آموزش رایگان دوره نتورک‌پلاس (Network+) (بخش 57)

در شماره گذشته آموزش نتورک‌پلاس با سامانه پیشگیری از نفوذ، سیستم‌های امنیت اطلاعات و مدیریت رویداد، مدیریت سوییچ، Switch Path Management، فرآیند مسیریابی با پروتکل STP و چارچوب AAA آشنا شدیم. در این شماره مبحث فوق را ادامه خواهیم داد.

برای مطالعه بخش پنجاه و ششم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

تایید هویت محلی (Local Authentication)

فرآیندهای احراز هویت محلی روی دستگاه محلی انجام می‌شوند که در نتیجه نام کاربری و گذرواژه به صورت محلی ذخیره می‌شوند که دارای مزایا و معایب زیر است:

• **امنیت پایین** - اکثر دستگاه‌های کاربران نهایی سطح ایمنی کمتری نسبت به سرورهای شبکه دارند. یک هکر می‌تواند از طریق پیاده‌سازی یک حمله جست‌وجوی فراگیر یا سایر بردارهای حمله به یک دستگاه مستقل حمله کرده و اگر گواهی‌نامه‌ها و اختیارات مشابهی روی سایر دستگاه‌ها استفاده شده باشد، همه دستگاه‌ها را در معرض خطر قرار دهد. همچنین، احراز هویت محلی امکان قفل کردن یک حساب کاربری از راه دور را مقدور نمی‌کنند.

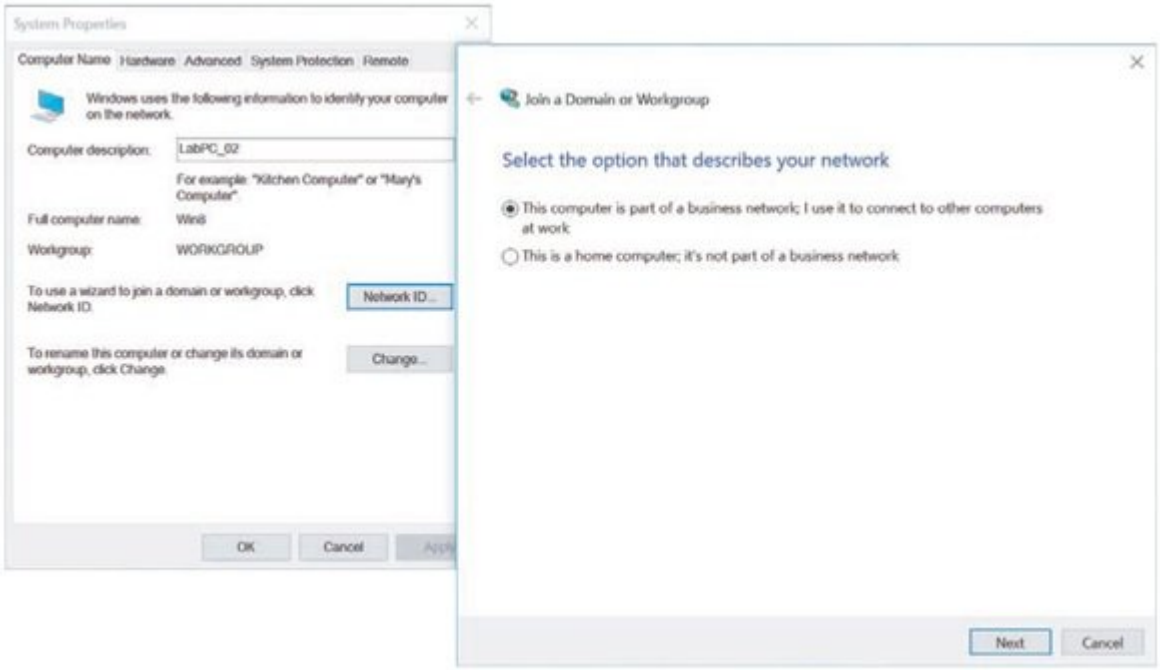
• **راحتی در ابتدا، پیچیدگی در ادامه متفاوت است** - فقط برای تعداد انگشت شماری از دستگاه‌ها، مدیریت حساب‌های محلی را می‌توان به سادگی روی یک دامنه ویندوز (اکتیو دایرکتوری) تنظیم کرد. اما زمانی که تعداد دستگاه‌ها به یک مرتبه افزایش پیدا کنند، فرآیند احراز هویت محلی دیگر آن سادگی و سهولت را نخواهد داشت.

