بسمه تعالی

ارزیابی امنیتی سرویس دهنده های پست الکترونیک

فهرست مطالب

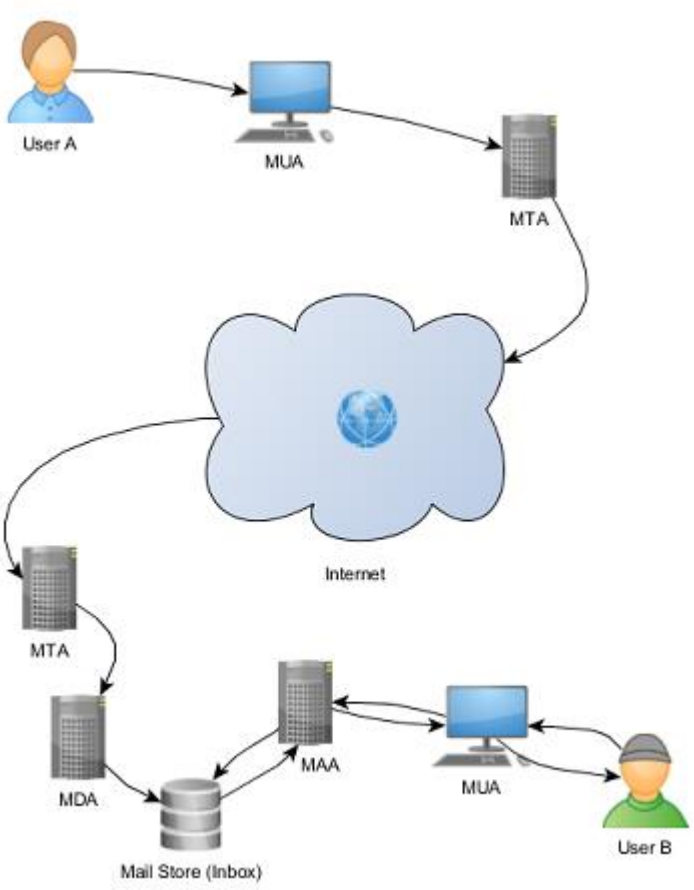
۱ مقدمه

بسیاری از سازمان ها از سرویس پست الکترونیک سازمانی مخصوص به خودشان استفاده می کنند. تامین امنیت سرویس های پست الکترونیکی سازمانی یکی از چالش های امنیتی مهم در کسب و کار آن سازمان به حساب می آید. اگر امنیت یک سرویس پست الکترونیکی به خوبی برقرار نشود مورد سوء استفاده بسیاری از هکر ها قرار می گیرد. یکی از این سوء استفاده های که می توان انجام داد، این است که از یک برنامه نامه بر برای ارسال هرزنامه استفاده کرد. یکی دیگر از سوء استفاده های که می توان انجام داد این است که یک فرد خود را به جای یک فرد دیگری قرار دهد و اقدام به ارسال نامه های الکترونیکی از طرف آن فرد کند. این سوء استفاده ها به خاطر این است که اگر برنامه نامه بر به خوبی پیکره بندی نشده باشد، می توان بدون احراز هویت اقدام به ارسال نامه های الکترونیکی نمود.

از دیگر خطراتی که برای میل سرور یک سازمان وجود دارد این است که اگر میل سرور به درستی پیکره بندی نشده باشد، می توان پیام های میان پروتوکل های مختلف یک میل سرور برای مثال بین پروتکل SMTP و پروتکل POP3 را شنود کرد. و با استفاده از شنود این نوع از اطلاعات می توان داده های حساس کاربران میل سرور را شنود کرد. بنابراین باعث می شود که محرمانگی اطلاعات که یکی از مهمترین ویژگی های سیستم های امنیت اطلاعات می باشد به مخاطره افتد.

