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:

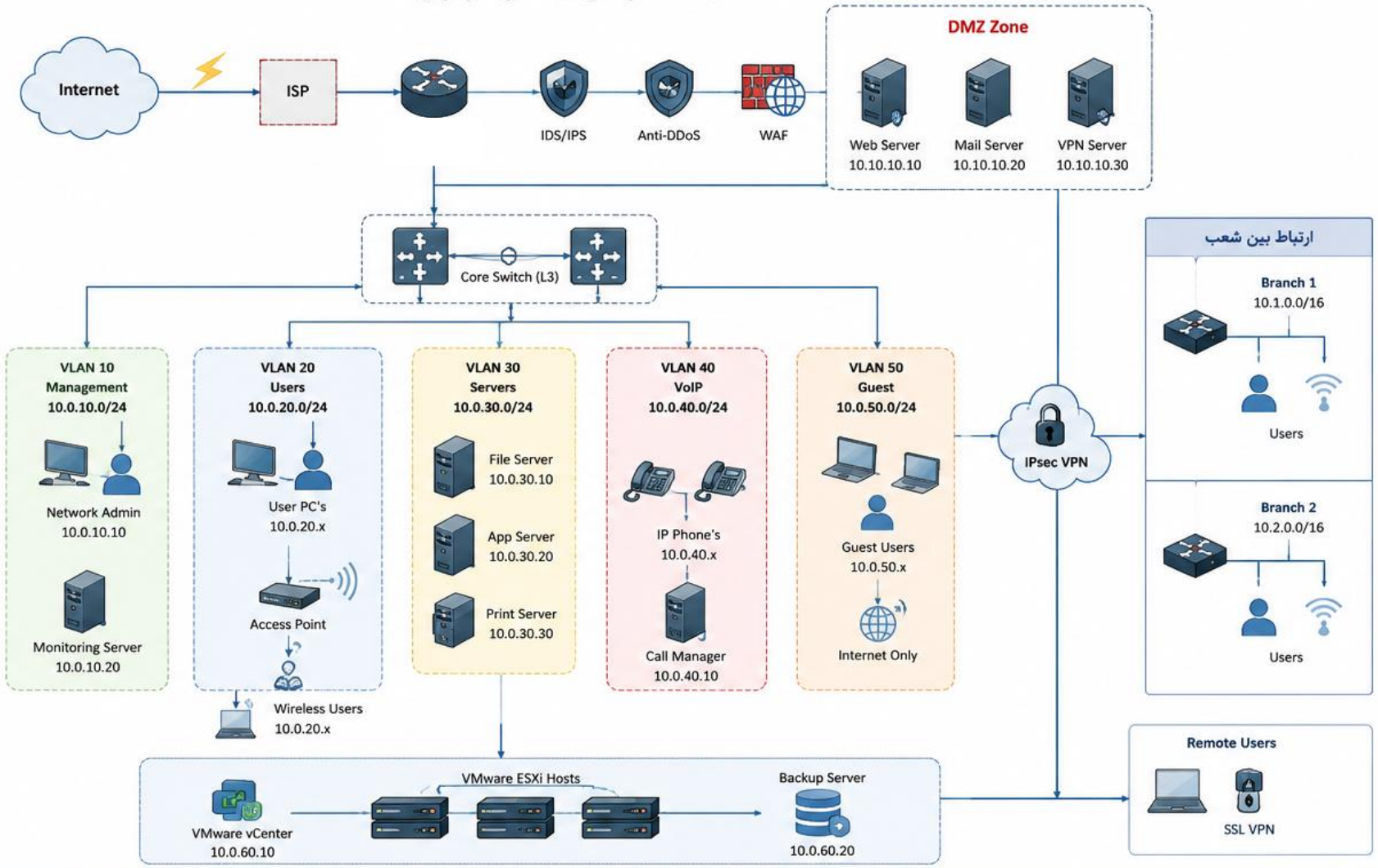
- سرویس های دایرکتوری (Active Directory)
- سرورهای فایل و پرینت
- سرور برنامه کاربردی تحت وب
- سیستم تلفنی تحت شبکه (VoIP)
- دسترسی کاربران به اینترنت
- ارتباط امن بین شعب از طریق VPN
- زیرساخت مجازی سازی با VMware

