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:

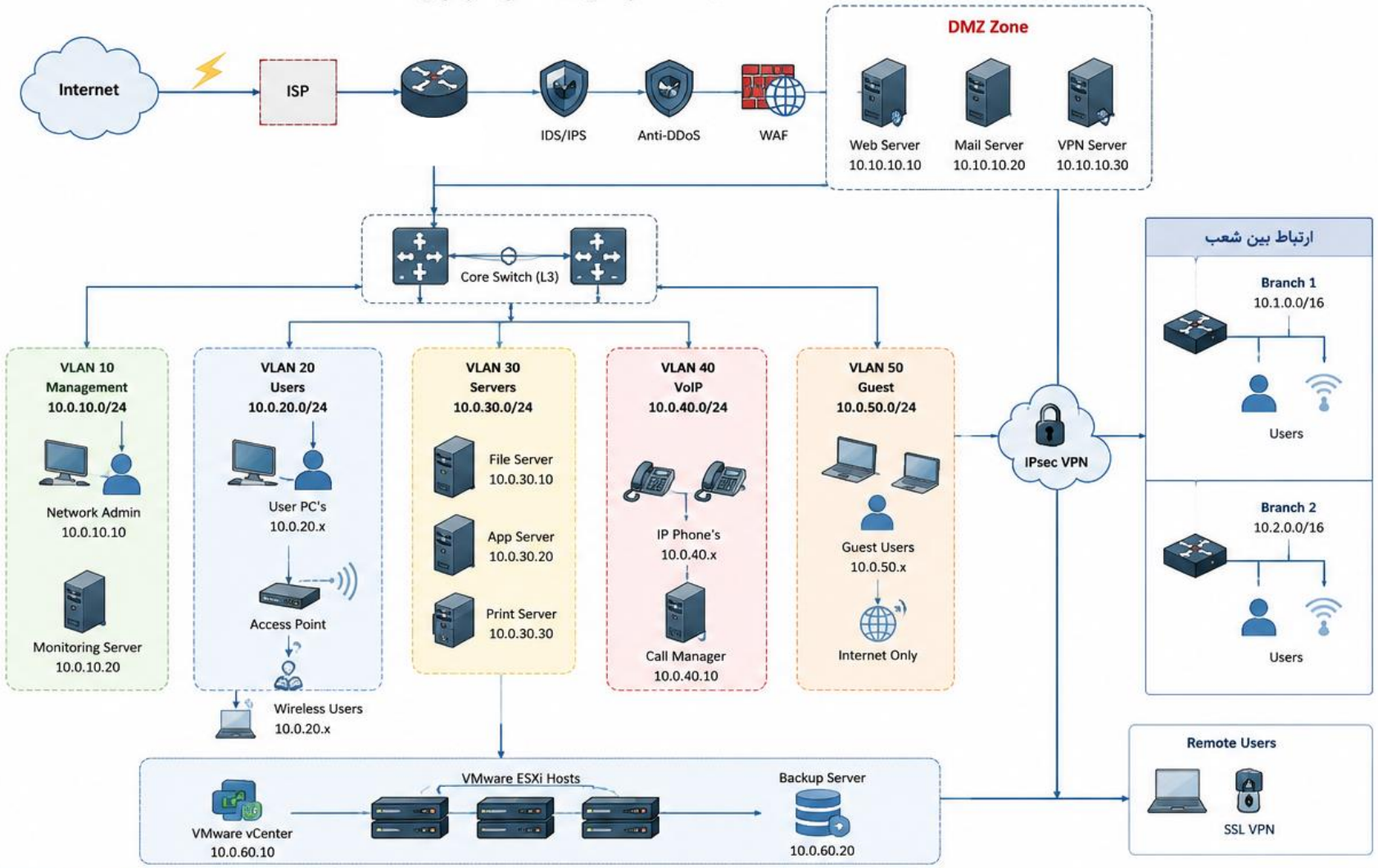
- سرویس های دایرکتوری (Active Directory)
- سرورهای فایل و پرینت
- سرور برنامه کاربردی تحت وب
- سیستم تلفنی تحت شبکه (VoIP)
- دسترسی کاربران به اینترنت
- ارتباط امن بین شعب از طریق VPN
- زیرساخت مجازی سازی با VMware

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

غیرفعال کردن NTLM

- غیرفعال کردن **NTLM (NT LAN Manager)** در Active Directory به این دلیل انجام می‌شود که NTLM یک **پروتکل احراز هویت قدیمی و ناامن‌تر** نسبت به Kerberos است و در بسیاری از حملات رایج AD مورد سوءاستفاده قرار می‌گیرد.

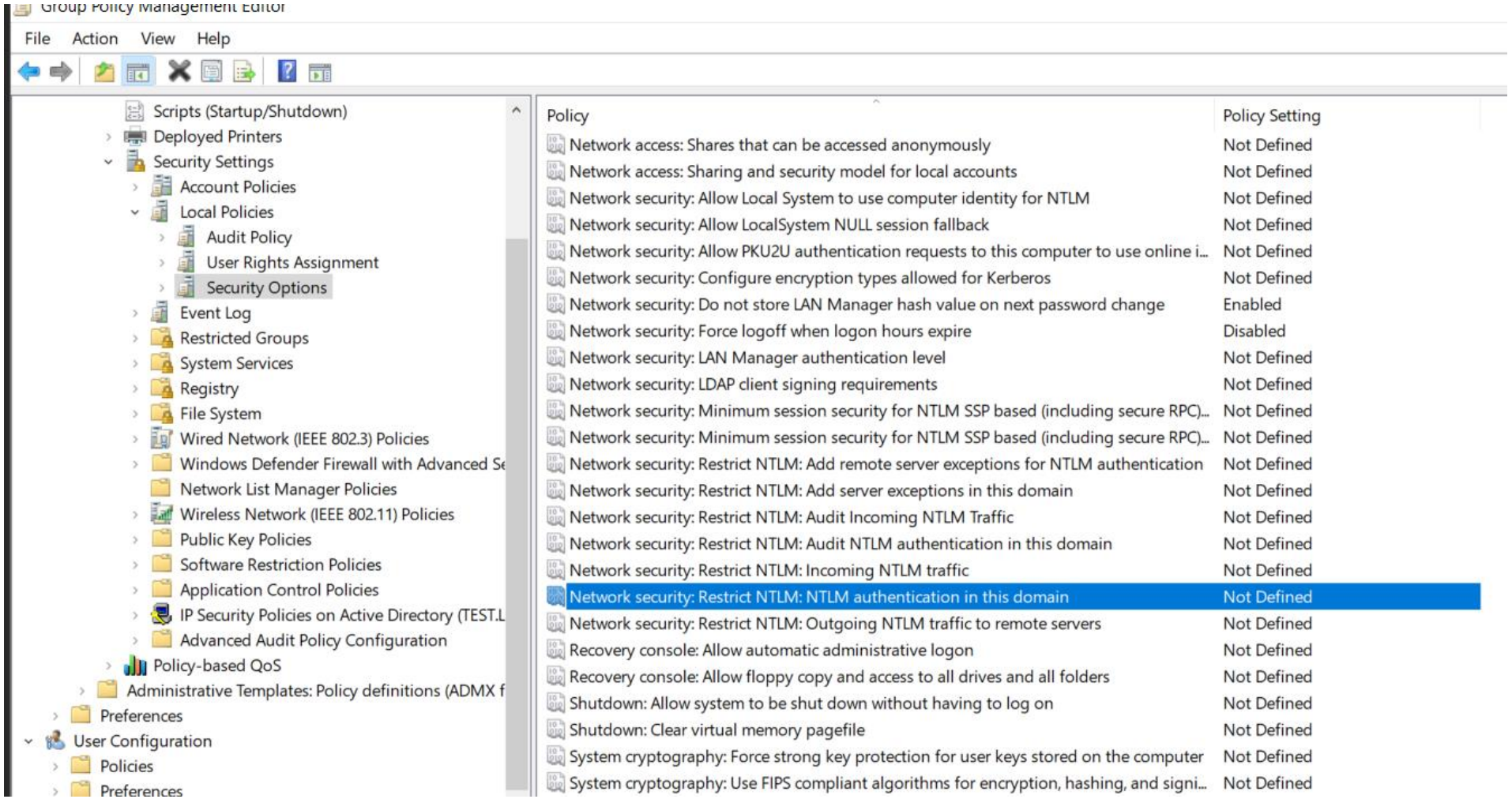
- **چرا NTLM خطرناک محسوب می‌شود؟**
- **۱. امکان انجام حمله NTLM Relay**
- در این حمله، مهاجم احراز هویت NTLM کاربر را می‌گیرد و بدون دانستن رمز عبور آن را به یک سرویس دیگر **Relay** می‌کند.
- مثال:
- کاربر به یک سرور جعلی وصل می‌شود
- مهاجم NTLM authentication را دریافت می‌کند
- همان authentication را به **LDAP یا SMB در Domain Controller** ارسال می‌کند
- و می‌تواند دسترسی مدیریتی بگیرد
- این یکی از **رایج‌ترین حملات در Pentest های Active Directory** است.

- **آسیب‌پذیری در برابر Pass-the-Hash**
- در NTLM، هش رمز عبور در حافظه یا شبکه استفاده می‌شود. اگر مهاجم هش را به دست آورد، می‌تواند بدون دانستن رمز عبور واقعی وارد سیستم شود.
- به این حمله می‌گویند:
- **Pass the Hash (PtH)**

- **جلوگیری از حرکت جانبی مهاجم (Lateral Movement)**
- در بسیاری از حملات AD، مهاجم بعد از نفوذ اولیه با استفاده از NTLM در شبکه حرکت می‌کند و به سیستم‌های دیگر دسترسی می‌گیرد.
- غیرفعال کردن NTLM این مسیر را محدود می‌کند.

