# Утиліти

# NETCAT

# CRYPTCAT

Для успішної роботи - як для тестування інформаційних систем з метою захисту, так і для проведення заходів забезпечення безпеки інформації необхідно визначити якими інструментами для цього користуватися.

Їх можна розділити на чотири частини частини:

- Багатофункціональні засоби,
- Інструменти аудиту систем, які об’єднані в мережі,
- Засоби аудиту мережі і
- Допоміжні засоби виявлення інцидентів в інфраструктурі.

Утиліти, які ми розглянемо сьогодні належать до багатофункціональних засобів - **NETCAT** і **CRYPTCAT.**

Netcat встановлює і підтримує

**TCP** (Transmission Control Protocol) і

**UDP** (User Datagram Protocol) з'єднання,

читає і записує дані по цих з'єднанням до тих пір, поки вони не будуть закриті.

Це основа роботи мережної підсистеми TCP/IP, що дозволяє користувачам взаємодіяти по мережі за допомогою команд або скриптів з мережевими програмами та службами на прикладному рівні.

Програма дає можливість побачити пакети TCP і UDP даних до того, як вони будуть запаковані відповідно до протоколів більш високого рівня, такими як

**FTP** (File Transfer Protocol),

**SMTP** (Simple Mail Transfer Protocol), або

**HTTP** (Hypertext Transfer Protocol).

В NetCat немає графічного інтерфейсу користувача (GUI),
і не виводить дані у вигляді красивого звіту.

Але NetCat працює на базовому рівні - тому вона зручна для використання в багатьох ситуаціях.

NetCat повинна використовуватися в парі з іншими утилітами або програмами при застосуванні певних технічних схем.

Керувати нею з командної стрічки досить незручно.

NetCat можна отримати з багатьох джерел, і кожен з безлічі дистрибутивів *nix містить вже готовий до роботи модуль NetCat

Можна завантажити вихідні тексти цієї програми і відкомпілювати її самостійно.

За умовчанням, NetCat скомпільований з меншою, ніж це б хотілося, кількістю опцій. Завантаживши вихідні тексти і скомпілювавши їх самостійно, ви зможете повністю проконтролювати які можливості NetCat будуть у вашому розпорядженні.

Деякі опції при самостійній компіляції компіляції:

**GAPING_SECURITY_HOLE** ("відкрита дірка безпеки“) - можливість віддаленого запуску деяких команд (напр. jболонки shell)

**TELNET**

# Командна стрічка

**nc** [options] host ports

де host -імя хоста або його IP-адреса для пошуку,

а ports — це або номер порту, або діапазон номерів портів, або декілька номерів портів розділених пропусками.

**-d** Доступна лише у Windows.

Переводить Netcat в режим невидимки. Можна запустити програму в режимі прослухування, не відкриваючи вікно режиму MS-DOS. Це також дозволяє зловмисникам краще маскувати працюючу програму від системних адміністраторів.

**-e** <command>

Якщо Netcat скомпільований з опцією Gaping_security_hole, програма може виконувати команду <command> всякий раз, коли хто - небудь встановлює з'єднання з відкритим портом, до тих пір, поки клієнт NetCat не перенаправить ввід/вивід працюючій програмі.

Використовувати цю опцію досить небезпечно, якщо ви не до кінця уявляєте собі, що ви робите. Це швидкий і простий спосіб відкрити «чорний хід» у вашу систему.

**-i** <seconds>

Інтервал затримки між пересилками порцій даних. Якщо через конвеєр Netcat проходить файл, то програма чекає <seconds> секунд перед тим, як передати наступний рядок, який прийшов на вхід. Якщо ви використовуєте NetCat для управління декількома портами на одному хості, NetCat чекає <second> секунд перед тим, як з'єднається з наступним портом з перерахованих в рядку. Це дає можливість трохи замаскувати передачу даних або атаку системної служби, і це дозволяє замаскувати сканування портів від деяких програмних засобів, що аналізують спроби під’єднання і від системних адміністраторів.

**-g <route-list>**

Ви можете визначити до восьми -g опцій в командному рядку, щоб змусити NetCat передавати трафік через певні IP-адреси, які зазвичай використовуються у випадку, якщо ви підміняєте IP-адресу, з якої поступає ваш трафік (наприклад, для того, щоб спробувати здолати брандмауер або перевірку дозволених для доступу хостів).

-G <hop pointer>

Ця опція дозволяє внести зміни до списку маршрутізації, визначений параметром -g з тим, щоб визначити, до якої з адрес переходити. Оскільки IP-адреса - це чотирьох - байтове число, цим аргументом завжди є число, кратне чотирьом, де 4 означає першу IP-адресу в списку, 8 — другу, і так далі.

