EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

OPERAČNÍ SYSTÉMY

Zdroje logů

Metodický list

Autor: Giovanni Guadagno, Metodik: Ing. Roman Koláčný

Recenzenti: doc. Ing. Jaroslav Dočkal, CSc.

Rok vydání: 2023

Obsah

Cíle

- Student popíše, co to je log
- Student vysvětlí přínosy logování
- Student popíše, jak lze logy zpracovávat a používat

Dovednosti

- Student analyzuje raw log, najde různé vzory logů
- Student dokáže samostatně vyhledat zdroje logů
- Za pomocí otevřených zdrojů dokáže student z logu číst informace

Pracovní prostředí

Úlohu lze realizovat v prostředí Cylab JCEKB

Pro práci budeme potřebovat následující:

- Zdroj raw logů (v tomto případě Linux, Windows, Mikrotik Router, pfSense firewall)
- Nedílnou součástí cvičení je také výuková prezentace

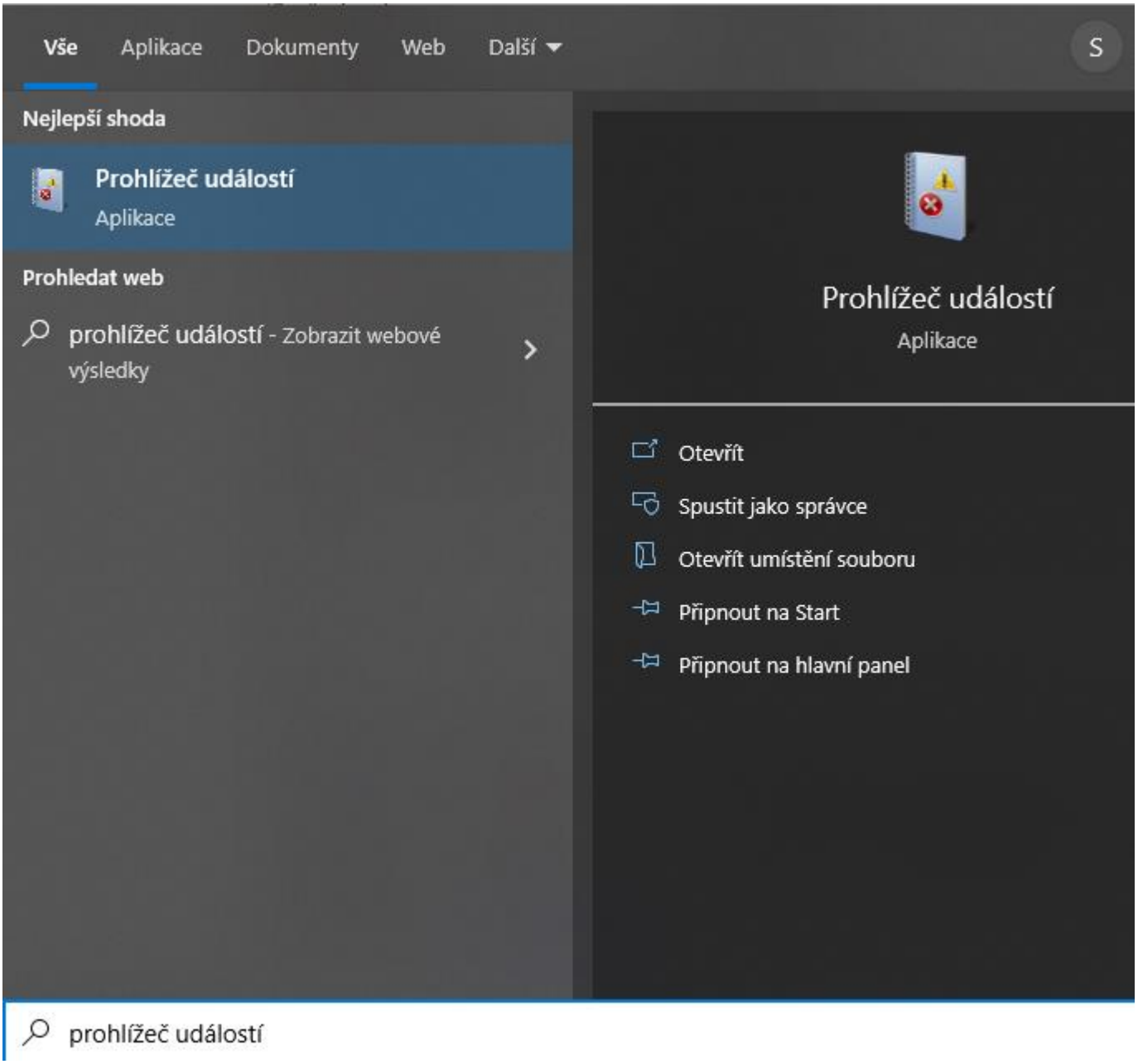
Průběh výuky

1 Příprava

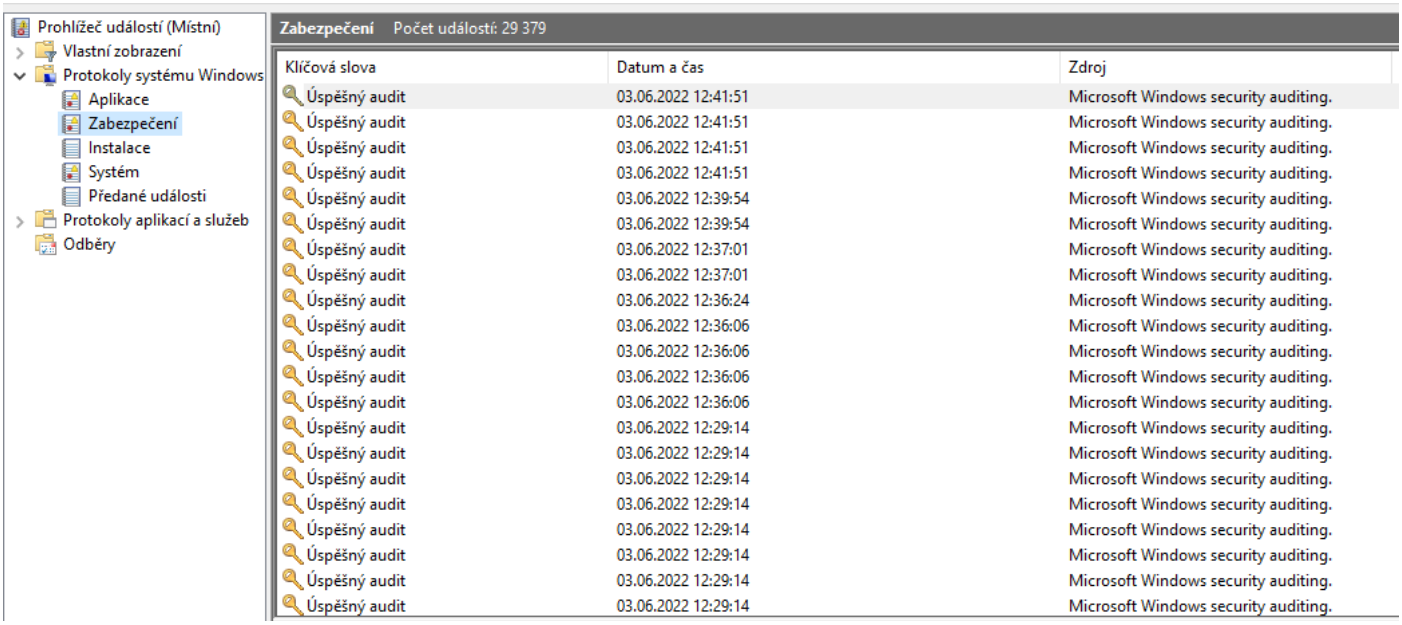
Prvních 20–30 minut diskuse a výklad na téma logy, k čemu slouží a podobně – viz výuková prezentace. Nachystání Windows a Linux stanic. Ověřit funkčnost pfSense FW a Mikrotik routeru.

2 Logy Windows

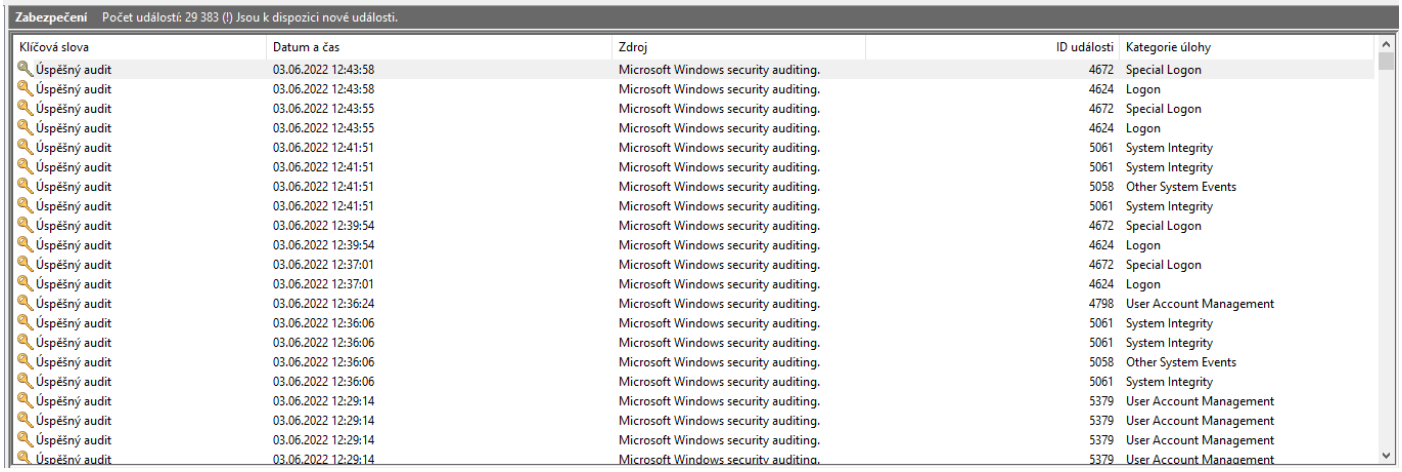
Prvními logy, s nimiž se bude pracovat, budou logy Windows. Do nabídky hledání napíšeme „Prohlížeč událostí“, případně „Event viewer“



Nejvíce nás budou zajímat security logy. K nim je možno se dostat následovně:

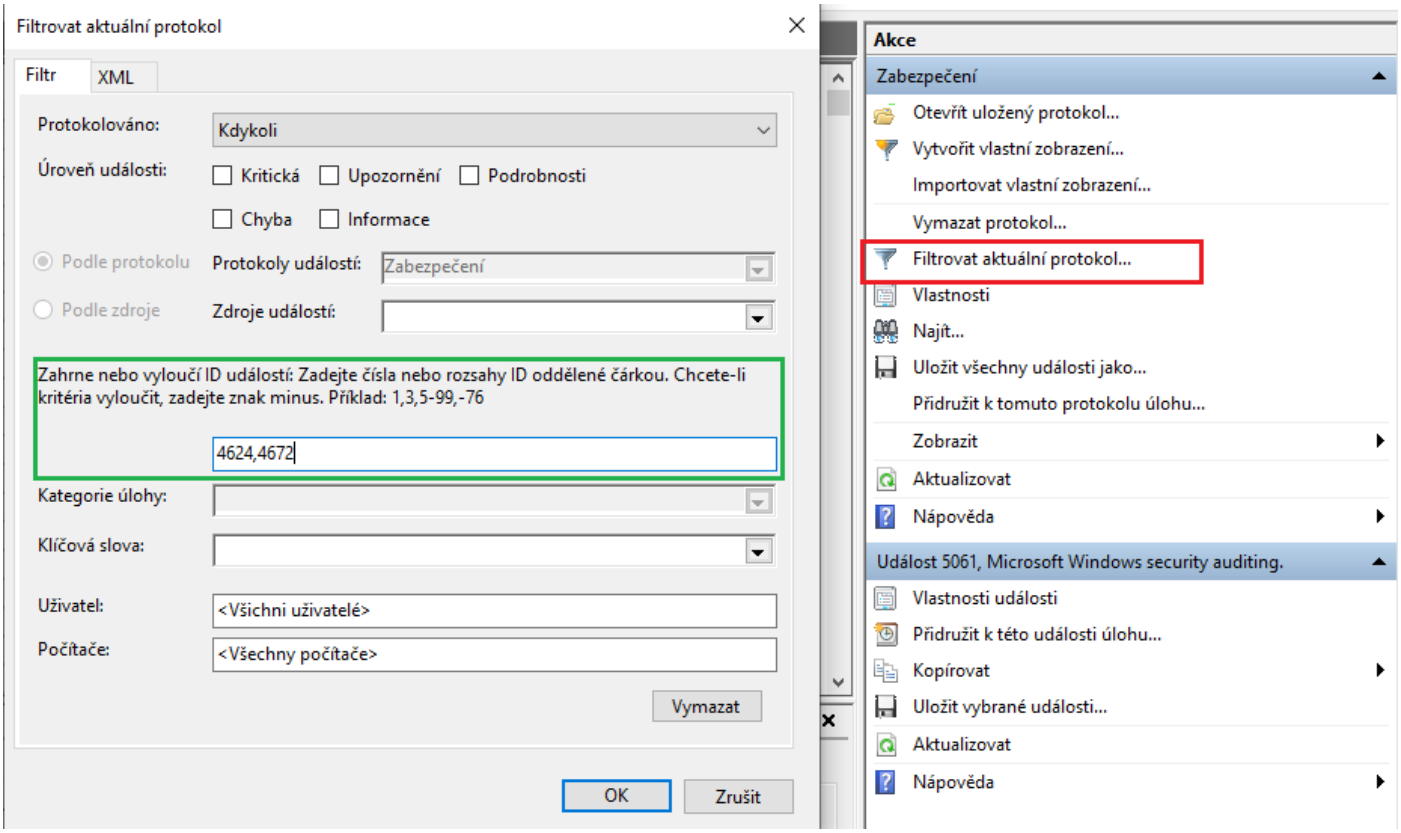


V této sekci, kde se nachází security logy, u nakždého z nich vidíme, zda byl audit úspěšný nebo ne, dále časové razítko, zdroj, tzn. „kdo“ log vygeneroval, dále ID události dle toho, o jaký log se jedná (například ID 4672 bude událost Special Logon apod.)



