Виндоусын аюулгүй байдлыг лог үүсгэн хяналт тавих
Monitoring Windows Security & Log

Намнансүрэн Баасандорж

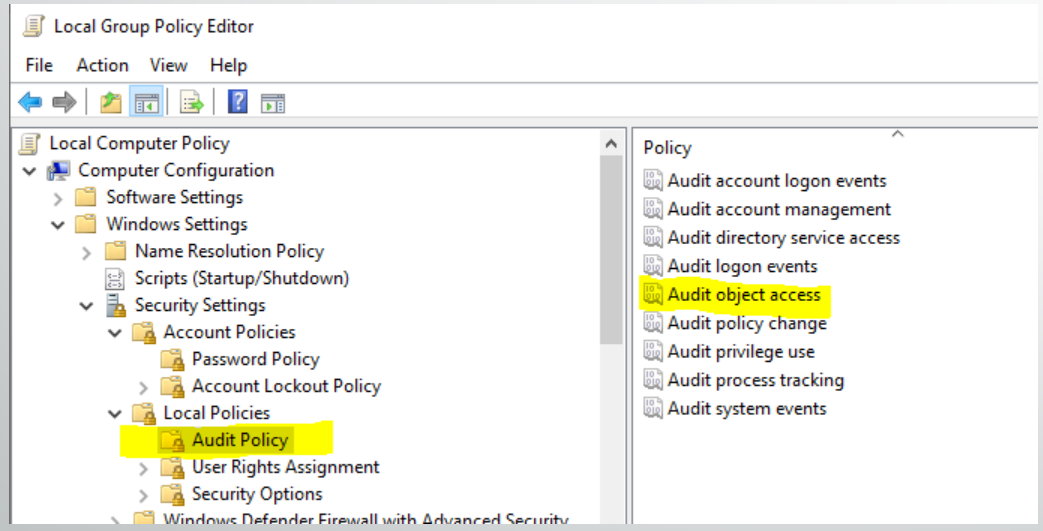
IBM

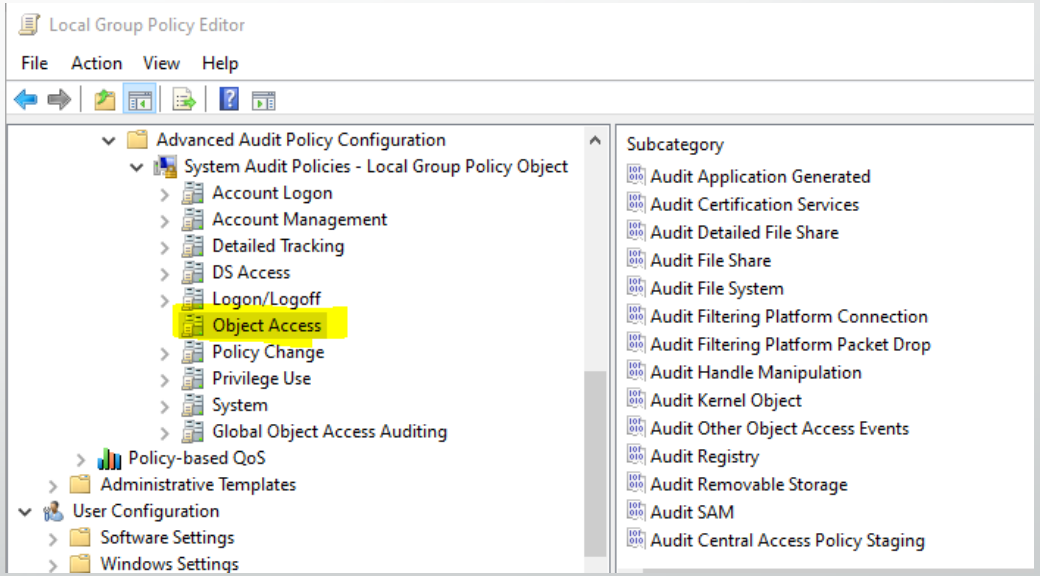
MNSEC 2020

Агуулга / Agenda

- Өргөтгөсөн аудит хяналтын тухай – Advanced Audit Policy
- Түгээмэл хэрэгцээт үйлдлийн бүртгэл - Some Useful Windows Security Events
- Windows Powershell бүртгэлийг тохируулах – Windows Powershell Log Monitoring
- Microsoft Sysinternals Sysmon програмын ашиглан лог авах – Use Sysmon for Monitoring

