УДК 004.891

К.В. Заїчко,
начальник відділу ДНДІ МВС України, м. Київ
Д.С. Назарок,
старший науковий співробітник ДНДІ МВС України, м. Київ

СТІЙКІСТЬ МІЖМЕРЕЖНИХ ЕКРАНІВ (ДЕЯКІ АСПЕКТИ)

У статті розглянуто основні поняття брандмауерів, приділено увагу пакетним фільтрам та протоколам підтримки, наведено приклади окремих сервісів та можливих недоліків роботи. Зосереджено увагу на основних функціях брандмауерів та описано особливості захисту. Приведено приклад моделі вірогідної атаки, розглянуто можливість віддаленого керування та процес відслідковування маршруту у випадку виявлення брандмауера. Вивчені окремі утиліти для проведення процедур сканування та трасування.

Ключові слова: *брандмауер, функції, стійкість.*

В статье рассмотрены основные понятия брандмауэров, уделено внимание пакетным фильтрам и протоколам поддержки. Приведены примеры отдельных сервисов и возможных недостатков в их работе. В материале статьи сосредоточено внимание на основных функциях работы брандмауэров, описано особенности защиты от вероятного влияния атак. Приведен пример модели вероятной атаки, рассмотрены возможность дистанционного управления и процесс отслеживания маршрута в случае обнаружения брандмауэра. Изучены отдельные утилиты для проведения процедур сканирования и трассировки.

Ключевые слова: *брандмауэр, функции, стойкость.*

Paper covers the basic concepts of firewalls, packet filters and support protocols. Examples of individual services and possible shortcomings in their work are given. Paper focuses on the main functions of firewalls, describes the features of protection against the likely impact of attacks. An example of a model of a probable attack is given, the possibility of remote control and the route tracking process are considered in the case of detection of a firewall. Separate utilities for scanning and tracing procedures are considered.

Keywords: *firewalls, function, durability.*

Вступ

До головних цілей захисту інформації слід віднести конфіденційність, цілісність та доступність інформації. Поставлені цілі можуть бути досягнуті як організаційними заходами та програмно-апаратними засобами. Стійкість міжмережевих екранів не є простим завданням, оскільки зміна способів загроз є причиною дотримання необхідного рівня стійкості міжмережевих екранів. Проаналізуємо структуру міжмережевих екранів та визначимо найбільш вірогідні вразливі місця.

Стосовно засобів захисту комп'ютерних мереж крім поширеного терміна "брандмауер" і англомовного "firewall" рекомендується використовувати термін "мережний екран" або "міжмережний екран" (МЕ).

Міжмережні екрани, або *брандмауери* призначені для захисту внутрішніх ресурсів мереж шляхом обмеження можливостей обміну між ними.

Комп'ютер, на якому виконується програмне забезпечення міжмережного екрану, або спеціалізований програмно-апаратний пристрій, що реалізує функції МЕ, є шлюзом між двома мережами, найчастіше – між Інтернет і корпоративною мережею.

Брандмауер (*brandmauer*) – німецький еквівалент англійського терміна *firewall*, що означає протипожежну капітальну стіну. Інші переклади, такі як "стіна вогню" чи "вогняна стіна" є не коректними. Вважається, що цей термін увійшов в українську мову з німецької.

До основних загроз можна віднести вторгнення, викрадення, модифікацію та відмову в обслуговуванні. Основним видом захисту крім брандмауеру можуть бути сервіси автентифікації, шифрування даних, перевірки цілісності (електронні цифрові підписи).

Брандмауер є бар'єром, що керує потоками між мережами: між довіреною та недовіреною мережами, а також застосовується між корпоративною (захищеною) мережею і Інтернетом (незахищеною мережею). Вважається, що брежмауер є захистом від "хакерів" у тій частині, що змушує користувачів входити/виходити з мережі лише через добре керовану точку, забезпечує упевненість, що трафік обміну є прийнятним (відповідає політиці безпеки).

У загальному випадку робота брандмауера базується на динамічному виконанні двох груп функцій: фільтрації інформаційних потоків, що проходять крізь нього, та посередництва при реалізації міжмережної взаємодії (проксі-сервер).