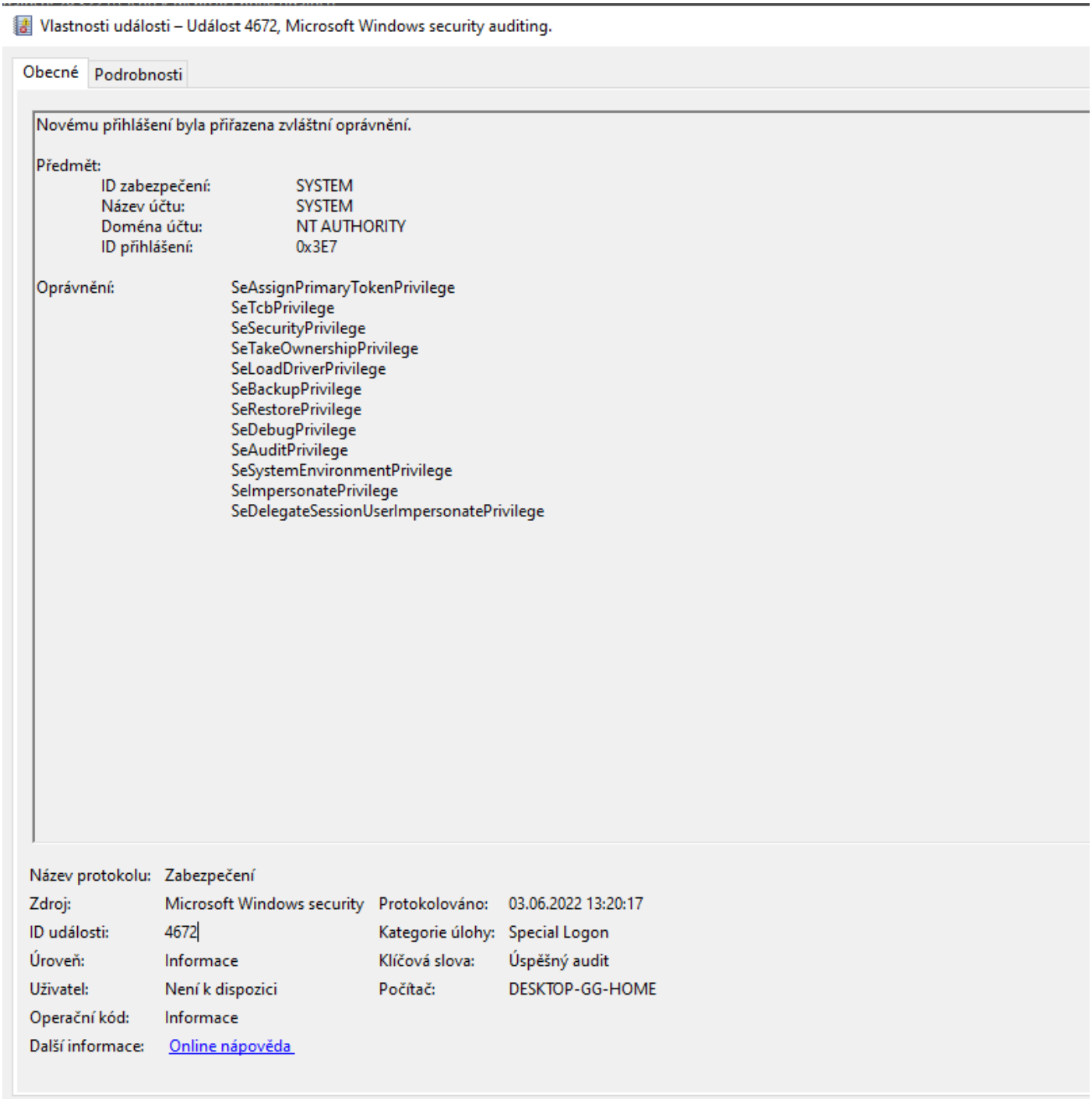
Dle ID, ale i jiných identifikátorů, lze logy filtrovat, a to přes nabídku vlevo – „filtrovat aktuální protokol“. Vyfiltrujme například události s ID 4624 a 4672 – to jsou logy o přihlášení.

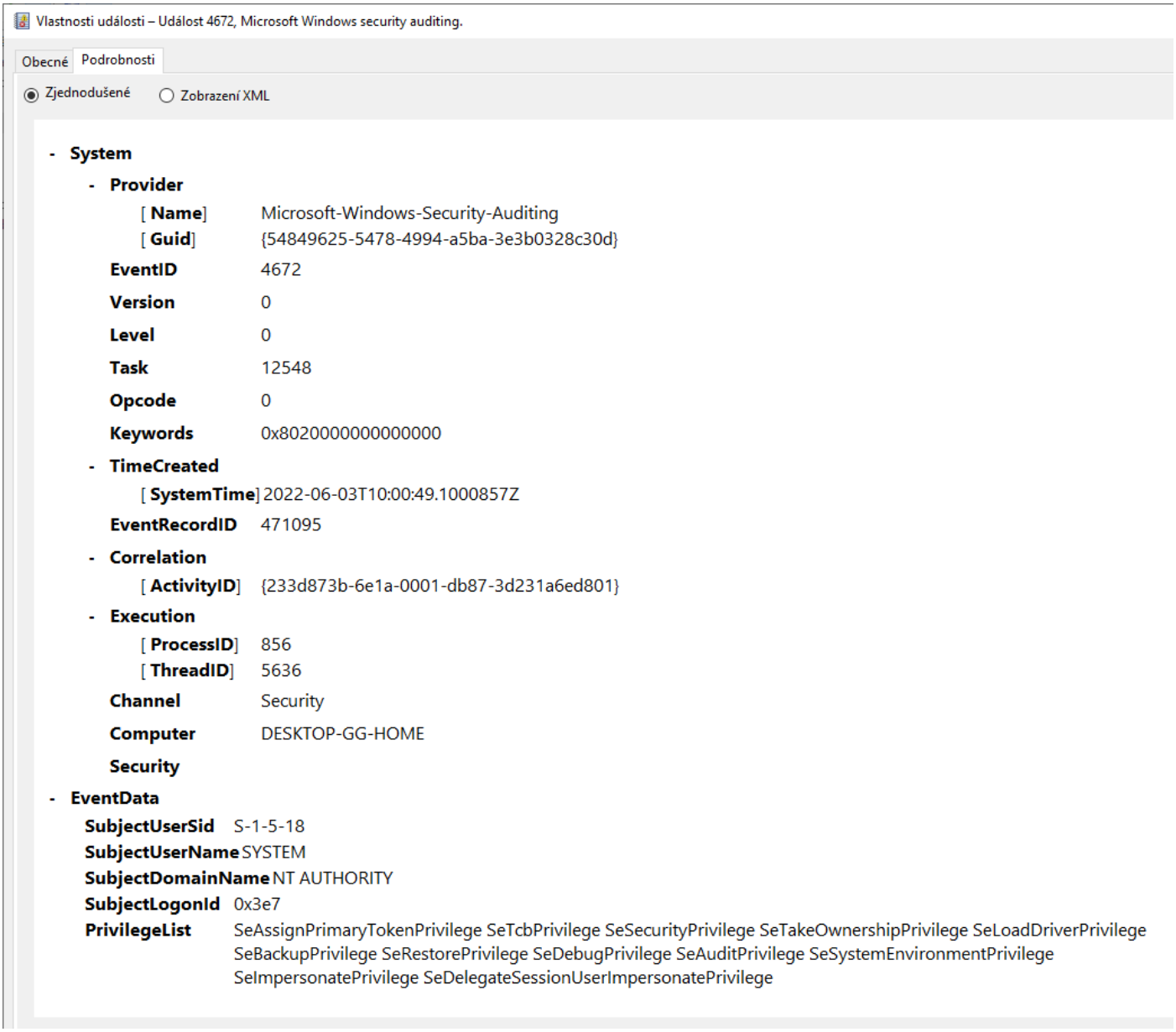
Do pole zadáme ID a jelikož chceme jejich výčet, oddělíme je čárkou. Volbu potvrdíme a dostaneme námi požadované logy.