• **دسترسی به نسخه پشتیبان قابل اعتماد** - در صورت خرابی شبکه یا سرور، تنها گزینه قابل اجرا، احراز هویت محلی است. به همین دلیل دستگاه‌های شبکه و سرورها باید با یک حساب محلی اختصاصی که فقط زمانی که سرویس‌های تأیید هویت در شبکه غیرقابل دسترسی هستند پیکربندی شده و استفاده شوند. لازم به توضیح است که این حساب باید امنیت بالایی داشته باشد.

در فرآیند احراز هویت محلی، ایمنی هر کامپیوتر متصل به شبکه بر عهده خودش است. اگر چند کامپیوتر قصد دارند به یک فایل سرور دسترسی پیدا کنند هر کاربر باید حساب کاربری محلی خود را روی فایل سرور در اختیار داشته باشد. هرچه شبکه محلی بزرگ‌تر می‌شود مدیریت این حساب‌های کاربری برای مدیر شبکه به یک کابوس تبدیل می‌شود.

در ویندوز شما می‌توانید احراز هویت محلی را به احراز هویت شبکه تغییر وضعیت دهید. برای این منظور باید در

پنجرهSystem Properties روی دکمه Network ID کلیک کرده و سپس گزینه This computer is part of a business network; I use it to connect to other computers at work را انتخاب کنید. دکمه Next را فشار داده و سپس My company uses a network with a domain را انتخاب کنید. زمانی که روی دکمه Next کلیک کردید در ادامه باید گذرواژه، نام کاربری، نام دامنه ویندوز و نام کامپیوتر خود که در دامنه ویندوز قرار دارد را وارد کنید. همه این اطلاعات باید از قبل روی اکتیو دایرکتوری ویندوز سرور شبکه ذخیره شده باشد. زمانی که این فرآیند به درستی کامل شد، در مراجعه بعدی احراز هویت از طریق نام کاربری و گذرواژه متصل به شبکه انجام می‌شود. (دقت کنید این روش برای زمانی است که شما در محلی کار می‌کنید که کامپیوترتان متصل به شبکه است.)



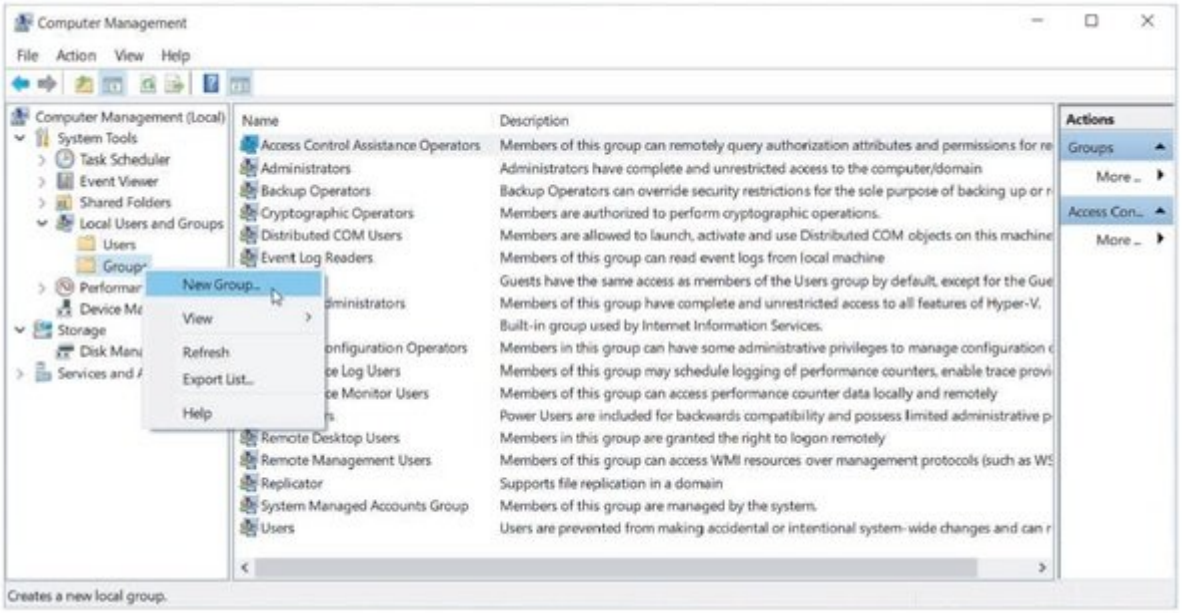
سطح دسترسی (Authorization)

