CYBER DEFENSE

❖ حسین ملک زاده

مشاور و تحلیل گر ارشد امنیت سایبری

کارشناس ارشد امنیت اطلاعات ازدانشگاه Sapienza Universityرم – ایتالیا

مدرس و عضو هیات علمی دانشگاه بین المللی نورث وست Northwest International University

مدرس و عضو هیات علمی دانشگاه نیوجرسی New Jersey International Open University

مدرس و عضو هیات علمی موسسه دانشگاهی DEI Institute - Online Universityآفریقا

دارای مدرک دکترا مدیریت امنیت سایبری DBA - Cyber Security Management از دانشگاه بین المللی نورث وست

ممیز و سرممیز امنیت اطلاعات ISMS ISO27001-2013

دارای مدارک سطح عالی امنیت اطلاعات CISSP , CISA

دارای مدرک مشاور ارشد امنیت سیستمی SSCP

طراح – مشاور و مجری پروژه¬های شبکه و امنیت اطلاعات ISMS , SOC , NOC

دارای بیش از ۲۴ سال سابقه آموزشی – اجرایی و مدیریتی درزمینه پروژه¬های شبکه و امنیت در داخل و خارج از کشور

مدرس دوره¬های تخصصی شبکه و امنیت با بیش از دوازده هزارساعت تدریس درموسسات داخلی و بین المللی

دارای تحصیلات و مدارک بین المللی :

MCSE , CCNA ,CCNA Security , CCNP , CEH , CISSP , CWNA , ISMS , SSCP, GSNA

عضوانجمن مهندسین کامپیوتر و فناوری آمریکا IEEE , ACM

مولف کتاب هنر هک کردن انسان در حوزه امنیت در مهندسی اجتماعی Social engineering

www.Hosseinmalekzadeh.com

Mobile: 09153133217

E-mail: Hoseeinmalekzadeh@Gmail.com

Telegram Channel : https://t.me/HosseinMalekzadeh

http://www.linkedin.com/in/hosseinmalekzadeh

@HOSSEINMALEKZADEH2015

@HOSSEINMALEKZADEH

By. Hossein Malekzadeh

Cyber Security Consultant and Manager

www.Hosseinmalekzadeh.com

Mobile : 09153133217

نقشه شبکه سازمان (دفتر مرکزی)

سناریوی سازمان

یک سازمان متوسط با حدود ۵۰۰ کارمند
دارای دفتر مرکزی و دو شعبه
خدمات اصلی سازمان شامل:

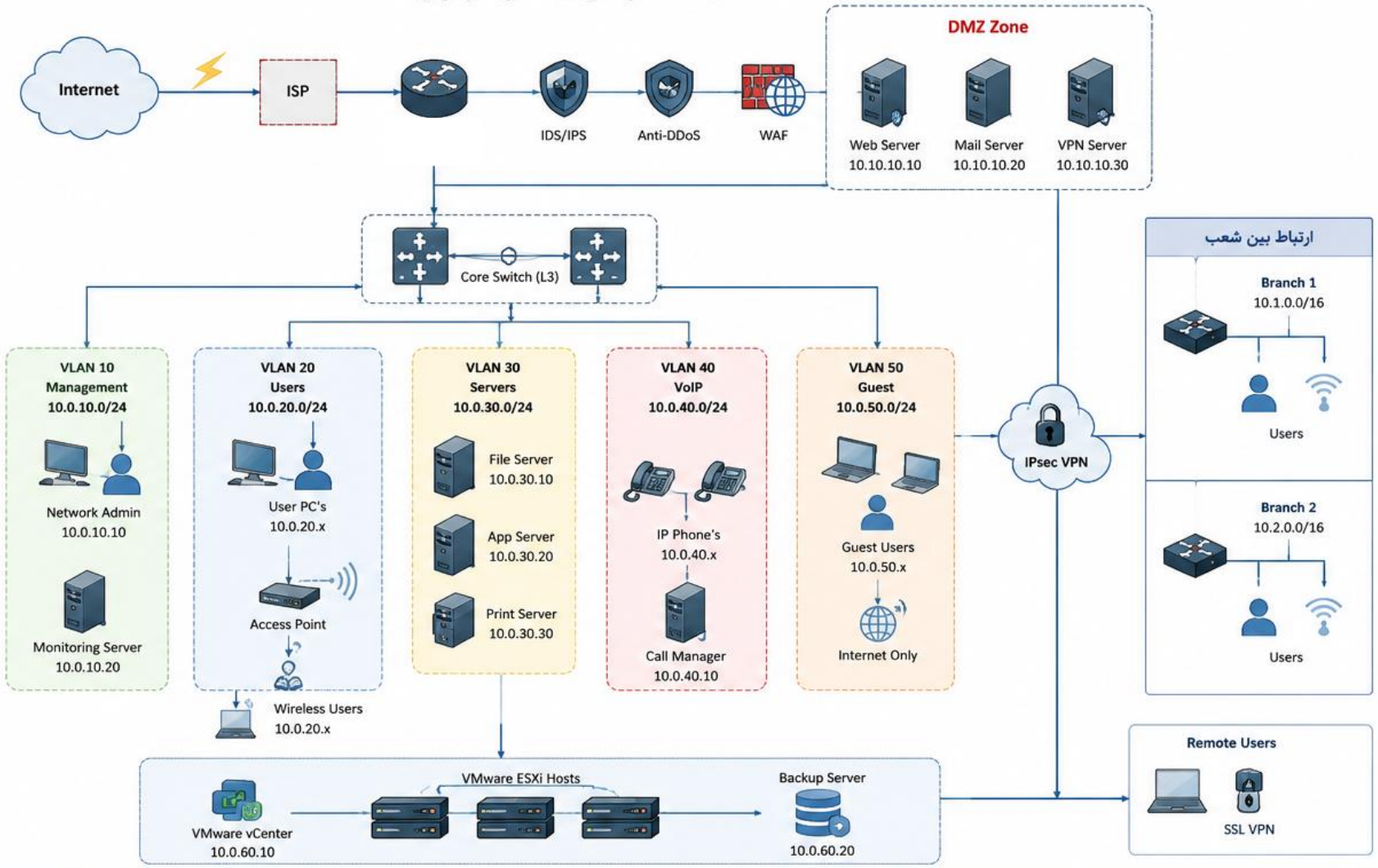
- سرویس های دایرکتوری (Active Directory)
- سرورهای فایل و پرینت
- سرور برنامه کاربردی تحت وب
- سیستم تلفنی تحت شبکه (VoIP)
- دسترسی کاربران به اینترنت
- ارتباط امن بین شعب از طریق VPN
- زیرساخت مجازی سازی با VMware

