255.255.250	SSDP	180	M-SEARCH * HTTP/1.1



MITM – ARP SPOOFING - PRZYKŁAD



MITM – ARP SPOOFING - PRZYKŁAD



MITM – ARP SPOOFING - PRZYKŁAD

887	79.636184384	142.251.129.131	192.168.80.139	OCSP	756 Response
919	79.688514255	192.168.80.139	142.251.129.131	OCSP	481 Request
933	79.816769897	142.251.129.131	192.168.80.139	OCSP	756 Response
1324	117.227657645	192.168.80.139	192.16.58.8	OCSP	478 Request
1329	117.233061514	192.16.58.8	192.168.80.139	OCSP	853 Response
1441	126.166231843	192.168.80.139	44.228.249.3	HTTP	592 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
1445	126.428321590	44.228.249.3	192.168.80.139	HTTP	330 HTTP/1.1 302 Found (text/html)
1447	126.428127950	192.168.80.139	44.228.249.3	HTTP	461 GET /login.php HTTP/1.1
1453	126.676752889	44.228.249.3	192.168.80.139	HTTP	2802 HTTP/1.1 200 OK (text/html)
1945	219.825996579	192.168.80.139	190.98.140.10	OCSP	477 Request
1951	219.834898831	190.98.140.10	192.168.80.139	OCSP	942 Response
2017	220.130656633	192.168.80.139	190.98.140.10	OCSP	477 Request
2021	220.142342810	190.98.140.10	192.168.80.139	OCSP	943 Response
2176	235.603153480	192.168.80.187	35.232.111.17	HTTP	141 GET / HTTP/1.1
2178	235.771459579	35.232.111.17	192.168.80.187	HTTP	202 HTTP/1.1 204 No Content
<pre>Accept-Encoding: gzip, deflate\r\nContent-Type: application/x-www-form-urlencoded\r\nContent-Length: 22\r\n[Content length: 22]\r\nOrigin: http://testphp.vulnweb.com\r\nConnection: keep-alive\r\nReferer: http://testphp.vulnweb.com/login.php\r\nUpgrade-Insecure-Requests: 1\r\n\r\n[Full request URI: http://testphp.vulnweb.com/userinfo.php]\r\n[HTTP request 1/2]\r\n[Response in frame: 1445]\r\n[Next request in frame: 1447]\r\nFile Data: 22 bytes</pre>					
<pre>HTML Form URL Encoded: application/x-www-form-urlencoded\r\n Form item: "uname" = "admin"\r\n Form item: "pass" = "admin"</pre>					



MITM – ARP SPOOFING - PRZYKŁAD

The screenshot shows a Wireshark capture of an FTP session on interface *eth0. The session is titled "ftp" and shows traffic between two hosts: 192.168.80.144 and 192.168.80.139. The protocol is identified as FTP. The captured frames include:

No.	Time	Source	Destination	Protocol	Length	Info
575	29.944231161	192.168.80.144	192.168.80.139	FTP	74	Response: 220 (vsFTPD 2.3.4)
576	29.975430081	192.168.80.139	192.168.80.144	FTP	68	Request: OPTS UTF8 ON
578	29.975627565	192.168.80.144	192.168.80.139	FTP	80	Response: 200 Always in UTF8 mode.
598	35.576850026	192.168.80.139	192.168.80.144	FTP	69	Request: USER msfadmin
599	35.576969381	192.168.80.144	192.168.80.139	FTP	88	Response: 331 Please specify the password.
613	39.242678898	192.168.80.139	192.168.80.144	FTP	69	Request: PASS msfadmin
614	39.244245012	192.168.80.144	192.168.80.139	FTP	77	Response: 230 Login successful.



DZIĘKI ZA UWAGĘ !