حتا بهترین روش‌های احراز هویت، از جمله رمزگذاری، قفل درب اتاق کامپیوتر، خط‌مشی‌های امنیتی و قوانین تعیین گذرواژه‌ها اگر شما به کاربران غیرمجاز و بدون مجوز اجازه دهید به شبکه و زیرساخت‌ها دسترسی داشته باشند غیرکارآمد خواهند بود. کاربران به دو شکل به منابع شبکه دسترسی دارند:

1. کاربرانی که مجوز اجرا، نصب و حذف نرم‌افزارها را دارند

2. کاربرانی که مجوز خواندن، تغییر، ایجاد یا حذف فایل‌ها و پوشه‌های داده‌ای را دارند.

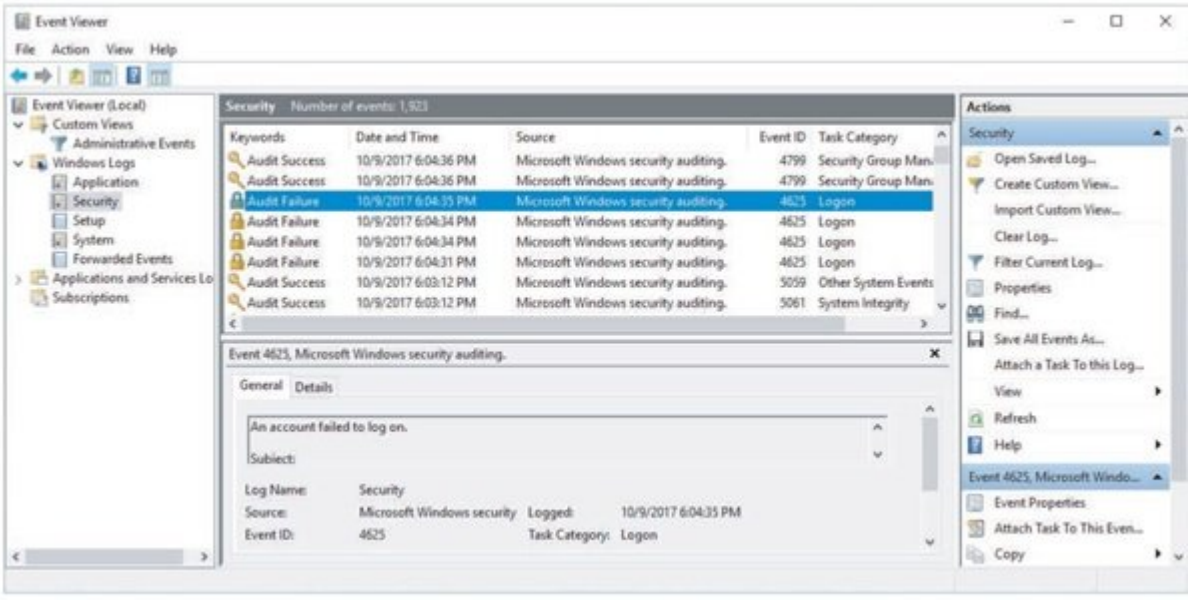
محبوب‌ترین روش مجوزدهی روش کنترل دسترسی مبتنی بر نقش (**RBAC**) سرنام **role-based access control** است. در مکانیزم فوق مدیر شبکه از سرپرست کاربران توضیح دقیقی در ارتباط با نقش‌ها یا شغلی که در سازمان عهده‌دار انجام آن‌ها هستند سوال می‌کند. مدیر شبکه مسئل است تا امتیازات و مجوزهای لازم برای هر کاربر را بر مبنای نقشی که در سازمان دارد به او تخصیص دهد. البته کاربران ممکن است به برخی از منابع عمومی و خاص شبکه نیاز داشته باشند که البته این دسترسی عمومی به یک چنین منابعی محدود است. با کنترل دسترسی مبتنی بر نقش، مدیر شبکه، گروه‌های کاربری مرتبط با این نقش‌ها را ایجاد می‌کند و امتیازات و مجوزها را برای هر گروه کاربری اختصاص می‌دهد. در این حالت هر کاربر به یک گروه کاربری وارد می‌شود. توجه داشته باشید که یک کاربر می‌تواند به بیش از یک گروه کاربری تعلق داشته باشد. هرچند پیشنهاد می‌شود برای مدیریت بهتر تا جایی که امکان دارد یک چنین کاری انجام نشود. شکل زیر پنجره مدیریت کامپیوترها، کاربران و گروه‌ها در ویندوز را نشان می‌دهد. پیشنهاد می‌کنم برای آشنایی بهتر با این مبحث به Computer Management رفته و اطلاعات بیشتری در ارتباط با نحوه تعریف گروه‌ها، کاربران و تخصیص کاربران به گروه‌های مختلف اطلاعاتی کسب کنید.