۲ معماری سرویس دهنده پست الکترونیک

با توجه به شکل زیر عملیات لازم برای فرستادن ایمیل توسط یک کاربر و دریافت آن توسط شخص دیگر به صورت زیر است:



۱. یک عامل کاربر ایمیل MUA[۱] یک برنامه است که به کاربر اجازه ساخت، ارسال و دریافت ایمیل را می دهد. معمولا به یک MUA یک سرویس گیرنده ایمیل[۲] گفته می شود. Microsoft Outlook نمونه ای از این برنامه ها هستند ولی اکثر MUA ها بصورت برنامه های مبتنی بر وب پیاده سازی می شوند، مانند آنچه که هنگام ورود به Gmail یا Hotmail دیده می شود.

[۱] Mail User Agent
[۲] Mail Client

۲. ایمیل ساخته شده توسط سرویس گیرنده ایمیل به عامل انتقال ایمیل[۳] (MTA) فرستاده می شود. عامل انتقال ایمیل مسئول فرستادن ایمیل به MTA گیرندگان ایمیل می باشد. MTA پیام های پستی را توسط پروتکل SMTP بین دو کامپیوتر انتقال می دهد. Postfix نمونه ای از MTA ها هست.

۳. MTA گیرنده ها، ایمیل را دریافت کرده و آن را به عامل تحویل ایمیل[٤] (MDA) انتقال می دهند. MDA صندوق پست کاربران را مدیریت می کند. Dovecot نمونه ای از یک MDA هست.

٤. علاوه بر MDA از عامل دسترسی ایمیل (MAA[٥]) استفاده می شود که دسترسی راه دور برای خواندن پیام های کاربران را میسر سازد.

۵. گیرنده برای بررسی و دریافت پیغام هایش از MUA استفاده می کند.

۳ احراز هویت برای MDA و MTA

ایمیل سرور را می توان طوری راه اندازی کرد که نیاز به احراز هویت نداشته باشد. به عبارت دیگر فردی می تواند بدون احراز هویت از پروتکل SMTP برای فرستادن ایمیل استفاده کند. در واقع بدون وجود داشتن نام کاربری مشخص می توان باز هم اقدام به ارسال ایمیل کرد. برای مثال وقتی با دستور telnet به پورت ۲۵ متصل شدید (پورت ۲۵ پورتی است که به صورت پیش فرض SMTP از آن استفاده می کند) آنگاه از دستور mail from:<anyuser> برای ارسال ایمیل استفاده کنید. در اینجا anyuser هر کاربری می تواند باشد حتی نام کاربری که در سیستم وجود ندارد. بنابراین بسیاری از افراد بدون آنکه شناخته شوند می توانند با استفاده از این آسیب پذیری برای ارسال اسپم از میل سرور سازمان استفاده کنند.

---

[۳] Mail Transfer Agent
[٤] Mail Delivery Agent
[٥] Mail Access Agent

۴ پروتکل SMTP

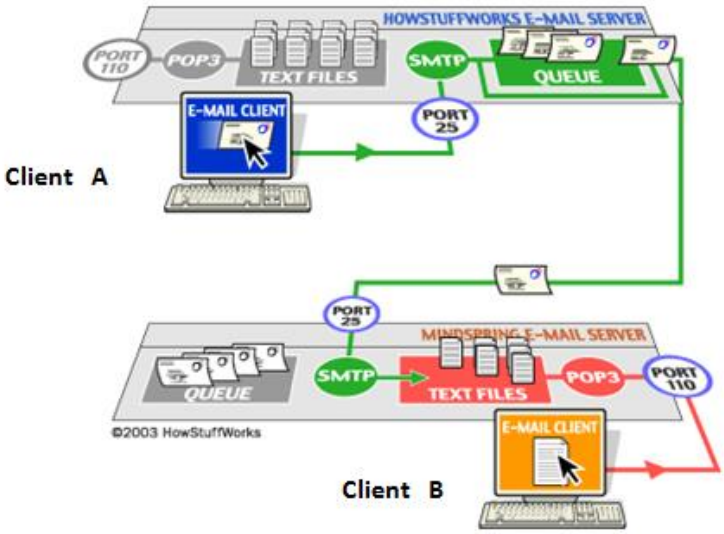
پست الکترونیکی یکی از مهمترین سرویس های اینترنت است که شباهت زیادی به پست معمولی دارد .این سرویس، اتصال غیر هم زمان رابرای افراد پدید می آورد .بدین معنا که افراد هر زمان مایل باشند می توانند اقدام به ارسال و یا مطالعه ی نامه های خود نمایند، بدون این که نیاز باشد این اعمال را با زمان و برنامه ریزی دیگران منطبق کنند .هنگامی که یک نامه ی الکترونیکی ارسال می شود، انتظار این است که سرویس دهنده ی پست الکترونیکی، آن نامه را به درستی به مقصدارسال نماید .مراحل ارسال بدون توجه به سخت افزار و نرم افزار و تنها با استفاده از پروتکل های انتقال پست الکترونیکی انجام می شود.