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

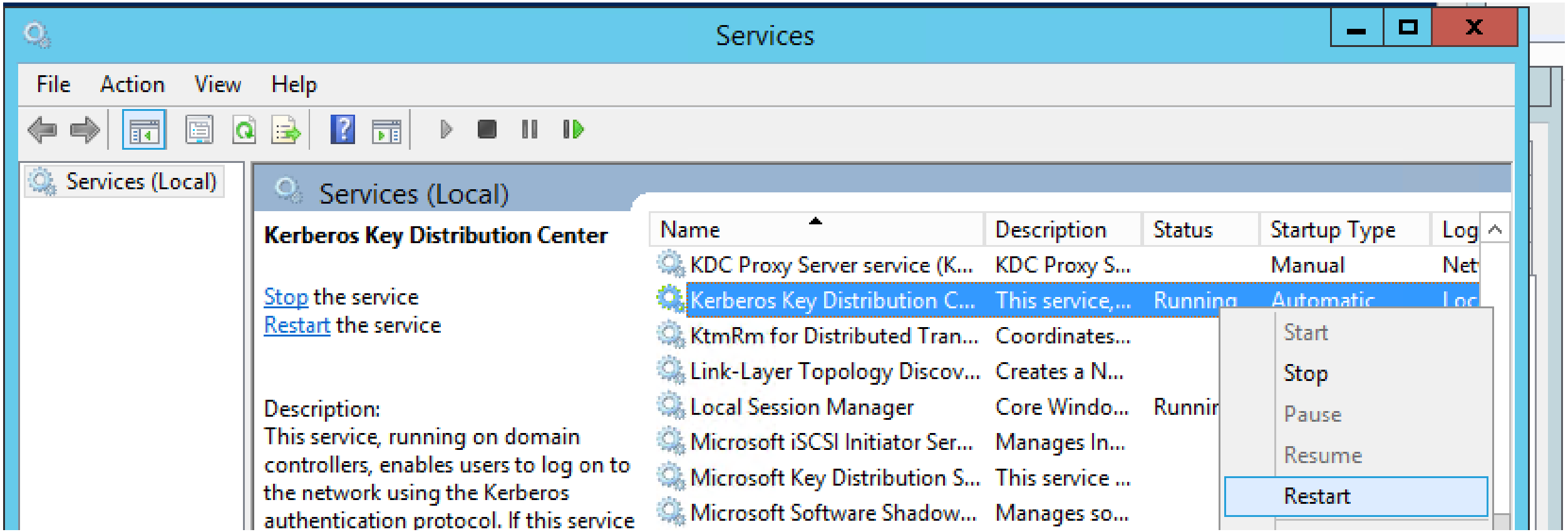
- زمانی که سرور را به Domain Controllerارتقا میدهید، اکانتی به نام krbtgtساخته میشود. اما در حقیقت اغلب ادمین های اکتیو دایرکتوری دانش کافی درباره این اکانت ندارند هرچند این اکانت از نظر امنیتی و کارکرد domainبسیار حائز اهمیت است.

- اکانت krbtgtبا RIDبه شماره ۵۰۲ در زمانی که اولین Domain Controllerساخته میشود، ایجاد میگردد. این اکانت به صورت پیشفرض غیر فعال است و به دو security groupاعمال میشود:

- Domain Usersو .Denied RODC Password Replication Groupنمیتوانید نام این اکانت را تغییر دهید، فعال کنید یا آن را حذف نمایید. این اکانت برای کار کردن KDCو Kerberosدر اکتیو دایرکتوری بسیار مهم است.

