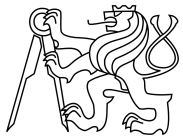
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Správa bezpečnostních událostí na Windows serveru 2008 R2
Student:	Silvie Müllerová
Vedoucí:	prof. Ing. Róbert Lórencz, CSc.
Studijní program:	Informatika
Studijní obor:	Informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	Do konce zimního semestru 2017/18

Pokyny pro vypracování

Proveďte rešerši možností nastavení zásad auditu zabezpečení Windows serveru 2008 R2 za účelem detekce bezpečnostních incidentů a reakce na ně.
Navrhněte a proveďte nastavení vhodné sady konkrétních zásad auditu zabezpečení a proveďte následný monitoring bezpečnostních událostí. Pro výpis vybraných bezpečnostních událostí vytvořte skript v powershellu. Tento skript použijte a otestujte na zachycených událostech.

Seznam odborné literatury

Dodá vedoucí práce.

L.S.

prof. Ing. Róbert Lórencz, CSc.
vedoucí katedry

prof. Ing. Pavel Tvrdík, CSc.
děkan

V Praze dne 15. března 2016

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra počítačových systémů

Bakalářská práce

Správa bezpečnostních událostí na Windows serveru 2008 R2

Silvie Müllerová

Vedoucí práce: prof. Ing. Róbert Lórencz, CSc.

17. května 2016

Poděkování

Děkuji vedoucímu práce prof. Ing. Róbertu Lórenczovi za trpělivost při psaní této práce.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 17. května 2016 .....

České vysoké učení technické v Praze
Fakulta informačních technologií
© 2016 Silvie Müllerová. Všechna práva vyhrazena.
Tato práce vznikla jako školní dílo na Českém vysokém učení technickém v Praze, Fakultě informačních technologií. Práce je chráněna právními předpisy a mezinárodními úmluvami o právu autorském a právech souvisejících s právem autorským. K jejímu užití, s výjimkou bezúplatných zákonných licencí, je nezbytný souhlas autora.

Odkaz na tuto práci

Müllerová, Silvie. *Správa bezpečnostních událostí na Windows serveru 2008 R2*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2016.

Abstrakt

Tato bakalářská práce má vybraným administrátorům, IT specialistům a bezpečnostním manažerům umožnit nahlédnout do problematiky bezpečnostních logů a jeho managementu v podnikovém prostředí. První část práce je věnována úvodu do problematiky a vysvětlení základních pojmů, které s tvorbou logů souvisejí. Druhá část je zaměřena především na praktickou ukázku automatického sběru logů a analýzu. Popisuje metodologický proces, jak by mohla organizace v případě logování událostí správně postupovat. Tato část je zaměřena na současné prostředí provozované jednou organizací ve státním sektoru, kde je majoritně prosazována platforma MS Windows.

Klíčová slova Log, analýza, klasifikace, log management, MS Windows, audit, servery, PowerShel

Abstract

This bachelor thesis should make it possible for administrators, IT specialists and security managers to look into problems security logs related to management in enterprise environment. The first part of the thesis is focused on introduction to the problem and explanation of elementary terms, which are closely connected with generating log events. The second part is primary aimed at practice demonstration of automatic collecting log events and analyze of them. It describes a methodological process how the organization should proceed correctly in a case of collecting log events. This practical part is focused on the actual environment of an organization which operates in a public sector where is majority implemented the MS Windows platform.

Keywords Log, analyze, classification, log management, MS vindows, audit, servers, PowerShell

Obsah

Seznam obrázků

Úvod

V současné době, kdy je většina sfér trhu závislá na informačních technologiích, je bezpečnost informací neustále se skloňujícím pojmem. Její význam neustále roste a stává se významnější v závislosti na vzrůstajícím počtu uživatelů, systémů, nároků na výkon hardwarových i softwarových technologii a v nich uchovávaných datech.

Vzniklá data jsou mnohdy pro jejich vlastníky neocenitelná a systémové prostředky potřebné pro jejich využívání omezené. Z těchto důvodů je nutné činit veškerá bezpečnostní opatření na všech bezpečnostních úrovních, a to takovým způsobem, aby se riziko zneužití, úplné ztráty či neschopnosti poskytnout služby eliminovalo na minimum.

Bezpečnost je pojem, který se jen těžce vyjadřuje finančními prostředky v případě, že nastane incident natolik vážný, že ochromí fungování jakéhokoliv celku v jeho individuálních cílech. Klíč ke snížení rizika dopadů kybernetických útoků je v prevenci a neustálé analýze bezpečnostních hrozeb.

Jedním ze základních nástrojů k identifikaci vzniklé situace je analyzování bezpečnostních záznamů v podobě logů. Drtivá většina technologií napříč systémem logy produkuje. Tyto systémové logy jsou v heterogenních prostředích generovány v obrovských objemech a dokáží významným způsobem zabírat dostupné systémové prostředky, tím systémy zpomalit a v některých případech zcela zastavit. V takovýchto případech při neuváženém nastavení auditování všech událostí může být velice rychle zahlcen log, což může vést k nedostupnosti stanice či serveru, přerušení logování nebo případně k přepisování starších logů atd. Takovéto incidenty mohou být využity například pro útoky typu DoS a DDoS.

Navíc pokud není nastavena v zájmovém systému nějaká strategie monitorování logů, může dojít k situaci, že se v takovém množství velice snadno ztratí či přehlédne důležitá událost nebo posloupnost událostí, jejichž význam upozorňuje na vznik nestandardní a potenciálně nebezpečné situace.

Díky využívání proaktivního monitoringu lze při správné analýze logů odhalit takovéto nebezpečí včas a zamezit tak vzniku bezpečnostnímu incidentu,

který by mohl vést k více či méně závažným škodám.

Hlavní výzvou a zároveň základním problémem je nalezení rovnováhy mezi kvalitou informační hodnoty a kvantitou sledovaných událostí. Ne všechny typy logů, které jsou takto produkovány, nesou pro monitorování bezpečnosti užitečná data. Je nutné nepodcenit výběr typů logů v závislosti na bezpečnostní strategii organizace. Touto disciplínou se zabývá log management. Základními funkcemi log managementu je výběr zájmových logů, jejich klasifikace, filtrace, vytěžování informace, notifikace, vyvolání reakce bezpečnostního systému a auditní řízení. Ačkoli se v médiích hovoří především o externích hackerských útocích, nejčastější útoky přicházejí zevnitř organizací vlastními zaměstnanci.

V případě nastalého bezpečnostního incidentu jsou bezpečnostní logy hlavním důkazním materiálem. Se špatně nastavenými zásadami auditování se ale o tyto cenné informace můžeme velice snadno připravit.

Použití systému zabývajícího se log managementem je zahrnuta i v mnoha národních a mezinárodních normách a standardech. Jmenovitě např. ISO 27001, ISO 27002, COSO Framework, zákon o kybernetické bezpečnosti 181/2014 v aktuálním znění, apod.

Kapitola 1

Bezpečnostní monitoring OS Windows

Bezpečnostní monitoring informačního systému je nedílnou součástí řízení informační bezpečnosti. Jeho hlavním úkolem je sledování a vyhodnocování bezpečnostních událostí a případná reakce na ně.

V operačním systému Windows se bezpečnostní události zaznamenávají do logu zabezpečení, který je zahrnut v OS Windows od verze NT 3.1 a vyšší. Defaultně mají přístup k tomuto souboru pouze administrátorské a uživatelské účty. Částečně je možné použít k prohlížení protokolu událostí textový editor, pro kompletní zobrazení ale není dostačující. Součástí OS Windows je prohlížeč událostí (snap-in modul MMC konzole), který nabízí přehledně uspořádané úplné zobrazení všech zaznamenaných událostí a je možné skrze něj přistupovat i k protokolům na vzdálených systémech.

Pro sběr, monitoring a analýzu logů existuje mnoho nástrojů, jak nativních přímo v prostředí MS, tak i SW třetích stran, které nabízí širokou škálu možností. Existují však případy, ať už z důvodu omezeného rozpočtu nebo striktně nastavených pravidel bezpečnostní politiky IS, která jasně vymezuje povolený SW, kdy takovéto nástroje není možné použít.

Z toho důvodu se bude tato práce zabývat právě možností monitoringu a analýzy událostí pomocí Powershellu, který je od verze MS Windows server 2008, potažmo MS Windows Vista vestavěnou součástí operačního systému. V rámci bezpečnostního monitoringu jsou vymezeny tři hlavní oblasti, kterými je třeba se zabývat. Jsou to zejména:

- detekce porušení bezpečnostní politiky,
- identifikace útoku,
- forenzní analýza.

Pro identifikaci neobvyklého chování v rámci počítačové sítě je třeba zvážit, co je typické pro konkrétní prostředí a co by se již dalo klasifikovat jako anomálie.

Další podmínkou či doporučením pro zjištění případných anomálií je nastavení výchozí úrovně zabezpečení, tzv. baseline security, na veškeré počítače v doméně.

Jednou ze základních metod operačního systému Windows je použití bezpečnostních šablon. Bez těchto nastavení by bylo obtížné identifikovat počítače, které nevyhovují základním bezpečnostním požadavkům. Následující část bude věnovaná právě detekci porušení bezpečnostních politiky.

1.1 Detekce porušení bezpečnostních zásad

Porušení bezpečnostních zásad informačního systému nemusí hned znamenat cílený útok či jinou nekalou činnost. Ve všech případech ale tvoří problém, s jakým se musí organizace vypořádat. Pro včasnou detekci narušení systému je základem proaktivní monitoring a analýza bezpečnostně relevantních událostí. Mezi rizikové aktivity, které stojí za to sledovat, patří:

- přístup ke zdrojům pomocí změny oprávnění,
- přístup ke zdrojům pomocí resetu hesla,
- vytvoření, změna nebo odstranění uživatelského účtu,
- umístění uživatele do skupiny,
- pokus o použití neautorizovaného účtu,
- interaktivní přihlášení s pověřením servisního účtu,
- spuštění neautorizovaného programu,
- přístup k neautorizovaným zdrojům,
- zničení autorizovaných souborů,
- zavedení neautorizovaného systému,
- získání pověření jiného uživatele,
- pokus obejít auditování,
- vytvoření nebo zrušení vztahu důvěry domén (AD DS trust),
- provedení neoprávněných změn zásad zabezpečení.[1]

Mezi nejčastější způsoby porušení pravidel patří neúmyslný pokus běžného uživatele o přístup k souboru či adresáři, ke kterému nemá běžně oprávnění. Omezením práv uživatele se tak předchází vzniku škody.

Mnohem závažnější však může být porušení pravidel administrátorem. Administrátoři disponují vysokým stupněm přístupových práv a oprávnění pro

výkon své práce. Mají možnost vytvářet účty, měnit hesla, oprávnění, příslušnost ke skupinám. Nicméně fakt, že mohou vykonávat určité procedury v systému, ještě neznamená, že je to v souladu s bezpečnostní politikou systému.

Přístup k informacím by se měl z pohledu bezpečnosti vždy řídit principem tzv. „need to know“. Jinými slovy, pokud osoba není pověřená, aby se seznamovala s určitými informacemi, neměla by k nim mít možnost přistupovat.

Je důležité, aby organizace oddělily role osob zainteresovaných do příslušného informačního systému a striktně definovaly jejich povinnosti a pravomoci. Dle doporučení DISA STIG (The Defense Information Systems Agency Security Technical Implementation Guides) by měla být vytvořena skupina zodpovědná za audit událostí, která by měla mít plnou kontrolu nad logy. Oprávnění administrátorů vůči aplikačním a systémovým logům a logům zabezpečení by měla být zredukována pouze na Read (čtení) a Execute (spouštění). Skupina auditorů by kromě výše uvedených práv neměla mít žádná vyšší oprávnění týkající se správy systému.

Při implementaci funkčního bezpečnostního monitoringu založeném na událostech zabezpečení OS MS Windows je nutné vzít v úvahu obrovský objem událostí zabezpečení. S ohledem na bezpečnostní politiku organizace a konkrétní informační systém je nutné pečlivě zvážit, jaké zásady auditu zabezpečení povolit a jaké naopak zakázat. Podrobnější popis zásad auditu zabezpečení na Windows serveru 2008 R2 bude následovat v dále v textu.

V následujících podkapitolách budou popsány jednotlivé aktivity včetně souvisejících událostí, které mohou značit porušení bezpečnostních zásad systému.

1.2 Přístup ke zdrojům pomocí změny oprávnění

Administrátoři mohou přistupovat k souborům, ke kterým nemají oprávnění, a volně s nimi nakládat. To se děje prostřednictvím převzetí vlastnictví k danému souboru s následným přidáním svého účtu do seznamu uživatelů oprávněných k manipulaci se souborem.

Je kontraproduktivní nastavit auditování přístupu k objektům na všech souborech a složkách, protože případná nežádoucí aktivita by byla rázem ztracena v ohromném množství událostí generovaných běžnou oprávněnou manipulací se soubory či složkami. Proto by auditování mělo být nastaveno jen po důkladném zvážení u souborů vysoké hodnoty obsahujících obzvlášť citlivá data.

Pro odhalení možného nežádoucího přístupu k souborům je třeba znát následující faktory:

- Který uživatel zažádal o přístup?

- Na který objekt se cílilo?
- Měl uživatel oprávnění k přístupu?
- O jaký typ přístupu (čtení, zápis, spuštění, atd.) se jednalo?
- Byla událost úspěšná nebo neúspěšná?
- Z jakého počítače se uživatel pokusil o přístup?

Prohlížeč událostí neumožňuje detailní filtrování událostí podle předchozích faktorů, nicméně za pomoci powershellu, případně jiných nástrojů, které již ale nejsou vestavěnou součástí operačního systému, je možné sestavit velice podrobné filtry.

Následující přehled zobrazuje události zabezpečení týkající se přístupu k objektům:

- **ID 4656**:
  Byl vyžádán handle objektu – tato událost spadá do několika podkategorií kategorie „Object Access“. Konkrétní podkategorie závisí na typu objektu, vždy ale musí být zároveň povolena podkategorie „Handle manipulation“. Pokud je povoleno auditování objektů, je toto první událost, která se vygeneruje při pokusu aplikace o přístup k objektu. Událost může být úspěšná nebo neúspěšná podle toho, zda uživatel získal na základě svého požadavku příslušná práva nebo ne. Podává informace o jménu uživatele a ID relaci přihlášení, o objektu a programu, prostřednictvím kterého byl handle vyžádán. Pro ujištění, zda vyžádaná práva byla nakonec uplatněna, je potřeba se podívat po události ID 4663 se stejným Handle ID.
- **ID 4663**:
  Byl učiněn pokus o přístup k objektu – tato událost již podává informaci o tom, že byla použita konkrétní oprávnění. Zahrnuje informaci o jménu uživatele, typu a názvu objektu, použitých oprávněních a názvu procesu.

