GO-TO CVE
CVE-2023-51766

SMTP SMUGGLING
Week 9
Author : Ali Soltani

1LIANGROUP.NET

مقدمه

سلام به همه عزیزان! خوش آمدید به هفته نهم از برنامه GO-TO CVE. این هفته، به بررسی یکی از آسیب‌پذیری‌های مهم در دنیای امنیت ایمیل می‌پردازیم CVE-۲۰۲۳-۵۱۷۶۶. با استفاده از این آسیب‌پذیری، امکان اجرای حملات SMTP Smuggling فراهم می‌شود که می‌تواند به مهاجمان اجازه ارسال ایمیل‌های جعلی با دامنه‌های معتبر را بدهد و روی نسخه های EXIM قبل از نسخه ۴,۹۷,۱ تاثیر گذار است که با AV:N/AC:L/PR:N/UI:N/S:U/ C:N/I:L/A:N و اسکور ۵,۳ را به خود اختصاص داده است و شرایط لازم برای آن عبارت است از:

- Exim قابلیت PIPELINING و CHUNKING را بر روی اتصالات ورودی ارائه دهد.
- برای دریافت پیام از دستور DATA به جای BDATاستفاده شود.
- سرور رله داده‌های پیام شامل یکی از رشته‌های «CR LF. LF»، «LF . LF» یا «LF. CR LF» را ارسال کند.
- Exim این رشته‌ها را به عنوان پایان داده تفسیر کند و پیام اول را بپذیرد.
- Exim داده‌های بیشتر را به عنوان داده‌های بدنه پیام تفسیر کند که می‌تواند شامل دستورات SMTP مانند BDAT، RCPT، MAIL و غیره باشد.

چند سطرحی همراه با پروتوکل SMTP

برای این که درکی بهتر از مفهوم SMTP smuggling داشته باشیم اول باید پروتوکل SMTP را کمی بهتر بشناسیم پروتکل SMTP (Simple Mail Transfer Protocol) یکی از پروتکل‌های استاندارد برای ارسال ایمیل در شبکه‌های اینترنتی و دیگر شبکه‌های مبتنی بر IP است. SMTP در دهه ۱۹۸۰ توسعه یافته شده است و همچنان یکی از اصلی‌ترین پروتکل‌های مورد استفاده برای ارسال ایمیل‌هاست.

کاربردهای SMTP

۱. ارسال ایمیل‌ها: SMTP عمدتاً برای ارسال ایمیل‌ها از سرویس‌دهنده (سرور) ایمیل فرستنده به سرویس‌دهنده ایمیل گیرنده استفاده می‌شود.
۲. ارتباط بین سرورها: SMTP همچنین برای انتقال ایمیل‌ها بین سرویس‌دهنده‌های ایمیل (mail servers) استفاده می‌شود. وقتی یک ایمیل از یک سرور به سرور دیگری منتقل می‌شود، SMTP مسئول انتقال آن است.
۳. ارسال از کلاینت به سرور: بسیاری از برنامه‌های ایمیل کلاینت، مثل Outlook و Thunderbird، از SMTP برای ارسال ایمیل‌های کاربر به سرور ایمیل استفاده می‌کنند.

نمونه‌هایی از سرویس‌های ایمیل معروف که از SMTP استفاده می‌کنند:

- Gmail
- Yahoo Mail
- Outlook.com
- Proton Mail
- Zoho Mail

و کلی از اسامی محبوب دیگر مثل POSTFIX که بشخصه علاقه زیادی بهش دارم.

نوع ارسال و دریافت پکت‌ها در SMTP

SMTP از مدل ارتباطی مبتنی بر متن استفاده می‌کند و پیام‌ها را در قالب دستورات ASCII ارسال می‌کند. هر پیام شامل چندین جزء است، شامل سربرگ‌ها (headers) و بدنه پیام (body) .

فرآیند ارسال ایمیل با استفاده از SMTP

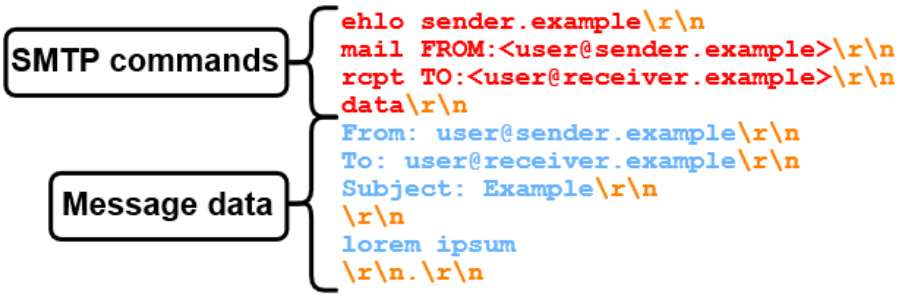
۱. ایجاد ارتباط: ابتدا کلاینت با سرور SMTP ارتباط برقرار می‌کند، معمولاً از طریق پورت ۲۵، ۵۸۷ یا ۴۶۵ (برای ارتباطات امن).
۲. احراز هویت: در صورت نیاز، کلاینت با استفاده از دستورات AUTH احراز هویت می‌شود.
۳. شروع جلسه: کلاینت دستور HELO یا EHLO را به سرور ارسال می‌کند تا شروع جلسه را اعلام کند.
۴. فرستنده ایمیل: کلاینت دستور MAIL FROM را به همراه آدرس فرستنده به سرور می‌فرستد.
۵. گیرنده ایمیل: کلاینت دستور RCPT TO را به همراه آدرس گیرنده به سرور ارسال می‌کند.
۶. ارسال داده‌ها: کلاینت دستور DATA را ارسال می‌کند و سپس بدنه ایمیل را به همراه سربرگ‌های مورد نیاز ارسال می‌کند.
۷.پایان: کلاینت با دستور QUIT جلسه را خاتمه می‌دهد.

فرآیند دریافت ایمیل با استفاده از SMTP

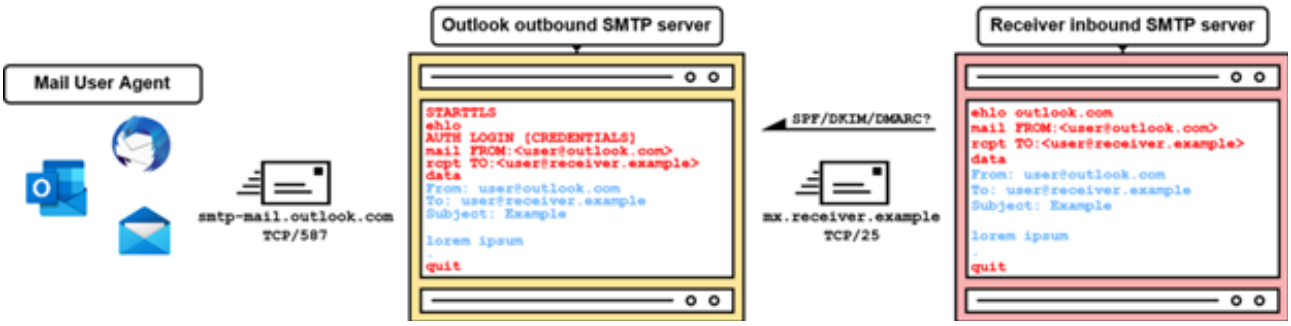
در واقع، SMTP تنها برای ارسال ایمیل‌ها استفاده می‌شود. دریافت ایمیل‌ها معمولاً از طریق پروتکل‌های دیگری مثل POP۳ (Post Office Protocol ۳) یا IMAP (Internet Message Access Protocol) انجام می‌شود.

دستورات رایج SMTP

- HELO/EHLO معرفی کلاینت به سرور
- MAIL FROM مشخص کردن فرستنده ایمیل
- RCPT TO مشخص کردن گیرنده ایمیل
- DATA شروع انتقال بدنه ایمیل
- QUIT پایان جلسه SMTP
- AUTH احراز هویت کاربر



در توضیح عکس بالا این عکس را مشاهده کنید که بهتر توضیح میدهد روی شکل در عکس پایین میتوانید فرایند کامل را در یک عکس مشاهده فرمایید .



توضیحات روند عکس بالا در ارسال ایمیل از طریق SMTP

اتصال کلاینت ایمیل به سرور Outlook:

- کاربر ایمیل MUA - Mail User Agent)) برنامه‌هایی مثل Outlook، Thunderbird و Windows Mail .
- عامل انتقال ایمیل اوتلوک MTA - Mail Transfer Agent)) سروری که به ارسال ایمیل‌های خروجی اختصاص دارد.
- پورت ۵۸۷/TCP پورت ارسال پیام برای اتصال MUA به MTA.