اهداف امنیتی

- حفاظت لایه به لایه از اطلاعات و سرویس ها
- جلوگیری از دسترسی غیرمجاز
- جلوگیری از حرکت جانبی مهاجم در شبکه
- مانیتورینگ و پاسخ به رخدادها
- پشتیبان گیری و تداوم کسب و کار

چالش ها / تهدیدات

- حملات اینترنتی (Brute Force, Exploit, DDoS)
- فیشینگ و مهندسی اجتماعی
- بدافزار و باج افزار
- تهدیدات داخلی و دسترسی بیش از حد
- نشت اطلاعات
- خرابی تجهیزات و از دسترس خارج شدن سرویس ها



راهنمای نمادها

اینترنت — کلاینت — فایروال / روتر
سیستم امنیتی — تلفن تحت شبکه — سوئیچ لایه ۳
دسترسی بی سیم — سرور

نکات طراحی امنیتی (Defense in Depth)

- لایه محیطی: فایروال, IDS/IPS, Anti-DDoS, WAF
- لایه شبکه: تقسیم بندی VLAN, Private VLAN, Private VLAN Security
- لایه سیستم: هاردنینگ سررورها و کلاینت ها، بروزرسانی Patch Management
- لایه هویت و دسترسی: Mtive Directory Security, Least Privilege Security
- لایه مانیتورینگ: جمع آوری و تحلیل لاگ ها در SIEM
- لایه داده: رمزنگاری: DLP, Backup منظم
- لایه پنجم پاسخ: Incident Response Plan و تمرین دوره ای

جدول آدرس دهی

VLAN	Network	Gateway	Description
10	10.0.10.0/24	10.0.10.1	Management
20	10.0.20.0/24	10.0.20.1	Users
30	10.0.30.0/24	10.0.30.1	Servers
40	10.0.40.0/24	10.0.40.1	VoIP
50	10.0.50.0/24	10.0.50.1	Guest
60	10.0.60.0/24	10.0.60.1	Virtualization/Backup
DMZ	10.10.10.0/24	10.10.10.1	DMZ Zone

چگونه ایمیل های ارسال شده را Unsend کنیم؟

- ممکن است گاهی اوقات برخی از ایمیل‌ها را به اشتباه ارسال کنید یا در نوشتن بعضی از ایمیل‌های رسمی که ارسال شده، متوجه وجود یک غلط املایی شوید.
- اینجاست که برگرداندن ایمیل ارسالی می‌تواند یکی از بهترین گزینه‌های پیش روی شما باشد. در این مطلب قصد داریم چگونگی برگرداندن ایمیل های ارسالی از طریق جیمیل و Outlookرا توضیح بدم .

- به طور کلی امکان برگرداندن ایمیل‌های ارسالی در جیمیل امکان پذیر نیست. در واقع سرویس ایمیل گوگل به شما اجازه نمی‌دهد که پس از دریافت ایمیل ارسالی توسط مخاطب بتوانید آن را برگردانید. اما جیمیل برای رفع این نیاز راه **حلی نصفه و نیمه** دارد.

- در جیمیل وقتی روی **دکمه‌ی Send می‌زنید** با یک تاخیر چند ثانیه‌ای ایمیل به دست مخاطبتان می‌رسد و در این حین می‌توانید ارسال ایمیل را متوقف کنید.
- زمان یاد شده می‌تواند توسط کاربر تنظیم شود. بنابراین اگرچه امکان بازگرداندن ایمیل‌های ارسال شده وجود نخواهد داشت، اما با استفاده از روش پیش رو چند ثانیه زمان خواهید داشت تا ارسال پیام خود را لغو کنید.

- برای تنظیم زمان مورد نظر خود کافیست مراحل زیر را طی کنید:

- وارد حساب کاربری جیمیل خود شوید.
- از بالا سمت راست صفحه روی **چرخ دنده کلیک کرده** و سپس Settings را انتخاب کنید.
- از بخش Undo Send گزینه‌ی **Enable Undo Send** را فعال کنید.
- زیر گزینه‌ی قبل بخشی را مشاهده می‌کنید که با برچسب Send Cancellation periodمشخص شده است.
- در این بخش می‌توانید مقدار زمان مد نظر خود برای تاخیر ارسال ایمیل را مشخص کنید. گزینه‌های شما ۵، ۱۰، ۲۰ و ۳۰ ثانیه خواهند بود.
- در نهایت **Save Changes** را انتخاب کنید.

Settings

General | Labels | Inbox | Accounts and Import | Filters and Blocked Addresses | Forwarding and POP/IMAP | Add-ons | Chat and Meet | Advanced | Offline | Themes

Language:

Gmail display language: English (US) Change language settings for other Google products

☑ **Enable input tools** - Use various text input tools to type in the language of your choice - Edit tools - Learn more

◉ **Right-to-left editing support off**
○ **Right-to-left editing support on**

Phone numbers:

Default country code: Iran

Maximum page size:

Show 100 **conversations per page**

Undo Send:

Send cancellation period: 5 **seconds**

Default reply behavior:
Learn more

○ **Reply**
○ **Reply all**

Hover actions:

◉ **Enable hover actions** - Quickly gain access to archive, delete, mark as read, and snooze controls on hover.
○ **Disable hover actions**

Send and Archive:
Learn more

◉ **Show "Send & Archive" button in reply**
○ **Hide "Send & Archive" button in reply**

Default text style:
(Use the 'Remove formatting' button on the toolbar to reset the default text style)

Tahoma

This is what your body text will look like.

مهمترین فرمان CMD جهت امنیت داده پاک شده

Cipher – 1

پاک کردن فایل‌ها از روی یک دیسک سخت، به معنای آن نیست که این فایل‌ها و داده‌ها برای همیشه پاک شده‌اند، بلکه به این معناست که این فایل‌ها دیگر قابل دسترسی نیستند و فضای متعلق به آن‌ها آزاد شده است. این داده‌ها و فایل‌ها، همگی قابل بازیابی هستند، مگر آنکه با داده‌های جدید رونویسی شوند که این کار البته کمی زمان می‌برد.

فرمان cipher فضای آزاد روی حافظه شما را با داده‌های اتفاقی رونویسی و به این ترتیب از بازیابی داده‌های پاک شده جلوگیری می‌کند؛ مثلا برای پاکسازی کامل درایو C خود باید دستور cipher /w: c را اجرا کنید. این فرمان هیچ تأثیری بر داده‌ها و فایل‌هایی که پاک نشده، ندارد در نتیجه مشکلی برای سیستم عامل و داده‌های موجود شما درست نمی‌کند.