ویندوز گزینه‌ای برای ایجاد گروه‌های محلی در ایستگاه‌های کاری شخصی فراهم کرده است. البته Active Directory گزینه‌های بیشتری برای ایجاد گروه‌های محلی دامنه (domain local groups) فراهم می‌کند که کل شبکه را مدیریت می‌کنند.

حسابرسی (Accounting)

یک سیستم کامپیوتری گزارش‌های مختلفی را تولید می‌کند که یک مدیر می‌تواند برای عیب‌یابی و ممیزی یک سیستم از آن‌ها استفاده کرده و نکات جالبی را کسب کند. در سیستم‌عامل‌های لینوکس یا مک، گزارش‌ها اغلب در قالب فایل‌های متنی ذخیره می‌شوند. فایل‌های متنی طولانی که مدیر شبکه مسئول است که اجازه ندهد فضای ذخیره‌سازی سیستم به واسطه این فایل‌ها بیش از اندازه از دست برود. در ویندوز، شما می‌توانید ابزار Event Viewer را برای مشاهده گزارش‌های تولید شده از سوی ویندوز استفاده کنید. در شکل زیر رویدادی را مشاهده می‌کنید که مالک یک حساب کاربری موفق نشده است به سیستم ورود کند. همان‌گونه که در شکل دیده می‌شود، رویدادهای حسابرسی در Windows Logs و Security group از Event Viewer ظاهر می‌شوند. البته قبل از این‌که رویدادهای ورود به سیستم ذخیره شوند، شما در ابتدا باید از Group Policy برای فعال کردن این ویژگی استفاده کنید.