- **چرا Kerberos بهتر است؟**
- Kerberos از مکانیزم **Ticket-based authentication** استفاده می‌کند:
- رمز عبور در شبکه ارسال نمی‌شود
- احراز هویت دوطرفه (Mutual Authentication) دارد
- در برابر Relay attack مقاوم‌تر است
- امنیت بالاتری دارد

- Computer Configuration
- Windows Settings
- Security Settings
- Local Policies
- Security Options



Group Policy Management Editor

ile Action View Help

- 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) Pol
  - Windows Defender Firewall wi
  - Network List Manager Policies
  - Wireless Network (IEEE 802.11)
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Active D
  - Advanced Audit Policy Config
- Policy-based QoS
- Administrative Templates: Policy defin
- Preferences
- User Configuration
  - Policies
  - Preferences

Network security: Restrict NTLM: NTLM authentication in t... ? ×

Security Policy Setting | Explain

Network security: Restrict NTLM: NTLM authentication in this domain

☑ Define this policy setting

Deny all

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: Restrict NTLM: NTLM authentication in this domain in the Security Policy Technical Reference.

OK | Cancel | Apply

	Policy Setting
ly	Not Defined
ounts	Not Defined
entity for NTLM	Not Defined
k	Not Defined
o this computer to use online i...	Not Defined
Kerberos	Not Defined
on next password change	Enabled
	Disabled
	Not Defined
	Not Defined
P based (including secure RPC)...	Not Defined
P based (including secure RPC)...	Not Defined
tions for NTLM authentication	Not Defined
this domain	Not Defined
raffic	Not Defined
ion in this domain	Not Defined
	Not Defined
this domain	Not Defined
o remote servers	Not Defined
	Not Defined
ves and all folders	Not Defined
to log on	Not Defined
	Not Defined
er keys stored on the computer	Not Defined
encryption, hashing, and signi...	Not Defined
ws subsystems	Not Defined

Metasploit

- تکنیک‌های brute-force مانند Kerberos Username Bruteforce به‌ویژه در محیط‌هایی که دارای تنظیمات امنیتی ضعیف یا پیکربندی‌های اشتباه هستند بسیار خطرناک‌اند و به مهاجمان امکان می‌دهند به‌صورت سیستماتیک نام‌های کاربری معتبر را شناسایی کرده و به دسترسی غیرمجاز دست یابند.

- ماژول **auxiliary/scanner/kerberos/kerberos_login** در Metasploit می‌تواند اعتبارنامه‌های Kerberosرا در برابر طیفی از ماشین‌ها بررسی کرده و لاگین‌های موفق را گزارش دهد.
- این ماژول قادر است اطلاعات زیر را از KDCشناسایی کند:
  - حساب‌های معتبر / نامعتبر
  - حساب‌های قفل‌شده یا غیرفعال
  - حساب‌هایی با رمز عبور منقضی‌شده (در صورتی که رمز عبور مطابقت داشته باشد)
-

- use auxiliary/scanner/kerberos/kerberos_login
- set rhosts 192.168.1.48
- set domain ignite.local
- set user_file users.txt
- Run

- گزینه USER_FILE برای مشخص کردن فایلی استفاده می‌شود که شامل لیستی از نام‌های کاربری است؛ این فایل به ماژول امکان می‌دهد تا با کوئری زدن به Domain Controller تشخیص دهد که آیا این نام‌ها در دامنه هدف وجود دارند یا خیر.

- **تشخیص و مقابله با تهدیدات Kerberos**
- روش‌های تشخیص:

- مانیتورینگ Event Logها
- با پایش مستمر رویدادهای زیر در سیستم‌های مبتنی بر Active Directory می‌توان فعالیت‌های مشکوک مرتبط با سوءاستفاده از Kerberosرا شناسایی کرد:

- Event ID **4768** – درخواست‌های Ticket Granting Ticket (TGT)
- Event ID **4769** – درخواست‌های Ticket Granting Service (TGS)
- Event ID **4771** – تلاش‌های ناموفق برای ورود از طریق Kerberos

نحوه امن کردن اکانت ادمین Local در ویندوز

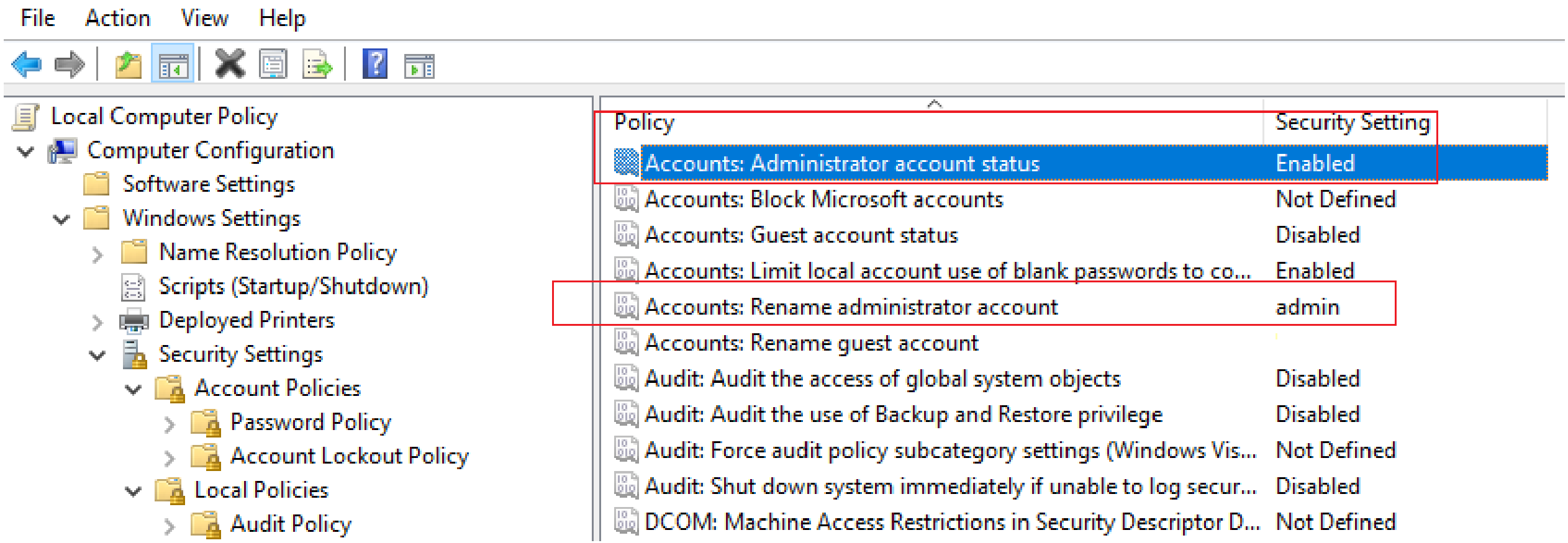
- غیر فعال کردن و تغییر نام اکانت ادمین
- برای حفاظت از اکانت ادمین در برابر حملات brute-forceتوصیه میکنیم آن را غیر فعال کنید یا حداقل نام آن را تغییر دهید.

- ساده ترین روش برای تغییر نام اکانت ادمین استفاده از Group Policyاست. Group Policyمحلی (gpedit.msc)یا تحت دامنه (gpmc.msc)باز کنید و و ارد مسیر زیر شوید:

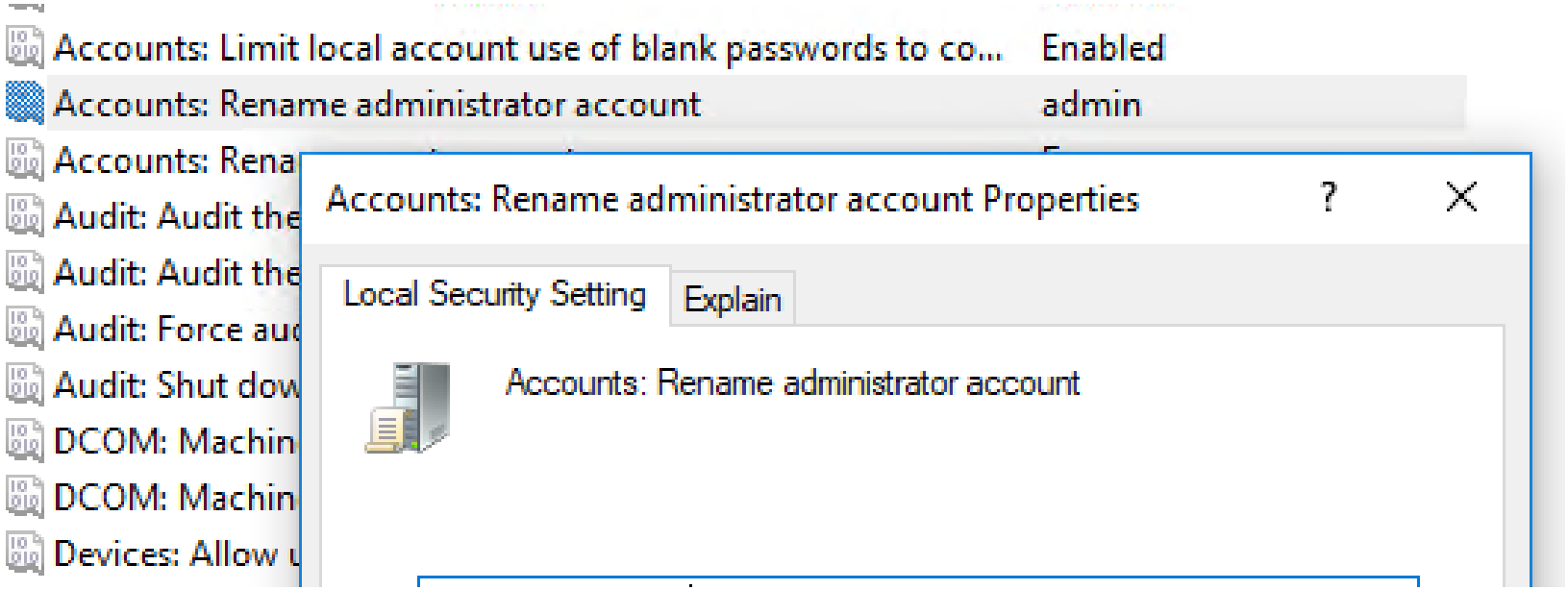
- Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options.

