

Windows Threat Hunting

UBNetDef, Spring 2024 **Vicrosoft** Week 6

Presenter: Anthony Magrene



Agenda – Week 6

Incident Response (IR) High Level Windows Concepts Network Forensics PowerShell for IR Hands-on Activity 1-2 Windows Management Instrumentation (WMI) & Services Hands-on Activity 3 Persistence Hands-on Activity 4





Incident Response





Windows Concepts



Notable File Types

NetDef

Dynamic Link Library (.dll)

- Windows implementation of shared libraries
- Prevents redundant storage commonly used code

This PC > Local Disk (C:) > Windows > System32 >

Name	Date modified	Туре	Size
aadauthhelper.dll	12/11/2020 6:13 PM	Application exten	449 KB
aadcloudap.dll	12/11/2020 6:13 PM	Application exten	970 KB
aadjcsp.dll	3/12/2021 10:15 PM	Application exten	101 KB
aadtb.dll	1/12/2021 1:43 PM	Application exten	1,383 KB
aadWamExtension.dll	1/12/2021 1:43 PM	Application exten	150 KB
AarSvc.dll	3/12/2021 10:15 PM	Application exten	434 KB
AboutSettingsHandlers.dll	1/12/2021 1:43 PM	Application exten	431 KB
AboveLockAppHost.dll	3/12/2021 10:15 PM	Application exten	410 KB
accessibilitycpl.dll	2/11/2021 3:15 PM	Application exten	275 KB
accountaccessor.dll	1/12/2021 1:44 PM	Application exten	268 KB
AccountsRt.dll	1/12/2021 1:44 PM	Application exten	426 KB
AcGenral.dll	10/23/2020 3:20 PM	Application exten	362 KB
AcLayers.dll	12/11/2020 6:14 PM	Application exten	319 KB
acledit.dll	12/7/2019 4:09 AM	Application exten	11 KB
🚳 aclui.dll	12/7/2019 4:09 AM	Application exten	574 KB
acmigration.dll	3/12/2021 10:15 PM	Application exten	381 KB
ACPBackgroundManagerPolicy.dll	1/12/2021 1:43 PM	Application exten	191 KB
acppage.dll	1/12/2021 1:43 PM	Application exten	87 KB
acproxy.dll	12/7/2019 4:09 AM	Application exten	13 KB

NetDef

Portable Executable (.exe)

Machine code that is executed by the operating system
 May be written using high-level languages
 GO, C++, C, Ruby etc.

	🕬 HxD - [C:\\	Vind	ows\r	notep	ad.ex	e]												
	📓 File Edit	Sear	ch V	ïew	Analy	sis	Tools	Wi	ndow	v He	lp							
	📄 🚵 🕶 🗐		9	<u>.</u>	•	• 16	i	\sim	Win	idows	s (AN	SI)		- 1	ex	~	aeckodriver.exe	10/12/2019 8:38 AM
	inotepad.ex	e															genoanene	10, 10, 2010 0100 7 111
	Offset(h)	00	01	02	03 (04 (05 0	6 0	7 08	8 09) OA	ов	oc	OD	DE OF	Decoded text		
	00000000	41	5A	90	00 (03 (00 0	0 0	0 0	4 00	00	00	FF	FF	00 00	Mzÿÿ		
	00000010	BS	00	00	00 (00	00 0	0 0	0 40	0 00	00	00	00	00	00 00			
	00000020	00	00	00	00 0	00	00 0	00 0	0 00	0 00	00	00	00	00	00 00			
	00000030	00	00	00	00 0	00	0000	000	0 00	0 00	00	00	F8	21	00 00)ØØ		
	00000040	60	72	20	70 1	72	04 U		2 6	1 50	201	40	CD CD	21 : 68 :	01 00 17 61			
	00000050	74	20	62	65	20	72 7		Z 0.	0 60	20	20	44	45	23 20 DE 01	t be rup in DOS		
	00000070	61	6F	64	65 3	2E (A 2	4 00	00	00	00	00 1	00 00) mode\$		
1	00000080	14	D9	54	C8 1	50 1	B8 3	BA 9	B 50	0 BE	38	9B	50	B8	3A 9E	.ÙTÈP.:>P.:>P.:>		
	00000090	59	CO	A9	9B -	7E 1	88 3	A 9	B 4	4 D3	3E	9A	5A	B8 :	3A 9E	YÀ©>~.:>DÓ>šZ.:>		
	000000A0	44	D3	39	9A .	53 1	88 3	A 9	B 4	4 D3	3B	9A	59	B8 :	3A 9E	DÓ9šS,:>DÓ;šY,:>		
	00000B0	50	B8	3B	9B *	7C 1	BD 3	A 9	B 4	4 D3	32	9A	4E	B8 :	3A 9E	P,;> 3:>DÓ2šN,:>		
	00000000	44	D3	3F	9A 1	71 1	88 3	8 A 9	B 44	4 D3	C7	9B	51	B8 :	3A 9E	DÓ?šq,:>DÓÇ>Q,:>		
	00000D0	44	D3	C5	9B \$	51 1	88 3	8 A 9	B 44	4 D3	38	9A	51	B8 :	3A 9E	DÓÅ>Q,:>DÓ8šQ,:>		
	000000E0	52	69	63	68 5	50 1	B8 3	8 A 9	B 00	0 00	00	00	00	00	00 00	RichP,:>		
	000000F0	00	00	00	00 (00	00 0	0 0	0 50	0 45	00	00	64	86	07 00)PEdt		
	00000100	69	BD	FC	86 (00	00 0	00 0	0 00	0 00	00	00	FO	00 :	22 00) i¥sütð.".		
	00000110	OE	02	0E	14 (00 -	4A 0	02 0	0 00	0 E2	: 00	00	00	00	00 00)Jâ		
	00000120	BC	ЗD	02	00 (00	10 0	00 0	0 00	0 00	00	40	01	00	00 00	°=@		
	00000130	00	10	00	00 (00	02 0	0 0	0 02	A 00	00	00	0A	00	00 00			
	00000140	07	00	00	00 0	00	00 0	00 0	0 00	0 80	03	00	00	04	00 00)€€		
	00000150	BU	10	03	00 0	12	00 0		1 UI	0 00	108	00	00	00		· · K A		
	00000180	00	10	01	00 0					0 00	10	00	10	00				
	00000180	00	10	00	00 0				0 0	9 00	00	00	30	02		,		
	00000190	00	60	03	00 1	08	DBO	0 0	0 0	0 30	03	00	28	11	00 00			
	000001A0	00	00	00	00 0	00	00 0	00 0	0 0	0 70	03	00	D4	02	00 00)		
	000001B0	50	AD	02	00	54	00 0	00 0	0 0	0 00	00	00	00	00	00 00	PT		
	000001C0	00	00	00	00 0	00	00 0	00 0	0 8	8 67	02	00	28	00	00 00),q(
								-			-							

Application

3.483 K



PowerShell Script (.ps1)

PowerShell Integrated Scripting Environment (ISE)
 Extensive .NET integration

Wi	indov	vs Pow	erShel	I ISE										
E	dit	View	Tool	s Del	bug	Add-o	ons H	Help						
)	0		K		Ċ)	×	5	0				9	$\mathbf{\Sigma}$	E
SA.	psi													
		Stop	D=&Ta Int14	ilse in=10	1									
		[Big]	[nt]	q=10	3									
		Bigl	[nt]	N=\$p	*\$q									
		[Big]	Int]	T1N=	(Sp- N-[m	1)*(\$q-1) ct(\$Ni	Ň					
		[Biq]	[nt]	sqrt	fin=	[mat	h]:::	Sqrt((Nift					
	•	vrite	e-hos	t \$f	in									
		SNT ac	tors	. = @	0									
		SeRul	les =	@()	eO									
		i=2												
		#bull		st o	† 1	< e -	< 11 0)5	(N) L [.]	ist i	s \$e	Rules			
	۲		e(ast		eq s		ΞΛ							
		۷	vhile	(\$i_	-lt){							
			1	eRul	es+=									
		1		0.44										
		. 4		=\$tr										
	L	1												
	1	fact	ors	of N	and	fac	tors	of f	i (N)					
		i=1												
		while	(\$st	OD -	ea 🖇	fals	e)							
		[
			dei la		10									
			i	f((s	N %	\$i)	-eq (}(0						
					Nfac		+=	\$1						
					Ntac	tors	+=	\$N/\$1						
			3											
		4		i++										
			1-1											
		v	vhile	(\$i	-le		tfin){						
			j	f((\$	fin	% \$ 1) -e	1 (0 p						
	Ĭ				e : 110									
					1.1141	accu	(a +	40-1						



Event Log (.evtx)

Stores Windows Logs

Located C:\Windows\System32\winevt\Logs\

Action ⊨ 🔿 🛛 🔂 Event Viewer 🚔 Custom Vi 👔 Windows L Applic Applic Securi Setup Syster Forwar

📑 Subscriptio

Event viewer used to view logs

nt Viewer (Local)	System Number						Actions
Custom Views	Level		Date and Time	e	Source	^	System
Windows (togs Application Support Support System System Forwarded Events Applications and Services Logs Swel Logs Subscriptions	A Warning Event 4, FilterMan General Details	ager : :eter 1dEndopintWatcheDDr	Uste and imp 3/29/2021 6-3 3/29/2021 6-3 3/29/2021 6-3 3/29/2021 6-3 3/29/2021 6-3 3/29/2021 6-3 3/29/2021 6-3 3/29/2021 6-1 3/29/2021 6-1 3/29/2021 6-1 3/29/2021 6-1	e 127 PM 127 PM 127 PM 127 PM 127 PM 127 PM 127 PM 127 PM 127 PM 127 PM 128 PM 129 PM 129 PM 129 PM	Source FilterManager FilterMan	×	Open Saved Log Open Saved Log Open Saved Log Import Custor View Clear Log Filer Current Log Filer C
	URRO". The filt condition. If t Log Name: Source: Event ID: Level: User: OpCode: More Informati	er furthjolin rrecting his condition persists, cont System FilterManager 4 Warning SYSTEM Info	In the status of the second act the vendor. Logged: Task Category: Keywords: Computer:	2024. This filter and/or its supporting 3/29/2021 6:31:27 PM : None DESKTOP-3MU806	applications should handle this	v	Attach Task to Parket Attach Task To This Event Copy Save Selected Events Refresh Help



The Registry



Registry

Hierarchical database
 Stores low-level settings

Computer\HKEY_LOCAL_MACHINE



- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG



<u>NetDef</u>

Registry cont.