2.1 Ukázka Microsoft Windows security auditing – 4672

Nyní budeme log zkoumat podrobněji – dvojklikem se zobrazí bližší informace. Začněme logem s ID 4672 – Special logon. Tento log říká, že přihlášení byla přidělena zvláštní oprávnění. Vidíme, o jaký účet se jedná, v jaké doméně se nachází, kdo práva udělil, jaké bylo ID přihlášení, dále výčet udělených oprávnění včetně časového razítka. Na kartě podrobnosti lze ve stromovém uspořádání vidět další podrobnější informace, pro další zpracování je i možné je vyexportovat ve formátu XML.

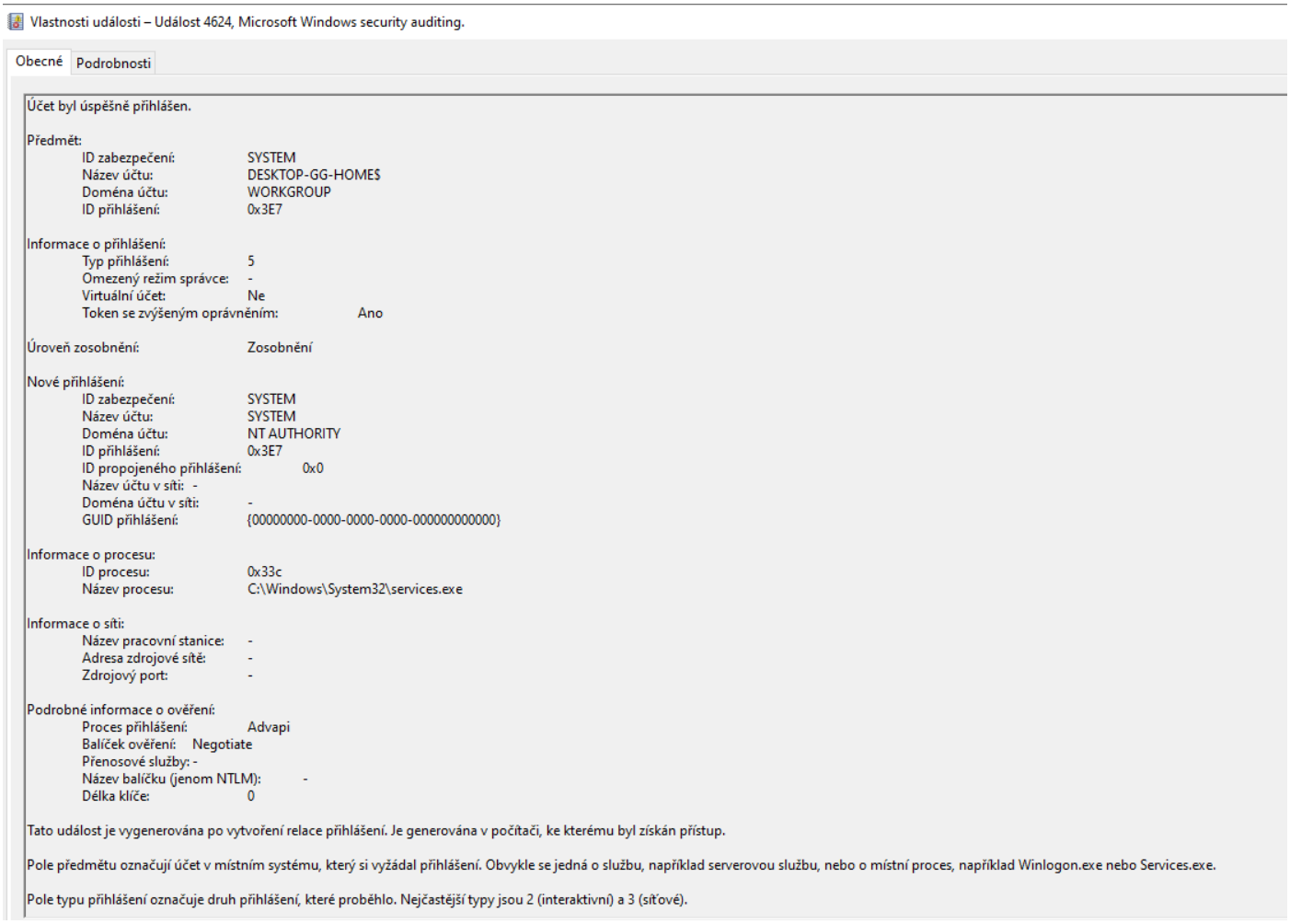

Vlastnosti události – Událost 4672, Microsoft Windows security auditing.
Obecné
Podrobnosti
Novému přihlášení byla přiřazena zvláštní oprávnění.
Předmět:
ID zabezpečení: SYSTEM
Název účtu: SYSTEM
Doména účtu: NT AUTHORITY
ID přihlášení: 0x3E7
Oprávnění: SeAssignPrimaryTokenPrivilege
SeTcbPrivilege
SeSecurityPrivilege
SeTakeOwnershipPrivilege
SeLoadDriverPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeDebugPrivilege
SeAuditPrivilege
SeSystemEnvironmentPrivilege
SeImpersonatePrivilege
SeDelegateSessionUserImpersonatePrivilege
Název protokolu: Zabezpečení
Zdroj: Microsoft Windows security
Protokolováno: 03.06.2022 13:20:17
ID události: 4672
Kategorie úlohy: Special Logon
Úroveň: Informace
Klíčová slova: Úspěšný audit
Uživatel: Není k dispozici
Počítač: DESKTOP-GG-HOME
Operační kód: Informace
Další informace: Online nápověda



