بسمه تعالی

# ارزیابی امنیتی سرویس دهنده های پست الکترونیک

## عدم انطباق در dns معکوس در سرویس های پست الکترونیک

## (SMTP Reverse DNS Mismatch)

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 پست الکترونیک و کاربردها

امروزه مکانیزه و هوشمند سازی فعالیت‌های اداری در سازمان‌ها بسیار حائز اهمیت است. یکی از اجزا و ابزارهای اساسی و لاینفک سامانه‌های اداری در هر اداره و سازمانی پست الکترونیکی می باشد. اهمیت این ابزار به حدی رسیده است که گاه از آن به عنوان ابزاری رده بالا جهت انتقال اطلاعات حساس از جمله نامه‌های محرمانه و ... استفاده می‌شود. با وجود آنکه ابزارهای مختلف و متعدد فناوری اطلاعات جهت بهبود عملیات اداری در سازمان‌ها توسعه داده شده است و پست الکترونیکی از این حیث جزو ابزارهای قدیمی محسوب می‌شود اما این مساله باعث کاهش اهمیت آن نشده است. در زیر برخی از دلایلی را که باعث شده‌است این ابزار همچنان به طور گسترده مورد توجه و کارکرد قرار گیرد، بررسی می‌کنیم:

- پست الکترونیکی ساختاری قابل اعتماد دارد که رسیدن پیام به مخاطب را تا حد زیادی تضمین می‌کند.

- پروتکل پست الکترونیکی یک پروتکل عمومی است که در اختیار همه سازمان‌هاست در نتیجه ارتباط بین سازمانی به راحتی و بدون نیاز به هیچ گونه همگام سازی فناورانه بین سازمان‌های مختلف امکان برقراری ارتباط میان سازمانی را فراهم می‌کند. این مساله دست سازمان را برای استفاده از این ابزار صرفا در سطح سازمانی یا برای ارتباط بین سازمانی باز می‌گذارد.
- پیاده سازی نرم‌افزاری، سخت‌افزاری و نگهداری سامانه‌های پست الکترونیکی ساده و کارآمد است.

مجموعه عوامل و دلایل بالا در کنار برخی دلایل دیگر باعث شده است که با وجود توسعه فناوری‌های جدید و به روزتر همچنان پست الکترونیکی به عنوان یک ابزار سازمانی به کار خود ادامه دهد.

اما اگر بخواهیم کاربردهای پست الکترونیک در سازمان‌ها را بررسی کنیم می‌توان موارد بسیاری را شمرد که برخی از آن‌ها از این قرار هستند:

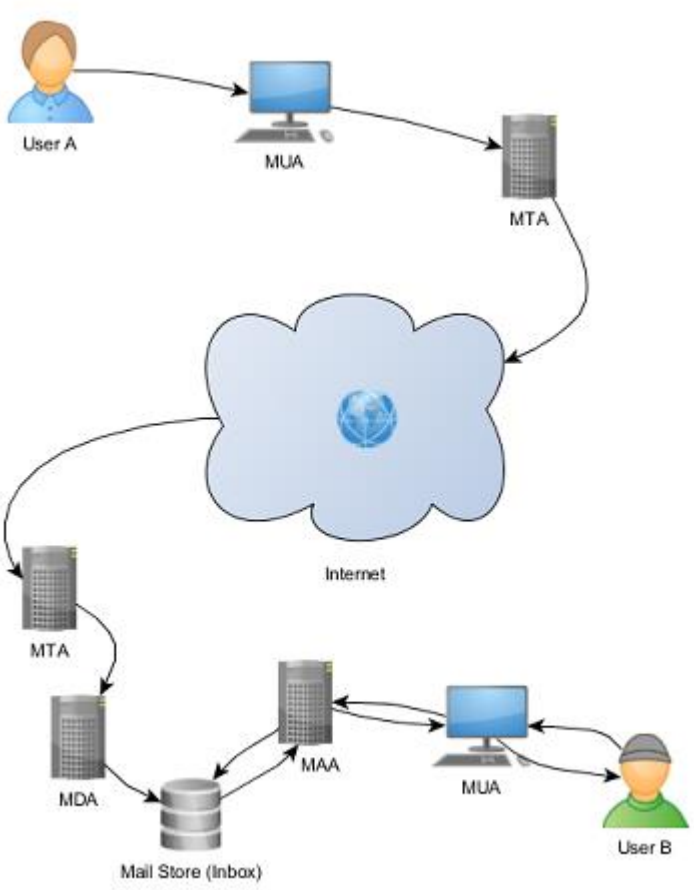
- ارسال اطلاعات و مدارک به صورت عمومی برای تعداد زیادی از افراد
- ارسال اطلاعات و مدارک به صورت خودکار و هوشمند با اتصال سامانه‌های خودکار به سیستم
- استفاده از پروتکل پست الکترونیکی به عنوان زیرساخت سامانه‌های نرم افزاری نظیر اتوماسیون اداری
- استفاده از آدرس پست الکترونیک برای ارسال اطلاعات به عنوان یک امضای تایید هویت