Розглянемо основні поняття та переваги брандмауерів

Більшість корпоративних мереж "відгороджено" за периметром налаштованими брандмауерами, що захищають внутрішніх користувачів від впливу зовнішніх факторів. Між тим для досвідчених користувачів навіть якісно та грамотно налаштований брандмауер не є перешкодою.

Брандмауер (він же фаервол) у загальному випадку – це сукупність систем, що забезпечують належний рівень розмежування доступу, який досягається шляхом керування прохідним трафіком за більш чи менш гнучким набором критеріїв (правил поведінки). Тобто брандмауер пропускає лише ту частину трафіку, що дозволена адміністратором та блокує все інше.

На ринку домінують декілька типів брандмауерів – пакетні фільтри, які також називають шлюзами фільтрації пакетів (packet filter gateway) та програмні проксі (application proxy). Прикладом першого типу є Firewall від компанії Check Point, а другого – Microsoft Proxy Server.

Пакетні фільтри є повністю прозорими та продуктивними для користувачів, однак недостатньо надійними. Фактично, це різновид маршрутизаторів, що приймають пакети як із-за меж, так і всередині мережі й вирішують, як з ними вчиняти – пропускати далі або знищити, за необхідності повідомляє відправника про це.

Більшість брандмауерів зазначеного вище типу працюють на IP-рівні, причому повнота підтримки IP-протоколу та якість фільтрації залишають бажати кращого, у зв'язку з цим атакувальник може їх обійти. На домашніх комп'ютерах подібні брандмауери ще мають сенс, але наявність маршрутизатора здорожують

систему, нічого не даючи натомість, оскільки ті ж самі правила фільтрації пакетів можна задати на брандмауері!

Програмні проксі – це звичайні проксі-сервери, які прослуховують задані порти (наприклад, 25, 110, 80) і підтримують взаємодію з наперед зумовленим переліком мережевих сервісів. На відміну від фільтрів, що передають IP-пакети "як є", проксі самостійно збирають TCP-пакети, викушуючи з них дані користувачів та наклеюючи на них новий заголовок, та знову розбирають отриманий пакет на IP, за необхідності здійснюючи трансляцію адрес. Якщо брандмауер не містить помилок, оминути його на мережевому рівні вже не вдасться. До того ж він приховує від атакувальника структуру внутрішньої мережі – ззовні залишається лише брандмауер. А для досягнення найвищої захищеності адміністратор може організувати на брандмауері додаткові процедури авторизації та автентифікації, "накидаючись" на супротивника ще на дальньому кордоні оборони.

Особливості на недоліки брандмауерів

Що стосується недоліків, то програмні проксі обмежують користувачів брандмауер у виборі додатків. Вони працюють набагато повільніше пакетних фільтрів та серйозно знижують продуктивність (особливо швидкісних каналів).

Брандмауери обох типів зазвичай включають у себе урізану версію системи виявлення вторгнення (Intruder Detection System, IDS), що аналізує характери мережевих запитів та виявляє потенційно шкідливі дії – звернення до неіснуючих портів (характерно для сканування), пакети з TTL, рівним одиниці, (характерно для трасування) та ін. Зазначені заходи суттєво ускладняють атаку, відповідно, доводиться діяти дуже обережно, оскільки будь-який невірний крок безпосередньо виявить (атакувальника). Однак інтелектуальність інтегрованих систем розпізнавання достатньо невелика й більшість адміністраторів перекладає зазначене завдання на спеціалізовані пакети, такі як Real Secure від Internet Security System.

Залежно від конфігурації мережі брандмауер може бути встановлений на виділений комп'ютер або може ділити системні ресурси ще з ким-небудь. Персональні брандмауери, широко розповсюджені у світі Windows, у більшості випадків встановлюються безпосередньо на сам комп'ютер, що захищається. Якщо цей пакетний фільтр реалізовано без похибок, відповідно захищеність системи висока та атакувати її складно, як і на виділеному брандмауері. Локальні програмні проксі захищають комп'ютер лише від деяких типів атак (наприклад, блокують засилання вірусів через IE), залишаючи систему повністю відкритою. В UNIX-like-системах пакетний фільтр присутній на початку, а у штатний комплект постачання входить велика кількість різноманітних проксі-серверів, у зв'язку з цим необхідності придбання програмного забезпечення немає.