ارسال دستورات SMTP و داده‌های پیام:

- دستورات SMTP : شامل دستورات STARTTLS و AUTH LOGIN .
- STARTTLS استفاده برای ارتقاء به یک جلسه رمزگذاری شده TLS . به طور کلی، SMTP رمزگذاری نشده است و در غیر این صورت اطلاعات اعتبارسنجی ممکن است برای حمله‌کنندگان قابل شنود باشد.
- AUTH LOGIN دستور SMTP برای احراز هویت کاربر با استفاده از نام کاربری و رمز عبور.

ارزیابی اعتبارسنجی:

- پس از ارزیابی اینکه آیا کاربر احراز هویت‌شده مجاز به ارسال ایمیل برای آدرس‌های ایمیل مشخص شده در فیلدهای mail FROM و From است، سرور SMTP اوتلوک ایمیل ورودی را به سرور SMTP ورودی (inbound SMTP server) در receiver. Example ارسال می‌کند.

ارسال ایمیل به سرور SMTP گیرنده:

- پورت ۲۵/TCP : پورت استاندارد برای ارسال ایمیل‌ها به سرور SMTP ورودی.
- داده‌های SMTP : داده‌های ارسال شده به سرور SMTP ورودی مشابه داده‌های ارسال شده به سرور SMTP خروجی است، اما شامل دستور AUTH LOGIN نمی‌شود و در این حالت از STARTTLS استفاده نمی‌کند.

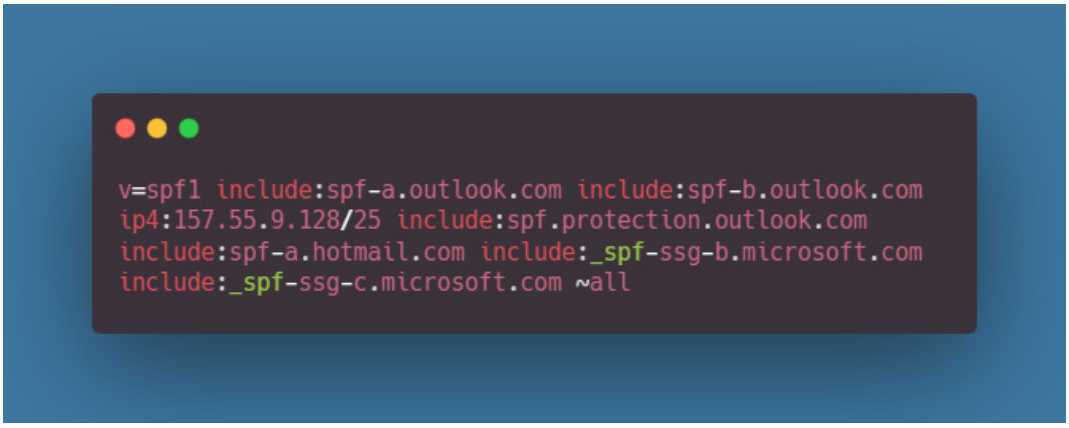
این روند ارسال ایمیل را به پایان می‌رساند. اما حالا چطور سرور SMTP ورودی مطمئن می‌شود که سرور SMTP خروجی واقعاً مجاز به ارسال ایمیل‌ها برای دامنه outlook.com است؟ و چرا هر کسی نمی‌تواند ایمیل‌هایی برای دامنه outlook.com ارسال کند؟

توضیحات مکانیزم‌های احراز هویت ایمیل SPF، DKIM و DMARC

SPF (Sender Policy Framework)

قبل از اینکه سرور SMTP ورودی (inbound SMTP server) یک ایمیل را بپذیرد، صحت فرستنده را از طریق مکانیزم‌های احراز هویت ایمیل مانند SPF، DKIM و DMARC بررسی می‌کند. این کار مهم است زیرا در غیر این صورت، مهاجمان می‌توانند از دامنه‌های دلخواه ایمیل ارسال کنند. به عنوان مثال، ارسال ایمیلی با آدرس admin@outlook.com از سرور مهاجم ممکن میسازد.

مکانیزم احراز هویت ایمیل که بیشتر رایج است SPF نامدارد که با مجاز کردن آدرس‌های IP فرستنده در رکوردهای ویژه SPF/TXT در DNS کار می‌کند. رکورد SPF برای دامنه outlook.com شامل محدوده‌های IP زیر برای انتقال ایمیل است:



اگر شما از یکی از این محدوده‌های IP ارسال نکنید، چک SPF ناموفق میشود و احتمالاً ایمیل شما ارسال نمی‌شود یا به عنوان اسپم علامت‌گذاری می‌شود. اما کدام دامنه واقعاً باید بررسی می‌شود؟ مشکل SPF به تنهایی این است که فقط دامنه MAIL FROM در ایمیل بررسی می‌شود. سربرگ From در داده‌های پیام، که در ایمیل دریافتی نمایش داده می‌شود، می‌تواند مقدار دلخواهی داشته باشد.

DKIM (Domain Keys Identified Mail)

همین موضوع برای DKIM نیز صدق می‌کند. DKIM امکان امضای داده‌های پیام، از جمله سربرگFrom، را فراهم می‌کند. این امضا می‌تواند توسط گیرنده با استفاده از یک کلید عمومی که در DNS قرار دارد تأیید شود. اما مشخص نمی‌کند کدام دامنه کلید عمومی را نگه می‌دارد.

در این حالت، پیام از user@sender.example ممکن است امضا شده باشد، اما کلید تأیید در dkim._domainkey.attacker.example قرار دارد. این مکان از ترکیب «dkim» (s=) «selector»، مقدار ثابت «_domainkey» و دامنه (d=) «attacker.example» به دست می‌آید. بنابراین، حتی اگر ایمیل یک رکورد SPF معتبر و یک امضای DKIM معتبر داشته باشد، مکانیزمی برای تعیین اینکه آیا ایمیل از یک فرستنده مخرب است یا خیر وجود ندارد.

DMARC (Domain-based Message Authentication, Reporting & Conformance)

خوشبختانه DMARC وجود دارد که مخفف Domain-based Message Authentication, Reporting and Conformance است. DMARC معرفی‌کننده‌ی «هماهنگی شناسه» برای SPF و DKIM است و به فرستندگان اجازه می‌دهد تا سیاست‌های هماهنگی را برای هر دو روش مشخص کنند. DMARC بررسی می‌کند که آیا دامنهFrom ایمیل با چک‌های SPF و/یا امضاهای DKIM هماهنگ است. بنابراین، چک DMARC ناموفق باشد اگر بین دامنه MAIL FROM و دامنه From ناسازگاری وجود داشته باشد.

نمونه‌ای از سیاست DMARC

یک مثال برای یک سیاست DMARC که همیشه در یک رکورد TXT در _dmarc.[domain] قرار دارد، به شرح زیر است:

- p=reject سیاستی که به سرور گیرنده می‌گوید ۱۰۰ درصد پیام‌هایی که چک DMARC را پاس نمی‌کنند رد کند.
- pct=۱۰۰ تعیین می‌کند که ۱۰۰ درصد پیام‌ها باید بررسی شوند.
- پیام تنها در صورتی پذیرفته می‌شود که رکورد SPF معتبر ویا امضای DKIM معتبر داشته باشد.

وضعیت در صورت نبود رکورد DMARC

در صورتی که رکورد DMARC وجود نداشته باشد، به طور کلی، مدیریت اصالت ایمیل به شدت به پیکربندی و نرم‌افزار سرور SMTP ورودی بستگی دارد. به عنوان یک قاعده کلی، اگر هم‌راستایی SPF یا DKIM وجود داشته باشد، احتمال پذیرش ایمیل زیاد است.

در ادامه SMTP Smuggling

حال که پایه و اساس مکانیزم‌های احراز هویت ایمیل توضیح داده شد، می‌توانیم به موضوع اصلی یعنی SMTP smuggling بپردازیم.

این مکانیزم‌ها با هم تضمین می‌کنند که فقط سرورهای مجاز می‌توانند ایمیل‌هایی به نمایندگی از یک دامنه خاص ارسال کنند و ایمیل‌ها در مسیر ارسال دستکاری نمی‌شوند. این کمک می‌کند تا از ارسال ایمیل‌های جعلی و سوءاستفاده از دامنه‌های معتبر جلوگیری شود.