1.3 Přístup ke zdrojům pomocí resetu hesla

Další možností, jak neoprávněně přistoupit ke zdrojům, je pomocí resetu hesla administrátorem. Tuto událost je opět možné monitorovat se správným nastavením zásad auditu, konkrétně zapnutím podkategorie „Audit User Account Management” (správa uživatelských účtů), a to pomocí následujících událostí:

- **ID 4723**:
  Pokus o změnu uživatelského hesla – tato událost je vygenerována při pokusu uživatele (lokálního i doménového) o změnu vlastního hesla. Pokud

nové heslo není akceptováno z důvodu, že nesplňuje požadavky zásad hesel, vznikne událost typu „Failure“. V případě, že uživatel zadá špatně původní heslo, není tato událost vůbec vyvolána. Místo ní se pro doménové účty vygeneruje neúspěšná událost ID 4771, kde je jako „Service name“ uvedeno kadmin/changepw.

- **ID 4724**:
  Pokus o reset uživatelského hesla – uživatel uvedený v sekci „Subject“ se pokusil o reset hesla uživatele uvedeného v sekci „Target“. Tito uživatelé jsou zpravidla rozdílní. V mnoha případech se jedná o požadavek oprávněného uživatele, který zapomněl heslo a zásahem administrátora mu je nastaveno nové, většinou s vynucením změny hesla při dalším přihlášení. Tato událost se opět loguje jak pro lokální, tak pro doménové účty.

- **ID 4794**:
  Pokus o nastavení Directory Services Restore Mode – událost se vygeneruje kdykoli, je-li úspěšně nastaveno DSRM administrátorské heslo,například pomocí nástroje ntdsutil.exe. Toto heslo je důležité, protože umožňuje obnovit nebo jakkoli jinak přistoupit k databázi Active Directory.

1.4 Vytvoření, změna nebo odstranění uživatelského účtu

Osoba s administrátorskými právy může velice snadno vytvořit účet pro neexistujícího zaměstnance a následně pod tímto účtem neoprávněně přistupovat k důvěrným datům nebo páchat jinou neoprávněnou činnost. Proto by vytváření, nebo změny uživatelských účtů měly být pod kontrolou a vždy probíhat v souladu s jasně stanovenými procesy danými bezpečnostní politikou organizace.

V některých organizacích se pro automatizaci správy účtů a přidělování oprávnění využívají „provisioning“ systémy, které bývají propojeny například na personální databázi a tím vnáší nad těmito procesy větší míru kontroly. Ovšem i v organizacích, které podobnými automatizovanými systémy nedisponují, by mělo platit, že každá událost, která zaznamená vytvoření, případně změnu či zrušení uživatelského účtu, by měla korespondovat s oficiálním požadavkem.

Zároveň by měl mezi okamžikem vytvoření uživatelského účtu a okamžikem prvního zalogování uživatele a prvotní změny hesla existovat jen krátký interval. Pokud se uživatel během předepsaného času nepřihlásí, měl by být účet zablokován a bezpečnostní správce by měl zjistit důvod, proč nedošlo k aktivaci. U určitých systémů, často s vyšším stupněm utajení, bývá toto prvotní přihlášení ošetřeno tak, že po zřízení uživatelského účtu na základě oficiálního

požadavku je účet zakázán, a až ve chvíli, kdy je přítomen konkrétní uživatel, je daný účet povolen.

Níže jsou uvedeny související události z podkategorie správy uživatelských účtů:

- **ID 4720**:
  Vytvoření uživatelského účtu – v sekci „Subject“ pod položkou „Account Name“ je zaznamenáno, kdo účet vytvořil. V sekci „New Account“ pod položkou „Account Name“ je pak název nového účtu. Obě tato jména je vhodné pro kontrolu prověřit a zkontrolovat, že nový účet byl vytvořen oprávněně.

- **ID 4726**:
  Odstranění uživatelského účtu.

- **ID 4738**:
  Změna uživatelského účtu – uživatel v sekci „Subject“ změnil účet uživatele uvedeného v sekci „Target Account“. Změněné parametry jsou uvedeny v sekci „Attributes“.

- **ID 4781**:
  Změna uživatelského jména Logování těchto událostí je možné povolit nastavením podkategorie „Audit User Account Management” na hodnoty „Success“ a „Failure“.

1.5 Umístění uživatele do skupiny

Ve službě „Active Directory“ existují dva typy skupin: distribuční skupiny a skupiny zabezpečení. Distribuční skupiny slouží k vytvoření seznamů pro distribuci e-mailů, zatímco skupiny zabezpečení umožňují přiřazovat oprávnění pro přístup ke sdíleným prostředkům. K zavedeným bezpečnostním praktikám patří princip nejnižších oprávnění, kdy se jedná jednoduše o to, že je uživatelům přiřazeno pouze nutné minimum oprávnění potřebné k vykonávání jejich práce.

Z důvodu snadnější a bezpečnější správy je nanejvýš vhodné zařadit všechny uživatele do doménových uživatelských skupin a do skupin zabezpečení vycházejících standardně z organizační struktury.

Zařazení uživatele do skupin s vyššími oprávněními, jako jsou „Domain“ nebo „Enterprise Admins“, by mělo být vždy podloženo oficiálním požadavkem. Změny v těchto skupinách by rozhodně neměly být na denním pořádku a měli by být podrobeny důkladnějšímu zkoumání.

Dalším typem skupin jsou distribuční skupiny, které samy o sobě nepředstavují riziko neoprávněného přístupu. Nicméně může se stát, že chybným přidáním uživatele do špatné skupiny, např. skupiny ředitelství, může tento

uživatel obdržet e-mail s důvěrnými informacemi, které by se rozhodně neměly dostat mimo oprávněnou skupinu.

Níže jsou uvedeny některé události týkající se změn skupin. Všechny tyto události spadají pod kategorii Audit správy účtů, konkrétně do podkategorie Správa skupin zabezpečení. U všech událostí lze vyčíst, kdo operaci provedl, na jaké skupině, případně s jakým členem.

- Globální skupiny
  - **ID 4727**: Byla vytvořena globální skupina zabezpečení.
  - **ID 4728**: Do globální skupiny zabezpečení byl přidán nový člen.
  - **ID 4729**: Z globální skupiny zabezpečení byl odebrán jeden člen.
  - **ID 4730**: Byla odstraněna globální skupina zabezpečení.
  - **ID 4737**: Byla změněna globální skupina zabezpečení.

  U výše uvedených událostí je třeba se zaměřit především na skupiny mající rozsáhlá přístupová oprávnění jako např. skupina „Domain Admins“ pro ověření, že nedošlo k žádným neoprávněným změnám. Název skupiny, které se operace týká, je pod položkou „Target Account Name“.

- Lokální skupiny
  - **ID 4731**: Byla vytvořena lokální skupina zabezpečení.
  - **ID 4732**: Do lokální skupiny zabezpečení byl přidán nový člen.
  - **ID 4733**: Z lokální skupiny zabezpečení byl odebrán jeden člen.
  - **ID 4734**: Byla odstraněna lokální skupina zabezpečení.
  - **ID 4735**: Byla změněna lokální skupina zabezpečení.

  U těchto událostí je vhodné se zaměřit na skupiny jsou „Administrators“, „Server Operators“, „Backup Operators“ a další skupiny s vyššími právy.

- Univerzální skupiny
  - **ID 4754**: Byla vytvořena univerzální skupina zabezpečení.
  - **ID 4755**: Byla změněna univerzální skupina zabezpečení.
  - **ID 4756**: Do univerzální skupiny zabezpečení byl přidán nový člen.
  - **ID 4757**: Z univerzální skupiny zabezpečení byl odebrán jeden člen.
  - **ID 4758**: Byla odstraněna univerzální skupina zabezpečení.

- Změna typu skupiny
  - **ID 4764**: Původní i nový typ skupiny je uveden pod položkou Change Type.

1.6 Pokus o použití neautorizovaného účtu

Velkým nebezpečím bývá pokus o prolomení účtu administrátora. Při vytváření domény vznikne v „Active Directory“ i vestavěný účet „Administrator“, který je defaultně členem skupiny „Domain Admins“, „Administrators“ a v případě, že se jedná o kořenovou doménu tzv. „root domain“, tak i o „Enterprise Admins“. Tento účet může být zakázán, ale při startu v nouzovém režimu je automaticky povolen. Není možné ho ani smazat ani uzamknout. Je to jediný účet, na který se neaplikuje zásada zamykání účtů.

To přímo vybízí útočníky pokusit se u tohoto účtu prolomit heslo. Z toho důvodu je doporučené přejmenovat tento účet a změnit popis tak, aby nebylo patrné, že se jedná o účet s nejvyššími oprávněními. Všechny události pokusu o přihlášení k administrátorskému účtu by měly být monitorovány, přičemž zvlášť velká pozornost by měla být věnována neúspěšným událostem.

Dalším případem bývá pokus o přihlášení se k zakázaným nebo expirovaným účtům. Může se jednat o bývalé zaměstnance nebo servisní pracovníky smluvních partnerů, kterým byl přidělen dočasný účet. Pokud tyto události nastanou, vyžadují okamžité detailní prozkoumání.

Mezi relevantní události, jež je třeba sledovat, patří:

- **ID 4624**:
  Účet byl úspěšně přihlášen – toto je v případě vyšetřování bezpečnostního incidentu zásadní událost, která poskytuje velmi cenné informace o každém úspěšném pokusu o přihlášení. Kromě názvu přihlášeného uživatelského účtu informuje mimo jiné o názvu stanice a IP adrese, z které přihlášení proběhlo, dále o typu přihlášení, což bývá nejčastěji interaktivní a sítové přihlášení. Pomocí „LogonID”, které vymezuje danou relaci přihlášení (začíná okamžikem přihlášení a končí okamžikem odhlášení uživatelského účtu). Je možné provázat tuto událost s následujícími událostmi, které proběhly pod daným uživatelským účtem v dané relaci.

- **ID 4625**:
  Přihlášení k účtu selhalo – další významnou událostí je neúspěšný pokus o přihlášení. Zaznamenává každé selhání přihlášení k účtu nehledě na typ účtu, typ nebo místo přihlášení. V sekci „Failure Information“ jsou obsaženy podrobnější informace o důvodu selhání. Velmi důležité je všímat si především většího množství opakovaných selhání v řadě, protože mohou signalizovat útok hrubou silou tzv. „Brute Force“ nebo slovníkový útok.

- **ID 4672**:
  Novému přihlášení byla přiřazena speciální oprávnění – většina těchto událostí se loguje pro systémové služby a naplánované úlohy, nicméně pomáhá detekovat i přihlášení uživatele s vyššími (administrátorskými oprávněními). Typicky těsně následuje událost ID 4624 dokumentující

přihlášení účtu administrátora (lze provázat pomocí Logon ID). Logování této události se povoluje nastavením auditování podkategorie „Sensitive Privilege Use“, jež je součástí kategorie „Audit privilege use”.

1.7 Interaktivní přihlášení s pověřením servisního účtu

Když služba startuje, musí se prokázat přihlašovacími oprávněními. V některých případech mohou servisní účty vyžadovat doménový účet za účelem připojení a spuštění služeb na vzdáleném počítači, jindy zase potřebují ke svému běhu administrátorská oprávnění.

Služby, které potřebují síťové připojení, mohou využívat účet „NT AUTHORITY\NetworkService“. Je třeba se ujistit, že všechny uživatelské účty, které jsou využívány službami, mají dostatečně silná hesla. Události přihlášení těchto účtů by měly nastat jen při spouštění příslušných služeb.

Zvýšená pozornost by měla být věnována případu, kdy se servisní účet přihlásí interaktivně (Logon Type 2) namísto přihlášení jako služba (Logon Type 5). Tato situace může nastat, když se útočníkovi podaří získat heslo servisního účtu a interaktivně se pomocí něj přihlásí. Pokud má tento účet administrátorská oprávnění, může útočník rozvrátit celý systém.

Mezi související události auditu zabezpečení patří:

- **ID 4624**:
  Úspěšné přihlášení k účtu. – pokud se zaznamená tato událost pro servisní účet s typem přihlášení 2 (Interactive) nebo 10 (RemoteInteractive), jedná se pravděpodobně o známku útoku a je třeba začít okamžitě jednat.

- **ID 4625**:
  Neúspěšné přihlášení k účtu – pokyny viz předchozí událost.

- **ID 4696**:
  Procesu byl přiřazen primární token – tato událost často nastává, když se služba nebo naplánovaná úloha spouští s oprávněním jiného uživatele. Tomu často předchází události ID 4624 a 4648, případně 4776 nebo 4748. Obsahuje název a ID jak samotného procesu, tak i jeho rodiče. Událost spadá pod kategorii Process Tracking – Process Creation.

- **ID 4697**:
  Byla nainstalovaná nová služba – vzhledem k tomu, že instalace služeb nepatří ke každodenním aktivitám, měla by se tato událost vyskytovat velice zřídka a každý její výskyt by měl být podroben bližšímu zkoumání. Auditní záznam obsahuje informace o jménu služby, jejím typu a způsobu spouštění a servisním účtu, pod kterým služba běží. Tato událost spadá pod kategorii Audit system events Security System Extension.

1.8 Spuštění neautorizovaného programu

Administrátoři jsou osoby s pravomocí mimo jiné instalovat a spouštět programy. Vždy by se ale měli držet seznamu odsouhlaseného programového vybavení. Pokud takový seznam není, měl by být organizací vytvořen a zároveň s ním by měl být popsán proces pro schvalování nového software. S výjimkou testování nového softwaru na izolovaném testovacím pracovišti by tedy administrátor neměl instalovat žádný SW, který není uveden na seznamu.

Neautorizovaný proces nemusí být spuštěn jen uživatelem či administrátorem, ale může se jednat i o malware. Častou technikou, kterou se malware snaží zakrýt svojí přítomnost, je změna hlásek u názvů standardních procesů (scvhost.exe, iexplore.exe, svcdost.exe) a spuštění procesů z nestandardního umístění (např. „C:\Windows\svchost.exe“ namísto standardního „C:\Windows\System32\svchost.exe“).[2]

Podezřelé je rovněž umístění procesu začínající malým písmenem označující diskovou jednotku, což naznačuje spuštění z příkazové řádky, dávkového souboru nebo skriptu.