Уламжлалт аудит болон өргөтгөсөн аудит гол ялгаа





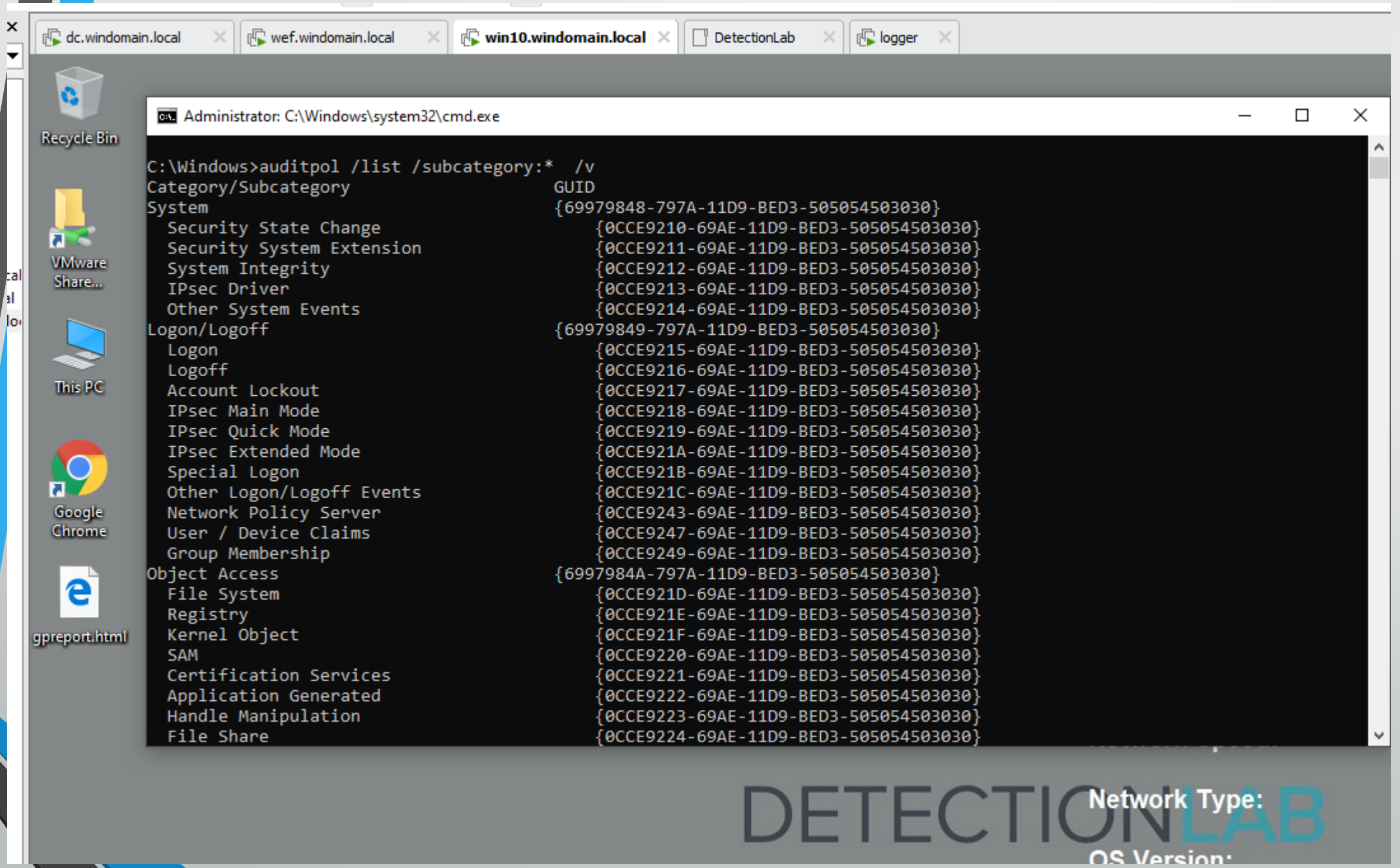
Өргөтгөсөн аудит хяналтын тохиргооны бүлгүүд

Тохиргоо	Дэд тохиргооны тоо
Account Logon	4
Account Management	6
Detailed Tracking	6
DS Access	4
Logon/Logoff	11
Object Access	14
Policy Change	6
Privilege Use	3
System	5

9 үндсэн болон 59 дэд тохиргоо байдаг

Advanced Audit Policy and Logs

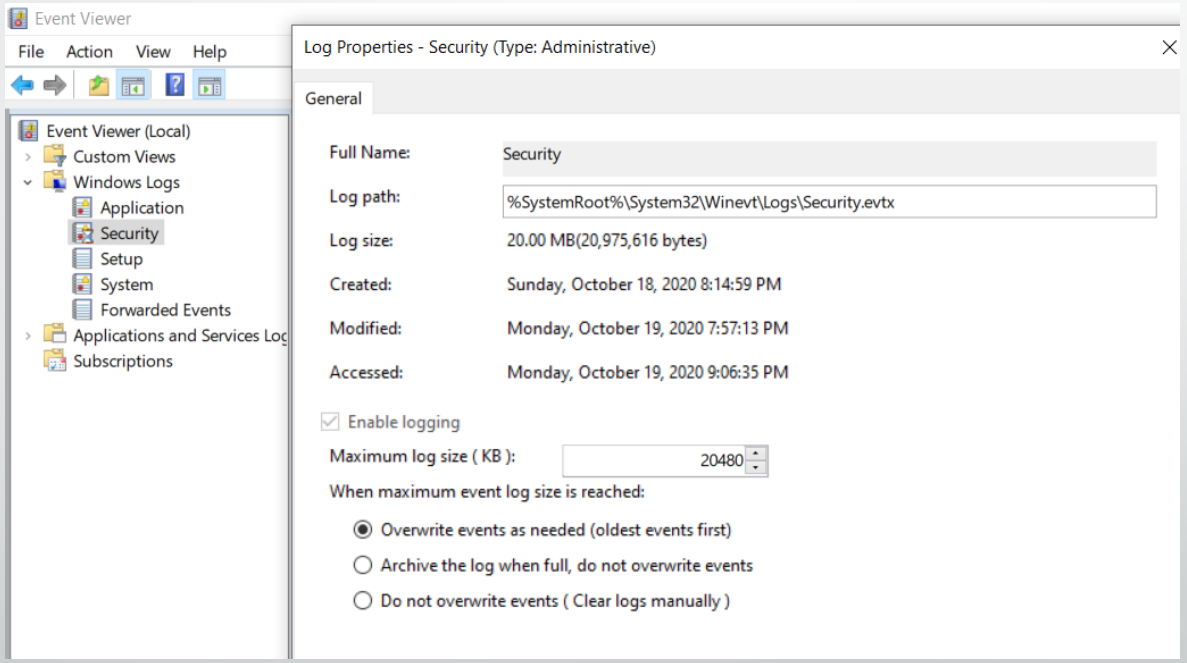
- Windows 7 , Windows 2008 R2 эхлэн бий болсон
- Auditpol коммандыг ашиглан локал компьютерийн тохиргоог унших өөрчлөх боломжтой, домэйн компьютер бол group policy ашиглана.
- Success – үйлдэл амжилттай, Failure – үйлдэл амжилтгүй
- No auditing – хийхгүй, Not configured – тохируулаагүй буюу өмнөх тохиргоог өөрчлөхгүй авна
- Gpedit.msc – Local Group Policy Editor
  Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\
- Тохиргоог өөрчилвөл энэ файл өөрчлөгдөнө.
  “%WINDIR%\system32\grouppolicy\machine\microsoft\windows nt\audit\audit.csv”