Основні функції та особливості захисту брандмауеру

Розглянемо від чого захищає та що не робить брандмауер.

Пакетні фільтри у загальному випадку дозволяють закривати усі вхідні/вихідні TCP-порти, що повністю або частково дозволяють блокувати деякі протоколи (наприклад, ICMP), запобігають встановленню з'єднань з даними IP-адресами та ін. Правильно зконфігурована мережа має складатися, не менш як із двох зон: внутрішньої корпоративної мережі (corporative network), огородженої брандмауером та населеної робочими станціями, мережевими, intranet-серверами, серверами баз даних та іншими ресурсами подібного типу, а

також демілітаризованої зони (demilitarized zone, або, скорочено, DMZ), у якій розміщено публічні сервера, доступні з Інтернету. Брандмауер, налаштований на найбільш жорсткий рівень захисту має:

– закривати усі порти, крім тих, що належать публічним мережевим службам (HTTP, FTP, SMTP и т.д.);

– пакети, що надходять на заданий порт, відправляти тільки тим вузлам, на які встановлені відповідні служби (наприклад, якщо WWW-сервер розміщено на вузлі A, а FTP-сервер на вузлі B, то пакет, направлений на 80 порт вузла B, повинен блокуватися брандмауером);

– блокувати вхідні з'єднання із зовнішньої мережі, направлені до корпоративної мережі (правда, у цьому випадку користувачі мережі не мають змогу працювати із зовнішніми FTP-серверами у активному режимі);

блокувати вихідні з'єднання від DMZ-зони, направлені у внутрішню мережу (виключаючи FTP- та DNS-сервера, яким вихідні з'єднання необхідні);

– блокувати вхідні з'єднання із DMZ-зони, направлені у внутрішню мережу (якщо цього не зробити, то атакувальник, що захопив керування одним з публічних серверів, безперешкодно проникне і до корпоративної мережі);

– блокувати вхідні з'єднання до в DMZ-зону зі зовнішньої мережі за службовими протоколами, часто використовуючи для атаки (наприклад, ICMP);

– повне блокування ICMP створює значні проблеми, наприклад, перестає працювати ping та стає неможливим автоматичне визначення (найбільш вдалий для застосування MTU);

– блокувати вхідні/вихідні з'єднання з портами та/або IP-адресами зовнішньої мережі, заданим адміністратором.

Фактично роль брандмауера зводиться до огородження корпоративної мережі від всіляких зацікавлених посягань. Тим не менш, міцність цього огородження тільки уявна. Якщо клієнт корпоративної мережі використовує вразливу версію браузера або електронної пошти клієнта (більша частина програмного забезпечення вразлива), атакувальнику достатньо заманити його на трояновану WEB-сторінку або надіслати йому листа із вірусом усередині, та через короткий час локальна мережа буде уражена. Навіть якщо вихідні з'єднання з корпоративної мережі заборонені, shell-код зможе використати вже встановлене TCP-з'єднання, через що він був закинутий на атакований вузол, передаючи атакувальнику керування віддаленою системою.

Брандмауер може і сам бути об'єктом атаки, бо він, як і будь-яка складна програма, не обходиться без дірок. Дірки у брандмауерах виявляються постійно та далеко не відразу затикаються (особливо якщо брандмауер реалізовано на "апаратному" рівні). Поганий брандмауер не тільки не збільшує, але навіть зменшує захищеність системи (у першу чергу це стосується персональних брандмауерів, популярність яких останнім часом надзвичайно висока).

Виявлення та ідентифікація брандмауера

Передумовою успішної атаки є своєчасне виявлення та ідентифікація брандмауера (або загалом *IDS*, у цьому матеріалі будемо вважати, що вона суміщена з брандмауером).

Більшість брандмауерів відкидають пакети, за винятком TTL (Time To Live – час життя), блокуючи таким чином трасування маршруту і розкриваючи себе. Аналогічним чином поводяться і деякі маршрутизатори, однак, як зазнача-

лось вище, між маршрутизатором та пакетним фільтром відсутня принципова різниця.

