

Лабораторна робота №16(5.1.16)

Сканування SMB вразливостей за допомогою enum4linux

Хід роботи:

Частина 1: Запуск Ettercap та дослідження можливостей

Крок 1: Налаштування атаки ARP spoofing

Завдання: Підготуйте середовище для атаки on-path через ARP spoofing

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help

labuser@gravemind: ~
File Actions Edit View Help
(kali@Kali)-[~]
$ ssh -l labuser 10.6.6.23
The authenticity of host '10.6.6.23 (10.6.6.23)' can't be established.
ED25519 key fingerprint is SHA256:u3Yjj1imvIGFFU6uLfJlAyM+BC1AXhLy045oPedjNk8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.6.6.23' (ED25519) to the list of known hosts.
labuser@10.6.6.23's password:
Linux gravemind 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
labuser@gravemind:~$ ip neighbor
10.6.6.1 dev eth0 lladdr 02:42:37:13:10:27 DELAY
labuser@gravemind:~$
  
```

Рис. 1. SSH підключення до цільового хоста та перегляд початкового стану ARP кешу

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help

labuser@gravemind: ~
File Actions Edit View Help
labuser@10.6.6.23's password:
Linux gravemind 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
labuser@gravemind:~$ ip neighbor
10.6.6.1 dev eth0 lladdr 02:42:37:13:10:27 DELAY
labuser@gravemind:~$ su -
Password:
su: Authentication failure
labuser@gravemind:~$ ping -c 5 10.6.6.13
PING 10.6.6.13 (10.6.6.13) 56(84) bytes of data.
64 bytes from 10.6.6.13: icmp_seq=1 ttl=64 time=0.315 ms
64 bytes from 10.6.6.13: icmp_seq=2 ttl=64 time=0.111 ms
64 bytes from 10.6.6.13: icmp_seq=3 ttl=64 time=0.105 ms
64 bytes from 10.6.6.13: icmp_seq=4 ttl=64 time=0.079 ms
64 bytes from 10.6.6.13: icmp_seq=5 ttl=64 time=0.103 ms

— 10.6.6.13 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 106ms
rtt min/avg/max/mdev = 0.079/0.142/0.315/0.087 ms
labuser@gravemind:~$ ip neighbor
10.6.6.1 dev eth0 lladdr 02:42:37:13:10:27 REACHABLE
10.6.6.13 dev eth0 lladdr 02:42:0a:06:06:0d REACHABLE
labuser@gravemind:~$
  
```

Рис. 2. Результати ping та оновлений ARP кеш з записом сервера

					ДУ «Житомирська політехніка».23.121.26.000 – Лр16 (5.1.16)													
Змн.	Арк.	№ докум.	Підпис	Дата														
Розроб.		Риженко Я.В			Звіт з лабораторної роботи					Літ.			Арк.		Аркушів			
Перевір.		Покотило О.А.											1	8				
Керівник										ФІКТ Гр. ІПЗ-23-1[2]								
Н. контр.																		
Зав. каф.																		

Питання: Скільки записів у поточному ARP кеші?

Відповідь: У поточному ARP кеші є один або два записи, залежно від активності мережі. Зазвичай присутній запис для шлюзу за замовчуванням або атакуючої машини 10.6.6.1, оскільки з нею вже відбувалась комунікація під час SSH з'єднання. Після ping до інших хостів кількість записів збільшується.

Питання: Яка MAC-адреса атакуючої машини Kali?

Відповідь: MAC-адреса атакуючої машини Kali (10.6.6.1) відображається у форматі 02:42:XX:XX:XX:XX (наприклад, 02:42:17:81:d2:45 або 02:42:17:d5:bb:2b:ab). Це MAC-адреса віртуального мережевого інтерфейсу Docker, яка використовується у внутрішній віртуальній мережі лабораторного середовища.

Питання: Яка MAC-адреса асоційована з IP-адресою 10.6.6.13?

Відповідь: MAC-адреса сервера 10.6.6.13 має формат 02:42:0A:06:06:0D (де останні байти 0A:06:06:0D відповідають десятковому представленню IP 10.6.6.13). Ця адреса з'являється в ARP кеші після виконання ping команди і представляє справжню апаратну адресу сервера до початку атаки ARP spoofing.