Další technikou, jak snadno obelstít uživatele, aby spustil program, který se vydává za něco co není, bývá vložení dlouhého řetězce mezer do názvu procesu, který pak může vypadat následovně: „UserGuide.pdf .exe“. Škodlivý spustitelný program tak na první pohled může působit jako neškodný pdf soubor.

Jednou z technik, jak detekovat škodlivé procesy, je také analýza vztahu rodič-potomek mezi procesy reprezentovanými svými ID (PPID a PID). Většina systémových procesů totiž mívá jasně definované rodičovské procesy.

Všechny výše uvedené techniky vyžadují dobré oko a pokročilou znalost systému. K souvisejícím událostem, které je potřeba monitorovat patří:

- **ID 4688:**
  Byl vytvořen nový proces – tato událost dokumentuje každý spuštěný program, uživatele a proces, který jej spustil. Proces vznikne při každém spuštění programu a trvá až do jeho ukončení. Tento proces je identifikován svým ID, pomocí něhož je možné sledovat události vyvolané daným procesem.

- **ID 4698**: Byla vytvořena naplánovaná úloha.

- **ID 4699**: Byla smazána naplánovaná úloha.

- **ID 4700**: Byla povolena naplánovaná úloha.

- **ID 4701**: Byla zakázána naplánovaná úloha.

- **ID 4702**: Byla updatována naplánovaná úloha.

1.9 Zničení autorizovaných souborů

V tomto případě uživatel úmyslně zničí soubory, ke kterým má přístup, bez ohledu na následky. Často se tak stává v případech, kdy dotyčný zaměstnanec dostal výpověď, ale administrátor mu ještě nestihl zakázat uživatelský účet.

Pro omezení takových případů je ideálním řešením zavést „provisioning“ systém. V případě odchodu zaměstnance by se pak okamžitě odebrala jeho identita uživatele z úložiště identit a odstranil by se nebo zakázal jeho účet ze všech systémů, k nimž měl přístup.

1.10 Zavedení neautorizovaného systému

Neautorizovaný operační systém může značně podlomit bezpečnost celého systému. Vystavuje systém zvýšenému ohrožení viry a malwarem nebo může také způsobit kolizi IP adres z důvodu použití stejné IP adresy, jakou již používá jiné zařízení v síti.

Zavedení neautorizovaného operačního systému je možné několika způsoby. Uživatel může například přeinstalovat systém pomocí instalačního CD. V tomto případě je možné v logu událostí najít pokusy o přihlášení uživatele Administrator s nedefinovanou skupinou nebo s defaultní skupinou Workgroup.

Další z možností je použití Microsoft Virtual PC. Jedná se o kompletní emulaci operačního systému s vlastním názvem počítače, vlastními uživatelskými účty, skupinami, programy atd. běžící na hostujícím počítači. Virtual PC může zažádat o přidělení IP adresy a přistoupit tak ke zdrojům ve firemní síti nebo umožňuje namapovat síťová úložiště.

Problémem může být také vzdálené připojení pomocí např. domácího počítače, nebo live CD nějaké open source distribuce operačního systému. V případě druhého jmenovaného je problém v tom, že open source běží nezávisle na OS MS Windows a není možné zaznamenat jeho běh v logu událostí. Pokud se však v logu událostí objeví pokusy o přihlášení uživatele root, může to signalizovat právě tento případ.

V rámci bezpečnostního monitoringu je vhodné zaměřit se na události obsahující informace o neznámých uživatelských účtech, počítačích, skupinách nebo doménách, na duplikaci IP adres, případně IP adresy mimo přidělený rozsah, neznámé procesy a v neposlední řadě na události, kde je jako uživatel uveden Administrator (defaultní administrátorský účet, který by měl být z bezpečnostních důvodů vždy přejmenován). Z konkrétních událostí se jedná především o úspěšné i neúspěšné události pokusu o přihlášení (ID 4624 a 4625) a vytvoření nového procesu (ID 4688).

1.11 Získání pověření jiného uživatele

Nechtěným vedlejším efektem dobře nastavených zásad použití hesel, jako je jejich délka, komplexnost nebo vynucení změny hesla, bývá fakt, že si uživatelé heslo někam napíší, aby ho nezapomněli. Pak může být takové heslo poměrně snadno zneužito neoprávněnou osobou.

S tím se dá ale těžko bojovat. Pomocí událostí zabezpečení je možné například vysledovat, že se určitý uživatel přihlašuje z jiné pracovní stanice, než je obvyklé. To ale vyžaduje sledování a analýzu všech událostí přihlášení napříč sítí a znalost prostředí a chování uživatelů. Spíš než během proaktivního monitoringu si lze tuto analýzu lépe představit při vyšetřování konkrétního incidentu.

Další variantou úniku hesla je případ, kdy během zadávání přihlašovacích údajů na pracovní stanici uživatel omylem vepíše heslo do pole Username a potvrdí klávesou Enter. S právy pro čtení protokolu událostí lze sledováním bezprostředně následujících událostí odhadnout, o jakého uživatele se jedná, a snadno tak zneužít jeho přihlašovací údaje. Proto je třeba být při monitoringu událostí pozornými vůči nezvykle vypadajícím uživatelským jménům v událostech selhání přihlášení (ID 4625).

1.12 Pokus obejít auditování

V případě napadení systému se útočník s nejvyšší pravděpodobností pokusí zakrýt své stopy. Mezi metody, jak toho dosáhnout, patří změna zásady auditu, díky níž se nebudou logovat podezřelé aktivity, změna systémového času, v důsledku čehož nebude možné ze záznamu určit, kdy k daným událostem ve skutečnosti došlo, případně rovnou smazání logu.

Tyto události jsou součástí typických síťových operací a jejich výskyt není ničím ojedinělým. Je ale třeba je monitorovat a zbystřit ve chvíli, kdy původcem těchto událostí není systém, ale běžný uživatel, případně administrátor. K souvisejícím událostem patří:

- **ID 4608**:
  Start systému MS Windows – tuto událost je třeba prošetřit v případě, že došlo k neočekávanému restartu.

- **ID 4609**:
  Vypínání systému MS Windows – u kritických systémů se vypínání a restart počítačů řídí jasně definovanou politikou. Zejména pokud se tato událost objeví na serveru je nutné okamžitě zjistit, proč a jak k vypnutí či restartu počítače došlo.

- **ID 4612**:
  Z důvodu vyčerpání prostředků alokovaných pro zprávy auditu došlo

ke ztrátě některých záznamů – tato událost by se měla vygenerovat ve chvíli, kdy příliš mnoho událostí zahltí log událostí, který již není schopný zaznamenávat další události. Prevencí by měla být pravidelná kontrola logu včetně kontroly jeho velikosti a pravidelná archivace daná bezpečnostní politikou organizace. Pokud i přesto dojde k zahlcení logu, indikuje to téměř jistě provozní nebo bezpečnostní problém. Pokud k zahlcení dochází často, měly by se přehodnotit zásady auditu a nastavení velikosti logu událostí.

- **ID 1102**:
  Byl smazán audit log – událost ID 1102 je generována kdykoli je smazán security log bez ohledu na nastavení zásad auditu. Položky „Account Name“ a „Domain Name“ identifikují jméno uživatele, který log smazal. Pomocí „Logon ID“ lze tuto událost provázat s dalšími událostmi ve stejné přihlašovací relaci.

- **ID 4616**:
  Byl změněn systémový čas – tato událost zobrazí původní a nový systémový čas. V sekci „Subject“ je dále uvedeno, kdo změnu provedl, a v sekci „Process information“ pomocí jaké služby či aplikace došlo ke změně. Pokud je jako „Subject“ uveden „LOCAL SERVICE“ a jako proces svchost.exe, může být tato událost ignorována. Změna času z hlavního panelu využívá službu rundll.exe, pokud je jako „Subject“ navíc uveden běžný uživatel, měla by být tato událost prošetřena.

- **ID 4704**:
  Byla přiřazena uživatelská práva – tato událost dokumentuje přiřazení uživatelských práv mimo práv pro přihlášení (viz událost ID 4717). Jméno uživatele, kterému byla práva přidělena, nelze zjistit přímo ze záznamu této události, ale prostřednictvím Logon ID je možné ho získat z události přihlášení (ID 4624).

- **ID 4705**:
  Byla odebrána uživatelská práva.

- **ID 4719**:
  Byly změněny zásady auditu – tato událost se zaznamená vždy, kdykoli je zakázána nějaká zásada auditu bez ohledu na nastavení kategorie „Audit Policy Change“. Pokud se zásady auditu nastavily prostřednictvím „Group Policy“, nebude v položce „Subject“ uveden skutečný původce změny, ale jen počítač, na kterém změna proběhla.

- **ID 4717**:
  Byla udělena práva přístupu – tato událost informuje o udělení práv přístupu, mezi která patří:

  - povolení přístupu k počítači ze sítě,
  - povolení lokálního přihlášení,
  - povolení přihlášení přes terminálové služby,
  - přihlášení se jako dávková úloha,
  - přihlášení se jako služba.

  Stejně jako u jiných práv, která jsou definována pomocí Group Policy Objects, bývá jako uživatel uveden sám systém. Pro určení konkrétního uživatele, kterému byla práva udělena, je možné provázat tuto událost s událostí přihlášení (ID 4624) se shodným Logon ID.

- **ID 4718**:
  Účtu byla odebrána přístupová práva – odebrání určitých přístupových práv viz předchozí událost.

- **ID 4739**:
  Byla změněna doménová politika – tato událost se zaznamená pokud byla změněna zásada „Security Settings\Account Policy“ nebo „Account Lockout Policy” prostřednictvím „Local Security Policy“ nebo „Group Policy“ v „Active Directory“.

  Bohužel ani u této události není možné zjistit uživatele, který změnu provedl. Místo toho je v poli „Subject“ uveden lokální počítač, pod kterým byl příkaz gpupdate spuštěn.

1.13 Vytvoření nebo zrušení vztahu důvěry domén (AD DS trust)

Vztahy důvěry umožňují uživatelským účtům z jedné domény přistupovat k síťovým prostředkům jiné domény. Vytvoření vztahu domény nepatří zrovna k častým operacím a mělo by vždy proběhnout jen skrze jasně definovaný a schválený proces. Stejně tak přerušení vztahu důvěry by mělo být provedeno jen po důkladné analýze dopadů na současný stav sítě. Prostřednictvím zásad auditu podkategorie Authentication Policy Change (změna zásad ověřování), lze zaznamenávat následující události:

- **ID 4706**:
  Byl vytvořen nový vztah důvěry (trust) – tato událost se zaznamená, kdykoli je vytvořen nový vztah důvěry vůči aktuální doméně.

- **ID 4707**:
  Byl odstraněn vztah důvěry – tato událost je zaznamenána ve všech případech, kdy je smazán vztah důvěry s připojením k této doméně.

- **ID 4716**:
  Vztah důvěry byl modifikován – tato událost je zaznamenána ve všech případech modifikace vztahu důvěry k této připojené doméně. I když je událost označena jako „Trusted“, týká se jak vztahů důvěry, tak vztahů založených na důvěře.

1.14 Provedení neoprávněných změn zásad zabezpečení

Mezi nastavení zásad zabezpečení, které by se v rámci definovaného prostředí nemělo měnit, patří:

- Nastavení skupinových zásad:
  - Zásady hesel uživatelských účtů;
  - Zásady zamykání uživatelských účtů;
  - Zásady auditu;
  - Zásady IPSecu;
  - Zásady bezdrátové sítě;
  - Zásady veřejného klíče, především ty aplikované na EFS (Encrypting File System);
- Nastavení zabezpečení:
  - Možnosti zabezpečení;
  - Zásady hesel uživatelských účtů;
  - Přidělení uživatelských oprávnění;
- **ID 4719**:
  Byly změněny zásady auditu – tato událost se zaznamená vždy, kdykoli je zakázána nějaká zásada auditu bez ohledu na nastavení kategorie „Audit Policy Change“. Pokud se zásady auditu nastavily prostřednictvím „Group Policy“, nebude v položce „Subject“ uveden skutečný původce změny, ale jen počítač, na kterém změna proběhla.
- **ID 4714**:
  Byla změněna zásada Encrypted data recovery – tato bezpečností událost zaznamenává změny učiněné v „Settings\Public Key Policies\Encrypting File System data recovery agent“ prostřednictvím „Local Security Policy“ nebo „Group Policy“ v „Active Directory“. Bohužel ale neidentifikuje objekt, který politiku změnil, protože tato politika nebyla přímo nakonfigurována administrátory. Namísto toho je zaznamenána v objektu „Group Policy“, který se pak aplikuje na daný počítač. Z tohoto

důvodu tato událost ukazuje lokální počítač, který změnil politiku. Takovýto počítač je považován za bezpečný objekt, na kterém běží příkaz gpupdate.

Kapitola 2

Windows server 2008 R2 Advanced Audit

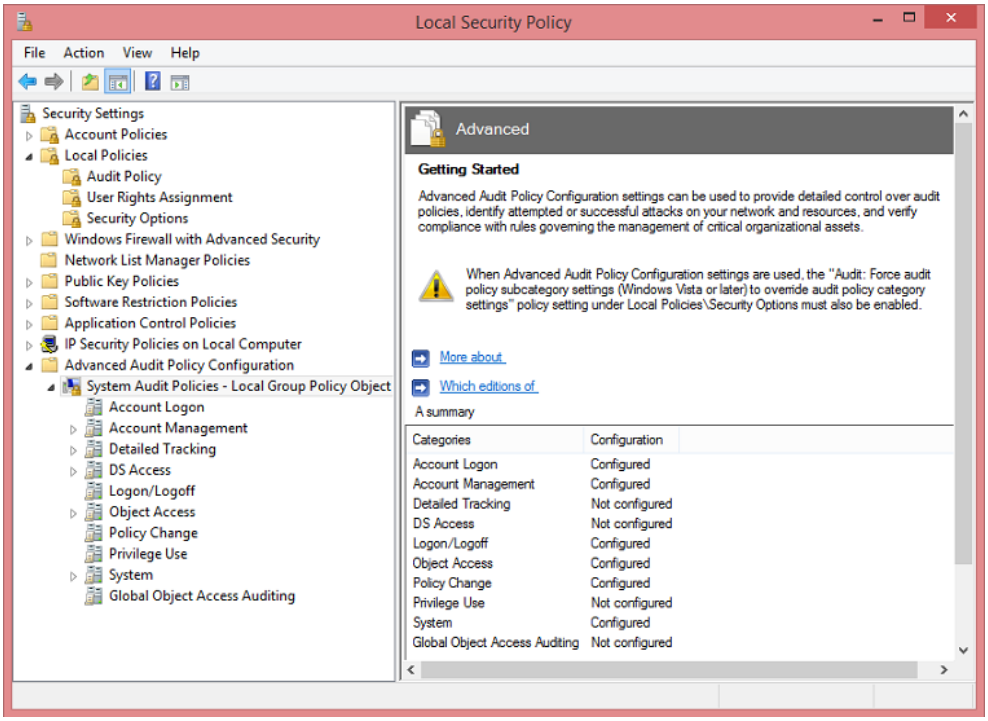
Windows server 2008 R2 je serverový operační systém vydaný v roce 2009 společností Microsoft. Je postaven na Windows NT 6.1, který používá i klientský operační systém Windows 7, proto je doporučeno, aby v doméně postavené na OS Windows 2008 R2 byly použity klientské stanice s OS Windows 7.