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server

🗸 😓 Computer	^	Name	Туре	Data
> 📙 HKEY_CLASSES_ROOT		(Default)	REG_SZ	(value not set)
> HKEY_CURRENT_USER		BAIIowRemoteRPC	REG_DWORD	0x0000000 (0)
✓ HKEY_LOCAL_MACHINE		🕮 DelayConMgrTi	REG_DWORD	0x0000000 (0)
> BCD0000000		BeleteTempDirs	REG_DWORD	0x00000001 (1)
> A HARDWARE		fDenyTSConnecti	REG_DWORD	0x00000001 (1)
		BingleSessionPe	REG_DWORD	0x00000001 (1)
		BassSessionId	REG_DWORD	0x0000002 (2)
SYSTEM		ab InstanceID	REG_SZ	a768dfc0-b17d-495e-a613-c89b0f6
>]_ ActivationBroker		8 NotificationTime	REG_DWORD	0x0000000 (0)
> 📙 ControlSet001		PerSessionTemp	REG_DWORD	0x0000000 (0)
✓		ab ProductVersion	REG_SZ	5.1
V 📙 Control		RailShowallNotif	REG_DWORD	0x00000001 (1)
- [{7746D80F-97E0-4E26-9543-26B41FC22F79}		RCDependentSer	REG_MULTI_SZ	CertPropSvc SessionEnv
AccessibilitySettings		8 RDPVGCInstalled	REG_DWORD	0x00000001 (1)
		ab SnapshotMonitors	REG_SZ	1
AppReadiness		8 StartRCM	REG_DWORD	0x00000000 (0)
> Arbiters		TSUserEnabled	REG_DWORD	0x0000000 (0)
Audio				

BackupRestore

NetDef

Registry cont.

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server

v 🗢 Computer	<u>^</u>	Name	Туре	Data
Edit DWORD (32-bit) Value ×		ab (Default)	REG_SZ	(value not set)
		AllowRemoteRPC	REG_DWORD	0x0000000 (0)
V L Value name:		🔀 DelayConMgrTi	REG_DWORD	0x0000000 (0)
fDenyTSConnections		🔀 DeleteTempDirs	REG_DWORD	0x0000001 (1)
Value data: Base		fDenyTSConnecti	REG_DWORD	0x0000001 (1)
1 Nexadecimal		fSingleSessionPe	REG_DWORD	0x0000001 (1)
Decimal		GlassSessionId	REG_DWORD	0x0000002 (2)
▶		ab InstanceID	REG_SZ	a768dfc0-b17d-495e-a613-c89b0f6
OK Cancel		NotificationTime	REG_DWORD	0x0000000 (0)
		PerSessionTemp	REG_DWORD	0x0000000 (0)
V 📕 CurrentControlSet		ProductVersion	REG_SZ	5.1
V Control		RailShowallNotif	REG_DWORD	0x00000001 (1)
[7746D80F-97E0-4E26-9543-26B41FC22F79]		RCDependentSer	REG_MULTI_SZ	CertPropSvc SessionEnv
> AccessibilitySettings		RDPVGCInstalled	REG_DWORD	0x0000001 (1)
		SnapshotMonitors	REG_SZ	1
		🕮 StartRCM	REG_DWORD	0x0000000 (0)
> Arbiters		TSUserEnabled	REG_DWORD	0x0000000 (0)



Task Manager

NetDef

Task Manager

Provides high-level view of what is running

d Task Manager										
e Options View										
ocesses Performance Apphistory Startup Users Details Services										
		× 7%	40%	0%	0%	3%				
ame	Status	CPU	Memory	Disk	Network	GPU	GPU engine	Power usage	Power usage trend	
詞 Task Manager		1.2%	33.9 MB	0 MB/s	0 Mbps	0%		Low	Very low	
Zoom Meetings (32 bit) (2)		0.9%	154.1 MB	0 MB/s	0.5 Mbps	0.5%	GPU 0 - 3D	Low	Very low	
Desktop Window Manager		0.9%	71.3 MB	0 MB/s	0 Mbps	1.3%	GPU 0 - 3D	Low	Very low	
Razer Central (32 bit)		0.5%	45.8 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	
 OVRServer_x64.exe (CAPI: 1.58.0) 5daae4b95499-public SC:1781609 		0.4%	79.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
System		0.4%	0.1 MB	0.1 MB/s	0 Mbps	0.7%	GPU 0 - Copy	Very low	Very low	
Discord (32 bit) (3)		0.3%	200.3 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low	
Windows Audio Device Graph Isolation		0.3%	7.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
🙀 Windows Explorer		0.3%	77.8 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	
i WMI Provider Host		0.2%	4.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Steam Login (2)		0.2%	193.2 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low	
Malwarebytes Service		0.2%	245.0 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	
CTF Loader		0.2%	22.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Client Server Runtime Process		0.1%	1.4 MB	0 MB/s	0 Mbps	0.3%	GPU 0 - 3D	Very low	Very low	
OVR Redir		0.1%	1.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
ARMOURY CRATE User Session Helper		0.1%	16.0 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	
Razer Synapse Service Process (32 bit)		0.1%	17.7 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	
AsusCertService.exe (32 bit)		0.1%	1.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
G Service Host: Connected Devices Platform User Service_dd18eab		0.1%	8.9 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low	
Microsoft Text Input Application		0.1%	10.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Razer Synapse Service (32 bit)		0.1%	92.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Service Host: DNS Client		0.1%	3.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
③ SteelSeries Engine 3 Core		0.1%	65.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Service Host: Windows Management Instrumentation		0.1%	21.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
System interrupts		0.1%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Microsoft PowerPoint		0%	192.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Google Chrome (47)		0%	2,978.2 MB	0.1 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low	
VMware Authorization Service (32 bit)		0%	3.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Services and Controller app		0%	7.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Antimalware Service Executable		0%	742.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Service Host: Diagnostic Policy Service		0%	47.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Game Controller Mapping Service		0%	8.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
NO HxD Hex Editor		0%	13.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
2 Service Host: Network List Service		0%	3.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
 Discord (32 bit) 		0%	7.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low	
Fewer details									End task	
										4





How to open it?

antess	oets apps re		Wallua	LOCAL 3YS	tem
on Identity	Determines		Manual (Trig	Local Sen	vice
on Information	Facilitates t	Running	Manual (Trig	Local Sys	tem
on Layer Gateway	Provides su		Manual	Loca	
on Management	Processes in		Manual	Loca	Toolbars
ployment Service (Provides inf		Manual	Loca	
AccessManager Se	AssignedAc		Manual (Trig	Loca	Search
e Zone Updater	Automatica		Disabled	Loca	
rvice	This is Audi	Running	Manual (Trig	Loca	News and
ind Intelligent Tran	Transfers fil		Manual	Loca 🧹	Show Tasl
ind Tasks Infrastruc	Windows in	Running	Automatic	Loca	
ring Engine	The Base Fil	Running	Automatic	Loca	Show Peo
Drive Encryption	BDESVC hos		Manual (Trig	Loca	
el Backup Engine	The WBENG		Manual	Loca	Show Wir
h Audio Gateway S	Service sup		Manual (Trig	Loca	Show tou
n Support Service	The Bluetoo		Manual (Trig	Loca	511047 100
h User Support Ser	The Bluetoo		Manual (Trig	Loca	
ache	This service		Manual	Netv	Cascade
y Access Manager	Provides fac		Manual	Loca	Show win
ervice_65f7e	Enables opti		Manual	Loca	
ervice_dfere331		Running	Automatic	Loca	Show win
					Show the
Clipboard User S	Service				Task Man
s				~	Lock the t
0 🚄	. 49	.		*	Taskbar se

en .			
em			
Toolbars	>		
Search			
News and interests			
Show Task View button			
Show People on the taskbar			
Show Windows Ink Workspace button			
Show touch keyboard button			
Cascade windows			
Show windows stacked			
Show windows side by side			
Show the desktop			
Task Manager		ardSvc	~
Lock the taskbar			
Tackhar cettings			anne

ndows 10 Enterprise Eval Windows License is e 18362.19h1_release.19031 및 ↓₈ ↓₈ 5:20 PM ↓ 2/28/2022

All Apps Documents Settings	Photos	More 🔻
Best match		
Task Manager App	\rightarrow	
Settings		Task Manager
View system resource usage in Task Manager	>	Арр
		📑 Open
		🗟 Run as administrator
		Dpen file location
		-ta Pin to Start
		-🛱 Pin to taskbar
Ø task manager	-	H 🕥 🥖 🖿 🙋 🔍



Can be used to find the location a running executable.

~	🔛 MSBuil	d (32 bit)	1	0%	5.8 MB	0 MB/s	0 Mbps	Very low	
	🔍 MSBL	Collapse						-	
	Dunting	End task		0%	1.2 MD	0 MP/s	0 Mhns	Vendeur	
		Provide feedback		0%	I'' IND	U IVID/S	o ivibps	very low	
>	💷 Runtim	Resource values >		0%	3.6 MB	0 MB/s	0 Mbps	Very low	
>	🗾 Runtim	Create dump file		0%	1.1 MB	0 MB/s	0 Mbps	Very low	
>	🔅 Setting	Go to details	Ŷ	0%	0 MB	0 MB/s	0 Mbps	Very low	
>	🖶 Spoole	Open file location		0%	3.3 MB	0 MB/s	0 Mbps	Very low	
>	💷 Start	Search online		0%	11.9 MB	0 MB/s	0 Mbps	Very low	
>	Svstem	Properties		0%	2.6 MB	0 MB/s	0 Mbps	Very low	

Show the properties of an executable

> 📧 Microsoft Network	c Realtime Ins	0%	2.8 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft OneDriv	e	0%	13.5 MB	0 MB/s	0 Mbps	Very low	Very low
> 📧 Microsoft Software	e Protection P	0%	5.2 MB	0 MB/s	0 Mbps	Very low	Very low
🔒 Microsoft Window	s Search Filte	0%	1.1 MB	0 MB/s	0 Mbps	Very low	
> 🔒 Microsoft Window	s Search Inde	0%	5.2 MB	0.1 MB/s	0 Mbps	Very low	Very low
🔒 Microsoft Window	s Search Prot	0%	1.2 MB	0 MB/s	0 Mbps	Very low	Very low
 MSBuild (32 bit) 	Collapse	0%	6.0 MB	0 MB/s	0 Mbps	Very low	Very low
🔍 MSBuild	End task						
📧 Opera GX auto-u	Provide feedback	0%	0.9 MB	0 MB/s	0 Mbps	Very low	
📧 Opera GX auto-u;	Resource values >	0%	1.4 MB	0 MB/s	0 Mbps	Very low	
📧 Opera GX auto-u;	Create dump file	0%	0.9 MB	0 MB/s	0 Mbps	Very low	
📧 Opera GX auto-u;	Go to details	0%	1.3 MB	0 MB/s	0 Mbps	Very low	
🔘 Opera GX Internel	Open file location Search online	0.2%	1.4 MB	0.7 MB/s	0 Mbps	Very low	
🔘 Opera GX Internet	Properties	0.2%	1.5 MB	1.3 MB/s	0 Mbps	Very low	