Command Prompt - cipher /w:d

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Iraj>cipher /w:d
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
.
```

Windows Registry attacks

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- **بدافزار Kovter** که کدهای آسیب پذیری خود را در حالت استارت آپ ویندوز داخل این مسیر قرار می دهد تا هربار که کاربرسیستم خود را بوت می کند این اسکریپت اجرا شود .

- **HKCU\Software\Classes\clsid**
- انتقال بدافزار از طریق به روز رسانی های جعلی
- یکی از این به روز رسانی های جعلی مربوط به کدهای مخرب Adobe Flash هست که در این کلید نوشته می شود . که با کلیک کاربر روی آپدیت منجر به انتقال بدافزار بر روی این کلید می شود .

- HKLM\System\CurrentControlSet\Services\svcname\ImagePath

- این کلید بیشتردرگیر حملات Image Path می باشد که این تهدیدات برای اجرای یک باینری مخرب است که هکر یک فایل اجرایی مخرب را طریق یک سرویس تغییر می دهد .

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

- این کلید برای تهدیدات سایبری که نیاز دسترسی گرفتن از راه دور را دارند می باشد . این دسترسی ها از طریق انتقال تروجان های RAT صورت می گیرد . که با هربار راه اندازی سیستم اجرا می شود

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- Ransomware Activation (Ryuk)

- این باج افزار در هنگام راه اندازی سیستم در این کلید قرار می گیرد و یک مقدار جدید اضافه می کند تا روال رمزگذاری خود را پیش ببرد .

- HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRestore

- تنظیمات ریجستری را تغییر می دهد تا بازیابی سیستم را کنترل کند و فعالیت های مخرب را در این کلید پنهان نماید . تا از بازیابی و پشتیبان گیری جلوگیری نماید . و در اصل ورود بدافزار به این قسمت عمل restore کردن یا بازیابی را غیرفعال می کند .

- HKLM\Software$$Antivirus Name]\RealTimeProtection

- این کلید ریجستری مرتبط با نرم افزار آنتی ویروس است و مقدار آن را روی صفر قرار میدهد تا محافظت از آنتی ویروس را خاموش یا غیرفعال کند .

- HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit
- User Logon Hijacking

- کلیدهای User init یا Shell برای اجرای اسکریپت های مخرب در هنگام ورود کاربر است

- HKLM\System\CurrentControlSet\Control\SessionManager\BootExecute
  - بدافزار روت کیت قبل از بوت شدن سیستم در کلید قرار می گیرد

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs
- DLL Hijacking
  - آسیب پذیری مربوط به فایل DLL که آن را با یک DLL جعلی عوض می کند

- HKLM\Software\Policies\Microsoft\WindowsFirewall\DomainProfil
  - کلیدهای عادی ریجستری را اصلاح یا حذف می کند تا عملیات عادی سیستم را مختل کند و هکر قوانین یا رول های فایروال را قبل از نفوذ غیرفعال می کند .

- **Endpointچیست؟**
- دیوایس هایی که به شبکه متصل می شوند و معمولا نقطه پایانی شبکه هستند مانند کامپیوتر، لپ تاپ، موبایل هوشمند، تبلت، سرور. Endpointدر شبکه و ... نقاط بسیار مهم و البته آسیب پذیر برای ورود، تخریب و... هستند.

