УДК 004.056.5

В.П. Пасько, Ю.О. Халавчук

ТЕСТУВАННЯ РІВНЯ БЕЗПЕКИ ПРОТОКОЛУ IPV6

Анотація: у статті описано створення тестової лабораторії для дослідження рівня безпеки мережевого протоколу IPv6 та запропоновано методи, спрямовані на підвищення рівня безпеки комп'ютерних мереж, що використовують IPv6. Проведено аналіз заходів безпеки та їх реалізації на обладнанні Cisco та Juniper.

Ключові слова: комп'ютерна мережа, рівень безпеки, вразливості, тестування рівня безпеки, протокол ICMPv6, протокол IPv6.

Вступ

Процес впровадження мережевого протоколу нового покоління IPv6 відбувається поступово протягом останніх років (Всесвітній запуск якого відбувся 6 червня 2012 року). Але, темпи розвитку всесвітньої мережі Інтернет, значно вищі, що стимулює прискорення переходу на IPv6.

Одна із перешкод, що необхідно подолати є страх перед невідомим, так як переналаштування обладнання для роботи з новим протоколом може призвести до непередбачуваних наслідків, зокрема при одночасній роботі з IPv4. Окрім цього, для забезпечення надійного розгортання мережевого протоколу IPv6 необхідно акцентувати увагу на проблемах безпеки. При розробці протоколу IPv4 це був далеко не основний критерій, тому він мав багато вразливостей. З огляду на те, що протокол IPv4 використовувався протягом багатьох років, більшість недоліків, що йому притаманні усувались по мірі їх виявлення, і ці практики добре себе зарекомендували. Та, на час впровадження IPv4, мережі були досить невеликі, і це було не так критично, враховуючи масштаби сучасних мереж, подібні помилки можуть призвести до серйозніших наслідків.

Ця робота допоможе відповісти на важливе питання, чи справді в протоколі IPv6 реалізовано рівень безпеки, який відповідає сучасним вимогам? Для цього зібрано наявну на сьогоднішній день інформацію про реалізацію безпеки протоколу IPv6, що спирається на досвід, накопичений через використання IPv4. Загрози та виявлені вразливості протоколу розглядаються на обладнанні Cisco та Juniper. Запропоновані заходи щодо підвищення безпеки перевіряються у тестовій лабораторії.

Постановка задачі

Статистичні дані свідчать, що протокол мережевого рівня IPv6 є не досить розповсюдженим. Лише 14% провайдерів завершили його впровадження у своїх мережах і лише 4% почали пропонувати

 ISSN 1560-8956

IPv6 своїм кінцевим користувачам [1]. На сьогодні безпека протоколу IPv6 є однією з основних проблем, що гальмують його поширення. Оскільки на даний момент цей протокол не використовується в мережах за замовчуванням (відбувається поступовий перехід з IPv4 на IPv6), немає ні найкращих практик та рекомендацій для мережевих адміністраторів, ні будь-яких гарантій, що реалізовані стеки протоколів IPv6 і методи забезпечення безпеки не мають помилок [2]. Це визначає необхідність дослідження його рівня безпеки. Задача полягає в організації тестової лабораторії для дослідження рівня безпеки протоколу IPv6 та реалізації заходів для її підвищення.

Різновиди атак

Розгортання протоколу IPv6 відбувається одночасно із появою нових загроз безпеки кінцевих користувачів та їхніх даних. Загалом, проблеми безпеки пов'язані з протоколом IPv6 можна розділити на дві категорії: ті, що успадковані від його попередника – протоколу IPv4 та нові проблеми, пов'язані із новими можливостями, що були додані до протоколу. Деякі вразливості протоколу не враховані його специфікацією. Такі недоліки неможливо усунути, при цьому не змінюючи сам протокол. Вирішення подібних проблем зазвичай лягає на плечі розробників.

Основні види атак та загрози, які варто розглянути.