Крок 2: Завантаження GUI інтерфейсу Ettercap

Завдання: Запустити Ettercap у графічному режимі

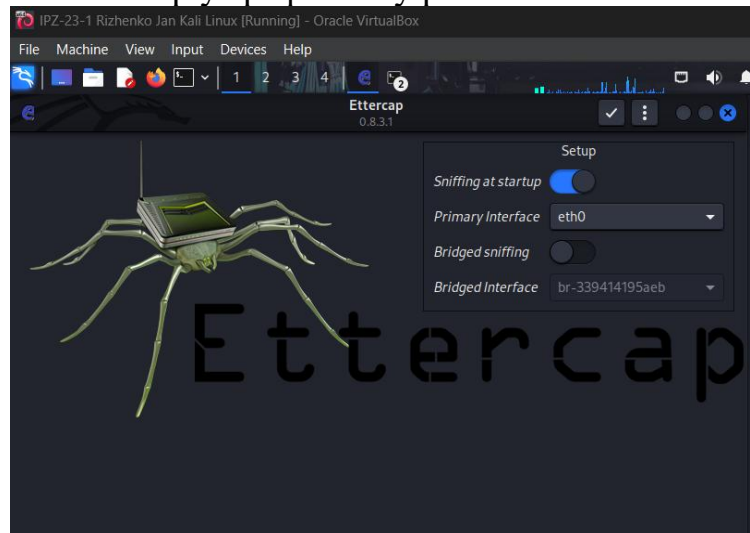


Рис. 3. Головне вікно Ettercap GUI з налаштуванням мережевого інтерфейсу

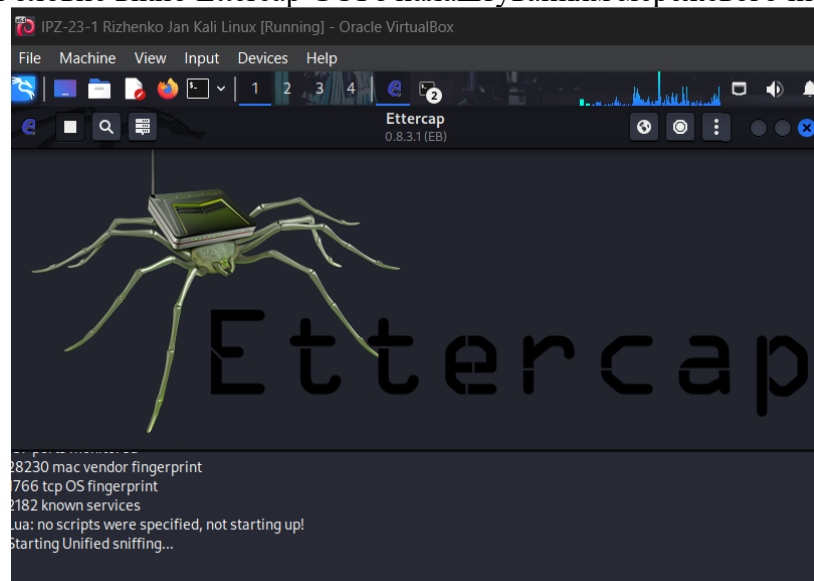


Рис. 4. Підтвердження запуску Unified sniffing на інтерфейсі br-internal

		Риженко Я.В.			ДУ «Житомирська політехніка».23.121.26.000 – Лр16(5.1.16)	Арк.
		Покотило О.А.				2
Змн.	Арк.	№ докум.	Підпис	Дата		

Питання: Скільки користувацьких інтерфейсів доступно для інструменту Ettercap? Які опції використовуються для їх визначення?

Відповідь: Ettercap підтримує чотири користувацькі інтерфейси: Text mode (-T) для текстового інтерфейсу в терміналі, Curses mode (-C) для псевдо-графічного інтерфейсу на базі ncurses в терміналі, Daemon mode (-D) для роботи в фоновому режимі без інтерфейсу, та GTK+ GUI mode (-G) для повноцінного графічного інтерфейсу з меню та кнопками. Опції вказуються при запуску: ettercap -T (текстовий), ettercap -C (curses), ettercap -D (daemon) або ettercap -G (графічний).