2.2 Ukázka Microsoft Windows security auditing – 4624

Tento log je poněkud obsáhlejší – je vygenerován, dojde-li k úspěšnému přihlášení. Dvojklikem opět zjistíme podrobnosti. Již nyní víme, co přesně se stalo (viz přiložený screen) – účet byl úspěšně přihlášen. Zároveň vidíme typ přihlášení 5. V dolní části logu vidíme další informace, které by mohly prozradit více.

Tento log má jako Logon tyep (typ přihlášení) 5, v dolní části logu však máme nápovědu pouze k 2 a 3. Přepněme proto kartu na kartu Podrobnosti – zde bychom již měli být schopni zjistit, o jaký typ přihlášení by se mělo jednat.



Tato událost je vygenerována po vytvoření relace přihlášení. Je generována v počítači, ke kterému byl získán přístup.

Pole předmětu označují účet v místním systému, který si vyžádal přihlášení. Obvykle se jedná o službu, například serverovou službu, nebo o místní proces, například Winlogon.exe nebo Services.exe.

Pole typu přihlášení označuje druh přihlášení, které proběhlo. Nejčastější typy jsou 2 (interaktivní) a 3 (síťové).

Pole Nové přihlášení označují účet, pro který bylo vytvořeno nové přihlášení, tj. přihlášený účet.

Pole Síť označují původ požadavku na vzdálené přihlášení. Název pracovní stanice není vždy k dispozici a v některých případech může být toto pole prázdné.

Pole úrovně zosobnění označuje rozsah, ve kterém může být proces v přihlašovací relaci zosobněn.

Pole s informacemi o ověření poskytují podrobné informace o tomto konkrétním požadavku na přihlášení.
- GUID přihlášení je jednoznačný identifikátor, který je možné použít ke spojení této události s událostí KDC.
- Přenosové služby označují pomocné služby, které se podílely na tomto požadavku na přihlášení.
- Název balíčku označuje dílčí protokol z protokolů NTLM, který byl použit.
- Délka klíče označuje délku generovaného klíče relace. Tato hodnota bude 0, pokud nebyl požadován žádný klíč relace.

Karta podrobnosti (4624):

+ **System**
- **EventData**

SubjectUserSid	S-1-5-18
SubjectUserName	DESKTOP-GG-HOME$
SubjectDomainName	WORKGROUP
SubjectLogonId	0x3e7
TargetUserSid	S-1-5-18
TargetUserName	SYSTEM
TargetDomainName	NT AUTHORITY
TargetLogonId	0x3e7
LogonType	5
LogonProcessName	Advapi
AuthenticationPackageName	Negotiate
WorkstationName	-
LogonGuid	{00000000-0000-0000-0000-000000000000}
TransmittedServices	-
LmPackageName	-
KeyLength	0
ProcessId	0x33c
ProcessName	C:\Windows\System32\services.exe
IpAddress	-
IpPort	-
ImpersonationLevel	%%1833
RestrictedAdminMode	-
TargetOutboundUserName	-
TargetOutboundDomainName	-
VirtualAccount	%%1843
TargetLinkedLogonId	0x0
ElevatedToken	%%1842

Vidíme, že cílem byl NT AUTHORITY\SYSTEM, stejně tak i pohled na ProceasName indikuje, že by to mohl být nějaký systémový proces. Domněnku ověříme z otevřených zdrojů:

When Windows starts a service which is configured to log on as a user, Windows will create a new logon session for this service. This happens only if the service uses a "common" user account. If it uses special accounts, e.g. "Local System", "NT AUTHORITY\LocalService" or "NT AUTHORITY\NetworkService", Windows won't create new logon sessions. The opened logon session will be closed when the service stops and a logoff event (4634) will be registered. Note that event description doesn't contain any information about the service name, process information lists only name of the service control manager (services.exe). When Audit Failure logon event (4625) is registered with

logon type = 5, this commonly means that the "designated" user has changed password, and you should update service logon details.[1]

3 Logy Linux

Tato kapitola se bude zabývat logy z Linuxu. Konkrétně logy auditními. Nacházejí se v /var/log/audit. Běžnému uživateli je však vstup zamítnut. Je nutné chodit pod rootem.

```
cd var/log/audit
```