راه‌حل‌های کنترل دسترسی به شبکه (Network Access Controls Solutions)

همان‌گونه که شبکه‌ها رشد کرده و سازمان‌ها از راه‌حل‌های دستگاه خود را بیاورید (BYOD) پیروی می‌کنند، مدیران شبکه باید نهایت تلاش خود را به کار گیرند تا توازنی میان سطح دسترسی به شبکه و امنیت شبکه برقرار کنند. این چالش‌ها باعث به وجود آمدن راه‌حل‌های متنوعی شده‌اند تا مدیریت پیچیدگی‌ها ساده‌تر شود. مکانیزم کنترل دسترسی به شبکه (NAC) سه رویکرد احراز هویت، سطح دسترسی و حساب‌رسی را وارد فاز جدیدی کرد. یک سیستم NAC مجموعه‌ای از قواعد که خط‌مشی‌های شبکه نامیده می‌شوند را برای تعیین سطح و نوع دسترسی به یک دستگاه زمانی که دستگاه به شبکه متصل است تعیین می‌کند. یک راه‌حل NAC ارائه شده از سوی سیسکو شامل دیوارهای آتش سیسکو، روترها، سوئیچ‌ها و دستگاه‌های (ASA) سرنام Adaptive Security Appliance است که همگی در قالب یک راه‌حل‌واحد کار می‌کنند. علاوه بر این، مایکروسافت نیز نرم‌افزار حفاظت از دسترسی به شبکه **NAP** سرنام **Network Access Protection** را ارائه کرده است که به عنوان یک راه‌حل NAC در ویندوز سرور عمل می‌کند. سیستم‌های NAC تأیید هویت و تعیین سطح دسترسی دستگاه‌ها را مطابق با معیارهای امنیتی از پیش تعریف شده است انجام می‌دهند. در برخی از شبکه‌ها، قبل از اینکه دستگاه بتواند تأیید هویت شود، نرم‌افزاری به نام عامل (**agent**) باید روی دستگاه نصب شود. این عامل وضعیت دستگاه را در رابطه با امنیت و انطباق امنیت آن با معیارهای امنیتی و سازگار بودن با این معیارها ارزیابی می‌کند. دو نوع رایج از این عامل‌ها به شرح زیر هستند:

• یک عامل غیرپایدار (**nonpersistent agent**) یا قابل تعویض به مدت زمان طولانی روی یک دستگاه قرار می‌گیرد تا صحت آن‌را تایید کرده و پس از آن‌که احراز هویت دستگاه کامل شد از روی آن حذف شود. در برخی موارد باید این عامل از روی دستگاه‌ها پاک شده و دومرتبه نصب شود تا فرآیند تأیید صحت تکمیل شود.

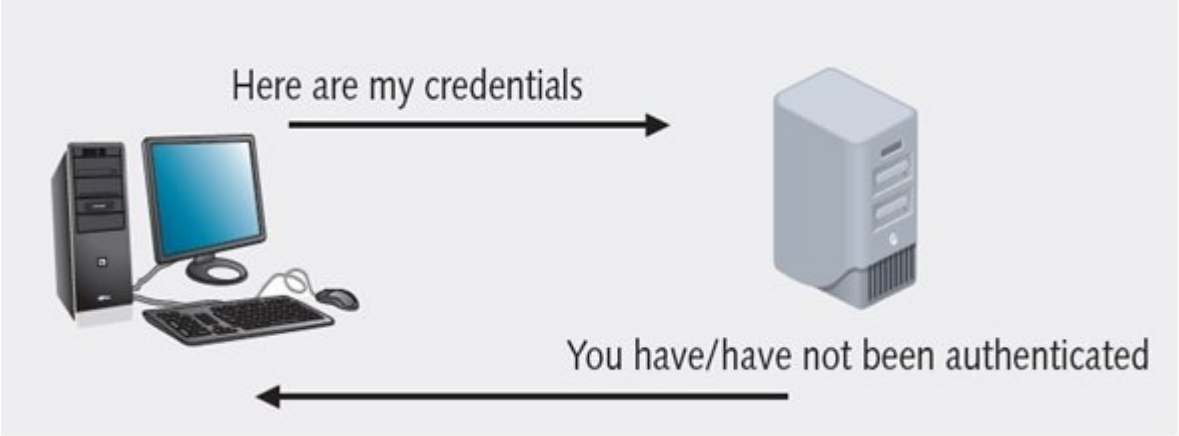
• عامل ماندگار (**persistent agent**) به‌طور دائمی در یک دستگاه نصب می‌شود. این عامل یک برنامه قدرتمند است که در اغلب موارد اقدامات امنیتی بیشتری را همچون پاک کردن راه دور، اسکن ویروس‌ها و انبوه پیام‌ها انجام می‌دهد.