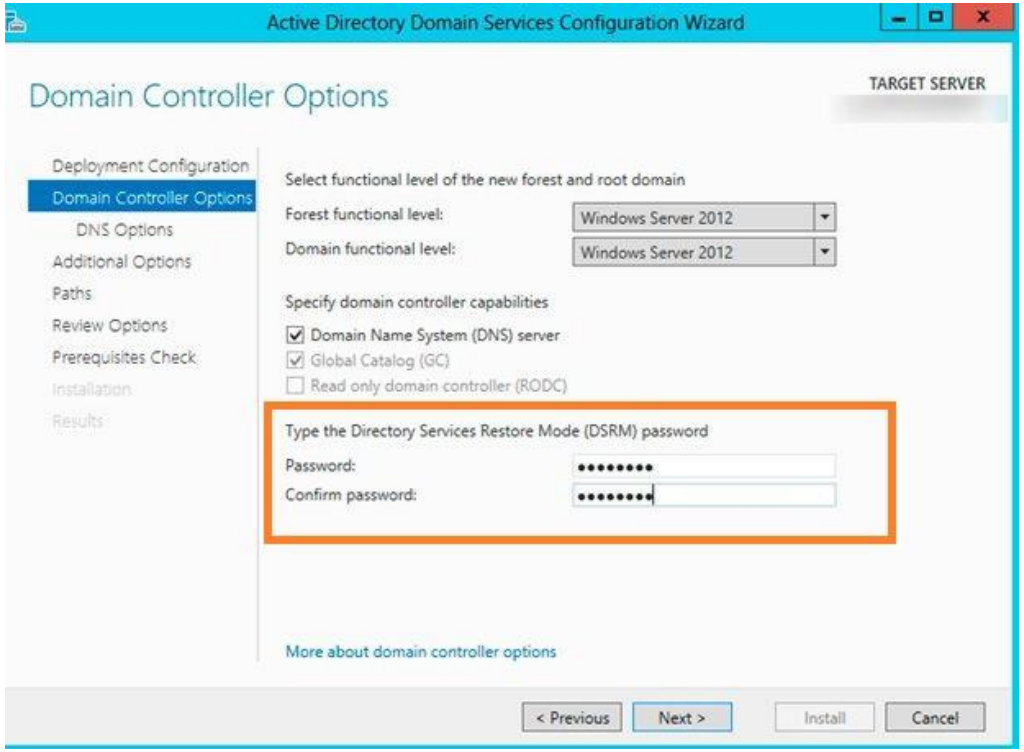
- سرویس (KDC (Kerberos Distributionکه روی domain controllerاجرا میشود و وظیفه اش پردازش کردن درخواست های Kerberosاست. برای ایجاد یک کلید خصوصی که برای رمزنگاری و رمزگشایی بلیط های TGTکاربرد دارد، رمز عبور اکانت krbtgtاستفاده میشود.

- برای کاهش ریسک تغییر رمز عبور krbtgt باید سرویس Kerberos Key Distribution Centerرا روی همه domain controllerها با استفاده از کنسول services.mscریست کنید (روی Kerberos Key Distribution Centerکلیک راست کنید و سپس Restartبزنید.)
- بنا به توصیه مایکروسافت هر ۱۸۰ روز یکبار پسورد یوزر KRBTGTرا ریست کنید



- Directory Services Restore Mode یا DSRM یک boot mode خاص در دامین کنترلر است. هنگامی که سرور Active Directory از کار افتاد یا object نیاز به بازیابی و Restore شدن دارد DC را در این حالت بوت می کنیم و با آن به ویندزو لاگین می کنیم.

- هنگام پیکربندی Active Directory از ما خواسته می شود که پسورد DSRM را هم تخصیص دهید. اکانتی که با آن در این حالت لاگین می کند Administrator است ولی متفاوت از Administrator دامین است. این اکانت فقط برای بوت سیستم در حالت DSRM و لاگین استفاده می شود.



- اگر شماپسورد DSRMرا فراموش کرده باشید و یا به هر دلیلی پسورد DSRMرا ندارید، می توانید آن را ریست کنید.
- برای این منظور در ویندوز سرورتان Command Promptرا به صورت Run as administratorاجرا کرده و سپس دستورات زیر را یک به یک وارد کنید:

Administrator: Command Prompt - ntdsutil

```
Microsoft Windows [Version 10.0.17763.1]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ntdsutil
ntdsutil: set dsrm password
```

```
Reset DSRM Administrator Password: reset password on server null
Please type password for DS Restore Mode Administrator Account: **********
Please confirm new password: **********
Password has been set successfully.

Reset DSRM Administrator Password: quit
ntdsutil: quit

C:\Users\Administrator>
```

- ولی یادتون باشه این تغییرات باید هر چه سریعتر به DCهای دیگر Replicationشود وگرنه سرویس های مثل Exchangeیا احرازهویت کاربران، دسترسی کاربران به سرویسها مختل می شود. (روزهای تعطیل اینکار را انجام دهید).