dc.windomain.local
wef.windomain.local
win10.windomain.local
DetectionLab
logger
Recycle Bin
VMware Share...
This PC
Google Chrome
gpreport.html
Administrator: C:\Windows\system32\cmd.exe
C:\Windows>auditpol /list /subcategory:* /v
Category/Subcategory GUID
System {69979848-797A-11D9-BED3-505054503030}
Security State Change {0CCE9210-69AE-11D9-BED3-505054503030}
Security System Extension {0CCE9211-69AE-11D9-BED3-505054503030}
System Integrity {0CCE9212-69AE-11D9-BED3-505054503030}
IPsec Driver {0CCE9213-69AE-11D9-BED3-505054503030}
Other System Events {0CCE9214-69AE-11D9-BED3-505054503030}
Logon/Logoff {69979849-797A-11D9-BED3-505054503030}
Logon {0CCE9215-69AE-11D9-BED3-505054503030}
Logoff {0CCE9216-69AE-11D9-BED3-505054503030}
Account Lockout {0CCE9217-69AE-11D9-BED3-505054503030}
IPsec Main Mode {0CCE9218-69AE-11D9-BED3-505054503030}
IPsec Quick Mode {0CCE9219-69AE-11D9-BED3-505054503030}
IPsec Extended Mode {0CCE921A-69AE-11D9-BED3-505054503030}
Special Logon {0CCE921B-69AE-11D9-BED3-505054503030}
Other Logon/Logoff Events {0CCE921C-69AE-11D9-BED3-505054503030}
Network Policy Server {0CCE9243-69AE-11D9-BED3-505054503030}
User / Device Claims {0CCE9247-69AE-11D9-BED3-505054503030}
Group Membership {0CCE9249-69AE-11D9-BED3-505054503030}
Object Access {6997984A-797A-11D9-BED3-505054503030}
File System {0CCE921D-69AE-11D9-BED3-505054503030}
Registry {0CCE921E-69AE-11D9-BED3-505054503030}
Kernel Object {0CCE921F-69AE-11D9-BED3-505054503030}
SAM {0CCE9220-69AE-11D9-BED3-505054503030}
Certification Services {0CCE9221-69AE-11D9-BED3-505054503030}
Application Generated {0CCE9222-69AE-11D9-BED3-505054503030}
Handle Manipulation {0CCE9223-69AE-11D9-BED3-505054503030}
File Share {0CCE9224-69AE-11D9-BED3-505054503030}
DETECTIONLAB
Network Type:
OS Version:

...

- auditpol /export /file:filename.ini,
- auditpol /import /file:filename.ini,
- auditpol /clear – бүх тохиргоог хүчингүй болгоно
- Disable: auditpol /set /option:CrashOnAuditFail /value:disable
- Enable: auditpol /set /option:CrashOnAuditFail /value:enable
- Security логын 4906 дугаартай лог утга өөрчлөгдвөл үүснэ

Лог хаана бичигдэх вэ ... eventvwr.msc



Security логын тохиргоо

- Windows Registry

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security\

  - File
  - MaxSize – Логын хамгийн их хадгалах хэмжээ
  - Retention
    - 0: Disabled - Лог дүүрвэл шинэ бичлэгээр хуучинг дарна
    - oxffffffff: Enabled – Дараах тохиргооноос хамаарч лог файлыг хэрхэн хадгалахыг шийднэ
  - AutoBackupLogFiles
    - 1 – Лог дүүрвэл хуучин лог файлыг нөөцлөн шинээр лог файл үүсгэнэ
    - 0 – Лог дүүрвэл шинэ бичлэг хадгалахгүй

...

- Group policy

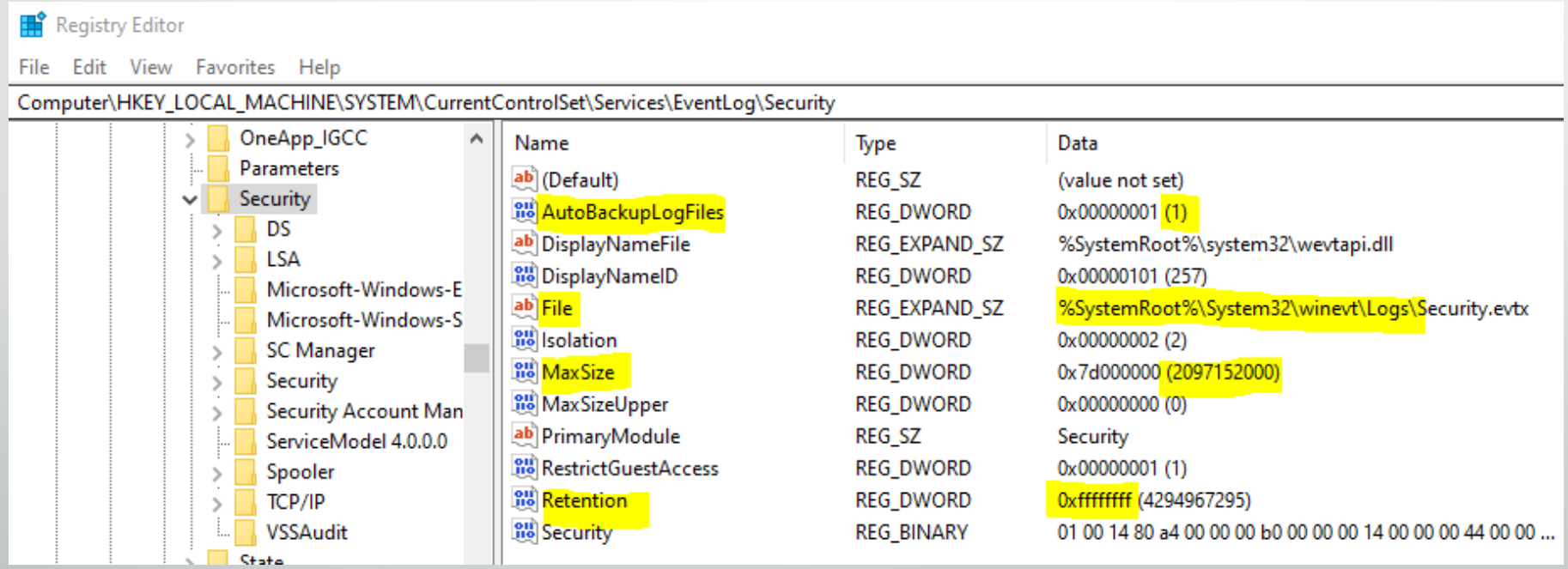
  Дараах хоёр байршилд лог файлын хэмжээг заана.

  Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\ Specify the maximum log file size (KB) - давуу эрхтэй, хамгийн багадаа 20480 KB утга авна

  Computer Configuration\Policies\Windows Settings\Security Settings\Event Log\Maximum security log size

  “Control event log behavior when the log file reaches its maximum size” : enabled – лог файлыг нөөцөлнө.
  Archive- FILENAME - YYYY - MM - DD - hh - mm - ss – msec.evtx
  EventID: 1105

Location, MaxSize, Retention …



Account Logon – LM, NTLM, NTLMv2 протоколын хэрэглээг хянах

Дэд тохиргоо	**Үйлдлийн дугаар - EventID**
Audit Credential Validation	4774, 4775, **4776**, 4777
Audit Kerberos Authentication Service	4768, 4771, 4772
Audit Kerberos Service Ticket Operations	4769, 4770
Audit Other Account Logon Events	4649, 4778, 4779, 4800, 4801, 4802, 4803, 5378, 5632, 5633

- 4776 – нэвтрэлт шалгагдсан бол үүснэ. Гэхдээ хаашаа нэвтэрч буй компьютерийн нэрээс эхлээд дэлгэрэнгүй мэдээлэл бичигдэхгүй, харин нууц үр буруу, байхгүй хэрэглэгч зэрэг алдааны код бичигдэнэ.

Account Management

Дэд тохиргоо	Үйлдлийн дугаар - EventID
Audit Application Group Management – Microsoft Auth manager basic and LDAP query application groups	4783, 4784, 4785, 4786, 4787, 4788, 4789, 4790, only AD
Audit Computer Account Management	4741, 4742, 4743, only AD
Audit Distribution Group Management	4744, 4745, 4746, 4747, 4748, 4749, 4750, 4751, 4752, 4753, 4759, 4760, 4761, 4762
Audit Other Account Management Events	4782, 4793 – Password policy checking or hash import API
Audit Security Group Management	4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4754, 4755, 4756, 4757, 4758, 4764 – local or AD group
Audit User Account Management – бараг бүгдийг идэвхжүүлэх	**4720, 4722, 4723, 4724, 4725, 4726, 4738, 4740, 4765, 4766, 4767, 4780, 4781, 4794, 5376, 5377**

4728 гишүүн глобал групт(зөвхөн домэйн) нэмэгдэх.

4732 гишүүн локал групт нэмэгдэх.

4720	A (local) user account was created
4722	A user account was enabled
4723	An attempt was made to change an account's password.
4724	An attempt was made to reset an account's password.
4725	A user account was disabled.
4726	A user account was deleted.
4738	A user account was changed
4740	A user account was locked out .....

Detailed Tracking

Дэд тохиргоо	Үйлдлийн дугаар - EventID
Audit DPAPI Activity	4692, 4693, 4694, 4695
Plug and Play Events	6416, 6419, 6420, 6421, 6422, 6423, 6424
Audit Process Creation – хамгийн чухал хэсэг	4688, 4696
Audit Process Termination – хэрэг болохгүй	4689
Audit RPC Events – ямарч лог үүсэхгүй	5712

6416 - шинэ төхөөрөмж USB портонд холбогдох
4688 - хамгийн чухал дугаар процесс шинээр үүсэх үед энэ лог үүснэ
4696 - процесс UAC, RunAS ашиглан өөр токен эрхээр ажиллах үед энэ лог үүснэ

DS Access

Дэд тохиргоо	Үйлдлийн дугаар - EventID
Audit Detailed Directory Service Replication	4928, 4929, 4930, 4931, 4934, 4935, 4936, 4937
Audit Directory Service Access	4662
Audit Directory Service Changes	5136, 5137, 5138, 5139, 5141
Audit Directory Service Replication	4932, 4933

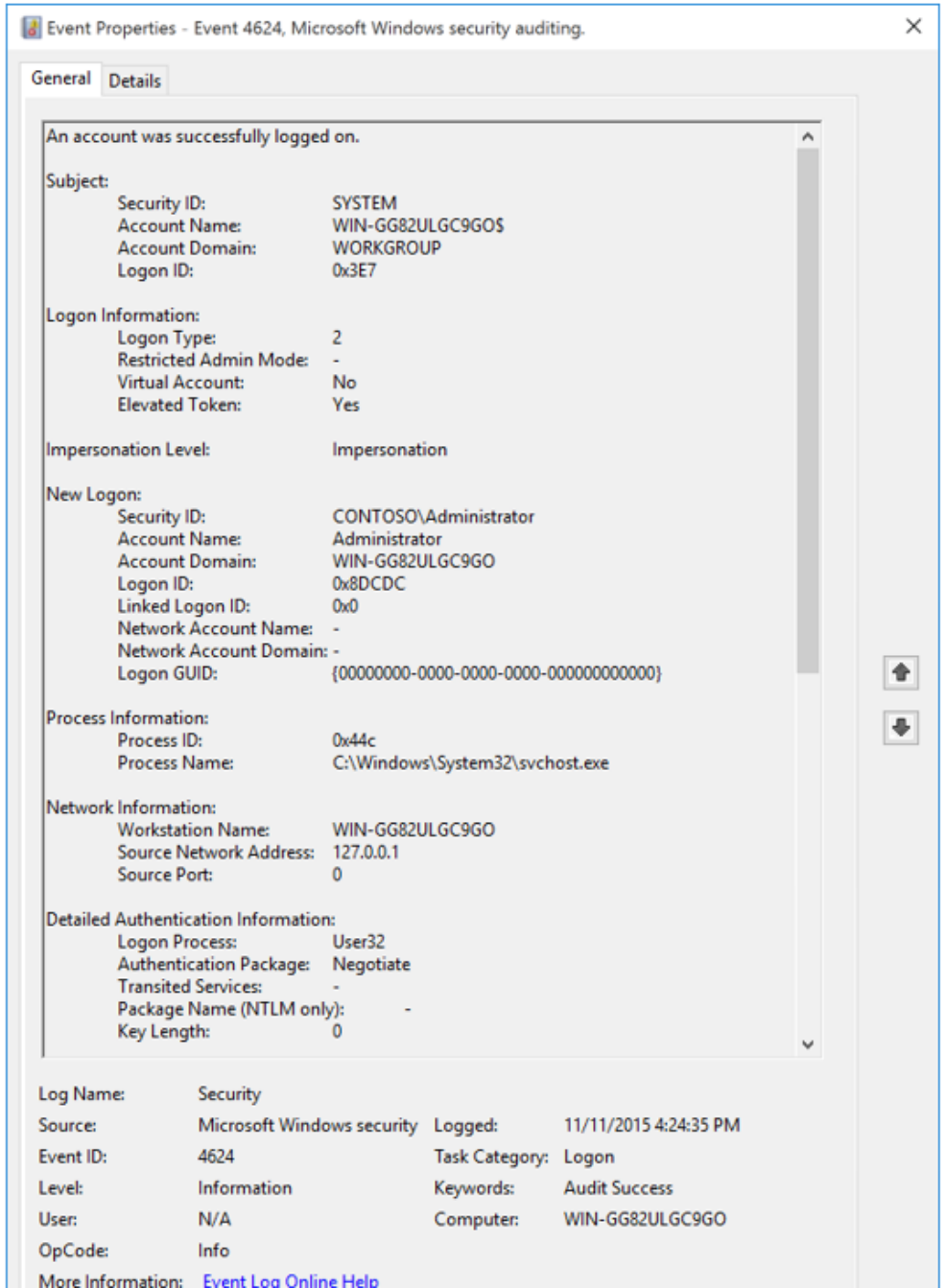
Зөвхөн домэйнд зориулагдсан тохиргооны хэсэг
Directory Service Access: Failure тохируулсан үед domain replication хийвэл хэдэн арван сая Event 4662 их хэмжээгээр үүснэ. Энэ log collector зогсооход хүргэж болно.

