



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



jihomoravský kraj

OPERAČNÍ SYSTÉMY

Zdroje logů

Metodický list

Autor: Giovanni Guadagno, Metodik: Ing. Roman Koláčný

Recenzenti: doc. Ing. Jaroslav Dočkal, CSc.

Rok vydání: 2023

Zdroje logů podléhá licenci CC BY-SA 4.0 International License (Offline use:

<http://creativecommons.org/licenses/by-nc-sa/4.0/>).



Obsah

Dovednosti	2
Pracovní prostředí	2
Průběh výuky	3
1 Příprava	3
2 Logy Windows	3
2.1 Ukázka Microsoft Windows security auditing – 4672.....	5
2.2 Ukázka Microsoft Windows security auditing – 4624.....	7
3 Logy Linux.....	10
4 Logy pfSense (firewall).....	11
5 Logy Mikrotik (router)	12
Shrnutí a závěr	13
Seznam použitých zdrojů.....	14

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 pomoci 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

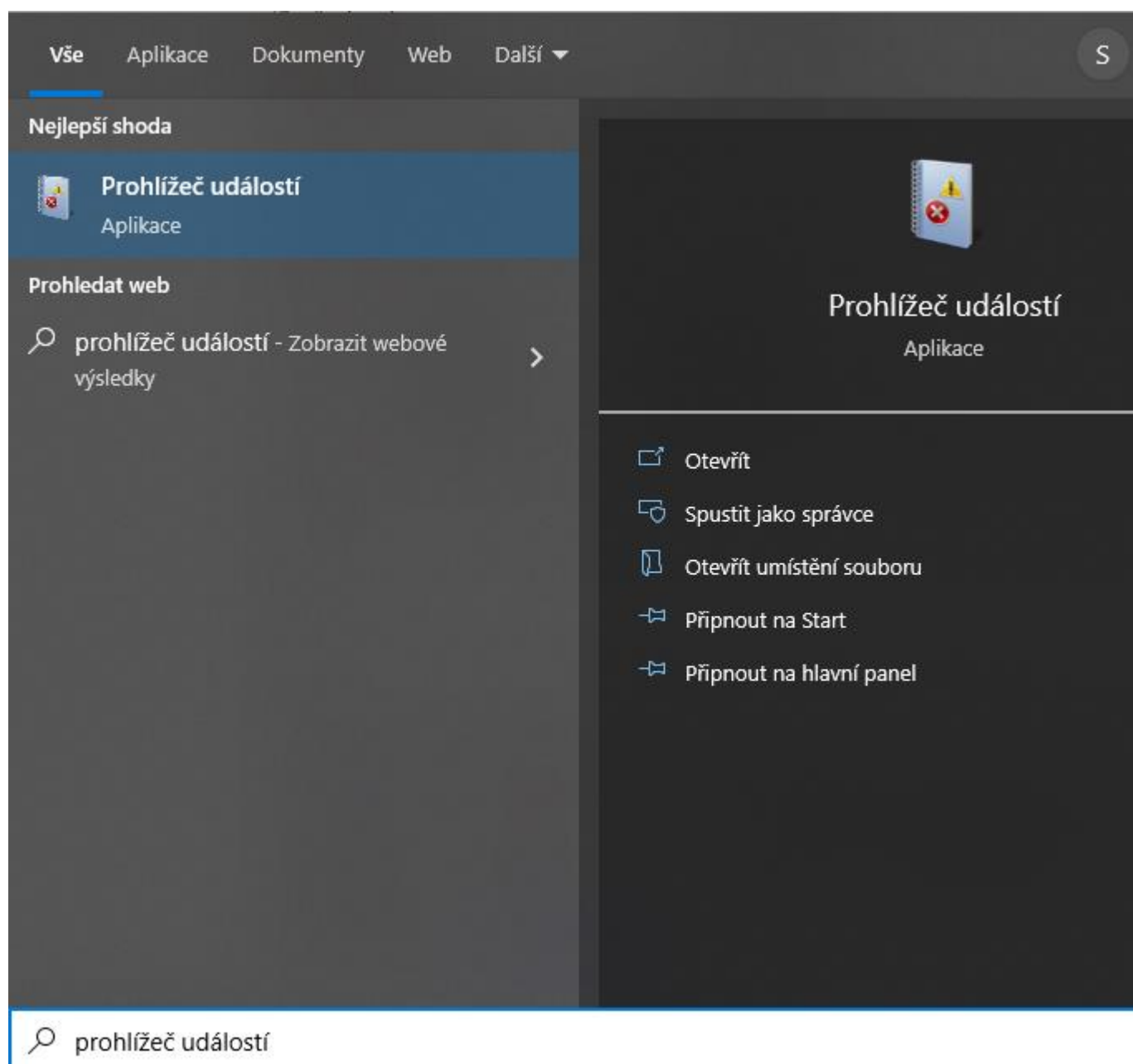
Průběh výuky