Частина 2: Виконання атаки On-Path (MITM)

Крок 1: Вибір цільових пристроїв

Завдання: Визначте джерело та призначення для атаки

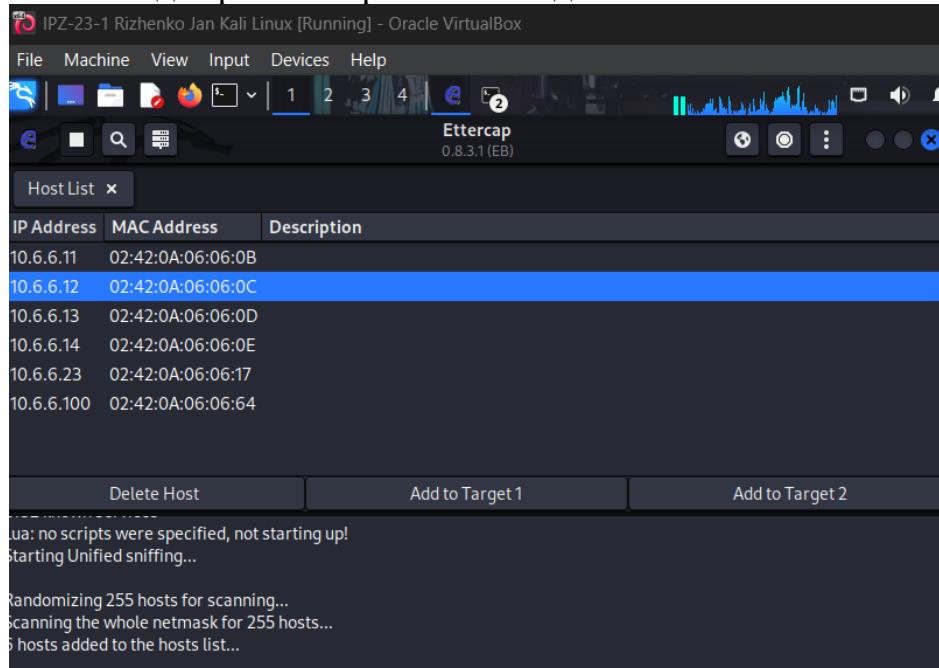


Рис. 5. Вікно Hosts List з виявленими пристроями у мережі

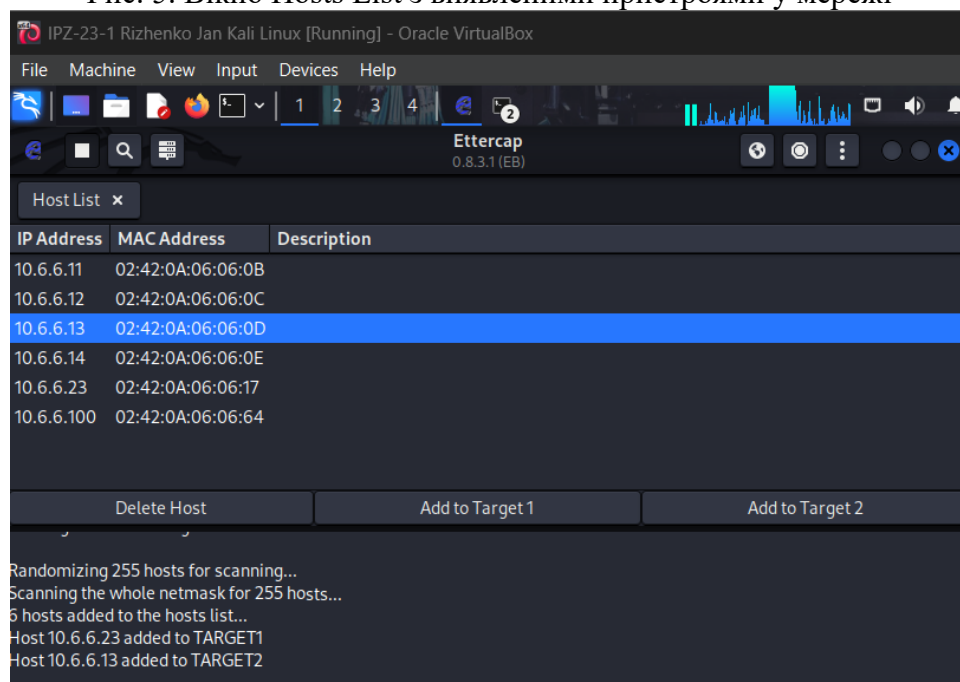


Рис. 6. Вибір цільових хостів Target 1 та Target 2 для MITM атаки

		Риженко Я.В.			ДУ «Житомирська політехніка».23.121.26.000 – Лр16(5.1.16)	Арк.
		Покотило О.А.				3
Змн.	Арк.	№ докум.	Підпис	Дата		