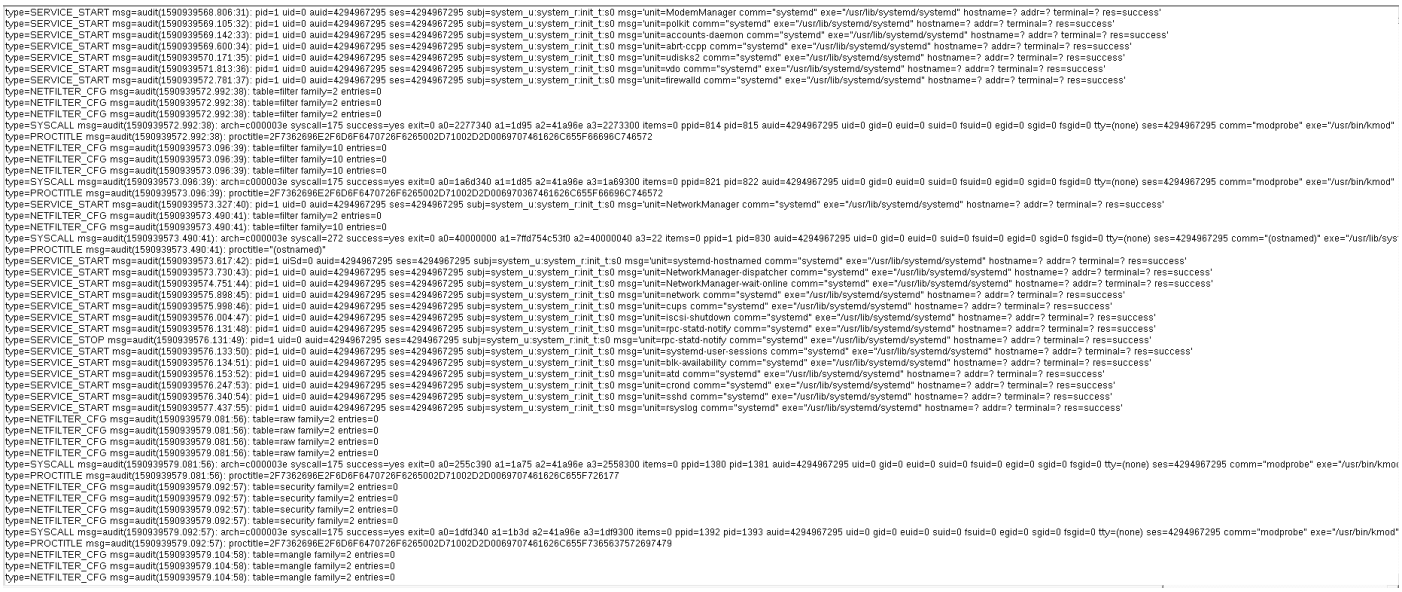
V této složce je soubor audit.log – ten uchovává veškerou auditní stopu a je možné z něj vyčíst, co se na stanici dělo. Zkusme jej nyní otevřít.

```
cat audit.log //zobrazí veškerý obsah souboru
head -n 3 audit.log //zobrazí první 3 řádky
```

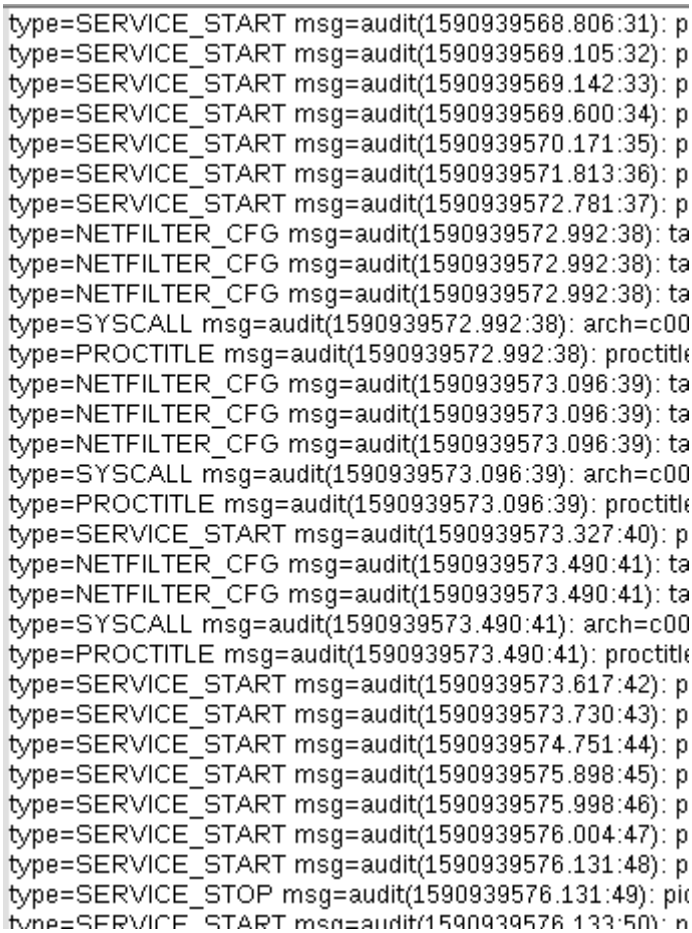
Pokud nevíme, co přesně hledat, je vhodnější log prozkoumat v nějakém textovém editoru – vhodný je například Notepad++. Pokud víme, co chceme hledat, můžeme si informace z logu „grepnout". Řekněme, že budume chtít hledat všechny logy, které indikují změnu konfigurace (CONFIG_CHANGE). Potom by byl příkaz následovný:

```
cat audit.log | grep CONFIG_CHANGE //zobrazí veškeré logy obsahující CONFIG_CHANGE
head -n 5 audit.log | grep CONFIG_CHANGE //zobrazí 5 prvních řádků, pokud obsahují CONFIG_CHANGE
```

Nyní otevřeme celý soubor s logy v nějakém textovém editoru, a to z důvodu jednoduššího zkoumání jeho formátu.



