[illegible]

[illegible] (Network+) [illegible] (57

[illegible] Switch Path Management[illegible] STP [illegible] AAA [illegible]

[illegible] **(Network+)** [illegible]

[illegible] (Local Authentication)

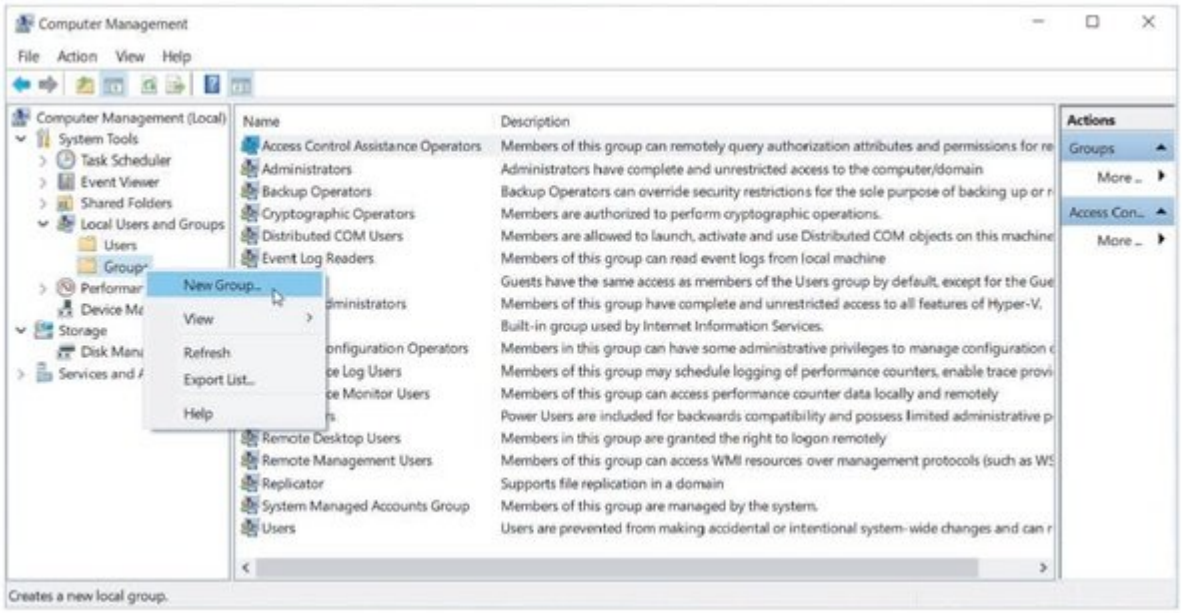
[illegible]:

• [illegible] - [illegible]

• [illegible] - [illegible] (Domain Controller) [illegible]

(Authorization)

role-based access control (RBAC) [illegible] Computer Management [illegible]



Active [illegible] Directory [illegible] (domain local groups) [illegible]

(Accounting) [illegible]

[illegible] Event Viewer [illegible] Windows Logs [illegible] Security group [illegible] Event Viewer [illegible] Group [illegible] Policy [illegible]

Event Viewer
File
Action
View
Help
Event Viewer (Local)
Custom Views
Administrative Events
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
Security
Number of events: 1,923
General
Details
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 4625, Microsoft Windo...
Event Properties
Attach Task To This Even...
Copy

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/9/2017 6:04:36 PM	Microsoft Windows security auditing.	4799	Security Group Man
Audit Success	10/9/2017 6:04:36 PM	Microsoft Windows security auditing.	4799	Security Group Man
Audit Failure	10/9/2017 6:04:35 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	10/9/2017 6:04:34 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	10/9/2017 6:04:34 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	10/9/2017 6:04:31 PM	Microsoft Windows security auditing.	4625	Logon
Audit Success	10/9/2017 6:03:12 PM	Microsoft Windows security auditing.	5059	Other System Events
Audit Success	10/9/2017 6:03:12 PM	Microsoft Windows security auditing.	5061	System Integrity

Event 4625, Microsoft Windows security auditing.

An account failed to log on.

Subject:

Log Name: Security
Source: Microsoft Windows security
Logged: 10/9/2017 6:04:35 PM
Event ID: 4625
Task Category: Logon

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 .

Here are my credentials
You have/have not been authenticated

- 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 .

Here is a challenge
1
Here is the challenge, plus my encrypted password
2
You have/have not been authenticated
3
Client
Server

- 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 OpenLDAP 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 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 دقیق 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 .

نویسنده :
حمیدرضا تائبی
دسته بندی:
فناوری شبکه
تاریخ انتشار :
13:05 - 11/03/1398
برچسب:
آموزش رایگان شبکه - دوره رایگان نتورک پلاس - دوره نتورک پلاس - آموزش نتورک پلاس - آموزش رایگان دوره نتورک پلاس - آموزش دوره نتورک پلاس - آموزش رایگان +Network - +Network - امنیت شبکه - امنیت در طراحی شبکه - تایید هویت محلی - سطح دسترسی - توپولوژیهای کنترل دسترسی - آموزش رایگان +Network

---

نشانی
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