Graphical user interface, text, application, email, website

Description automatically generated

Đây là 1 trong số các bài ở mức độ Hard (Windows) là mk làm mà ko cần đọc writeup 😊. Cũng mất gần 2 ngày (chủ yếu là research phần mk chưa biết) để hoàn thành. Bắt đầu thôi.

1. Dò quét

rustscan -b 900 -a 10.10.135.167 (mk sử dụng rustscan dò quét cổng cho nhanh)

Graphical user interface

Description automatically generated

Kết quả trả về thấy có port 88 => liên tưởng luôn tới Active Directory!

1. Enum

Với những bài liên quan tới Active Directory mk thường bắt đầu với “Ldapsearch”

ldapsearch -x -h 10.10.135.167 -s base namingcontexts

Output trả về “DC=fusion,DC=corp” và chúng ta kết hợp với dò quét bằng Nmap => Tìm được domain là fusion.corp

Graphical user interface, text

Description automatically generated

Chi tiết hơn xem có gì ko!

Text

Description automatically generated

Nothing 😊

Chuyển qua port 135 với Rpc xem sao

A screenshot of a computer

Description automatically generated with low confidence

Nothing tiếp 😊 Truy cập bị từ chối

Còn port 80 – web xem có gì ko

Graphical user interface, website

Description automatically generated

Có tên của nhân viên đây rồi phải note lại cái đã

Graphical user interface, application, website

Description automatically generated

Tạo danh sách các username từ tên nhân viên => bruteforce với kerbrute xem sao

Graphical user interface, text, application, chat or text message

Description automatically generated

Lại nothing tiếp rồi =))

Text

Description automatically generated

Nãy giờ bế tắc quá, chuyển qua tìm file/folder ẩn xem có gì hay ho ko

Text

Description automatically generated

A nó đây rồi. Chính nó “backup”. Ở ngoài thực tế chắc ko bh xảy ra ntn luôn =)). Vào thư mục “backup” thấy có file “employees.ods” rồi tải về. Và đây là nội dung của file:

Table

Description automatically generated

Có username -> Copy những username này rồi bruteforce với kerbrute lần nữa

Graphical user interface, application

Description automatically generated

Username “lparker” ko yêu cầu xác thực trước. Tham khảo AE-REP roasting để biết thêm chi tiết. => Sử dụng công cụ impacket-GetNPUsers để lấy hash của user này

A screenshot of a computer

Description automatically generated with medium confidence

Sau khi có hash chúng ta sẽ tiến hành crack để tìm password

A screenshot of a computer

Description automatically generated with medium confidence

Mật khẩu cũng phức tạp ghê =)). Với username/password tìm được chúng ta có thể login qua công cụ evil-winrm để lấy flag1.

evil-winrm -i 10.10.135.167 -u lparker -p ‘!!abbylvzsvs2k6!’

Text

Description automatically generated

Ko có gì đặc biệt. Enum tiếp xem trong domain còn những user nào

Text

Description automatically generated

Hoặc chúng ta có thể sử dụng “rpcclient”

Graphical user interface, application

Description automatically generated

Chạy đâu cho thoát “jmurphy” với pass là “u8WC3!kLsgw=#bRY”. Login thôi:

evil-winrm -i 10.10.135.167 -u jmurphy -p ‘u8WC3!kLsgw=#bRY’

Sau khi login thành công chúng ta sẽ có được flag 2 ở thư mục Desktop

Graphical user interface, text, chat or text message

Description automatically generated

“SeBackupPrivilege” và “SeRestorePrivilege” nhìn khá lạ. Lên google search thử xem có gì ko. Sau thời gian tìm kiếm thấy được bài này: <https://www.hackingarticles.in/windows-privilege-escalation-sebackupprivilege> khá hữu ích => let’s go làm theo thôi.

Text

Description automatically generated

Dự là ntn: chúng ta sẽ transfer 2 file “sam” và “system” về máy để lấy username-hash rồi pass-the-hash user administrator rồi sau đó lấy flag3. Mà ko hiểu sao lệnh “download” của evil-winrm thành công rồi mà ko thấy 2 file đã download đâu =)). Đành dung cách khác vậy.

Graphical user interface, text, application

Description automatically generated



Sau khi transfer thành công chúng ta dump để lấy username/hash với công cụ “pypykatz”

Graphical user interface, application, chat or text message

Description automatically generated

Pass the hash thôi:

evil-winrm -u administrator -H 2182eed0101516d0a206b98c579565e6 -i 10.10.135.167

Graphical user interface

Description automatically generated with medium confidence

Error rồi. Thế thì cách này ko phải rồi. Hmm. Research tiếp vậy. Sau 1 thời gian khá dài mk tìm được bài này https://medium.com/r3d-buck3t/windows-privesc-with-sebackupprivilege-65d2cd1eb960. Làm theo thôi =))

Text

Description automatically generated

Text

Description automatically generated



Sau đó chúng ta transfer 2 file “ntds.dit” và “system” về máy để crack.

Text

Description automatically generated

Chúng ta thu được hash của Administrator => pass the hash thôi:

Evil-winrm -i 10.10.135.167 -u administrator -H 9653b02d945329c7270525c4c2a69c67

Sau khi login thành công chúng ta có được flag3 ở thư mục Desktop

\*Bonus: Persistence 1 chút cho vui



Sau đó chúng ta sử dụng administrator:p@ssword123! Để login trên dịch vụ RDP

xfreerdp /v:10.10.135.167 /u:'fusion.corp\administrator' /p:'p@ssword123!' +clipboard

A screenshot of a computer

Description automatically generated