Logon/Logoff

Дэд тохиргоо	Үйлдлийн дугаар - EventID
Audit Account Lockout	4625
Audit IPsec Extended Mode	4978, 4979, 4980, 4981, 4982, 4983, 4984
Audit IPsec Main Mode	4646, 4650, 4651, 4652, 4653, 4655, 4976, 5049, 5453
Audit IPsec Quick Mode	4977, 5451, 5452
Audit Logoff	4634, 4647
Audit Logon	4624, 4625, 4648, 4675
Audit Network Policy Server	6272, 6273, 6274, 6275, 6276, 6277, 6278, 6279, 6280
Audit Other Logon/Logoff Events	4649, 4778, 4779, 4800, 4801, 4802, 4803, 5378, 5632, 5633
Audit Special Logon	4964

4624 – нэвтрэх процесс амжилттай болсон үед дэлгэрэнгүй лог үүснэ, Logon type 3 бол сүлжээнээс, 10 RDP ээр нэвтэрсэн.
4625 – нэвтрэх процесс амжилтгүй болсон үед дэлгэрэнгүй лог үүснэ
4648 – Процесс давуу эрхтэй хэрэглэгчээр ажиллах үед үүснэ
Account lockout: Success зөвхөн байвал зохимжтой

4624(S): An account was successfully logged on.



Event Description:

This event generates when a logon session accessed, where the session was created.

Note For recommendations, see Security

Event XML:

```
- <Event xmlns="http://schemas.microsoft.
- <System>
  <Provider Name="Microsoft-Windows-Sec
  <EventID>4624</EventID>
  <Version>2</Version>
  <Level>0</Level>
  <Task>12544</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keyw
  <TimeCreated SystemTime="2015-11-12T
  <EventRecordID>211</EventRecordID>
  <Correlation ActivityID="{00D66690-1CDF
  <Execution ProcessID="716" ThreadID="7
  <Channel>Security</Channel>
  <Computer>WIN-GG82ULGC9GO</Compu
  <Security />
  </System>
- <EventData>
  <Data Name="SubjectUserSid">S-1-5-18</
```

Logon/Logoff

Logon Type	Logon Title	Description
2	Interactive	A user logged on to this computer.
3	Network	A user or computer logged on to this computer from the netw
4	Batch	Batch logon type is used by batch servers, where processes ma intervention.
5	Service	A service was started by the Service Control Manager.
7	Unlock	This workstation was unlocked.
8	NetworkCleartext	A user logged on to this computer from the network. The user unhashed form. The built-in authentication packages all hash c credentials do not traverse the network in plaintext (also calle
9	NewCredentials	A caller cloned its current token and specified new credentials same local identity, but uses different credentials for other ne
10	RemoteInteractive	A user logged on to this computer remotely using Terminal Se
11	CachedInteractive	A user logged on to this computer with network credentials th controller was not contacted to verify the credentials.

Object Access

Дэд тохиргоо	Үйлдлийн дугаар - EventID
Audit Certification Services	4868, 4869, 4870, 4871, 4872, 4873, 4874, 4875, 4876, 4877, 4878, 4879, 4880, 4881, 4882, 4883, 4884, 4885, 4886 ,4887, 4888, 4889, 4890, 4891, 4892, 4893, 4894, 4895, 4896, 4897, 4898
Audit Detailed File Share	5145
Audit File Share	5140, 5142, 5143, 5144, 5168
Audit File System	4664, 4985, 5051
Audit Filtering Platform Connection	5031, 5140, 5150, 5151, 5154, 5155, 5156, 5157, 5158, 5159
Audit Filtering Platform Packet Drop	5152, 5153
Audit Handle Manipulation	4656, 4658, 4690
Audit Kernel Object	4659, 4660, 4661, 4663
Audit Other Object Access Events	4671, 4691, 4698, 4699, 4700, 4701, 4702 ,5148, 5149, 5888, 5889, 5890, COM+, Scheduled task etc …
Audit SAM	4661
Removable Storage	4656,4658,4663

Audit detailed File Share – бүх сүлжээнд share хийсэн файл, хавтаснуудын хандалтыг дэлгэрэнгүй бүртгэнэ (SACL тавих хэрэгтэй)
Audit File Share – share үүсэх, болиулах, өөрчлөх, зөвхөн хандалтын эхний хэсэг зэрэг үйлдэл хянагдана. (SACL тавих хэрэгтгүй учир бүг share хянагдана)
Audit Other Object Access Events – Event ID 4662, Bitlocker зэрэг лог их хэмжээгээр үүсгэдэг эх сурвалжуудыг хаах
Filtering platform – EventID 5152, 5157 их үүсэх учир Multicast Name Resolution хаах

Policy Change

Дэд тохиргоо	Үйлдлийн дугаар - EventID
Audit Audit Policy Change	4715, 4719, 4817, 4902, 4904, 4905, 4906, 4907, 4908, 4912
Audit Authentication Policy Change	4713, 4716, 4717, 4718, 4739, 4864, 4865, 4866, 4867
Audit Authorization Policy Change	4704, 4705, 4706, 4707, 4714
Audit Filtering Platform Policy Change	4709,4710,4711,4712,5040,5041,5042,5043,5044,5045,5046,5047,5048,5440,5441,5442,5443,5444,5446,5448,5449,5450,5456,5457,5458,5459,5460,5461,5462,5463,5464,5465,5466,5467,5468,5471,5472,5473,5474,5477
Audit MPSSVC Rule-Level Policy Change	4944,4945,4946,4947,4948,4949,4950,4951,4952,4953,4954,4956,4957,4958
Audit Other Policy Change Events	4714,4819,4826,4909,4910,5063,5064,5065,5066,5067,5068,5069,5070,5447,6144,6145
Audit Non Sensitive Privilege Use	4673, 4674, 4985
Audit Other Privilege Use Events	4985
Audit Sensitive Privilege Use	4673,4674,4985