Відслідковування маршруту зазвичай здійснюється утилітою traceroute, що підтримує трасування через протоколи ICMP та UDP, причому ICMP блокується набагато частіше. Обравши вузол, наперед захищений брандмауером (наприклад, www.intel.ru), спробуємо прослідкувати до нього маршрут командою tracerou-te −I wwww.intel.ru.

```
$traceroute −I wwww.intel.ru
Трасування маршруту до bouncer.glb.intel.com [198.175.98.50]
з максимальною кількістю стрибків 30:
1 1352 ms 150 ms 150 ms 62.183.0.180
2 140 ms 150 ms 140 ms 62.183.0.220
3 140 ms 140 ms 130 ms 217.106.16.52
4 200 ms 190 ms 191 ms aksai-bbn0-po2-2.rt-comm.ru [217.106.7.25]
5 190 ms 211 ms 210 ms msk-bbn0-po1-3.rt-comm.ru [217.106.7.93]
6 200 ms 190 ms 210 ms spb-bbn0-po8-1.rt-comm.ru [217.106.6.230]
7 190 ms 180 ms 201 ms stockholm-bgw0-po0-3-0-0.rt-comm.ru [217.106.7.30]
8 180 ms 191 ms 190 ms POS4-0.GW7.STK3.ALTER.NET [146.188.68.149]
9 190 ms 191 ms 190 ms 146.188.5.33
10 190 ms 190 ms 200 ms 146.188.11.230
11 311 ms 310 ms 311 ms 146.188.5.197
12 291 ms 310 ms 301 ms so-0-0-0.IL1.DCA6.ALTER.NET [146.188.13.33]
13 381 ms 370 ms 371 ms 152.63.1.137
14 371 ms 450 ms 451 ms 152.63.107.150
15 381 ms 451 ms 450 ms 152.63.107.105
16 370 ms 461 ms 451 ms 152.63.106.33
17 361 ms 380 ms 371 ms 157.130.180.186
18 370 ms 381 ms 441 ms 192.198.138.68
19 * * * Перевищено інтервал очікування для запиту.
20 * * * Перевищено інтервал очікування для запиту.
```

Результат: трасування доходить до вузла 192.198.138.68, а потім помирає, що вказує або на брандмауер, або на недемократичний маршрутизатор. Пізніше розглянемо, як можна пройти крізь нього, а поки що оберемо для трасування інший вузол, наприклад, www.zenon.ru

```
$traceroute −I www.zenon.ru
Трасування маршруту до distributed.zenon.net [195.2.91.103] з максимальною кількістю стрибків 30:
1 2444 ms 1632 ms 1642 ms 62.183.0.180
2 1923 ms 1632 ms 1823 ms 62.183.0.220
3 1632 ms 1603 ms 1852 ms 217.106.16.52
4 1693 ms 1532 ms 1302 ms aksai-bbn0-po2-2.rt-comm.ru [217.106.7.25]
5 1642 ms 1603 ms 1642 ms 217.106.7.93
6 1562 ms 1853 ms 1762 ms msk-bgw1-ge0-3-0-0.rt-comm.ru [217.106.7.194]
7 1462 ms 411 ms 180 ms mow-b1-pos1-2.telia.net [213.248.99.89]
8 170 ms 180 ms 160 ms mow-b2-geth2-0.telia.net [213.248.101.18]
9 160 ms 160 ms 170 ms 213.248.78.178
```

10 160 ms 151 ms 180 ms 62.113.112.67
11 181 ms 160 ms 170 ms css-rus2.zenon.net [195.2.91.103]
Трасування завершено.

На цей раз трасування відбувається нормально. Можна зробити висновок, що навколо брандмауера zenon\'a відсутній? Є певна вірогідність, але для впевненої відповіді необхідна додаткова інформація. Вузол 195.2.91.193 належить мережі класу С (три старших біта IP-адреса рівні 110), та, якщо ця мережа захищена брандмауером, більшість її вузлів мають відгукуватися на ping, що у цьому випадку і відбувається. Сканування виявляє 65 відкритих адрес. Відповідно, або маршрутизатор відсутній, або він безперешкодно пропускає наш ping.