SMTP مهمترین پروتکل انتقال پست الکترونیکی می باشد. پروتکل SMTP مخفف **SIMPLE MAIL TRANSFER PROTOCOL** بوده که از این پروتکل برای ارسال پیام‌های الکترونیکیE-mail استفاده می‌شود. . تا قبل از آن از پروتکل UUCP(Unix-to-Unix Copy) برای ارسال پیام‌های الکترونیکیE-mail استفاده می‌شد.

این پروتکل دارای ویژگی های بسیار زیادی است که آن را به یکی از مهمترین پروتکلهای اینترنت تبدیل کرده است .اما با این وجود، این پروتکل محدودیت هایی از قبیل محدودکردن بدنه ی نامه های الکترونیکی به هفت بیت کد اسکی را از زمان گذشته با خود به همراه دارد .این محدودیت تا اوایل دهه1980 میلادی که انتقال و ارسال نامه های الکترونیکی بسیار کم و به ندرت بود، مشکلی ایجاد نمی کرد .اما امروزه و در عصر رسانه های چند منظوره، محدودیت هفت بیت کد اسکی دردسرساز است .زیرا نیاز دارد که داد ه های مالتی مدیای باینری، قبل از ارسال از طریق SMTPبه کد اسکی تبدیل شوند و پس از انتقال از طریق این پروتکل از اسکی به باینری برگردانده شوند.

پروتکل smtp به دلیل محدودیت‌هایی در نگهداری نامه‌ها، معمولا با پروتکل‌های POP3 یا (post office protocol3) یا IMAP (internet message access protocol) استفاده می‌شود که برای کاربران امکان ذخیره نامه‌ها را روی یک سرور یا دانلود آنها را از سرور فراهم می‌کند. در حقیقت می‌توان گفت، SMTP برای ارسال نامه‌ها و POP3 یا IMAP برای دریافت نامه‌ها به کار می‌روند. به عبارت ساده‌تر، سرور SMTP، مانند وب سرور یک رایانه است که مانند مسیریاب عمل می‌کند. هنگامی که پیام‌های پست الکترونیکی از کاربران را دریافت می‌کند آنها را به گیرندگان مورد نظر می‌فرستند. SMTPفقط به نام کاربری و دامنه نیاز دارد تا مستقیم پیغام را به سمت گیرنده مسیریابی کند و به طور پیشفرض بر روی پورت ۲۵ قرار دارد. البته مدیران سرور برای افزایش امنیت می توانند پورت آن را تغییر دهند.

