

Politechnika Wrocławska, Informatyka Stosowana

ATAKI NA KOMUNIKACJĘ

Cyberbezpieczeństwo, Laboratorium nr.8 - raport

Autor: Aleksander Stepaniuk
Nr. Indeksu: 272644

4. Problemy i pytania

Pytanie 1.1;

Ataki aktywne typu MitM polegają na przechwytywaniu oraz modyfikacji ruchu w czasie rzeczywistym, np. zatrucie ARP czy modyfikacja pakietów. Pasywne ataki MitM ograniczają się do podsłuchiwania i analizy ruchu bez jego zmiany (np. przechwytywanie wiadomości / pliku wysłanego email). Ataki pasywne są znacznie trudniejsze do wykrycia od aktywnych, ponieważ osoba trzecia pozostaje niewidoczna dla obydwu stron komunikacji.

Pytanie 1.2;

Można stosować statyczne tablice ARP lub filtrowanie ARP w routerze, co uniemożliwia modyfikację tablic ARP przez atakującego. Alternatywnie, użycie protokołu „DHCP Snooping” oraz dynamicznego ARP Inspection (DAI) w przełącznikach sieciowych znacznie ogranicza ryzyko takich ataków. Warto również dbać o aktualne oprogramowanie antywirusowe oraz zaporę sieciową (firewall), które również mogą wykrywać i blokować niepożądany ruch w sieci.

Pytanie 1.3;

DNSSEC zapewnia integralność danych DNS poprzez cyfrowe podpisy i szyfrowanie asymetryczne, co uniemożliwia fałszowanie odpowiedzi DNS. Chroni to użytkowników przed przekierowaniem na fałszywe strony, zmniejszając ryzyko kradzieży danych czy innych ataków (sam DNS nie zawiera żadnych mechanizmów zabezpieczających i każdy użytkownik może uruchomić w sieci własny serwer DNS i przekierować na niego ruch sieciowy).

Pytanie 1.4;

Tryb monitorowania pozwala karcie sieciowej przechwytywać wszystkie pakiety w zasięgu danej sieci, niezależnie od tego, czy są one przeznaczone dla danego urządzenia. Używa się go do analizy ruchu, diagnozowania problemów w sieci, wykrywania ataków, a także do przeprowadzania audytów bezpieczeństwa. W połączeniu z narzędziami takimi jak Wireshark, pozwala dokładnie analizować dane przesyłane w sieci, przechwytywać dane uwierzytelniające lub identyfikować podatności. W sieciach bezprzewodowych może służyć do wykrywania nieautoryzowanych urządzeń lub prób przejęcia sesji.

5. Zadania

Adresy IP:

- Ubuntu: 192.168.188.34/24
- Kali: 192.168.188.35/24
- Meta: 192.168.188.36/24
- Domyślna brama: 192.168.188.1/24

```
File Actions Edit View Help
(stud@kali-vm)-[~]
$ locate etter.dns
/etc/ettercap/etter.dns
/usr/share/ettercap/etter.dns.examples

(stud@kali-vm)-[~]
$ cd /etc/ettercap

(stud@kali-vm)-[/etc/ettercap]
$ ls
etter.conf  etter.dns  etter.mdns  etter.nbns

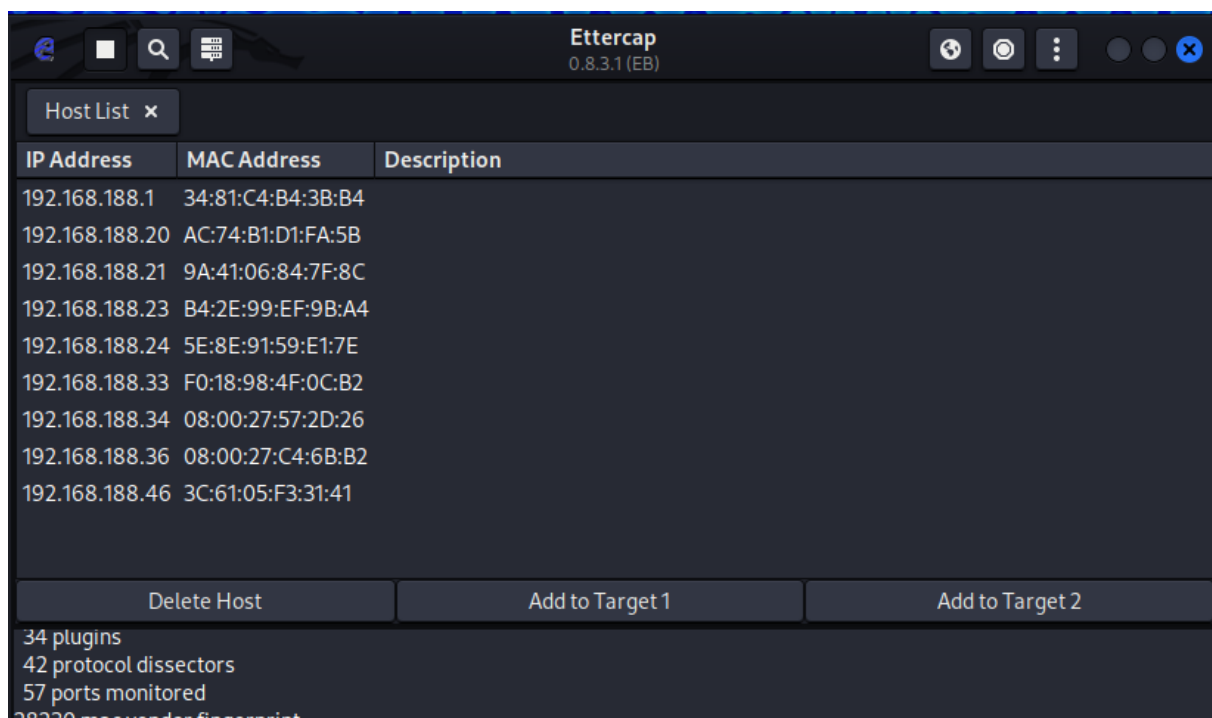
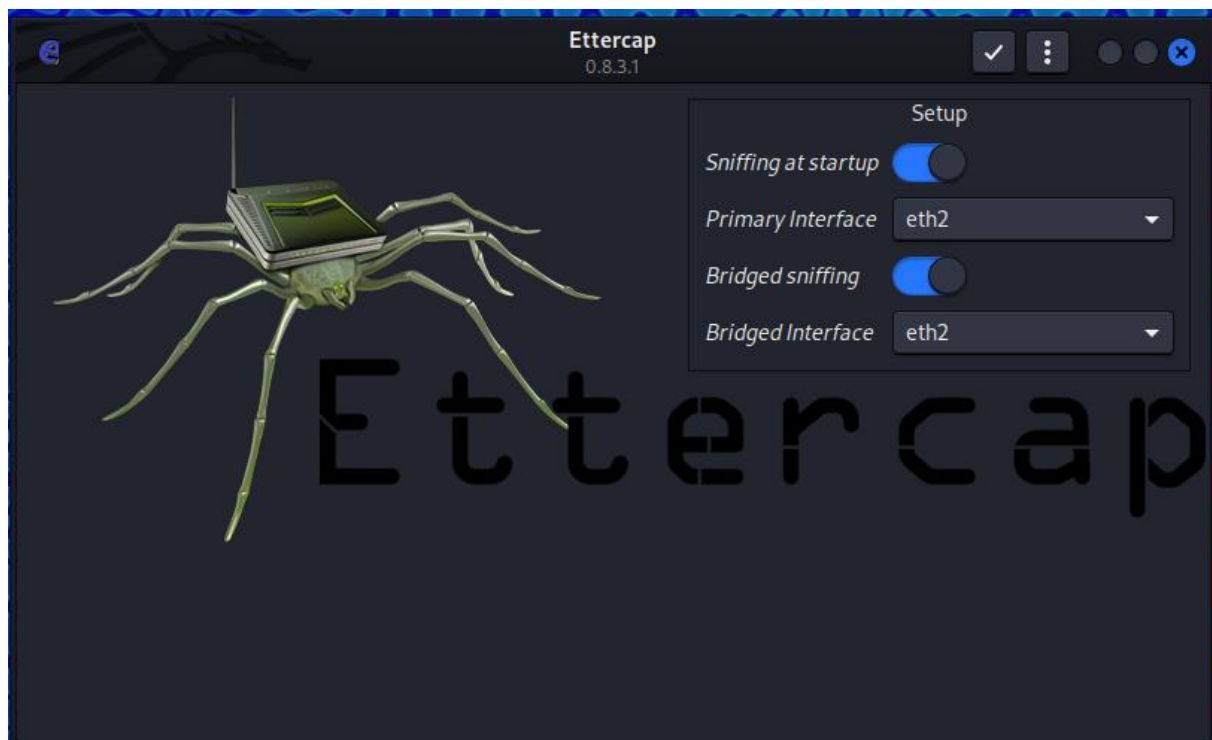
(stud@kali-vm)-[/etc/ettercap]
$
```

```
GNU nano 8.2      etter.dns
#
# or for TXT query (value must be wrapped in double quotes):
#   google.com TXT "v=spf1 ip4:192.168.0.3/32 ~all" [TTL]
#
# NOTE: the wildcarded hosts can't be used to poison the PTR requests
#       so if you want to reverse poison you have to specify a plain
#       host. (look at the www.microsoft.com example)
#
# NOTE: Default DNS TTL is 3600s (1 hour). All TTL fields are optional.
#
# NOTE: IPv6 specific do not work because ettercap has been built without
#       IPv6 support. Therefore the IPv6 specific examples has been
#       commented out to avoid ettercap throwing warnings during startup.
#
#####


# vim:ts=8:noexpandtab

pwr.edu.pl A 192.168.188.35
www.pwr.edu.pl PTR 192.168.188.35
```

```
(stud@kali-vm)-[/etc/ettercap]
$ service apache2 status
• apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; prese>
  Active: active (running) since Tue 2024-11-26 14:59:53 CET; 14min ago
  Docs: https://httpd.apache.org/docs/2.4/
  Process: 668 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/>
  Main PID: 710 (apache2)
```