- به دو پالیسی زیر دقت کنید:

- **Accounts: Administrator account status**: به شما اجازه میدهد که اکانت ادمین را قفل کنید.
- **Accounts: Rename Administrator account** : این گزینه نیز به شما اجازه تغییر نام اکانت ادمین را میدهد.



- برای تغییر نام اکانت، پالیسی را فعال کنید و نام کاربری جدیدی به آن تخصیص دهید.



- تغییر نام اکانت، حمله brute forceرا به این اکانت سخت تر میکند، چون حمله کننده باید نام اکانت را بداند و سپس اقدام به اجرای حمله brute forceکند.

- تغییر نام اکانت امنیت را افزایش میدهد ولی این کار خیلی موثر نیست. اکانت ادمین یک مقدار معروف به نام Security Identifier (SID)دارد که راه های متفاوتی وجود دارد که میتوان از طریق SIDبه جای نام کاربری احراز هویت کرد.

- بنابراین روش بهتر برای حفاظت در برابر اکانت ادمین، غیر فعال کردن آن است. برای این کار پالیسی Accounts: Administrator account statusرا فعال کنید و مقدار آن را به Disabledتغییر دهید.

- **جلوگیری از ورود به سیستم بوسیله ورود ادمین محلی**
- محدود کردن دسترسی های ادمین محلی سخت است، بنابراین برای افزایش سطح حفاظت، میتوانید ورود اکانت ادمین محلی را چه به صورت محلی یا به صورت ریموت، غیر فعال کنید. برای این کار میتوانید از GPO استفاده کنید. وارد مسیر زیر شوید:

- Computer Configuration > Policies > Windows Settings -> Security Settings > Local Policies > User Rights Assignment

- **Deny Log on locally**: میتوانید با استفاده از این پالیسی ورود ادمین محلی را غیر فعال کنید.

- **Deny log on through Remote Desktop Service**: با این پالیسی میتوانید ورود از طریق Remote Desktop Service (RDP)را غیر فعال کنید.

- **Deny access to this computer from the network**: با استفاده از این پالیسی میتوانید اکانت های مشخصی را از دسترسی به این کامپیوتر منع کنید.

- **Deny log on as service**: با استفاده از این پالیسی میتوانید از رجیستر کردن سرویس به وسیله کاربر جلوگیری کنید.

- **Deny log on as a batch job:** به شما این امکان را میدهد که کاربر را برای رجیستر کردن به صورت یک جاب batchجلوگیری کند (به وسیله Task Schedulerو برخی سرویس های دیگر استفاده میشود).

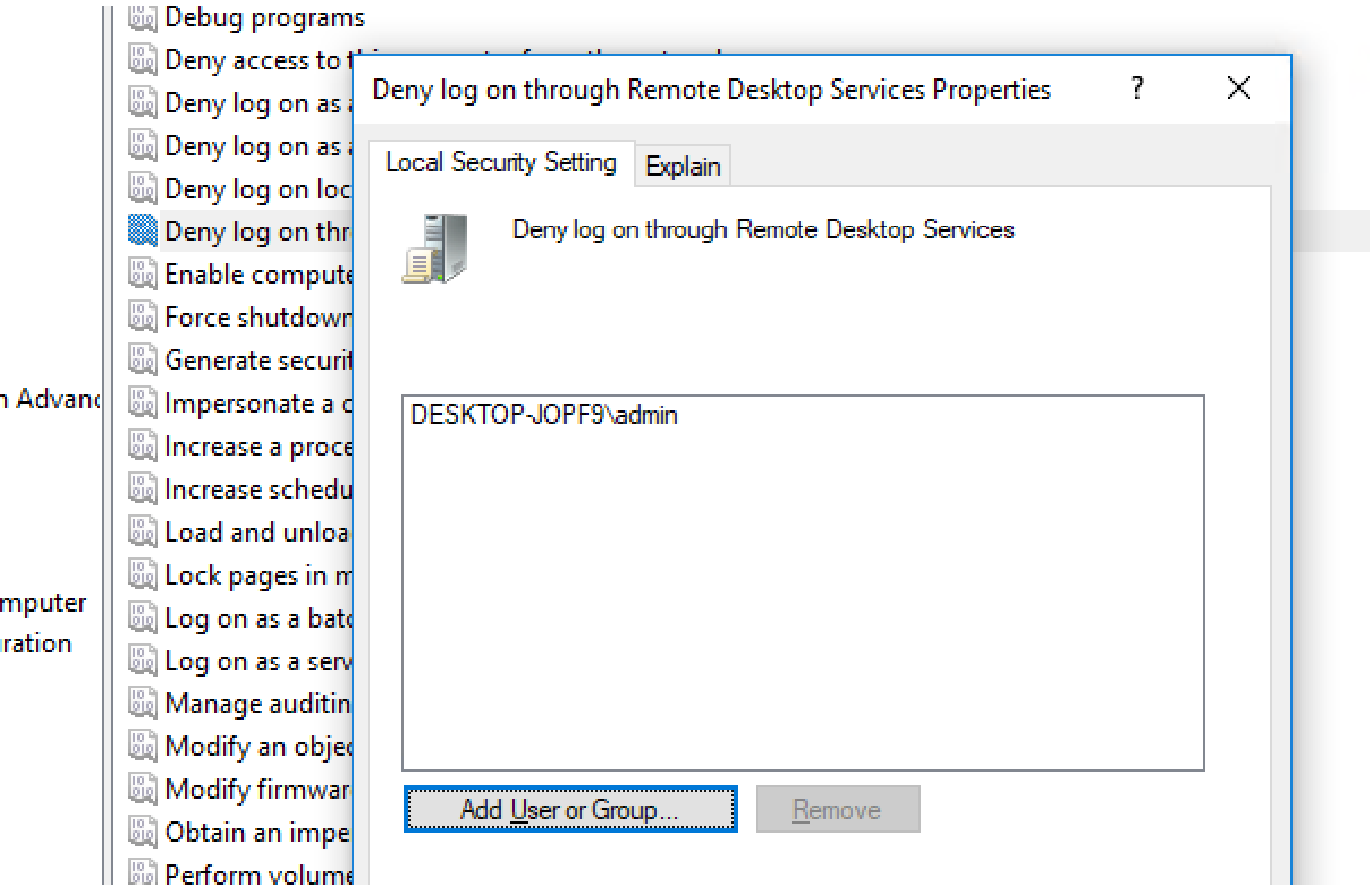
File Action View Help

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Policy
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Windows Defender Firewall with Advanc
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Computer
        - Advanced Audit Policy Configuration

Policy

- Create a token object
- Create global objects
- Create permanent shared objects
- Create symbolic links
- Debug programs
- Deny access to this computer from the network
- Deny log on as a batch job
- Deny log on as a service
- Deny log on locally
- Deny log on through Remote Desktop Services
- Enable computer and user accounts to be trusted for delegation
- Force shutdown from a remote system
- Generate security audits
- Impersonate a client after authentication
- Increase a process working set
- Increase scheduling priority
- Load and unload device drivers
- Lock pages in memory
- Log on as a batch job
- Log on as a service

- هر کدام از این پالیسی ها را میتوانید با زدن تیک Define this policy Settings و افزودن اکانت ادمین به پالیسی، فعال کنید.



- مایکروسافت توصیه میکند که همه روش های لاگین برای ادمین محلی را به جز ورود محلی غیر فعال کنید.

- در پایان به نکات زیر توجه کنید:

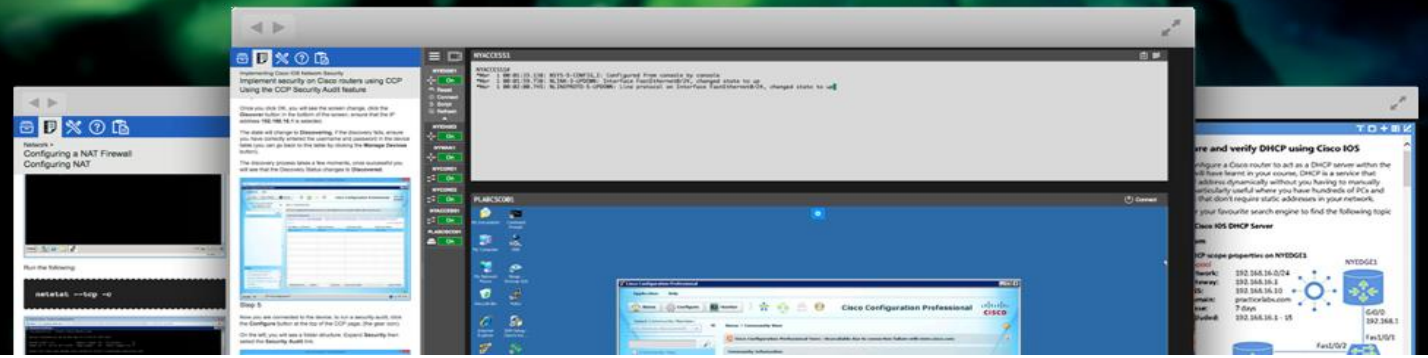
- اگر تصمیم به غیر فعال کردن اکانت ادمین داخلی ویندوز گرفتید، به خاطر داشته باشید که حداقل یک اکانت با دسترسی ادمین بسازید.