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:

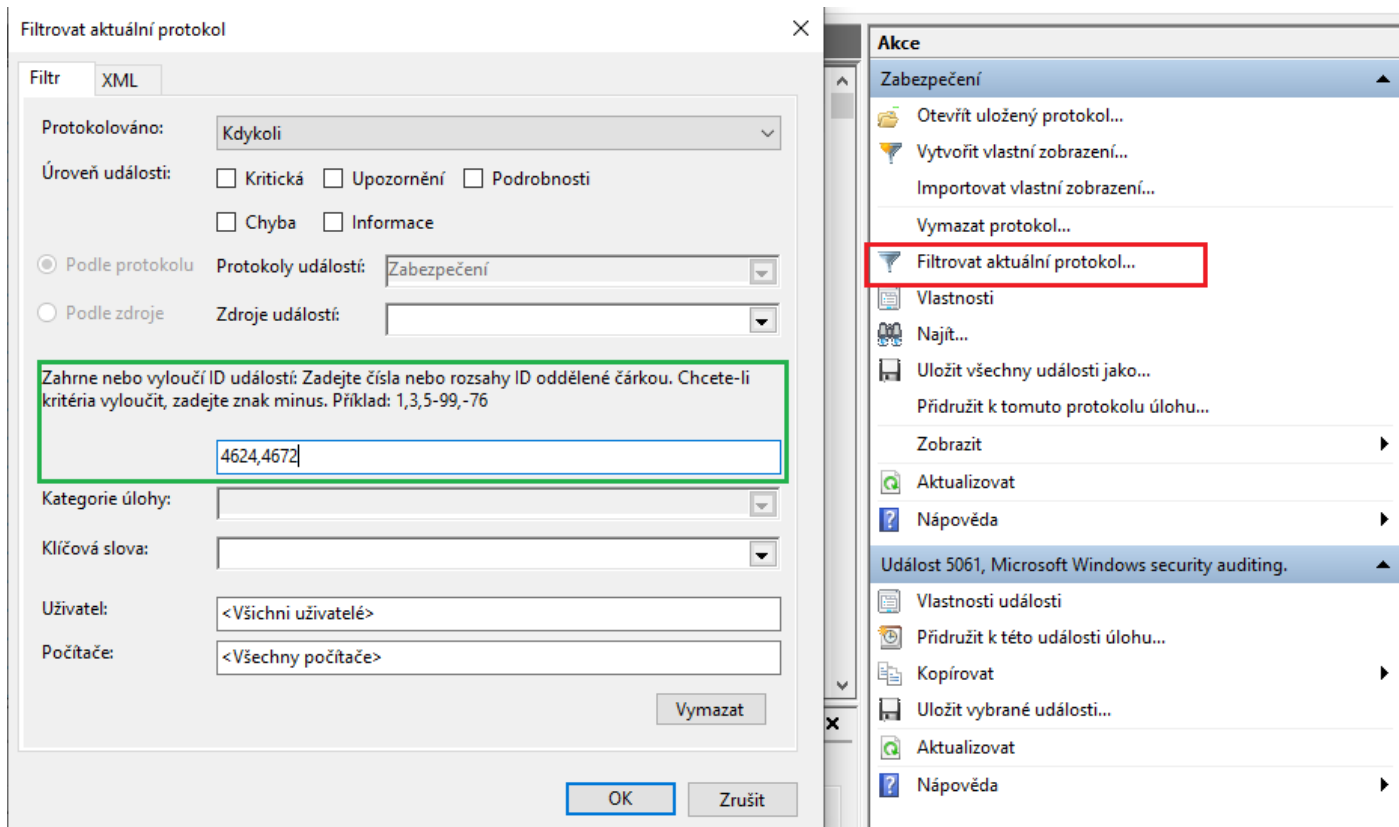
Klíčová slova	Datum a čas	Zdroj
Úspěšný audit	03.06.2022 12:41:51	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:41:51	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:41:51	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:41:51	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:39:54	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:39:54	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:37:01	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:37:01	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:36:24	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:36:06	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:36:06	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:36:06	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:36:06	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.