🔒 pwr.edu.pl



Apache2 Debian Default Page

debian

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview


Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|  
|-- ports.conf
```

Widać, że połączenie jest niezabezpieczone (protokół HTTP zamiast HTTPS) i atak jest skuteczny, bo przeniosło nas na domyślną stronę apache.

🔒 192.168.188.36/dvwa/login.php



Username

Password



Username

pan

Password

Login

ARP poisoning victims:

GROUP 1: 192.168.188.34 08:00:27:57:2D:26

GROUP 2: 192.168.188.36 08:00:27:C4:6B:B2

HTTP : 192.168.188.36:80 -> USER: pan PASS: kowalski INFO: http://192.168.188.36/dvwa/login.php

CONTENT: username=pan&password=kowalski&Login=Login

Kali Lab 2024/2025 [Uruchomiona] - Oracle VM VirtualBox

Plik Maszyna Widok Wejście Urządzenia Pomoc

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.188.34

No.	Time	Source	Destination	Protocol	Length	Info
16	3.365138209	192.168.188.34	224.0.0.22	IGMPv3	60	Membership Re
134	86.171932123	192.168.188.34	192.168.188.36	TCP	74	53858 → 80 [S
135	86.176198515	192.168.188.34	192.168.188.36	TCP	74	[TCP Retransm
136	86.176647036	192.168.188.36	192.168.188.34	TCP	74	80 → 53858 [S
137	86.183483111	192.168.188.36	192.168.188.34	TCP	74	[TCP Retransm
138	86.183928831	192.168.188.34	192.168.188.36	TCP	66	53858 → 80 [A
139	86.183928981	192.168.188.34	192.168.188.36	HTTP	724	POST /dvwa/lo
140	86.195378375	192.168.188.34	192.168.188.36	TCP	66	53858 → 80 [A
141	86.195666285	192.168.188.34	192.168.188.36	TCP	724	[TCP Retransm
142	86.204879942	192.168.188.36	192.168.188.34	TCP	66	80 → 53858 [A
143	86.207664906	192.168.188.36	192.168.188.34	TCP	66	[TCP Dup ACK
144	86.338599689	192.168.188.36	192.168.188.34	HTTP	458	HTTP/1.1 302
145	86.348225909	192.168.188.36	192.168.188.34	TCP	458	[TCP Retransm
146	86.348785291	192.168.188.34	192.168.188.36	TCP	66	53858 → 80 [A
147	86.357025849	192.168.188.34	192.168.188.36	HTTP	582	GET /dvwa/log
148	86.357310821	192.168.188.34	192.168.188.36	TCP	66	53858 → 80 [A
150	86.363537493	192.168.188.34	192.168.188.36	TCP	582	[TCP Retransm
151	86.414987862	192.168.188.36	192.168.188.34	TCP	66	80 → 53858 [A
152	86.419476040	192.168.188.36	192.168.188.34	TCP	66	[TCP Dup ACK

Frame 134: 74 bytes on wire (592 bits), 74 bytes captured on interface eth0

Ethernet II, Src: PCSSystemtec_57:2d:26 (08:00:27:57:2d:26), Destination: PCSSystemtec_f5:63:f7 (08:00:27:f5:63:f7), Source: PCSSystemtec_57:2d:26 (08:00:27:57:2d:26)

wireshark_eth2TIRVX2.pcapng Packets: 189 · Displayed: 37 (19.6%) Profile: Default