- توصیه نمیشود که این پالیسی ها را به domain controllerها اعمال کنید. حقیقت این است که اکانت محلی در DCها وجود ندارد و این پالیسی ها به اکانت ادمین DSRM اعمال میشوند. اگر این اکانت از دسترس خارج شود نمیتوانید برای Restore کردن اکتیو دایرکتوری، log in کنید.

VIRTUAL LAB

MICROSOFT BASELINE SECURITY ANALYZER

CYBRScore



- Microsoft Baseline Security Analyzer تحلیل‌گر امنیتی پایه مایکروسافت که مایکروسافت برای تعیین وضعیت امنیتی سیستم از طریق ارزیابی به روزرسانی های امنیتی نصب نشده و تنظیمات امنیتی کمتر امن (less-secure) در سیستم‌عامل ویندوز ارائه کرده‌است.
- این تنظیمات امنیتی شامل تنظیمات مولفه‌های ویندوز مانند اینترنت اکسپلورر، سرویس اطلاعاتی اینترنت (IIS) در وب سرورها، SQL سرور مایکروسافت و مایکروسافت آفیس می‌شود.

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer

Microsoft

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: WORKGROUP\MACBOOKXP (this computer)

IP address: . . .

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

- [x] Check for Windows administrative vulnerabilities
- [x] Check for weak passwords
- [x] Check for IIS administrative vulnerabilities
- [x] Check for SQL administrative vulnerabilities
- [x] Check for security updates
  - [ ] Configure computers for Microsoft Update and scanning prerequisites
  - [ ] Advanced Update Services options:
    - ( ) Scan using assigned Update Services servers only

Start Scan | Cancel

Microsoft Baseline Security Analyzer 2.2

Microsoft Baseline Security Analyzer

Microsoft

Report Details for WORKGROUP - USER-PC (2011-10-22 19:19:42)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name:	WORKGROUP\USER-PC
IP address:	192.168.0.164
Security report name:	WORKGROUP - USER-PC (22.10.2011 19-19)
Scan date:	22.10.2011 19:19
Scanned with MBSA version:	2.2.2130.0
Catalog synchronization date:	
Security update catalog:	Microsoft Update

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
	Developer Tools, Runtimes, and Redistributables Security Updates	2 security updates are missing. What was scanned Result details How to correct this
	Office Security Updates	8 security updates are missing. 3 service packs or update rollups are missing. What was scanned Result details How to correct this
	Windows Security Updates	5 security updates are missing. 1 service packs or update rollups are missing. What was scanned Result details How to correct this
	SDK Components Security Updates	No security updates are missing. What was scanned Result details
	SQL Server Security Updates	No security updates are missing. What was scanned Result details

Print this report Copy to clipboard Previous security report Next security report

OK

S
N
M
P
SIMPLE
NETWORK
MANAGEMENT
PROTOCOL

- SNMPیک پروتکل لایه برنامه برای نظارت و مدیریت دستگاه‌های شبکه در یک شبکه محلی (LAN)یا شبکه گسترده (WAN)است. هدف این پروتکل ارائه دستگاه‌های شبکه مانند روتر، سرورها و چاپگرها با یک زبان مشترک برای به اشتراک‌گذاری اطلاعات با یک سیستم مدیریت شبکه (NMS)است.

- بهره برداری از پروتکل نظارت بر شبکه (SNMP) ، که می تواند برای سرقت اطلاعات حساس شبکه و نفوذ به یک شبکه مورد سوء استفاده قرار گیرد.
- ثانیا، مهاجمان از نرم افزارها و سیستم عامل های قدیمی استفاده کرده اند تا کل سازمان ها را به خطر بیندازند

با بررسی های بیشتر، مشخص شد که تقریباً **٤٠٠٠٠** وجود دارددستگاه های متصل به اینترنت با پورت های SNMP، با سیسکو سیستم های پیشتاز نمودار و پس از آن **Mikrotik.** علاوه بر این، کشف شد که بیش از **١٠٠٠٠** دستگاه از این دستگاه‌ها نسخه **SNMP 1** را اجرا می‌کنند که خطر بالایی را به همراه دارد.

- برای بخش‌های فناوری اطلاعات که به دنبال استفاده از قدرت SNMPهستند، داشتن یک نرم‌افزار snmpضروری است. نرم‌افزار این پروتکل می‌کند می‌تواند اکتشاف خودکار را در شبکه اجرا کند و دستگاه‌ها را برای استخراج داده‌ها جست‌وجو کنند، که نظارت جامع را در همه دستگاه‌های شبکه را آسان‌تر می‌سازد.

- یکی از نرم‌افزارهای محبوب در این زمینه Intermapper از SNMP است که برای متغیرهای پایگاه اطلاعات مدیریت (MIB)از آن استفاده می‌شود.
- به‌عنوان یک انتخاب پیشرو در نرم‌افزار، **Intermapper** دارای صدها پروب شبکه داخلی است که طیف گسترده‌ای از داده‌ها را در مورد عملکرد شبکه ارائه می‌دهد و با آخرین نسخه پروتکل **SNMPv3**سازگاری دارد.

- همچنین کاربران توانایی ایجاد پروب‌های سفارشی خود را دارند. این دستگاه‌های SNMPرا قادر می‌سازد تا به‌روزرسانی‌های وضعیت دستگاه را به گونه‌ای ارائه کنند که کیفیت کلی نظارت و مدیریت شبکه را افزایش دهد.

نسخه های مختلف پروتکل SNMP

- **SNMPv1** –اولین نسخه SNMPاست که در دهه ۱۹۸۰ ایجاد شد و از ویژگی‌های امنیتی ضعیفی برخوردار است. سرورهایی که تحت SNMPv1 هستند، مدیران می‌توانند بدون رمزگذاری و احراز هویت درخواست اطلاعات از نماینده داشته باشند.
- این بدان معنا است که هر کسی که به شبکه دسترسی دارد می‌تواند نرم‌افزار sniffing را برای رهگیری اطلاعات مربوط به شبکه اجرا کند. همچنین از این طریق یک دستگاه غیرمجاز می‌تواند به‌راحتی وانمود کند که یک مدیر قانونی در هنگام کنترل شبکه است.
- این در حالی است که SNMPv1از اعتبارنامه‌های پیش‌فرض خاصی استفاده می‌کند که ادمین‌ها همیشه آن‌ها را به‌روزرسانی نمی‌کنند در نتیجه دسترسی افراد غیرمجاز به اطلاعات حساس در مورد شبکه را آسان می‌سازد. با این‌حال به‌دلیل سازگاری گسترده و عملکرد بسیار آسان SNMPv1در حد زیادی سرورها از این ورژن استفاده می‌کنند.
- **و فقط از UDP استفاده می کند.**

- **SNMPv2** – این ورژن نسخه‌ی ارتقاء یافته SNMPv1است که در سال ۱۹۹۳ با پیشرفت‌های امنیتی ارائه شد.
- اگرچه این ورژن عملکرد و امنیت را تا حد زیادی بهبود بخشید اما باز هم از رمزگذاری استفاده نمی‌کند.
- از UDPاستفاده می کند اما می تواند برای استفاده از TCPپیکربندی شود.

- **SNMPv3**: – در حالی‌که مسائل امنیتی در SNMPv1باعث شد SNMPدر برخی محافل به‌عنوان ابزار بدی نام برده شود اما SNMPv2و به‌ویژه SNMPv3این مشکلات را حل کردند. نسخه‌ی جدیدتر SNMPبا نام SNMPv3در سال ۱۹۹۸ ارائه شد که روش‌های به‌روز و ایمنی را برای نظارت بر شبکه ارائه می‌دهد.

- **SNMPv3** رمزگذاری داده‌ها را امکان‌پذیر می‌سازد. همچنین به ادمین‌ها اجازه می‌دهد تا الزامات مختلف احراز هویت را به‌صورت جزئی برای مدیران و نمایندگان تعیین کنند.

- **SNMP v3** امنیتی را فراهم می‌کند که محرمانگی و صحت دسترسی به داده‌های شبکه را تضمین می‌کند. SNMP version 3 از مکانیزم‌های تأیید هویت و رمزگذاری برای جلوگیری از دسترسی‌های غیرمجاز به دستگاه‌های شبکه استفاده می‌کند. همچنین، از پروتکل برقراری امنیت در شبکه برای اطمینان از دخالت نکردن چیزی با داده‌ها در طول انتقال، پشتیبانی می‌کند.

- **تأیید هویت**: برای احراز هویت از MAC مبتنی بر Hash با MD5 یا SHA و برای حفظ حریم خصوصی از DES-56 استفاده می کند. این نسخه از TCP استفاده می کند

- **رمزگذاری**: با **SNMP version 3** ، برای جلوگیری از دسترسی غیرمجاز در طول انتقال داده، از رمزگذاری استفاده می‌شود و اطلاعات حساس را از حملات کنندگان پتانسیل محافظت می‌کند.

- **کنترل دسترسی**: **SNMPv3** کنترل دسترسی دقیق را فراهم می‌کند و به مدیر شبکه اجازه می‌دهد سطوح دسترسی مختلف را برای کاربران یا گروه‌های کاربری مختلف تعریف کند و مطمئن شوند که وظایف به درستی جدا شده باشند.

