ПОРІВНЯННЯ МЕТОДІВ ЕНУМЕРАЦІЇ BLOODHOUND У ПОРІВНЯННІ З СТАНДАРТНИМИ МЕТОДАМИ

Снігуров А.В., Яковенко Д.О.

Харківський національний університет радіоелектроніки,
кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Україна.

E-mail: arkadiy.snigurov@nure.ua,
dmytro.iakovenko@nure.ua

Abstract

The report contains analysis of standard enumeration methods of Windows Server Active Directory using PowerShell and comparing its methods with new generation instrument BloodHound. It can help and make it easy to find hidden ways to get access the domain alongside sensitive information that can leads to protentional loses of money or reputation. The main goal is to explain and justify how investigation with this instrument can be better or worse than standard methods.

В реаліях сучасних компаній Windows Server з Active Directory є незамінною річчю у побудові мережевої інфраструктури. В той самий час Active Directory або служба активного каталогу є дуже об'ємною, через що конфігурація іноді потребує багато часу та знань. Через це в деяких випадках залишаються надлишкові права у користувачів, або використовуються занадто слабкі методи контролю доступу. Крім цього деякі можливості використання служб Windows Server потребують користувачів з правами, наприклад, на використання MSSQL або інших служб, як IIS. Дані дії є потенційними точками входу в домен та підвищення привілеїв у ньому.

Тому для визначення слабких місць домену, проводяться тестування на проникнення [1]. Під час якого найважливішим етапом є енумерація [2]. В даному етапі важливим є по-перше обізнаність тестувальника, а по-друге чи правильно працюють ті засоби, на які він повлягається, для того, щоб збудувати картину домена. Раніше доводилось будувати інтелектуальну карту вручну, що додавало роботи, а в купі з неправильними інструментами це призводило до того, що вразливості залишались не поміченими.

Все змінилось після виходу такого інструменту, як BloodHound (Neo4j та Sharphound для збору даних). BloudHound це одно сторінковий веб інструмент розроблений на основі платформи Linkurious з використанням JavaScript, скомпільований через Electron та побудований на базі даних Neo4j, яку наповнює колектор даних, реалізований на C#. BloodHound використовує теорію графів для виявлення прихованих і часто небажаних взаємозв'язків у середовищі Active Directory або Azure [3].

Наразі даний інструмент є незамінним рішенням, як для Blue Team так і для Red Team.

Метою даної роботи було проаналізувати та порівняти методи інструменту BloodHound з типовими методами енумерації контролерів домену з Active Directory.

Так як BloodHound лише інструменти ілюстрації графів, то для дослідження був використаний внутрішній інструмент SharpHound. Даний інструмент збору інформації використовує powershell скрипт, який звантажується на систему файл SharpHound та запускає його. Конвертувавши його з base64 було отримано .net код, в якому можна побачити, що програма використовує бібліотеку Windows та прості команди, як get_Name(), get_CollectAllProperties() і т.д., після чого конвертує зібрані дані до Json формату, а після також архівує отримані файли в zip. Швидкість збору вражає проте є деякі недоліки. Першим та найголовнішим недоліком є те, що для запуску даний інструмент потребує .net framework специфічної версії, що іноді не працює з досліджуваним доменом. Також

версія збирача даних повинна відповідати версії BloudHound, проте знайти відповідні версії програм іноді буває важко.

Для тестування було використано Windows Server 2012 з Active Directory та деякими базовими ролями, які можуть використовуватися у домені. Для запуску SharpHound було також встановлено .NET та відключено захист в PowerShell (була використана команда Set-Execution-Policy -Scope CurrentUser -ExecutionPolicy Bypass -Force;). Як вже було згадано раніше сбір даних відбувається майже миттєво, тому на рисунку 1 відразу було продемонстровано граф з даних про домен.

