بسمه تعالی

امنیت در دسترسی به رایانه از راه دور
Remote Connection Security

فهرست مطالب

۱. مقدمه ۲

۲. امنیت در RDP ۲

۳. استفاده از One Time Password ۵

۴. استفاده از انواع VPN ها ۵

۱. مقدمه

یکی از مباحث مهم در دنیای کامپیوتر، دسترسی به سیستم از راه دور می باشد. در بسیاری از مواقع ما احتیاج داریم که به صورت Remote به کامپیوتر شرکت و یا محل زندگی خود دسترسی داشته باشیم. حال روشهای مختلفی برای این کار ابداع شده است که در برخی از این گونه دسترسی ها، شخص می تواند به صورت GUI به سیستم خود از راه دور دسترسی داشته باشد و در برخی موارد دیگر هم می توان به سیستم خود از راه دور به صورت Command دسترسی داشت.

حال که روشهای مختلفی برای این کار وجود دارد، بحث مهمی که این میان به وجود می آید، امنیت این سیستم های دسترسی از راه دور می باشد. اگر شخصی بتواند از این گونه دسترسی ها به صورت غیرمجاز استفاده کند و یا اینکه بتواند اطلاعات حساس کاربرانی را که در حال استفاده از این سیستم هستند را بدزدد، استفاده از این گونه سیستم ها خطرناک خواهد بود. حال متخصصان دنیای امنیت راه هایی را برای امن کردن این سیستم دسترسی از راه دور پیشنهاد می دهند که در ادامه به بررسی این پیشنهادها می پردازیم.

۲. امنیت در RDP

همانطور که می دانید، سرویس Remote Desktop در سیستم عامل های ویندوز به خودی خود دارای یک رمزنگاری قوی اطلاعات و Packet های درحال رد و بدل در شبکه می باشد. اما در این میان مباحث امنیتی هم وجود خواهد داشت. به عنوان نمونه، یک ضعف امنیتی که بر روی نسخه های ویندوز سرور ۲۰۰۳ و ۲۰۰۸ وجود داشت که بر روی این سرویس RDP بود باعث می شد که امکان شنود ترافیک از جانب نفوذگران وجود داشته باشد.. در همین راستا به مواردی در مورد امنیت در استفاده از سرویس RDP می پردازیم.

- **به روز رسانی**

یکی از مباحث مهم، به روز رسانی سیستم عامل ویندوز می باشد. توسط این کار، نقطه های ضعف امنیتی کشف شده بر روی سیستم عامل به صورت خودکار توسط وصله های امنیتی منتشر شده توسط کمپانی مایکروسافت پوشش داده خواهند شد.

- **استفاده از گذرواژه قوی**

همواره سعی کنید که از گذرواژه های قوی استفاده کنید. منظور از گذرواژه قوی، یک گذرواژه شامل ترکیبی از حروف کوچک و بزرگ، اعداد، کاراکترهای غیر متعارف و همچنین طول گذرواژه بیشتر از ۱۰ کاراکتر می باشد. به عنوان نمونه، در زیر یک گذرواژه قوی را مشاهده می فرمایید:

!amiR66%13_(95)#

- **استفاده از دیوارآتش**

یکی از راه های خوب جلوگیری از حملات علیه سرویس RDP استفاده از دیوار آتش می باشد. استفاده از این دیوار آتش می تواند به ۲ صورت امکان پذیر باشد. یکی اینکه اولا بجز Port 3389 که مخصوص سرویس RDP است، دیگر پورت های روی سرور را بسته نگاه داریم تا آسیبی از این جهت به سرور ما وارد نشود. دوم اینکه می توان محدودیت اتصال IP را بر روی پورت انجام

داد. بدین صورت که تنها اجازه داد که از طریق یک IP خاص به سرویس RDP متصل شد. با این کار می توان از دسترسی های غیر مجاز به سرویس RDP جلوگیری کرد.