چگونه سرورهای ویندوزی را با پروتکل SNMP V3 مانیتور کنیم ؟

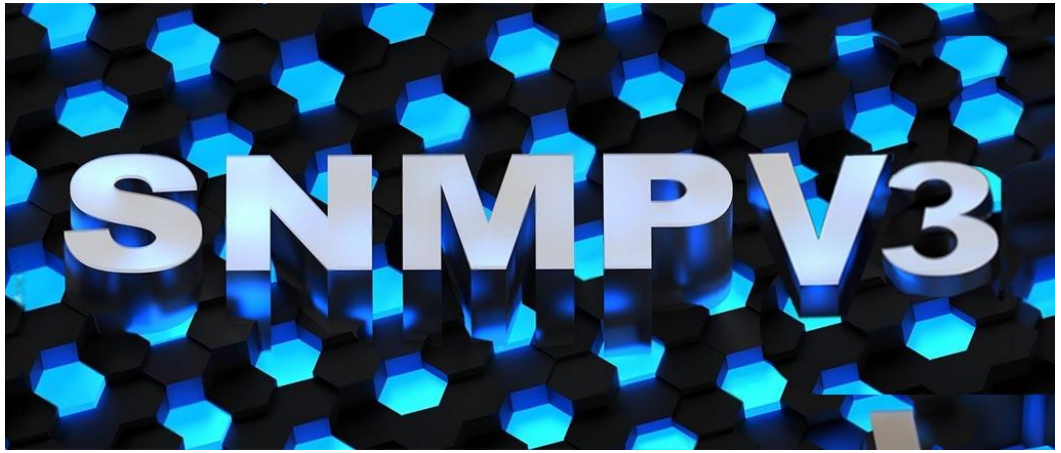
- **سیستم عامل های ویندوز از نسخه شماره ۳ پروتکل SNMPپشتیبانی نمیکنند**، و مایکروسافت نیز اعلام کرده که قرار نیست در آینده این پشتیبانی به سیستم عامل هایش اضافه شود.
- سیستم عامل های ویندوز به صورت پیش فرض از **SNMPv2** پشتیبانی میکنند ولی اگر حتما لازم باشد از **SNMPv3** استفاده کنید، لازم است ابزار های دیگری برای این منظور روی ویندوز نصب شود.

- از سه نرم افزار زیر میتوانید برای افزودن پشتیبانی از **SNMPV3** روی سیستم عامل های ویندوز استفاده کنید:

- **MG-SOFT** – لایسنس تجاری
- **SNMP-Informant** – لایسنس تجاری
- **Net-SNMP** – لایسنس غیر تجاری

- همچنین، قابلیت هندلینگ خطا و گزارش دهی بهتر را فراهم می‌کند که به مدیران اجازه می‌دهد به سرعت مشکلات را شناسایی و حل کنند.

- **SNMPv3** برای کارآیی بیشتر از نسخه‌های قبلی طراحی شده است و هزینه مدیریت دستگاه‌های شبکه را کاهش می‌دهد.
- این پروتکل از پهنای باند و منابع CPU کمتری استفاده می‌کند که مناسب برای استفاده در شبکه‌های بزرگ و پیچیده است. این باعث بهبود عملکرد و کاهش لطفا شبکه می‌شود.



root@kali: /usr/share/nmap

File Edit View Search Terminal Help

```
root@kali:/usr/share/nmap# nmap -sU -p 161 192.168.102.220
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-27 10:02 EDT
Nmap scan report for 192.168.102.220
Host is up (0.014s latency).

PORT    STATE SERVICE
161/udp open  snmp
MAC Address: C2:01:11:71:00:00 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
root@kali:/usr/share/nmap#
```

```
root@kali:/usr/share/nmap# nmap -sV -sU -p 161 192.168.102.220
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-27 10:03 EDT
Nmap scan report for 192.168.102.220
Host is up (0.016s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; ciscoSystems SNMPv3 server (public
)
MAC Address: C2:01:11:71:00:00 (Unknown)
Service Info: Host: R1

Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
```

```
┌──(root㉿kali)-[/home/hesam]
└─# cd /

┌──(root㉿kali)-[/]
└─# /usr/share/nmap/scripts

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# ls | grep snmp
snmp-brute.nse
snmp-hh3c-logins.nse
snmp-info.nse
snmp-interfaces.nse
snmp-ios-config.nse
snmp-netstat.nse
snmp-processes.nse
snmp-sysdescr.nse
snmp-win32-services.nse
snmp-win32-shares.nse
snmp-win32-software.nse
snmp-win32-users.nse

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─#
```

در این فولدر Script های NMAP قابل مشاهد هست برای پروتکل SNMP از اسکریپت Brute.nse برای پیدا کردن Community استفاده می گردد .

```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -sU -p 161 --script snmp-brute.nse 192.168.100.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-06 04:41 EDT
Nmap scan report for 192.168.100.100
Host is up (0.00041s latency).

PORT     STATE         SERVICE
161/udp open|filtered snmp
MAC Address: 00:0C:29:5A:CC:49 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─#
```

```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -sU -p 161 --script snmp-interfaces.nse 192.168.100.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-06 04:47 EDT
Nmap scan report for 192.168.100.1
Host is up (0.0084s latency).

PORT     STATE  SERVICE
161/udp closed snmp
MAC Address: 74:D2:1D:87:50:F1 (Huawei Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─#
```

```
PORT     STATE SERVICE
161/udp open  snmp
| snmp-interfaces:
|   FastEthernet0/0
|     IP address: 192.168.102.220  Netmask: 255.255.255.0
|     MAC address: c2:01:11:71:00:00 (Unknown)
|     Type: ethernetCsmacd  Speed: 10 Mbps
|     Status: up
|     Traffic stats: 22.90 Kb sent, 26.12 Kb received
|   FastEthernet0/1
|     MAC address: c2:01:11:71:00:01 (Unknown)
|     Type: ethernetCsmacd  Speed: 10 Mbps
|     Status: down
|     Traffic stats: 0.00 Kb sent, 0.00 Kb received
|   Null0
|     Type: other  Speed: 4 Gbps
|     Status: up
```

```
root@kali:/usr/share/nmap/scripts# nmap -sU -p 161 --script snmp-brute.
nse 192.168.102.220
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-27 10:12 EDT
Nmap scan report for 192.168.102.220
Host is up (0.0055s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-brute:
|_  public - Valid credentials
MAC Address: C2:01:11:71:00:00 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.83 seconds
```

DNS TUNNELLING ATTACK

- به خاطر سپردن همه آیپی ها کار سخت و نشدنی است، به همین دلیل از سرویسی استفاده میکنیم تا نام دامنه را که برای انسان قابل فهم است را به IP مقصد مورد نظر تبدیل کند

- برای مثال به خاطر سپردن IP سرور گوگل (۱۷۲.۲۱۷.۱۷.۱۱۰) ممکن است برای انسان کار دشواری باشد، اما اگر یک نام دامنه برای مثال (Google.com)از آن سرویس وجود داشته باشد به راحتی میتوان به آن دسترسی داشت.

- درواقع DNS Server مانند دفترچه تلفن اینترنت کار میکند، در دفترچه تلفن شما نام یک نفر را جست و جو میکنید و در آن به شماره آن فرد میرسید و در دنیای اینترنت هم شما به دنبالIP یک نام دامنه میگردید و نام دامنه را از DNS Server درخواست میکنید و پاسخ را دریافت میکنید.

- DNS Tunnelling
  - تونل DNS یک حمله‌ی پیچیده است. که برای دسترسی دائمی مهاجمان به یک هدف مشخص طراحی می‌شود.
  - از آنجایی که بسیاری از سازمان‌ها نمی‌توانند بر ترافیک DNS نظارت کنند، مهاجمان می‌توانند بدافزار را در کوئری‌های DNS وارد یا تونل کنند.
  - این بدافزار برای ایجاد یک کانال ارتباطی پایدار استفاده می‌شود. و اکثر فایروال‌ها قادر به شناسایی آن نخواهند بود.

- قبل از اینکه هکرها از تونل‌سازی DNS برای سرقت اطلاعات از شبکه یک سازمان استفاده کنند، ابتدا نیاز به دسترسی به شبکه سازمان دارند که این امر اغلب با فیشینگ یا شکل دیگری از بدافزارها حاصل می‌شود.

- ناگفته نماند که پروتکل DNS یا Domain Name System در کنار پروتکل‌هایی چون HTTP، SNMP، HTTPS، یکی از معروف‌ترین پروتکل‌های شبکه است و قسمت عمده‌ای از اتفاقاتی که دور از نگاه کاربر، در پسِ زمینه‌ی مرورگر و درون شبکه انجام می‌شود تبادل بسته‌های این پروتکل بین رایانه‌ی کاربر و سرورهای DNS یا سرورهای DNS Cache است.

- DNSبه خودی خود ایمن نیست

- DNSدر دهه ۱۹۸۰ طراحی شد که اینترنت بسیار کوچکتر بود و امنیت در طراحی آن از اهمیت اساسی برخوردار نبود.
- در نتیجه، وقتی یک recursive resolver کوئری را به یک سرور نا معتبر می فرستد، resolverراهی برای تأیید صحت پاسخ ندارد.
- resolver فقط می تواند بررسی کند، پاسخی از همان آدرس IP که resolver مدنظرش است باشد. اما اتکا به منبع پاسخ آدرس IP یک مکانیسم احراز هویت قوی نیست،
- زیرا آدرس IP منبع یک بسته پاسخ DNS می تواند به راحتی جعل شود.