Od verze operačního systému Windows Server 2008 přišel Microsoft s novinkou rozšířeného nastavení auditu, která s sebou přinesla 53 podkategorií umožňující detailnější selekci výběru auditovaných událostí. Navíc přibyla nová kategorie auditu, Global Object Access Auditing, která umožňuje definovat na celý počítač SACL (Security Access Control List). Ten se aplikuje buď na celý souborový systém, nebo na celý registr Windows. Výhodou je, že není nutné specifikovat jednotlivé složky, soubory a cesty ale automaticky je sledováno vše, na co je politika SACL aplikovaná.

Tyto nové zásady auditování, tzv. Advanced Auditing, přibyly k původním zásadám auditu s 9 základními kategoriemi nastavení. U verze Windows server 2008 bylo ale možné spravovat tyto rozšířené zásady auditu pouze pomocí nástroje auditpol.exe v příkazové řádce. Možnost konfigurovat auditování na úrovni podkategorií pomocí Group Policy se objevila právě u Windows serveru 2008 R2.

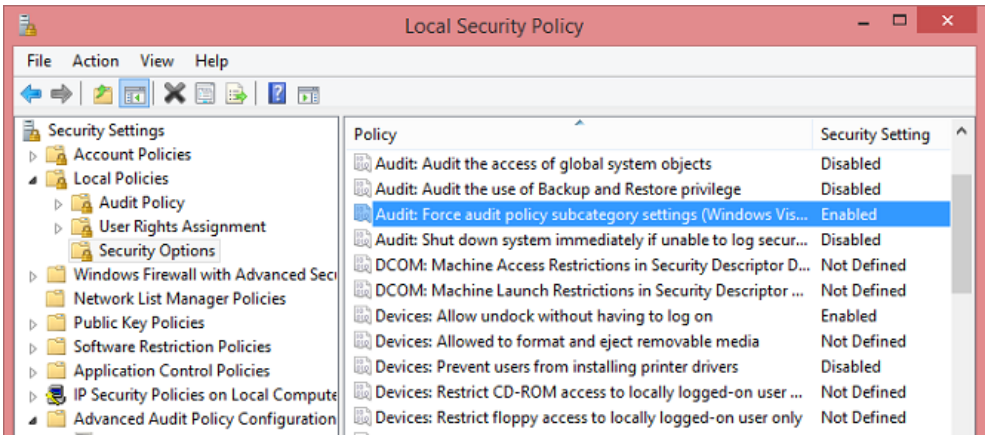
Rozšířené zásady auditu jsou dostupné buď prostřednictvím Group Policy pod „**Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies**“ , nebo prostřednictvím Local Security Policy pod „**Security Settings\ Advanced Audit Policy Configuration\System Audit Policies**“

Zásady skupin se používají při nastavení zásad auditování pro celou lokalitu, doménu, nebo organizační jednotku, zatímco místní zásady zabezpečení se týkají jednotlivých pracovních serverů nebo stanic a lze je přepsat pomocí zásad skupiny. V případě, že dojde ke konfliktu mezi základními a rozšířenými zásadami auditu, vyhrají defaultně nastavení základních zá-



Obrázek 2.1: Local Security Policy – Advanced Audit Policy Configuration

sad auditu. Aby se vynutilo nastavení podkategorií v rámci Advanced Audit Policy, je třeba, aby se v možnostech Security Options dostupnými pod **„\Security Settings\Local Policices\Security Option“** povolila zásada **Audit: Force audit policy subcategory settings**.



Obrázek 2.2: Security Options – Audit: Force audit policy subcategory settings

V následujících podkapitolách jsou popsány jednotlivé kategorie a podka-

tegorie zásad Advanced Auditu.

2.1 Audit account logon events

Tato politika určuje, zda se bude auditovat každá instance přihlášení či odhlášení uživatele. Ověření doménového účtu uživatele generuje události přihlášení do logu zabezpečení (security log) na doménovém řadiči, který provedl ověření. Ověření lokálního účtu uživatele generuje události přihlášení do logu zabezpečení přímo na pracovní stanici.

Ověření pověření nemá odpovídající událost odhlášení pro události přihlášení k účtu jako je tomu u událostí přihlášení. Vzhledem k tomu, že událost přihlášení k účtu může být zaznamenána na libovolném platném řadiči v doméně, měly by být za účelem analýzy událostí přihlášení k účtu v doméně sloučeny protokoly událostí zabezpečení ze všech řadičů v doméně.[3]

2.1.1 Credential Validation

Tato podkategorie zaznamenává informace o výsledcích ověření oprávnění vystavených na základě žádosti o přihlášení uživatelského účtu. K těmto událostem dochází na serveru, který je k tomuto autoritativně pověřen. Zatímco pro doménové účty je autoritativně pověřen doménový řadič, pro místní účty je touto rolí pověřen lokální počítač. V doménovém prostředí se většina událostí přihlášení k účtu objevuje v logu zabezpečení autoritativních doménových řadičů.

Doporučení: nastavit auditování pouze typu „Failure“ z důvodu odhalení případných chyb v autentizaci. Nastavením „Success“ by se dosáhlo velkého objemu událostí s minimální užitnou hodnotou.[4]

2.1.2 Kerberos Authentication Service

Kerberos je autentizační protokol zajišťující vzájemné bezpečné ověření identity komunikujících subjektů v nezabezpečené síti. Tato podkategorie podává informace generované autentizačním serverem Kerberos a tím umožňuje monitorovat stav a potenciální hrozby služby Kerberos. Události ověřování protokolu Kerberos se zaznamenávají na počítači, který je autoritativní poskytovat oprávnění.

Níže jsou popsány vybrané události této podkategorie:

- ID 4768: Byl obdržen autentizační TGT tiket. Tato událost je logována jen na doménových řadičích a jsou logovány oba případy, tedy jak úspěšné instance, tak i neúspěšné. Na začátku dne, kdy si uživatel sedne ke své pracovní stanici a zadá své přihlašovací údaje (tzv. uživatelské jméno a heslo) do domény, stanice kontaktuje lokální DC a vyžádá si TGT. Když jsou přihlašovací údaje správné a uživatelský účet projde

úspěšně procesem, DC udělí TGT klíč a zaloguje událost s ID 4768 o vydání ověřeného tiketu. Uživatelské pole pro tuto událost (a všechny další události týkajících se auditování v kategorii „Audit account logon“) však neposkytuje informace o identitě uživatele, toto pole se vždy čte jako N/A „Not Available”. Informace o identitě jsou uvedeny v informacích o účtu. Pole, které přímo identifikuje uživatele, který se přihlásil, obsahuje i DNS příponu uživatelského účtu (tzv. DNS suffix). Pole ID uživatele obsahuje SID daného účtu. Windows loguje i další instance události ID 4768 v případě, když se počítač umístěný v doméně, potřebuje být ověřen od DC např. při restartu serveru nebo při zavádění systému.[5]

- ID 4771: Kerberos preautentizace selhala. Během preautentizace ověří doménový řadič uživatelské jméno a heslo s následným vydáním autentizačního tiketu. Pokud ověření selže, vygeneruje se na doménovém řadiči tato událost a TGT nebude udělen. Pomocí chybového kódu lze zjistit důvod selhání preautentizace. Stejně jako u předchozí události nelze zjistit identitu uživatele z položky User, která je vždy N/A, ale až z informací pod Account Information.[6]

Doporučení: dle doporučení Microsoftu je vhodné nastavit auditování této podkategorie na „Success“ i „Failure“ na doménových řadičích.

2.1.3 Kerberos Service Ticket Operations

Události této podkategorie podávají informace o procesech týkajících se žádostí o Kerberos tiket. Tyto události jsou generovány protokolem Kerberos na DC, který je autoritou pro doménový účet. K událostem této podkategorie patří:

- 4769: A Kerberos service ticket was requested. Windows užívá tuto událost pro oba případy žádostí, jak pro úspěšné, tak pro neúspěšné výsledky. Typ událostí je označen svým kódem, který je možně vyhledat v technické dokumentaci a dekódovat jeho význam. Zatímco událost ID 4768 umožňuje sledovat inicializaci přihlášení pomocí udělování TGT klíčů, událost ID 4769 umožňuje sledovat udělení servisních tiketů. Servisní tikety jsou vždy vyžádány pokaždé, když uživatel nebo počítač přistupuje k serveru na síti. Např. když si uživatel namapuje jednotku na souborovém serveru, jeho žádost o servisní tiket vygeneruje log události ID 4769 na DC.

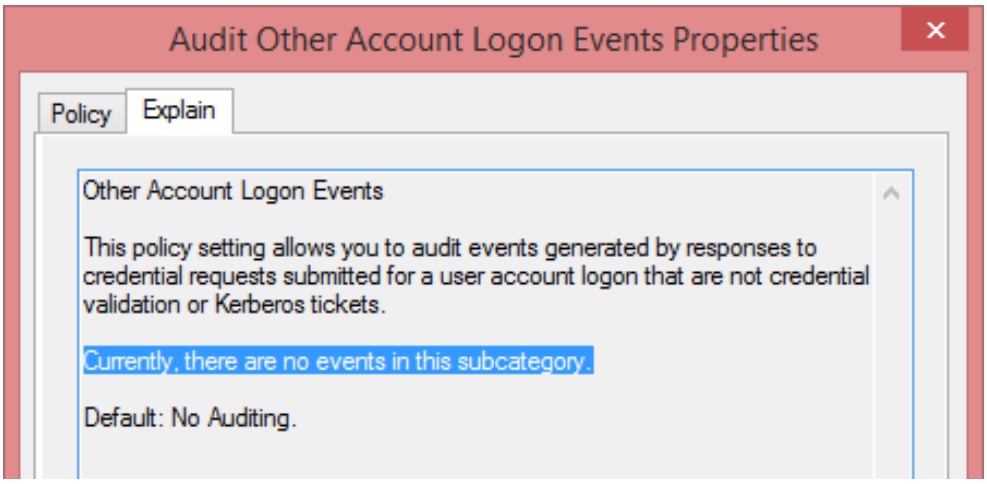
- 4770: A Kerberos service ticket was renewed. Protokol Kerberos limituje platnost tiketu. Když daný limit tiketu expiruje ale uživatel je stále přihlášený, Windows automaticky kontaktuje DC, aby obnovil tiket, který spustil příslušnou událost.[5]

Doporučení: auditovat události typu „Failure“ jen na DC. Celkově je objem generovaných událostí malý a proto by případné povolení auditování úspěšných událostí nemělo příliš vliv na velikost protokolu zabezpečení.

2.1.4 Other Account Logon Events

Toto nastavení zásad by mělo být použito ke sledování množství různých síťových aktivit, včetně pokusů o připojení ke vzdálené ploše, síťových připojení, bezdrátových připojení, atd. Tato podskupina zaznamenává události, které se vyskytují v reakci na pověření předložených k žádosti o přihlášení uživatelského účtu, které se nevztahují k ověření pověření nebo Kerberos tiketům.

Poznámka: popis této podkategorie není na webu Microsoftu korektní (konkrétně: `https://technet.microsoft.com/en-us/library/dd772704(v=ws.10).aspx`). Události, které jsou uvedeny u této podkategorie, patří ve skutečnosti pod kategorii auditu „Logon/Logof“ – „Other Logon/Logoff Events“. Dle popisu přímo v záložce „Explain“ neobsahuje tato podkategorie momentálně žádné události a je určena pro budoucí použití.



Obrázek 2.3: Doporučení: ponechat v defaultním nastavení, což je „No Auditing“

2.2 Audit account management

Nastavení této politiky určuje, zda se má auditovat každá událost správy účtu, jakou je vytvoření, změna, zrušení, přejmenování, zablokování či odblokování uživatelského účtu, nastavení nebo změna hesla, vytvoření, změna nebo zrušení skupiny apod. Na první pohled by se mohlo zdát, že do této kategorie

patří i změna uživatelských práv, není tomu ale tak. Události změny uživatelských práv spadají pod kategorii Změny zásad. V rámci organizace by měly být určeny osoby pověřené správou doménových i lokálních účtů. Díky auditování úspěšných událostí je pak možné kontrolovat, zda tyto události správy účtů souhlasí s oficiálními požadavky. Pokud dojde k neoprávněným změnám v uživatelských účtech, může se jednat o nerespektování bezpečnostní politiky organizace administrátorem, nebo také o úmyslný útok. Neúspěšné události zase svědčí o pokusu neautorizované osoby o provedení změny v uživatelských účtech, nebo účtech skupin, a měly by být prošetřeny.

2.2.1 Application Group Management

Pod touto podkategorií jsou generovány všechny úspěšné události týkající se správy skupin aplikací, jako je vytvoření, změna, zrušení skupiny aplikací, přidání nebo odebrání aplikace ze skupiny. Skupiny aplikací jsou součástí řízení přístupu aplikací pod OS Windows a jsou spravovány pomocí nástroje Správce autorizací, který je snap-in modulem MMC konzole. Nejsou zde generovány žádné neúspěšné události, tedy v případě nastavení auditování by mělo smysl nastavit jen možnost „Success“. Množství událostí je nízké.[7]
Doporučení: ponechat v defaultním nastavení, tedy bez auditování.