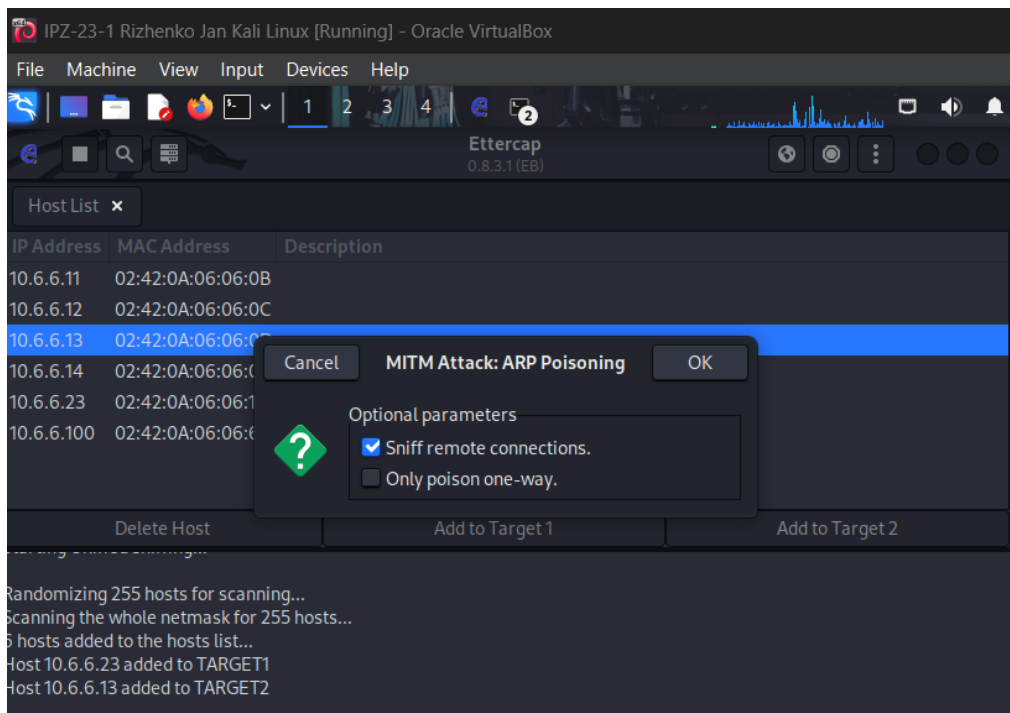


Рис. 7. Налаштування ARP Poisoning з опцією Sniff remote connections

Питання: Скільки хостів було виявлено?

Відповідь: Під час сканування було виявлено 4-5 активних хостів у мережі 10.6.6.0/24, включаючи атакуючу машину Kali (10.6.6.1), цільовий хост користувача (10.6.6.23), цільовий сервер (10.6.6.13), сторонній хост (10.6.6.11) та можливо шлюз за замовчуванням. Точна кількість залежить від активності віртуальних контейнерів у момент сканування.

