використанням останніх версій TLS бібліотек. Перевірити на неправильну, або неактуальну конфігурацію веб-серверу можна за допомогою спеціальних аналізаторів, наприклад – ssllabs.com.

Список використаних джерел

1. Anicas M. 5 Common Server Setups For Your Web Application [Електронний ресурс] / Mitchell Anicas – Режим доступу до ресурсу: https://www.digitalocean.com/community/tutorials/5-common-server-setups-for-your-web-application.
2. Banga S. Web Application Architecture: Definition, Models, Types, and More [Електронний ресурс] / Swapnil Banga – Режим доступу до ресурсу: https://hackr.io/blog/web-application-architecture-definition-models-types-and-more.
3. Web Application Architecture: Definition, Models, Types, and More [Електронний ресурс] – Режим доступу до ресурсу https://www.commonplaces.com/blog/6-common-website-security-vulnerabilities/
4. Ellingwood J. How Fail2Ban Works to Protect Services on a Linux Server [Електронний ресурс] / Justin Ellingwood – Режим доступу до ресурсу: https://www.digitalocean.com/community/tutorials/how-fail2ban-works-to-protect-services-on-a-linux-server

---

УДК 004.056.5

ОПТИМІЗАЦІЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ ПЕРЕДАЧІ ТРАФІКУ НА БАЗІ TOR МЕРЕЖІ

Чулінда О. С., студ. гр. КБ-161
Науковий керівник: **Базилевич В. М.,** к.е.н., доцент
Національний університет «Чернігівська політехніка»

На даний момент в мережі анонімність є великою проблемою тому, що дані про відвідини інтернет-ресурсів можна зібрати з локальних пристроїв. Тому зараз все більш користувачів використовую програми для анонімності в мережі. У зв'язку з цим в мережі з'являється більше нових програм VPN, але не всі VPN дійсно надають анонімність. Деякі працюють з різними умовами такими як анонімність лише HTTP трафіку, або данні користувачів попадають в інтернет через неуважність розробників.

Для надання анонімності необхідно щоб трафік системи потрапляв на проміжні вузли для надійного маскування, чим більше вузлів тим краще маскування в мережі. Для цього можна використовувати Tor – це метод анонімного зв'язку, використовуваний для анонімної передачі мережевого трафіку. Повідомлення шифрується і відправляється на декілька вузлів. Кожен маршрутизатор розшифровує один шар повідомлення і передає на наступний маршрутизатор.

За допомогою Tor можна відключити вразливі сервіси, такі як скрипти та Flash. Через мережу Tor сайти не зможуть використовувати історію переглядів для створення таргетованої реклами. Tor забезпечить анонімність для обходу заблокованих сайтів. Але є і мінуси у використанні Tor, мережа Tor працює дуже повільно і не підходить для сервісів які вимагають швидкого підключення. Вихідні вузли можуть бути розкриті. Дані можуть бути вкрадені якщо не використовувати протокол HTTPS. Якщо використовувати Tor браузер, то захищений буде лише трафік браузера. На більшості вузлів Tor заборонено завантажувати торрент.

Tor славиться своїми функціями анонімізації інтернет-трафіку, однак можливості цієї мережі обмежені, а сама вона вразлива перед атаками й витоками даних. Вихідний вузол може створити хто завгодно в тому числі та зловмисник. Tor не використовує наскрізне шифрування, тому при переході на сайти які не використовують HTTPS власник вихідного вузла зможе дізнатися що і куди відправляє користувач. Якщо ви відправляєте через Tor конфіденційні дані або авторизуєтесь на сайті, то власник вихідного вузла отримує доступ до вашої інформації. VPN-сервіси, у свою чергу, використовують наскрізне шифрування, завдяки чому ваші дані на 100% захищені від хакерів і шпигунів.

Більшість VPN пропонують користувачам можливість скористатися функцією екстреного відключення від Мережі, яка закриє Інтернет-підключення, щоб уникнути витоків даних якщо переривається підключення до VPN. У мережі Tor такої проблеми не виникне, але в мережі можуть попастися не довірені вузли, що збирають трафік і данні користувачів які проходять через них. На відміну від VPN, для Tor не придумано такої функції екстреного відключення, яка могла б виявляти небезпечні вузли та закривати підключення до них. У VPN, є свої недоліки, але при використанні VPN ризик стати жертвою зловмисника або зіткнутися з витоком даних менше. Найпотужнішим способом захисту анонімності в мережі буде використання VPN і Tor. Якщо використовувати Tor без VPN то можна дізнатися використовують користувачі Tor чи ні, Але з VPN це не буде видно. Використовуючи підключення Tor і VPN, спершу необхідно під'єднатися до VPN, а потім виходити в Tor. VPN зашифрує ваш трафік, потім відправить його в мережу Tor, завдяки чому провайдер не дізнається, що користувач використовує Tor. Підключення VPN і Tor працює в напрямку, протилежному підключенню Tor і VPN. По перше необхідно під'єднатися до мережі Tor, а потім через неї до VPN. Але цей метод складніший в реалізації з технічної точки зору, тому, що необхідно налаштувати VPN так щоб він працював з Tor. Це забезпечить вихідному вузлу Tor направляти трафік до VPN. Після чого можна забути про ризик, пов’язаний з витоком даних через вихідні вузли, оскільки трафік користувача буде розшифрований після виходу з мережі Tor. Але провайдер буде знати що користувач використовує Tor, але не буде знати що використовує VPN.

VPN також має свої мінуси в порівнянні з Tor, зазвичай VPN платний і працює за підпискою на певний період. Tor являється безкоштовним для всіх користувачів.

Таблиця порівнянь Tor та VPN.