2.2.2 Computer Account Management

Touto politikou se nastaví auditování událostí správy účtů počítače, které zahrnují, vytvoření, změnu či odstranění účtu počítače. Tyto události jsou generovány pouze na řadiči domény a jsou pouze typu „Success“. Defaultně není tato podkategorie nakonfigurována. Množství generovaných událostí je nízké.[8]
Doporučení: nastavit auditování úspěšných událostí na DC.

2.2.3 Distribution Group Management

Nastavením této podkategorie se budou auditovat všechny události týkající se správy distribučních skupin, jako např. vytvoření, změna, zrušení distribuční skupiny, přidání nebo odstranění člena z distribuční skupiny. Počet generovaných událostí je poměrně nízký. Všechny události správy distribučních skupin jsou pouze typu „Success“.[9]
Doporučení: nastavit auditování úspěšných událostí na DC.

2.2.4 Other Account Management Events

Tato podkategorie není defaultně nastavená. Pokud se nastaví, generuje velmi málo událostí, které jsou pouze typu „Success“. Za povšimnutí stojí následující událost ID 4782: Byl zpřístupněn hash hesla. Tato událost je typicky

vygenerovaná během přesunu dat obsahující informace o heslech pomocí nástroje Active Directory Migration Tool.[10]
Doporučení: nastavit auditování úspěšných událostí.

2.2.5 Security Group Management

Tato podkategorie zaznamenává všechny události týkající se správy skupin zabezpečení, jako např. vytvoření, změna, zrušení skupiny zabezpečení, přidání nebo odstranění člena ze skupiny zabezpečení. Počet generovaných událostí je poměrně nízký. Všechny události správy skupin zabezpečení jsou pouze typu Success. Jak již bylo psáno v kapitole „Detekce porušení bezpečnostních zásad – Umístění uživatele do skupiny“, je doporučeno povolit auditování úspěšných událostí této podkategorie z důvodu potřeby kontroly nad všemi operacemi týkající se skupin zabezpečení.[11]
Doporučení: nastavit auditování úspěšných událostí na všech DC.

2.2.6 User Account Management

Tato podkategorie zaznamenává všechny události týkající se správy uživatelských účtů, jako je vytvoření, změna, přejmenování, odstranění, povolení, či zakázání účtu, změna či nastavení hesla a další. Všechny tyto události je důležité monitorovat, viz kapitola „Detekce porušení bezpečnostních zásad – Vytvoření, změna nebo odstranění uživatelského účtu“. Kromě události ID 4766 (selhání pokusu o přidání SID historie), která je typu „Failure“, jsou všechny události správy účtů typu „Success“.[12]
Doporučení: nastavit „Failure“ na všech serverech. „Success“ nastavit jen na DC.

2.3 Audit directory service access

Tato politika definuje, zda se bude auditovat přístup a změny provedené v Active Directory. Lze takto například sledovat změny v účtech uživatelů, počítačů a skupin, ale také změny schématu AD a další události AD, jako např. replikace. Samotné nastavení těchto zásad ale pro účely auditování objektů nestačí. Aby se mohly zaznamenávat události této kategorie, je třeba, aby byly na jednotlivých objektech správně definované příslušné systémové přístupové seznamy, tzv. SACL (System Access Control List). Pomocí SACL je možné nastavit, zda se budou auditovat úspěšné a/nebo neúspěšné pokusy o přístup k objektu, případně zda neauditovat vůbec žádné události. Neuváženým použitím této kategorie je velmi snadné zahltit log zabezpečení na řadiči domény. Proto je zde obzvlášť důležité provést důkladnou analýzu a následně nastavit prostřednictvím SACL auditování pouze na těch objektech, u kterých je vyžadován monitoring. Určité informace je ale možné získat i prostřednic-

tvím auditování kategorie správy účtů, proto není od věci rozmyslet se, zda by ke stejnému účelu nepostačila ona.

2.3.1 Detailed Directory Service Replication

Tato podkategorie podává detailní informace související s replikací dat mezi doménovými řadiči. Množství těchto událostí může být vysoké a jejich přínos je spíše při řešení potíží provozního charakteru. Zaznamenávají se pouze na DC.[13] **Doporučení:** nastavit „No Auditing“.

2.3.2 Directory Service Access

Tato podkategorie zaznamenává události přístupu k objektům AD DS. Aby byl tento přístup auditován, je potřeba nastavit auditování i prostřednictvím SACL na konkrétních objektech. Tyto události se zaznamenávají pouze na serverech, na nichž běží služba AD DS. Jsou pouze typu „Success“. Množství generovaných dat může velmi vysoké v závislosti na nastavení SACL.[14]
Doporučení: nastavit „Success“ na DC. Zároveň je ale třeba věnovat čas důkladnému nastavení SACL, aby se auditoval přístup jen k objektům zájmu.

2.3.3 Directory Service Changes

Tato podkategorie zásad auditu zaznamenává události o změnách na objektech v AD DS, k nimž patří vytvoření, změna, přesun nebo odstranění objektu. V případě změny objektu podává událost informace o původní i nové změněné hodnotě. Auditování se uplatňuje ale jen na objektech, které mají definované auditování příslušných operací ve svých SACL. Zásady Directory Service Changes se aplikují jen na doménových řadičích. Všechny události jsou typu „Success“.[15]
Doporučení: nastavit „Success“ na DC. Zároveň je ale třeba věnovat čas důkladnému nastavení SACL, aby se auditoval přístup jen k objektům zájmu.

2.3.4 Directory Service Replication

Události této podkategorie zaznamenávají informace o zahájení a ukončení replikace mezi doménovými řadiči, což jsou údaje, které by se mohly přijít vhod. Tyto události jsou pouze typu „Success“. Generují se v relativně malém množství.[16]
Doporučení: nastavit „Success“ na všech DC.

2.4 Audit logon events

Události přihlášení se zaznamenávají při každém přihlášení a odhlášení účtů, a to na počítači, na kterém k pokusu o přihlášení došlo. V případě přihlášení

k vzdálenému počítači se událost zaznamená právě do jeho logu zabezpečení. Rozdíl mezi událostmi přihlášení a událostmi přihlášení k účtu je ten, že události přihlášení vznikají na tom počítači, kde se účet bude používat, a to vždy při vzniku a zániku přihlašovací relace, kdežto události přihlášení k účtu vznikají na počítači nebo serveru, který účet ověřil.[17]

2.4.1 Account Lockout

Podkategorie Account Lockout zaznamenává události uzamčení uživatelského účtu z důvodu opakovaně neúspěšných pokusů o přihlášení. Množství těchto událostí není příliš vysoké a je užitečné jak z provozních, tak z bezpečnostních důvodů za účelem možné detekce útoku. Dle dokumentace spadá do této podkategorie jediná událost, a to ID 4625 – selhání přihlášení k účtu. Navzdory tomu, že je tato událost pouze typu „Failure“, tvrdí dokumentace, že v defaultním nastavení je zapnuto auditování „Success“ událostí, což celkem postrádá smysl.[18]
Doporučení: nastavit „Failure“ na všech serverech a počítačích v síti.

2.4.2 Audit IPSec subcategory

Jedná se o 3 podkategorie týkající se auditování protokolu IPSec:

- Extended Mode – rozšířený režim protokolu IPSec.
- IPsec Main Mode – hlavní režim protokolu IPSec.
- IPsec Quick Mode – rychlý režim protokolu IPSec.

Tyto podkategorie jsou užitečné především pro řešení problémů s protokolem IPsec. Generují velké množství událostí.
Doporučení: dle Microsoftu ponechat bez auditování, případně dočasně povolit auditování úspěšných i neúspěšných událostí pro účely troubleshootingu. [19]

2.4.3 Logoff

Tato podkategorie zaznamenává události odhlášení od systému do logu zabezpečení na tom počítači, na kterém k odhlášení došlo. Při síťovém přihlášení se tedy tyto události zapíší do logu zabezpečení na vzdáleném počítači. V případě interaktivního nebo vzdáleného odhlášení se zaznamená událost ID 4647 – uživatel inicioval odhlášení. Pokud ale uživatel například vypne počítač, systém nestihne před vypnutím zaznamenat událost odhlášení a až po opětovném startu systému vygeneruje událost ID 4634 – účet byl odhlášen. Z toho důvodu bývá čas události odhlášení odlišný od skutečného odhlášení. Pomocí Logon ID lze události odhlášení navázat na odpovídající událost přihlášení a vymezit tak relaci přihlášení daného uživatele. Události této podkategorie jsou pouze

typu „Success“.[20]
Doporučení: nastavit auditování „Success“ událostí na všech serverech i počítačích v síti.

2.4.4 Logon

Podkategorie „Logon“ zaznamenává pokusy o přihlášení k systému. Tyto události se vyskytují na počítači, na kterém byl proveden pokus o přihlášení. V případě síťového připojení budou tedy zaznamenány na vzdáleném počítači, ke kterému se uživatel pokusil přihlásit. Úspěšné události poskytují záznam o tom kdy a na jakém počítači se uživatel přihlásil (ID 4624), což v případě vyšetřování bezpečnostního incidentu může být zásadní důkazní materiál. Prostřednictvím identifikátoru relace přihlášení (Logon ID) lze dále zjistit, jaké operace byly daným účtem v dané relaci přihlášení provedeny. Množství neúspěšných událostí pokusu o přihlášení v řadě (ID 4625) může zase signalizovat pokus o prolomení hesla. Další z podkategorie přihlášení je událost ID 4648 – byl proveden pokus o přihlášení prostřednictvím explicitních pověření. Jedná se o případ, kdy uživatel použije jiná pověření. Typickým příkladem je spuštění příkazu prostřednictvím volby „Run as“, nejčastěji jako „Run as administrator“. Doporučení: Z výše uvedených důvodů by auditování této podkategorie mělo být nastaveno na „Success“ i „Failure“ na všech serverech i počítačích v síti.

2.4.5 Network Policy Server

Network Policy Server (NPS) slouží k vytváření a vynucení zásad přístupu k síti, správě ověření a autorizací přístupu k síti a správě zásad stavů klienta. NPS lze nakonfigurovat jako RADIUS server, RADIUS proxy, Network Access Protection (NAP) policy server nebo libovolnou kombinaci předchozích funkcí. Auditováním této podkategorie lze monitorovat události Network Policy Serveru jako jsou například poskytnutí nebo odmítnutí přístupu uživatele, uzamknutí nebo odemknutí uživatelského účtu apod.[21] Doporučení: zapnout „Success“ i „Failure“ události pro NPS servery. Pro ostatní nastavit „No Auditing“.

2.4.6 Other Logon/Logoff Events

Tato podkategorie zaznamenává události, jakými jsou například uzamknutí nebo odemknutí pracovní stanice, spuštění nebo ukončení spořiče obrazovky, připojení či odpojení terminálových služeb, požadavky na autentizaci k drátové i bezdrátové síti a další. Z hlediska bezpečnosti je zajímavá událost ID 4649 – byl detekován replay attack. Standardně je množství generovaných událostí spíš nízké. Na terminálových serverech může být množství událostí vyšší.[22]
Doporučení: nastavit „Success“ i „Failure“.

2.4.7 Special Logon

Pokud je tato skupina nastavená pro auditování, zaznamenají se události, kdy je buď použit „Special logon“, nebo kdy se přihlásil člen skupiny „Special Group“. Special logon je přihlášení, které má oprávnění ekvivalentní k administrátorským oprávněním. Special Group je vlastnost OS Windows, která umožňuje administrátorům nastavit seznam identifikátorů zabezpečení (SID) do registru. Pokud je některý z těchto SIDů použit při procesu přihlášení a zároveň je zapnutá podkategorie zásad auditu „Special Logon“, zaznamená se událost do logu zabezpečení. Události této podkategorie jsou jen typu „Success“. Množství těchto událostí není vysoké.[23]
Doporučení: nastavit pouze „Success“ na všech serverech i PC.

2.5 Audit object access

Toto bezpečnostní nastavení určuje, zdali OS bude auditovat uživatele pokoušejícího se přistupovat objektům, které nejsou v AD. Auditní záznamy jsou generovány pouze pro objekty, které jsou specifikovány v SACL a to pouze v případě, že typ žádosti o přístup (číst, psát nebo modifikovat) je v souladu s účtem žádajícím o přístup a přitom odpovídá nastavení SACL. Nastavení SACL je možné učinit přes bezpečnostní nastavení v dialogovém okně ve vlastnostech objektu. Definuje jaká operace a kým provedená se má logovat, případně že se nemá vůbec logovat. Jestliže je povolen audit úspěšných událostí, je auditní záznam generovaný pokaždé, když některý z účtů úspěšně přistoupí k non-AD objektu. Jestliže je povolen záznam neúspěšných událostí, je auditní záznam generovaný pokaždé, když některý z účtů neúspěšně žádá o přístup k non-AD objektu. V obou případech platí, že dané objekty musí mít definováno auditování v SACL, a to jak operace, které se mají auditovat, tak uživatele, kteří tyto operace provádějí.

2.5.1 Application Generated (generování aplikace)

Tato podkategorie zaznamenává události v případech, kdy některé aplikace přistupují k MS Windows Auditing API. Tyto aplikace využívají tuto podkategorii pro logování vlastních událostí, přičemž úroveň, množství nebo důležitost se odvíjí od konkrétní aplikace.[24]
Doporučení: ponechat v defaultním nastavení, tj. „No Auditing“.

2.5.2 Certification Services (certifikační služby)

Tato podkategorie podává zprávu o operacích certifikační služby, je-li služba v systému povolena.[25]
Doporučení: ponechat v defaultním nastavení, tj. „No Auditing“.

2.5.3 Detailed File Share

Toto nastavení zásad dovoluje auditovat pokusy o přístup ke sdíleným souborům a složkám. Pokud je nastaveno auditování, vytváří se logy pokaždé, když je soubor nebo složka zpřístupněna. Naopak nastavení auditování sdílených souborů (tzv. File Share) vytváří logy jen jednou, a to v případě, když se vytvoří spojení mezi klientem a sdíleným souborem. Pro sdílené složky se nedefinuje SACL. Pokud je zásada povolena, logují se veškeré přístupy ke všem sdíleným složkám a souborům v systému. To má za následek ohromný objem událostí.
Doporučení: ponechat v defaultním nastavení, tj. „No Auditing“. Velký objem událostí bez možnosti specifikovat objekty prostřednictvím SACL by mohl rychle zaplnit log.