Zaměřme se na jeho části postupně zleva doprava:



Každý log nejprve začíná tím, proč/kým/z jakého důvodu byl vygenerován. Následuje poměrně podstatný údaj, a sice časové razítko (timestamp) ve formátu Epoch time – tj. čas od 1. 1. 1970 v sekundách. Formát logů se již pak dále liší v závislosti na tom, z jakého důvodu byl vygenerován. I v „raw“ formátu je poměrně čitelný.

4 Logy pfSense (firewall)

Třetími logy budou logy firewallové, a sice pfSense. Logy se nachází v **BUDE DOPLNĚNO DLE DOMLUVY V JCEKB (WEB VIEW NEBO CONSOLE)**.

Do textového formátu jsou logy logovány do /var/log/filter.log. Ačkoli jsou logy na první pohled změtí různých čísel, jejich uspořádání je poměrně logické a po chvíli práce s nimi se jejich čtení stává jednoduchým. Některé hodnoty jsou však pro naše účely redundantní.

```
Aug  1 08:00:00 master filterlog: 5,16777216,,1000000103,em0,match,pass,in,4,0x10,,128,0,0,
none,17,udp,328,77.75.75.172,46.255.231.42,443,4443,308
```

Log již tradičně začíná časovým razítkem (timestamp), následuje hostname. Prvním hodnotou je číslo FW pravidla, které tento traffic zachytilo. Další zajímavější hodnotou je „tracker“ – unikatní ID per FW rule (začínající 1000…). Následuje interface, důvod logu (zde match – match FW rule), akce FW (pass, případně block), jakým směrem se komunikovalo (in/out), následuje verze IP (4 nebo 6).

Formát logu se v této chvíli začne lišit v závislosti na verzi IP protokolu. Další zajímavou hodnotou je zde TTL – zde 128. None zde reprezentuje IP vlajky – v tomto případě zde žádné nejsou. Následuje ID protokolu (17) a protokol (UDP), další hodnotou je délka zprávy. Následují zdrojová a cílová adresa a zdrojový a cílový port. Poslední hodnotou je délka dat.

Log by však mohl dále pokračovat – kdyby byl jako transportní protokol použit protokol TCP, log by dále obsahoval TCP vlajky nebo číslo sekvence. Kdyby se jednalo o protokol ICMP, log by opět pokračoval a nesl data, která protokol ICMP standardně generuje. Více o logování a o formátu logů z FW pfSense lze najít na tomto odkaze [2].

5 Logy Mikrotik (router)

Dalšími logy, které se zde budou probírat, budou logy z routerů, konktrétně od výrobce Mikrotik. Logy si můžeme lokálně zobrazit po připojení na router, a to následujícím příkazem

```
[admin@mujrouter] /log> print
```

Mikrotik routery logují jednak „systémové“ události, tj. například přihlášení na router, změny pravidel apod., jednak také samotný provoz, tedy odkud, kam, jakým interfacem a kolik toho přes router proteklo.

Formát logů je navíc velmi jednoduchý a čitelný – viz výpis níže

```
[admin@mujrouter] /log> print

jan/02/1970 02:00:09 system,info router rebooted
sep/15 09:54:33 system,info,account user admin logged in from 10.1.101.212 via winbox
sep/15 12:33:18 system,info item added by admin
sep/15 12:34:26 system,info mangle rule added by admin
sep/15 12:34:29 system,info mangle rule moved by admin
sep/15 12:35:34 system,info mangle rule changed by admin
sep/15 12:42:14 system,info,account user admin logged in from 10.1.101.212 via telnet
sep/15 12:42:55 system,info,account user admin logged out from 10.1.101.212 via telnet
01:01:58 firewall,info input: in:ether1 out:(none), src-mac 00:21:29:6d:82:07, proto UDP,
10.1.101.1:520->10.1.101.255:520, len 452
```

První log indikuje reboot routeru. Další události, které se zalogovaly 15. září v čase od 12:33:18 do 12:42:55 , indikují přihlášení/odhlášení účtu admin přes winbox a telnet z adresy 10.1.101.212 a změny pravidel. Poslední log, zalogovaný „dnes“ (chybí datum) v 01:01:58, indikuje příchozí komunikaci portem ether1, přičemž zdrojová MAC adresa zařízení je 00:21:29:6d:82:07, zdrojová IP 10.1.101.1, port 520, cílová IP 10.1.101.255, port 520, přičemž komunikace byla realizována přes protokol UDP. Poslední informací je délka – 452. Další informace lze najít zde [3]

Shrnutí a závěr

Ruční kontrola logů tak, jak byla názorně předvedena v tomto scénáři, je však použitelná pouze pro domácí užití. Pro správu logů „ve velkém“ (v organizaci) a navíc z více zařízení zároveň, je standardně využíváno sofistikovanějších nástrojů – příkladem budiž Syslog, který sesbíráveškeré logy z organizace, obohatí je (timestamp, severity, hostname) a centralizuje na server. Pro další analýzu je možno využít nejrůznějších Log Managemetn nástrojů (například ArcSight Logger, který je nasazen i v prostředí JCEKB).

Po absolvování tohoto cvičení by student měl být schopen obhájit, k čemu je logování určené, z jakých zařízení lze logy sbírat, samostatně je za užití otevřených zdrojů vyhledávat a porozumět jejich formátu. Dále by měl vysvětlit, jakým způsobem se zdroji logů dále pracovat (ruční kontroly, centralizace, ukládání).

Seznam použitých zdrojů

1. https://eventlogxp.com/blog/logon-type-what-does-it-mean/
2. https://docs.netgate.com/pfsense/en/latest/monitoring/logs/raw-filter-format.html
3. https://wiki.mikrotik.com/wiki/Manual:System/Log