За бажанням можна спробувати просканувати порти, однак, по-перше, наявність відкритих портів ще ні про що не свідчить (можливо, брандмауер блокує лише один порт, але найбільш потрібний, наприклад, захищає RPC з дірками від посягань ззовні), а, по-друге, під час сканування атакувальнику буде важко залишитись непоміченим. З іншого боку, порти сканують всі, хто завгодно, і адміністратори не звертають на це особливої уваги.

Утиліта nmap дозволяє виявляти деякі з брандмауерів, встановлюючи статус порту у "firewalled". Такі події відбувається кожен раз, коли у відповідь на SYN віддалений вузол повертає ICMP-пакет типу 3 з кодом 13 (Admin Prohibited Filter) із діючим IP-адресою брандмауера в заголовку (nmap його не відтворює; тобто це – власний сканер або, використовуючи будь-який сніфер, самостійно проаналізувати пакет, що повертається). Якщо повернеться SYN/ACK – порт, що сканується є відкритим. RST/ACK визначає зачинений або заблокований брандмауером порт. Не усі брандмауери генерують RST/ACK під час спроби підключення до заблокованих портів (Check Point Firewall – генерує), деякі відсилають ICMP-повідомлення, як було показано вище, або нічого не надсилають взагалі.

Більшість брандмауерів підтримує віддалене керування через Інтернет, відчиняючи один або декілька TCP-портів, унікальних для кожного брандмауера. Так, наприклад, Check Point Firewall відкриває 256, 257 та 258 порти, а Microsoft Proxy – 1080. Деяким чином повідомляють своє ім'я та версію програмного продукту при підключенні до них за netcat (або telnet), особливо це відбувається за участі проксі-сервера. Послідовно опитуючи усі вузли, що розміщені поперед хоста, який досліджується на предмет прослуховування характерних для брандмауерів портів, здебільшого можемо не тільки виявити їх присутність, але і визначити IP-адресу. Розуміючи, що порти можуть бути зачинені як на самому брандмауері (однак, не усі брандмауери це дозволяють), так як і у маршрутизаторі, що знаходиться перед (але тоді брандмауером буде неможливо керувати через Інтернет).

Сканування та трасування через брандмауер

Пряме трасування через брандмауер частіше за все стає неможливим (більшість адміністраторів приховують топологію мереж) та атакувальник змушений звертатися до інших заходів.

Утиліта Firewalk – це класичний трассер, що посилає TCP- або UDP-пакети, з урахуванням того що на вузлі, який слідує безпосередньо за брандмауером, їх TTL перетворює на нуль, змушуючи систему генерувати повідомлення

ICMP_TIME_EXCEEDED. Завдяки цьому Firewalk впевнено працює там, де штатні засоби вже не справляються, хоч надійно захищений брандмауер їй, звичайно, не пробити і атакувальнику доводиться використовувати більш просунуті.

Будемо виходити з того, що з кожним IP-пакетом, що відправляється, система збільшує його ID на одиницю (як це частіше за все і відбувається). З іншого боку, згідно зі специфікацією RFC-793, що описує TCP-протокол, будь-який хост, отримавши сторонній пакет, який не належить до встановленого TCP-з'єднанням, має реагувати на нього посиланням RST. Для реалізації атаки знадобиться віддалений вузол, що не обробляє на цей час жодного стороннього трафіка, але генерує передбачувану послідовність ID. Такий вузол називається dump. Виявити німий хост доволі легко – достатньо лише відправити йому серію IP-пакетів та проаналізувати ID, що повертається у заголовках. Запам'ятаємо ID останнього пакета. Потім оберемо жертву та відправимо їй цей SYN-пакет, вказавши у зворотній адресі IP німого вузла. Вузол, який атакують, вважає, що німий хост хоче встановити з ним TCP-з'єднання, відповідь: SYN/ACK. Німий хост спіймав сторонній SYN/ACK, поверне RST, збільшуючи свій лічильник ID на одиницю. Відправивши німому хосту ще один IP-пакет та проаналізувавши ID, що повернувся, є можливість дізнатися, чи надіслав німий хост жертві RST-пакет або ні. Якщо надіслав, це означає, що хост, який атакується, активний та підтверджує встановлення TCP-з'єднання на заданий порт. За бажанням атакувальник може просканувати усі порти, не ризикуючи опинитися замічений, бо вирахувати його за IP важко – сканування здійснюється чужими "руками" німого вузла та, з точки зору атакувальника, виглядає як звичайне SYN-сканування.