MSBuild.exe Properties ×											
General Comp	patibility Security Details Previous Versions										
	MSBuild.exe										
Type of file:	Application (.exe)										
Description:	MSBuild	MSBuild									
Location:	C:\Program Files (x86)\Microsoft.NET\RedistList										
Size:	60.6 MB (63,570,788 bytes)										
Size on disk:	60.6 MB (63,574,016 bytes)										
Created:	Wednesday, October 20, 2021, 4:22:21 AM										
Modified:	Wednesday, October 20, 2021, 4:22:21 AM										
Accessed:	Today, February 28, 2022, 6 minutes ago										
Attributes:	Read-only Hidden Advanced										
Security:	This file came from another computer and might be blocked to help protect this computer.										
	OK Cancel Apply										

General Compatibility Security Details Previous Versions Property Value
Property Value Description MSBuild Type Application File description 16.9.0.195 Product name Microsoft® Product version 16.9.0.195 Copyright ®Microsoft Corporation. All rights reserved Size 60.6 MB Date modified 10/20/2021 4:22 AM Language Language Neutral Original filename MSBuild.dll



Event Viewer



Event Viewer

Log viewer for Windows

🛃 Event Viewer		-		×							
File Action View Help											
 Event Viewer (Local) Custom Views Windows Logs 	Event Viewer (Local) Overview and Summar	Event Viewer (Local)									
Image: Applications and Services Lo Image: Subscriptions	Coverview	Create Custom View Import Custom View									
	occurred on your	Connect to Another Computer									
	Summary of	View		•							
		Refresh									
	Event Type Event ~ Recently Viewed Nodes • Name • Log Summary • Loo Name • •	Help		Þ							
,		1									



Event Viewer

Can be opened by searching for "event" and clicking open





Event Viewer cont.

Logs are stored in a hierarchical structure

Event Viewer (Local)

- 📑 Custom Views
- 👔 Windows Logs
- Applications and Services Logs
 - 🛃 Subscriptions





Event Viewer cont.

Windows activities are stored within the "Windows Logs" folder



NetDef

Event Viewer cont.

Windows Logs are divided into 5 categories

Application

Logs related to some applications installed on system

- Security
 - Security related logs (authentication actions are found here)
- Setup

Installation of software on system (e.g., update installs are logged)

- System
 - Low-level system events
- Forwarded events

Events forwarded to local machine by remote machines





Event Viewer cont.

🔡 Event Viewer

Individual logs are listed in the middle pane

Custom Views Windows Logs Event UD Task Category Windows Logs Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management Audit S. 37/022 54827 Microsoft Will 5379 User Account Management	Event Viewer (Local)	Security Nun	mber of events: 32	,731			
Window Logs Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827. Microsoft WL 5379 User Account Management Audit S. 37/2022 54827 Microsoft Windows security Logget User Kont Name Key Microsoft Windows security Logget User Kont Name Key Microsoft Windows security Logget User Kont Management Key Microsoft Windows security Logget User Kont Key Wind Kont Manag	Custom Views	Keywords Da	ate and Time	Source	Event ID	Task Category	
I Security Security Security Security Security Security Step Audit S. 37/2022 S482.2 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.2 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.2 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.7 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.7 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.7 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.7 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.7 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.7 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.7 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.7 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.7 Microsoft Will S73 User Account Management Audit S. 37/2022 S482.7 Microsoft Will S73	Windows Logs	Audit S 3/	1/2022 5-49-27	Microsoft Wi	5370	Licer Account Management	
Initial Subscriptions Operation Setup Setup Microsoft Will System Initial Subscriptions Audit S. 37/2022 S4827 Microsoft Will System System Initial Subscriptions Audit S. 37/2022 S4827 Microsoft Will System System Audit S. 37/2022 S4827 Microsoft Will System System System Audit S. 37/2022 S4827 Microsoft Will System System System Audit S. 37/2022 S4827 Microsoft Will System System System Audit S. 37/2022 S4827 Microsoft Will System System System Audit S. 37/2022 S4827 Microsoft Will System System System Audit S. 37/2022 S4827 Microsoft Will System System System Audit S. 37/2022 S4827 Microsoft Will System System System Credential Manager credentials were read. System System System System Steprint ID System LAPTOP-2LNSC412 System Microsoft Will System System Credential Manager Credential Manager Credential Manager <td>Application</td> <td>Audit S 3/</td> <td>1/2022 5:48:27</td> <td>Microsoft Wi</td> <td>5379</td> <td>User Account Management</td> <td></td>	Application	Audit S 3/	1/2022 5:48:27	Microsoft Wi	5379	User Account Management	
Express Subscriptions	security	Q Audit S 3/	1/2022 5:48:27	Microsoft Wi	5379	User Account Management	
Proverded Events Audit 5. 3/1/2022 54827 Microsoft Will. 5379 User Account Management Audit 5. 3/1/2022 54827 Microsoft Will. 5379 User Account Management Audit 5. 3/1/2022 54827 Microsoft Will. 5379 User Account Management Audit 5. 3/1/2022 54827 Microsoft Will. 5379 User Account Management Audit 5. 3/1/2022 54827 Microsoft Will. 5379 User Account Management Audit 5. 3/1/2022 54827 Microsoft Will. 5379 User Account Management Audit 5. 3/1/2022 54827 Microsoft Will. 5379 User Account Management Audit 5. 3/1/2022 54827 Microsoft Will. 5379 User Account Management Audit 5. 3/1/2022 54827 Microsoft Will. 5379 User Account Management Audit 5. 3/1/2022 54827 Microsoft Will 5379 User Account Management Audit 5. 3/1/202 54827 Microsoft Will 5379 User Account Management Audit 5. 3/1/202 54827 Microsoft Will 5379 User Account Management Audit 5. 3/1/202 54827 Microsoft Will Solition Event 5379 User Account Management Subject: Security ID: Solition: Event 70P-21/NSC412 Event 600 Subject: Sec	System	Audit S. 3/	1/2022 5:48:27	Microsoft Wi	5379	User Account Management	
Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Wi. 5379 User Account Management Audit S. 3//2022 54827. Microsoft Windows security auditing. Event Size Microsoft Windows security is a read operation on stored credentials in Credential Manager. Ice Microsoft Windows security is a read operation on stored credentials in Credential Manager. Ice Microsoft Windows security is a read operation on stored credentials in Credential Manager. Ice Microsoft Windows security is a read operation on stored credentials in Credential Manager. Ice Microsoft Windows security is a read operation on stored credentials in Credential Manager. Ice Microsoft Windows security is a read operation on stored credentials in Credential Management Event ID: 5379 Kincosoft Windows security is a read operation on stored credentials Wicrosoft Windows Security is a read operation on stored credentials in Credential Management Event ID: 5379 Kincosoft Windows Security is a read operation on stored credentials Wicrosoft Windows Security is a read operation on stored credentials Wicrosoft Windows Security is a read operation on stored Credentials Wicrosoft Windows Securi	Eorwarded Events	Audit S. 3/	1/2022 5:48:27	Microsoft Wi.	5379	User Account Management	
Subscriptions Audit S. 3/1/2022 54827 Microsoft Will 5379 User Account Management Audit S. 3/1/2022 54827 Microsoft Will 5379 User Account Management Audit S. 3/1/2022 54827 Microsoft Will 5379 User Account Management Audit S. 3/1/2022 54827 Microsoft Will 5379 User Account Management Audit S. 3/1/2022 54827 Microsoft Will 5379 User Account Management Audit S. 3/1/2022 54827 Microsoft Will 5379 User Account Management Audit S. 3/1/2022 54827 Microsoft Will 5379 User Account Management Audit S. 3/1/2022 54827 Microsoft Will 5379 User Account Management Credential Manager credentials were read. Subject: Scurity ID: LAPTOP-2LNSC412/anthony Account Name anthony Account Vame anthony Account Vame Immerate Credentials This event occurs when a user performs a read operation on stored credential Manager. Log Name Security Source 3/1/2022 54827 PM Source Microsoft Windows security i Logged: 3/1/2022 54827 PM Event ID: 5379 Task Category: User Account Man	Applications and Services Logs	Audit S. 3/	1/2022 5:48:27	Microsoft Wi	5379	User Account Management	
Audit S. 31/2022 54827 Microsoft Wi 5379 User Account Management Audit S. 31/2022 54827 Microsoft Wi 5379 User Account Management Audit S. 31/2022 54827 Microsoft Wi 5379 User Account Management Audit S. 31/2022 54827 Microsoft Wi 5379 User Account Management Audit S. 31/2022 54827 Microsoft Windows security auditing. Security Management General Details Credential Manager credentials were read. Subject: Security ID: LAPTOP-2LNSC412(anthony Account Management Account Domain: LAPTOP-2LNSC412(anthony Account Management Logo Name: Security ID: LAPTOP-2LNSC412 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. Source: Microsoft Windows security: Logged: 31/2022 54827 PM Source: Microsoft Windows security: Logged: 31/2022 54827 PM Event ID: S379 Task Category: User Account Management Level: Information Keywords: Audit Succeas	Subscriptions	Audit S., 3/	1/2022 5:48:27	Microsoft Wi	5379	User Account Management	
Audit S. 3/1/2022 54827 Microsoft Wil. 5379 User Account Management Audit S. 3/1/2022 54827 Microsoft Wil. 5379 User Account Management Audit S. 3/1/2022 54827 Microsoft Wil. 5379 User Account Management Audit S. 3/1/2022 54827 Microsoft Wil. 5379 User Account Management Event 5379, Microsoft Windows security auditing. Event 5379, Microsoft Windows security auditing. Event 5379, Microsoft Windows security auditing. General Details Credential Manager credentials were read. Subject: Subject: Subject: Security ID: LAPTOP-2LNSC412/anthony Account Domain: LAPTOP-2LNSC412 Log on ID: Account Domain: LAPTOP-2LNSC412 Log on ID: Dec6037188 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. Microsoft Windows security + Logged: 31/2022 54827 PM Source: Microsoft Windows security + Logged: 31/2022 54827 PM Event ID: Size Event ID: Size Size Microsoft Windows security - LAPTOP-2LNSC412 OpCode Info User		Audit S., 3/	1/2022 5:48:27	Microsoft Wi	5379	User Account Management	
Audit S. 3/1/2022 54827. Microsoft Wi 5379 User Account Management Event 5379 Microsoft Windows security auditing. General Details Credential Manager credentials were read. Subject: Scurity ID: Account Name: anthony Account Ware: Enumerate Credentials Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. Source: Microsoft Windows security: Logged: 31/2022 54827 PM Source: Microsoft Windows security: Logged: 31/2022 54827 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: <t< td=""><td></td><td>Q Audit S., 3/</td><td>1/2022 5:48:27</td><td>Microsoft Wi</td><td>5379</td><td>User Account Management</td><td></td></t<>		Q Audit S., 3/	1/2022 5:48:27	Microsoft Wi	5379	User Account Management	
Audit S. 3/1/2022 54827		Audit S., 3/	1/2022 5:48:27	Microsoft Wi	5379	User Account Management	
Event 3378, Microsoft Windows security auditing. General Details Credential Manager credentials were read. Subject: Scurity ID: Account Name anthony Account Tomain: LAPTOP-2LN9C412(anthony Account Domain: LAPTOP-2LN9C412 Logon ID: Doc60A718B Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. Log Name: Security Source: Microsoft Windows security: Logged: 3/1/2022 54827 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success Use: N/A Compute: LAPTOP-2LNSC412 OpCode Information Keywords: Audit Success		Audit S., 3/	1/2022 5:48:27	Microsoft Wi	5379	User Account Management	
Event 3379, Microsoft Windows security auditing. General Details Credential Manager credentials were read. Subject: LAPTOP-2LN9C412(anthony Account Name: anthony Account Domain: LAPTOP-2LN9C412 boot Db: 0x60X188 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. Log Name: Security Source: Microsoft Windows security i Logged: 3//2022 54827 PM Event 1D: 5379 Event Signer: N/A Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LNSC412 OpCode: Information Keywords: Audit Success		<u></u>					
General Details Credential Manager credentials were read. Subject: Souriy ID: LAPTOP-2LN9C412(anthony) Account Domain: LAPTOP-2LN9C412 Logon ID: 0x60A7188 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. Log Name: Security Source: Microsoft Windows security i Source: Microsoft Windows security i Event ID: 5379 Task Category: User Account Management Level: Information Vise: N/A Computer: LAPTOP-2LN9C412 OpCode: Information Kevends: Audit Success Use: N/A Computer: More Information: Event Log Online Help		Event 5379, Mic	rosoft Windows s	ecurity auditing.			
Credential Manager credentials were read. Subject: Security ID: LAPTOP-2LN9C412(anthony Account Name: Lantony Account Name: LaPTOP-2LN9C412 Logon ID: 0x60A7188 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. Log Name: Security Source: Microsoft Windows security : Source: Microsoft Windows security : Event ID: 5379 Task Category: User Account Management Level: Information Vise: N/A Compute: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help		General Deta	ails				
Credential Manager credentials were read. Subject: Security ID: LAPTOP-2LN9C412_Lonthony Account Name: anthony Account Domain: LAPTOP-2LN9C412_LogOn/21 Logon ID: 0x60A7188 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. Log Name: Security Source: Microsoft Windows security: Logged: 3/1/2022 5/4827 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Keywords: Audit Success							
Subject: Security ID: LAPTOP-2LN9C412\anthony Account Domain: LAPTOP-2LN9C412\controls Log on ID: Ox60A7188 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. Log Name: Security Source: Microsoft Windows security / Logged: 3/1/2022 5/4827 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audi Success User: N/A Compute: LAPTOP-2LN9C412 OpCode: Info Keywords: Audi Success		Credential N	Manager credenti	als were read.			
Account Name: antiony Account Name: 0x60A7188 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. Log Name: Security Source: Microsoft Windows security i Source: Microsoft Windows security i Event ID: 5379 Task Category: User Account Management Level: Information Vise: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help		Subject:	curity ID:	LAPTOP-2L	.N9C412\anthony	/	
Logon ID: 0x60A7188 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. It is event occurs when a user performs a read operation on stored credentials in Credential Manager. Log Name: Security Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode Info Keywords: Audit Success More Information: Event Log Online Help Keywords: Audit Success		Ac	count Domain:	LAPTOP-2L	N9C412		
Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager. Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode Info More Information: Event Log Online Help		Lo	gon ID:	0x60A71B8			
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5:48:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help		Rei	ad Operation:	Enumerate	Credentials		
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help		This event o	occurs when a use	er performs a read o	peration on store	ed credentials in Credential Manag	er.
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help					peration on stor.		
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5:48:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info Hore Hore More Information: Event Log Online Help Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5:48:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Logged: 3/1/2022 5:48:27 PM Source: Microsoft Windows security i Logged: 3/1/2022 5:48:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log_Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x827 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x8:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5/48:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help							
Log Name: Security Source: Microsoft Windows security i Logged: 3/1/2022 5x827 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: <u>Event Log Online Help</u>							
Log Name: Security Logged: 3/1/2022 5x48:27 PM Source: Microsoft Windows security i Logged: 3/1/2022 5x48:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info Hore Information: Event Log Online Help							
Source: Microsoft Windows security i Logged: 3/1/2022 5x48:27 PM Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help		Log Name:	Security				
Event ID: 5379 Task Category: User Account Management Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help		Source:	Microsoft	Windows security a	Logged:	3/1/2022 5:48:27 PM	
Level: Information Keywords: Audit Success User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: <u>Event Log Online Help</u>		Event ID:	5379		Task Category:	User Account Management	
User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: <u>Event Log Online Help</u>		Level:	Informatio	on	Keywords:	Audit Success	
OpCode: Info More Information: <u>Event Log Online Help</u>		User:	N/A		Computer:	LAPTOP-2LN9C412	
More Information: Event Log Online Help		OpCode:	Info				
		More Inform	ation: Event Log	g Online Help			