روش‌های جلوگیری از حملات DNS

- از آنجایی که طیف گسترده‌ای از حملات DNS وجود دارد، برخی از آن‌ها از کنترل فرد یا سازمان خارج است. با این حال، هنوز راهکارهای زیادی وجود دارد که سازمان شما می‌تواند برای جلوگیری از حملات DNS انجام دهد:

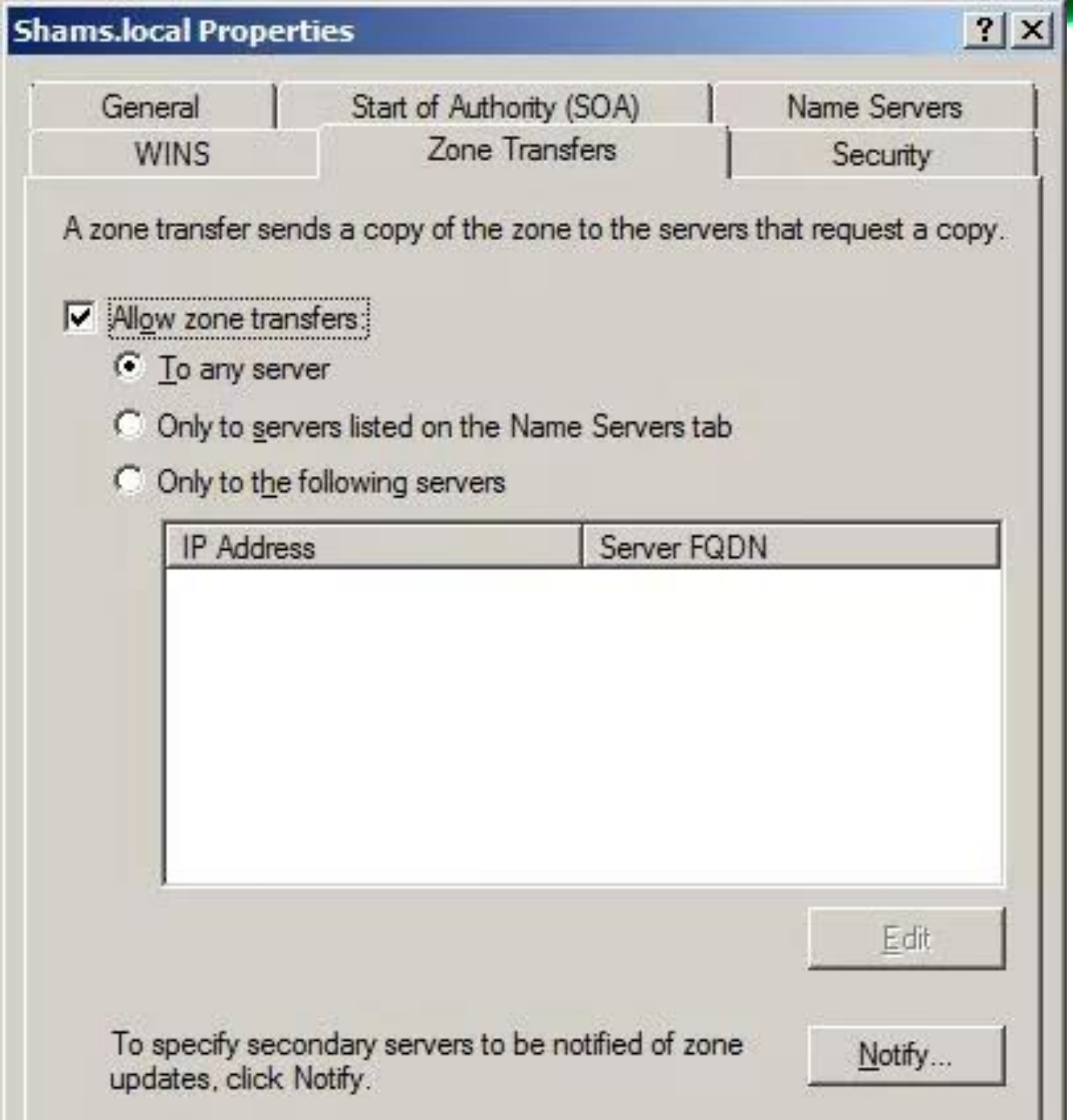
- **بازرسی** :DNS ممیزی و بازنگری DNS در کشف آسیب‌پذیری‌های مربوط به DNS به شما کمک می‌کند تا مشکلات مربوط به DNSهای قدیمی و نرم‌افزارهای منسوخ شده را شناسایی کنید و از دسترسی مهاجمان به سرور سازمان جلوگیری کنید.

DNS Manager

File Action View Help

- DNS
  - WIN-MTVCKBEAD08
    - Forward Lookup Zones
      - _msdcs.class.local
      - class.local
        - _msdcs
        - _sites
        - _tcp
        - _udp
        - DomainDnsZones
        - ForestDnsZones
    - Reverse Lookup Zones
    - Trust Points
    - Conditional Forwarders

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[29], v
(same as parent folder)	Name Server (NS)	win-r
(same as parent folder)	Host (A)	192.1
(same as parent folder)	IPv6 Host (AAAA)	2a01::
(same as parent folder)	IPv6 Host (AAAA)	2a01::
(same as parent folder)	IPv6 Host (AAAA)	fd74:c
win-mtvckbead08	Host (A)	192.1
win-mtvckbead08	IPv6 Host (AAAA)	fd74:c
win-mtvckbead08	IPv6 Host (AAAA)	2a01::
win-mtvckbead08	IPv6 Host (AAAA)	2a01::



محدود کردن منطقه انتقال: اگر محدوده انتقال DNSشما به دست یک مهاجم بیفتد، درک بهتری از ساختار شبکه شما را در اختیار او قرار خواهد داد.

با رفتن به فایل پیکربندی نرم افزار DNSخود و محدود کردن منطقه انتقال به آدرس‌های خاص IP، می‌توانید از حملات منطقه‌ای مهاجمان جلوگیری کنید.

برسی و پیاده سازی موارد امنیتی DNS Server

SERVER2 Properties

Debug Logging | Event Logging | Trust Anchors | Monitoring | Security
Interfaces | Forwarders | Advanced | Root Hints

Server version number:

6.1 7601 (0x1db1)

Server options:

- [ ] Disable recursion (also disables forwarders)
- [ ] BIND secondaries
- [ ] Fail on load if bad zone data
- [x] Enable round robin
- [x] Enable netmask ordering
- [x] Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

- [ ] Enable automatic scavenging of stale records

Scavenging period: 0 days

- در کنسول DNS روی نام آن کلیک راست و سپس Properties می گیریم

- Disable Recursion:
  - توانایی forwardکردن از DNSسرور گرفته می شود.

- Bind Secondaries:
  - برای برقراری ارتباط بین DNSسرور با یک DNS serverلینوکسی می باشد.

- Fail On load if bad zone data:
  - در صورتی که DNSسرور قادر به پاسخگویی نباشد، DNSسرور را failمی کند تا بررسی شود.

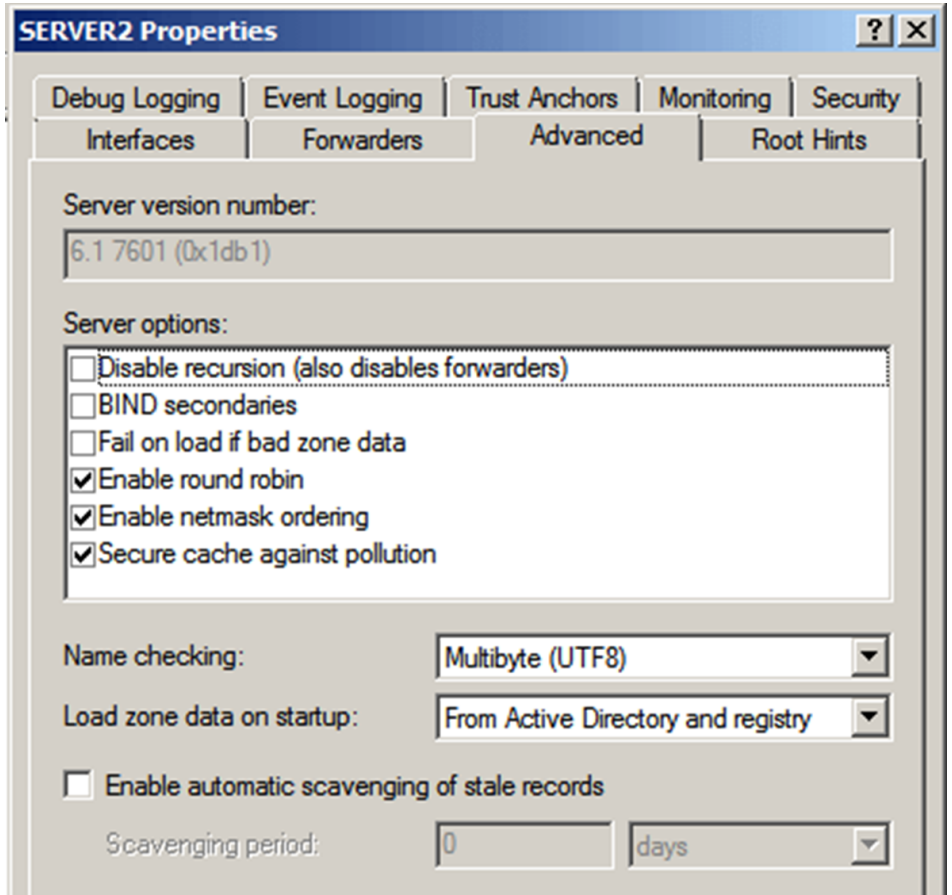
- Enable round robin:
  - اگر چند DNSسرور داشته باشیم برای برقراری تعادل بین آنها، موجب می شود که requestها بین DNSسرور ها تقسیم شود.

