УДК 004.056
DOI: 10.31673/2409-7292.2022.013437

Маницький В.Є.

REVERSE-SHELL ЯК ІНСТРУМЕНТ ОТРИМАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ

У даній статті проаналізовано способи та наслідки використання такого інструменту як Reverse Shell при атаках на сервери. В чому полягає основна небезпека, як виглядає схема цього підключення від «жертви» до зловмисника та які інструменти використовуються для підготовки атаки. Також надано базові рекомендації щодо захисту і попередження атак з використанням reverse shell, які включають в себе як інженерно-технічні засоби захисту інформації так і роботу з персоналом.

Ключові слова: кібератака, зловмисник, шкідливе програмне забезпечення, скрипт, несанкціонований доступ, shell.

Вступ

В сучасному світі існує безліч різних кібератак, але серед них можна виділити один інструмент який в певних ситуаціях може використати зловмисник без особливих навичок і отримати доступ до як мінімум серверу на який проводилась атака. Мова йде про Reverse-shell. Його важливим аспектом також є людський фактор, адже коли відбувається атака з використанням reverse-shell, ініціалізація підключення відбувається зі сторони «жертви». Саме так, машина на яку проводиться атака сама підключається до сервера зловмисника і дуже часто тут не обійтись без додаткових дій зі сторони адміністратора чи простого користувача «жертви». По ходу цей процес буде описано більш детально.

Після проведення цієї атаки зловмисник може отримати доступ до shell (командного рядка) цільової машини. У випадку отримання доступу з правами суперадміністратора – root в linux-системах, або Administrator у Windows, зловмисник отримує повний контроль над системою з подальшої можливістю виходу у локальну мережу, тощо. Але навіть якщо доступ був отриманий від звичайного користувача, залишається небезпека через неправильну конфігурацію прав доступу, а також зловмисник має можливість спробувати знайти і використати вразливість для підвищення прав доступу. І навіть без цього він отримує зв’язок з локальною мережею жертви, що становить потенційну загрозу іншим машинам у мережі.

Якщо згадати, що для проведення цієї атаки в більшості випадків немає необхідності мати глибокі знання у сфері програмування, кібербезпеки, тощо – стає зрозуміло в чому саме полягає високий рівень небезпеки і чому Reverse-shell потребує особливої уваги.

Основна частина

Reverse Shell (або Reverse TCP, або connect-back, або зворотне підключення) - це схема взаємодії з віддаленим комп'ютером. При її використанні потрібно, щоб атакуючий спочатку запустив на машині сервер, при цьому цільова машина буде грати роль клієнта, який підключається до цього сервера, після чого атакуючий отримує доступ до оболонки цільового комп'ютера. Також для цього цільова машина має запустити скрипт або програму яка і проведе підключення до серверу. Саме тут і грає роль людський фактор. Скачана програма або скрипт невідомого походження може мати в собі payload який і буде в собі містити вказівки для підключення до серверу зловмисника. Та слід враховувати, що не завжди для запуску цього payload потрібна пряма взаємодія зі сторони «жертви». Прикладом може слугувати php-shell – він використовується при атаці через web-сервер. В цьому випадку, якщо сервер вже містив в собі помилки конфігурації, зловмисник сам зможе виконати цей скрипт за допомогою http-запитів.

Якщо підсумувати все сказане вище, одразу стає очевидним навіщо потрібне розуміння як працює Reverse Shell, адже атака може бути направлена на будь-яку машину що має вихід у інтернет і для створення payload може використовуватись будь який тип файлів, від .sh скриптів до .exe файлів для Windows. Також атака несе додаткову загрозу через те, що вона може бути як спрямована на конкретну ціль, так і на будь яку «жертву». Тобто зловмисник може завантажити шкідливий файл у відкритий доступ і просто чекати коли до його серверу

будуть підключатись клієнти-жертви. А далі вже перевіряти, чи має ця машина для нього цінність. У випадку з ПК – зловмисник може отримати доступ до особистих файлів жертви з ціллю шантажу, а при доступу до серверу якоїсь компанії варіантів стає набагато більше. Від спроб отримати доступ до всієї підмережі, до викрадення даних із серверу для перепродажу. Дії на які буде здатний зловмисник, обмежуються тільки його фантазією, адже ще раз наголошую, в більшості випадків він отримує повний доступ до серверу одразу, якщо скрипт для Reverse Shell був запущений від адміністратора, або згодом, при вдалій експлуатації вразливості для підняття рівню доступу.