- **EPPچیست؟**
- یک پلتفرم حفاظت از (Endpoint (Endpoint Protection Platformاست که راه حل یکپارچه امنیتی برای شناسایی و بلاک کردن تهدیدات در **سطح دستگاه ها** می باشد.

- معمولا شامل آنتی ویروس، ضد تروجان، رمزنگاری دیتا، فایروال، سیستم پیشگیری از نفوذ (IPS)و جلوگیری از نشت اطلاعات DLP است.

- EPPاز رایج ترین حملات سایبری جلوگیری می کند. EPPهای مرسوم ذاتا پیشگیرانه هستند و رویکرد آنها مبتنی بر امضاء می باشد.
- شناسایی تهدیدات جدید و تازه کشف شده بر اساس تهدیدات و فایل هایی که از قبل شناسایی کرده و با مطابقت دادن امضاء آنها انجام می شود.
- هرچند آخرین راهکارهای EPPتکامل یافته است و برای تکنیک های تشخیص روی طیف گسترده ای از تهدیدات استفاده می شود.
- **بعضی از EPPهای شناخته شده عبارتند از:**

- Kaspersky Lab Product
- McAfee Endpoint Protection Advanced Suite (Legacy)
- Windows Defender ATP
- SentinelOne Endpoint Protection Platform
- Symantec Endpoint Protection
- Trend Micro OfficeScan

- EDRچیست؟
- یک پلتفرم و سیستم امنیتی شناسایی و پاسخ (Endpoint Detection and Endpoint) Responseاست که المان های آنتی ویروس های نسل بعدی Next-Gen Antivirusبا ابزار های بیشتری مثل تشخیص و اعلان هشدار ناهنجاری های سیستمی به صورت Real Timeرا دارد و قابلیت تجزیه و تحلیل جرائم (Forensic Analysis)و قابلیت اصلاح Endpointرا با هم ترکیب می کند.

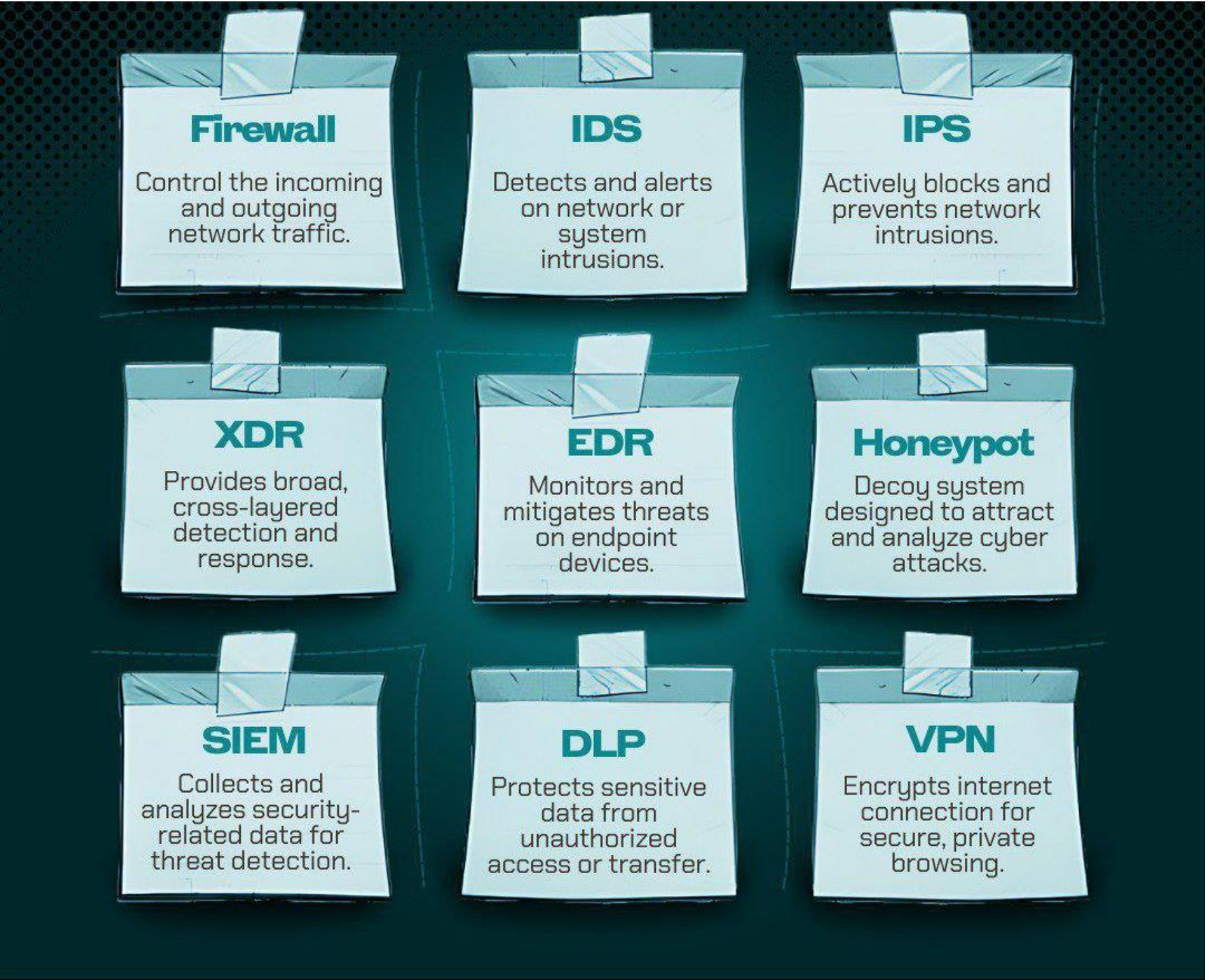
- EDRحملاتی را که شناسایی می کند که EPP نمی تواند آن را شناسایی و تشخیص دهد.

- با ثبت کردن وقایع هر گونه اجرا و تغییر فایل، تغییر در ریجستری، اتصال به شبکه و اجرای فایل های باینری در Endpointسازمان ها، قابلیت شناسایی تهدیدات در EDRبه مراتب بهتر از EPPمی شود.

- بعضی از EDRهای شناخته شده عبارتند از:

- CrowdStrike Falcon
- Carbon Black
- FireEye Endpoint Security (HX)
- RSA Netwitness Endpoint
- Endgame

- در مواجهه با این دو، انتخاب بین EDRو EPPآسان است. EPPیک مکانیزم دفاعی در خط اول مقابله با تهدیدات شناخته شده است.
- EDRلایه بعدی امنیتی است که ابزاری های بیشتری را برای شکار تهدیدات، تجزیه و تحلیل جرائم مربوط به نفوذ و پاسخگویی سریع و موثر به حملات در اختیار ما قرار می دهد.
- در حالیکه EDRیک انتخاب اولیه و راه حل برای سازمان ها وشرکت های بزرگ با مراکز عملیاتی Cyber Securityقرار گرفته است.
- پذیرش EDRدر حال افزایش است زیرا شناسایی تهدیدات به علاوه قابلیت پاسخگویی به آن – تهدید– ضروری برای سازمان ها،شرکت ها و... می باشد.



نقش های مهمی که در
تقویت دفاع امنیت
سایبری ایفا می کند

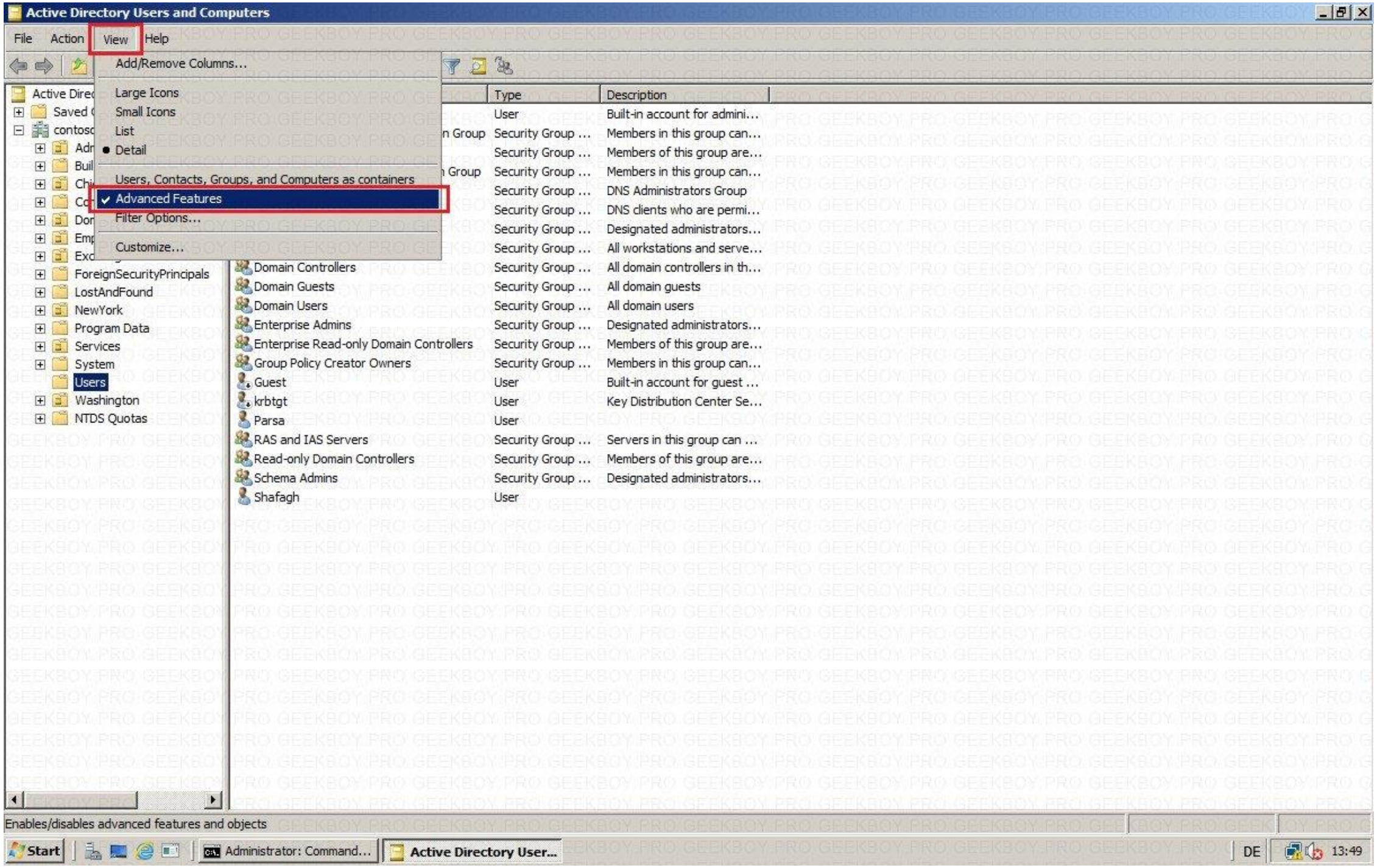
- **مواردی که نقش مهمی در تقویت دفاع امنیت سایبری ایفا می کند**
- **Firewall**
- ترافیک ورودی و خروجی شبکه را کنترل کنید.
- **IDS**
- شناسایی و هشدار در مورد نفوذ شبکه یا سیستم.
- **IPS**
- به طور فعال نفوذ شبکه را مسدود کرده و از آن جلوگیری می کند.