V této sekci, kde se nachází security logy, u každého 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.)

Klíčová slova	Datum a čas	Zdroj	ID události	Kategorie úlohy
Úspěšný audit	03.06.2022 12:43:58	Microsoft Windows security auditing.	4672	Special Logon
Úspěšný audit	03.06.2022 12:43:58	Microsoft Windows security auditing.	4624	Logon
Úspěšný audit	03.06.2022 12:43:55	Microsoft Windows security auditing.	4672	Special Logon
Úspěšný audit	03.06.2022 12:43:55	Microsoft Windows security auditing.	4624	Logon
Úspěšný audit	03.06.2022 12:41:51	Microsoft Windows security auditing.	5061	System Integrity
Úspěšný audit	03.06.2022 12:41:51	Microsoft Windows security auditing.	5061	System Integrity
Úspěšný audit	03.06.2022 12:41:51	Microsoft Windows security auditing.	5058	Other System Events
Úspěšný audit	03.06.2022 12:41:51	Microsoft Windows security auditing.	5061	System Integrity
Úspěšný audit	03.06.2022 12:39:54	Microsoft Windows security auditing.	4672	Special Logon
Úspěšný audit	03.06.2022 12:39:54	Microsoft Windows security auditing.	4624	Logon
Úspěšný audit	03.06.2022 12:37:01	Microsoft Windows security auditing.	4672	Special Logon
Úspěšný audit	03.06.2022 12:37:01	Microsoft Windows security auditing.	4624	Logon
Úspěšný audit	03.06.2022 12:36:24	Microsoft Windows security auditing.	4798	User Account Management
Úspěšný audit	03.06.2022 12:36:06	Microsoft Windows security auditing.	5061	System Integrity
Úspěšný audit	03.06.2022 12:36:06	Microsoft Windows security auditing.	5061	System Integrity
Úspěšný audit	03.06.2022 12:36:06	Microsoft Windows security auditing.	5058	Other System Events
Úspěšný audit	03.06.2022 12:36:06	Microsoft Windows security auditing.	5061	System Integrity
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.	5379	User Account Management
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.	5379	User Account Management
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.	5379	User Account Management
Úspěšný audit	03.06.2022 12:29:14	Microsoft Windows security auditing.	5379	User Account Management

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. Začneme 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.

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](#)

Vlastnosti události – Událost 4672, Microsoft Windows security auditing.

Obecné Podrobnosti

Zjednodušené Zobrazení XML

```

- System
  - Provider
    [ Name]      Microsoft-Windows-Security-Auditing
    [ Guid]      {54849625-5478-4994-a5ba-3e3b0328c30d}
  EventID      4672
  Version      0
  Level        0
  Task         12548
  Opcode       0
  Keywords     0x8020000000000000
  - TimeCreated
    [ SystemTime] 2022-06-03T10:00:49.1000857Z
  EventRecordID 471095
  - Correlation
    [ ActivityID] {233d873b-6e1a-0001-db87-3d231a6ed801}
  - Execution
    [ ProcessID] 856
    [ ThreadID] 5636
  Channel      Security
  Computer     DESKTOP-GG-HOME
  Security
- EventData
  SubjectUserSid S-1-5-18
  SubjectUserName SYSTEM
  SubjectDomainName NT AUTHORITY
  SubjectLogonId 0x3e7
  PrivilegeList  SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege
                 SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege
                 SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege

```

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 příložený 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 typ (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.

Obecné Podrobnosti

Účet byl úspěšně přihlášen.

