امنيت شبکه

عليرضا سلطانی نشان

98111033302016

ترم 4

استاد: مهدی احمدی

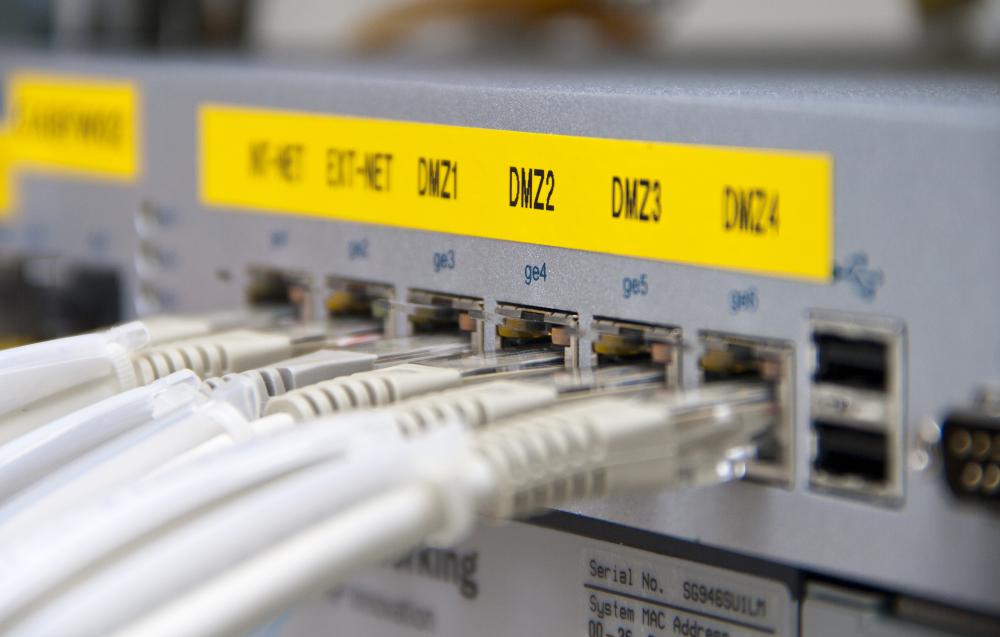
**تسک اول**

تحقیق، شبکه **TAN** و **DMZ**

**لیست مطالب**

[در شبکه های کامپیوتری DMZ به چه معناست؟ 2](#_Toc65531348)

[شبکه TAN از نظر اندازه و مقایس: 5](#_Toc65531349)

****

**در شبکه های کامپیوتری DMZ به چه معناست؟**

توضیح مختصری از درک، شاولند:

**DMZ** از سرکلمات **D**e**m**ilitarized **Z**one گرفته شده، یک شبکه غیر نظامی شده است که از دیگر شبکه ها جدا می­باشد. بسیاری از سازمان ها و شرکت ها به دنبال این هستند که شبکه داخلی خود، که معمولا از LAN استفاده می­کنند را از شبکه اینترنت جدا نمایند، ممکن است در ابتدا فکر کنید که برای کنترل بروی شبکه این عمل را انجام می­دهند. این امر باعث می­شود که امنیت بیشتری برقرار شود چرا که آن ها با این کار شبکه شرکت یا سازمان را از شبکه عمومی (اینترنت) جدا می­کنند. ممکن است بگویید به چه دردی می­خورد؟ باید گفت این عمل باعث می­شود که یک ماشین خاص از شبکه (شبکه های دیگه) جدا شود و بتوانیم آن را به خارج از محیط محافظت فایروال قرار داد، که بطور کلی می­توان گفت هدف از تشکیل آن ایجاد امنیت بیشتر در شرکت ها و سازمان هاست.