- Directory Services Restore Mode (DSRM)

- پسورد DSRMرا نیز باید به ترتیب هر نیم سال یا ۱۸۲ روز یکبار ریست شود:

- برای اینکار:

Administrator: Windows PowerShell

```
PS C:\Windows\system32> cmd
Microsoft Windows [Version 10.0.17763.1397]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ntdsutil
ntdsutil: set dsrm password
Reset DSRM Administrator Password: reset password on server dc-1
Please type password for DS Restore Mode Administrator Account: ********
Please confirm new password: ********
Password has been set successfully.

Reset DSRM Administrator Password: quit
ntdsutil: quit
```

راه اندازی یک دامین کنترولر در حالت Directory Services Restore Mode

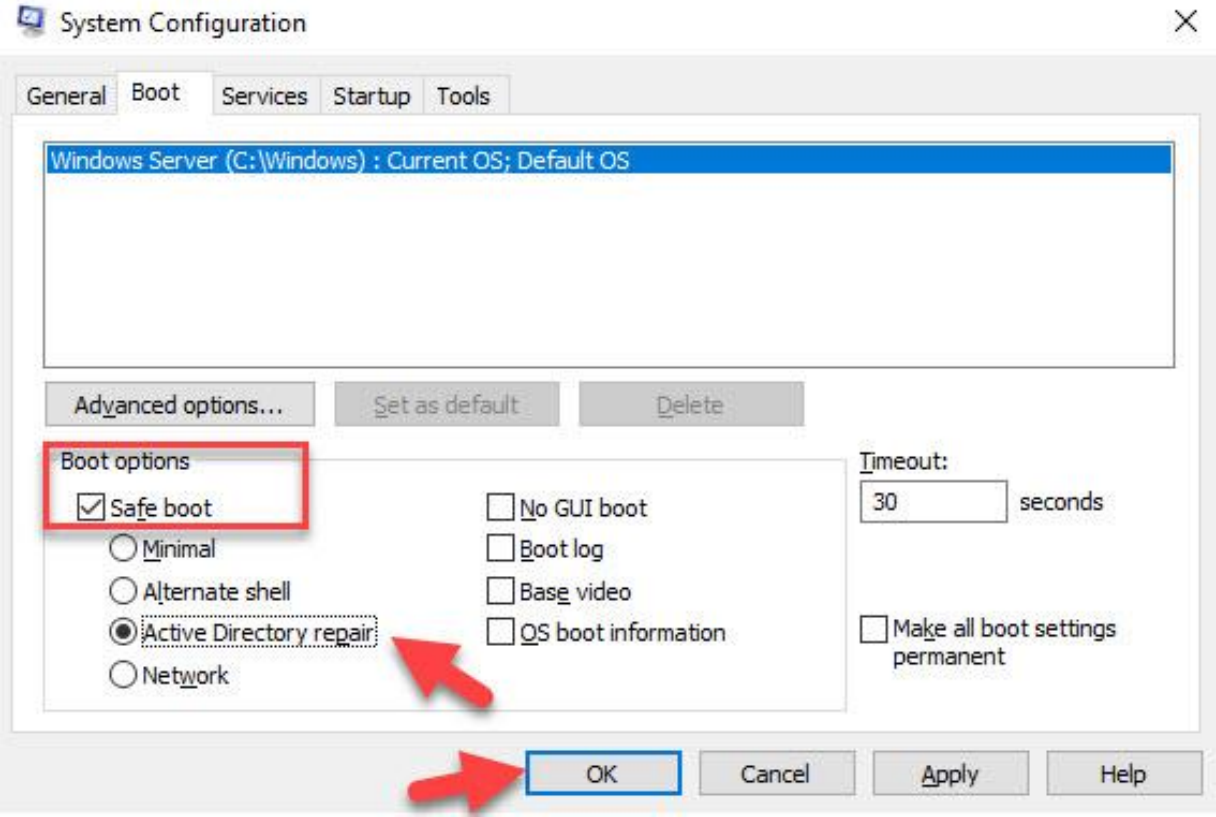
- قبل از آنکه بخواهید سروریس دومین اکتیو دایرکتوری را به زور forceحذف کنید، شما باید دومین کنترولر را با مد Directory Services Restore Modeراه اندازی کنید.