Předmět:

ID zabezpečení:	SYSTEM
Název účtu:	DESKTOP-GG-HOMES
Doména účtu:	WORKGROUP
ID přihlášení:	0x3E7

Informace o přihlášení:

Typ přihlášení:	5
Omezený režim správce:	-
Virtuální účet:	Ne
Token se zvýšeným oprávněním:	Ano

Úroveň zosobnění: Zosobnění

Nové přihlášení:

ID zabezpečení:	SYSTEM
Název účtu:	SYSTEM
Doména účtu:	NT AUTHORITY
ID přihlášení:	0x3E7
ID propojeného přihlášení:	0x0
Název účtu v síti:	-
Doména účtu v síti:	-
GUID přihlášení:	{00000000-0000-0000-0000-000000000000}

Informace o procesu:

ID procesu:	0x33c
Název procesu:	C:\Windows\System32\services.exe

Informace o síti:

Název pracovní stanice:	-
Adresa zdrojové sítě:	-
Zdrojový port:	-

Podrobné informace o ověření:

Proces přihlášení:	Advapi
Balíček ověření:	Negotiate
Přenosové služby:	-
Název balíčku (jenom NTLM):	-
Délka klíče:	0

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).

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

Vidíme, že cílem byl NT AUTHORITY\SYSTEM, stejně tak i pohled na ProcessName 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 možné 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 „grehnout“. Řekněme, že budeme 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.

```
type=SERVICE_START msg=audit(150939568.806.31): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=ModemManager comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939568.806.32): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=NetworkManager dispatcher comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939568.142.33): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=accounts-daemon comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939568.600.34): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=abrt-cpp comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939571.111.35): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=udisks2 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939571.813.36): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=xdm comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939572.781.37): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=irenewal comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=NETFILTER_CFG msg=audit(150939572.892.38): table=filter family=2 entries=0
type=NETFILTER_CFG msg=audit(150939572.892.38): table=filter family=2 entries=0
type=NETFILTER_CFG msg=audit(150939572.892.38): table=filter family=2 entries=0
type=SYSCALL msg=audit(150939572.892.38): arch=c000003e syscall=175 success=yes exit=0 a0=2277340 a1=1d95 a2=41a96e a3=2273300 items=0 ppid=814 pid=815 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="mmodprobe" exe="/usr/bin/kmod"
type=PROCTITLE msg=audit(150939572.892.38): proctitle=2F736269622F6D6F6470726F6265002D71002D2D0069707461626C655F6668696746572
type=NETFILTER_CFG msg=audit(150939573.096.39): table=filter family=10 entries=0
type=NETFILTER_CFG msg=audit(150939573.096.39): table=filter family=10 entries=0
type=NETFILTER_CFG msg=audit(150939573.096.39): arch=c000003e syscall=175 success=yes exit=0 a0=1a6d340 a1=1d85 a2=41a96e a3=1a69300 items=0 ppid=821 pid=822 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="mmodprobe" exe="/usr/bin/kmod"
type=PROCTITLE msg=audit(150939573.096.39): proctitle=2F736269622F6D6F6470726F6265002D71002D2D0069707461626C655F6668696746572
type=SERVICE_START msg=audit(150939573.327.40): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=NetworkManager comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=NETFILTER_CFG msg=audit(150939573.490.41): table=filter family=2 entries=0
type=NETFILTER_CFG msg=audit(150939573.490.41): table=filter family=10 entries=0
type=SYSCALL msg=audit(150939573.490.41): arch=c000003e syscall=272 success=yes exit=0 a0=40000000 a1=7fd754c530 a2=40000040 a3=22 items=0 ppid=1 pid=830 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="(ostnamed)" exe="/usr/lib/ysys"
type=PROCTITLE msg=audit(150939573.490.41): proctitle="(ostnamed)"
type=SERVICE_START msg=audit(150939573.817.42): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=systemd-hostnamed comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939573.730.43): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=NetworkManager dispatcher comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939574.751.44): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=NetworkManager-wait-online comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939575.898.45): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=networkd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939575.998.46): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=cups comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939576.004.47): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=iscsi-shutdown comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939576.131.48): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=pc-stati-notly comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_STOP msg=audit(150939576.131.49): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=pc-stati-notly comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939576.133.50): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=systemd-user-sessions comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939576.134.51): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=lib-availability comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939576.153.52): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=atd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939576.247.53): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=cron comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939576.340.54): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=sshd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=SERVICE_START msg=audit(150939577.437.55): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u.system_r.initt_t0 msg=unit=rsyslog comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
type=NETFILTER_CFG msg=audit(150939579.081.56): table=raw family=2 entries=0
type=NETFILTER_CFG msg=audit(150939579.081.56): table=raw family=2 entries=0
type=NETFILTER_CFG msg=audit(150939579.081.56): table=raw family=2 entries=0
type=SYSCALL msg=audit(150939579.081.56): arch=c000003e syscall=175 success=yes exit=0 a0=255c390 a1=1a75 a2=41a96e a3=2559300 items=0 ppid=1380 pid=1381 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="mmodprobe" exe="/usr/bin/kmod"
type=PROCTITLE msg=audit(150939579.081.56): proctitle=2F736269622F6D6F6470726F6265002D71002D2D0069707461626C655F6668696746572
type=NETFILTER_CFG msg=audit(150939579.092.57): table=security family=2 entries=0
type=NETFILTER_CFG msg=audit(150939579.092.57): table=security family=2 entries=0
type=NETFILTER_CFG msg=audit(150939579.092.57): table=security family=2 entries=0
type=SYSCALL msg=audit(150939579.092.57): arch=c000003e syscall=175 success=yes exit=0 a0=1dd340 a1=1b3c a2=41a96e a3=1d93300 items=0 ppid=1392 pid=1393 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="mmodprobe" exe="/usr/bin/kmod"
type=PROCTITLE msg=audit(150939579.092.57): proctitle=2F736269622F6D6F6470726F6265002D71002D2D0069707461626C655F6668696746572
type=NETFILTER_CFG msg=audit(150939579.104.58): table=mangle family=2 entries=0
type=NETFILTER_CFG msg=audit(150939579.104.58): table=mangle family=2 entries=0
```