آسیب‌پذیری‌های SMTP :

SMTP به دلیل طراحی اولیه‌اش که بر مبنای اعتماد بین سرورهای ایمیل بوده است، دارای برخی ابهامات و ضعف‌های امنیتی است. این نقاط ضعف شامل نقص‌هایی در فرآیند احراز هویت و صحت پیام‌ها می‌شود که می‌توانند توسط مهاجمان برای انجام حملات مورد سوءاستفاده قرار گیرند.

این پروتکل ساده و موثر است و یکی از اجزای کلیدی زیرساخت ایمیل در اینترنت به شمار می‌رود.

حملات فیشینگ و نفوذ به داده‌ها:

فیشینگ یک روش حمله سایبری است که در آن مهاجم با استفاده از ایمیل‌های جعلی و فریبنده، کاربران را به افشای اطلاعات حساس مانند نام کاربری، گذرواژه‌ها، و اطلاعات مالی ترغیب می‌کند. نفوذ به داده‌ها نیز شامل دسترسی غیرمجاز به داده‌های محرمانه و حساس است که می‌تواند منجر به افشای اطلاعات شخصی و تجاری شود.

توضیحی متخصری بر دنیای Smuggling بخش SMTP Smuggling

جعل SMTP (SMTP Smuggling) یک تهدید تقریبا جدید در حوضه امنیت سایبری است که چندی پیش مرکز توجه قرار گرفته بود. این تکنیک پیشرفته از آسیب‌پذیری‌های موجود در پروتکل انتقال email یا همان SMTP، که یک فناوری بنیادی برای انتقال ایمیل است، سوءاستفاده می‌کند. با دستکاری ابهامات ذاتی این پروتکل، مهاجمان می‌توانند محتوای مخرب یا پیام‌های ایمیل جعل شده را «Smuggle» کنند و از روش های امنیتی قدیمی مانند SPF و DMARC عبور کنند. این اقدام به صحت ارتباطات ایمیلی آسیب می‌رساند و درهای جدیدی برای حملات فیشینگ پیشرفته و نفوذ به داده‌ها باز می‌کند. به عنوان یک چالش نسبتاً جدید در چشم‌انداز سایبری، جعل SMTP نیاز به آگاهی بیشتر و بازنگری در استراتژی‌های امنیتی موجود برای ایمیل های شما و سازمانتان را دارد.

هدف از این تحقیق

هدف اصلی این تحقیق، آزمایش پروتکل SMTP در برابر برخی حملات رایج و خاصی بود که بر روی سایر پروتکل‌ها، مانند HTTP، عمل می‌کنند که این حمله الهام گرفته از حمله ایست که در زمینه SMTP نیز قابل استفاده است، HTTP request smuggling می‌باشد.

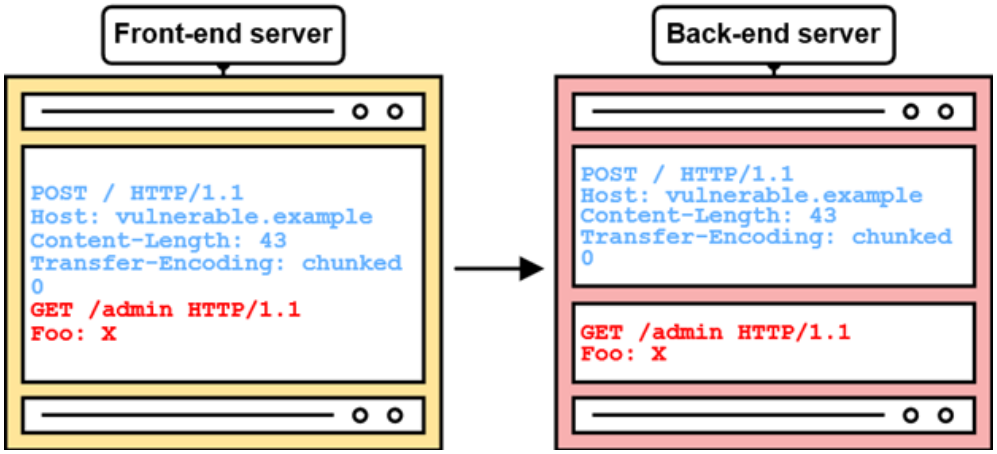
HTTP Request Smuggling چیست؟

در نوعی از حملات HTTP request smuggling، از تفاوت‌های تفسیری در تفسیر و پردازش هدرهای HTTP مانندContent-Length و Transfer-Encoding بهره‌برداری می‌شود. این تفاوت‌ها به مهاجم اجازه می‌دهد

که درخواست HTTP دلخواهی را به یک سرور پشتیبان غیرقابل دسترس ارسال کند.

تشابهات آن با SMTP

در پروتکل SMTP نیز می‌توان از تفاوت‌های تفسیری بین سرورهای SMTP خروجی outbound SMTP servers)) و ورودی (inbound SMTP servers) مثل حمله قبل بهره‌برداری کرد. اگر این سرورها به روش‌های متفاوتی دنباله پایان داده data sequence <CR><LF>.<CR><LF> end-of- را تفسیر کنند، امکان حمله SMTP smuggling به وجود می‌آید. در این حالت، مهاجم می‌تواند از داده‌های پیام خارج شده و دستورات SMTP دلخواه را مشخص کند یا حتی ایمیل‌های جداگانه‌ای ارسال کند مشابه با حمله HTTP request smuggling که در زیر فلو آن را مشاهده میفرمایید .



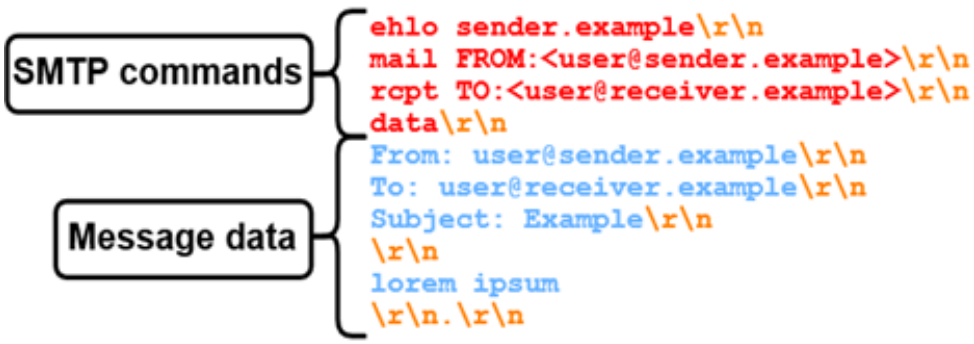
ساخت حساب در ارائه‌دهندگان ایمیل:

ابتدا حساب‌های ایمیل در ارائه‌دهندگان عمومی که از ارسال ایمیل از طریق SMTP پشتیبانی می‌کنند (مانند gmx.net، gmail.com، outlook.com و غیره) ثبت شد.

ارسال ایمیل و بررسی تفاوت‌هایشان:

با ارسال ایمیل‌ها از طریق سرورهای SMTP خروجی این ارائه‌دهندگان و دریافت آن‌ها در سرور تحلیل SMTP ورودی، تفاوت‌های موجود در پیاده‌سازی پروتکل SMTP بررسی شد.