NetDef

Event Viewer cont.

Individual logs vary in complexity
 Windows generates many logs

 Many of these logs are not helpful

An account was successfully logged on. Subject: Security ID: SYSTEM LAPTOP-2LN9C412\$ Account Name: Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 2 Restricted Admin Mode: Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: LAPTOP-2LN9C412\anthony Account Name: anthony Account Domain: LAPTOP-2LN9C412 Logon ID: 0x40A47CA Linked Logon ID: 0x40A47FD Network Account Name: Network Account Domain: -Logon GUID: Process Information: Process ID: 0x88c Process Name: C:\Windows\System32\svchost.exe Network Information: Log Name: Security Source: Microsoft Windows security ¿ Logged: 2/28/2022 4:53:53 PM Event ID: Task Category: 4624 Logon Level: Keywords: Audit Success Information User: N/A Computer: LAPTOP-2LN9C412 OpCode: Info More Information: Event Log Online Help



Event Viewer cont.

Event IDs

 Identifier numbers Microsoft assigns to types of events.

Resource for Security Event IDs

<u>https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx</u>

Event Viewer cont.



letdef

Event Viewer cont.

⇐ Windows Security Log Event ID 4624 ➡

4624: An account was successfully logged on

On this page

- · Description of this event
- Field level details
- Examples
- Discuss this event
- · Mini-seminars on this event

This is a highly valuable event since it documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. You can tie this event to logoff events 4634 and 4647 using Logon ID.

Win2012 adds the Impersonation Level field as shown in the example.

Win2016/10 add further fields explained below.

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and
Category • Subcategory	Logon/Logoff • Logon
Туре	Success
Corresponding events in Windows 2003 and before	528,540

Discussions on Event ID 4624

2022

• Where does descriptive text come from at the end of 4624?

• 4624 Type 3 Filtering Help

Security N	Number of events: 32,737	(!) New events available		
Filtered	: Log: Security; Source: ;	Event ID: 4624. Number of e	vents: 1,663	
Keywords	Date and Time	Source	Event ID	Task Category
🔍 Audit S	3/1/2022 6:13:59 PM	Microsoft Wi	4624	Logon
🔍 Audit S	3/1/2022 6:03:24 PM	Microsoft Wi	4624	Logon
🔍 Audit S	3/1/2022 6:03:22 PM	Microsoft Wi	4624	Logon
🔍 Audit S	3/1/2022 5:48:26 PM	Microsoft Wi	4624	Logon
🔍 Audit S	3/1/2022 5:47:27 PM	Microsoft Wi	4624	Logon
🔍 Audit S	3/1/2022 5:37:42 PM	Microsoft Wi	4624	Logon
🔍 Audit S	3/1/2022 5:36:37 PM	Microsoft Wi	4624	Logon
🔍 Audit S	3/1/2022 5:36:34 PM	Microsoft Wi	4624	Logon
🔍 Audit S	3/1/2022 5:35:36 PM	Microsoft Wi	4624	Logon
Audit S	3/1/2022 5:34:15 PM	Microsoft Wi	4624	Logon

Event 4624, Microsoft Windows security auditing

General Details

An account was successfully logged on.

Subject:									
	Security I	D:	SYSTEM						
	Account	Name:	LAPTOP-2LI	N9C412\$					
	Account	Domain:	WORKGROUP						
	Logon ID	:	UX3E7						
Logon Ir	nformation	1:							
	Logon Ty	pe:	5						
	Restricted	d Admin Mode:	ī.,						
	Virtual Ad	count:	No						
	Elevated	loken:	Yes						
Imperso	nation Lev	vel:	Impersonati	on					
New Log	jon:								
	Security I	D:	SYSTEM						
Account Name:			SYSTEM						
Account Domain:			NI AUTHOR	a i y					
	Linked Le	agon ID:	0x5E7						
	Network	Account Name:	-						
	Network	Account Domain	: -						
	Logon Gl	JID:	{0000000-0	000-0000-0000-0	000000000000000000000000000000000000000				
Process	Informatio	on:							
	Process II	D:	0x470						
	Process N	lame:	C:\Windows\System32\services.exe						
Network	Informati	ion:							
Log Nam	e:	Security							
Source:		Microsoft Windo	ows security a	Logged:	3/1/2022 6:13:59 P				
Event ID:	1	4624		Task Category:	Logon				
.evel:		Information		Keywords:	Audit Success				
Jser:		N/A		Computer:	LAPTOP-2LN9C412				
OpCode:		Info							
More Info	ormation:	Event Log Onlin	ne Help						







Event Viewer cont.