- **استفاده از NLA**

در نسخه های ویندوز Vista، Windows7 و Windows 2008 یک لایه امنیتی جدید به نام Network Level Authentication یا همان NLA به ویندوز اضافه شد که جهت برقرای یک ارتباط امن تر بین ویندوز سرور و client می باشد. اما اگر شخصی به عنوان client از ویندوز XP SP3 استفاده کند، برای بهره گیری از سیستم جدید NLA به راهنمای زیر مراجعه کند:

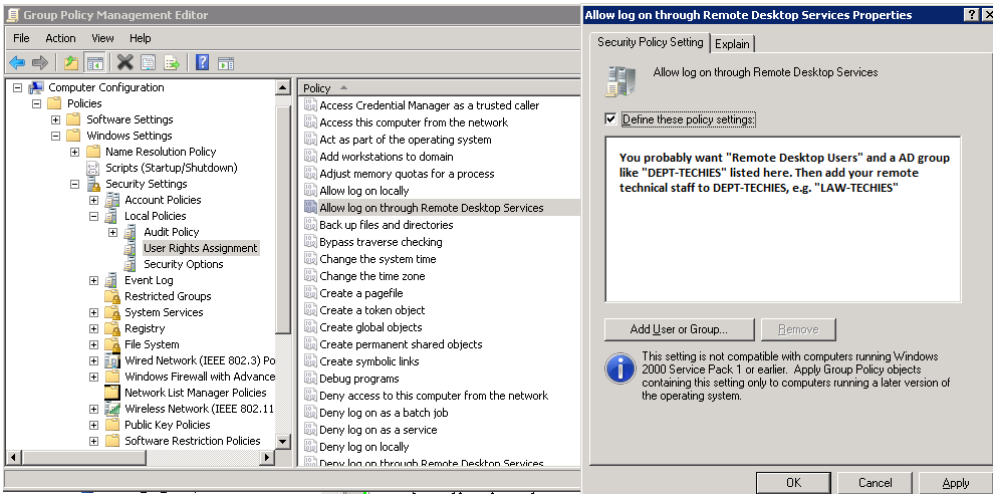
http://support.microsoft.com/kb/951608

- **محدود کردن دسترسی کاربران**

یکی از مباحثی که در ویندوز های سرور وجود دارد این است که دسترسی Administrator برای RDP همواره برقرار می باشد. البته این مشکل را ویندوز سرور ۲۰۱۲ مرتفع کرده است. اما در نسخه های پایین تر این مشکل وجود دارد. چرا که در بسیاری از مواقع ما نمی خواهیم تمامی مدیران به سرویس RDP دسترسی داشته باشند و تنها برخی از مدیران و یا کاربران بتوانند به این سیستم دسترسی داشته باشند. برای این کار مراحل زیر را انجام می دهیم:

1. Start -> Programs -> Administrative Tools -> Local Security Policy
2. Local Policies -> User Rights Assignment

هنگامی که به آدرس فوق رسیدیم، در پنل سمت راست بر روی عبارت Allow logon through Terminal Services دابل کلیک می کنیم تا پنجره مورد نظر باز شود. حال Administrative Groups را حذف کرده و Local Users Group را که همان کاربران مجازی هستند که باید بتوانند از سیستم RDP استفاده کنند را به حال خود رها می کنیم. در تصویر زیر آدرس و پنجره های مربوطه را مشاهده می فرمایید:



- **دفعات ورود گذرواژه**

یکی از حملات معروفی که علیه سرویس RDP انجام می گیرد، حملات Password Brute Forcing می باشد که جهت حدس زدن و کشف پسورد ورودی RDP می باشد. برای جلوگیری از این حمله، می توانیم تعداد دفعات وارد کردن گذرواژه را محدود کنیم. به عبارت دیگر، تعداد دفعاتی را که شخص کاربر می تواند گذرواژه نادرست را مجددا سعی کند کم می کنیم. تجربه نشان داده که قرار دادن ۲ بار امکان وارد کردن گذرواژه کافی می باشد. برای این کار به آدرس زیر می رویم:

1. Start -> Programs -> Administrative Tools -> Local Security Policy
2. Account Policies -> Account Lockout Policies

حال با قرار دادن عدد ۲ در مقدار عنوان Account Lockout Threshold و سپس قرار داند یک زمان مناسب همچون ۱۵ دقیق برای بازگشایی این سیستم در قسمت Reset Account Lockout Counter After ،این سیستم را تنظیم نمایید.