	VPN	Tor
Ціна	Поширюється через підписку на сервіс на певний період	Безкоштовний
Анонімність	Надає анонімність	Надає анонімність але можна виявити факт використання Tor
Шифрування	Наскрізне шифрування	Тільки на вихідному вузлі
Швидкість	Висока	Низька
Сумісність з пристроями	Може бути встановленим на всіх платформах а також на маршрутизаторах	Windows, MacOS, Linux, Android.
Інші можливості	Деякі VPN пропонують функцію відключення від мережі в разі від'єднання від VPN	Є можливість використати з proxy

VPN і Tor - це потужні інструменти захисту даних і анонімності в інтернеті.

Можна використовувати VPN або Tor для того, щоб безпечно підключатися з будь-якої точки світу і бути впевненим що данні або анонімність буде збережена. Але якщо об’єднати VPN і Tor, то можна захистити данні ще більш надійним шляхом.

Якщо необхідно захистити історію переглядів або банківські дані під час роботи в мережі, краще використовувати VPN через Tor.

Список використаних джерел

1. Грайворонський М. В., Новіков О. М. Г14 Безпека інформаційно-комунікаційних систем. – К.: Видавнича група ВНУ, 2009. – 608 с.

2. Attacking Tor: How the NSA Targets Users' Online Anonymity [Електронний ресурс] – Режим доступу до ресурсу: https://www.schneier.com/essays/archives/2013/10/attacking_tor_how_th.html.

3.Особливості застосування технології VPN [Електронний ресурс] – Режим доступу до ресурсу: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5123/1/AUConferenceCyberSecurity_November2016_p74.pdf.

4. Cells Breaks the Tor’s Anonymity: Onion Router [Електронний ресурс] – Режим доступу до ресурсу: https://www.ukessays.com/essays/computer-science/cells-breaks-tors-anonymity-onion-6798.php.

5.Tor и VPN [Електронний ресурс] – Режим доступу до ресурсу: https://rus.privateinternetaccess.com/pages/tor-vpn-proxy.

6.Офіційний сайт Tor [Електронний ресурс] – Режим доступу до ресурсу: https://www.torproject.org/about/reports/.

7.Tor: Pluggable Transports [Електронний ресурс] – Режим доступу до ресурсу: https://2019.www.torproject.org/docs/pluggable-transports.

8. Бертсекас Д., Галлагер Р. Сети передачи данных: Пер. с англ.- М.: Мир, 1989.- 544 с.

9.Анонимный браузер TOR - что это такое? [Електронний ресурс] – Режим доступу до ресурсу: http://procomputer.su/program-obespechenie/118-anonimnyj-brauzer-tor-chto-eto-takoe.

10. Анонимность в сети с помощью Tor Browser [Електронний ресурс] – Режим доступу до ресурсу: https://safe.roskomsvobodaorg/tor/.

УДК: 004.056.53

ДО ПИТАННЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Марченко В. С., студ. гр. КБ-161, **Ткач Ю. М.,** д.пед.н., доц.
Національний університет «Чернігівська політехніка»

Кожен день збільшується кількість організацій і підприємствах котрі використовують для своєї роботи інформацію котру потрібно захищати. Дуже велику роль грає технічний захист даної інформації від зловмисників, але ще впливає на захист людський фактор, а саме знання працівників у сфері захисту інформації.

Від витоку інформації колами електроживлення я порекомендую використати фільтри ЕМСБІ типу ФЗП103-2 котрі надійно захищають в широкому у межах частот – починаючи зі звукових (10 кГц) до надвисоких (1000 МГц) або Засіб активної оборони автоматизованих систем «DELTA-7» котрий створює захисні перешкоди у межах частот від 9 кГц до 3,3ГГц, підлаштованні до частотного розподілу приладів.

Пристрій «KVS-3000» призначений для створення електромагнітних завад в смузі частот від 9 кГц до 2 ГГц з метою захисту інформації від витоку каналами побічних електромагнітних випромінювань і наведень в інформаційно-телекомунікаційних системах та на об'єктах електронно-обчислювальної техніки. За своїх технічних характеристик він дозволяє створювати захист інформації від її витоку по лініях електроживлення і заземлення.

Трансформатор розділовий з екранованої обмоткою потужністю 10 кВт "PIAC-4TP / 10" його призначення для гальванічної розв'язки і технічного захисту інформації в однофазних і двофазних ланках мережі електроживлення напругою яка становить до 250 В, частотою 50 Гц від її витоку через канал, який створюється за рахунок акустично-електричних перетворень і паразитних модуляцій мовних сигналів високочастотного сигналу "накачування", створюваного засобами технічної розвідки.

Для захисту від витоку інформації акустичним і віброакустичним каналом я порекомендую використати генератор "Топаз ГША-4" спільно з вібро-акустичним випромінювачем "Топаз ВІ-1" котрий забезпечує захист за допомогою маскування можливої інформації, при реалізації методу енергетичного приховування акустичного і вібро-акустичного небезпечного сигналу, що виникає під впливом мови на повітря і навколишні конструкції приміщення. Або БАЗАЛЬТ-4ДА, котрий активно захищає мовну інформацію від витоку акустичним і віброакустичним каналом.

Для захисту мережевих даних я використав би Фаєрвол Fortinet FG-300D- це пристрій мережевої безпеки котрий пропонує комплексну мережевий захист на одній платформі, з однієї операційної системи мережевої безпеки і з єдиною системою управління в одному вікні на основі заданих правил, що забезпечує максимальний захист підприємств від цільових атак і безперервно удосконалюються загроз для безпеки. Він дуже потужний і за це він може забезпечувати комплексний мережевий захист для середніх компаній, філій і відділень. В