Event viewer sucks when trying to search logs in bulk.We can extract logs to a CSV file

	Security Number of events: 32,710 (!) New events available						Actions	
Custom Views	Keywords Date and Time Source	Event ID Task Category				^ ^	Security	•
Application	Audit S., 3/1/2022 6:16:02 PM Microsoft Wi.,	5379 User Account Management					🧑 Open Saved Log	
Security	Audit S., 3/1/2022 6:16:02 PM Microsoft Wi.,	5379 User Account Management					Y Create Custom View	
Setup	Audit S., 3/1/2022 6:16:02 PM Microsoft Wi.,	5379 User Account Management					Import Custom View	
System	Audit S. 3/1/2022 6:16:02 PM Microsoft Wi.	5379 User Account Management					Clear Lon	
Applications and Services Loos	Audit S. 3/1/2022 0:1002 PM Microsoft Wi.	5379 User Account Management					T Elter Current Ion	
Subscriptions	Audit S., 3/1/2022 6:16:02 PM Microsoft Wi.,	5379 User Account Management					Prive content cog	
	Q Audit S 3/1/2022 6:16:02 PM Microsoft Wi	5379 User Account Management					00 automotion	
	Audit S., 3/1/2022 6:16:02 PM Microsoft Wi.,	5379 User Account Management					We Find_	
	Audit S., 3/1/2022 6:16:02 PM Microsoft Wi.,	5379 User Account Management					Save All Events As	
	Audit S. 3/1/2022 6:16:02 PM Microsoft Wi.	5379 User Account Management				~	Attach a Task To this Log	
	Event 5379, Microsoft Windows security auditing.					×	View	,
	Con El const				~]		Refresh	
	Ge a save As				~		R Help	,
	c ← → ~ ↑ ■ · anthony · Desktop		~	Ö Search Desktop	1		Event 5379, Microsoft Windows security auditing.	
	S Organize - New folder				B: - 0		Event Properties	
					0		Attach Task To This Event	
	Desktop # Name	Date modified	Type Size				Save Selected Events	
	Downloads # CPTC	11/13/2021 12:11 PM	File folder				Copy	
	📓 Documents 🥒						G Refresh	
	1 E Pictures 🖈							
	📙 Anayl						Comp.	
	Discrete							
	SysSec							
	UB Files							
	This MC							
	= insic							
	J SO Objects							
	Desktop							
	2 Documents							
	Downloads							
	🎝 Music 🧹							
	File name: Security				-			
	Save as type: CSV (Comma Separated) (*.csv)							
	Sq ^ Hide Folders			Save	Cancel			
	Event ID: 5379 Task Ca	tegory: User Account Management						
	Level: Information Keywor	ds: Audit Success						



Event Viewer cont.

Excel can interpret these logs and be used to search them.
 The CSV must be imported properly



Importing Logs in Excel

₽ 5°∂°																		S	ign in			
File Home	Insert Pag	e Layout For	rmulas Da	ata Revie	w View	Developer	Help														∕⊊ Share	e
Get From Fro Data • Text/CSV We	om From Table leb Range Get & Transform I	/ Recent Ex Sources Con Data	kisting Re nections A	efresh All + Queries	eries & Conr operties It Links & Connection	nections 2	↓ <mark>⊼ 2</mark> ↓ Sort	Filter	tvanced C	Text to Flas Columns Fil	h Remove Duplicate	e Data es Validation Data	Consolida • Tools	te Relations	hips Mana Data M	ge Wha odel Analy	it-If Foreca rsis - Sheet Forecast	st Group	Jngroup Su	tline		~
		fx																				^
A 1 2 3 3 4 5 6 6 7 7 8 9 10 11 12 13 13 14 15 16	8 C	D	E	F	G	H			K		M	N	0	P	Q	R	S	T	U			
17 18 19 20 21 22 23 24 25 26 She	eet1												4						8			



Importing Logs in Excel

Coganize New folder Organize New folder Outick access Desktop Downloads Downloads Downloads Pictures Anayl Discrete SysSec UB Files Microsoft Excel This PC Downloads File name: Security.esv File name: Security.esv Tools Tools Import Cancel	XII Import Data								>	
Organize New folder Quick access Desktop Downloads Downloads Downloads Pictures Anayl Disrete SysSec U BF files Microsoft Excel SysSec Dobjects Desktop Documents Documents Downloads File name: Security.csv Tools Import Cancel	\leftarrow \rightarrow \checkmark \uparrow \blacksquare > This PC > Desktop	× ت)	Q	Sear	ch De	sktop			
Quick access Desktop Documents Crc SysSec UB Files Microsoft Excel This PC Documents Documents	Organize • New folder						•		?	
File name: Security.csv Tools ▼ Import Cancel	Quick access Desktop Downloads Documents Documents Documents Pictures Anayl Discrete SysSec UB Files Microsoft Excel This PC 3D Objects Desktop Documents									
File name: Security.csv Iext Files (*.pm,*.btt;*.csv) Tools Import Cancel	Downloads		_	-						
	File name: Security.csv	Tools	•	ſex	t Files	(*.prn;' rt	".txt;*.c	sv) Cance	× I	

Importing Logs in Excel

Security.csv

<

File Origin			Delimiter		Data Type Detection		
65001: Unico	de (UTF-8)	-	Comma	*	Based on first 200 rows	*] 🗋
Keywords	Date and Time		Source	Event ID	Task Category		
Audit Success	3/1/2022 6:21:00 PM	Micros	oft-Windows-Security-Auditing	4798	User Account Management	A user's local gro	up membership was enur
Audit Success	3/1/2022 6:21:00 PM	Micros	oft-Windows-Security-Auditing	4798	User Account Management	A user's local gro	up membership was enur
Audit Success	3/1/2022 6:20:54 PM	Micros	oft-Windows-Security-Auditing	4798	User Account Management	A user's local gro	up membership was enur
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
Audit Success	3/1/2022 6:16:02 PM	Micros	oft-Windows-Security-Auditing	5379	User Account Management	Credential Manag	ger credentials were read
•							Ť

Load 🔻 Transform Data Cancel

Logs in Excel

1 Key	words 💌	Date and Time 💌	Source 🗸	Event ID 💌	Task Categor	/	Column1
2 Audi	it Success	3/1/2022 18:21	Microsoft-Windows-Security-Auditing	4798	User Account	Management	A user's local group membership was enumerated.Subject:Security ID:LAPTOP-2LN9C412\anthony
3 Audi	it Success	3/1/2022 18:21	Microsoft-Windows-Security-Auditing	4798	User Account	Management	A user's local group membership was enumerated.Subject:Security ID:LAPTOP-2LN9C412\anthony
4 Audi	it Success	3/1/2022 18:20	Microsoft-Windows-Security-Auditing	4798	User Account	Management	A user's local group membership was enumerated.Subject:Security ID:LAPTOP-2LN9C412\anthony
5 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
6 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
7 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
8 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
9 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
10 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
11 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
12 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
13 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
14 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
15 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
16 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
17 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
18 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
19 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
20 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
21 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
22 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
23 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
24 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
25 Audi	t Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
26 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
27 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
28 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
29 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
30 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
31 Audi	t Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
32 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
33 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
34 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
35 Audi	t Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
36 Audi	t Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
37 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
38 Audi	t Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
39 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
40 Audi	it Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account	Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
Logs in Excel

Within Excel we can search logs using filters.

	A	В		<u> </u>		E	F
1	Keywords 💌	Date and Time 💌	Source	· · · · · · · · · · · · · · · · · · ·	Event ID 💌	Task Category 🛛	Column1
	Audit Success	3/1/2022 18:21	Micros 🗍	Sort Smallest to Largest		User Account Management	A user's local group membership was enumerated.Subject:Security ID:LAPTOP-2LN9C412\anthonyA
	Audit Success	3/1/2022 18:21	Micros ZJ	Sort Largest to Smallest		User Account Management	A user's local group membership was enumerated.Subject:Security ID:LAPTOP-2LN9C412\anthonyA
	Audit Success	3/1/2022 18:20	Micros	Sort by Color		User Account Management	A user's local group membership was enumerated.Subject:Security ID:LAPTOP-2LN9C412\anthonyA
	Audit Success	3/1/2022 18:16	Micros	Sort by Color		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros			User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros			User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros	Number Filters		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros	Humber Litters		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros	Search	۶	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micro	(Select All)	^	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros	-1100		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros	4608		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros	4674		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros			User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros			User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros			User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros			User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros			User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros			User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros			User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros			User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros	4799	~	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros			User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros	ОК	Cancel	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Micros		.:	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
34	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
38	Audit Success	3/1/2022 18:16	Microsoft	-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount

Logs in Excel

	A	В	C	D	E	F
1	Keywords 👱	Date and Time 💌	Source	Event ID 🍼	Task Category 🗾 💌	Column1 🔹
81	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
83	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
85	Audit Success	3/1/2022 18:13	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
87	Audit Success	3/1/2022 18:03	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
89	Audit Success	3/1/2022 18:03	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
185	Audit Success	3/1/2022 17:48	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
187	Audit Success	3/1/2022 17:47	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
206	Audit Success	3/1/2022 17:37	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
322	Audit Success	3/1/2022 17:36	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
494	Audit Success	3/1/2022 17:36	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
891	Audit Success	3/1/2022 17:35	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
903	Audit Success	3/1/2022 17:34	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
904	Audit Success	3/1/2022 17:34	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1476	Audit Success	3/1/2022 17:33	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1494	Audit Success	3/1/2022 17:33	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1500	Audit Success	3/1/2022 17:33	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1502	Audit Success	3/1/2022 17:33	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1503	Audit Success	3/1/2022 17:33	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1510	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1512	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1516	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1524	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1528	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1529	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1531	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1537	Audit Success	2/28/2022 22:40	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1607	Audit Success	2/28/2022 22:40	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1609	Audit Success	2/28/2022 22:39	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1611	Audit Success	2/28/2022 22:39	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1614	Audit Success	2/28/2022 22:22	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1616	Audit Success	2/28/2022 22:08	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1618	Audit Success	2/28/2022 22:08	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41



Homework Hint

The initial vector of breach is in the Windows logs.
The attack was a brute force attack against one of the Windows remote access tools.



Questions?



Network Forensics

Network Forensics Hands-on

- Sign onto the machine in your team folder called "WINIRForClass"
 - Username: sysadmin
 - Password: Change.me!



Wireshark

Packet analyzer
Free
Open-source
Available on:

Windows
Linux
MacOS





In Class Activity WireShark



Hands on 0 - Wireshark

Locate suspicious network trafficCreate a Windows firewall rule to block the traffic

Network Forensics Hands-on

The Wireshark Network Analyzer	-	σx	
e Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help			
II 2 0 I C C C C C C C C C C C C C C C C C C			
Apply a display filter <ctrl-></ctrl->			
Welcome to Wireshark			
Open			
C:\Users\sysadmin\Documents\cSharpServiceTraffic.pcapng (4700 Bytes)			
Canture			
	▼ All interfaces shown ▼		
Local Area Connection* 8 Local Area Connection* 7 Local Area Connection* 6			
Adapter for loopback traffic capture			
Learn			
User's Guide Wiki Questions and Answers Mailing Lists			
You are running Wireshark 3.6.0 (v3.6.0-0-g3a34e44d02c9). You receive automatic updates.			
Ready to load or capture	No Packets	Profile: Default	
		11	













PowerShell For IR



PowerShell

Automation and configuration tool

<u>https://docs.microsoft.com/en-us/powershell/</u>

Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\anthony>

Cmdlets

Cmdlets are commands in PowerShell
 Cmdlets use verb-noun format

 Get-computerinfo
 Get-filehash
 Write-output
 Etc...