تفاوت‌های مشاهده شده

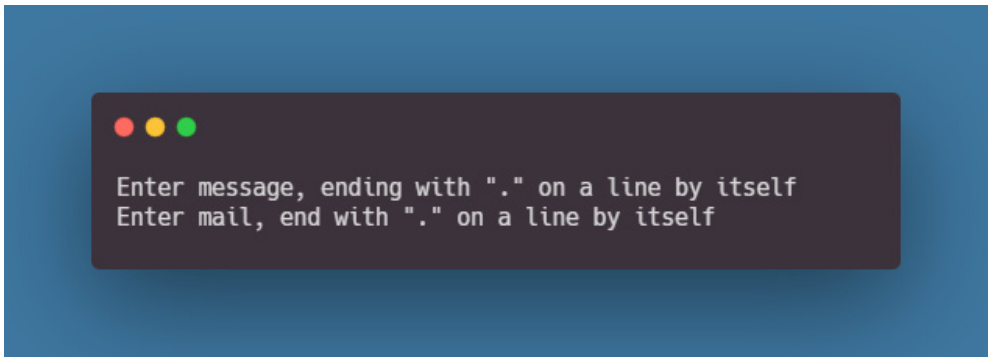


در هنگام ارسال دستور DATA، پاسخ‌های متفاوتی از سرورهای ایمیل دریافت شد:

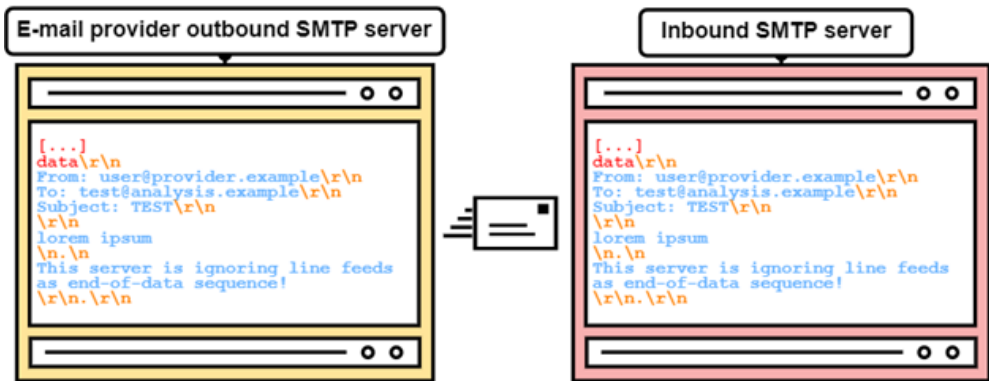
این پاسخ‌ها به نظر نمی‌رسید که برای هدف ما که smuggling است مفید باشند، زیرا تنها تفاوت‌های جزئی در متن داشتند.
خوب انگیزمان را از دست نمیدهیم و به راه خود ادامه میدیهم و راه به هکر درون خود میسپاریم .

تفاوت در تفاسیر سیستم‌عامل‌ها

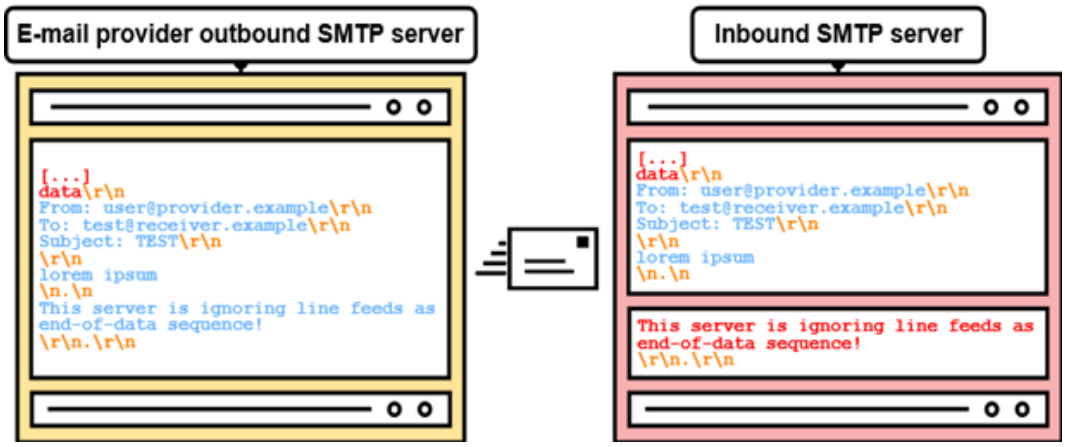
پاسخ‌هایی که خوشحال کننده به نظر می‌رسیدند شامل موارد زیر بودند:



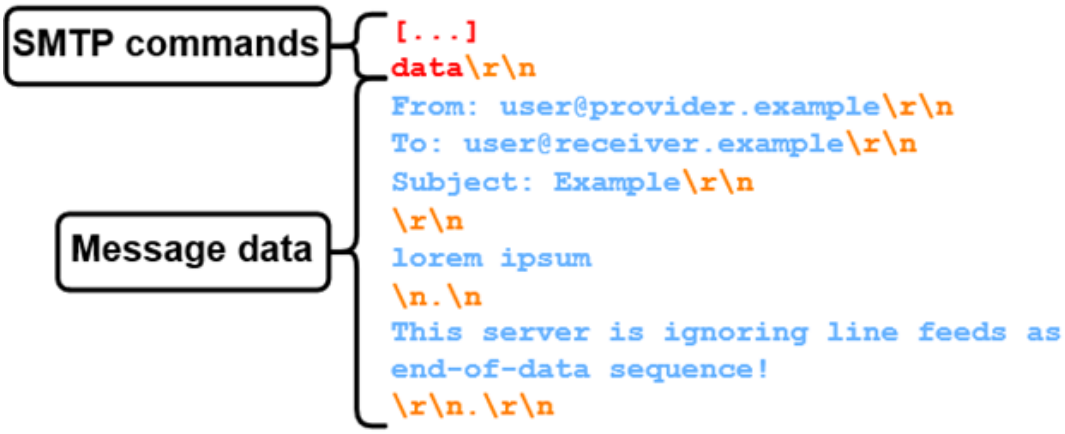
تفاوت در تفاسیر سیستم‌عامل‌ها باعث این امیدواری شد. در ویندوز، «.» به تنهایی در خط با دو Carriage Return <Line Feed <CR><LF>.<CR><LF یا \r\n.\r\n\)) جدا می‌شود، در حالی که در لینوکس، «.» به تنهایی در خط با دو <Line Feed <LF>.<LF یا (\n.\n\) جدا می‌شود. که در ویندوز شکل زیر



و مرحله بعدی آن به صورت زیر است .



که ساختار آن به این صورت است .

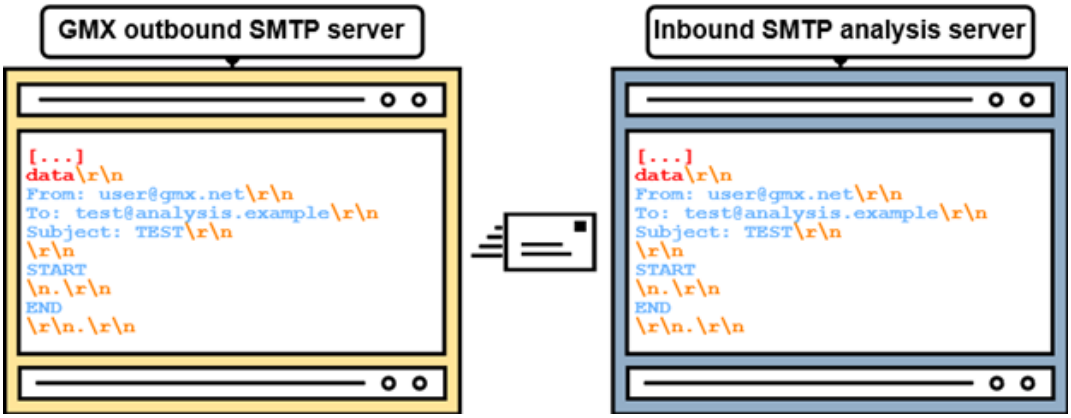


نتیجه‌گیری این بخش

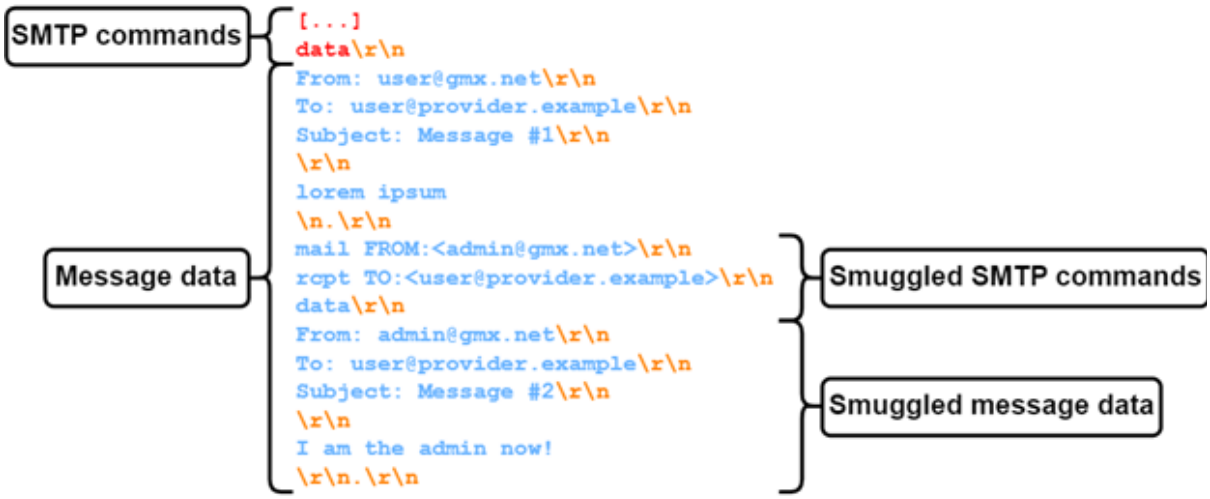
با درک این تفاوت‌ها، می‌توان بهره‌برداری‌های مختلفی از تفاسیر مختلف پروتکل SMTP انجام داد. در ادامه، به بررسی عمیق‌تر و پیاده‌سازی‌های عملی حمله SMTP smuggling پرداخته می‌شود تا میزان کارایی و بهره‌برداری از این حملات در شرایط واقعی بررسی گردد.