البته همه شبکه‌ها به عامل نیازی ندارند. گزینه دیگری که پیش‌رو است، Active Directory است که احراز هویت فارغ از عامل (**agentless authentication**) را پیشنهاد می‌کند. در این روش کاربر با استفاده از یک دامنه احراز هویت می‌شود. در ادامه اکتیو دایرکتوری دستگاه را برای انطباق الزامات با NAC پویش می‌کند. در این حالت، هر دستگاهی که به شبکه حفاظت شده NAC متصل نیست، به عنوان یک دستگاه تایید شده شناخته نخواهد شد. در نقطه مقابل، دستگاه‌هایی که مطابق با الزامات رعایت شده یا مشخص شده شناخته شده‌اند، اما در معرض خطر قرار گرفته‌اند، باید در یک شبکه قرنطینه (**quarantine network**) که جدا از منابع حساس شبکه است به فعالیت ادامه دهند. البته سطح دسترسی این دستگاه‌ها به شبکه کاملا محدود خواهد بود تا مراحل بازسازی و ترمیم تکمیل شود.

توپولوژی‌های کنترل دسترسی

از سه فرایند اصلی AAA، احراز هویت تمایل به پیچیدگی بیشتری دارد. پروتکل‌های تأیید اعتبار قوانینی هستند که کامپیوترها برای انجام احراز هویت از آن‌ها تبعیت می‌کنند. سرویس‌ها و پروتکل‌های تأیید هویت مختلفی وجود دارند که برخی از آن‌ها شامل مولفه‌های تعیین سطح دسترسی و ممیزی هستند. از جمله این پروتکل‌ها به موارد زیر می‌توان اشاره کرد:

• PAP (پروتکل تأیید رمز عبور) – یک کلاینت از PAP برای ارسال درخواست احراز هویت که شامل اعتبار نیز می‌شود، استفاده می‌کند. سرور این درخواست را با اطلاعاتی که از کاربر درون بانک‌اطلاعاتی دارد مقایسه می‌کند. اگر مجوزها مطابقت داشته باشند، سرور با یک پیام تأیید اعتبار به کلاینت پاسخ می‌دهد و دسترسی مشتری به منابع امن را امکان‌پذیر می‌کند. اگر اعتبارها مطابقت نداشته باشند، سرور درخواست تأیید اعتبار را رد می‌کند. شکل زیر پروسه احراز هویت دو مرحله‌ای PAP را نشان می‌دهد. PAP یک پروتکل احراز هویت ساده است که ما ایمن نیست. همچنین، اعتبارنامه کلاینت را به صورت متنی و بدون رمزنگاری ارسال می‌کند.



• پروتکل چالش تأیید دست دادن Challenge Handshake Authentication Protocol – برعکس PAP در پروتکل CHAP نام‌های کاربری و گذرواژه‌ها برای انتقال رمزگذاری می‌شوند. همچنین فرآیند احراز هویت در سه مرحله که دست‌دهی سه مرحله‌ای است انجام می‌شود. شکل زیر این سه مرحله را نشان می‌دهد.

• پروتکل چالش تأیید دست دادن مایکروسافت (Microsoft Challenge Handshake Authentication Protocol) –پروتکل MS-CHAP که از سوی مایکروسافت توسعه یافته شبیه به پروتکل CHAP بوده و با کامپیوترهای ویندوزی استفاده می‌شود. یک نقص احتمالی در فرآیند احراز هویت هر دو پروتکل این است که یک شخص در شبکه می‌تواند به استراق سمع پرداخته و رشته‌های کاراکترها که گذرواژه هستند را رمزگشایی کرده و به گذرواژه‌های کلاینت‌ها دسترسی پیدا کند.