2.5.4 File Share

Pokud je nastaveno auditování podkategorie File Share, zaznamenávají se události vždy, když se vytvoří spojení mezi klientem a sdíleným souborem. Pro sdílené složky se nedefinuje SACL. Pokud je zásada povolena, logují se veškeré přístupy ke všem sdíleným složkám a souborům v systému. To má za následek ohromný objem událostí.[26]
Doporučení: ponechat v defaultním nastavení, tj. „No Auditing“. Velký objem událostí bez možnosti specifikovat objekty prostřednictvím SACL by mohl rychle zaplnit log.

2.5.5 File System

Tato podkategorie zaznamenává události v případě, když jsou zpřístupněny objekty v systému souborů. Auditní záznamy jsou generovány pouze pro objekty v systému souborů, které mají definované auditování v SACL a jen v případě, jsou-li použitá přístupová práva v souladu s těmi nastavenými v příslušném SACL.
Doporučení: nastavit auditování „Success“ i „Failure“ událostí, ale jen v případě, že je předem věnován dostatečný čas důkladné analýze a je jasně stanoveno, jaké soubory či složky mají auditování podléhat. Na těchto objektech je pak třeba definovat odpovídající SACL.

2.5.6 Filtering Platform Connection

Pokud je povolená tato podkategorie, jsou generovány události vždy při povolení nebo blokování spojení, nebo naslouchání aplikace či služby prostřednictvím WFP (Windows Filtering Platform). Objem těchto událostí je vysoký.[27]
Doporučení: ponechat v defaultním nastavení, tj. „No Auditing“.

2.5.7 Filtering Platform Packet Drop

Tato podkategorie podává zprávu v případě, že WFP (tzv. Windows Filtering Platform) pakety zahodí. Tyto události mohou opět dosahovat velkých objemů.
Doporučení: ponechat v defaultním nastavení, tj. „No Auditing“.

2.5.8 Handle Manipulation

Tato podkategorie zaznamenává události, kdy je vyžádán nebo ukončen handle objektu. Tyto události se generují pouze u objektů, u nichž je povoleno auditování v odpovídající podkategorii v rámci zásad Audit Object Access, a to jen v případech, kdy provedené operace odpovídají nastavení auditování v SACL. Pokud je povoleno auditování, generuje velké množství dat (v závislosti na nastavení SACL).[28]
Doporučení: ponechat v defaultním nastavení, tj. „No Auditing“.

2.5.9 Kernel Object

Toto nastavení zásad umožňuje auditovat pokusy o přístup k jádru systému. Stejně jako v ostatních případech kategorie Audit Object Access je třeba, aby objekty jádra měly povoleno auditování v SACL.[29]
Doporučení: ponechat v defaultním nastavení, tj. „No Auditing“.

2.5.10 Other Object Access Events

Tato podkategorie zahrnuje další události přístupu k objektům. Předmětem zájmu by měly být zejména události týkající se naplánovaných úloh, tedy jejich vytvoření, změna, zákaz či aktualizace. K dalším událostem patří přidání, modifikace, nebo odebrání objektu z COM+ katalogu a jiné. Tyto události jsou pouze typu „Success“. Množství generovaných záznamů je nízké.[30]
Doporučení: nastavit „Success“ na všech serverech i koncových PC.

2.5.11 Registry

Tato podkategorie zaznamenává události přístupu k registru. Auditní záznamy jsou generovány jen pro objekty registru s definovaným SACL, a to jen v případech, kdy provedené operace odpovídají nastavení auditování v SACL. Všechny události jsou typu „Success“.[31]
Doporučení: po pečlivé rozvaze, jaké registry by bylo vhodné monitorovat a následné definici auditování prostřednictvím SACL, nastavit u této podkategorie auditování úspěšných událostí. V opačném případě ponechat v defaultním nastavení, tj. „No Auditing“.

2.5.12 SAM

Nastavení této politiky umožňuje auditovat jak úspěšné, tak neúspěšné události pokusu o přistup k SAM objektům (tzv. „Security Accounts Manager“). SAM, neboli Správce zabezpečení účtů, je databáze, ve které jsou uloženy místní uživatelské účty a skupiny. SAM spravuje zabezpečení těchto účtů. Toto se týká především členských serverů a pracovních stanic.U doménový řadičů, které bývají omezeny pouze na přihlášení správce, má SAM pouze informativní roli pro ostatní služby.[32] Na doménových řadičích je počet generovaných událostí poměrně vysoký.[33]
Doporučení: zapnout auditování „Success“ a „Failure“ událostí na členských serverech.

2.6 Audit Policy Change

Tato politika určuje, zda se bude auditovat každá změna přiřazení uživatelských práv, nastavení Windows Firewallu, zásady důvěryhodnosti nebo změny samotné politiky auditu. Z hlediska bezpečnosti má tato kategorie velký význam. Pokud se například útočník pokusí povýšit svá práva, je to právě kategorie Audit Policy Change, která může toto jednání prokázat.[34]

2.6.1 Audit Policy Change

Tato podkategorie zaznamenává všechny změny provedené v zásadách auditu včetně změn v SACL. V případě konfigurace zásad auditu prostřednictvím Group Policy, není nutné zapínat auditování této kategorie na serverech, které nejsou doménovými řadiči.[35] K dalším událostem patří modifikace tabulky přihlášení „Special group“ skupiny, změna hodnoty CrashOnAuditFail, provedení změny v registraci zdroje událostí. Tato podkategorie nemá žádné „Failure události“.[36]
Doporučení: nastavit „Success“.

2.6.2 Authentication Policy Change

Auditování podkategorie Authentication Policy Change zahrnuje události vytváření, modifikace či zrušení vztahů důvěryhodnosti mezi doménami, změny doménové politiky, nebo změny zásad protokolu Kerberos.[37]
Doporučení: nastavit „Success“.

2.6.3 Authorization Policy Change

Podkategorie Authorization Policy Change zaznamenává udílosti přidělení nebo odebrání uživatelských práv, změnu zásad EFS (Encrypting File Systém), vytvoření nebo zrušení vztahu důvěry mezi doménami. Pokud je auditování této podkategorie povoleno, generuje málo událostí. Všechny události

jsou pouze typu „Success“.[38]
Doporučení: nastavit „Success“.

2.6.4 Filtering Platform Policy Change (změna zásad architektury Filtering Platform)

Windows Filtering Platform poskytuje prostředí pro filtrování a kontrolu TCP/IP paketů, monitoring připojení, zpracování dat protokolem IPSec a RPC filtrování. Tato podkategorie tedy umožňuje auditování souvisejících událostí, jako jsou informace o stavu a změnách nastavení IPsec apod. Množství událostí se udává jako nižší.[39]
Doporučení: Defaultní nastavení je „No Auditing“. Microsoft u této podkategorie nepředkládá žádné doporučení.

2.6.5 MPSSVC Rule-Level Policy Change

Tato politika umožňuje auditovat změny zásad pravidel služby MPSSVC (Microsoft Protection Service), která je využívána Windows Firewallem. Tyto události zahrnují změny pravidel, nastavení Windows Firewallu, oznámení o tom, že nějaká pravidla byla ignorována, nebo nebyla aplikována, nebo změny v Group Policy aplikované na Windows Firewall.[40]
Doporučení: vzhledem k nízkému množství událostí a důležité roli Windows Firewallu je vhodné nastavit auditování úspěšných i neúspěšných událostí.

2.6.6 Other Policy Change Events

Tato podkategorie zaznamenává události související se změnami nastavení TPM (Trusted Platform Module) modulu a operacemi šifrování. Množství generovaných událostí je nízké.
Doporučení: Defaultní nastavení je „No Auditing“. Pro účely případného odhalení HW a SW chyb by mohlo být nastaveno auditování „Failure“ událostí, které vzhledem ke svému malému množství nijak neovlivní chod systému či velikost logu.

2.7 Audit Privilege Use

Tato politika definuje, zda se budou auditovat události, kdy uživatelé nebo služby použijí pro nějaké úkony uživatelská práva. Defaultně není tato politika nastavená. Pokud se nastaví, generuje ohromné množství událostí. Úspěšné události se zaznamenávají při každém úspěšném použití uživatelských práv, což je možné považovat za standardní stav, a proto by mohly být ponechány bez auditování. Oproti tomu neúspěšné události mohou značit problémy v síti nebo také pokus o prolomení bezpečnosti systému a proto by měly být monitorovány.

2.7.1 Non Sensitive Privilege Use

Tato podkategorie zahrnuje události použití práv, která nepatří mezi citlivá. Jako příklad lze uvést právo přidat pracovní stanici do domény, právo upravit paměťové kvóty pro proces, právo povolit či odepřít lokální přihlášení, přihlášení prostřednictvím terminálové služby či jako dávkový soubor nebo služba apod., právo obejít křížovou kontrolu, změnit systémový čas, vytvořit globální objekt, vypnout systém či vynutit vypnutí ze vzdáleného systému, právo zvýšit plánovací prioritu, právo synchronizovat data adresářové služby a jiné. Pokud je tato podkategorie zapnutá, generuje ohromné množství událostí.[41]
Doporučení: Ponechat v defaultním nastavení, tedy „No Auditing“.

2.7.2 Sensitive Privilege Use (použití citlivých oprávnění)

Tato podkategorie generuje události, pokud dojde k použití citlivých práv. Mezi ně patří například právo jednat jako část operačního systému, právo zálohovat nebo obnovit soubory a adresáře, právo vytvořit objekt tokenu, ladit programy, povolit počítačům a uživatelským účtům právo pro delegování, upravit hodnoty proměnných systému, právo spravovat log zabezpečení, právo převzít vlastnictví souboru nebo jiných objektů a další. Tyto události mohou být teoreticky užitečné při vyšetřování bezpečnostního incidentu, ale jejich množství je tak vysoké, že převažuje tento potenciální přínos.[42]
Doporučení: Ponechat v defaultním nastavení, tedy „No Auditing“.

2.7.3 Other Privilege Use

Tato podkategorie je určená pro budoucí použití. Negeneruje žádné události, nemá tedy smysl ji povolovat.
Doporučení: Ponechat v defaultním nastavení, tedy „No Auditing“.

2.7.4 Audit the use of Backup and Restore privilege

Tato zásada spadá pod zásady Security Settings\Local Policices\Security Option. Není tedy přímo součástí nastavení Advanced Auditu, ale svým způsobem se váže na kategorii auditování oprávněného použití. Pokud jsou zapnuty obě kategorie, auditují se všechny události oprávněného použití včetně zálohování a obnovy dat. Naopak, pokud je auditování oprávněného použití vypnuto, nevygeneruje se při zálohování nebo obnově souboru jediná událost i přesto, že bude tato kategorie zapnuta pro auditování. V případě, že je povoleno auditování v rámci obou kategorií, může obrovské množství generovaných událostí rychle zaplnit log zabezpečení.
Doporučení: nastavit tuto zásadu na „Disabled“.

2.8 Audit Detailed Tracking

Zapnutím auditování sledování procesů získáme podrobné logování událostí, jako jsou vytvoření a ukončení procesů, nepřímý přístup k objektům nebo zdvojení popisovače. Množství generovaných událostí je ale velmi vysoké, a ačkoli mohou být určité informace poměrně přínosné, je lepší ponechat tuto kategorii v defaultním nastavení, což je No Auditing. Auditování je užitečné povolit v případě řešení provozních problémů, ale mělo by se jednat spíš o dočasnou záležitost. Výjimkou by mohly být události vytvoření procesu, které jsou užitečné z hlediska bezpečnosti, ale je třeba se připravit na opravdu vysoké množství událostí, které budou jen informačního charakteru. K podkategoriím podrobného sledování procesů patří:

- DPAPI Activity – aktivita rozhraní Data Protection API.[43]
  Doporučení: ponechat v defaultním nastavení (No Auditing). Případné nastavení auditování „Success“ událostí bude mít za následek jen malý počet záznamů, proto to v případě zájmu není nic proti ničemu. „Failure“ události zde nejsou žádné.

- Process Creation – události vytvoření procesu.[44]
  Doporučení: ponechat v defaultním nastavení (No Auditing). V případě kritických systému povolit auditování „Success“ událostí. Je ale třeba počítat s extrémně vysokým objemem generovaných událostí, proto stojí za zvážení, jestli tyto události budou opravdu reálně vyhodnocovány. „Failure“ události zde nejsou žádné.

- Process Termination – ukončení procesu.
  Doporučení: ponechat v defaultním nastavení (No Auditing).

- RPC Events – události vzdáleného volání procedur.
  Doporučení: ponechat v defaultním nastavení (No Auditing).

2.9 Audit system events

Tato kategorie je velice důležitá, protože umožňuje auditovat z hlediska bezpečnosti důležité systémové události. Mezi tyto události patří zapnutí, vypnutí nebo restart počítače, zaplněný log událostí, změna systémového času, provedení změn v ověřovacích balících a další události, které mohou ovlivnit systém. V rámci monitoringu systémových událostí je určitě víc než vhodné sledovat restarty systému, které, pokud jsou neplánované, mohou být projevem bezpečnostního incidentu nebo přinejmenším provozního problému. Množství generovaných událostí je relativně nízký, zatímco jejich přínos je poměrně vysoký.

2.9.1 IPsec Driver

Nastavením této podkategorie se povoluje auditovat události generované ovladačem IPSec, mezi které patří například zahájení a ukončení služeb IPSec, zahození síťových paketů, doručení paketu s chybným SPI (Security Parameter Index) nebo selhání spuštění IPSec filtru. Velké množství zahozených paketů může svědčit o pokusu neautorizovaného systému přistoupit do sítě.[45]
Doporučení: nastavit „Success“ a „Failure“.

2.9.2 Other System Events

K událostem podkategorie ostatních systémových událostí patří především události služby a ovladače Windows Firewallu. Za pozornost stojí zejména události zastavení či selhání spuštění Windows Firewallu, nebo problémy s aplikací politik. Nefunkčnost Windows Firewallu může vest k ohrožení systému a z toho důvodu je vhodné tyto události monitorovat.[46]
Doporučení: nastavit „Success“ a „Failure“.

2.9.3 Security State Change

Mezi další systémové události patří změna stavu zabezpečení. Jedná se o události vypnutí a spuštění operačního systému, změny systémového času nebo události obnovení systému administrátorem po vynuceném vypnutí z důvodu zahlceného logu zabezpečení.[47]
Doporučení: nastavit „Success“.