- راه اندازی با این مد، دومین کنترولر را به مد offlineمیبرد، این به آن معنا است که قابلیتهای آن مانند یک سرور memberمیشود و نه مانند یک دومین کنترولر.

- در طول نصب کردن سرویس دومین اکتیو دایرکتوری، شما یک پسورد برای Logonکردن به مد Directory Services Restore Modeست کرده بودید .

حالا برای اینکه در حالت DSRMبه ویندوز لاگین کنید، Runرا باز کرده و دستور MSConfigرا وارد و Enterکنید تا پنجره System Configurationباز شود.

در این پنجره به تب Bootرفته و از قسمت Boot optionsتیک گزینه Safe Boots را فعال کرده و گزینه Active Directory Repairرا فعال و OKکنید.



- تکمیل و بهبود تنظیمات Auditing:

- تنظیمات پیش فرض سیاستهای Auditing در دومین مناسب و ناکافی می باشد و شما نمی توانید تمام تراکنش های انجام شده در ساختار را Track کنید.
-

Policy Path	Policy Setting	Configured setting
Account Logon	Audit Credential Validation	Failure
Account Logon	Audit Kerberos Authentication Service	Success and Failure
Audit Logon	Audit Kerberos Service Ticket Operations	Failure
Account Management	Audit Computer Account Management	Success
Account Management	Audit Other Account Management	Success
Account Management	Audit Security Group Management	Success
Account Management	Audit User Account Management	Success and Failure
Detailed Tracking	Audit PNP Activity	Success
Detailed Tracking	Audit Process Creation	Success
DS Access	Audit Directory Services Access	Failure

Success	Audit Directory Service Changes	DS Access
Failure	Audit Account Lockout	Logon/Logoff
Success	Audit Group Membership	Logon/Logoff
Success and Failure	Audit Logon	Logon/Logoff
Success and Failure	Audit Other Logon/Logoff Events	Logon/Logoff
Success	Audit Special Logon	Logon/Logoff
Failure	Audit Detailed File Share	Object Access
Success and Failure	Audit File Share	Object Access
Success and Failure	Audit Other Object Access	Object Access
Success and Failure	Audit Removable Storage	Object Access
Success	Audit Policy Change	Policy Change
Success	Audit Authentication Policy Change	Policy Change
Success and Failure	Audit MPSSVC Rule-Level Pol-icy Change	Policy Change

Failure	Audit Other Policy Change Events	Policy Change
Success and Failure	Audit Sensitive Privilege Use	Privilege Use
Success and Failure	Audit Other System Events	System
Success	Audit Security State Change	System
Success	Audit Security System Extension	System
Success and Failure	Audit System Integrity	System

پیکربندی دستگاه های بیسیم که از windows Connect now استفاده میکنند بایدغیرفعال باشد.

- اجازه افشا و پیکربندي دستگاه هایی که بصورت بیسیم هستند رامیدهد. دستگاه هاي بیسیم باید مدیریت شوند. اگر یک دستگاه ناشناس مشکوك به سیستم متصل شود یک خطر بالقوه براي اطلاعات حساس هست که ممکن است فاش بشوند

- Administrative Templates -> Network -> Windows Connect Now -> "Configuration of wireless settings using Windows Connect Now" to "Disabled".

Group Policy Management Editor

File Action View Help

- Control Panel
- Network
  - Background Intelligent Transfer Service
  - BranchCache
  - DirectAccess Client Experience Settings
  - DNS Client
  - Fonts
  - Hotspot Authentication
  - Lanman Server
  - Lanman Workstation
  - Link-Layer Topology Discovery
  - Microsoft Peer-to-Peer Networking Ser
  - Network Connections
  - Network Connectivity Status Indicator
  - Network Isolation
  - Network Provider
  - Offline Files
  - QoS Packet Scheduler
  - SNMP
  - SSL Configuration Settings
  - TCPIP Settings
  - Windows Connect Now
  - Windows Connection Manager
  - Wireless Display

Windows Connect Now

Configuration of wireless settings using Windows Connect Now

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting allows the configuration of wireless settings using Windows Connect Now (WCN). The WCN Registrar enables the discovery and configuration of devices over Ethernet (UPnP), over In-band 802.11 WLAN, through the Windows Portable Device API (WPD), and via USB Flash drives.