• پروتکل چالش تأیید دست دادن مایکروسافت نگارش 2 (Microsoft Challenge Handshake Authentication Protocol, version 2) - مایکروسافت برای حل مشکلات سه پروتکل قبلی سعی کرد از یک الگوریتم رمزنگاری قوی برای رمزگذاری رشته‌هایی که قرار است انتقال پیدا کنند استفاده کند. شما هنوز هم می‌توانید MS-CHAPv2 را در ارتباط با برخی از کسب‌وکارها، به ویژه در سیستم‌های قدیمی VPN و در محیط‌های WPA2-Enterprise مشاهده کنید.

سرویس‌های دایرکتوری

برای این‌که کلاینت‌ها برای دسترسی به منابع شبکه تأیید اعتبار شوند، روی سرورها به بانک‌های اطلاعاتی که اطلاعات حساب‌ها همچون گذرواژه‌ها، نام‌های کاربری و سایر اطلاعات اعتباری را نگه‌داری می‌کنند نیاز داریم. در دنیای ویندوز ما از اکتیو دایرکتوری Active Directory و در دنیای لینوکس عمدتا از ماهیتی شبیه بهOpenLDAP یا 389 Directory Server استفاده می‌کنیم. همه این گزینه‌ها سازگار با قرارداد دسترسی سبک‌وزن راهنما (LDAP) سرنام Lightweight Directory Access Protocol که پروتکلی برای دسترسی به یک دایرکتوری موجود است سازگاری

دارند. LDAP می‌تواند محاوره‌ای با بانک‌اطلاعاتی انجام داده و و اطلاعات مورد نیاز را دریافت کند. همچنین می‌تواند برای اضافه کردن اطلاعات جدید یا ویرایش داده‌های موجود استفاده شود. به‌طور پیش‌فرض اکتیو دایرکتوری پیکربندی شده است که از پروتکل Kerberos استفاده کند. با این حال، اکتیودایرکتوری می‌تواند از LDAP و Kerberos استفاده کند. با پشتیبانی از هر دو این فناوری‌ها تأیید و تعیین سطح مجوزها به شکل دقیقی در یک شبکه انجام می‌شود.

Kerberos

Kerberos پروتکل احراز هویتی است که به‌طور پیش‌فرض برای Active Directory پیکربندی شده است.
Kerberos یک پروتکل احراز هویت چند سکویی است که از رمزنگاری کلید برای تأیید هویت کلاینت‌ها و تبادل ایمن اطلاعات پس از ورود یک کلاینت به یک سیستم استفاده می‌کند. Kerberos به‌طور خودکار به کلاینت‌ها اعتماد ندارد. در نتیجه، کلاینت‌ها باید هویت خود را از طریق بخش ثالثی برای Kerberos به اثبات برسانند. این رویکرد مشابه با زمانی است که گیت‌ها از شما پاسپورت درخواست می‌کنند تا هویت شما برای کشوری که قصد ورود به آن‌را دارید به اثبات برسد. علاوه بر بررسی اعتبار یک سرویس گیرنده، ارتباطات Kerberos رمزگذاری می‌شوند و بعید است که اطلاعات در حال انتقال از سوی هر دستگاهی در شبکه و به غیر از سرویس گیرنده رمزگشایی شوند. برای درک دقیق اینکه چگونه یک کلاینت از Kerberos استفاده می‌کند، باید با یکسری اصطلاحات مرتبط با این فناوری آشنا شوید که در شماره آینده این موضوع را بررسی خواهیم کرد.

در شماره آینده آموزش **نتورک‌پلاس** مبحث فوق را ادامه خواهیم داد.

تاریخ انتشار:

11 خرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15465/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-network-%D8%A8%D8%AE%D8%B4-57