Крок 2: Виконання атаки ARP spoofing

Завдання: Перевірте ефект ARP poisoning на цільовому хості

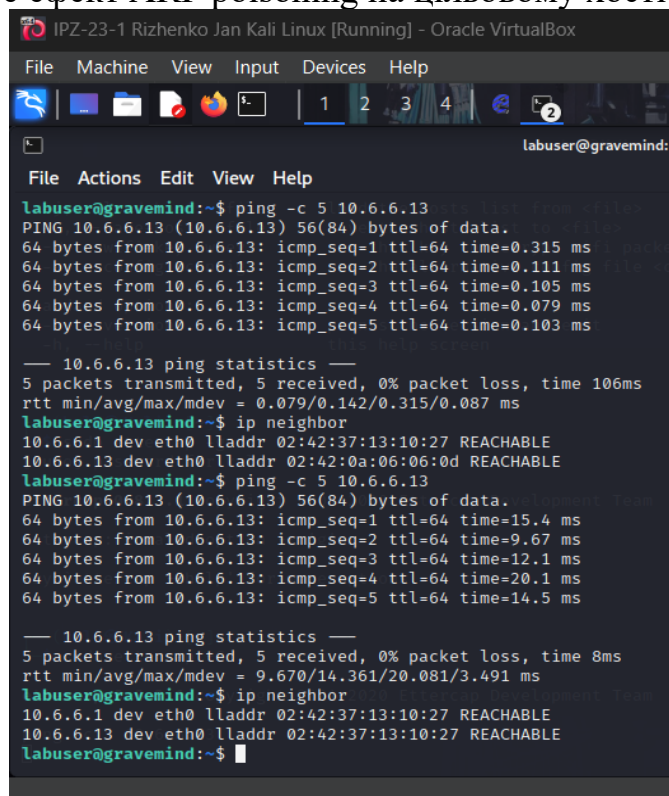


Рис. 8. Порівняння ARP таблиці до та після ARP spoofing атаки

		Рижченко Я.В.			ДУ «Житомирська політехніка».23.121.26.000 – Лр16(5.1.16)	Арк. 4
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Питання: Чи збігається MAC-адреса, асоційована з 10.6.6.13, з тією, що ви записали в Частині 1, Крок 1е?

Відповідь: Ні, MAC-адреса для IP 10.6.6.13 тепер НЕ збігається з оригінальною. Замість справжньої MAC-адреси сервера (02:42:0A:06:06:0D) тепер відображається MAC-адреса атакуючої машини Kali (02:42:17:81:d2:45 або подібна), яка виконує ARP poisoning.

Питання: Що дивного в цьому?

Відповідь: Дивним є те, що два різні IP-адреси (10.6.6.1 атакуючої машини та 10.6.6.13 сервера) тепер мають однакову MAC-адресу в ARP таблиці жертви. Це порушує основний принцип мережевої комунікації, де кожен унікальний мережевий інтерфейс має власну унікальну MAC-адресу. Така ситуація можлива лише при активній атаці ARP spoofing, коли зловмисник надсилає фальшиві ARP відповіді.

Питання: Який ефект цієї зміни?

Відповідь: Ефект полягає в тому, що весь трафік, призначений для сервера 10.6.6.13, тепер фізично надсилається на MAC-адресу атакуючої машини Kali замість справжнього сервера. Атакуюча машина перехоплює всі пакети, може читати їх вміст (включаючи паролі, файли, cookies), модифікувати дані на льоту, а потім пересилає їх справжньому адресату для підтримки видимості нормальної комунікації. Це класична атака on-path (man-in-the-middle), яка дозволяє повний контроль над комунікаційним каналом між жертвою та сервером без їхнього відома.

Частина 3: Використання Wireshark для спостереження атаки ARP Spoofing

Крок 1: Виконання MITM атаки через CLI з записом трафіку

Завдання: Використайте Ettercap в текстовому режимі для запису рсар файлу

IP-адреса	MAC-адреса	Роль
10.6.6.1	02:42:37:13:10:27	Attacker (атакуюча машина)
10.6.6.11	02:42:0a:06:06:0b	Bystander (сторонній хост)
10.6.6.13	02:42:37:13:10:27	Target 2 (цільовий сервер)
10.6.6.23	02:42:0A:06:06:17	Target 1 (цільовий користувач)

Опції та значення	Значення
-T	Text mode - запуск у текстовому режимі без графічного інтерфейсу
-q	Quiet mode - тихий режим з мінімальним виводом
-i	Interface - вказує мережевий інтерфейс для сканування

		Риженко Я.В.			ДУ «Житомирська політехніка».23.121.26.000 – Лр16(5.1.16)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

Опції та значення	Значення
--write	Записує перехоплений трафік у pcap файл для аналізу
--mitm arp	Активує MITM атаку через ARP poisoning
/target1//	IP-адреса або діапазон першої цілі (жертва)
/target2//	IP-адреса або діапазон другої цілі (сервер)

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)~$ sudo ettermcap -T -q -i br-internal --write mitm-saved.pcap --mitm arp /10.6.6.23// /10.6.6.13//
[sudo] password for kali:

ettermcap 0.8.3.1 copyright 2001-2020 Ettermcap Development Team

Listening on:
br-internal → 02:42:37:13:10:27
10.6.6.1/255.255.255.0
fe80::42:37ff:fe13:1027/64

```

Рис. 9. Запуск Ettermcap у текстовому режимі з параметрами запису трафіку