- **XDR**
- تشخیص و پاسخ گسترده و چند لایه را ارائه می دهد.
- **EDR**
- تهدیدها را در دستگاه های نقطه پایانی نظارت و کاهش می دهد.
- **Honeypot**
- سیستم فریب طراحی شده برای جذب و تجزیه و تحلیل حملات سایبری.
- **SIEM**
- داده های مربوط به امنیت را برای تشخیص تهدید جمع آوری و تجزیه و تحلیل می کند.
- **DLP**
- از داده های حساس در برابر دسترسی یا انتقال غیرمجاز محافظت می کند.
- **VPN**
- اتصال اینترنت را برای مرور امن و خصوصی رمزگذاری می کند.

چگونه مجوزهای واگذار شده در اکتیو دایرکتوری را ببینیم یا حذف کنیم

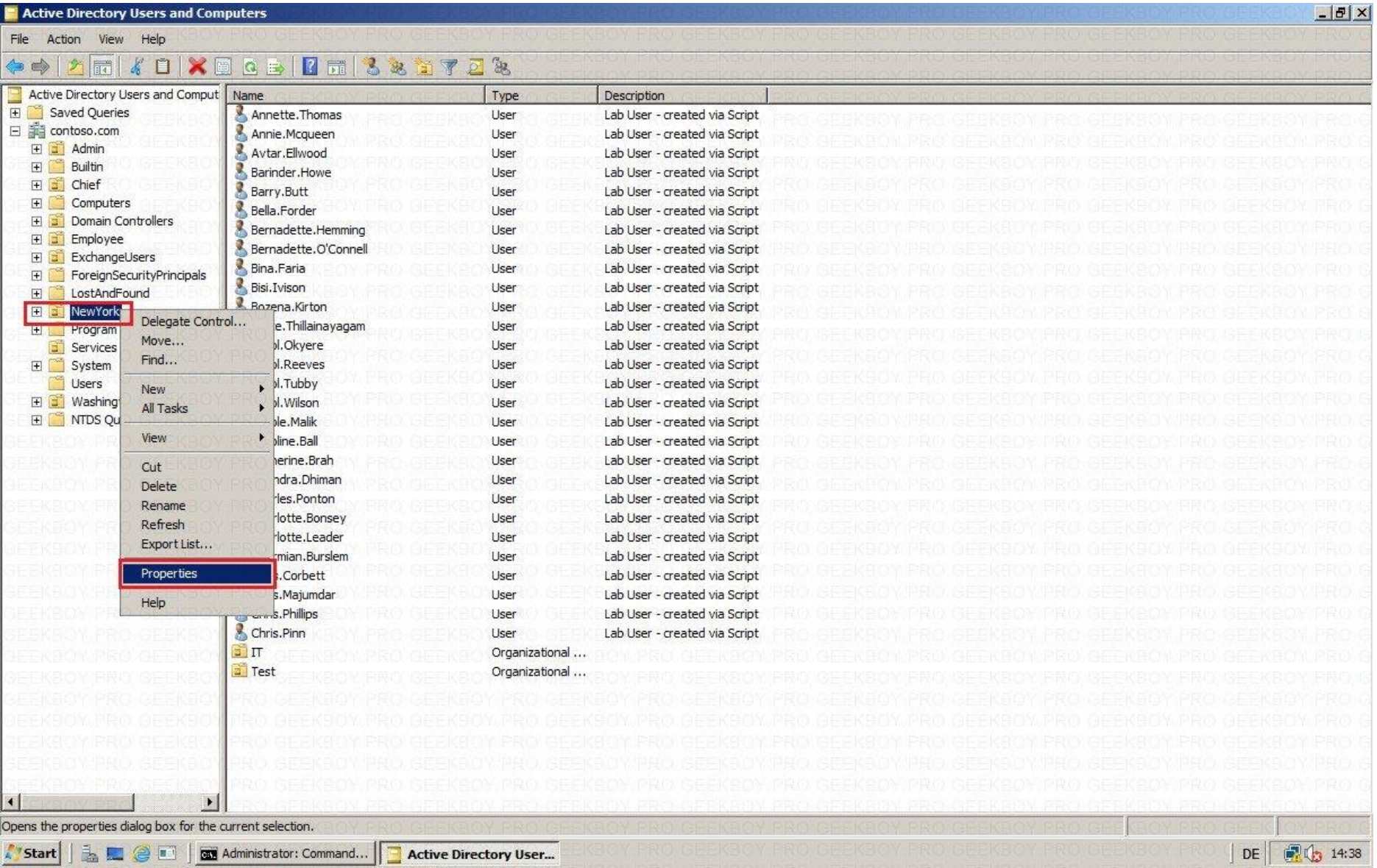
Microsoft
Active Directory

- چگونه مجوزهای واگذار شده در اکتیو دایرکتوری را ببینیم یا حذف کنیم؟ برای دیدن View یا حذف Delete مجوزهای واگذار شده Delegated Permissions در اکتیو دایرکتوری Active Directory – AD میتوان از روشهای زیر استفاده کرد.

- برای دیدن مجوزهای اختصاص داده شده assigned permissions بر روی یک Organizational Unit – OU میتوانیم از کنسول Active Directory Users and Computers استفاده کنیم.
- برای دیدن شما باید در قسمت View، قابلیت Advanced Features فعال کنید.


Active Directory Users and Computers
File
Action
View
Help
Add/Remove Columns...
Large Icons
Small Icons
List
Detail
Users, Contacts, Groups, and Computers as containers
Advanced Features
Filter Options...
Customize...
Type
Description
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
Enterprise Read-only Domain Controllers
Group Policy Creator Owners
Guest
krbtgt
Parsa
RAS and IAS Servers
Read-only Domain Controllers
Schema Admins
Shafagh
ForeignSecurityPrincipals
LostAndFound
NewYork
Program Data
Services
System
Users
Washington
NTDS Quotas
Enables/disables advanced features and objects
Start
Administrator: Command...
Active Directory User...
DE
13:49

- بعد از این کار، روی OU مورد نظر بطور مثال OU=NewYork کلیک سمت راست کرده و Properties را انتخاب میکنیم .



Active Directory Users and Computers

File Action View Help

2

Active Directory Users and Comput
- Saved Queries
- contoso.com
  - Admin
  - Builtin
  - Chief
  - Computers
  - Domain Controllers
  - Employee
  - ExchangeUsers
  - ForeignSecurityPrincipals

1

Name	Type
Annette.Thomas	User
Annie.Mcqueen	User
Avtar.Ellwood	User
Barinder.Howe	User
Barry.Butt	User
Bella.Forder	User
Bernadette.Hemming	User
Bernadette.O'Connell	User
Bina.Faria	User

Lab User - created via Script

NewYork Properties

General | Managed By | Object | Security | COM+ | Attribute Editor

Group or user names:
- SELF
- Authenticated Users
- SYSTEM
- Ed Price (Ed.Price@contoso.com)
- Domain Admins (CONTOSO\Domain Admins)
- Enterprise Admins (CONTOSO\Enterprise Admins)

Add... Remove

Permissions for SELF	Allow	Deny