- Enable netmask ordering:

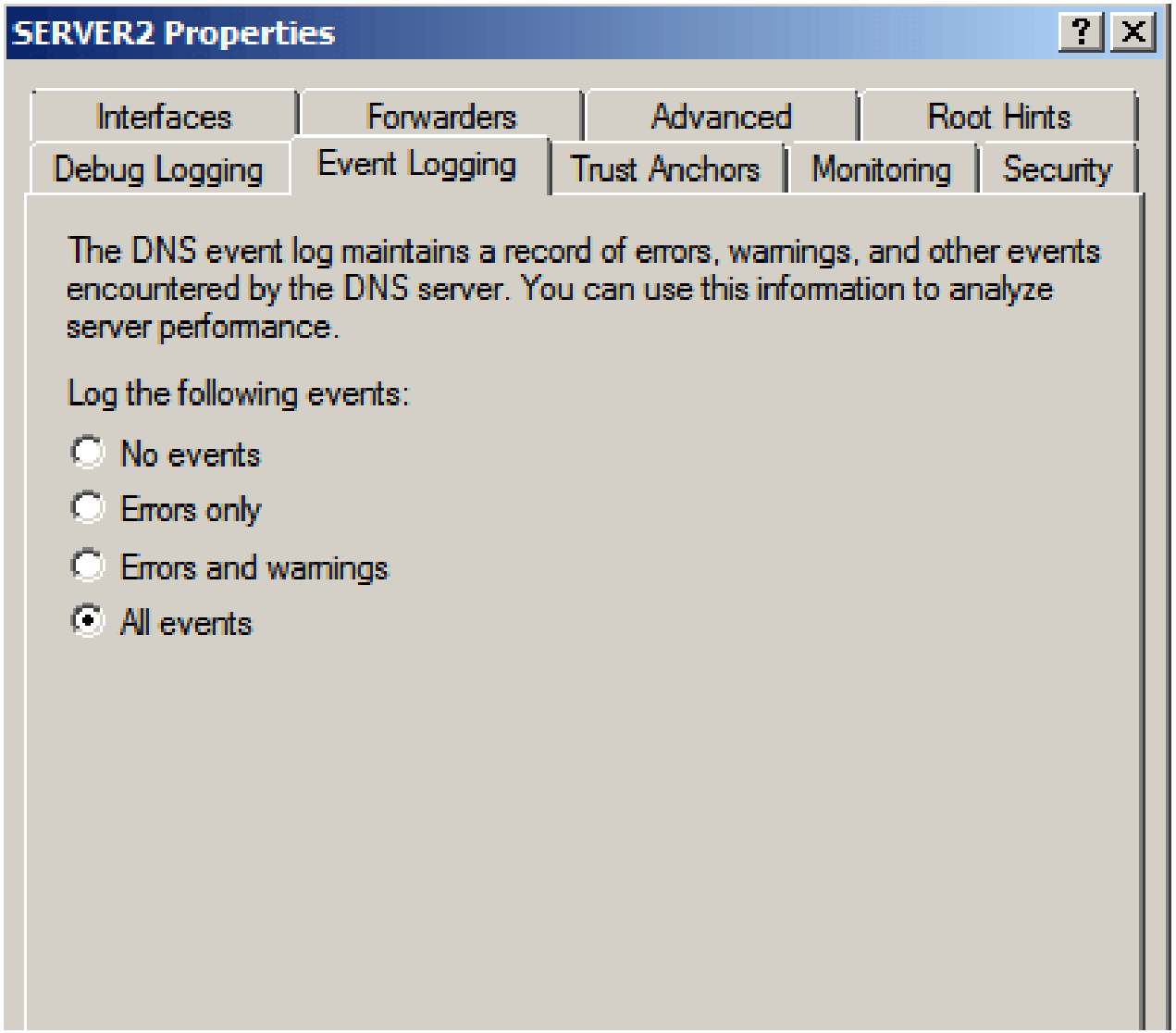
  - در صورت فعال بودن این گزینه، وقتی یک requestبه DNS serverمی رسد اولویت با پاسخگویی با DNS serverاست که در محدوده IPکاربر قرار دارد.

- Secure Cache against pollution:

  - در صورت ایجاد خرابی در recordها با آن مقابله خواهد کرد.

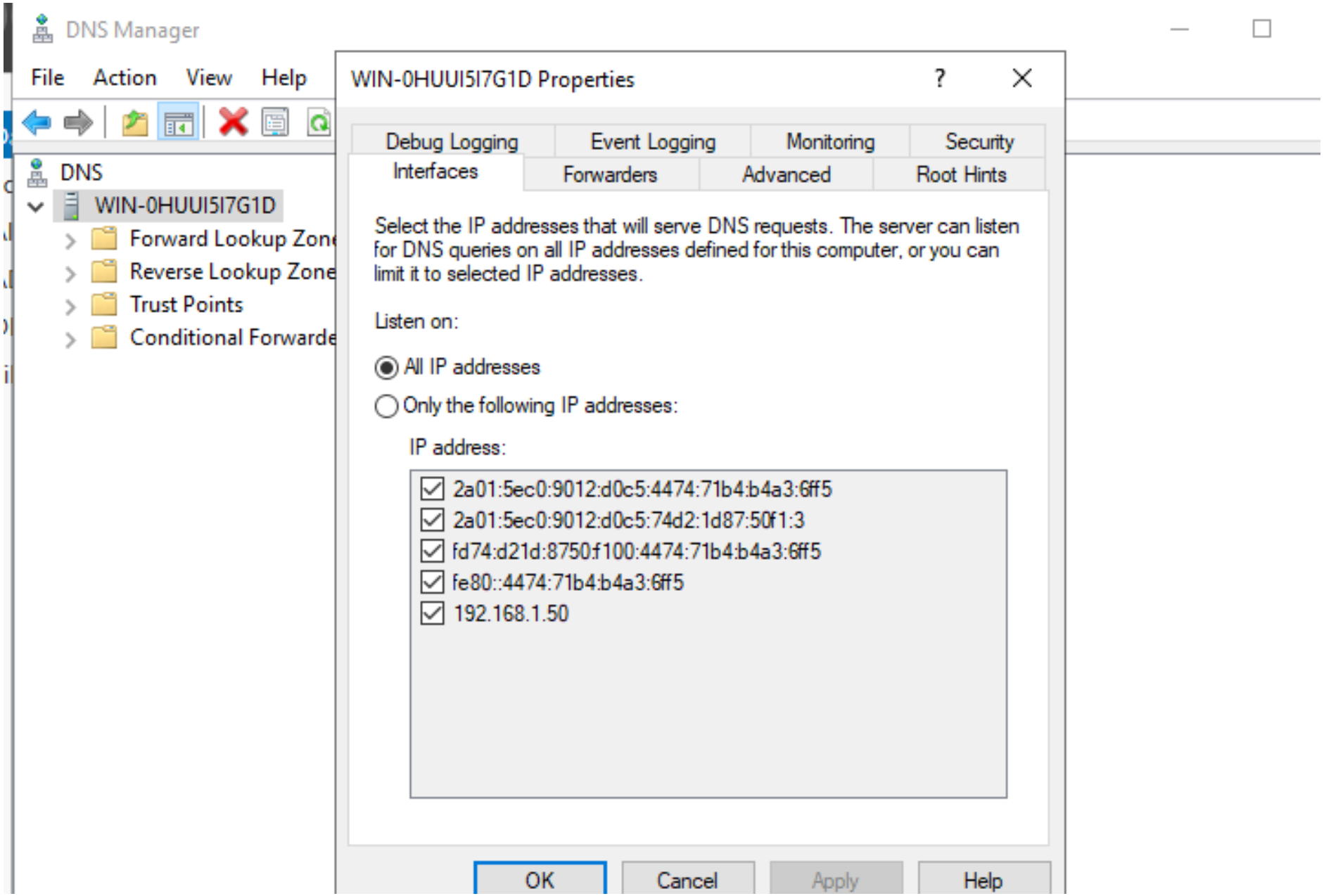


Event Logging:

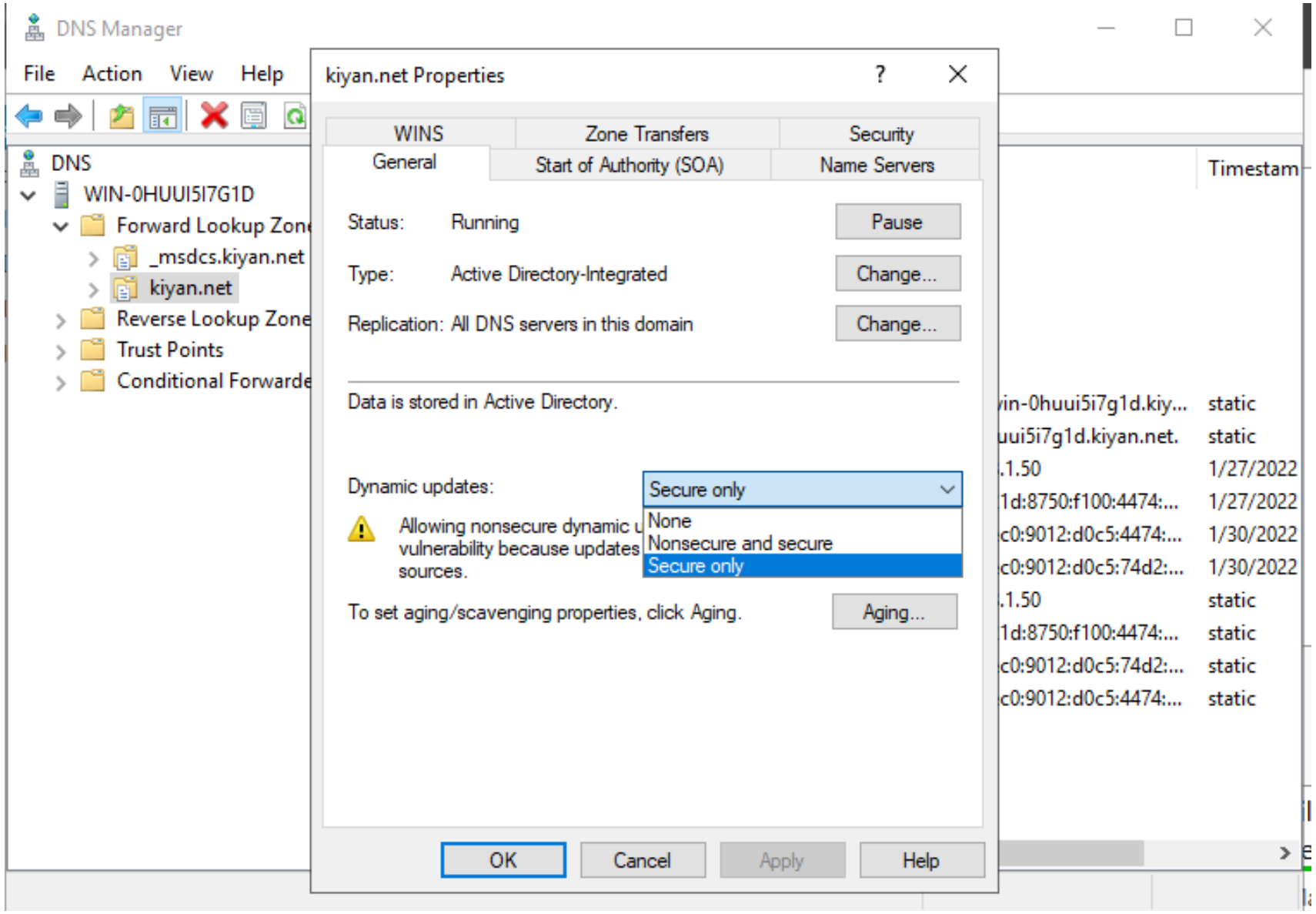


- مشخص می کنیم که چه eventهایی ثبت شوند.