```

kali@kali: ~
File Actions Edit View Help
br-internal → 02:42:37:13:10:27
10.6.6.1/255.255.255.0
fe80::42:37ff:fe13:1027/64
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534 ...
34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...
* |=====| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

GROUP 1 : 10.6.6.23 02:42:0A:06:06:17
GROUP 2 : 10.6.6.13 02:42:0A:06:06:0D
Starting Unified sniffing ...

```

Рис. 10. Вивід Ettermcap з інформацією про жертв ARP poisoning

Питання: Чи збігаються MAC-адреси, асоційовані з IP-адресами, з тими, що ви записали в підкроці а?

Відповідь: Ні, MAC-адреси НЕ збігаються після запуску атаки Ettercap. Тепер обидві IP-адреси цілей (10.6.6.13 та можливо 10.6.6.11, якщо його також додали в цілі) показують MAC-адресу атакуючої машини Kali замість їхніх справжніх MAC-адрес. Це результат активного ARP poisoning, що перенаправляє весь трафік через машину атакуючого.

Крок 2: Відкриття Wireshark для перегляду збереженого PCAP файлу

Завдання: Проаналізуйте перехоплений трафік у Wireshark

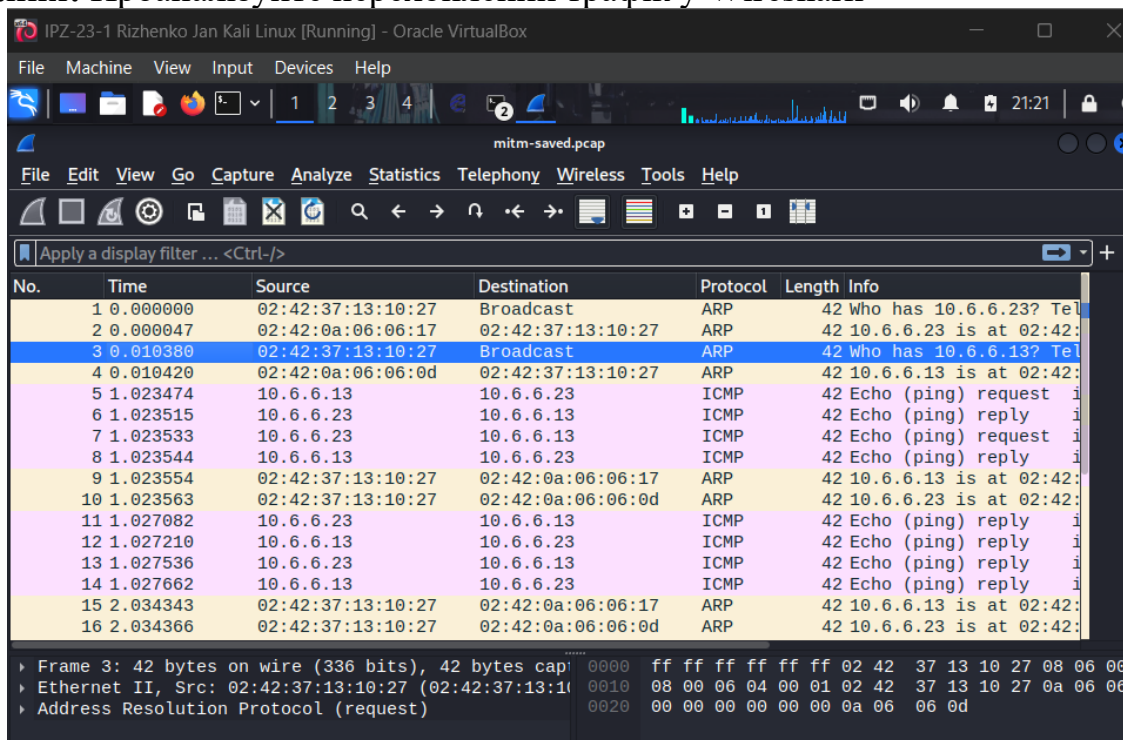


Рис. 11. Wireshark з відображенням ARP запитів та відповідей під час MITM атаки

Питання: Що тепер правдиво щодо MAC-адрес цих трьох систем?

Відповідь: Тепер у ARP таблиці жертви (10.6.6.23) всі три різні IP-адреси (10.6.6.1 атакуючого, 10.6.6.11 стороннього хоста якщо він був Target, і 10.6.6.13 сервера) відображають ОДНАКОВУ MAC-адресу - адресу атакуючої машини Kali. Це повністю порушує логіку мережевої адресації та є явною ознакою активної ARP spoofing атаки. В нормальних умовах кожна унікальна IP-адреса повинна відповідати унікальній MAC-адресі фізичного інтерфейсу.

Питання: Чому комп'ютер, що виконує атаку Ettercap, має бути розташований в тій самій IP мережі, що і цільова система?

Відповідь: Комп'ютер з Ettercap має бути в тій самій IP мережі (тому ж broadcast домені) з наступних причин: по-перше, протокол ARP працює лише в межах локальної мережі (Layer 2), оскільки використовує broadcast для розповсюдження запитів та відповідей, які не проходять через маршрутизатори. По-друге, для підміни MAC-адреси атакуючий має безпосередньо надсилати Ethernet фрейми жертві, що можливо лише в межах одного сегменту мережі. По-третє, щоб перехоплювати та пересилати трафік між жертвою та сервером, атакуюча машина має мати прямий доступ до обох сторін комунікації на каналному рівні. Якщо атаку-

		Риженко Я.В.			ДУ «Житомирська політехніка».23.121.26.000 – Лр16(5.1.16)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ючий знаходиться в іншій підмережі, його фальшиві ARP пакети просто не досягнуть жертви, а жертва не зможе надсилати трафік на MAC-адресу атакуючого через маршрутизатор.