Full control	☐	☐
Read	☐	☐
Write	☐	☐
Create all child objects	☐	☐
Delete all child objects	☐	☐

For special permissions or advanced settings, click Advanced.

Advanced

Learn about access control and permissions

OK Cancel Apply Help

Advanced Security Settings for NewYork

Permissions | Auditing | Owner | Effective Permissions

To view or edit details for a permission entry, select the entry and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Ed Price (Ed.Price@cont...	Special	<not inherited>	Descendant Group objects
Allow	Ed Price (Ed.Price@cont...	Create/delete Gro...		This object and all desce...
Allow	Ed Price (Ed.Price@cont...	Special		Descendant User objects
Allow	Ed Price (Ed.Price@cont...	Create/delete User...		This object and all desce...
Allow	SYSTEM	Full control	<not inherited>	This object only
Allow	Domain Admins (CONTO...	Full control	<not inherited>	This object only
Allow	Authenticated Users	Special	<not inherited>	This object only
Allow	ENTERPRISE DOMAIN ...	Special	<not inherited>	This object only
Allow	Account Operators (CON...	Create/delete Com...	<not inherited>	This object only
Allow	Account Operators (CON...	Create/delete User...	<not inherited>	This object only

ACEs

Add... Edit... Remove Restore defaults

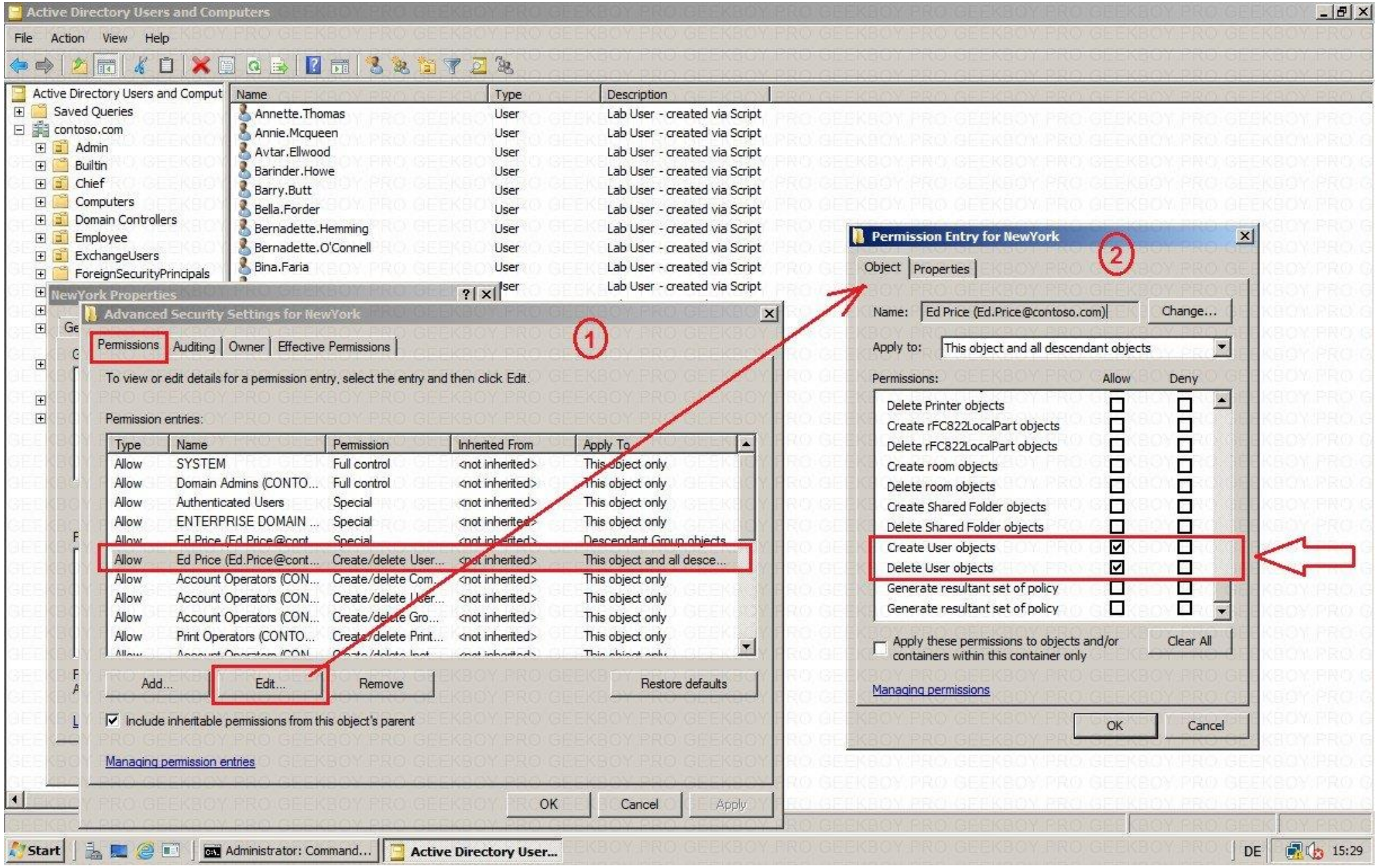
☑ Include inheritable permissions from this object's parent

Managing permission entries

OK Cancel Apply

Start | Administrator: Command... | Active Directory User... | DE | 15:11

- میتوانید از کنسول Active Directory Users and Computers استفاده کرده و این لیست را بهتر متوجه شوید



- لیزا LIZA یک برنامه مجانی است که توسط آن میتوان Security و Permission و ACL را بر روی اکتیو دایرکتوری Active Directory فقط دید یا آنالیز کرد.
- https://www.ldapexplorer.com/en/liza.htm

- با اجرای برنامه، در سمت راست ترکیب یا ساختار اکتیو دایرکتوری را در سمت راست میبینیم. با کلیک کردن بر روی OU=NewYork، در سمت راست میتوانیم تمام مجوزهای موجود برای OU=NewYork را ببینیم.
- همانطور که در عکس مشاهده میکنید، نام یوزر Ed.Price در آنجا است.

DC1.CONTOSO.COM [CONTOSO\administrator] - LIZA 1.5

Object OU=NewYork,DC=contoso,DC=com Go to

Objects (53)

- contoso.com
  - Admin
  - Builtin
  - Chief
  - Computers
  - Deleted Objects
  - Domain Controllers
  - Employee
  - ExchangeUsers
  - ForeignSecurityPrincipals
  - Infrastructure
  - LostAndFound
  - NewYork
  - NTDS Quotas
  - Program Data
  - Services
  - System
  - Users
  - Washington

Security Descriptor

Permissions | Audit | Owner

Type	I	Name	Scope	F	R	W	L	C	D	S	Propagation
Grant		[Authenticated Users]		☐	☑	☐	☐	☐	☐	☐	This object only