به وقت حمله .....

در اولین قدم از GMX استفاده میکنیم که یک میل سرور قدیمیست و که حدود ۲۰ ملیون کاربردارد چیزی که در ارسال مشاهده کردیم به صورت زیر است .

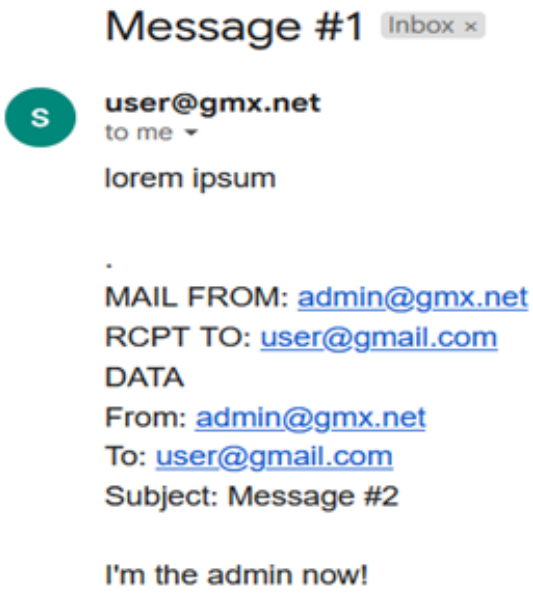


بر اساس تفاوت هایی که مطرح شد درست حدس زدید حالا میتوانیم با <LF>.<CR><LF> خارج شویم.

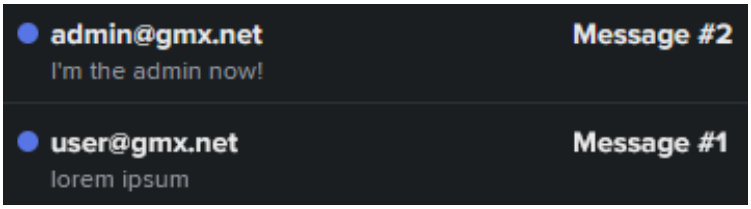


SMTP smuggling from admin@gmx.net to user@provider.example

در تلاش های اولیه که به این شکل بود <LF>.<CR><LF> با شکست مواجه شد و به داده هایمان که قصد اسماگل کردن آنها رو داشتیم پایان نداد که میتوانید عکس آن را مشاهده می کنید.



ولی برای برخی دیگر کار کرد و انجام شد مثل



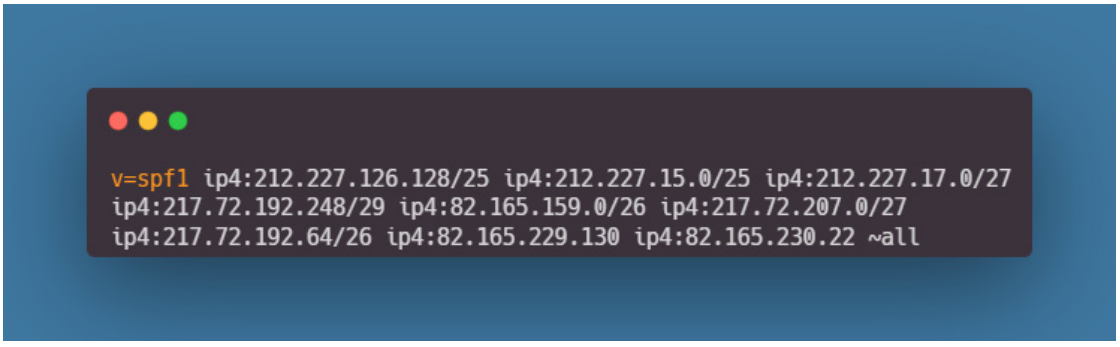
که اولین SMTP smuggling روی GMX رخ داد و با بررسی هدر ها فهمیدم که از صد SPF هم گذشت .

SMTP smuggling بهمراه جعل دامنه ها و پیامدهای آن

پروتکل SMTP می‌تواند از طریق تکنیک‌های اسماگلینگ مورد سوء استفاده قرار گیرد و به مهاجمان این امکان را بدهد که ایمیل‌هایی ارسال کنند که از فیلترهای اسپم و مکانیزم‌های احراز هویت دامنه عبور کنند. در این بخش، نحوه دستیابی به جعل بین دامنه‌ای SMTP و تأثیرات احتمالی آن که بر امنیت ایمیل تاثیر دارد را تاحدی بررسی میکنیم.
با سوء استفاده از سرور خروجی SMTP شرکت GMX، توانستیم برای دامنه gmx.net امکانی برقرار کنیم که کنیم که ایمیل‌ها حتی تحت سیاست‌های سختگیرانه DMARC نیز از فیلترهای اسپم عبور کنند. این امر احتمال جعل دامنه‌های دیگر را که از همان سرور SMTP استفاده می‌کنندرا برای ما فراهم میسازد.

تجزیه و تحلیل رکوردهای SPF

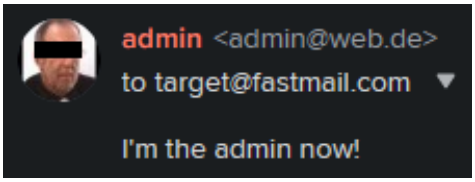
با بررسی رکورد SPF دامنه web.de مشخص شد که آدرس IP سرور خروجی SMTP شرکتGMX (`۲۱۲,۲۲۷,۱۵,۱۵`) نیز در این رکورد گنجانده شده است:



این بدان معناست که می‌توانیم پیام‌های اسماگل کردن SMTP را تغییر دهیم و از دامنه web.de به عنوان دامنه فرستنده استفاده کنیم.

شبیه‌سازی سناریوی واقعی

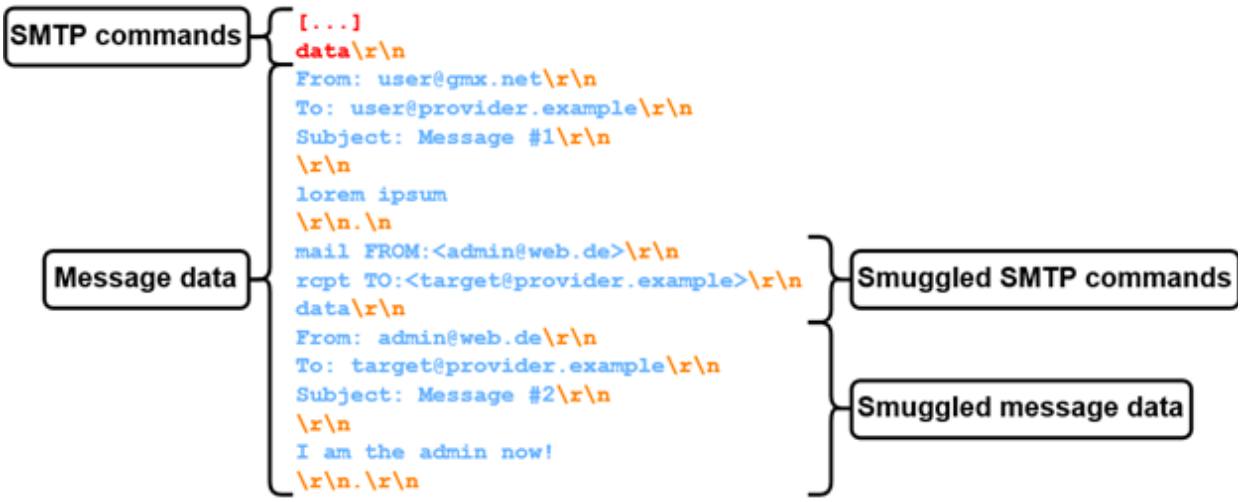
برای شبیه‌سازی یک سناریوی واقعی، یک پیام را با استفاده از دامنه web.de به مقصد مورد نظر ارسال می‌کنیم. در این حالت، در برخی گیرنده ها حتی ممکن است تصویر پروفایل مرتبط با admin@web.de واقعی را ببینند که در عکس زیر مشاهده میفرمایید.