**فلسفه:**

در سال **1950** جنگی خونین بین دو کشور، کره شمالی و کره جنوبی ایجاد شد که در طی آن اتفاقات مختلفی رخ داد، سازمان ملل متحد یک پیشنهادی را صادر کرد که بین این دو کشور یک منطقه ای را ایجاد کنند که مردم بتوانند در آن منطقه امرار و معاش خودشان را انجام بدهند چرا که هر دو کشور داشتند از هر نظر از جمله جنبه اقتصادی بسیار ضعیت می­شدند، این پیشنهاد باعث شد که مردم دو کشور در حالی که هیچ کدامشان به یکدیگر اعتمادی نداشتند با هم دیگر در یک منظقه ای به دور از جنگ و خون ریزی منطقه غیر نظامی با یکدیگر تعامل و امرار معاش خود را انجام بدهند. این فلسفه نیز در مورد DMZ یا یک منطقه غیر نظامی صادق است، چرا که در حالی که اعضای شبکه به هیچ کدام یعنی هم به شبکه داخلی خودشان Local و هم به شبکه public یا اینترنت اعتماد ندارند، بتوانند در یک محیطی اجازه برقرای ارتباط داشته باشند، شبکه DMZ یک نوع الگوی طراحی شبکه هاست بطوری که اجازه نمی­دهند هیچ کسی به شبکه DMZ از خارج (اینترنت) وارد شود و باعث ازبین رفتن اعتماد و امنیت شبکه شود در همین راستا از داده ها و اطلاعات سازمان میتوان محافظ کرد.

ساختار DMZ معمولا توسط فایروال ها یا Proxy serverهایی طراحی و پیاده می­شود که در لایه های مختلفی از شبکه قرار میگیرند. در یک ساختار DMZ ساده یک سرور با نام Host معرفی می­شود که تمام request هایی که کاربران دارند (که معمولا باز کردن وب سایت ها هستند) به سمت Host خواهد آمد، این Host درخواست ها را به سمت شبکه public یا همان اینترنت هدایت میکند و Response ها را توسط همان جلسه ای که بین کاربر و سرور ایجاد شده بود را ارسال خواهد کرد. در این نوع از ارتباط در این شبکه بسیار ساده، هیچ کسی نمیتواند از بیرون به شبکه داخلی سازمان ارتباط برقرار کند. حالا هر کاربری که در شبکه خارجی اینترنت قرار داشته باشد، فقط میتواند در خواست های خودش را به Hostی که برای شبکه DMZ استفاده می­کنیم ارسال کند، و به هیچ وجه نمیتوان به شبکه داخلی دسترسی پیدا کند.

آن صفحات وبی که قرار است به عنوان پاسخ به کاربران درون شبکه ای نمایش داده شود در آن سرور عنوانی Host قرار میگیرد و به صورت مستقیم اجازه دسترسی کاربران را به این وب سایت ها نمی­دهد، به همین خاطر اگر هکر بتواند وارد این Host شود و بخواهد تخریب اطلاعاتی خود را انجام دهد، نمیتواند کاری کند چرا که در این محل هیچ دسترسی به اطلاعات وجود ندارد.

از نظر امنیتی، میتوان DMZ را یک نوع کانفیگ ادونس در فایروال دانست، در تنظیمات DMZ کامپیوتر های کلاینتی که در شبکه داخلی قرار دارند در پشت فایروال قرار می­گیرد، که این فایروال به شبکه اینترنت یا شبکه عمومی متصل است. از طرفی دیگر چند سرور هم بعد از فایروال قرار دارند که در شبکه لوکال نیستند، این سرور ها بعد از فایر وال قرار می­گیرند که request های کاربران داخلی را همانطور که در بالاتر توضح دادم از شبکه داخلی دریافت کرده و بعد آنها را به شبکه public اینترنت می­فرستد.

نکته مهمی که باید در این بین اشاره کنم آن است که واژه DMZ را معمولا در بسیاری از مودم ها و روتر های خانگی و غیره مشاهده کرده ایم، اما در حقیقت آن ها DMZ نیستن بلکه فقط قابلیت پشتیبانی از این نوع کانفیگ را دارند. این نوع تجهیزات با طراحی واقعی DMZ در ساختار های سازمانی به کلی متفاوت هستن، آنها فقط چند تا Rule هایی از پیش تنظیم شده هستند که با DMZ که در سرور ها و تجهیزات سازمان ها طراحی می­شود متفاوت است.