Ямар Security policy эхсүл аль нэг зүйлийн SACL өөрчлөлт орох үед лог үүснэ

System

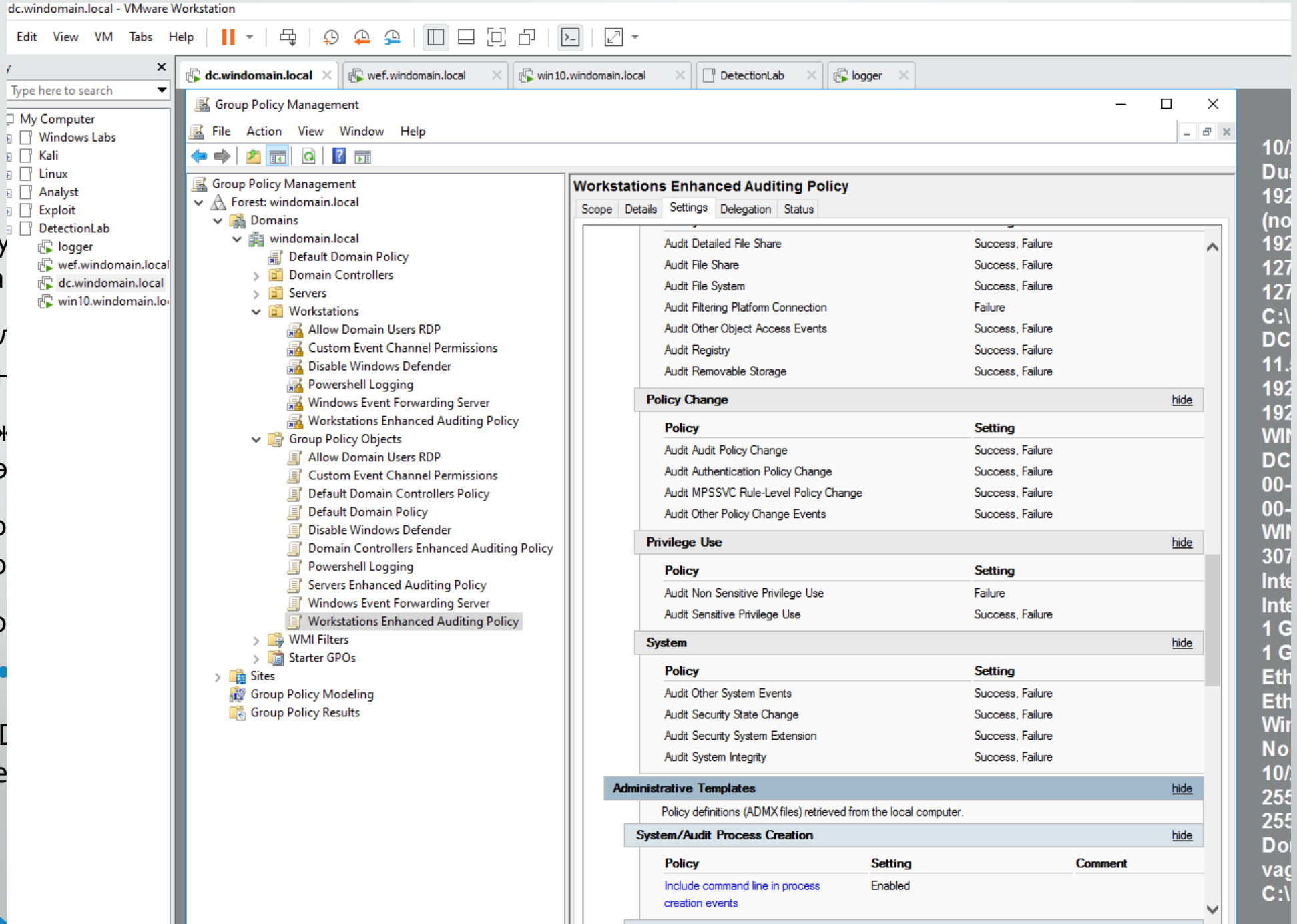
Дэд тохиргоо	Үйлдлийн дугаар - EventID
Audit IPsec Driver	4960, 4961, 4962, 4963, 4965, 5478, 5479, 5480, 5483, 5484, 5485
Audit Other System Events	5024, 5025, 5027, 5028, 5029, 5030, 5032, 5033, 5034, 5035, 5037, 5058, 5059, 6400, 6401, 6402, 6403 ,6404, 6405, 6406, 6407, 6408
Audit Security State Change	4608, 4609 ,4616, 4621
Audit Security System Extension	4610, 4611, 4614, 4622, 4697
Audit System Integrity	4612, 4615, 4618, 4816, 5038, 5056, 5057, 5060, 5061, 5062, 6281

4608 – цаг өөрчлөгдөх

Виндоусын коммандын лог

- Виндоус үйлдлийн системд ажлуулсан коммандуудын логыг авах боломжтой байдгийг түрүүн дурдсан. Гэхдээ энэ нь хангалтгүй учир бусад тохиргоотой хамт ашиглах ёстой.
- Энэ боломжийг Windows 7 гоос дээш хувилбарт ашиглах боломжтой бөгөөд ажлуулсан коммандын мөрийг бүтнээр нь лог уруу хадгална.
- Идэвхжүүлэхдээ gpedit.msc буюу ауюлгүй байдлын тохиргоо хийгч коммандыг ашиглан дараах хоёр хэсэгт хийнэ.
  - Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies\Detailed Tracking:Success
  - Computer Configuration\Administrative Templates\System\Audit Process Creation
    - "Include command line in process creation events": Enable
- Event ID 4688 дугаартай лог бичлэг үүснэ. Лог унших боломжтой бүх хүн коммандын параметерүүдийг харна.