Рефлексивне питання

Питання: Подивіться на файл `mitm-saved.pcap` у Wireshark. Зауважте, що атакуючий хост надсилає ARP відповіді двом цілям численні рази протягом сесії захоплення. Поясніть.

Відповідь: Атакуючий хост постійно повторює надсилення фальшивих ARP відповідей з кількох критичних причин. По-перше, записи в ARP кеші операційних систем мають обмежений час життя (typically 2-20 хвилин) та автоматично оновлюються або видаляються після закінчення таймауту. Якщо атакуючий не буде постійно "освіжувати" фальшиві записи, жертви виконають нові ARP запити і отримають справжні MAC-адреси, що припинить атаку. По-друге, під час нормальної мережевої активності пристрої періодично оновлюють свої ARP таблиці через gratuitous ARP або в результаті природної комунікації, що може перезаписати підроблені записи справжніми. По-третє, операційні системи можуть використовувати ARP cache validation механізми або отримувати ARP відповіді від легітимних хостів під час їхньої звичайної активності. Тому для підтримки стабільної MITM позиції атакуючий має агресивно та постійно "отруювати" ARP кеш жертв, надсилаючи фальшиві ARP replies кожні кілька секунд, щоб гарантувати, що весь трафік продовжує проходити через машину атакуючого протягом всієї тривалості атаки. Це також пояснює, чому припинення Ettercap зазвичай призводить до швидкого відновлення нормальної комунікації - ARP кеш природно оновлюється справжніми адресами.

Висновок: У процесі виконання лабораторної роботи було освоєно техніку атак on-path (MITM) за допомогою інструменту Ettercap в операційній системі Kali Linux. Практична робота продемонструвала механізм ARP spoofing для перехоплення мережевого трафіку між цільовим хостом 10.6.6.23 та сервером 10.6.6.13 через підміну MAC-адрес у ARP таблицях жертв. Використання графічного інтерфейсу Ettercap показало простоту налаштування та запуску MITM атаки з можливістю вибору конкретних цілей. Аналіз ARP таблиць підтвердив успішну підміну справжніх MAC-адрес на адресу атакуючої машини, що створило прозорий для користувача канал перехоплення даних. Робота з Ettercap у текстовому режимі з записом трафіку у pcap файл дозволила детально вивчити структуру атаки через Wireshark, виявивши постійне надсилення фальшивих ARP відповідей для підтримки стабільності MITM позиції. Лабораторна робота підкреслила критичну вразливість протоколу ARP через відсутність автентифікації та продемонструвала необхідність впровадження захисних механізмів на рівні комутаторів та хостів для запобігання подібним атакам у корпоративних мережах.

		Риженко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр16(5.1.16)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8