Наприклад, німий хост розміщений всередині DMZ, а жертва знаходиться всередині корпоративної мережі. Тоді, відправивши німому хосту SYN-пакет від імені жертви, ми зможемо проникнути через брандмауер, оскільки він буде вважати, що з ним встановлює з'єднання внутрішній хост, а з'єднання цього типу у 99,9 % випадках дозволені (якщо їх заборонити, користувачі корпоративної мережі не зможуть працювати зі своїми власними публічними серверами). Відповідно, усі маршрутизатори на шляху від атакувальника до німого хосту не повинні блокувати пакет із підробленою зворотною адресою, у іншому випадку пакет помирає ще задовго до того, як добирається до місця призначення.

Утиліта hping як раз і реалізує сценарій сканування цього типу, що робить її основною зброєю актувальника для досліджень корпоративних мереж, які огороджені брандмауером.

Як варіант, атакувальник може захопити один із вузлів, розміщених всередині DMZ, використовуючи їх як основу для подальших атак.

Проникнення через брандмауер

Збирання фрагментованих TCP-пакетів підтримують тільки найякісніші з брандмауерів, а інші аналізують лише перший фрагмент, безперешкодно пропускаючи усі інші. Посилаючи сильно фрагментований TCP-пакет, "розмазуючи" TCP-заголовок за декількома IP-пакетам, атакувальник приховує від брандмауера Acknowledgment Number та брандмауер не може відслідковувати приналежність TCP-пакета до відповідної TCP-сесії (можливо, він належить до легального з'єднання, встановленого корпоративному користувачу). Якщо тільки на брандмауері не активована опція "різати фрагментовані пакети", успіх атакувальної

операції гарантовано. Блокувальні фрагментовані пакети створюють багато проблем та заважають нормальній роботі мережі. Теоретично можна блокувати лише пакети з фрагментованим TCP-заголовком, однак далеко не кожен брандмауер підтримує таку гнучку політику налаштування. Атаки зазначеного типу називають Tiny Fragment Attack, вони мають надзвичайно потужну проникаючу властивість і тому є улюбленим способом більшості атакувальників.

Атаки з використанням внутрішньої маршрутизації

Внутрішня маршрутизація (маршрутизація від джерела або source routing) – найменш актуальна, але її варто розглянути. Як відомо, IP-протокол дозволяє долучати до пакету інформацію щодо маршрутизації. Під час відправлення IP-пакета жертві нав'язана атакувальником маршрутизація частіше за все ігнорується, та траєкторія переміщення пакета визначається винятково проміжними маршрутизаторами, але пакети відповіді повертаються за маршрутом, зворотним зазначеному у IP-заголовку, що створює сприятливі умови для його підміни. Більш спрощений варіант атаки обмежується лише однією підміною IP-адреси відправника. Грамотно налаштовані маршрутизатори (та більшість клонів UNIX) блокують пакети з внутрішньою маршрутизацією. Пакети з підробленими IP-адресами становлять дещо більшу проблему, однак якісний брандмауер дозволяє відсіювати і їх.

Таблиці маршрутизації можуть бути динамічно змінені посиланням повідомлення ICMP Redirect, що дозволяє (теоретично) направити трафік атакувальника в обхід брандмауера (ARP-spoofing), проте на цей час подібні системи практично не зустрічаються.

Втеча від брандмауера

Користувачі внутрішньої мережі, що огороджена брандмауером (із жорсткими налаштування), значно обмежені у своїх можливостях. Питання неможливості роботи з FTP-серверами в активному режимі було обговорено раніше. Також можуть бути заборонені деякі протоколи та закриті необхідні порти для атакувальника. У критичних випадках адміністратори ведуть чорні списки IP-адрес, блокуючи доступ до сайтів "непотрібної" тематики.