Additional options are available to allow discovery and configuration over a specific medium.

If you enable this policy setting, additional choices are available to turn off the operations over a

Setting	Stat
Prohibit access of the Windows Connect Now wizards	Not conf
Configuration of wireless settings using Windows Connect Now	Not conf

Extended Standard

Explorer Data Execution Prevention باید فعال باشد

- DEP (Prevention Execution Data) حفاظت بیشتری را از طریق چک کردن حافظه برای
- جلوگیری از اجرای کدهای مخرب کمک میکند فراهم میکند.

- Administrative Templates -> Windows Components -> File Explorer -> "Turn off Data Execution Prevention for Explorer" to "Disabled".

Group Policy Management Editor

File Action View Help

- AutoPlay Policies
- Biometrics
- BitLocker Drive Encryption
- Camera
- Cloud Content
- Connect
- Credential User Interface
- Data Collection and Preview Builds
- Delivery Optimization
- Desktop Gadgets
- Desktop Window Manager
- Device and Driver Compatibility
- Device Registration
- Digital Locker
- Edge UI
- Event Forwarding
- Event Log Service
- Event Logging
- Event Viewer
- File Explorer
- File History
- Find My Device
- Handwriting
- HomeGroup

File Explorer

Turn off Data Execution Prevention for Explorer

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:
Disabling data execution prevention can allow certain legacy plug-in applications to function without terminating Explorer.

Setting	State
Previous Versions	
Verify old and new Folder Redirection targets point to the same share before re...	Not configured
Set a default associations configuration file	Not configured
Location where all default Library definition files for users/machines reside.	Not configured
Disable binding directly to IPropertySetStorage without intermediate layers.	Not configured
Allow the use of remote paths in file shortcut icons	Not configured
Configure Windows Defender SmartScreen	Not configured
Start File Explorer with ribbon minimized	Not configured
Do not show the 'new application installed' notification	Not configured
Turn off numerical sorting in File Explorer	Not configured
Turn off shell protocol protected mode	Not configured
Show hibernate in the power options menu	Not configured
Show lock in the user tile menu	Not configured
Show sleep in the power options menu	Not configured
Set a support web page link	Not configured
Do not reinitialize a pre-existing roamed user profile when it is loaded on a mac...	Not configured
Turn off Data Execution Prevention for Explorer	Not configured
Turn off heap termination on corruption	Not configured