- **تعویض درگاه RDP**

یکی از راه های خوب امنیت بخشی به سرویس RDP تعویض Port پیش فرض آن می باشد. توسط این کار می توان از بدافزارهایی که به صورت خودکار به پورت ۳۳۸۹ حمله می کنند جلوگیری کرد و همچنین با این کار می توان پیدا کردن شماره درگاه این سرویس را برای نفوذگرانی که شروع به Port Scanning بر روی شبکه جهت یافتن درگاه های پیش فرض را می کنند، را بسیار مشکل تر کرد. برای این کار به آدرس زیر می رویم:

1. Start -> Run -> regedit
2. HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Control -> Terminal Server -> WinStations -> RDP-Tcp

حال می توانید شماره Port 3389 را به شماره دلخواه خود تغییر دهید. به یاد داشته باشید که در صورت اعمال این تغییر، باید این شماره درگاه جدید را به تنظیمات Firewall خود اضافه کنید.

- **استفاده از RDP Gateway**

یکی از راه های محدود کردن دسترسی به سرور RDP ، ایجاد یک Gateway در جلوی سرور مربوطه که سرویس RDP بر روی آن در حال اجرا هست، می باشد که با این کار می توان تنظیمات خاصی را برای جلوگیری از حملات مختلف سایبری بر روی این سرور Gateway انجام داد و همچنین می توان ارتباط کاملا امن رمزنگاری شده بین این سرور Gateway و سرور اصلی دارای سرویس RDP را اعمال کرد. با این ۲ کار هم می توان سرور اصلی دارای سرویس RDP را از انواع حملاتی همچون Brute Forcing نجات داد و هم اینکه تنها راه دسترسی به سرور اصلی RDP را از طریق دانش چگونگی اتصال به سرور Gateway محدود کرد. برای انجام این کار می توان از راهنمای زیر استفاده کرد:

http://technet.microsoft.com/en-us/library/dd983949

- **تونل کردن RDP Traffic**

یکی از راه های جالب امن سازی ارتباط با سرویس RDP ، تونل سازی این ارتباط توسط راه های ارتباطی امنی همچون SSH می باشد. این کار بدین صورت می باشد که client برای دسترسی به سرویس RDP باید در ابتدا یک Tunnel SSH امن به یک سرور و یا همان سرور مربوطه بزند و سپس این تونل به صورت خودکار ارتباط امن را به سرویس RDP منتقل می کند. این کار دارای این مزیت است که اولاً رمزنگاری Packet ها ۲ بار صورت می گیرد که شکستن آن را اساساً غیر ممکن می کند و دوماً اتصال اولیه به سرویس SSH خود یک درگاه جدید ورودی را در مقابل ورودی به RDP را ایجاد می کند. برای ایجاد این گونه سرویس های SSH می توان از نرم افزار Bitvise SSH که یک نسخه Port شده از SSH بر روی سیستم عامل ویندوز می باشد استفاده کرد.

۳. استفاده از One Time Password

یکی از راه های مهم امن کردن سرورها و سیستم هایی که می خواهیم از راه دور به آنها متصل شویم این است که از راه کار های OTP استفاده کنیم. این راه کارها جهت جلوگیری از دزدیدن پسوردها و همچنین جهت جلوگیری از حدث زدن پسوردها می باشد. این راه کار بدین صورت می باشد که از یک Device سخت افزاری که بر اساس یک الگوریتم خاص جهت ساختن رمزهای یگبار مصرف به کار می رود و در طرف دیگر بر روی سرور برنامه ای وجود دارد که این الگوریتم می فهمد و توسط این رمزهای یک بار مصرف می توان به سیستم دستیابی پیدا کرد.

۴. استفاده از انواع VPN ها

یکی دیگر از راه های امن سازی دسترسی به سرورها و سیستم ها از راه دور، استفاده از سرورهای VPN و یا سرویس های مختلف VPN می باشد. همانطور که می دانید، توسط یک ارتباط VPN می توانیم به صورت امن به یک شبکه و یا یک سیستم از راه دور دسترسی داشته باشیم. استفاده از سرورهای VPN در این راه کار می تواند این کمک را به ما بکند که توسط یک ارتباط امن بین سیستم client و سرور VPN دیگر شخص ثالثی نمی تواند با انجام حملاتی همچون MITM گذرواژه دسترسی راه دور سیستم ما را بدست بیاورد. استفاده از سرویس VPN هم بر روی همان سیستمی که می خواهیم یک ارتباط از راه دور با آن داشته باشیم هم این امکان را به ما می دهد که بعد از انجام یک ارتباط امن VPN با سرور، اقدام به Login از راه دور به سرویس مربوطه بر روی سرور کنیم.