Політика безпеки брандмауерів у більшості випадків розрахована на захист ззовні. Зсередини проходити оборону брандмауера набагато легше, достатньо лише скористатися будь-яким підходящим прокси-сервером, що знаходиться у зовнішній мережі та ще не занесений адміністратором до чорного списку. Наприклад, популярний клієнт ICQ дозволяє обмінюватися повідомленнями не прямо, а через сервер (не обов'язково сервер компанії-розробника). Існує значна кількість серверів, що підтримують роботу ICQ. Деякі існують у незміненому вигляді впродовж тривалого часу, інші динамічні то з'являються, то зникають. Якщо "старого" ще реально занести у стоп-лист, то слідкувати за серверами-одноденками адміністратор не в змозі.

Також можна скористатися протоколом SSH (Secure Shell), він розроблений для роботи через брандмауер та підтримує шифрування трафіка (на той випадок, якщо брандмауер почне шукати у ньому "заборонені" слова типу "sex", "hack" та ін.). SSH-протокол має можливість працювати за будь-яким доступним портом, наприклад, 80. Тоді, з точки зору брандмауера, все буде виглядати як легальна робота з WEB-сервером. Між тим, SSH є лише фундаментом для інших протоколів, з яких, у першу чергу, відмітимо telnet, що забезпечує взаємодію з

віддаленими терміналами. Сплачуючи невеликі кошти за хостинг будь-якому провайдеру, отримаємо акаунт, що підтримує SSH та дозволяє встановлювати з'єднання з іншими вузлами мережі (безкоштовні хостинги цієї можливості позбавлені, оскільки мають жорсткі обмеження).

Нарешті можна скористатися стільниковою телефонією, прямим модемним підключенням та іншими комунікаційними засобами, що встановлюють з'єднання з провайдером, в обхід брандмауера.

Висновки

Технології побудови брандмауерів не стоять на місці, так само як і фахівці у галузі інформаційної безпеки. З кожним днем атакувальнику стає важче. Проте на заміну закритим "діркам" знаходяться нові.

При використанні брандмауера необхідно дотримуватись набору правил, який має забезпечувати визначеність дій, що застосовуються до кожного пакета. Має існувати "правило за замовчуванням", що застосовується до будь-якого пакета, для якого не знайшлося відповідного йому фільтра.

Від того, яким є правило за замовчуванням, залежить принцип політики безпеки, який реалізує брендмауер. Фактично можливими є два правила за замовчуванням − пропустити або не пропустити пакет. Брендмауер має відфільтровувати всі потенційно небезпечні пакети, а решту пропускати за замовчуванням, при цьому він забезпечує доступність ресурсів мережі та не гарантує достатнього рівня захисту. Може бути пропущеним будь-який пакет з непередбаченими параметрами. Такий підхід вважається хибним. Необхідно відкинути всі пакети, що не відповідають явно заданим фільтрам. Якщо брандмауер дозволяє реалізувати принцип мінімуму повноважень: "заборонено все, що не дозволено явно", то такий підхід можна легко зіпсувати занадто ліберальними правилами, що пропускають пакети. За відсутності "ліберальних" правил потрібен окремий явний дозвіл для кожного сервісу, який має бути доступним у мережі.

У правоохоронній діяльності захист інформації є важливою функцією. Впровадження сучасних систем та методів захисту дозволяє підвищувати стійкість до впливу зовнішніх факторів на телекомунікаційні системи. Регулярне проведення тестування та налаштування брандмауерів дасть змогу підтримувати на належному рівні захист інформації та знизити вірогідність несанкціонованого її витоку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мережевий екран. Вікіпедія. Вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D0%B5%D0%BA%D1%80% D0%B0%D0%BD (дата звернення: 03.01.2018).

2. *Лопатін С.І., Зайчко К.В.* Особливості організації брандмауерів та виявлення слабких місць. Звіт про дослідно-конструкторську роботу "Розробка програмного забезпечення доступу до ПЕОМ, на яких активовані системи захисту від несанкціонованого втручання", шифр "Флеш". Київ, 2017. 79 с.

3. Как проверить пинг и трассировку. HostIQ. URL: https://hostiq.ua/wiki/ping-traceroute/ (дата звернення: 02.01.2018).

4. Безпека з ssh, Linux, Операційні системи, статті. Easycode. URL: http://easy-code.com.ua/2012/08/bezpeka-z-ssh-linux-operacijni-sistemi-statti/ (дата звернення: 02.01.2018).

Отримано 10.01.2018
Рецезент Марченко О.С., к.т.н.