سناریوی زیر عملیات پروتکل SMTP را به تصویر میکشد:



فرض کنید client Aمیخواهد یک نامه الکترونیکی ساده را به client B ارسال کند:

- clientA آدرس پست الکترونیکی clientB را در کارگزار کاربر(user agent) خود وارد کرده و پس از نوشتن نامه ی الکترونیکی، آن را ارسال مینماید.
- لازم به ذکر است که کارگزار کاربر (user agent) برنامه ای است که محیطی را برای نوشتن، خواندن، ارسال و دریافت نامه های الکترونیکی فراهم می کند.
- (user agent) clientA نامه را در صف نامه های سرویس دهنده ی پست الکترونیکی وی قرار می دهد.
- سرویس دهنده ی پست الکترونیکی clientA یک اتصالTCP با سرویس دهنده ی پست الکترونیکی clientB ایجاد می کند.
- پس از برقراری اتصال TCP نامه ی clientA از طریق آن اتصال منتقل میگردد.
- نامه ی ارسال شده از طریق سرویس دهنده ی پست الکترونیکی clientB دریافت شده و در فهرست نامه های clientB قرار می گیرد.
- clientB از طریق کارگزار کاربر خود نامه دریافتی را میخواند.

توجه به این نکته ضروری است که پروتکل SMTP برای ارسال نامه های الکترونیکی از سرویس دهندگان پست الکترونیکی میان مبداو مقصد استفاده نمی کند، حتی اگر دو سرویس دهنده ی مذکور در فاصله ی بسیار دوری از یکدیگر قرار داشته باشند .به عنوان مثال، اگر سرویس دهنده ی پست الکترونیکی clientA در ایران و سرویس دهنده ی پست الکترونیکی clientB درآلمان باشد، اتصال TCP مستقیما بین ایران و آلمان برقرار می گردد منظور از این جمله به طور دقیق تر این است که چنانچه سرویس دهنده ی پست الکترونیکی clientB دردسترس نباشد، نامه در سرویس دهنده ی پست الکترونیکیclientA باقی مانده و این سرویس دهنده سعی در برقراری اتصال مجدد با سرویس دهنده ی باب می نماید و نامه به هیچ وجه در سرویس دهندگان پست الکترونیکی میانی قرار نمی گیرد.

۵ تست رله باز

یکی از حفره های امنیتی در سرویس دهنده های پست الکترونیک باز بودن رله است. به این معنی که هر کسی از طریق میل سرور شما قادر خواهد بود به بیرون میل بفرستد بدون اینکه احراز هویت شود. این امر باعث خواهد شد که میل سرور به یک منبع ارسال کننده اسپم تبدیل شود و نتیجتا باعث قرار گرفتن ip میل سرور در blocklist ها می شود که این امر باعث تحویل داده نشدن ایمیل هایی می شود که از سرور شما ارسال می شود.

۶ استفاده از nmap

انمپ یک ابزار رایگان و متن باز است که برای کاوش و بررسی های امنیتی در شبکه به کار می‌رود . بسیاری از سیستم‌ها و مدیران شبکه نیز این ابزار را برای انجام وظایفی مثل اکتشاف شبکه ، مدیریت برنامه ارتقا سرویس ها و مانیتور میزبان ها یا آپتایم سرویس ها مفید می‌دانند.

انمپ از بسته های خام آیپی (Raw IP Packets) به شیوه ای جدید به منظور تشخیص اینکه چه میزبان هایی در شبکه وجود دارند استفاده می‌کند . اینکه چه سرویس هایی این میزبان ها ارایه می‌کنند . اینکه چه سیستم عاملی بر روی این میزبان ها قرار دارد و چه نوع فایروال بسته استفاده شده و ... موارد زیاد دیگری از این دست . انمپ به گونه‌ای طراحی شده است که شبکه‌های بزرگ را به صورت مستقیم اسکن کند ولی در میزبان های کوچک نیز کاربردی می‌باشد . یکی از ویژگی‌های برتر انمپ Nmap این است که بر روی همه سیستم عامل های بزرگ قابل اجرا می‌باشد و کد باینری آن برای تمامی سیستم عامل های بزرگ مثل لینوکس ، اپل و ویندوز موجود است.