در مورد کاربرد آخر باید این توضیح را ارئه کرد که آدرس پست الکترونیک چه برای افراد و چه برای سازمان‌ها یک ابزار احراز هویت محسوب می‌شود به این معنا که گیرنده، صحت فرستنده پیام را از روی آدرس پست الکترونیکی فرستنده بررسی می‌نماید. این مساله چه در ارتباطات درون سازمانی (نظیر ارسال اطلاعات از طرف یک مدیر بالادست) و چه در ارتباطات بین سازمانی اهمیت به سزایی دارد.

با در نظر گرفتن نقش پررنگی که پست الکترونیکی در سازمان‌ها ایفا می‌کند می‌توان به اهمیت این ابزار پی برد. یکی از ملزومات چنین ابزار مهمی تامین امنیت آن است.

# ۳ 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.

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

# ۴ DNS Server چیست

ساناد سرواژه‌ی **سامانه‌ی نام دامنه** (به انگلیسی:Domain Name System )، به اختصار (DNS) خوانده می‌شود. DNS یک سیستم سلسه‌مراتبی نام‌گذاری برای کامپیوترها، سرویس‌ها، و یا هر منبع دیگری که به شبکه اینترنت و یا یک شبکه خصوصی (LAN) متصل بوده، می‌باشد. وقتی می‌خواهید وارد وبگاهی شوید، باید نشانی کارساز وبش را بدانید. نشانی کارساز وب با نشانی آی‌پی مشخص می‌شود. اما به خاطر سپردن نشانی آی‌پی، دشوار است. می‌توان به جای نشانی آی‌پی، از نام‌های دامنه استفاده کرد. برای هر نشانی آی‌پی یک نام دامنه در نظر گرفته شده‌است. مثلاً نشانی آی‌پی وبگاه گوگل ۱۷۳,۱۹٤,۳۳,۱۰٤ است. برای دسترسی به گوگل، می‌توانید از این نشانی آی‌پی یا نام دامنه آن یعنی www.google.com استفاده کنید.

در ساناد، کل نشانی‌های اینترنت درون بانک‌های اطلاعاتی توزیع شده‌ای هستند که هیچ تمرکزی روی نقطه‌ای خاص از شبکه ندارند. روش ترجمه‌ی نام بدین صورت است که وقتی یک برنامه‌ی کاربردی مجبور است برای

---

[۳] Mail Transfer Agent
[۴] Mail Delivery Agent
[۵] Mail Access Agent

برقراری یک ارتباط، معادل نشانی آی‌پی از یک ماشین با نامی مثل cs.ucsb.edu را بدست بیاورد، قبل از هر کاری یک تابع کتابخانه‌ای (به انگلیسی: Library Function ) را صدا می‌زند، به این تابع کتابخانه‌ای تابع تحلیلگر نام (به انگلیسی Name Resolver) گفته می‌شود.

تابع تحلیلگر نام یک نشانی نمادین را که بایستی ترجمه شود، بعنوان پارامتر ورودی پذیرفته و سپس یک بسته‌ی درخواست به انگلیسی: (Query Packet ) به روش UDP تولید کرده و به نشانی یک کارساز DNS (که به صورت پیش فرض مشخص می‌باشد) ارسال می‌کند. همه ی ماشین‌های میزبان، حداقل باید یک نشانی آی‌پی از یک سرویس دهندهی ساناد را در اختیار داشته باشند. این «سرویس دهندهی محلی» پس از جستجو، نشانی آی‌پی معادل با یک نام نمادین را بر می‌گرداند.

DNS server دارای دو قسمت به نام های forward lookup zone و reverse lookup zone هست که هر کدام وضیفه خاصی دارند .Revers lookup zone مربوط به ترجمه اسم به ای پی و Forward lookup zone مربوط به ترجمه ای پی به اسم هست.