- *Розвідка в IPv6 мережі*. Замість широкомовної розсилки протокол IPv6 використовує групові повідомлення (*multicast*). І кожен вузол, що використовує IPv6 стає членом хоча б однієї *multicast* групи, наприклад, FF02::1 (всі вузли локальної мережі). Зловмисник може використовувати дану особливість для пришвидшення фази розвідки.
- *Перевантаження комутаторів.* Максимальна кількість IP-маршрутів та MAC-адрес комутатора або маршрутизатора обмежується максимальним розміром CAM і TCAM пам'яті. Включення маршрутизації IPv6 значно зменшує загальну кількість записів TCAM. Це робить комутатор більш уразливими до (T)CAM виснаження. Як результат, деякі платформи можуть переходити до процесорної обробки пакетів, викликаючи високе завантаження процесора або пересилати трафік через всі порти.
- *Заголовки розширення.* Заголовки розширення розміщуються між заголовком IPv6 та заголовком протоколу вищого рівня та містять у собі додаткову інформацію мережевого рівня. Ці заголовки використовуються для виконання таких функцій, як фрагментація, або для вказання проміжних пристроїв, через які повинен пройти пакет. Це доповнення протоколу може використовуватись зловмисником для проходження через систе-

ми виявлення атак та мережеві екрани, а також для створення так званих "прихованих каналів" для передачі даних у заголовках розширення.

- *Петля в маршрутизації, при використанні IPv6 тунелів.* Тунелювання використовується для передачі даних між островками, де використовується протокол IPv6, через мережу IPv4. Маршрутизатори, що знаходяться на кінцях тунелю працюють із обома протоколами і здійснюють передачу повідомлень, згідно особливостей протоколу тунелювання, що використовується. При використанні автоматичного тунелювання не відбувається перевірка наявності кінцевих точок тунелю. Зловмисник може використовувати це, надсилаючи пакет через вузол, що не є учасником тунелю в даний момент. В результаті, пакет пересилатиметься з тунелю знову, у нативну мережу IPv6. З цієї мережі, пакет направляється назад в точках входу в тунель. Таким чином пакет буде постійно передаватись в і з тунелю [4]. Жертвами такої атаки будуть вузли, що пересилають повідомлення з та в тунель.
- *Атаки пов'язані з роботою ICMPv6.* Протокол ICMPv6 є невід'ємною частиною протоколу IPv6. Він повідомляє про помилки та виконує діагностичні функції такі, як *ping* та *traceroute*, крім того, має базу для розширення та реалізації нових функцій. Процедура NDP - одна із вже реалізованих розширень, що повністю замінює та удосконалює функції протоколу ARP, що працює в мережах з IPv4 [3]. На жаль, і велика частка атак пов'язана саме із цим протоколом.
- *Виявлення однакових адрес.* Даний механізм використовується кінцевими пристроями для того щоб запобігти появі двох однакових адрес всередині мережі. Він може використовуватись зловмисником для організації DoS атаки.
- *Підміна повідомлення Router Advertisement (RA).* У протоколі IPv6 реалізовано функцію автоматичного налаштування кінцевих пристроїв. Коли пристрої кінцевих користувачів надсилають запити на отримання мережевих налаштувань (на відміну від DHCP, запит іде на групову адресу), зловмисник може у відповідь надсилати свої налаштування, цим самим виконуючи DoS або MitM атаку.
- *"Затоплення" RA повідомленнями.*

  Як і у попередньому випадку зловмисник підробляє RA повідомлення (можливо, додає нову інформацію про маршрут), але при цьому надсилає їх у великій кількості. Пристрій жертви перевантажується інформацією, що потребує обробки, вичерпуються ресурси. Тобто, ситуація призводить до відмови в обслуговуванні.

- *Підміна повідомлення Neighbor Advertisement (NA).* Функція, що замінює ARP, який використовується з протоколом IPv4. Зловмисник може видавати себе за "всі станції" в локальній мережі, і тим самим виконуючи DoS або MitM атаку.
- *"Затоплення" повідомленнями Neighbor Solicitation (NS).* Функція, що практично не відрізняється від ARP, який використовується з протоколом IPv4. Зловмисник може згенерувати велику кількість запитів на адресу жертви, тим самим перенавантажити інформацією, що потребує обробки. Ресурси пристрою жертви вичерпуються, що призводить до відмови у обслуговуванні.
- *Атаки пов'язані з роботою DHCPv6.* Окрім автоматичного налаштування в мережі IPv6 також може використовуватись вже знайомий протокол DHCP нової версії. Як не дивно, нова версія має ті ж самі вразливості.
- *Вичерпування простору адрес.* Зловмисник може вичерпати простір вільних адрес на DHCPv6 сервері.
- *Підміна DHCPv6 сервера.* Зловмисник може видати себе за DHCPv6 сервер для здійснення DoS або MitM атаки.