تأیید صحت SPF

پس از ارسال پیام، بررسی‌های SPF موفقیت‌آمیز بودند:

این نشان می‌دهد که پیام ارسالی از نظر سرور گیرنده معتبر است.



گسترش مشکل به دیگر سرویس‌های ایمیل

مشکل فراتر از GMX است. بسیاری از سرویس‌دهندگان بزرگ ایمیل از سرور SMTP مخصوص خودشان به نام NemesisSMTPd استفاده می‌کنند. GMX بخشی از Ionos است و خدمات ایمیل ارائه شده توسط Ionos نیز از NemesisSMTPd استفاده می‌کنند.

مشکل وسیع‌تر از GMX : بررسی و بهره‌برداری از NemesisSMTPd

تحقیقات اولیه ما نشان داد که سرور SMTP سفارشی GMX، به نام NemesisSMTPd، نسبت به حملات قاچاق SMTP آسیب‌پذیر است. با این حال، متوجه شدیم که این مشکل فراتر از GMX است و بسیاری از سرویس‌دهندگان بزرگ ایمیل دیگر نیز از NemesisSMTPd استفاده می‌کنند.

GMX و Ionos

GMX بخشی از Ionos است و خدمات ایمیل ارائه شده توسط Ionos نیز از NemesisSMTPd استفاده می‌کنند. با ثبت یک دامنه ایمیل در Ionos و بررسی امکان قاچاق SMTP، مشاهده کردیم که این تکنیک در اینجا نیز کار می‌کند.

بررسی رکوردهای SPF

برای درک بهتر مشکل، رکوردهای SPF دامنه‌های GMX و Ionos را بررسی کردیم. نتایج بررسی به شرح زیر است:

رکورد SPF برای Ionos :

```
$ dig _spf-eu.ionos.com TXT
"v=spf1 ip4:212.227.126.128/25 ip4:212.227.15.0/25 ip4:212.227.17.0/27
ip4:82.165.159.0/26 ip4:217.72.192.64/26 ?all"
```

رکورد SPF برای GMX :

```
$ dig _spf.gmx.net TXT
"v=spf1 ip4:212.227.126.128/25 ip4:212.227.15.0/25 ip4:212.227.17.0/27
ip4:82.165.159.0/24 ip4:74.208.4.192/26 ip4:217.72.207.0/27
ip4:82.165.229.31 ip4:82.165.230.21 ip4:213.165.64.0/23
ip4:74.208.5.64/26 ~all"
```

اشتراک محدوده‌های IP

با بررسی دقیق‌تر محدوده‌های IP مجاز در رکوردهای SPF، مشخص شد که این محدوده‌ها تا حد زیادی هم‌پوشانی دارند. این به ما امکان جعل ایمیل‌های نه تنها از دامنه‌های gmx.net و web.de ، بلکه از حدود یک میلیون دامنه دیگر میزبانی شده در Ionos را نیز می‌دهد.

نتیجه‌گیری این بخش

مشکل قاچاق SMTP در NemesisSMTPd گسترده‌تر از آن چیزی است که در ابتدا تصور می‌شد. این مشکل به مهاجمان این امکان را می‌دهد که از طریق استفاده از این آسیب‌پذیری، ایمیل‌هایی ارسال کنند که از فیلترهای امنیتی عبور کرده و به نظر می‌رسد از دامنه‌های معتبر ارسال شده‌اند. نیاز فوری به اقدامات اصلاحی و بهبود امنیت در سرویس‌دهندگان ایمیل بزرگ وجود دارد تا از وقوع چنین حملاتی جلوگیری شود.

Smuggling via Microsoft Exchange Online

تحلیل عمیق‌تر روی سرورهای SMTP : موارد خاص مثل outlook.com) Microsoft Outlook)

خصوصیات خاص سرور SMTP Outlook

در طی تحلیل دقیق‌تر بر روی سرورهای SMTP ، ویژگی خاصی در سرور SMTP Microsoft Outlook outlook.com)) مشاهده شدکه هنگام تلاش برای ارسال <LF>.<LF> < پیام ارسال نمی‌شود و پیام خطای زیر برگردانده شد که در عکس زیر مشاهده میکنید

محدودیت‌های ارسال پیام در Outlook

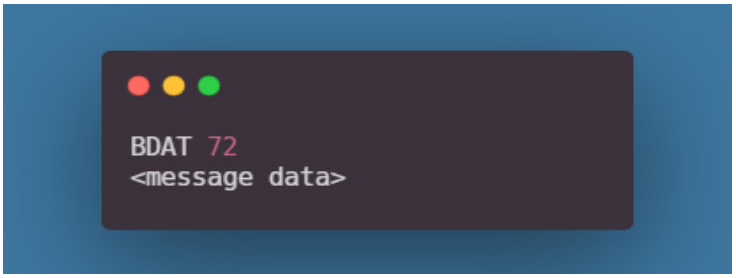
با این حال، مانند Outlook، GMX نیز <<LF><CR><LF را فیلتر نمی‌کند. با این وجود، امکان قاچاق SMTP به گیرندگان مشابه مانند Fastmail)) وجود نداشت. دلیل این موضوع استفاده Outlook از فرمان اختیاری BDAT در پروتکل SMTP است.

تفاوت BDAT و DATA

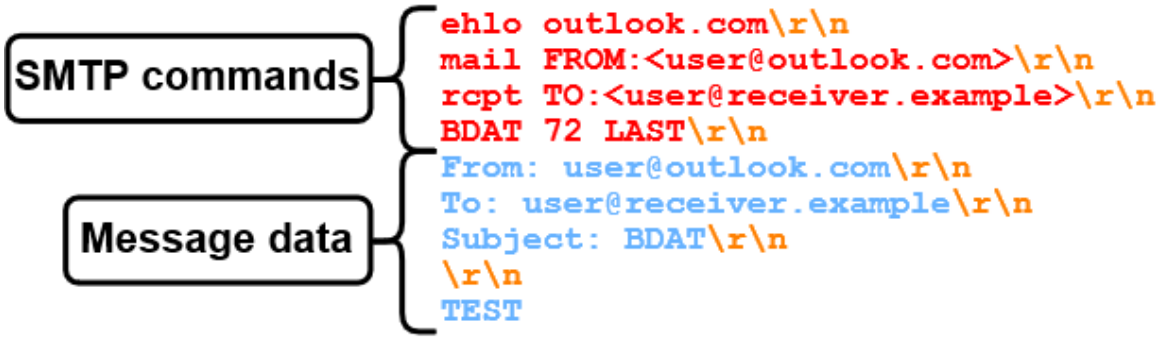
BDAT جایگزینی برای فرمان DATA است که برای انتقال داده‌های پیام استفاده می‌شود. در BDAT، طول پیام با استفاده از فرمان BDAT مشخص می‌شود، به جای اینکه به نقطه و چندکاراکتر پایان دهنده تکیه کند. به عنوان مثال، برای انتقال ۷۲ بایت از داده‌های پیام، می‌توانیم این کار را مانند شکل زیر انجام دهیم.