Get-Filehash

"Computes the hash value for a file by using a specified hash algorithm."



In Class Activity PowerShell

Hands on 1 – Piping Output

- Compute the SHA384 hash of test.exe on your desktop using get-filehash
- Get-Filehash documentation
 - <u>https://tinyurl.com/yw9zv3cw</u>



Hands on 1 – Piping Output

Any problems with the result?

Hands on 1 – Piping Output

We can send output from one command to another
 Output of command 1 is sent to command 2

 Ex: <command_1> | <command_2>

 Using the documentation below what command can we pipe to for the fix the output?

 <u>https://tinyurl.com/yw9zv3cw</u>

Searching PowerShell Output

Get-Service "Gets the services on the computer."

Service 4dd2c3d es Platform Service s Platform User Ser... agation Click-to-Run Service ervice (ClipSVC) ication

Protection HECI Se... Protection HDCP Se... mentManagerUserSvc ... rvices ess Launcher

ervice r Gateway Service rmation gement Client Service (AppXSVC) nager Service dpoint Builder (AxInstSV) dcast User Service ... ncryption Service ligent Transfer Ser.. pport Service 4dd2c3d Infrastructure Ser... Gateway Service

PS C:\Users\anthony> get-service

Status Namo

DisplayName

Stopped	AarSvc 4dd2c3d	Agent Activation Runtime 4dd2c3d
Running	AdobeARMservice	Adobe Acrobat Update Service
Running	AESMService	Intel® SGX AESM
Stopped	AJRouter	AllJoyn Router Service
Stopped	ALG	Application Layer Gateway Service
Stopped	AppIDSvc	Application Identity
Running	Appinfo	Application Information
Stopped	AppMgmt	Application Management
Stopped	AppReadiness	App Readiness
Stopped	AppVClient	Microsoft App-V Client
Running	AppXSvc	AppX Deployment Service (AppXSVC)
Stopped	AssignedAccessM	AssignedAccessManager Service
Running	AudioEndpointBu	Windows Audio Endpoint Builder
Running	Audiosrv	Windows Audio
Stopped	autotimesvc	Cellular Time
Stopped	AxInstSV	ActiveX Installer (AxInstSV)
Stopped	BcastDVRUserSer	GameDVR and Broadcast User Servic
Running	BDESVC	BitLocker Drive Encryption Servic
Stopped	BEService	BattlEye Service
Running	BFE	Base Filtering Engine
Stopped	BITS	Background Intelligent Transfer S
Stopped	BluetoothUserSe	Bluetooth User Support Service_4d
Running	BrokerInfrastru	Background Tasks Infrastructure S
Running	BTAGService	Bluetooth Audio Gateway Service
Running	BthAvctpSvc	AVCTP service
Running	bthserv	Bluetooth Support Service
Running	camsvc	Capability Access Manager Service
Stopped	CaptureService	CaptureService_4dd2c3d
Running	cbdhsvc_4dd2c3d	Clipboard User Service_4dd2c3d
Running	CDPSvc	Connected Devices Platform Servic
Running	CDPUserSvc_4dd2c3d	Connected Devices Platform User S
Stopped	CertPropSvc	Certificate Propagation
Running	ClickToRunSvc	Microsoft Office Click-to-Run Ser
Running	ClipSVC	Client License Service (ClipSVC)
Stopped	COMSysApp	COM+ System Application
Stopped	ConsentUxUserSv	ConsentUX_4dd2c3d
Running	CoreMessagingRe	CoreMessaging
Running	cphs	Intel(R) Content Protection HECI
Running	cplspcon	Intel(R) Content Protection HDCP
Stopped	CredentialEnrol	CredentialEnrollmentManagerUserSv
Running	CryptSvc	Cryptographic Services
Stopped	CscService	Offline Files
Rupping	Deaml aunch	DCOM Sonyon Process Launchon





Hands on 2 – Searching Output

Run get-service

Runget-service | select *

What is the difference of the output?

vetoef

Hands on 2 – Searching Output

PS C:\Users\anthony> get-service

Status Name Running AarSvc 197f19e7 Running AdobeARMservice Running AESMService Stopped AJRouter Stopped ALG Stopped AppIDSvc Running Appinfo Stopped AppMgmt Stopped AppReadiness Stopped AppVClient Stopped AppXSvc Running Audiosrv Stopped autotimesvc Stopped AxInstSV Running BDESVC Stopped BEService Running BFE Stopped BITS Running BTAGService Running BthAvctpSvc Running bthserv

DisplayName

Agent Activation Runtime 197f19e7 Adobe Acrobat Update Service Intel® SGX AFSM AllJoyn Router Service Application Layer Gateway Service Application Identity Application Information Application Management App Readiness Microsoft App-V Client AppX Deployment Service (AppXSVC) Stopped AssignedAccessM... AssignedAccessManager Service Running AudioEndpointBu... Windows Audio Endpoint Builder Windows Audio Cellular Time ActiveX Installer (AxInstSV) Stopped BcastDVRUserSer... GameDVR and Broadcast User Service_... BitLocker Drive Encryption Service BattlEve Service Base Filtering Engine Background Intelligent Transfer Ser... Stopped BluetoothUserSe... Bluetooth User Support Service 197f... Running BrokerInfrastru... Background Tasks Infrastructure Ser... Bluetooth Audio Gateway Service AVCTP service Bluetooth Support Service

PS C:\Users\anthony> get-service | select * | format-list

Name	AarSvc_197f19e7
RequiredServices	0
CanPauseAndContinue	False
CanShutdown	False
CanStop	True
DisplayName	Agent Activation Runtime 197f19
DependentServices	ñ –
MachineName	
ServiceName	AarSvc 197f19e7
ServicesDependedOn	0
ServiceHandle	
Status	Running
ServiceType	240
StartType	Manual
Site	
Container	
concarner	
Namo	AdoboABMconvico
RequiredServices	AUDDEANNISEI VICE
ConPousoAndContinuo	U Folco
CanFauseAndContinue	False
CanSton	Tause
	Adaha Asnahat Undata Samuisa
	n
MashiasNama	V.
NachineName Somui soNomo	• Adaha APMsamui sa
ServiceName	Adobearmservice
ServicesDependedOn	17
Servicenandie	Duration
Status	Kunning
ServiceType	winszownProcess
StartType	Automatic
Site	
Container	
	AF 6145
Name	ACSINSERVICE
RequiredServices	{RPCSS}
CanPauseAndContinue	False
CanShutdown	False
CanStop	True
DisplayName	Intel® SGX AESM
DependentServices	0
MachineName	
ServiceName	ALSMService
ServicesDependedOn	{RPCSS}
ServiceHandle	
Status	Running
ServiceType	Win320wnProcess
StartType	Automatic
Site	
Containon	

Hands on 2 – Searching Output

- List <u>ONLY</u> services that have a <u>StartType</u> as automatic
 Ensure the output <u>DOESN'T</u> get trimmed
- Use the below documentation
 - <u>https://tinyurl.com/z5psdn87</u>



WMI & Services.

Windows Management Instrumentation (WMI)

Can be used to manage Windows devices
 Allows remote communications through:

 Distributed Component Object Model (DCOM)
 Windows Remote Management (WINRM)

 Great tool for IT personnel and malicious actors

Services

Behind the scenes to keep things working
4 startup types
Automatic (Delayed Start)
Automatic
Manual
Disabled

General	Log On	Recovery	Dependencies			
Service	name:	AdobeARM	Iservice			
Display	name:	Adobe Acr	obat Update Ser	rvice		
Descrip	tion:	Adobe Acr up to date	robat Updater ke	eps your Ado	be software	Ŷ
Path to "C:\Pro	executabl gram Files	e: (x86)\Comm	non Files∖Adobe`	\ARM\1.0\ar	msvc.exe"	
Startup	type:	Automatic	:			~
Service	status : itart	Running Stop	p Pi	ause	Resume	_
You car from be	n specify t re.	he start para	meters that appl	y when you s	tart the service	e

Services

Can run as nt authority \system

nt authority \system!= root
Is more powerful than an "administrator"

Active even when no user is signed in
May be hosted by the service host (svchost.exe)
May executables that are designated to be services
Follow a defined service model



Service Model



How to list services?

Open Task Manager and navigate to services tab

👰 Task Manager					
File Options View					
Processes Performance A	pp history	Startup	Users	Details	Services
Name	PID	Descri	iption		1
AarSvc		Agent	Activat	tion Runt	ime
AarSvc_65f7e		Agent	Activat	tion Runt	inne_65f7
AJRouter		AllJoy	n Route	er Service	
ALG		Applic	cation L	ayer Gat	way Serv
AppIDSvc		Applic	cation lo	dentity	-
Appinfo	5348	Applic	cation li	nformatio	n
AppMgmt		Applic	cation N	/lanagem	ent
AppReadiness		App R	eadines	is 🖌	
AppVClient		Micro	soft Ap	p- Clien	t
AppXSvc		АррХ	Deploy	n ent Ser	vice (App
AssignedAccessManager	òvc	Assign	nedAcc	ssManad	jer Servic
AudioEndpointBuilder	2176	Windo	ows Au	dio Endpo	oint Build
Audiosrv	2324	Winde	ows Au	dio .	
autotimesvc		Cellul	ar Tine		
🔍 AxInstSV		Active	X Unstal	ller (AxIn	stSV)
BcastDVRUserService		Game	D R an	d Broadc	ast User S
BcastDVRUserService_65f7	/e	Game	VR an	d Broadc	ast User S
SDESVC		BitLo	ker Driv	e Encryp	tion Serv
🔍 BFE	2504	Base	iltering	Engine	
🔍 BITS	3416	Backg	round l	ntelligen	t Transfer
BluetoothUserService		Blueto	ooth Us	er Suppo	t Service
BluetoothUserService_65f	7e	Flueto	ooth Us	er Suppo	t Service
SrokerInfrastructure	856	Backg	round	Tasks Infra	astructur
STAGService		Blueto	ooth Au	dio Gatev	vay Servi
🔍 BthAvctpSvc	7120	AVCT	P servic	e	
k bthserv		Blueto	ooth Su	pport Ser	vice
amsvc		Capab	oility Ac	cess Mar	ager Serv
CaptureService	I	Captu	reServi	ce	
CaptureService_65f7e		Captu	reServi	ce_65f7e	
CaptureService_dfere331	3,36	Captu	reServi	ce_dfere3	31
🔍 cbdhsvc		Clipbo	oard Us	er Service	