Аналіз атак

Вказані атаки – це не весь список можливих небезпек, що можуть мати місце при використанні нового мережевого протоколу. Жертвами атак можуть бути як кінцеві користувачі, так і проміжне обладнання (маршрутизатори та комутатори).

При виконанні аналізу вразливостей можна виділити кілька категорій і врахувати приналежність однієї одразу до кількох із них. Виділено такі категорії:

- *внутрішні* – проблеми безпеки, що стосуються локальної мережі;
- *зовнішні* – проблеми безпеки, що стосуються глобальної (зовнішньої мережі);
- *DoS* – проблеми безпеки, які можуть призвести до відмови в обслуговуванні;
- *firewall* – проблеми безпеки, пов'язані з мережевим екраном або іншими фільтруючими пристроями;
- *приховані* – проблеми безпеки, які дають можливість створення прихованого каналу зв'язку;
- *розвідка* – проблеми безпеки, пов'язані з виявленням адресної інформації кінцевих пристроїв;
- *MitM* – проблеми безпеки, які можуть бути використані для підключення до каналу передачі даних між його учасниками з метою перехвату, видалення або зміни інформації.

Розгортання тестової лабораторії

Для розгортання тестової лабораторії використовувалось програмне забезпечення на базі Unix-систем, що дозволяє імітувати роботу комп'ютерної мережі з максимальним наближенням до реальної поведінки.

Використаний комплекс, дозволяє змоделювати віртуальну мережу, складовими частинами якої є:

- *маршрутизатори*;
- *комутатори*;
- *персональні комп'ютери (кінцеві користувачі).*

Для віртуалізації проміжного обладнання використано образи операційних системи *cisco IOS* та *juniper junOS*, тобто виконана повна емуляція обладнання. Для запуску віртуальних машин з операційною системою Windows 7, Windows 8 та *Ubuntu* використано утиліту *VMware*. Моделювання атак виконувалось за допомогою утиліти *Scapy*, що дає можливість створення та модифікації мережевих пакетів.

Вибрані топології для проведення тестування зображено на рис. 1 та рис. 2 для моделювання внутрішніх та зовнішніх атак відповідно.

При організації тестової лабораторії, розгортались окремі топології для перевірки обладнання кожного виробника. Приведемо приклад дослідження атак, на основі маніпуляцій із заголовками розширення.

На першому етапі тести виконувались при базовому налаштуванні проміжних пристроїв (без додаткових заходів безпеки). Здійснення атак відбувалось через окремий порт віртуального комутатора, до якого був доступ з комп'ютера , на якому розгорнуто топологію. На рис. 1 та рис. 2 цей комп'ютер зображено як *Attacking host*.

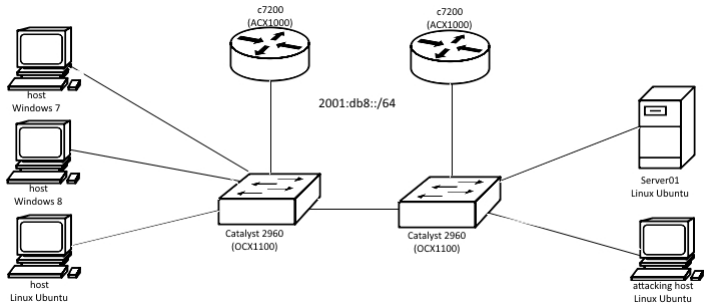

Рис. 1 – Топологія мережі для тестування внутрішніх атак

Спершу розглядалась можливість створення “прихованого каналу” за допомогою опції *PadN*, що знаходиться у заголовку розширення (Hop-by-Hop Extension Header та Destination Extension header).