مثال BDAT

برای انتقال ۷۲ بایت داده پیام با استفاده از BDAT، فرمان به شکل زیر است:



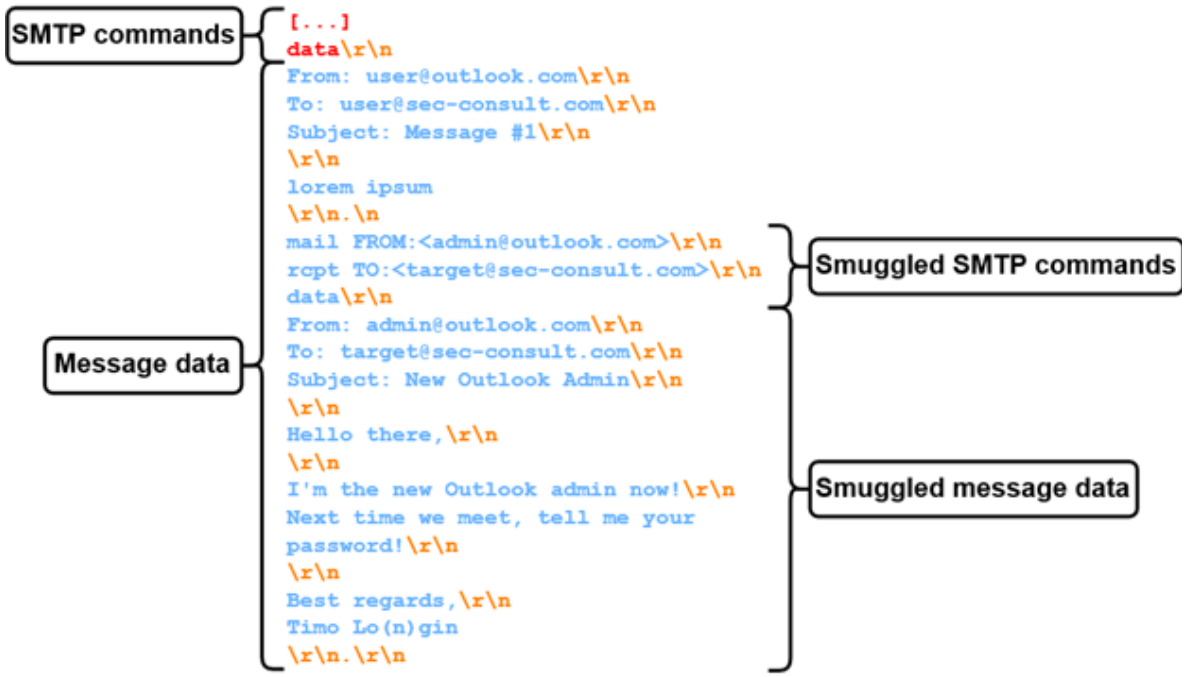
در اینجا، ۷۲ تعداد بایت‌های داده پیام است که قرار است انتقال یابد. این رویکرد از توالی‌های پایان داده مانند <CR><LF>.<CR><LF>> اجتناب می‌کند و بر طول دقیق پیام تمرکز می‌کند، که باعث کاهش آسیب‌پذیری‌های مرتبط با قاچاق SMTP می‌شود (اینها زرنگن ولی ما زرنگ تریم).



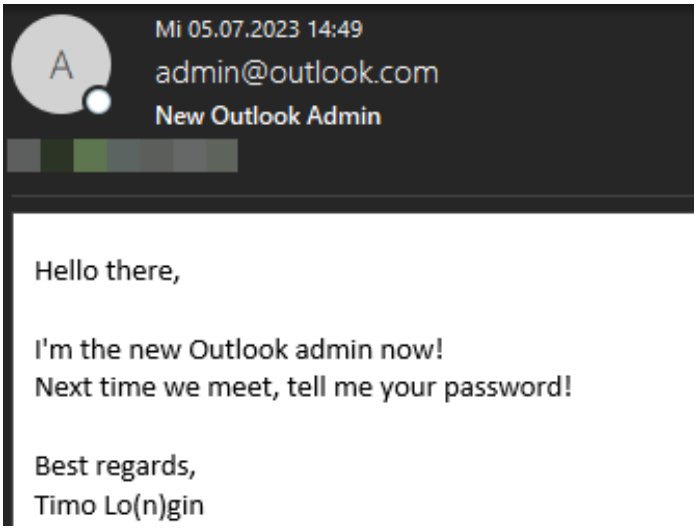
خوب به اینجا اکتفا نمیکنیم و به دنبال سرور هایی میگردیم که از BDAT استفاده نکنند که در ادامه به آن پرداختیم .

یافتن سرور SMTP آسیب‌پذیر

برای اجرای حملات قاچاق SMTP، ما به دنبال سروری هستیم که توالی <LF><CR><LF>> را به عنوان توالی پایان داده تفسیر کند و از فرمان BDAT پشتیبانی نکند. سرور SMTP sec-consult.com دقیقاً این شرایط را دارد. لازم به ذکر است که بسیاری از سرورها در اینترنت این شرایط را دارند، اما از آنجا که باید مطمئن شویم سیستم‌های خودمان امن هستند، از سرور sec-consult.com استفاده خواهیم کرد.
برای اطمینان از کارکرد حمله، اولین اقدام ما ارسال ایمیل‌های جعلی به دوستان خودمان است. این ایمیل‌ها به گونه‌ای طراحی می‌شوند که بررسی کنیم آیا سرور دریافت کننده SMTP قادر به تشخیص پیام جعلی هستند یا خیر.

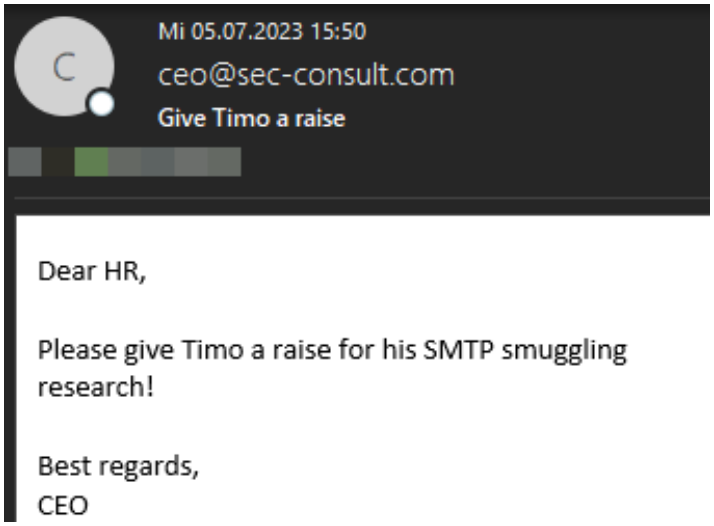


ایمل فیشنگ بالا را که نمونه از این ایمل هاست مشاهده میکنید که در اسپم قرار نگرفت .

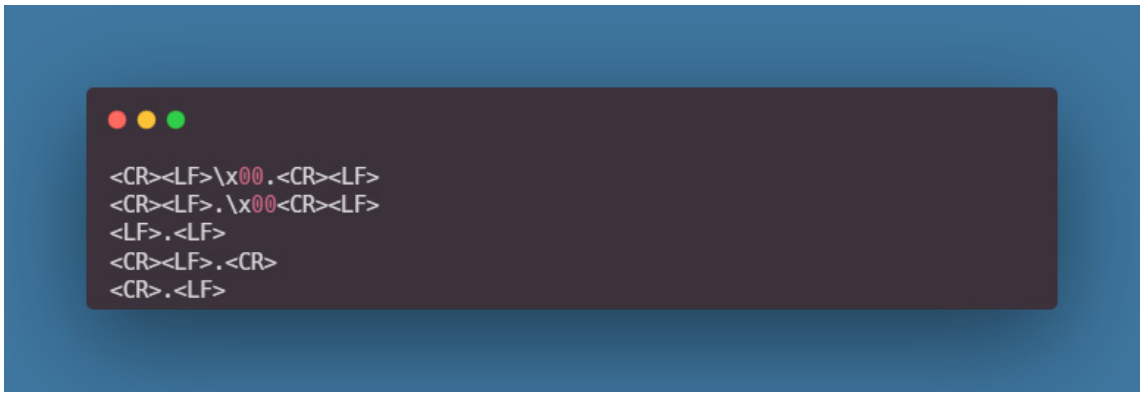


خوب حالا دوباره نگاهی به SPF هدر ها می اندازیم .

بدان معناست که میتوانیم از تمامی دامنه هایی که از Exchange Online استفاده میکنند ایمیل ارسال کنیم .
به عنوان مثال، شکل زیر نشان می‌دهد که چگونه ما می‌توانیم با استفاده از دامنه sec-consult.com ایمیل‌های جعلی ارسال کنیم. این کار نشان می‌دهد که آسیب‌پذیری موجود می‌تواند به طور گسترده‌ای سوءاستفاده شود و امنیت بسیاری از شرکت‌ها را به خطر بیاندازد.