**-l**

Ця опція перемикає режим «прослухування» Netcat. Вона використовується спільно з опцією -p, щоб прив'язати Netcat до певного tcp-порту і чекати вхідних з'єднань. Щоб використовувати udp-порт, скористайтеся опцією -u.

**-L**

Доступна лише у windows-версії програми, жорсткіша опція режиму «прослухування», чим -l. Вона вказує програмі на необхідність перезапуску з тими ж параметрами у випадку, якщо з'єднання було закрите. Це дає NetCat можливість відстежувати подальші з'єднання без втручання користувача, кожного разу після завершення первинного з'єднання. Як і у випадку з опцією -i, цю опцію необхідно використовувати спільно з опцією -p.

-n

повідомляє NetCat, що не потрібно здійснювати пошук яких-небудь хостів. Якщо ви використовуєте цю опцію, не слід вказувати жодних імен хостів як аргументи.

-p <port>

Опція дозволяє вам визначити локальний номер порту, який слід використовувати NetCat.

**-r.**

NetCat вибирає локальний і видалений порт випадковим чином. Ця опція корисна у разі, коли NetCcat використовується для здобуття інформації про великий інтервал номерів портів в системі і при цьому представити ситуацію так, щоб це було, в крайньому випадку, схоже на процедуру сканування портів. У випадку, якщо ця можливість використовується спільно з опцією **-i** і з чималим інтервалом, то велика вірогідність, що сканування портів не буде виявлене без уважного вивчення системного журналу адміністратором.

**-s**

визначає вихідну IP-адресу, яку NetCat використовує для установки з'єднання. Ця опція дозволяє зловмисникам виконувати декілька «фокусів»: приховати свою IP-адресу або підроблювати що-небудь ще. Але щоб отримати інформацію, що відправляється на підмінену адресу, їм необхідно використовувати опцію визначення порядка маршрутизації.

**-u**

Опція повідомляє програму про необхідність використовувати udp-протокол замість TCP, працюючи як в режимі прослухування, так і в режимі клієнта.

**-t**

Дає можливість вводити інформацію у відповідь на запрошення ввести login, при використанні TCP-з’єднання через 23 порт (для відкомпільованої з опцією – Telnet)

**-v**

визначає, наскільки детально програма інформує вас про те, що вона робить.

-w <seconds>

визначає проміжок часу, протягом якого NetCat чекає з'єднання.

-z

Якщо ви турбуєтеся лише про те, щоб визначити, який з портів відкритий, вам слід використовувати nmap. Але ця опція повідомляє NetCat про необхідність послати досить даних для пошуку відкритих портів в заданому діапазоні значень.

Є кілька способів, за допомогою яких системний адміністратор може виявити проникнення з використанням NetCcat.

- Використовувати утиліту Windows для пошуку файлів, що містять рядки «listen mode» або «inbound connection». Будь-який зі знайдених виконуваних модулів може виявитися програмою NetCat.
- Перевіряти список активних процесів на предмет пошуку будь-яких незрозуміло навіщо виконуваних файлів cmd.exe. За винятком випадків, коли зловмисник перейменував cmd.exe, ви зможете зловити його на використанні віддаленого виконання команд, оскільки cmd.exe буде виконуватися так, що ви не зможете отримати до нього доступ.
- Використовувати команду **netstat** або **fport**, щоб побачити, які порти використовуються в даний час і які програми їх використовують. Тим не менш, будьте обережні з використанням netstat. Netstat може бути легко замінений його «троянською» версією, спеціально створеною зловмисником для приховування своєї діяльності. Netstat також іноді не повідомляє про прослуховування TCP-сокетів до тих пір, поки хто-небудь не з'єднається з ним.

# Використання NETCAT.

Використавши NetCat або спеціально призначену для сканування портів програму для визначення, які порти в системі відкриті, ви можете отримати більш детальну інформацію про ці порти. Зазвичай це можна зробити, підключившись до порту; служба негайно повідомить вам номер версії, примірник і, можливо, відомості про керуючу операційну систему. У результаті ви отримаєте можливість використовувати NetCat для сканування певного інтервалу портів та отримання відомостей про працюючі служби.

Використовуючи Netcat в автоматичному режимі, ви не зможете вводити команди в командному рядку, оскільки програма не очікує введення інформації від користувача на стандартний ввід. Якщо ви просто запустите на виконання команду 192.168.1.100 20-80, ви не зможете нічого дізнатися, оскільки програма зупиниться на першому ж встановленому з'єднанні (можливо, це буде web-сервер, який прослуховує 80 порт) і потім буде очікувати, коли ви що-небудь зробите. Так що вам знадобиться обчислити, що подавати на вхід всім цим службам, щоб змусити їх повідомити вам про себе щось більше. Як тільки ви це зробите, передавши службі команду QUIT і внісши плутанину, вся інформація посиплеться на вас.