2.9.4 Security System Extension

Tato podkategorie zaznamenává události rozšíření systému zabezpečení, jako je například načtení autentizačního balíku. Velmi významnou událostí, která by neměla zůstat bez povšimnutí je pak událost ID 4697 – nainstalování nové služby. Množství generovaných událostí je nízké a objevují se primárně na řadičích domény.[48]
Doporučení: nastavit „Success“.

2.9.5 System Integrity

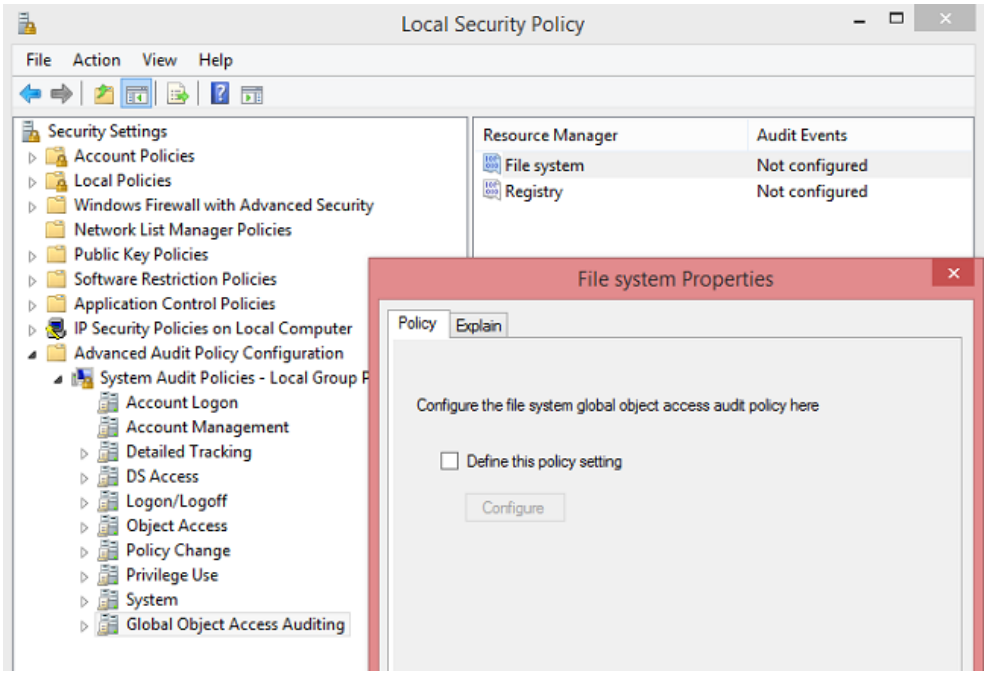
Integritou systému je myšlena vlastnost, že systém vykonává svojí funkci nenarušeným způsobem, bez záměrné nebo náhodné neautorizované manipulace se systémem. Tato podkategorie zahrnuje události, které mohou narušit integritu systému, jako je například problém se zápisem událostí zabezpečení, neplatné použití LPC portu, detekce vzdáleného volání procedur (RPC), které může kompromitovat systém, detekce neplatné hash hodnoty spustitelného souboru a další.[49]
Doporučení: nastavit „Success“ a „Failure“.

2.10 Global Object Access Auditing

Tato nová kategorie umožňuje administrátorům definovat SACL globálně na celý počítač, a to buď na souborový systém, nebo na registry. Není tedy nutné, jako v případě kategorie Audit Object Access, definovat SACL na jednotlivé objekty. Součástí Global Object Access Auditing jsou jediné dvě podkategorie:

- File System
- Registry

Oproti ostatním podkategoriím se na kartě Properties nenastavuje „Success“ a „Failure“, ale zaškrtává se volba „Define this policy settings“, na základě které se dále nastavuje globální SACL.



Obrázek 2.4: Global Object Access Auditing

Kapitola 3

Výpis událostí pomocí Powershellu

Powershell je skriptovací jazyk společnosti Microsoft založený na platformě .NET Framework. Od verze operačního systému Windows server 2008 R2 je již nativní součástí OS. V porovnání s UNIXovými shelly, které jsou textové, se Powershell odlišuje především tím, že je objektově orientovaný.

Co se týče zpracování událostí systému MS Windows, přináší Powershell oproti zabudovanému prohlížeči událostí výhodu spočívající v bohaté možnosti sestavení poměrně detailních filtrů. Pro práci s logy nabízí Powershell dva základní nástroje:

- Get-Eventlog,
- Get-WinEvent.

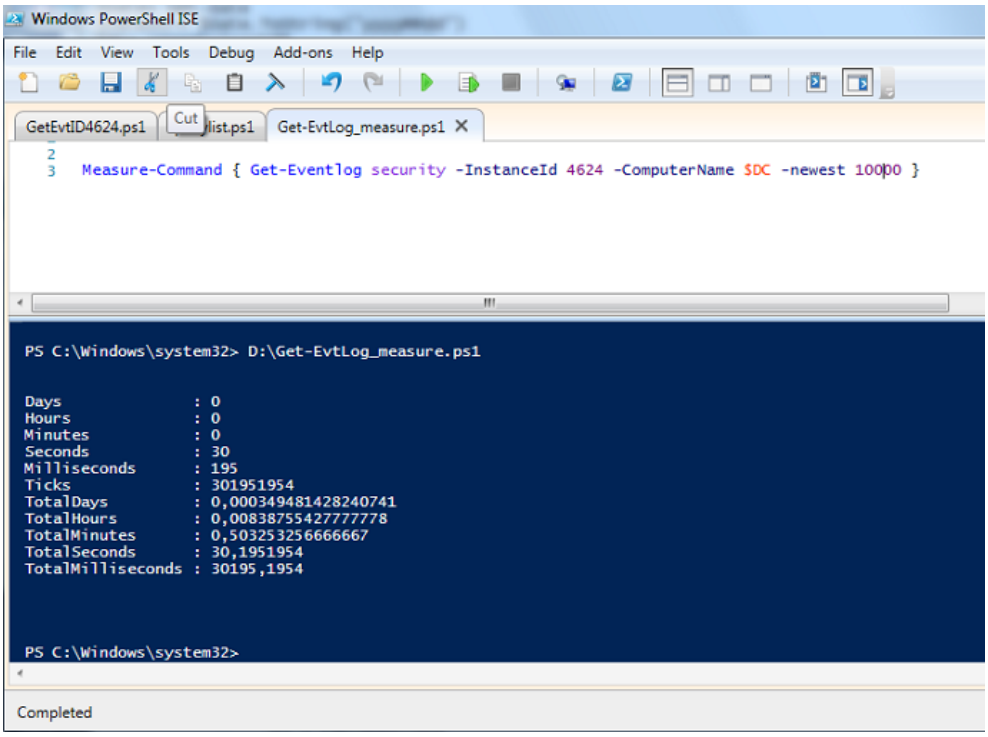
Nástroj Get-Eventlog je dostupný od verze 1.0. Slouží k získání událostí na lokálních i vzdálených systémech. Prostřednictvím přepínačů umožňuje základní vstupní filtrování. Je omezen pouze na zpracování základních Windows logů.

Nástroj Get-WinEvent je dostupný od verze 2.0. Oproti předchozímu příkazu umožňuje práci se všemi typy událostí, tedy nejen se standardními typy události jako jsou aplikační či systémové, ale i s událostmi aplikací, služeb a EWT logy. Poskytuje pokročilé možnosti filtrování prostřednictvím přepínačů, ať už se jedná o –FilterHashtable nebo –FilterXML, který umožňuje psaní obzvlášť detailních dotazů.

3.1 Porovnání příkazů pro zpracování událostí

Za účelem zvolení vhodného Powershell nástroje pro filtrování událostí na MS Windows serveru 2008 R2 bylo provedeno porovnání rychlosti provedení ekvivalentních příkazů. Všechny příkazy měly za úkol vyfiltrovat posledních 10000 událostí ID 4624 z logu zabezpečení na vzdáleném serveru.

V následujících dialogových oknech lze vidět 3 způsoby základního filtrování pomocí cmdletů Get-EventLog a Get-WinEvent. Během prvního testu byl použit příkaz Get-Eventlog se základními parametry. Celkový čas provedení dané operace byl 30,195 sekundy.



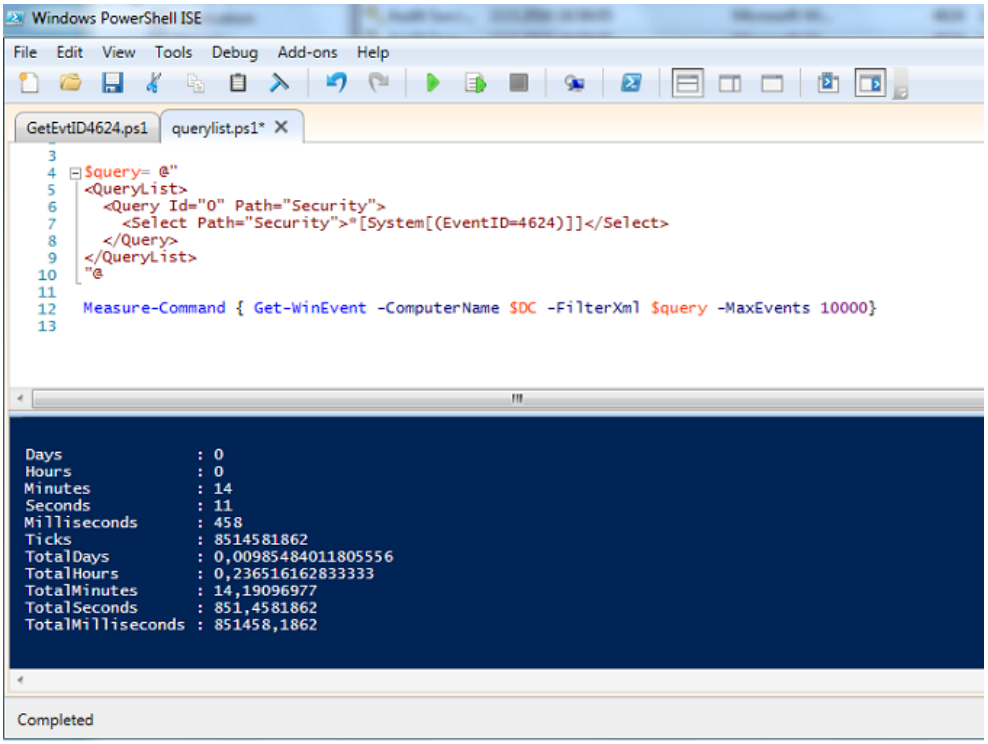
Obrázek 3.1: Měření rychlosti provedení příkazu Get-Eventlog

V druhém testu byl použít Get-WinEvent cmdlet s filtrováním pomocí jednoduchého XML dotazu. V tomto případě již dosáhl celkový čas 851,458 sekundy, což je 28 krát více než v prvním testu.

Jako třetí byl spuštěn opět cmdlet Get-WinEvent, tentokrát ale s přepínačem –FilterHashtable, který je doporučen pro efektivní zdrojové filtrování protokolu událostí. Doba trvání této operace činila 851,293 sekundy, což je téměř identický čas jako v předchozím případě.

Na závěr byl ještě proveden test s použitím stejného příkazu jako v prvním testu, tentokrát však pro celkový počet 100 000 událostí. Jak lze vidět, čas odpovídá zhruba desetinásobku času měřeného na 10 000 událostech.

Na základě provedení těchto měření byl pro účely dalšího filtrování vybrán jako základ právě příkaz Get-Eventlog.



Obrázek 3.2: Měření rychlosti provedení příkazu Get-WinEvent -FilterXML

3.2 Filtrování událostí

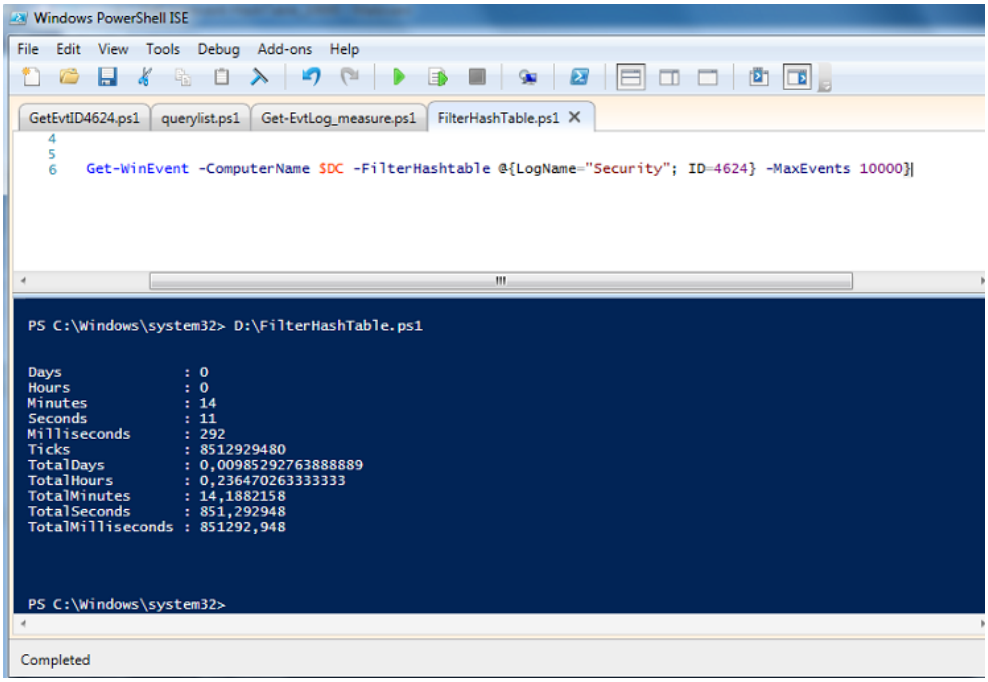
Aby bylo možné provést podrobné filtrování událostí podle jednotlivých položek, je třeba znát konkrétní XML schéma dané události. To je možné snadno zjistit přímo z konzole Powershellu viz následující výpis:

Pro účely filtrování je podstatné znát uspořádání položek dané události, jak je uvedeno v šabloně ve výše uvedeném výpisu. K jednotlivým položkám lze přistupovat jako k položkám pole pomocí ReplacementStrings [i], kde i značí index položky v poli. Toto pole se indexuje od nuly.

Vzhledem k tomu, že lze takto snadno přistoupit k jednotlivým položkám události a získat jejich hodnoty, lze stejně snadno pomocí operátorů definovat i podmínky jaké hodnoty chceme (-eq, -like, -match a další), nebo nechceme (-neq, -notlike) filtrovat.