### ۴–۱ Forward lookup zone

این zone اطلاعات تبدیل اسم دامنه به آدرس آی پی را در بردارد. آدرسی مثل www.subnet.ir را FQDN (Fully Qualified Domain Name) میگویم که subnet.ir اسم دامنه و www اسم هاست میباشد. پس به تعبیری دیگر forward lookup zone عمل تبدیل FQDN را به آی پی بر عهده دارد. host record ها در forward lookup zone قرار دارند.

### ۴–۲ Reverse lookup zone

این zone حاوی آدرس آی پی برای هاست و یکpointer (اشاره گر) برای host record ها در forward lookup zone میباشد.

## ۵ انواع رکوردها در DNS SERVER ها

در DNS server میشود رکوردهایی مثل A , NS, TXT , CNAME , MX, PTR و پارامتر SOA را تنظیم کرد. رکورد های رایج در زیر توضیح داده شده است.

### ۵–۱ A Record:

A Recordیا (Host Record) یک دامنه را به یک IP فیزیکی کامپیوتری که آن دامنه را میزبانی میکند مرتبط میکند.

رکوردی مشابه این رکورد به نام AAAA Record برای IPv6 وجود دارد.

### ۵-۲ PTR Record:

رکورد اشاره گر (Pointer Record) اطلاعات لازم برای Reverse DNS را فراهم می آورد که به منظور واقعه نگاری (Logging) و تطبیق (Verification) نام دامنه بکارگرفته می شود. همچنین با نام Inverse DNS شناخته می شود.

### ۵-۳ NS Record:

NSیا Name server رکورد هایی هستند که تعیین میکنند که کدامیک از سرور ها دارای اطلاعات دامنه مورد نیاز هستند. به طور مثال دی ان اس ir. دارای NS رکورد ac.ir هست و هروقت کاربر از سرور DNS خود درخواست سایت ut.ac.ir نماید، سرور DNS اول به ir. مراجعه میکند سپس به وسیله ی NS رکورد موجود در سرور ir. به سرور ac.ir که حاوی ut.ac.ir هست مراجعه میکند.

### ۵-۴ MX Record:

MX مخفف کلمه‌ی Mail Exchanger است. MX Record مسئول شناسایی ایمیل سرور(ها) برای دامنه است. زمانی که شما ایمیلی را به user@xyz.com ارسال می‌کنید، ایمیل سرور شما باید ابتدا دنبال MX Recordبرای دامنه xyz.com بگردد که ببیند اکنون کدام ایمیل سرور xyz.com را مدیریت می‌کند. در مرحله‌ی بعدی به دنبال A Record برای ایمیل سرور می‌گردد تا به IP ان متصل شود.

### ۵-۵ TXT Record:

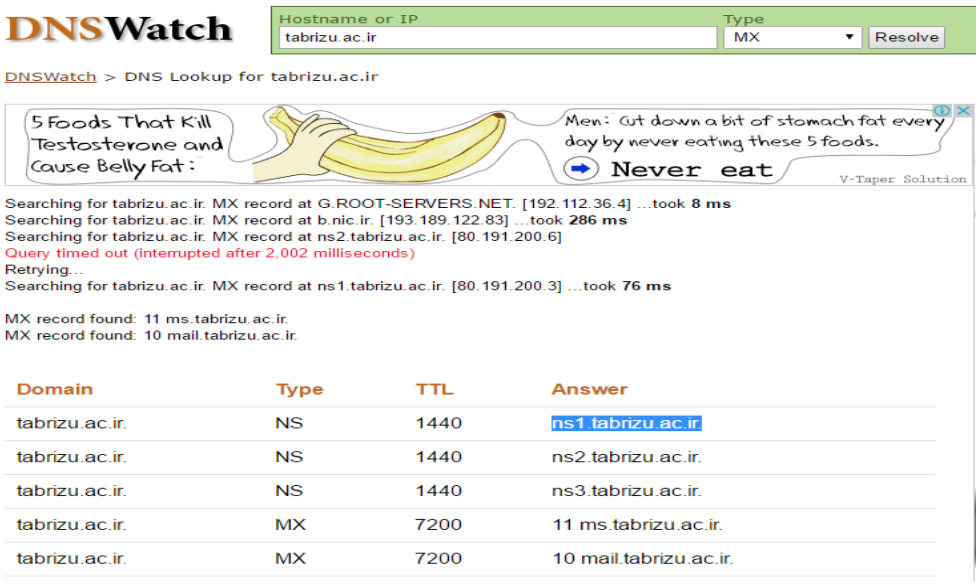
یک رکورد TXT اطلاعات متنی به منابع خارج از دامنه فراهم میکند که این اطلاعات میتواند متن خواندنی توسط ماشین ویا انسان باشد.