Іноді NetCat використовується як злегка поліпшений Telnet-клієнт. Незважаючи на те, що багато речей, які робляться за допомогою NetCat (начебто спілкування безпосередньо з HTTP-сервером), можна виконувати і за допомогою telnet, у нього є деякі обмеження, яких немає у NetCat. По-перше, telnet не може коректно передавати двійкову інформацію. Деякі такі дані інтерпретуються telnet, як команди. Отже, telnet не може коректно передавати потік даних транспортного рівня.

По-друге, telnet закриває з'єднання, як тільки він зустріне у вхідному потоці символ EOF. NetCat може залишатися відкритим до тих пір, поки з'єднання не буде закрито ззовні, що часто використовується для написання скриптів, які ініціюють з'єднання для очікування великими об'ємами даних, які надсилаються одним рядком.

Проте, ймовірно найнайкращою можливістю NetCat, в порівнянні з telnet, є його можливість взаємодіяти по протоколу UDP.

# Підміна IP-адрес.

Підміна IP-адрес справа проста. Брандмауери, які здійснюють маскування або трансляцію мережевих адрес (NAT), підміняють IP-адреси на постійній основі. Ці пристрої можуть отримувати пакети від внутрішніх IP-адрес, замінювати вихідні IP-адреси в пакетах на свою власну адресу, надсилати їх назовні і скасувати модифікацію, коли отримують дані назад ззовні. Таким чином змінювати зміст вихідних IP-адрес в IP-пакетах досить просто. Що насправді складно, так це мати можливість отримувати відповідь, послану на підмінну IP-адресу.

У NetCat є опція -s, що дозволяє визначити ту IP-адресу, яку потрібно. Хтось має можливість почати сканування портів і використовувати опцію -S, підлаштувавши справу так, ніби сканування веде компанія Microsoft або Федеральне Бюро Розслідувань. Проблема виникає якщо ви насправді хочете отримати відповідь від сканованих портів на реальну IP-адресу. Оскільки досліджуваний хост одержує запити від фірми Microsoft, наприклад, він буде посилати повідомлення про отримання на цю саму IP-адресу Microsoft. IP, звичайно, не має уявлення, про що повідомляє його досліджуваний хост і пошле йому відмову в з'єднанні.

Допомогти зламати машину може також опція, яка визначає порядок маршрутизації. Порядок маршрутизації дозволяє мережевим додаткам визначити маршрут, по якому ви хотіли б досягти кінцевої точки.

# Прихована передача файлів.

Зловмисник може використовувати Netcat для передачі файлів зовні системи, не використовуючи для цього способи, доступні для контролю. У той час як використання FTP або Secure copy (scp) залишає сліди в системному журналі, NetCat - ні. Коли зловмисник з'єднується з цим UDP-портом, то викрадає файл / etc / passwd, не залишаючи ніяких слідів (виключаючи випадок, коли в той же момент системний адміністратор виконає команду ps (статистика виконуваних процесів) або команду netstat).

# Встановлення пасток.

Запустивши примірник Netcat в режимі прослуховування портів, які найбільш часто перевіряються зловмисниками на предмет незахищеності, ви можете ввести зловмисника в оману, переконавши його, що ви робите щось, чого насправді немає. Якщо ви зробите це акуратно, то отримаєте можливість зловити зловмисника.

Ваш скрипт може передати на вихід все, що завгодно. Після завершення з'єднання (за допомогою команди EOF), скрипт повинен бути запущений заново тією ж командою NetCat. Але якщо хтось став надто допитливим, ви можете затопити атакуючого будь-яким сміттям, яким вам тільки буде до душі. Якщо ж ви віддаєте перевагу бути більш терпимим, то можете просто записати IP-адреси, з яких відбувається атака, в файл traplog.txt.

# CRYPTCAT.

Cryptcat - це всього лише співзвуччя, утворене з NetCat з шифруванням (net cat with encryption). Тепер ви можете шифрувати створені конвеєри та проксі. Зловмисники можуть приховувати створюваний NetCat-трафік так, що уважним системним адміністраторам знадобиться щось більше, ніж просто прослуховувати мережу, щоб зрозуміти, що відбувається.

Cryptcat використовує розширену версію протоколу шифрування Twofish. Аргументи командного рядка в нього ті ж, що і у NetCat. Очевидно, не найкраща думка використовувати CryptCat для сканування портів або спроб з'єднання з системними службами, які не використовують той самий метод шифрування. Але при використанні NetCat в режимі прослуховування на одному кінці, і ще одного для спроб з'єднання з ним, CryptCat може запропонувати деякі зручності, пов'язані із забезпеченням безпеки з'єднання.