موتور اسکریپت نویسی انمپ (Nmap Scripting Engine) که به اختصار NSE نامیده می شود قابلیت‌ها و امکاناتی را به یک اسکنر پورت ارایه می‌کند. این قابلیت ها و امکانات به کاربران به منظور نوشتن اسکریپت های اختصاصی برای انجام وظایف گوناگون کمک می کند.

۷ اسکریپت smtp-open-relay

این اسکریپت از دستورات SMTP استفاده می کند تا وجود آسیب پذیری رله باز را تشخیص دهد. این اسکریپت آرگومان های زیر را دارد:

smtp-open-relay.ip: این آرگومان آدرس IP ایمیل سرور را مشخص می کند.

smtp-open-relay.domain: این آرگومان دامنه ایمیل سرور را مشخص می کند.

smtp-open-relay.from: این آرگومان آدرس فرستنده ایمیل را مشخص می کند.

smtp-open-relay.to: این آرگومان آدرس گیرنده ایمیل را مشخص می کند.

اسکریپت smtp-open-relay از ترکیب های مختلف آرگومان های بالا استفاده می کند تا ۱۶ تست را از روی آنها بسازد. هر کدام از این تست ها موفقیت آمیز بود آنگاه ایمیل سرور آسیب پذیری رله باز را دارد. این تست ها به صورت زیر می باشند(لازم به ذکر است که متغیرهای ip، domain، from وto درتست های زیر به ترتیب برابر آرگومان های smtp-open-relay.ip، smtp-open-relay.domain، smtp-open-relay.from و smtp-open-relay.to می باشد:

```
local tests = {
    {
      from = "",
      to = string.format("%s@%s", to, domain)
    },
    {
      from = string.format("%s@%s", from, domain),
      to = string.format("%s@%s", to, domain)
    },
    {
      from = string.format("%s@%s", from, srvname),
      to = string.format("%s@%s", to, domain)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("%s@%s", to, domain)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("%s%%%s@[%s]", to, domain, ip)
```

```
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("%s%%%s@%s", to, domain, srvname)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("\"%s@%s\"", to, domain)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("\"%s%%%s\"", to, domain)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("%s@%s@[%s]", to, domain, ip)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("\"%s@%s\"@[%s]", to, domain, ip)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("%s@%s@%s", to, domain, srvname)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("@[%s]:%s@%s", ip, to, domain)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("@%s:%s@%s", srvname, to, domain)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("%s!%s", domain, to)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("%s!%s@[%s]", domain, to, ip)
    },
    {
      from = string.format("%s@[%s]", from, ip),
      to = string.format("%s!%s@%s", domain, to, srvname)
    },
  }
```