Аналіз кібератак з використанням Reverse Shell

Так як Reverse Shell підключення може бути використане до будь якої цільової машини в якої є вихід у інтернет необхідно детально розглянути як саме відбувається атака, що для цього використовується, які є різновиди і як захиститися.

Як саме працює підключення типу Reverse Shell

Як згадувалось раніше, підключення спочатку відбувається від «жертви» до серверу зловмисника, це підключення зображене на рисунку 1.

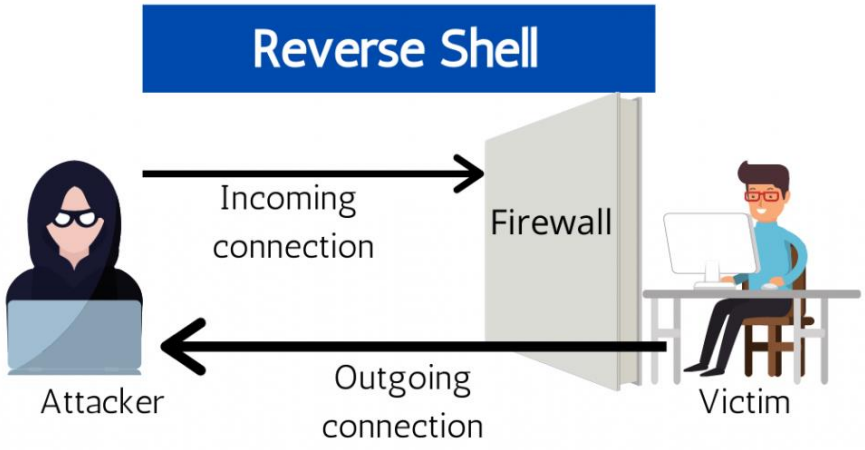

Рис.1. Reverse Shell підключення

То в чому ж його перевага і коли він використовується? Найпоширеніші приклади: сервер має firewall який не дає зловмиснику виконати підключення на потрібний порт, або сервер не має зовнішньої IP-адреси і знаходиться за NAT що не дає змоги виконати пряме підключення до серверу. І от саме тут зловмисник і використає Reverse Shell. Розберемо по пунктам порядок дій за якими відбувається атака:

1) Зловмисник генерує шкідливий код, який містить в собі вказівки для підключення жертви до його серверу
2) Файл з шкідливим кодом надсилається жертві. Тут можуть бути різні варіанти, такі як пошта, або розміщення файлу на «файлообміннику» тощо під видом легітимного файлу, звідки «жертва» сама його скачає.
3) Зловмисник починає «слухати» на своєму сервері вхідні підключення від цільової машини
4) «Жертва» запускає в себе на машині скрипт або програму яка була ласкаво надана зловмисником, цим самим ініціюючи підключення до серверу зловмисника
5) Зі своєї сторони зловмисник бачить, що сесію встановлено і отримує доступ до shell цільової машини.

І firewall дає встановити це підключення, особливо якщо він дивиться тільки ip і port вихідного підключення, не розбираючи трафік який там проходить. Якщо зловмисник відкрив на сервері наприклад 80-порт і у шкідливому коді дав вказівки цільовій машині

підключатись на нього, для firewally це може виглядати неначе жертва просто намагається зайти на звичайний web-сайт.