Grant		[Enterprise Domain Controllers]		☐	☑	☐	☐	☐	☐	☐	This object only
Grant	x	[Enterprise Domain Controllers]	'tokenGroups' attribute	☐	☑	☐	☐	☐	☐	☐	'computer' objects
Grant	x	[Enterprise Domain Controllers]	'tokenGroups' attribute	☐	☑	☐	☐	☐	☐	☐	'group' objects
Grant	x	[Enterprise Domain Controllers]	'tokenGroups' attribute	☐	☑	☐	☐	☐	☐	☐	'user' objects
Grant	x	[Self]		☐	☐	☐	☐	☐	☐	☑	This object and all child objects
Grant		[System]		☑	☑	☑	☑	☑	☑	☑	This object only
Grant		Account Operators	'computer' objects	☐	☐	☐	☐	☑	☑	☐	This object only
Grant		Account Operators	'group' objects	☐	☐	☐	☐	☑	☑	☐	This object only
Grant		Account Operators	'inetOrgPerson' objects	☐	☐	☐	☐	☑	☑	☐	This object only
Grant		Account Operators	'user' objects	☐	☐	☐	☐	☑	☑	☐	This object only
Grant	x	Administrators		☐	☐	☐	☐	☐	☐	☑	This object and all child objects
Grant		Domain Admins		☑	☑	☑	☑	☑	☑	☑	This object only
Grant		Ed Price		☑	☑	☑	☑	☑	☑	☑	'user' objects
Grant		Ed Price	'user' objects	☐	☐	☐	☐	☑	☑	☐	This object and all child objects
Grant	x	Enterprise Admins		☑	☑	☑	☑	☑	☑	☑	This object and all child objects
Grant	x	Pre-Windows 2000 Compatible Access		☐	☑	☐	☐	☐	☐	☐	'group' objects
Grant	x	Pre-Windows 2000 Compatible Access		☐	☑	☐	☐	☐	☐	☐	'inetOrgPerson' objects
Grant	x	Pre-Windows 2000 Compatible Access		☐	☐	☐	☑	☐	☐	☐	This object and all child objects
Grant	x	Pre-Windows 2000 Compatible Access		☐	☑	☐	☐	☐	☐	☐	'user' objects
Grant	x	Pre-Windows 2000 Compatible Access	Account Restrictions	☐	☑	☐	☐	☐	☐	☐	'inetOrgPerson' objects
Grant	x	Pre-Windows 2000 Compatible Access	Account Restrictions	☐	☑	☐	☐	☐	☐	☐	'user' objects
Grant	x	Pre-Windows 2000 Compatible Access	General Information	☐	☑	☐	☐	☐	☐	☐	'inetOrgPerson' objects
Grant	x	Pre-Windows 2000 Compatible Access	General Information	☐	☑	☐	☐	☐	☐	☐	'user' objects
Grant	x	Pre-Windows 2000 Compatible Access	Group Membership	☐	☑	☐	☐	☐	☐	☐	'inetOrgPerson' objects
Grant	x	Pre-Windows 2000 Compatible Access	Group Membership	☐	☑	☐	☐	☐	☐	☐	'user' objects
Grant	x	Pre-Windows 2000 Compatible Access	Logon Information	☐	☑	☐	☐	☐	☐	☐	'inetOrgPerson' objects
Grant	x	Pre-Windows 2000 Compatible Access	Logon Information	☐	☑	☐	☐	☐	☐	☐	'user' objects

☑ Inherit permissions from parent objects.

Show ACE

- اگر بخواهیم جزئیات ACEمربوط به یوزر Ed.Priceرا ببینم، روی یکی از این مجوزها کلیک کرده (روی اسم یوزر)، سپس در سمت راست، پایین دکمه Show ACLرا کلیک میکنیم.

DC1.CONTOSO.COM [CONTOSO\administrator] - LIZA 1.5

Object: OU=NewYork,DC=contoso,DC=com — Go to

Objects (53)

- contoso.com
  - Admin
  - Builtin
  - Chief
  - Computers
  - Deleted Objects
  - Domain Controllers
  - Employee
  - ExchangeUsers
  - ForeignSecurityPrincipals