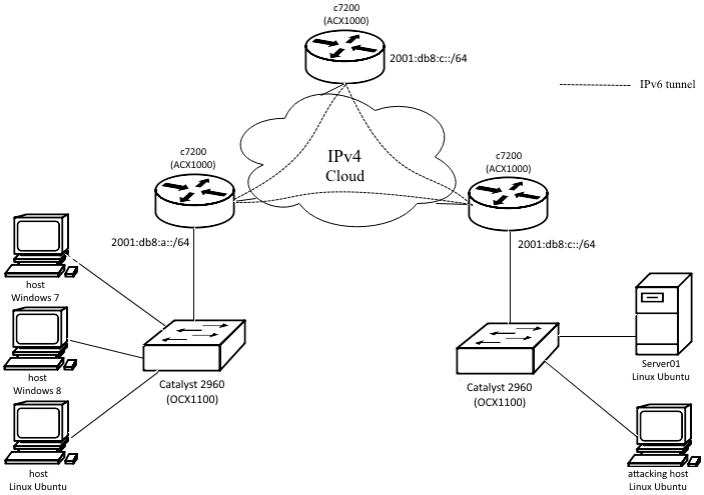

Рис. 2 – Топологія мережі для тестування зовнішніх атак

На пристрої *Attacking host* за допомогою *Scapy* формувалось повідомлення із інформацією прихованою в опціях *PadN* (‘\101’ – код символу ‘A’, ‘\102’ – код символу ‘B’) (рис. 3). На пристрої отримувача працювала програма *Wireshark*, що дала змогу побачити, що сформоване повідомлення прийшло неушкодженим (120 символів ‘A’ та 150 символів ‘B’) (рис. 4).

```
packet = IPv6(src=src_ip, dst=dst_ip) \
/IPv6ExtHdrDestOpt(options=PadN(optdata='\101'*120) \
/PadN(optdata='\102'*150) \
/ICMPv6EchoRequest()
send(CovertChannel)
```

Рис. 3 – Повідомлення із прихованою інформацією в опціях PadN

Таким чином, зловмисник має можливість передавати приховану інформацію. Але більшу небезпеку представляють заголовки розширення, при умові, що на проміжних пристроях використовуються списки доступу. Проходження правил списку доступу не виконується до того, як не буде опрацьовано інформацію заголовку розширення. Як наслідок відбувається завантаження комп’ютера проміжного пристрою. На пристрої *Attacking host* за допомогою

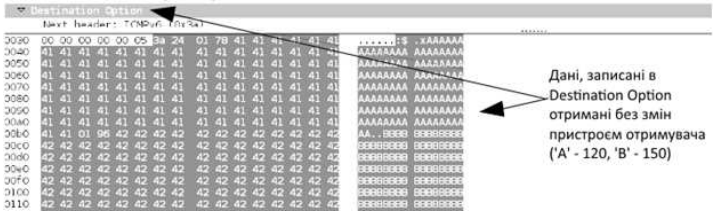

Рис. 4 – Отримане повідомлення із прихованою інформацією на пристрої отримувача

Scapy формувались повідомлення, показане на рис. 5. На рис. 6 та 7 показано завантаження комп'ютера при обробці даного повідомлення.

```
packet = IPv6(src=src_ip, dst=dst_ip) \
/IPv6ExtHdrHbyHOpt(options=PadN(optdata='\101'*10) \
/IPv6ExtHdrDestOpt(options=PadN(optdata='\101'*10) \
/IPv6ExtHdr Routing(addresses=["2001:78::1","2001:20::385"]) \
/ICMPv6EchoRequest()
TCP_SYN=TCP(sport=1500, dport=80, flags="S", seq=100)
TCP_SYNACK=sr1(ip/TCP_SYN)
send(CovertChannel)
```

Рис. 5 – Повідомлення із послідовністю заголовків розширення

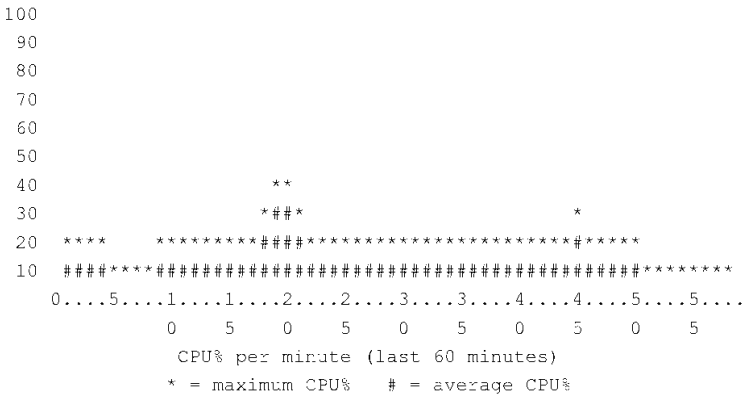

Рис. 6 – Середнє завантаження процесора маршрутизатора cisco

На другому етапі, здійснювався пошук можливих заходів безпеки та перевірка їхньої ефективності. Заходи безпеки застосовувались для проміжних пристроїв. Для боротьби з розглянутими атаками можуть використовуватись списки доступу для фільтрації

```
100
 90
 80
 70
 60
 50
 40                    ***
 30                   *****                          *
 20  *               ************************************
 10  ************************************************************
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
    x-axis => Mins, y-axis => CPU% (CPU usage for last 60 min)
*show the CPU usage for the last 60 minutes
*the top 2 rows vertically display the CPU% of that minute
*the CPU% for the last minute is 7%
```

Рис. 7 – Середнє завантаження процесора маршрутизатора juniper

повідомлень із певним типом заголовків розширення. Але при цьому нефальсифіковані повідомлення, що використовують заголовки розширення, невірно обробляються, або взагалі відкидаються.