Тепер варто розглянути які інструменти потрібні для проведення цієї атаки. Всі вони вже встановлені в Kali Linux – це спеціальний дистрибутив, що призначений для тестів на проникнення. Два основні інструменти це – msfconsole та msfvenom, що являються частиною проекту metasploit. Про них по-порядку.

Msfconsole – це головна утиліта metasploit які і містить в собі базу вразливостей та експлойтів до них. У випадку з Reverse Shell вона використовується для вказання параметрів за якими сервер зловмисника буде очікувати підключення від жертви. Друга утиліта – msfvenom, за її допомогою можна автоматично генерувати шкідливий payload який в себе має запустити жертва. Він має досить широкий список типу файлів які можуть бути згенеровані: .efi, .exe, .sh, .war, .jsp, .pl, .py. Як приклад, якщо взяти .sh – shell скрипт для linux. Msfvenom генерує shell рядок який просто можна виконати в консолі Linux і сервер виконає підключення до зловмисника. Це означає, що цей рядок коду можна додати до .sh скрипта який на перший погляд виконує звичайні дії і додати його на сервіс на кшталт Github, під виглядом скрипта який, наприклад, відправляє значення із серверу до вашого власного боту в месенджері, дуже зручно! І скрипт справді це буде робити, але окрім цього, при першому ж запуску він виконає підключення до серверу зловмисника і надасть йому доступ до машини жертви. На рисунку 2 зображено як це виглядає зі сторони зловмисника.

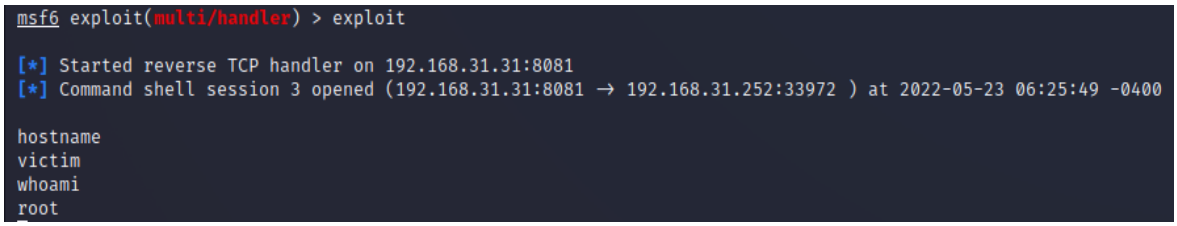

Рис.2. – Зловмисник отримав підключення.

[*] Started reverse TCP handler on 192.168.31.31:8081 – сервер зловмисника починає «слухати» підключення на 192.168.31.31:8081.

[*] Command shell session 3 opened (192.168.31.31:8081 -> 192.168.31.252:33972) at 2022-05-23 06:25:49 -0400 – сповіщення про вдале встановлення підключення до жертви (192.168.31.252)

А далі успішне виконання команд на машині «жертви». Все, зловмисник має повний контроль. Для атаки йому знадобились лише безкоштовний дистрибутив Linux та базові знання metasploit, що дозволили йому за допомогою однієї команди згенерувати шкідливий код. І також зловмисник має мати зовнішню IP-адресу, або налаштований port-forwarding, щоб цільова машина могла виконати підключення до його серверу.

У випадку з Linux-серверам ці атаки часто бувають набагато вдалішими, адже якщо користувач надав скрипту права на запуск, система запустить його без жодних перешкод. Ситуація з Windows-машинами дещо відрізняється, адже навіть стандартні засоби захисту в більшості випадків розпізнають за сигнатурою шкідливий код. В цьому випадку зловмиснику вже знадобляться навички програмування для того, щоб «закодувати» код, аби антивірусу чи іншим засобам захисту було складніше розпізнати в ньому шкідливі для системи наміри.