Services List

🌼 Services						- 🗆 X	(
File Action View Hel	lp						
← → 🔲 🖬 🔒	2 📷 🕨 🕨 🔳 💷 🕪						_
Services (Local)	Services (Local)						
Selec	ect an item to view its description.	Name	Description	Status	Startup Type	Log On As	^
		ActiveX Installer (AxInstSV)	Provides Us		Manual	Local System	
		Agent Activation Runtime	Runtime for		Manual	Local System	
		AllJoyn Router Service	Routes AllJo		Manual (Trig	Local Service	
		🆏 App Readiness	Gets apps re		Manual	Local System	
		Application Identity	Determines		Manual (Trig	Local Service	
		Application Information	Facilitates t	Running	Manual (Trig	Local System	
		🎑 Application Layer Gateway	Provides su		Manual	Local Service	
		Application Management	Processes in		Manual	Local System	
		🍓 AppX Deployment Service (Provides inf		Manual	Local System	
		🍓 AssignedAccessManager Se	AssignedAc		Manual (Trig	Local System	
		🍓 Auto Time Zone Updater	Automatica		Disabled	Local Service	
		AVCTP service	This is Audi	Running	Manual (Trig	Local Service	
		🍓 Background Intelligent Tran	Transfers fil		Manual	Local System	
		🖏 Background Tasks Infrastruc	Windows in	Running	Automatic	Local System	
		🍓 Base Filtering Engine	The Base Fil	Running	Automatic	Local Service	
		🖏 BitLocker Drive Encryption	BDESVC hos		Manual (Trig	Local System	
		🔍 Block Level Backup Engine	The WBENG		Manual	Local System	
		🔍 Bluetooth Audio Gateway S	Service sup		Manual (Trig	Local Service	
		Sluetooth Support Service	The Bluetoo		Manual (Trig	Local Service	
		Sluetooth User Support Ser	The Bluetoo		Manual (Trig	Local System	
		StanchCache	This service		Manual	Network Service	
		🖓 Capability Access Manager	Provides fac		Manual	Local System	
		😪 CaptureService_65f7e	Enables opti		Manual	Local System	
	,,	CaptureService_dfere331		Running	Automatic	Local System	۷

Services List

Services (Local)

Cryptographic Services

Stop the service Restart the service

Description:

Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be installed; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Automatic Root Certificate Update Service, which retrieves root certificates from Windows Update and enable scenarios such as SSL. If this service is stopped, these management services will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

*				
Name	Description	Status	Startup Type	Log On As
Client License Service (ClipS	Provides inf		Manual (Trig	Local System
🆏 Clipboard User Service_65f7e	This user ser	Running	Manual	Local System
🧠 CNG Key Isolation	The CNG ke	Running	Manual (Trig	Local System
🥋 COM+ Event System	Supports Sy	Running	Automatic	Local Service
🥋 COM+ System Application	Manages th	Running	Manual	Local System
🎑 Connected Devices Platfor	This service	Running	Automatic (Local Service
🎑 Connected Devices Platfor	This user ser	Running	Automatic	Local System
🧠 Connected User Experience	The Connec		Disabled	Local System
🎑 ConsentUX_65f7e	Allows Con		Manual	Local System
🥋 Contact Data_65f7e	Indexes con	Running	Manual	Local System
🎑 CoreMessaging	Manages co	Running	Automatic	Local Service
🎑 Credential Manager	Provides se	Running	Manual	Local System
CredentialEnrollmentMana	Credential E		Manual	Local System
Cryptographic Services	Provides thr	Running	Automatic	Network Service
Data Sharing Service	Provides da		Manual (Trig	Local System
🥋 Data Usage	Network da	Running	Automatic	Local Service
DCOM Server Process Laun	The DCOML	Running	Automatic	Local System
Delivery Optimization	Performs co		Automatic (Network Service
Device Association Service	Enables pair		Manual (Trig	Local System
Device Install Service	Enables a c		Manual (Trig	Local System
🔍 Device Management Enroll	Performs D		Manual	Local System
Device Management Wirele	Routes Wire		Manual (Trig	Local System
Device Setup Manager	Enables the		Manual (Trig	Local System
DeviceAssociationBroker_65	Enables app		Manual	Local System

Extended Standard

Services List

Services (Local)

Cryptographic Services

Stop the service Restart the service

Description:

Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be installed: Protected Root Service. which adds and removes Trusted Root Certification Authority certificates from this computer; and Automatic Root Certificate Update Service, which retrieves root certificates from Windows Update and enable scenarios such as SSL. If this service is stopped, these management services will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

 Name
 Description

 Q Client License Service (ClipS...
 Provides inf...

 Q Clipboard User Service_657e
 This user ser...

 Q Clopboard User Service_657e
 This user ser...

 Q COM+ Event System
 Supports Sy...

 Q COM+ Event System
 Supports Sy...

 Q COM+ System Application
 Manages th...

 Q Connected Devices Platfor...
 This user ser...

 Q Connected Devices Platfor...
 The Connec...

 Q ConsentUX_65f7e
 Allows Con...

 Q Contact Data_65f7e
 Indexes con...

 Q Credential Manager
 Provides se...

 Q CredentialEnrollmentMana...
 CredentialEnrollmentMana...

Start

Stop

Pause

Resume

Restart

All Tasks

Refresh

Help

Properties

🔍 Data Sharin

🖏 Data Usage

DCOM Serv

Delivery Op

Device Asso

Device Insta

🔍 Device Mar

💁 Device Mar

🔍 Device Setu

DeviceAsso

Status Description Startup Type Manual (Trig... This user ser... Running Manual The CNG ke... Manual (Trig... Running Supports Sy... Running Automatic Running Manages th... Manual This service ... Running Automatic (... This user ser... Running Automatic The Connec... Disabled Allows Con... Manual Manual Indexes con... Running Manages co... Running Automatic Provides se... Running Manual Credential E... Manual Provides thr... Running Automatic

> da... Manual (Trig... Local System da.. Running Automatic Local Service ML... Local System Running Automatic Network Service Automatic (... co... pair... Manual (Trig... Local System Manual (Trig... Local System c.... s D.... Manual Local System > Manual (Trig... Local System /ire... he ... Manual (Trig... Local System Manual Local System app...

Log On As

Local System

Local System

Local System

Local Service

Local System

Local Service

Local System

Local System

Local System

Local System

Local Service

Local System

Local System

Network Service

urrent selection.

Extended (Standard)

Services List

Cryptographic Services Properties (Local Computer)

 \times

General	Log On	Recovery	Dependencies							
Service name:		CryptSvc	CryptSvc							
Display name:		Cryptograp	Cryptographic Services							
Descript	tion:	Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be								
Path to	executabl	e.								
C-\Wine	lowe\evet	o. am 20\avebo	et eve Jr. Networ	k Service .n						
C. WVIIIC	Jows syst	CIII JZ ASVCI IU	SLEXE TO NELWOR	KJelvice p						
Startup type:		Automatic								
		Automatic Automatic Manual	(Delayed Start)							
Service	status:	Disabled Running								
S	tart	Stop	p Pa	iuse Resume	e:					
You car from her	n specify ti re.	he start para	meters that apply	when you start the sen	vice					
Start pa	rameters:									
			OK	Cancel /	hophy					

Services List

Cryptographic Services P		×	
General Log On Reco	very Dependencies		
Log on as:			
O Local System accourt	t		
Allow service to in	teract with desktop		
This account:	Network Service	Browse	K
Password:	•••••		
Confirm password:	•••••		

OK

Cancel

Apply

<u>NetDef</u>

Services List

Cryptographic Services Properties (Local Computer)

General Log On Recovery Dependencies

Select the computer's response if this service fails. Help me set up recovery actions.

×

 \sim

 \sim

Apply

First failure:	Restart the Service				
Second failure:	Take No Ac	tion			
Subsequent failures:	Take No Action				
Reset fail count after:	1	days			
Restart service after:	1	minutes			
Enable actions for stops wit	th errors.	Restart Comp	outer Options		
Run program					
Program:					
			Browse		
Command line parameters:					
Append fail count to end	l of command	line (/fail=%1°	%)		
	OK	Cance	App		

Services List

Cryptographic Services Properties (Local Computer)

General Log On Recovery Dependencies

Some services depend on other services, system drivers or load order groups. If a system component is stopped, or is not running properly, dependent services can be affected.

×

Cryptographic Services

This service depends on the following system components:

The following system components depend on this service:

OK Cancel Apply


In Class Activity

Find a Malicious Service



Hands on 3- Find a Malicious Service

Use the previous command we learned Get-WmiObject win32_Service ■ Add | ogv at the end Attackers often want constant access What StartType would an attacker use? If you see something say something Google anything suspicious Legitimate applications break often and people post online about them Remove the malicious service Hint[0]: sc delete <service name> Hint[1]: Can services be processes? 0





Hands on 3- Delete a Malicious Service

1. <REDACTED>

2. Using **Command Prompt**, enter: <**REDACTED**>

3. Reboot



RESTART YOUR WINDOWS VM



Persistence

Persistence

- Malware aims to survive
 - Restart
 - Settings Changes
 - Users signing on/off
 - Network connectivity loss
 - Countermeasures
 - Systems updates
 - Anything else....