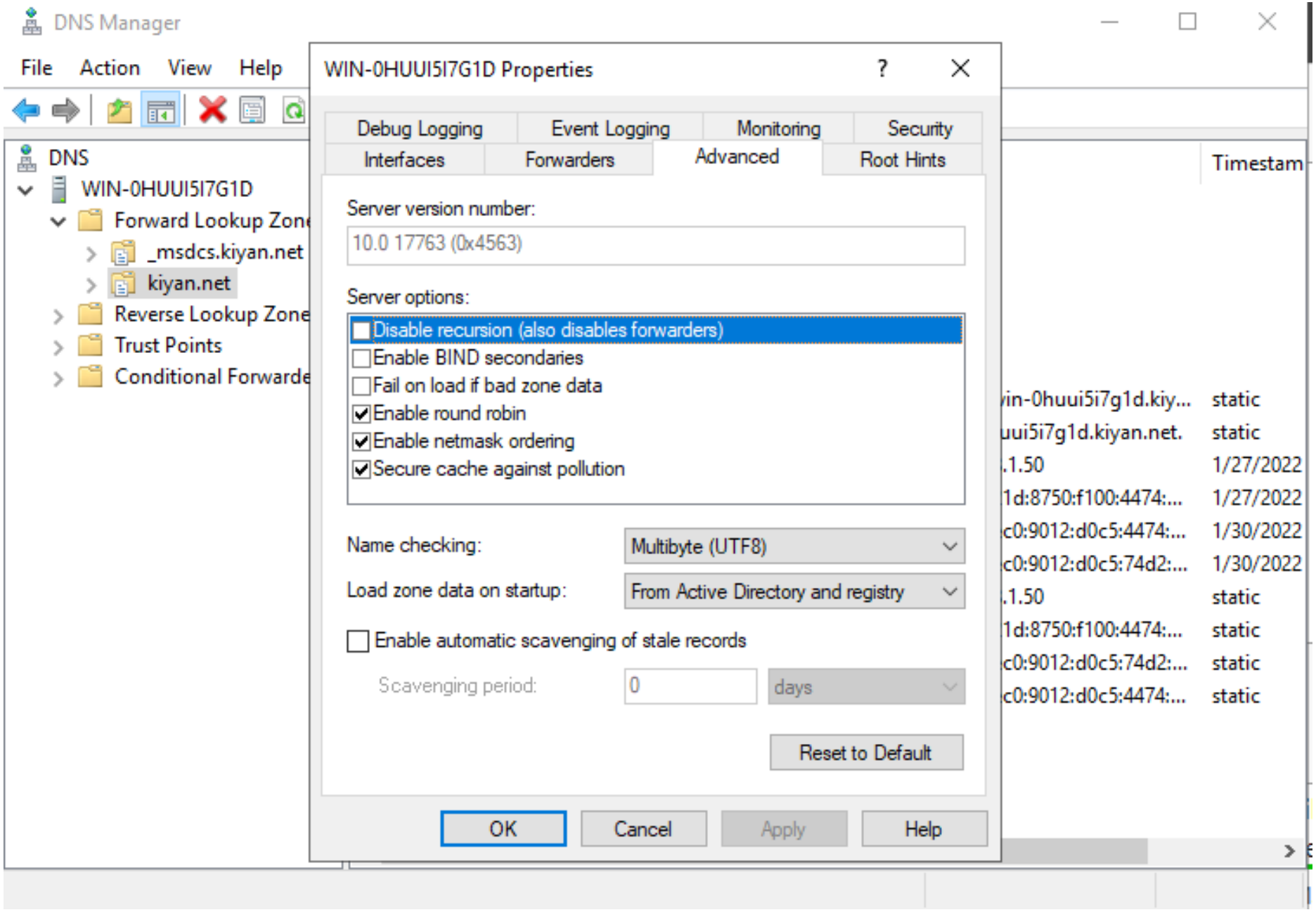
- با استفاده از روش زیر شنود سرویس دهنده DNS را محدود کرده



- دسترسی به سرویس DNS و حوزه و رکورهای منبع را کنترل و مدیریت کرده.
- با استفاده از تنظیمات زیر می توان حوزه ها را امن سازی کرد به این صورت که ابتدا بر روی حوزه راست کلیک کرده و سپس



- جستجوی بازگشتی را غیر فعال کرده.



- محدود سازی Zone Transfer
- برای افزایش امنیت باید تمام Zone Transferها تا زمانی که نیازی به آنها وجود ندارد غیرفعال شود. به طور پیش فرض Zone Transferبرای تمامی Zoneهایی که AD Integratedهستند غیرفعال می‌باشد. اما برای سایر Zone، تنظیمات پیش فرض برای Zone Transferتنها برای سرورهایی که در Name Server Resource Recordsلیست شده است، امکان پذیر خواهد بود.

- در صورتی که لازم است Zone Transferبین سرور هایی متمایز از لیست مذکور صورت گیرد، تنها باید برای IP Addressهای مشخص پیکربندی شود. فعال سازی Zone Transferبرای تمامی سرورها ممکن است منجر به فاش شدن داده‌های DNSبرای مهاجمینی که قصد شناسایی شبکه سازمانی را دارند، گردد.

DNS Manager

File Action View Help

DNS
WIN-0HUUI5I7G1D
Forward Lookup Zone
_msdcs.kiyan.net
kiyan.net
_msdcs
_sites
_tcp
_udp
DomainDnsZo
ForestDnsZon
Reverse Lookup Zone
Trust Points
Conditional Forwarde

Timestam

vin-0huui5i7g1d.kiy...	static
uui5i7g1d.kiyan.net.	static
.1.50	1/27/2022
1d:8750:f100:4474:...	1/27/2022
c0:9012:d0c5:4474:...	1/30/2022
c0:9012:d0c5:74d2:...	1/30/2022
.1.50	static
c0:9012:d0c5:74d2:...	static
c0:9012:d0c5:4474:...	static
1d:8750:f100:4474:...	static

kiyan.net Properties

General | Start of Authority (SOA) | Name Servers
WINS | Zone Transfers | Security

A zone transfer sends a copy of the zone to the servers that request a copy.

☐ Allow zone transfers:

- ◉ To any server
- ○ Only to servers listed on the Name Servers tab
- ○ Only to the following servers

IP Address	Server FQDN

Edit

To specify secondary servers to be notified of zone updates, click Notify.

Notify...

OK | Cancel | Apply | Help

- **امن سازی DNS Cache**
- به صورت پیش فرض DNS Serverدر مقابل (Cache Pollutionهنگامی که پاسخ‌های DNS Query شامل داده‌های Non Authoritativeو یا مخرب است) امن می‌باشد.
- ویژگی Secure Cache Against Pollutionاز آلوده کردن DNS Server Cacheتوسط مهاجم (با Resource Recordهایی که توسط DNS Serverدرخواست نشده‌اند)، جلوگیری می‌کند.
- تغییر در تنظیمات پیش فرض سبب می‌شود تا صحت پاسخ هایی که توسط سرویس DNS Serverفراهم می شود، کاهش یابد.

DNS Manager

File Action View Help

DNS
- WIN-0HUUI5I7G1D
  - Forward Lookup Zone
    - _msdcs.kiyan.net
    - kiyan.net
      - _msdcs
      - _sites
      - _tcp
      - _udp
      - DomainDnsZo
      - ForestDnsZon
  - Reverse Lookup Zone
  - Trust Points
  - Conditional Forwarde

Timestam

vin-0huui5i7g1d.kiy...	static
uui5i7g1d.kiyan.net.	static
.1.50	1/27/2022
1d:8750:f100:4474:...	1/27/2022
c0:9012:d0c5:4474:...	1/30/2022
c0:9012:d0c5:74d2:...	1/30/2022
.1.50	static
c0:9012:d0c5:74d2:...	static
c0:9012:d0c5:4474:...	static
1d:8750:f100:4474:...	static

WIN-0HUUI5I7G1D Properties

Debug Logging | Event Logging | Monitoring | Security
Interfaces | Forwarders | Advanced | Root Hints

Server version number:

10.0 17763 (0x4563)

Server options:

- [ ] Disable recursion (also disables forwarders)
- [ ] Enable BIND secondaries
- [ ] Fail on load if bad zone data
- [x] Enable round robin
- [x] Enable netmask ordering
- [x] Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

- [ ] Enable automatic scavenging of stale records

Scavenging period: 0 days

Reset to Default

OK | Cancel | Apply | Help