  - Infrastructure
  - LostAndFound
  - NewYork
  - NTDS Quotas
  - Program Data
  - Services
  - System
  - Users
  - Washington

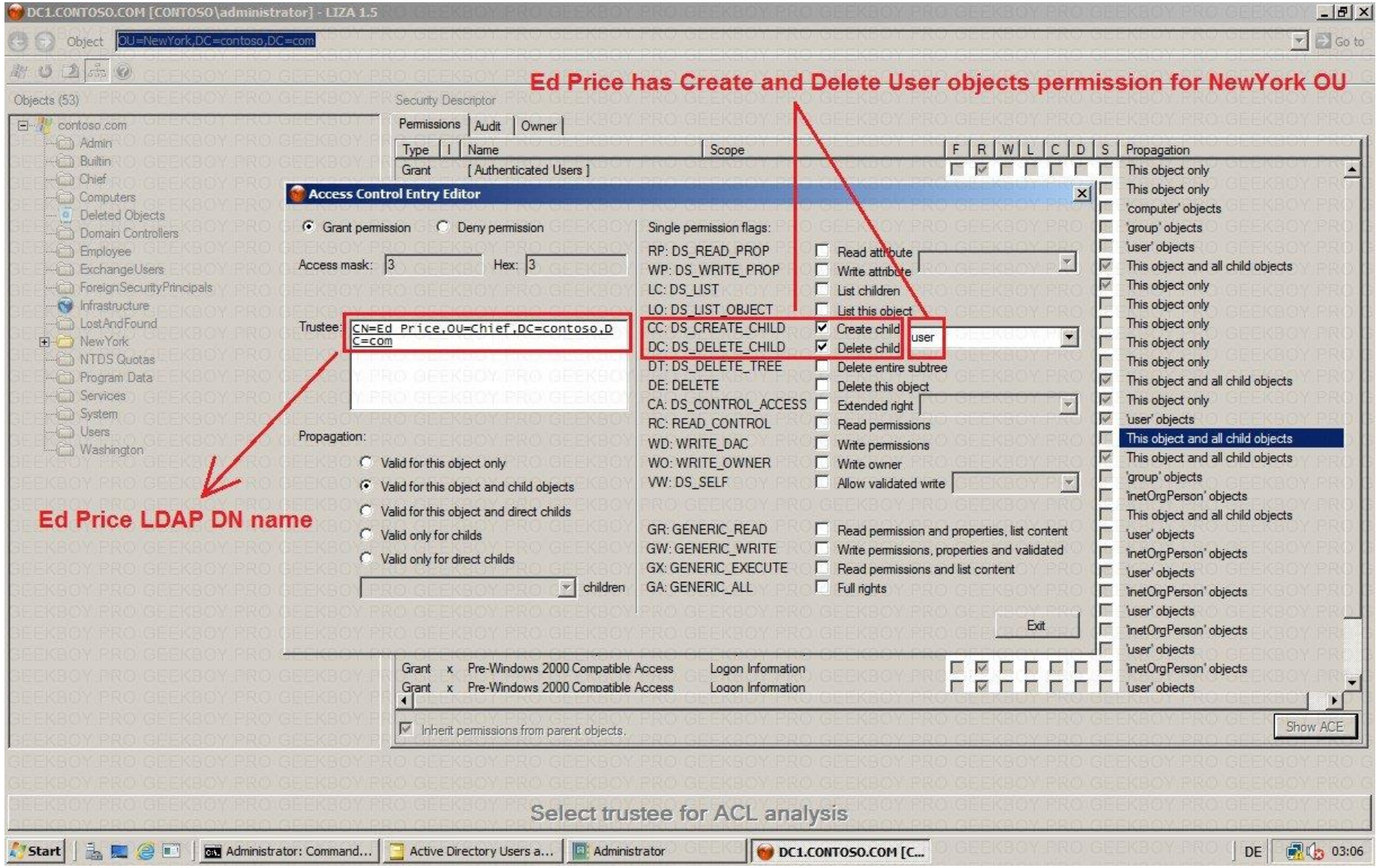
Security Descriptor — Permissions | Audit | Owner

Type	I	Name	Scope	F	R	W	L	C	D	S	Propagation
Grant		[Authenticated Users]			✓						This object only
Grant		[Enterprise Domain Controllers]			✓						This object only
Grant	x	[Enterprise Domain Controllers]	'tokenGroups' attribute		✓						'computer' objects
Grant	x	[Enterprise Domain Controllers]	'tokenGroups' attribute		✓						'group' objects
Grant	x	[Enterprise Domain Controllers]	'tokenGroups' attribute		✓						'user' objects
Grant	x	[Self]								✓	This object and all child objects
Grant		[System]		✓	✓	✓	✓	✓	✓	✓	This object only
Grant		Account Operators	'computer' objects					✓	✓		This object only
Grant		Account Operators	'group' objects					✓	✓		This object only
Grant		Account Operators	'inetOrgPerson' objects					✓	✓		This object only
Grant		Account Operators	'user' objects					✓	✓		This object only
Grant	x	Administrators								✓	This object and all child objects
Grant		Domain Admins		✓	✓	✓	✓	✓	✓	✓	This object only
Grant		Ed Price		✓	✓	✓	✓	✓	✓	✓	'user' objects
Grant		Ed Price	'user' objects					✓	✓		This object and all child objects
Grant	x	Enterprise Admins		✓	✓	✓	✓	✓	✓	✓	This object and all child objects
Grant	x	Pre-Windows 2000 Compatible Access			✓						'group' objects
Grant	x	Pre-Windows 2000 Compatible Access			✓						'inetOrgPerson' objects
Grant	x	Pre-Windows 2000 Compatible Access					✓				This object and all child objects
Grant	x	Pre-Windows 2000 Compatible Access			✓						'user' objects
Grant	x	Pre-Windows 2000 Compatible Access	Account Restrictions		✓						'inetOrgPerson' objects
Grant	x	Pre-Windows 2000 Compatible Access	Account Restrictions		✓						'user' objects
Grant	x	Pre-Windows 2000 Compatible Access	General Information		✓						'inetOrgPerson' objects
Grant	x	Pre-Windows 2000 Compatible Access	General Information		✓						'user' objects
Grant	x	Pre-Windows 2000 Compatible Access	Group Membership		✓						'inetOrgPerson' objects
Grant	x	Pre-Windows 2000 Compatible Access	Group Membership		✓						'user' objects
Grant	x	Pre-Windows 2000 Compatible Access	Logon Information		✓						'inetOrgPerson' objects
Grant	x	Pre-Windows 2000 Compatible Access	Logon Information		✓						'user' objects

☑ Inherit permissions from parent objects.

Show ACE

1 Click on Ed Price name

2 Click Show ACE

- حالا مشاهده میکنید که یوزر Ed.Price بر روی OU=NewYork دارای مجوز ساختن یوزر Create User objects و پاک کردن یوزر Delete User objects را دارد.