Анонімізація користувача в мережі інтернет за допомогою WHONIX

УДК 004.738.5

Ростислав Ткачук, Богдан Філіпчук, Богдана Федина

Львівський державний університет безпеки життєдіяльності, rlvtk@ukr.net, bohdanfil2015@gmail.com, fedynabogdana@gmail.com

Зі зростанням рівня розвитку інформаційних технологій, безпека комп'ютерних систем викликає щораз більше занепокоєння. Розвиток інформаційно-комунікаційних технологій та мережі Інтернет характеризується експоненціальним створенням інформаційних баз і реєстрів з персональними даними користувачів та їх численним дублюванням. Вимоги до ідентифікації суб'єктів є скрізь і стрімко зростають. Фактично ідентифікаційні дані стали стратегічним ресурсом будь-якої держави і потребують відповідного фізичного, технічного та правового регулювання, а також обов'язкового захисту. Для уникнення витоку персональних даних потрібно анонімізовуватися (приховувати свою особистість — використовувати псевдоніми та захищені, прозорі мережі) [1, 2, 9].

Анонімні мережі створені для досягнення анонімності в Інтернеті працюють поверх глобальної мережі. Специфіка таких мереж полягає в тому, що розробники змушені йти на компроміс між ступенем захисту та легкістю використання системи, її «прозорістю» для кінцевого користувача. Багаторівневе шифрування та розподілений характер анонімних мереж, усуваючи єдину точку відмови і єдиний вектор атак, дозволяють зробити перехоплення трафіку або навіть злом частини вузлів мережі не фатальною подією [3-5].

Для відкрито розробленого безкоштовного програмного забезпечення з відкритим вихідним кодом (FOSS), ліцензованого GPL гіпервізора, який може запускати Whonix, рекомендується використовувати віртуальну машину ядра (KVM), яка постачається з ОС GNU/Linux. KVM у поєднанні з Virtual Machine Manager має надавати знайомий, інтуїтивно зрозумілий і простий у використанні графічний інтерфейс. Вона використовує libvirt. Тому виконана на персональному комп'ютері зі засобом віртуалізації та гіпервізором QEMU/KVM [7, 8].

Завантаження образів операційних систем Whonix необхідно робити в захищеному середовищі та завжди перевіряти цілісність файлів. Це необхідно для того, щоб система з самого початку була цілісною і Whonix не був скомпроментований. Скачувати бажано через спеціальне дзеркало в мережі Tor. Для цього необхідно порівняти контрольну суму файлу та хеш суму на сайті [6].

Після перевірки файлів встановлюється гіпервізор з депозитаріїв, якщо він не встановлений, тоді добавляємо користувача до груп, щоб встановити політику безпеки.

Далі необхідно відредагувати конфігураційні файли під потреби користувача, а саме прописати шляхи до машин (рис. 1). Цю операцію необхідно зробити для двох файлів налаштувань.

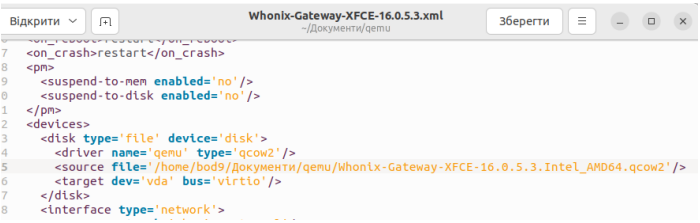

Рис. 1. Конфігураційний файли машини Gateway

Наступним кроком буде добавляння віртуальних мереж, та їх запуск. Також необхідно перевірити, чи утворилися необхідні мости. Після цього добавляємо системи в гіпервізор.

На певних операційних системах необхідно буде виконати додаткові налаштування конфігураційного файлу для коректної роботи систем (рис 2).