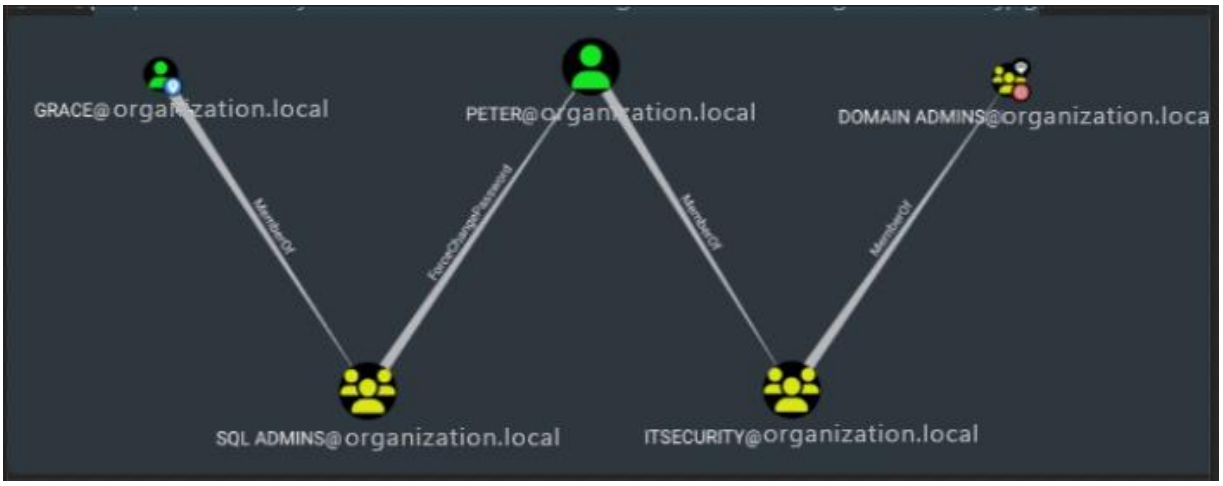

Рис. 1. Зібрані дані про домен

Крім цього можливо не тільки переглянути, які користувачі присутні, а й навіть переглянути технікі MITRE ATT&CK для подальшої експлуатації.

Наприклад у досліджуваному випадку можливо було провести атаку NTLM-Relay з використанням MSSQL, що і було описано, як тактика T1555.004 - Credential Access.

Щодо ручного тестування, то на відміну від C# коду, що потребує залежності у виді встановленого .net framework, можна використовувати відповідні команди PowerShell. У якості збірки таких команд буде виступати інструмент PowerSploit [6], який використовувався для енумерації (наразі даний вже не підтримується).

Дослідження даного інструменту показало, що пошук вразливостей та користувачів є дуже не тривіальною та складною задачею, також через те, що використовується оболонка PowerShell важко знайти саме приховані права та окрім цього енумерація, наприклад, портів та сервісів покладається на брутфорс замість оримання даних напряму. Це пов'язано з глибиною структури Windows. В той же SharpHound покладається на дані без такої абстрації, як PowerShell, тому енумерація з даним інструментом є більш проста. Крім за допомогою базової енумерації з PowerShell виокремлення тактик для атаки, є майже неможливим. Для цього потрібно буде витрачати дорогоцінний час.

Отже проаналізувавши два підходи до енумерації, можна дійти до висновку, що саме енумерація з BloodHound значно спрощує процес виявлення потенційних шляхів для підвищення привілеїв та подальшого експлуатаційного доступу. Водночас традиційні методи енумерації, як PowerShell, хоч і дають певну інформацію, але є менш точними та займають набагато більше часу.

Література

1. What is Penetration Testing?. URL: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/ (дата звернення 08.11.2024).

2. Enumeration in Ethical Hacking. URL: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/enumeration-ethical-hacking/ (дата звернення 08.11.2024).

3. BloodHound GitHub Repository. URL: https://github.com/BloodHoundAD/BloodHound (дата звернення 08.11.2024).4. https://www.sans.org/blog/bloodhound-sniffing-out-path-through-windows-domains/

5. BloodHound Documentation. URL: https://bloodhound.readthedocs.io (дата звернення 08.11.2024).

6. PowerSploit GitHub Repository. URL: https://github.com/PowerShellMafia/PowerSploit (дата звернення 08.11.2024).