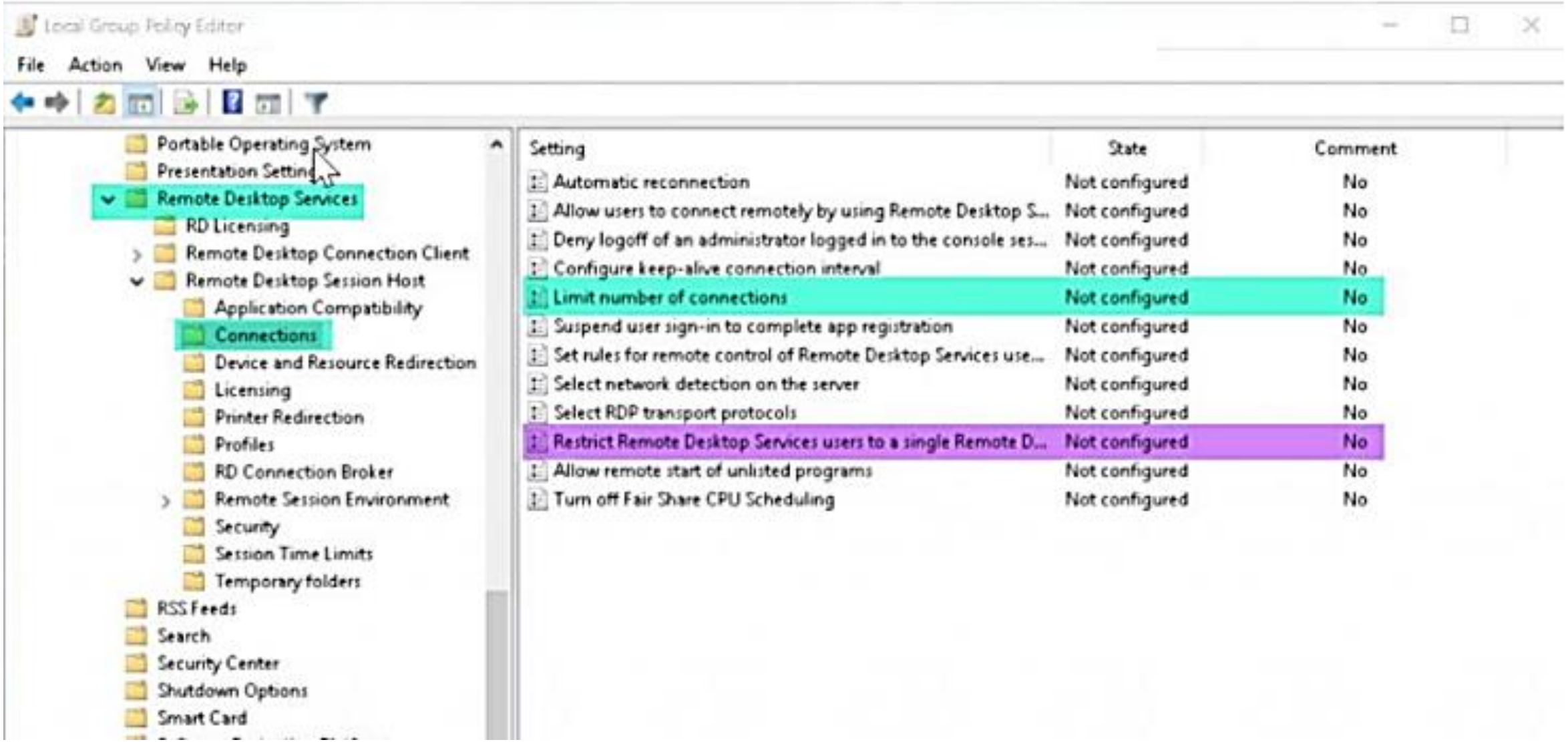
محدودیت ریموت دسکتاپ در سرور مایکروسافت

- **تنظیم محدودیت و ست کردن عدد زیاد برای تعداد نشست RDPدو مشکل احتمالی برای شما ایجاد خواهد کرد :**