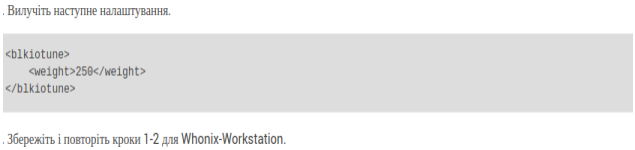

Рис. 2. Зміна конфігурації

Після виконання основних налаштувань (налаштування користувача, політики доступу та зміни паролів), далі налаштовується система під можливості персонального комп'ютера. Після цього можна запускати системи та починати активне їх використання. Дається дозвіл на мережу Tor (без цього дозволу Інтернет не появиться і спосіб не буде працювати). Далі виконуються запити на сайт, їх основна мета це показати IP-адресу (виконується на усіх системах та на персональному комп'ютері).

Після порівняння IP-адреси на системах (Whonix-Workstation [185.14.97.176], Whonix-Gateway [185.241.208.206], Host [93.178.254.150]), практично видно, що схема загортання трафіку в мережу Tor працює відмінно на всіх етапах, тобто анонімізація мережі виконана (рис. 3).

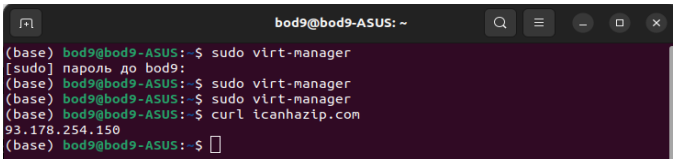

Рис. 3. IP-адрес Host

Таким чином зловмисникам буде дуже складно скомпрометувати систему Whonix-Workstation, тому що сама вона теж загортає трафік в мережу Tor і також шлюз операційної системи Whonix-Gateway теж загортає все в Tor і тому відслідкувати весь шлях інформації надзвичайно складно, отже таким чином ми добилися надійної анонімізації.

У роботі здійснювалося дослідження методу анонімізації за допомогою операційної системи Whonix. У результаті отримано систему, яка забезпечує анонімність власної IP-адреси та DNS (якщо ми його використовуємо), при чому анонімність складається з кількох обгортань в мережу Tor, що дає велику ефективність анонімізації трафіку. Також отримано змогу налаштування дозволів DNS через DNSCrypt та тунелювання UDP, що ще більше покращує анонімність користувача та забезпечує відповідний захист конфіденційних даних та унеможливлює контроль та цензуру свободи слова. Досягнутий результат роботи забезпечує прозоре користування інтернет ресурсами та високий рівень анонімності персонального комп'ютера, що є надійним методом захисту від компрометація локальної комп'ютерної мережі.

1. Anonymity on the Internet Must be Protected Karina Rigby [Електронний ресурс] — Режим доступу до ресурсу: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall95-papers/rigby-anonymity.html
2. Костенко О. В. Проблеми правового регулювання анонімізації та псевдонімізації [Електронний ресурс] — Режим доступу до ресурсу: https://t1p.de/9b21b
3. Анонімна мережа [Електронний ресурс] — Режим доступу до ресурсу: https://www.wiki.uk-ua.nina.az/%D0%90%D0%BD%D0%BE%D0%BD%D1%96%D0%BC%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0.html
4. Анонімність в Інтернеті [Електронний ресурс] — Режим доступу до ресурсу: https://repair.lviv.ua/anonimnist-v-interneti/
5. Філіпчук Б., Ткачук Р.Л., Репетило Т.Б. Потенційні вразливості брандмауера. Зб. тез доп. IV Міжнародної науково-практичної конференції “Інформаційна безпека та інформаційні технології”. (м. Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. С. 111-114.
6. How Does Whonix Make Kali Linux Anonymous & How to Prevent It? [Електронний ресурс] — Режим доступу до ресурсу: https://cybersecurity.att.com/blogs/security-essentials/how-does-whonix-make-kali-linux-anonymous-how-to-prevent-it
7. Whonix [Електронний ресурс] Режим доступу до ресурсу: https://cybersecurity.att.com/blogs/security-essentials/how-does-whonix-make-kali-linux-anonymous-how-to-prevent-it
8. Who uses Whonix ™ [Електронний ресурс] — Режим доступу до ресурсу: https://www.whonix.org/wiki/Users_of_Whonix
9. Мельцов В. В., Ткачук Р. Л. Організація захисту сайту створеного за технологіями: MONGODB, ANGULAR 12, HTML5, CSS3, JAVASCRIPT, NESTJS. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції “Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 84–85.