# ۶ عدم انطباق در dns معکوس در سرویس دهنده های پست الکترونیک

بسیاری از ایمیل سرور ها بر روی اینترنت طوری پیکره بندی شده اند تا ایمیل های ورودی مربوط به آی پی هایی که DNS معکوس را ندارند را قبول نکنند. بنابراین لازم است تا سازمان هایی که ایمیل سرور را خود راه اندازی می نمایند، DNS معکوس را نیز در نظر بگیرند. لازم به ذکر است بسیاری از ابزار های تست اسپم نیز از تست عدم انطباق برای تشخیص اسپم استفاده می نمایند.

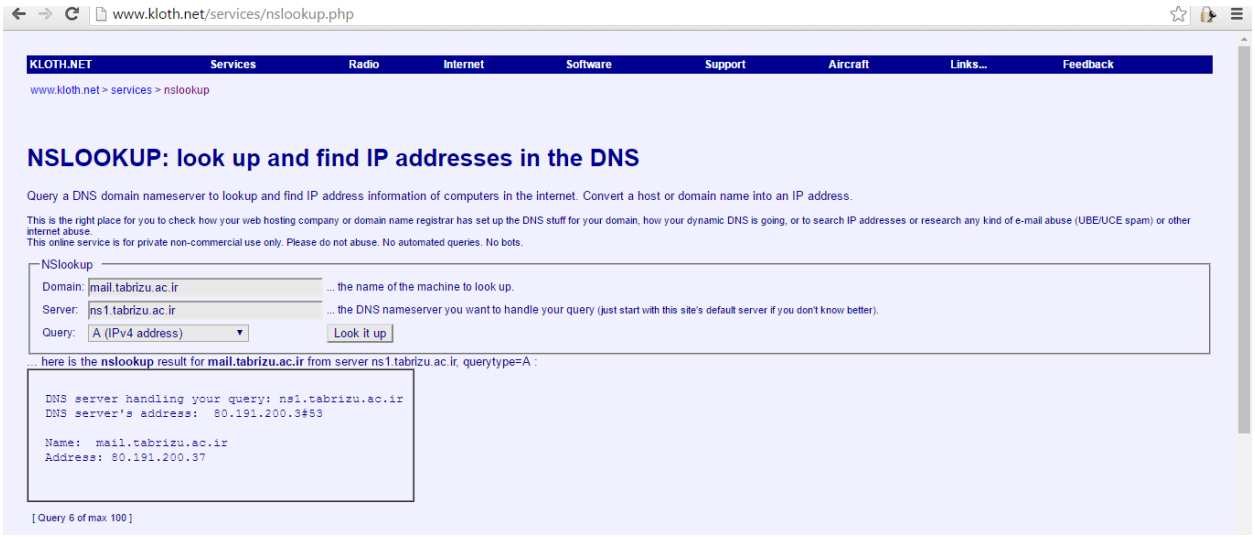
# ۷ نحوه ی تست کردن عدم انطباق در dns معکوس در سرویس دهنده های پست الکترونیک

فرض کنید که می خواهیم بررسی عدم انطباق در سرویس دهنده های پست الکترونیک دانشگاه تبریز را انجام دهیم. آدرس های ایمیل دانشگاه تبریز به صورت x@tabrizu.ac.ir می باشد. بنابراین از دامنه tabrizu.ac.ir استفاده می کنیم و یک پرس و جوی dns از نوع MX انجام می دهیم تا سروری را که مسئول ایمیل سرور است مشخص شود. این پرس و جو در شکل زیر نشان داده شده است. برای این کار از سایت dnswatch.info استفاده شده است.