Zaměříme se na jeho části postupně zleva doprava:

```

type=SERVICE_START msg=audit(1590939568.806:31): p
type=SERVICE_START msg=audit(1590939569.105:32): p
type=SERVICE_START msg=audit(1590939569.142:33): p
type=SERVICE_START msg=audit(1590939569.600:34): p
type=SERVICE_START msg=audit(1590939570.171:35): p
type=SERVICE_START msg=audit(1590939571.813:36): p
type=SERVICE_START msg=audit(1590939572.781:37): p
type=NETFILTER_CFG msg=audit(1590939572.992:38): ta
type=NETFILTER_CFG msg=audit(1590939572.992:38): ta
type=NETFILTER_CFG msg=audit(1590939572.992:38): ta
type=SYSCALL msg=audit(1590939572.992:38): arch=c00
type=PROCTITLE msg=audit(1590939572.992:38): proctitle
type=NETFILTER_CFG msg=audit(1590939573.096:39): ta
type=NETFILTER_CFG msg=audit(1590939573.096:39): ta
type=NETFILTER_CFG msg=audit(1590939573.096:39): ta
type=SYSCALL msg=audit(1590939573.096:39): arch=c00
type=PROCTITLE msg=audit(1590939573.096:39): proctitle
type=SERVICE_START msg=audit(1590939573.327:40): p
type=NETFILTER_CFG msg=audit(1590939573.490:41): ta
type=NETFILTER_CFG msg=audit(1590939573.490:41): ta
type=SYSCALL msg=audit(1590939573.490:41): arch=c00
type=PROCTITLE msg=audit(1590939573.490:41): proctitle
type=SERVICE_START msg=audit(1590939573.617:42): p
type=SERVICE_START msg=audit(1590939573.730:43): p
type=SERVICE_START msg=audit(1590939574.751:44): p
type=SERVICE_START msg=audit(1590939575.898:45): p
type=SERVICE_START msg=audit(1590939575.998:46): p
type=SERVICE_START msg=audit(1590939576.004:47): p
type=SERVICE_START msg=audit(1590939576.131:48): p
type=SERVICE_STOP msg=audit(1590939576.131:49): p
type=SERVICE_START msg=audit(1590939576.133:50): n

```

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 změní 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“ – unikátní 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, konkrétně 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 sesbírá veškeré logy z organizace, obohatí je (timestamp, severity, hostname) a centralizuje na server. Pro další analýzu je možno využít nejrůznějších Log Management 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>