- Виндоу
  дурдса
- Энэ бол
  комман
- Идэвхж
  хоёр хэ
  - Co
    Co
  - Co
    -
- Event ID
  параме



Windows Powershell логийг авах

- Виндоусын автоматжуулалтын скрипт програмчлалын хэл
- Windows Powershell, Powershell Core, Powershell 7, WinRM
- Batch, WMIC, VBScript илүү боломжтой, маш өргөн хэрэглэгдэж байна
- Windows 7/2008 серверын powershell 2.0 лог маш бага мэдээлэлтэй
- Дараагийн хувилбарууд нь илүү сайжруулсан лог авах боломжтой
- PowerSploit, Powershell Empire, Nishang, Powerup болон Evil-WinRM зэрэг олон хакерын програмууд бий болсон
- Файл үүсгэхгүйгээр вируснууд (File less malware) ажиллах болсоноор вирус хамгаалалтын програмууд илрүүлэх боломжгүй болж эхэлсэн

Lee Holmes – Аюулгүй байдлын боломжууд

	Event Logging	Transcription	Dynamic Evaluation Logging	Encrypted Logging	App Whitelisting	Antimalware Integration	Local Sandboxing	Remote Sandboxing	Untrusted Input Tracking
Bash	No**	No*	No	No	Yes	No	No	Yes	No
CMD / BAT	No	No	No	No	Yes	No	No	No	No
JScript	No	No	No	No	Yes	Yes	No	No	No
LUA	No	No	No	No	No	No	No	Yes	Yes
Perl	No	No	No	No	No	No	No	Yes	Yes
PHP	No	No	No	No	No	No	No	Yes	Yes
PowerShell	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No**
Python	No**	No	No**	No	No**	No**	No	No	No**
Ruby	No	No	No	No	No	No	No	No**	Yes
sh	No**	No	No	No	No	No	No	Yes	No
T-SQL	Yes	Yes	Yes	No	No	No	No**	No**	No
VBScript	No	No	No	No	Yes	Yes	No	No	No
zsh	No**	No	No	No	No	No	No	Yes	No

** Feature exists, but cannot be enforced via policies*
***Experimental*

Powershell логын тохиргооны шаардлага

- Windows 10, 2016 сервер сайжруулсан логийг авахад нэмэлт зүйл шаардлага үгүй.
- Windows 7/8.1/2008/2012 системүүд Powershell 5.0 суулгавал дараахыг суулгах хэрэгтэй:
  - .NET 4.5
  - Windows Management Framework (WMF) 4.0 (Windows 7/2008 зөвхөн)
  - Windows Management Framework (WMF) 5.0 энэ нь Powershell 5.0 суулгац юм
  - Windows 7 and 2008 R2 дээр эхэлж Windows Management Framework (WMF) 4.0 суулгаж байж WMF 5.0 суулгана.
- Windows 7/8.1/2008/2012 системүүд PowerShell 4.0 суулгавал дараахыг суулгах хэрэгтэй :
  - .NET 4.5
    Windows Management Framework (WMF) 4.0 е энэ нь Powershell 4.0 суулгац юм
    The appropriate WMF 4.0 update
    - 8.1/2012 R2 – KB3000850
    - 2012 – KB3119938
    - 7/2008 R2 SP1 – KB3109118
- Windows Powershell 2.0 авч хаях

Powershell лог тохируулах

- gpedit.msc – аюулгүй байдлын тохиргооны багаж комманд хэрэгтэй
- Дараах 3 хэсгийг идэвхжүүлэх
- Administrative Templates → Windows Components → Windows PowerShell
  - Module logging, Event ID 4103, модуль коммандын мөрийг болон үр дүн, мөн скриптын хэсгийг
    - HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ModuleLogging\EnableModuleLogging: 1
      HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ModuleLogging \ModuleNames : * *
  - Script Block, Event ID 4104, 4105 эхлэл,4106 төгсгөл, ажлуулсан скриптыг эхийг л бүтэн авна, үр дүн авахгүй
    - HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging\EnableScriptBlockLogging:1
    - Powershell 5.0 идэвхжүүлээгүй үед сэжигтэй кодыг EventID 4104 warning бүртгэж авна
  - Transcription, Powershell Terminal дээр ажлуулсан коммандын оролт, гаралт логыг хэрэглэгч тус бүртийн документ хавтсанд “Powershell_transcript” нэрээр эхэлсэн текст файлд хадгална. Зөвхөн бичих эрхтэй сүлжээний хавтсанд хадгалах зохимжтой.
    - HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\Transcription\EnableTranscripting: 1
      HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\Transcription\EnableInvocationHeader = 1
      HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\Transcription\OutputDirectory = “” (Enter path. Empty = default)
    - Бүх хэрэглэгчийн логыг авна гэвэл C:\Windows\System32\WindowsPowerShell\v1.0\profile.ps1,
      - a. $LogCommandHealthEvent = $true Command Line Details
      - b. $LogCommandLifecycleEvent = $true Command Line Details
      - c. $LogPipelineExecutionDetails = $true Module Loading (within scripts)
      - d. $PSVersionTable.PSVersion Shows the version of PowerShell installed
- Microsoft-Windows-PowerShell-Operational, EventID 4104 – скирптын коде,4100,4103,4104
- Application and Service Logs-Windows Powershell, EventID 200,400,500,501, 800
- AuditFileSsytem EventiD 4656 файл өөрчлөгдвөл
- Microsoft-Windows-Windows Remote Management-Operational

Boot Time: 10/25/2020 9:31 PM
CPU: Dual 2.20 GHz Intel Core i7-8750
Default Gateway: 192.168.38.1
DHCP Server: (none)
192.168.29.254

PowerShell_transcript.WIN10.XqJz_bfz.20201025221544.txt - Notepad

File Edit Format View Help

```
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
**********************
Command start time: 20201025221546
**********************
PS>. 'C:\Windows\System32\WindowsPowerShell\v1.0\profile.ps1'
**********************
Command start time: 20201025221552
**********************
PS C:\Windows> cls
**********************
Command start time: 20201025221602
**********************
PS C:\Windows> Get-Service

Status   Name               DisplayName
------   ----               -----------
Stopped  AarSvc_8044b       Agent Activation Runtime_8044b
Stopped  AJRouter           AllJoyn Router Service
Stopped  ALG                Application Layer Gateway Service
Stopped  AppIDSvc           Application Identity
Stopped  Appinfo            Application Information
Stopped  AppMgmt            Application Management
Stopped  AppReadiness       App Readiness
Stopped  AppVClient         Microsoft App-V Client
Stopped  AppXSvc            AppX Deployment Service (AppXSVC)
Stopped  AssignedAccessM... AssignedAccessManager Service
Running  AudioEndpointBu... Windows Audio Endpoint Builder
Running  Audiosrv           Windows Audio
Stopped  autotimesvc        Cellular Time
Stopped  AxInstSV           ActiveX Installer (AxInstSV)
```