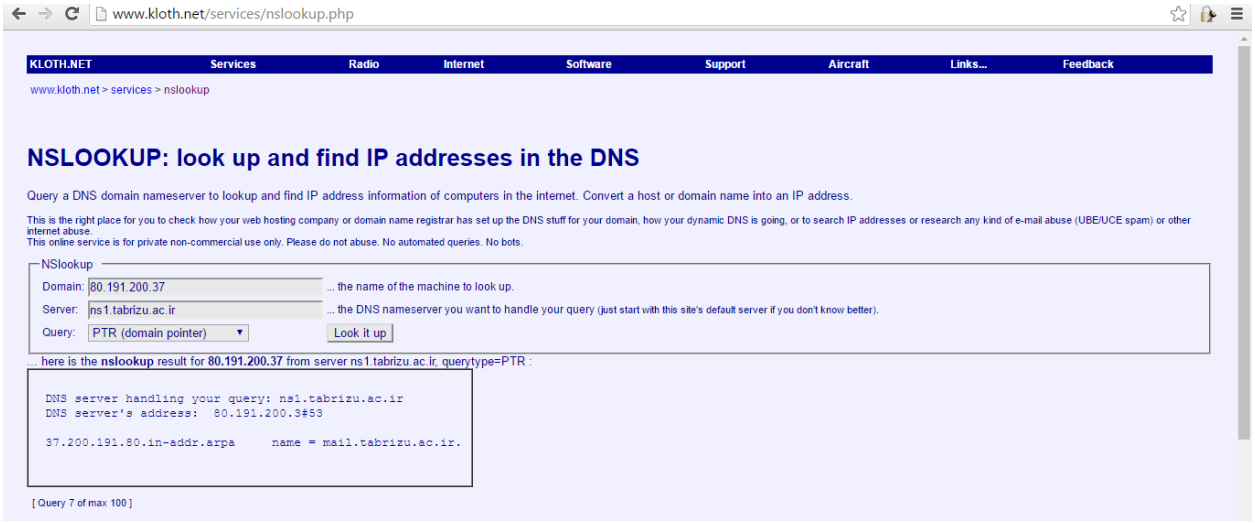

همان طور که در شکل بالا نشان داده شده است، NS رکوردهای دانشگاه تبریز ns1.tabrizu.ac.ir، ns2.tabrizu.ac.ir، ns3.tabrizu.ac.ir و MS رکوردهای دانشگاه تبریز که مسئول ایمیل سرور دانشگاه تبریز می باشد با نام های mail.tabrizu.ac.ir و ms.tabrizu.ac.ir مشخص شده اند.

برای پیدا کردن A رکورد دامنه mail.tabrizu.ac.ir را در قسمت domain و ns1.tabrizu.ac.ir را در قسمت server در سایت http://www.kloth.net/services/nslookup.php که یک ابزار nslookup آنلاین می باشد را وارد می نماییم. نتیجه در شکل زیر نشان داده شده است.




همان طور که در شکل بالا نشانA رکورد دامنه mail.tabrizu.ac.ir را به آی پی 80.191.200.37 بر می گرداند. تا اینجا آی پی آدرس مربوط به ایمیل سرور دانشگاه تبریز را بدست آوردیم. برای تست عدم انطباق ابتدا باید PTR رکورد مربوط به آی پی 80.191.200.37 بدست آورد و سپس باید با A رکورد خروجی PTR رکورد مقایسه کرد و اگر جواب ها یکی بود تست عدم انطباق موفقیت آمیز بوده است.

برای اینکه ببینیم که آی پی 80.191.200.37 به چه دامنه ای تبدیل می شود در همین سایت آی پی 80.191.200.37 را در قسمت سرور وارد می نماییم و رکورد را از نوع PTR انتخاب می نماییم. نتیجه در زیر نشان داده شده است.




همان طور که در شکل بالا نشان داده شده است آی پی 80.191.200.37 به دامنه mail.tabrizu.ac.ir تبدیل شده است. اکنون لازم است که ببینیم دامنه mail.tabrizu.ac.ir به چه اِی پی تبدیل می شود که همان طور که قبلا نشان داده شد به آی پی 80.191.200.37 تبدیل می شود.

همان طور که مشاهده شد دامنه mail.tabrizu.ac.ir به آی پی 80.191.200.37 و آی پی 80.191.200.37 به دامنه mail.tabrizu.ac.ir تبدیل شد. بنابراین این ایمیل سرور حاوی عدم انطباق نمی باشد.

# ۸ - جمع بندی

در این گزارش ما به صورت کلی ایمیل سرور ها را توضیح دادیم. درادامه توضیحاتی در مورد DNS و Reverse DNS و انواع آن را بررسی کردیم. سپس به بررسی عدم انطباق در dns معکوس در ایمیل سرور ها پرداختیم و

چگونگی انجام این تست را برای ایمیل سرور دانشگاه تبریز را توضیح دادیم.

# ۹