Останній етап роботи полягав у порівнянні ефективності заходів безпеки, доступних на використаному обладнанні. Результати представлені у табл. 1.

Висновки

При тестуванні виявлено вразливості операційних систем обладнання проміжних пристроїв та кінцевих користувачів. Усунення виявлених недоліків потребує глибокого знання специфіки роботи того чи іншого обладнання. В табл. 1 відображено виявлені вразливості обладнання та їх засоби попередження атак.

Варто відмітити, що вразливості, пов'язані з роботою ND, притаманні операційним системам кінцевих пристроїв. Unix-подібні системи мають засоби для попередження цих атак, але не всі вони працюють за замовчуванням. Що стосується Windows 7, 8, то деякі недоліки все ще не виправлені їх розробниками.

За результатами моделювання, довгий ланцюжок із заголовків розширення, що використовуються в IPv6 призводять до збільшення завантаження процесора на 9%. При "затопленні" такими повідомленнями можна добитись відмови в обслуговуванні. Засоби для попередження даної атаки не завжди є ефективними.

Утворення петель в маршрутизації можливе для обладнання обох виробників, при використанні автоматичного тунелювання *ISATAP* та 6to4.

Таблиця 1

Наявність засобів попередження атак обладнання cisco та juniper

Атаки	Внутрішні	Зовнішні	DoS	Firewall	Приховані	Розвідка	MitM	Наявність			
								вразливості		засобів попередження	
								cisco	juniper	cisco	juniper
Розвідка в IPv6 мережі	x	x				x		+	+	+	+
Перевантаження комутаторів	x		x	x				+	+	+	+
Заголовки розширення	x		x	x	x			+	+	-	+/-
Петля в маршрутизації, при використанні IPv6 тунелів	x	x	x					+	+	+/-	+/-
Виявлення однакових адрес	x		x	x				+	+	-	-
Підміна повідомлення RA	x		x	x			x	-	-	+	+
«Затоплення» RA повідомленнями	x		x					-	-	+	+
Підміна повідомлення NA	x		x	x			x	-	-	+	+
«Затоплення» повідомленнями NS	x		x					-	-	-	-
Вичерпування простору адрес	x		x					-	-	+	+
Підміна DHCPv6 сервера	x		x				x	-	-	+	+

Заходи з попередження розглянутих атак в тій, чи іншій мірі реалізовано на обладнанні обох виробників. Але деякі атаки залишили без уваги, можливо, з огляду на те, що для них такі заходи повинні бути реалізованими на кінцевих пристроях.

Тестова лабораторія дає можливість в повній мірі виконати моделювання мережі потрібної конфігурації, а у поєднанні із утилітою для створення та редагування мережевих пакетів, дозволяє перевірити поведінку обладнання у разі виникнення мережевих атак різних типів.

Вразливості, виявлені в ході дослідження, перевірено на базі обладнання cisco IOS та juniper junOS. Тестування показано, що якість інструментів по усуненню цих недоліків унеможливлює проведення розглянутих мережевих атак.

Список використаних джерел

1. IPv6 Readiness in the Communication Service Provider Industry. An Incognito Software Report, April 2014, 18 p.
2. Santosh Naidu P1, Amulya Patcha, IPv6: Threats Posed By Multicast Packets, Extension Headers and Their Counter Measures. IOSR Journal of Computer Engineering (IOSR-JCE), Nov. - Dec. 2013, 66-75 p.

3. T. Narten, E. Nordmark, W. Simpson, H. Soliman, Neighbor Discovery for IP version 6 (IPv6). Specification. RFC 4861, September 2007

4. Gabi Nakibly Michael Arov “Routing Loop Attacks using IPv6 Tunnels”- 7 USENIX Association Berkeley, CA, USA, 2009, 7 p.

5. Sander Degen, Arjen Holtzer Testing the security of IPv6 implementations - Nederland’s, March 2014, 42 p.

Отримано 16.04.2015 р.