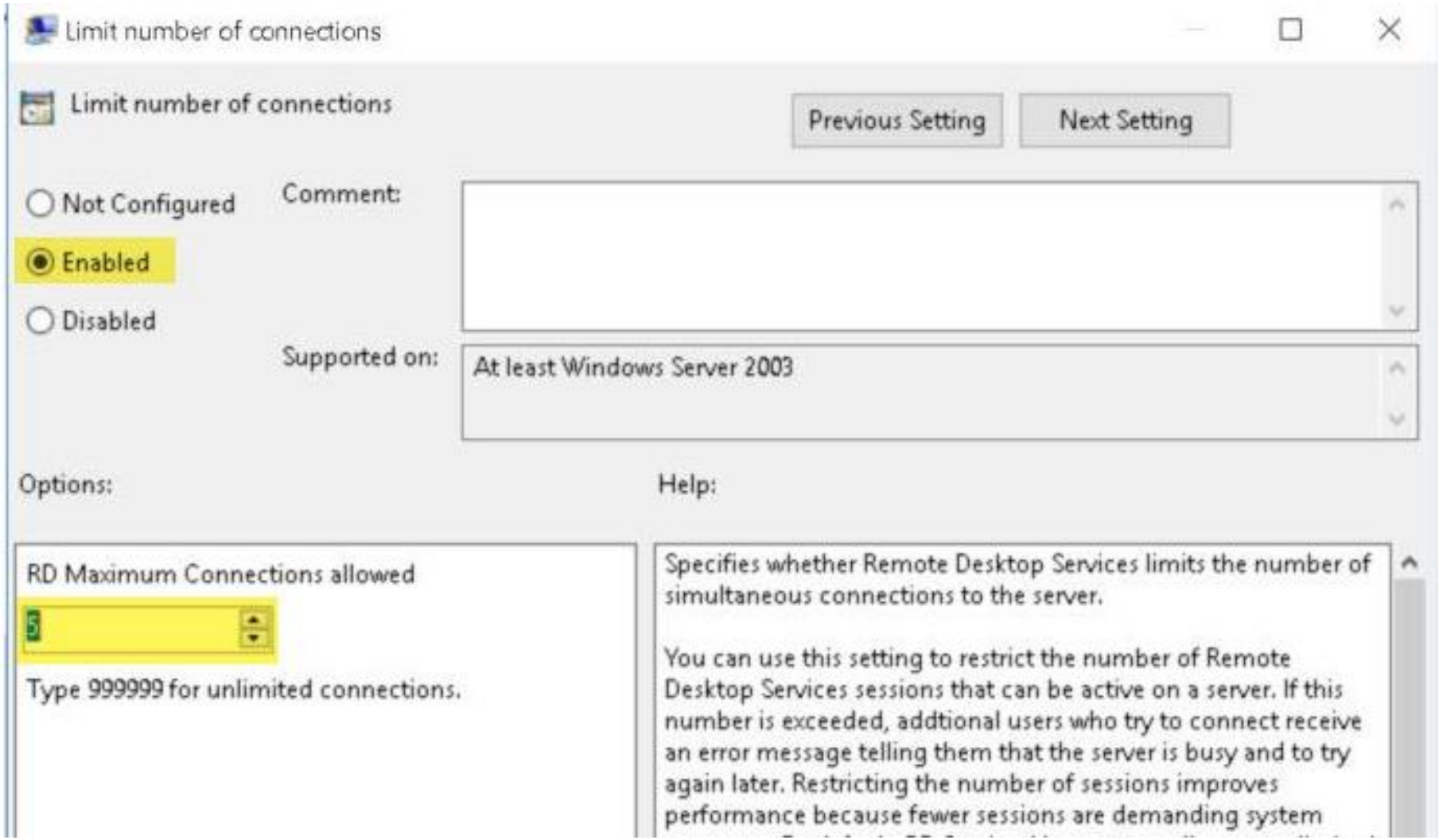
- اینکه اگر سرور شما هک شود احتمال اینکه متوجه آن بشوید چون کاربر دیگر همزمان به سرور متصل می شود کمتر می شود و همیشه باید حواستان به گزارش رخداد های اتصال موفق ریموت دسکتاپ باشد.

- اگر اجازه تعداد زیادی کاربر همزمان را به سرور بدهید ممکن است دچار کمبود منابع پردازشی روی سرور شوید ، چون هر اتصال کاربر نیاز به مقداری رم و منابع پردازنده خواهد داشت و هر یک از برنامه هایی که آنها اجرا کنند نیز منابع بیشتری اشغال خواهد نمود.

- محدودیت تعداد کاربر ریموت دسکتاپ همزمان را بر اساس توان پردازشی و رم سرور ویندوز خود ست کنید، زیرا اتصال کاربر متصل شده مقداری از رم و منابع پردازنده را اشغال خواهد کرد ، همچنین هر یک از برنامه‌هایی که آنها اجرا کنند نیز منابع بیشتری اشغال خواهد نمود



- ابتدا بر روی Limit number of connection کلیک کرده تا باز شود و پس از انتخاب گزینه Enabled تعداد مجاز کانکشن‌ها را در فیلد مشخص شده وارد کنید و بر روی Apply کلیک نمایید.



- بعد گزینه Restrict Remote Desktop Services users to a single Remote Desktop Services sessionرا انتخاب کرده تا باز شود و تنظیم را بر روی Disableقرار داده و Applyرا بزنید.
- حال شما می‌توانید چندین Remote Desktopرا به صورت همزمان داشته باشید.

نکاتی درباره مدیریت آسیب پذیری ها

- همه سیستم ها را حداقل یک بار در ماه اسکن کنید تا آسیب پذیری های بالقوه را پیدا کنید. البته توصیه میشود که اسکن ها را در بازه زمانی کوتاه تری انجام دهید.
- آسیب پذیری ها را اولویت بندی کنید و اقدام به برطرف کردن آسیب پذیری ها با اولویت بالا کنید.
- بروزرسانی ها را روی سیستم عامل به صورت اتوماتیک اعمال کنید.
- بروزرسانی ها را روی نرم افزار های شخص ثالث به صورت اتوماتیک اعمال کنید.
- نرم افزارهای تاریخ مصرف گذشته را پیدا و آن ها را بروزرسانی کنید.