**برخی از نکات:**

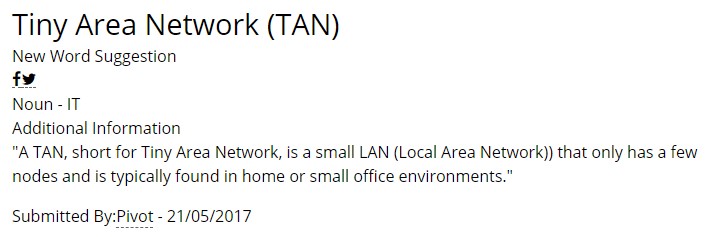
دسترسی ارتباط فقط درون شبکه DMZ است که بصورت محدود عمل می­کند. DMZ شبکه کوچک و ماژولار بین اینترنت و شبکه خصوصی که میتوان در هر قسمتی از سازمان آنرا لحاظ نمود. شبکه DMZ مالکی ندارد. حد وسط نه مثل شبکه داخلی ایمن است، نه مثل اینترنت public ناامن باشد.

شبکه هایی مانند سرور های ایمیل و DNS شبکه هایی هستند که پتانسیل زیادی دارند که مورد حمله قرار بگیرند، به همین خاطر به دلیل حمله و نفوذ پذیر بودنشون تو زیر مجموعه DMZ قرار میگیرند. تعداد هاست ها محدود، ارتباط بین DMZ و public net هم محدود شده است، تا امن باشه و برای استفاده از یکسری سرویس های خاص هم مناسب باشه،

اجازه ارتباط DMZ به داخل و خارج ، در صورتی که فایروال ترافیک کلی بین سرویس های DMZ و Client ها رو (عامل مخرب کنترل) کنترل کنه، و یه فایروال دیگه ای وجود داره که از DMZ در برابر شبکه خارجی محاظت کنه.

امکان اسنیف شدن باز هم پابر جا هست. سرویس های خارجی در DMZ هم موجوده، که باعث امن شدن بستر برخی از سرویس های ضروری می­شود.

**شبکه TAN از نظر اندازه و مقایس:**



از نظر کلی با توجه به نتایجی که در گوگل بدست آمد، آن است که شبکه TAN یک شبکه Tiny و کوچولو حتی از شبکه LAN کوچک­تر است، که معمولا بین دستگاه های اندکی که در خانه یا در محیط اداری یافت می­شوند مورد استفاده قرار میگیرد.

علاوه بر ترجمه متن بالا می­توان گفت، یک شبکه TAN یا Tiny Area Network در حالت ساده یک شبکه LAN خیلی کوچک است، (بطوری که در مباحث LAN بیان شده است که یک شبکه کوچک محلی درون ساختمانی می­باشد) TANها در خانه ها، محل های اداری خانگی و کسب و کار های کوچک محبوب شده اند. منافع زیادی برای داشتن یک شبکه TAN وجود دارد، شبکه شما کامپیوتر ها را قادر می­سازد که با بالاترین سرعت، مودم ها، روتر ها و پرینتر ها و فایل ها را به اشتراک بگذاریم.

زمانی که شما در کامپیوتر های خود از شبکه اینترنت استفاده می­کنید که بتوانید ایمیل هایتان را ارسال کنید یا اینکه در برخی از خانه ها بسیاری از افراد هستند که به بازی های آنلاین می­پردازند با خانواده خودشان، با یک شبکه TAN شما می­توانید از نرم­افزار های روتر یا پروکسی سرور خود، که امکان اتصال به اینترنت را در میان سایر کامپیوتر های شبکه را فراهم می­کند، به طور کامل و صریح استفاده کنید. به این ترتیب، همه افراد در شبکه می­توانند همزمان از مکان های مختلف اینترنت دیدن کنند.