Community String چیست؟ بررسی کاربرد در SNMP به زبان ساده (نسخه PDF)

قبلاً در وبسایت Tosinso بصورت مفصل درباره پروتکل SNMP و اجزای آن صحبت شده است اما در مورد Community String صحبتی به میان نیاورده شده است که بنده در این مقاله میخواهم بصورت مفصل درباره آن و انواع آن صحبت کنم. همانطور که میدانید پروتکل SNMP در ساده ترین حالت از یک SNMP سرور که به Network Management Server یا NMS نیز معروف است و یک SNMP Client که SNMP Agent بر روی آن نصب شده است و میتواند بر اساس اطلاعاتی که در دیتابیس MIB خود دارد میتواند سئوالاتی که از جانب SNMP Server از او پرسیده میشود در قالب جواب هایی مناسب که دارای OID یا شناسه منحصر بفردی هستند به سرور NMS ارسال کند تشکیل شده است. حالا ما در این مقاله میخواهیم نوع جواب هایی که از طرف SNMP Client به SNMP Server ارسال میشود را از لحاظ Community String مورد بررسی قرار دهیم.

Community String در SNMP شبیه به نام کاربری یا پسورد می باشد که خود این ها شامل String یا رشته حروف یا اعداد هستند Community String هم از این قاعده مستثنی نیست. در واقع Community String یک پارامتر امنیتی میباشد که وقتی که SNMP Server یک پیام از نوع Get-Request به دستگاه SNMP Client فرستاد SNMP Client این Community String را با Community String ای که در خودش دارد مقایسه می کند و در صورتی که این دو Community String با هم برابر بودند دستگاه SNMP Client پاسخ مناسبی را به SNMP Server ارسال می کند . حال در صورتی که این دو Community String با هم برابر نبودند SNMP Client به درخواست جواب نمی دهد و آنرا نادیده می گیرد. بسیاری از شرکت های سازنده تجهیزات شبکه ای مانند روتر ، سوئیچ ، فایروال ، UPS های تحت شبکه و ... به صورت پیشفرض Community String را برابر **Public** در نظر گرفته اند که در اصطلاح فنی Default Public Community String نامیده میشود.

همانطور که رمز عبور پیشفرض ورود به تنظیمات مودم ADSL تان admin هست و متاسفانه اکثر کاربران این رمز عبور را تغییر نمیدهند Default Public Community String نیز قابل تغییر هست و مدیر شبکه موظف است که برای بالا بردن امنیت شبکه سازمان این Community String را تغییر بدهد، زیرا اگر تغییر داده نشود یک فرد مهاجم یا هکر میتواند براحتی میتواند این Community String را شنود کند و در نتیجه میتواند به پاسخ هایی که از جانب یک SNMP Client به SNMP Server داده میشود دست پیدا کرده و کلی اطلاعات راجب تجهیزات شبکه بدست بیاورد و در پیشبرد حمله خود به شبکه سازمان تسریع کند. Community String ها به طور کلی دو نوع تقسیم بندی میشوند که عبارتند از **Read-Only Community String** و **Read-Write Community String**.

همانطور که از اسم Read-Only Community String هم مشخص است این نوع Community String ها به صورت فقط خواندنی یا Read Only در شبکه بین SNMP Client و SNMP Server رد و بدل میشود و احیاناً اگر فرد مهاجم بتواند به آن دست پیدا کند نمیتواند آنرا دستکاری کند اما اگر شما از نسخه ۱ یا ۲ پروتکل SNMP در شبکه استفاده کرده باشید فرد مهاجم براحتی میتواند آنرا بخواند زیرا بصورت Clear text در شبکه ارسال میشود اما اگر شما از نسخه ۳ پروتکل SNMP استفاده کنید اطلاعات درخوست شده توسط SNMP Server از SNMP Client توسط یک فرد احرازهویت شده و به صورت رمزنگاری شده فرستاده میشود تا اگر Community String بصورت Read-Write یا قابل نوشتن هم فرستاده شده باشد فرد مهاجم به سختی میتواند به محتویات آن دسترسی پیدا کند و تغییرش بدهد.

نوع دیگری از Community String نیز وجود دارد که به **SNMP Trap Community String** معروف است. SNMP Trap به طور کلی پیام هایی از سوی SNMP Client به SNMP Server هستند که توسط SNMP Server از SNMP Client درخواست نشده است و در صورتی که SNMP Trap روی دستگاه SNMP Client فعال شده باشد و برای آن تعیین شده باشد که برای مثال وقتی لینک مربوط به روتر یا سوئیچ UP یا Down شد به SNMP Server به صورت آنی پیغام فرستاده شود تا به مشکل پیش آمده رسیدگی شود. امیدوارم بخوبی مفهوم Community String ها را درک کرده باشید.

نویسنده : امیرحسین کریم پور

منبع : TOSINSO

مطلب اصلی