20201025

File Home Share View

« Windows 2016 (C:) › pslogs › 20201025

Search 20201025

Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network

Name	Date modified
PowerShell_transcript.DC.IZxWSIPn.20201025214402.txt	10/25/2020 9:44 P
PowerShell_transcript.DC.V68wII1y.20201025213454.txt	10/25/2020 9:38 P
PowerShell_transcript.WEF.8qXp_NzP.20201025054751.txt	10/25/2020 5:47 A
PowerShell_transcript.WEF.EiLAFMuj.20201025033545.txt	10/25/2020 3:35 A
PowerShell_transcript.WEF.IqgfMBw5.20201025043323.txt	10/25/2020 4:33 A
PowerShell_transcript.WEF.L6HgwxIX.20201025213642.txt	10/25/2020 9:40 P
PowerShell_transcript.WEF.RDHSSN50.20201025040059.txt	10/25/2020 4:01 A
PowerShell_transcript.WEF.Rf3eGQr1.20201025033600.txt	10/25/2020 3:36 A
PowerShell_transcript.WEF.rJ6DtWxy.20201025054750.txt	10/25/2020 5:47 A
PowerShell_transcript.WEF.WDbkEWRX.20201025043313.txt	10/25/2020 4:33 A
PowerShell_transcript.WEF.YpVNjwZa.20201025040100.txt	10/25/2020 4:01 A
PowerShell_transcript.WIN10.hYX0YV8q.20201025213525.txt	10/25/2020 9:40 P
PowerShell_transcript.WIN10.XqJz_bfz.20201025221544.txt	10/25/2020 10:15

13 items 1 item selected 691 bytes State: Shared

System Type: Server, Stand-alone, Terminal Se
User Name: vagrant
Volumes: C:\ 59.66 GB NTFS

Microsoft SysInternals Sysmon

- Sysmon програм нь системийн драйвер хэлбэрээр ажиллах бөгөөд виндоус үйлдлийн систем дээр дуудагдан ажиллаж буй процессын мэдээлэл болон түүнийг дуудан ажлуулсан процессийн нэрнээс гадна дараах мэдээлийг харгалзах EVENT ID гаар лог уруу бичнэ. Мөн файлын хаш буюу тухайн файлыг төлөөлөх математикийн үйлдлээр гаргаж авсан тоон цувааг авах боломжтой.

Event ID	Үйлдэл	Event ID	Үйлдэл	Event ID	Үйлдэл
1	Процесс үүсэх	10	Процесс уруу өөр процесс хандах	19	WMIEventFilter илрэх
2	Процессийн үүсгэгдсэн цаг өөрчлөгдөх	11	Файл үүсэх	20	WMIEventConsumer илрэх
3	Сүлжээнд холбогдох	12	Регистер үүсэх, устах	21	WMIEventConsumerToFilter илрэх
4	Sysmon өөрийнх статус өөрчлөгдөх	13	Регистер утга өөрчлөгдөх	22	DNS тэй холбоотой үйдэл
5	Процесс зогсох	14	Регистер нэр өөрчлөгдөх	23	Файл устах
6	Драйвар ачаалах	15	Татагдсан урсгалын хаш үүсэх	255	Sysmon алдаа
7	Процессээс модул дуудах	16	Service ын тохиргоо өөрчлөгдөх		
8	Процесс дотор өөр процесс орох	17	Named pipe үүсэх		
9	\\.\ буюу стандарт бус аргаар файл уруу хандах	18	Named pipe холбогдох		

Sysmon коммандын жишээ

- Суулгах

sysmon –accepteula –i c:\windows\config.xml

- Болиулж зогсоох

sysmon –u

- Тохиргоог шинэчлэх

sysmon –c c:\windows\config.xml

- Тохиргооны бүтэцийг харах

sysmon –s

- Процесс болон үйлдлүүдийг дүрмээр ялган лог авах боломжтой (is, is not, contains, excludes, begin with, end with, less than г.м)
- Microsoft-Windows-Sysmon/Operational
- Тохиргоо нь XML файл байх бөгөөд үйлдэл бүрд зориулсан өөр өөр талбаруудыг агуулсан бүтэцтэй байна.
- Жишээ нь:
  - https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml
  - https://github.com/olafhartong/sysmon-modular

"

Анхаарал тавьсанд баярлалаа.

"

baasandorj@gmail.com
Systems administrator
Global Technology Service
IBM

Ашигласан хэрэгцээт вэбүүд

- https://github.com/OTRF/ThreatHunter-Playbook
- https://github.com/cyberdefenders/DetectionLabELK
- https://docs.microsoft.com/en-us/archive/blogs/jepayne/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem
- https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES
- https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
- https://github.com/danielbohannon/Revoke-Obfuscation
- https://github.com/danielbohannon/Invoke-Obfuscation
- https://devblogs.microsoft.com/powershell/defending-against-powershell-attacks/
- https://docs.ansible.com/ansible/latest/user_guide/windows_winrm.html
- https://devblogs.microsoft.com/powershell/powershell-the-blue-team/
- https://aka.ms/WEF
- https://www.varonis.com/blog/disabling-powershell-and-other-malware-nuisances-part-i/

Ашигласан номнууд

- Windows Security Monitoring Scenarios and Patterns
  ISBN-13: 978-1119390640
- Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat
  ISBN-13: 978-1091433896

Хэрэгтэй бусад коммандууд

- secedit /export /cfg c:\temp\baska-secedit.csv
- wevtutil gl security
- wevtUtil qe Security /q:"*[System[(EventID=4688)]]" /rd:true /f:xml
- wevtUtil qe Security /q:"*[System[(EventID=4688)]]" /rd:true /f:text
- wevtutil el
- logman query providers
- secedit /configure /cfg Security.csv /db defltbase.sdb /verbose
- Get-WinEvent -ListLog *, Get-WinEvent -ListLog *wmi* | select logname
- https://community.spiceworks.com/how_to/108867-transfer-all-group-policy-settings-from-one-system-to-another

Ашигласан файлууд

- Windows Advanced Audit Policy Map to Event IDs.xlsx

https://github.com/Spacial/awesome-csirt

- Windows 10 and Windows Server 2016 Security Auditing and Monitoring Reference.docx

https://www.microsoft.com/en-us/download/details.aspx?id=52630