Також варто згадати про Reverse Shell атаки на web-сервери. Найчастіше це атаки з використанням мови php. Якщо web-сервер має проблеми з параметрами безпеки, зловмисник може завантажити на web-сервер свій шкідливий php-shell і запустити його після цього отримавши доступ до сервера. Для завантаження коду на сервер найчастіше всього використовуються поля для завантаження фото, якщо відсутня перевірка контенту, зловмисник може одразу завантажити .php файл, або спробувати завантажити фото у meta-

даних якого і буде зберігатись шкідливий код. Після того як зловмисник перейде за посиланням, по якому знаходиться завантажений ним файл – код який він вписав до файлу виконається(рис.3).

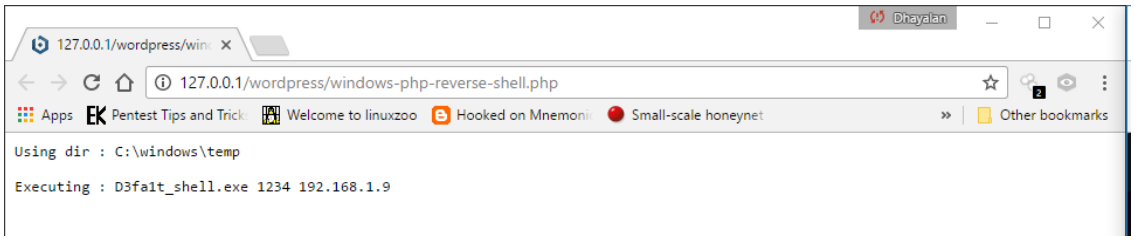

Рис.3. – Запуск php скрипта за допомогою пошукового рядку

Базові рекомендації щодо захисту від Reverse Shell

Спочатку варто згадати про firewall – при правильному налаштуванні ризик успішної атаки зменшується. Важливим пунктом є обмеження доступу, тобто сервер повинен мати вихід лише на ті порти і ip-адреси які необхідні йому для роботи. Всі зайві відкриті доступи – потенційний ризик для проведення атак. Також мають бути присутні системи IPS&IDS які будуть виявляти небажаний трафік та аномалії у мережі. Наступними, не менш важливим пунктами є підготовка персоналу, політики безпеки що забороняють встановлювати не перевірені програми на робочі машини. Ну і звісно використання антивірусу на робочих машинах, для перевірки встановлених програм. Адже в більшості випадків сучасні антивіруси одразу помічають шкідливі програми, що намагаються встановити невідомі підключення.

Щодо web-серверів, додаються рекомендації щодо оновлення компонентів web-додатку та перевірки їх конфігурації. Одним з основних пунктів має бути налаштування перевірки файлів, що завантажуються через web-сторінку. Тобто встановлення конкретних типів розширення файлів які можуть використовуватись, а також стирання meta-даних при завантаженні файлу (у випадках з завантаженням фото). Також заборона запуску будь-яких скриптів без певних прав доступу.

Висновок

Reverse Shell може бути дійсно небезпечним інструментом для атаки на сервери або персональні комп'ютери. Для виконання цієї атаки немає необхідності мати поглиблені знання та навички у сфері кібербезпеки, що робить цю атаку досить поширеною. Також в більшості випадків проведення цієї атаки сильно залежить від людського фактору, і навіть в наш час цьому приділяється замало уваги, що може стати проблемою.

В статті було детально описано як працює підключення типу reverse shell і яку це становить небезпеку, що дає змогу зрозуміти яких заходів варто вжити, основні з них були наведені в рекомендаціях щодо захисту від Reverse Shell.

Перелік посилань

1. What is a Reverse Shell? [Електронний ресурс] – Режим доступу до ресурсу: https://www.techslang.com/definition/what-is-a-reverse-shell/
2. Windows-php-reverse-shell [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/Dhayalanb/windows-php-reverse-shell
3. Metasploit [Електронний ресурс] – Режим доступу до ресурсу: https://docs.rapid7.com/metasploit/
4. Php-reverse-shell [Електронний ресурс] – Режим доступу до ресурсу: https://pentestmonkey.net/tools/web-shells/php-reverse-shell

Надійшла: 06.02.2022 Рецензент: д.т.н., професор Гайдур Г.І.