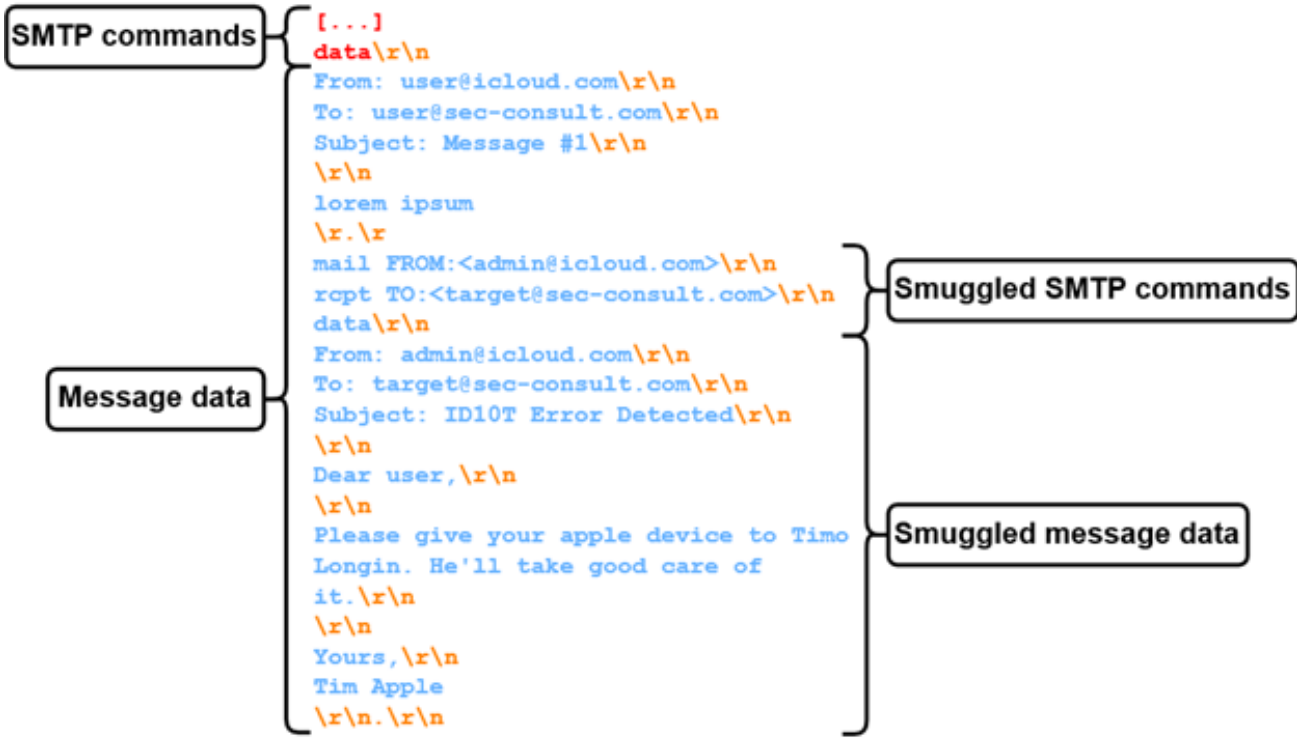


روش هایی دیگر هم هست برای دور زدن این که شاید به فکر شما هم برسد که میتوان از روش های زیر استفاده کرد و روش های خلاقانه ذهن هکر شما .



که به صورت زیر اعمال میشود

و فلوی کلی اسیب پذیری را در تصویر زیر مشاهده میفرمایید .



جزئیات و بهره برداری از آسیب پذیری

برای اکسپولیت دستی این اسیب پذیری از مافاهیم بالا میتوانید کمک بگیرد و برای اسکن کردن آن میتوانید از ابزار SMTP Smuggling Scanner استفاده نمایید .

این ابزار به شما امکان می‌دهد تا (End-of-Data Sequences) که توسط سرورهای SMTP خروجی نادیده گرفته می‌شوند اما توسط سرورهای SMTP ورودی پذیرفته می‌شوند را پیدا کنید. برای مثال، اگر سرور خروجی Exchange Online که به بررسی آن پرداختیم <LF>.<CR><LF> را بدون فیلتر عبور دهد و سرور ورودی آن را به عنوان پایان داده تفسیر کند، می‌توان از این آسیب‌پذیری بهره‌برداری کرد.

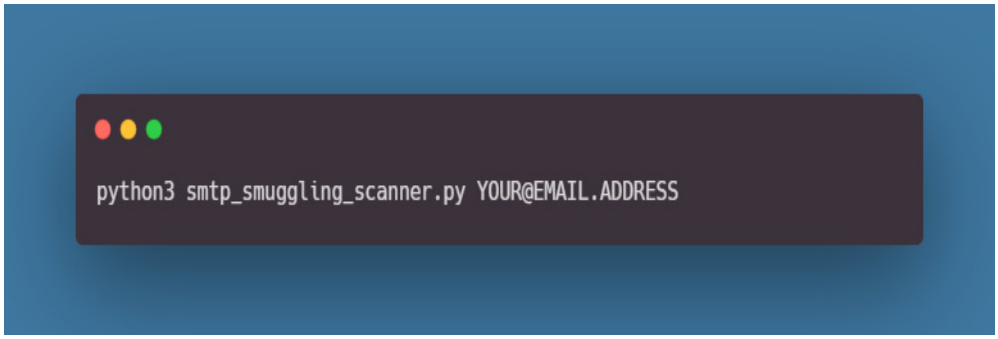
نصب و پیش‌نیازها

```
pip install -r requirements.txt
```

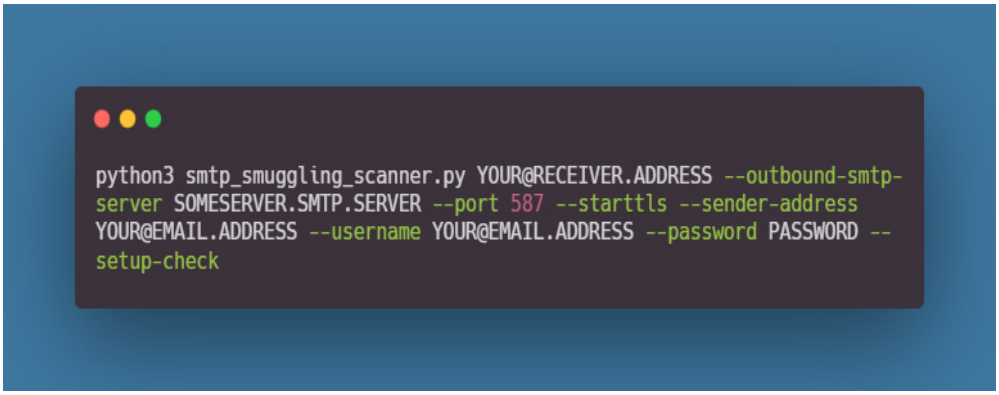
اسکن سرورهای SMTP

```
python3 smtp_smuggling_scanner.py --setup-check YOUR@EMAIL.ADDRESS
```

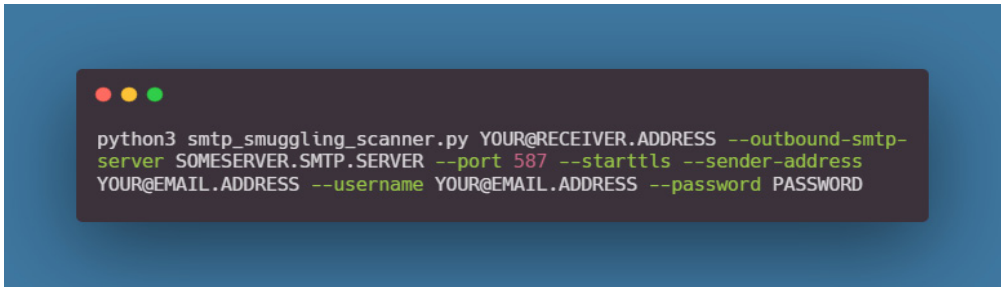
Smuggling Check



اسکن سرورهای SMTP خروج و اون دنباله های پایانی



Smuggling Check و چک کردن تکنیک های دور زدن که برخی از آنها رو توضیح دادم



برای اکسپولیت کردن این آسیب پذیری و آسیب پذیری های دیگر سیع کنید از درک مفهوم به اکسپولیت آن برسید ممنون از شما و همراهیتون تا اینجا .

جلوگیری

نسخه Exim خودرابه اخرین نسخه بروز کنید یا روش هایی که مطرح کردم و از BDAT استفاده کنید و در اخر همیشه بروز باشید و به توصیه های تیم امنیت خود گوش دهید به امید فردایی امن تر تا هفته های بعدی همراه ما باشید .

منابع

- sec-consult.com
- SMTP-Smuggling-Tools
- nvd.nist.gov
- redhat.com
- medium.com