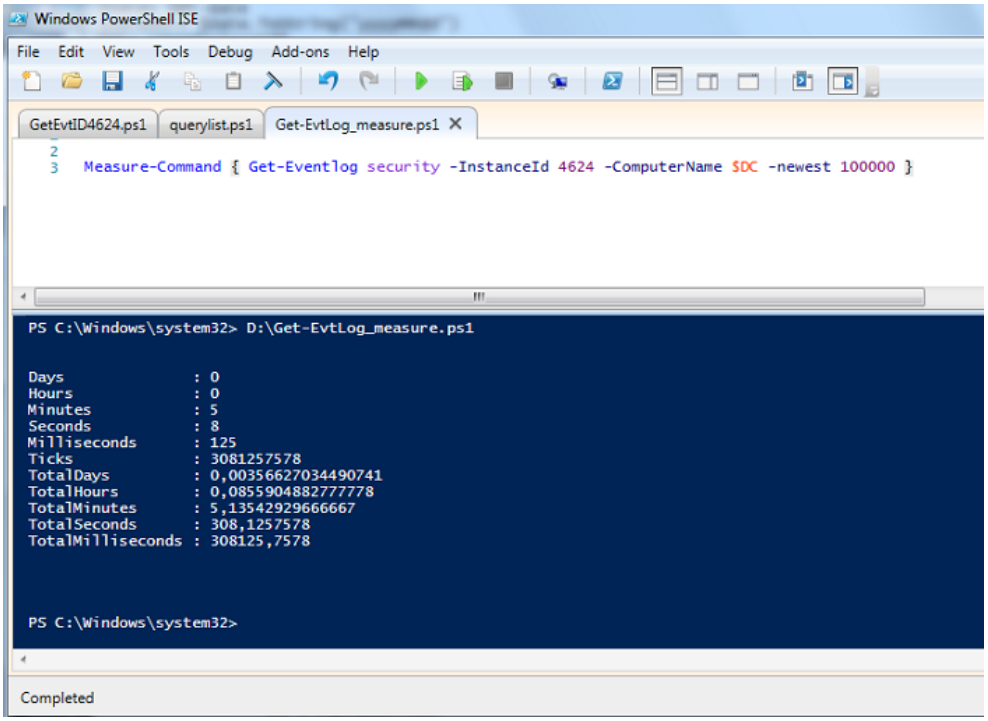
Na dalším obrázku lze vidět ukázku výpisu událostí ID 4624, kde hodnota položky LogonType se rovná třem. To znamená, že se filtrují pouze síťová připojení. LogonType je typu unsigned integer, jak je patrné z popisu šablony výše3.5. Pro porovnání byl použit operátor –eq (equal, tedy „je rovno“).

V případě, že je hodnota typu string, jako je tomu například u položky TargetUserName, používají se pro porovnávání hodnot operátory –like, -notlike, a další. V případě těchto operátorů lze použít zástupné znaky.3.7

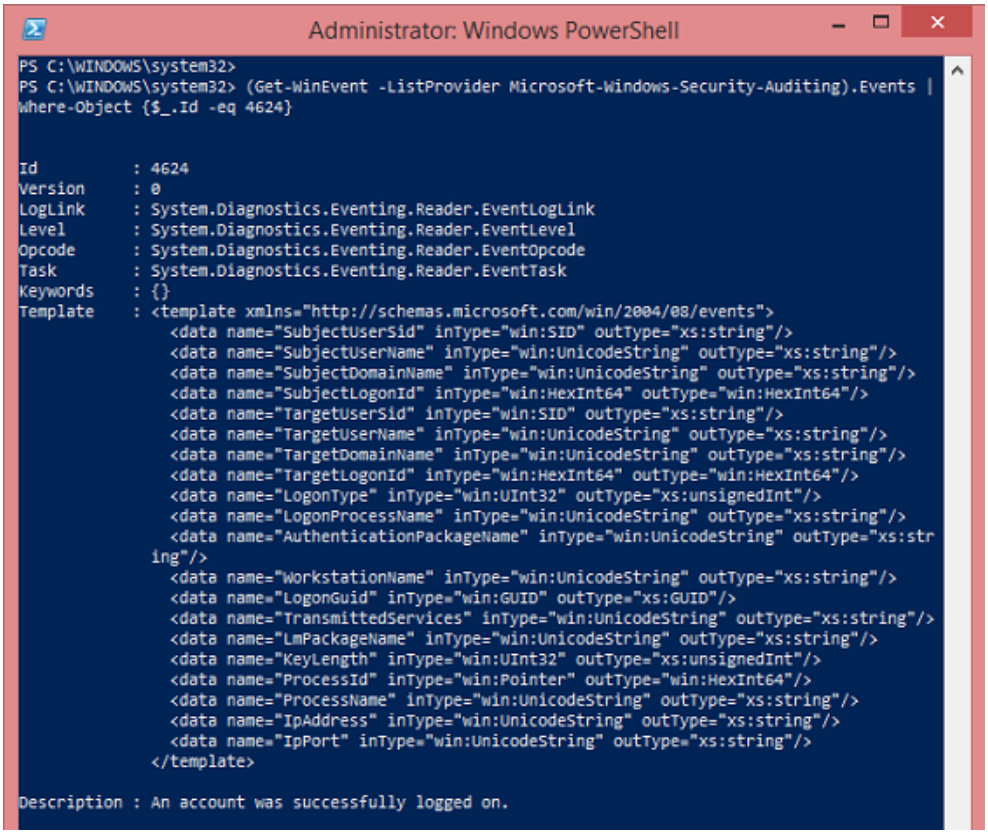


Obrázek 3.3: Měření rychlosti provedení příkazu Get-WinEvent -FilterHashTable

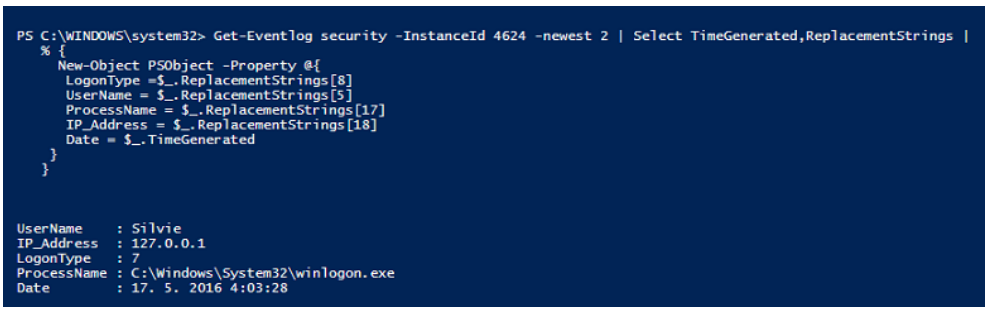
Tímto způsobem se dají sestavovat velmi podrobné filtry. Konkrétní použití záleží na potřebách administrátora, nebo bezpečnostního správce. Lze takto provádět vyhledávání konkrétních informací dle aktuální povahy situace, vytvářet reporty nebo detekovat vysoce podezřelé události.



Obrázek 3.4: Měření rychlosti provedení příkazu Get-Eventlog pro 100 000 událostí



Obrázek 3.5: Template události ID 4624



Obrázek 3.6: Výpis vybraných položek události ID 4624 s využitím přístupu k položkám prostřednictvím ReplacementStrings

```
PS C:\WINDOWS\system32> Get-Eventlog security -InstanceId 4624 | where { $_.ReplacementStrings[5] -like '*SER*' } |
 Select TimeGenerated,ReplacementStrings |
   % {
     New-Object PSObject -Property @{
      LogonType =$_.ReplacementStrings[8]
      UserName = $_.ReplacementStrings[5]
      ProcessName = $_.ReplacementStrings[17]
      IP_Address = $_.ReplacementStrings[18]
      Date = $_.TimeGenerated
    }
   }



UserName    : LOCAL SERVICE
IP_Address  : -
LogonType   : 5
ProcessName : C:\Windows\System32\services.exe
Date        : 16. 5. 2016 8:50:29

UserName    : NETWORK SERVICE
IP_Address  : -
LogonType   : 5
ProcessName : C:\Windows\System32\services.exe
Date        : 16. 5. 2016 8:50:29
```

Obrázek 3.7: Výpis událostí ID 4624, kde položka TargetUserName odpovídá všem uživatelským účtům, které mají v názvu „SERVICE“

Závěr

V první části této práce jsem čtenáře stručně seznámila s problematikou bezpečnosti informačních systémů, resp. s důležitostí významu bezpečnostních logů, užívanou terminologií, popisem a důležitých bezpečnostních událostí v prostředí zabezpečení Windows serveru 2008 R2 za účelem detekce bezpečnostních incidentů a reakce na ně.

Druhá část této práce se věnuje popisu jednotlivých kategorií a podkategorií zásad nastavení auditu včetně doporučeného nastavení.

Poslední část této práce jsem věnovala popisu možností zpracování a filtrování událostí zabezpečení OS Windows Server 2008 R2 prostřednictvím Powershallu 2.0. Porovnala jsem základní způsoby filtrování a otestovala jednotlivé příkazy na doménovém řadiči. Na závěr jsem ukázala možnosti podrobného filtrování na základě hodnot jednotlivých položek události. Tyto skripty jsem použila a otestovala na zachycených událostech v reálném provozu.

Myslím, že touto prací velmi ulehčím všem zájemcům, analytikům a začínajícím bezpečnostním správcům shánění ucelených informací o problematice identifikace událostí zabezpečení v prostředí MS Windows a ukážu alternativu nástrojů třetích stran pro filtrování událostí. Na základě takto získaných informací je možné projektovat obranné mechanismy a řešit tak dílčí cíle v hierarchické víceúrovňové bezpečnostní architektuře.

Literatura

[1] Microsoft: Security Monitoring and Attack Detection Planning Guide. jun 2005. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc163158.aspx

[2] Anthony, R.: Detecting Security Incidents Using Windows Workstation Event Logs. Červen 2012. Dostupné z: https://www.sans.org/reading-room/whitepapers/logging/detecting-security-incidents-windows-workstation-event-logs-34262

[3] Microsoft, T.: Audit account logon events. Leden 2005. Dostupné z: https://technet.microsoft.com/en-us/library/cc787176

[4] Microsoft, T.: Audit Credential Validation. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772679

[5] Microsoft, T.: Audit Kerberos Service Ticket Operations. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772667

[6] Microsoft, T.: Audit Kerberos Authentication Service. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772702

[7] Microsoft, T.: Audit Application Group Management. Červen 2013. Dostupné z: https://technet.microsoft.com/cs-cz/library/dn311463

[8] Microsoft, T.: Audit Computer Account Management. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772717

[9] Microsoft, T.: Audit Distribution Group Management. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772713

[10] Microsoft, T.: Audit Other Account Management Events. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd941586

[11] Microsoft, T.: Audit Security Group Management. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772663

[12] Microsoft, T.: Audit User Account Management. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772693

[13] Microsoft, T.: Audit Detailed Directory Service Replication. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd941628

[14] Microsoft, T.: Audit Directory Service Access. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd941618

[15] Microsoft, T.: Audit Directory Service Changes. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772641

[16] Microsoft, T.: Audit Directory Service Replication. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772741

[17] Ben, B. K., SMITH: *Zabezpečení systému a sítě Microsoft Windows*. Grada, 2006, 80-251-1260-8.

[18] Microsoft, T.: Audit Account Lockout. Červenec 2013. Dostupné z: https://technet.microsoft.com/cs-cz/library/dn319074

[19] Microsoft, T.: Audit Policy Recommendations. Červenec 2016. Dostupné z: https://technet.microsoft.com/cs-cz/library/dn487457

[20] Microsoft, T.: Audit Logoff. Červenec 2013. Dostupné z: https://technet.microsoft.com/cs-cz/library/dn319085

[21] Microsoft, T.: Audit Network Policy Server. Červenec 2013. Dostupné z: https://technet.microsoft.com/cs-cz/library/dn311469

[22] Microsoft, T.: Audit Other Logon/Logoff Events. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dn311470

[23] Microsoft, T.: Audit Special Logon. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772635

[24] Microsoft, T.: Audit Application Generated. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772620

[25] Microsoft, T.: Audit Certification Services. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772671

[26] Microsoft, T.: Audit File Share. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772690

[27] Microsoft, T.: Audit Filtering Platform Connection. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772661

[28] Microsoft, T.: Audit Handle Manipulation. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772749

[29] Microsoft, T.: Audit Kernel Object. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd941615

[30] Microsoft, T.: Audit Other Object Access Events. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/librarydd772744

[31] Microsoft, T.: Audit Registry. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd941614

[32] OSIF, M.: *Windows Server 2003*. Grada, 2003, 80-247-0396-3.

[33] Microsoft, T.: Audit SAM. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772719

[34] Microsoft, T.: Audit Policy. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc766468

[35] Microsoft, T.: Auditing Security Events Best practices. Leden 2005. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc778162

[36] Microsoft, T.: Audit Audit Policy Change. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772736

[37] Microsoft, T.: Audit Authentication Policy Change,. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772672

[38] Microsoft, T.: Audit Authorization Policy Change. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd941587

[39] Microsoft, T.: Audit Filtering Platform Policy Change. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd941600

[40] Microsoft, T.: Audit MPSSVC Rule-Level Policy Change. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772750

[41] Microsoft, T.: Audit Non-Sensitive Privilege Use. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772731

[42] Microsoft, T.: Audit Sensitive Privilege Use. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772724

[43] Microsoft, T.: Audit DPAPI Activity. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd941585

[44] Microsoft, T.: Audit Process Creation. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd941613

[45] Microsoft, T.: Audit IPsec Driver. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772695

[46] Microsoft, T.: Audit Other System Events. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772739

[47] Microsoft, T.: Audit Security State Change. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772631

[48] Microsoft, T.: Audit Security System Extension. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd772700

[49] Microsoft, T.: Audit System Integrity. Červenec 2009. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd941605

Příloha A

Seznam použitých zkratek

AD Active Directory

MS Microsoft

OS operační systém

NT New Technology

MMC microsoft management console

SW software

HW hardware

IS informační systém

ID Identification

DRSM Directory Services Restore Mode

CD Compact Disc

PC Personal Computer

EFS Encrypting File System

Příloha **B**

Obsah přiloženého CD

- `src`
  - `impl` ..... zdrojové kódy implementace
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF
  - `zadani.pdf` ..... zadání práce ve formátu PDF