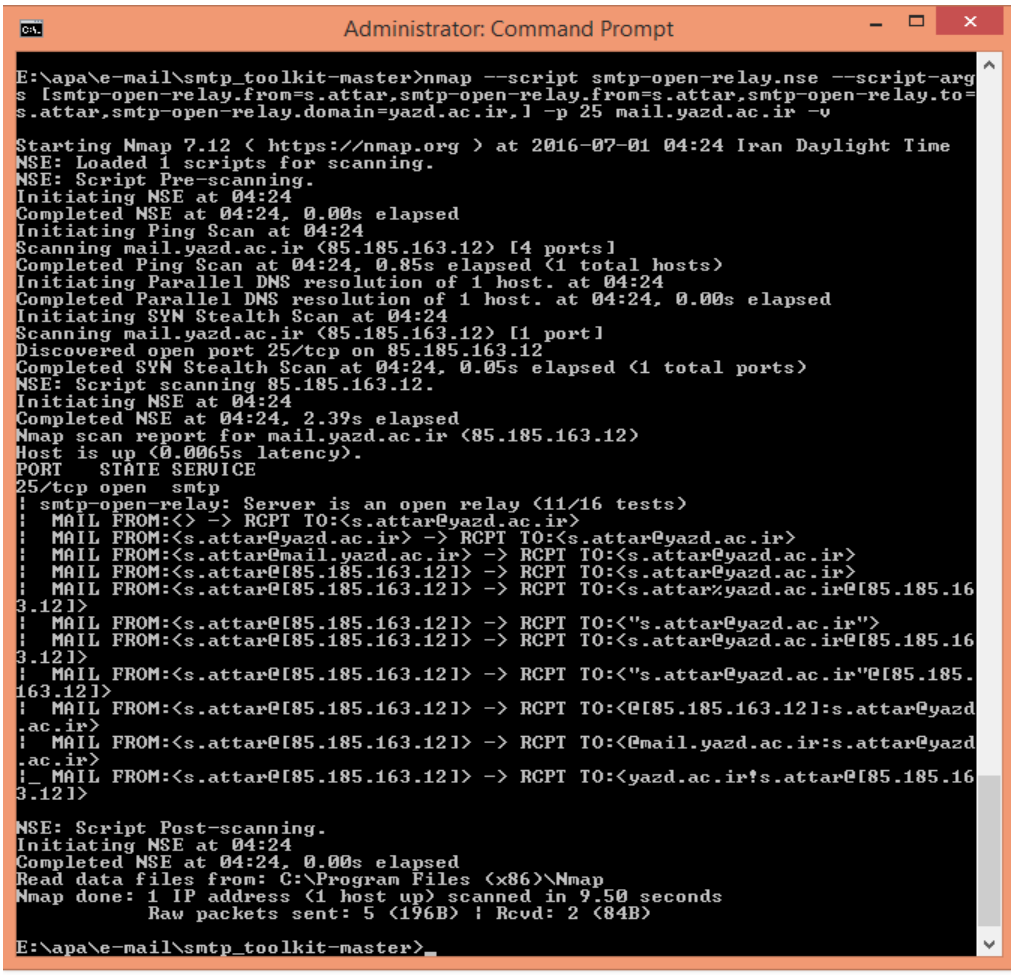
نکته ی مهم در استفاده از این اسکریپت تعیین آرگومان های درست می باشد و الا هیچ یک از این تست ها جواب نخواهد داد. در واقع استفاده از این اسکریپت نیاز به شخصی سازی برای هر ایمیل سرور دارد و نمی شود آرگومان های کلی را برای هر ایمیل سرور در نظر گرفت. اگر مقدار آرگومان های بالا برای همه ی ایمیل سرور ها را یکی در نظر بگیریم باعث می شود که تست رله باز fail شود. علت اینکه وقتی سازمان ها نیز از این ابزار های آنلاین استفاده می کنند و جواب تست رله باز منفی برای ایمیل سرور سازمان خود می گیرند نیز همین نکته است. برای استفاده از این اسکریپت لازم است که دستور زیر را به کار برد:

```
nmap --script smtp-open-relay.nse [--script-args smtp-open-relay.domain=<domain>,smtp-open-relay.ip=<address>,...] -p 25,465,587 <host>
```

دستور بالا را برای پیدا کردن این آسیب پذیری در دانشگاه یزد به صورت زیر استفاده می کنیم :

```
nmap --script smtp-open-relay.nse --script-args [smtp-open-relay.from=s.attar,smtp-open-relay.from=s.attar,smtp-open-relay.to=s.attar,smtp-open-relay.domain=yazd.ac.ir,] -p 25 mail.yazd.ac.ir -v
```

شکل زیر دستور بالا را برای پیدا کردن آسیب پذیری رله باز را در دانشگاه یزد را نشان می دهد:



۸ جمع بندی

در این گزارش ما به صورت کلی ایمیل سرور ها و به ویژه پروتکل SMTP را توضیح دادیم. درادامه توضیحاتی در مورد نرم افزار nmap و علی الخصوص موتور اسکریپت نویسی آن ارائه شد. با استفاده از موتور اسکریپت

نویسی nmap به بررسی آسیب پذیری open relay پرداختیم. در نهایت این اسکریپت را بر روی ایمیل سرور دانشگاه یزد تست کردیم.