Netnef

Persistence Methods

- Windows persistence methods and their complexity
 - Drivers (HIGH)
 - Registry Keys (LOW)
 - Startup Objects (LOW)
 - Scheduled Tasks (LOW-MEDIUM)
 - Image File Execution Options (MEDIUM)
 - Hint: Might be relevant for your homework this week
 - WMI Subscriptions (MEDIUM)
 - PowerShell Profiles (LOW-MEDIUM)
 - Malicious Group Policies (MEDIUM)



Registry Keys

Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				
> 📙 Mobility	^	Name	Туре	Data
Notifications		ab (Default)	REG_SZ	(value not set)
> PenWorkspace		ab Gaiiin.Net Updat	REG SZ	"C:\Users\anthony\AppData\Local\Gaiiin\Program
- 📙 Policies		ab Synapse3	REG SZ	"C\Program Files (x86)\Razer\Synapse3\WPEUI\Fra
> PrecisionTouchPad		~ [a]apres		

Registry Editor is a GUI way of viewing registry

 Get-ItemProperty can be used as well
 <u>https://tinyurl.com/9hbeh72f</u>

 Two directories for running at sign on

 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Computer\HKE\	loc	AL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				
	-	MicrosoftEdge ^		Name	Туре	Data
	>	MMDevices		ab (Default)	REG_SZ	(value not set)
	>	Mrt		ab RtkAudUService	REG_SZ	"C:\Windows\System32\DriverStore\FileRepository
	>	NcdAutoSetup		ab SecurityHealth	REG EXPAND SZ	%windir%\system32\SecurityHealthSystray.exe
	>	NetCache		ab SteelSeriesGG	REG SZ	"C\Drogram Files\SteelSeries\GG\SteelSeriesGG ex
	>	NetworkServiceTriggers	11	Sectornesoo	NE0_52	C.(Program mes(steelsenes(oo(steelsenesco.ex



Scheduled Tasks

Perform actions given specific triggers

Stored in C:\Windows\System32\Tasks as xml files

Task Scheduler							- 🗆 🗙				
le Action View Help											
👄 🖄 🔟 🖬 🖬											
Task Scheduler (Local)	Name	Status	Triggers	Next Run Time	Last Run Time	Last Run R ^	Actions				
ASUS	Adobe Acro	Ready	Multiple triggers defined	The operat	Task Scheduler Library						
V 📫 Microsoft	AdobeGCIm	Ready	At 11:29 AM every day	The operat	3 Create Basic Task						
Office	AMDAutoU.	. Ready	At 12:00 AM every 15 days	The operat	Create Task						
> 🛄 OneCore	() EventViewer	Disabled	Multiple triggers defined	The operat	Import Task						
> VisualStudio	CoogleUpda	Ready	Multiple triggers defined	3/30/2021 1:12:51 AM	3/29/2021 2:29:09 PM	The operat	Dirolay All Running Tarke				
V Windows	GoogleUpda	Keady Ready	At 1:12 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	3/29/2021 &12:51 PM	3/29/2021 6:29:09 PM	The operat	C Posta All Tele Line -				
Active Direc	MicrosoftEd	Ready Ready	At 11:51 AM even day - After trionered repeat even 1 hour for a duration of 1 day	3/20/2021 7:51-12 PM	3/20/2021 6-51-13 DM	The operat	Enable All lasks history				
AppID	() npcapwatch		At system startup	SPERIOR FOR THE PROPERTY OF	3/27/2021 10:13:39 AM	The operat	1 New Folder				
Application	NvBatteryBo	Ready	At log on of any user		3/29/2021 2:29:23 PM	The operat	View				
Application	NvDriverUp.	. Ready	At 12:25 PM every day	3/30/2021 12:25:46 PM	3/29/2021 2:29:09 PM	The operat	Q Refresh				
AppxDeplo	B NVIDIA GeF.	. Ready	On event - Log: Application, Source: NVIDIA GeForce Experience SelfUpdate Source, Event ID: 0		11/30/1999 12:00:00 AM	The task hi	2 Help				
Autochk	NvNodeLau	 Ready 	At log on of any user - After triggered, repeat every 1.00:00:00 indefinitely.		3/29/2021 2:27:23 PM	The operat	E risk				
Bluetooth	NvProfileUp	Ready	At 12:25 PM every day	3/30/2021 12:25:42 PM	3/29/2021 2:29:09 PM	The operat \checkmark	Selected Item				
BrokerInfra	<					>	Run				
CertificateS	General Trigg	ers Actions	Conditions Settings History (disabled)				End				
Chkdsk	Name	Adobe Acrol	hat Hodata Tark				Disable				
Clip	E	AUGUS AUTO	ues opuere reak				Export				
Cioudexper	Location:						A Properties				
Data Integri	Author:	Adobe Syste	ms Incorporated								
Defrag	Description:	This task kee	eps your Adobe Reader and Acrobat applications up to date with the latest enhancements and sec	urity fixes			× Delete				
Device Info							Help				
Device Setu											
DeviceDirec											
Diagnosis DirectX											
DiskCleanu											
DiskDiagno											
DiskFootpri											
DUSM											
EDP											
Enterpriserv											
> iii Feedback	-Security opti	205									
File Classifie	un open		and the full sector and the sector and t								
FileHistory	When running the task, use the following user account:										
> 🧾 Flighting	INTERACIONE										
HelloFace	Kun only when user is logged on										
InstallServic		and user is in	rggen of or not								
Internation	Don	n store passi	worus i me task will omly nave access to rocal resources								
LanguageC	L Run with	nignest privi	ieges								
📜 License Ma 🗸	Hidden	Config	ure for: Windows Vista™, Windows Server™ 2008			~					

Adobe Act General Trig When you Trigger At log on Daily

Scheduled Tasks cont.

Can be managed through Task Scheduler
 Consists of Triggers & Actions

 Triggers: When Do?
 Actions: What Do?

obat Update Task Properties (Local Computer)	×	Adobe Acrobat Update Task Properties (Local Computer) ×
gers Actions Conditions Settings History (disabled)		General Triggers Actions Conditions Settings History (disabled)
create a task, you can specify the conditions that will trigger the task.		When you create a task, you must specify the action that will occur when your task starts.
Details	Status	Action Details
At log on of any user - After triggered, repeat every 033000 indef_ At 12:00 PM every day - Trigger expires at 5/2/2027 12:05:00 PM.	Enabled	Start a program Ct/Program Files (v86)/Common Files/Adobe/ARM/10/AdobeARM.exe
Edit Delete		Kerner €dit Delete
OK	Cancel	OK Cancel

Name	Status	Triggers				Next Run Time	Last Run Time
Adobe Acrol	- Ready	Multiple triggers defined				11/18/2021 12:00:00 PM	11/18/2021 8:43:10 AM
MicrosoftEd	Ready	Multiple triggers defined				11/19/2021 10:47:05 AM	11/18/2021 10:47:06 AM
MicrosoftEd	Ready	At 10:17 AM every day - After trig	gered, repeat e	very 1 hour for a duration	in of 1 day.	11/18/2021 12:17:05 PM	11/18/2021 11:17:05 AM
NvBatteryBo	Ready	At log on of any user					11/18/2021 8:32:37 AM
NvDriverUp	d. Ready	At 12:25 PM every day				11/18/2021 12:25:52 PM	11/17/2021 5:12:28 PM
NVIDIA GeFe	a. Ready	On event - Log: Application, Sou	or: NVIDIA GeF	rce Experience SelfUpd	ate Source, Event ID: 0		11/30/1999 12:00:00 AM
NvNodeLau	Ready	At log on of any user - After trig	gered, repeat ev	ery 1.00:00:00 indefinitel	у.		11/18/2021 8:30:36 AM
NvProfileUp	Ready	At 12:25 PM every day				11/18/2021 12:25:47 PM	11/17/2021 5:12:28 PM
NvProfileUp	Ready	At log on of any user					11/18/2021 8:32:37 AM
NvTmRep_C	r Ready	At 12:25 PM every day				11/18/2021 12:25:52 PM	11/17/2021 5:12:28 PM
NvTmRep_C	r Ready	At 6:25 PM every day				11/18/2021 6:25:52 PM	11/17/2021 6/25:53 PM
NvTmRep_C	r Ready	At 12:25 AM every day				11/19/2021 12:25:52 AN	11/18/2021 8:33:33 AM
NvTmRep_C	r Ready	At 625 AM every day	Adobe Acr	obat Update Task Prop	erties (Local Computer)		×
OneDrive St	a Ready	At 1:00 AM on 5/1/1992 - After te					
Opera GX sc	Ready	Multiple triggers defined	General Tric	gers Actions Condi	ions Settings History (disabled)	
Opera GX sc	Ready	Multiple triggers defined	Name:	Adobe Acrobat Upda	e Task		
BRIXVoice_(B	2_ Running	At log on of any user					
Chundate-S-1-	Readu	At 319 PM every day - After from	Location:	\ 			
General Tring	ers Artions	Conditions Settings History	Author	Adobe Systems Inco	porated		
Mamor	Adaba Amab	at Landate Tech	Description:	This task keeps your enhancements and s	Adobe Reader and Acroba ecurity fixes	t applications up to date	with the latest
regimes	ADODE ADODA	it opdate lask					
Location:	1						
Author:	Adobe Syster	ns Incorporated	Security on	tions			
Description:	This task kee	ps your Adobe Reader and Acrob					
			when runi	ning the task, use the ro	llowing user account:		
			INTERACT	VE		(Thange User or Group
			Run on	y when user is logged	n		
			 Run wh 	ether user is logged on	or not		
			Do	not store password. Th	e task will only have acces	s to local computer reso	urces.
			🗌 Run wit	h highest privileges			
			Hidden	Configure for:	Windows Vista™, Window	ns Server™ 2008	÷
						_	
							UK Cancel

Task Scheduler (Local)



PowerShell Profile

Runs each time PowerShell.exe is openedA PowerShell script

Description	Path
All Users, All Hosts	\$PSHOME\Profile.ps1
All Users, Current Host	<pre>\$PSHOME\Microsoft.PowerShell_profile.ps1</pre>
Current User, All Hosts	\$Home\[My]Documents\PowerShell\Profile.ps1
Current user, Current Host	\$Home\[My]Documents\PowerShell\ Microsoft.PowerShell_profile.ps1

Malicious Group Policies

Group policies can soften the security posture of a device

- Disable anti-virus
- Turn off or flood logs
- Disable firewalls
- And more!
- Group Policies can be used to establish registry based persistence
- Malicious group policies are very dangerous



Hands on 4 – Combatting Persistence

Check services againWhat do you notice?



Hands on 4 – Combatting Persistence

- SysInternals is an open-source suite of tools for Windows
 - AutoRuns a tool to detect persistence
 - Run autoruns as Admin from the Sysinternals.

folder on your desktop

											F.
📕 I 🕑 🔜 🖛 I		Ma	inage	SYSInternalsS	uite					-1	
File Home :	Share View	Applica	tion Tools								Ŷ
$\in \rightarrow \times \uparrow$	> SYSInternals?	Suite					~	ō	Search SYSInternalsSuite		
	News		^		Data and different	· · · ·	e				
📌 Quick access	-				Date mounieu	Abe	Juce				
Desktop	* Acc	cesstnum.ex	e		10/20/2021 2:08 AM	Application		4/9 KE			
Downloads	Adi 🕥 Adi	Explorer.chm			10/20/2021 2:08 AM	Compiled HTML		SU KE			
Documente	ADI ADI	explorer.exe			10/20/2021 2:08 AM	Application		1,130 KE			
Distance State		explorerow.es	(e		10/20/2021 2:00 AM	Application		003 KE			
Fictures	7 III AD	unsignt.cnm			10/20/2021 2:08 AM	Complied Privic		595 KE			
OneDrive		Insight er			10/20/2021 2:05 AM	Application		1 721 65			
Thu DC	No.	insign104.ext			10/20/2021 2:00 AM	Application		242 85			
TIMBEC	ada	restoration and			10/20/2021 2:08 AM	Application		AM1 KE			
💣 Network	Aur	tologon eve			10/20/2021 2:08 AM	Application		334 KF			
	Aur	tologon64 ex			10/20/2021 2:08 AM	Application		431 KF			
	12 aut	toruns.chm	-		10/20/2021 2:08 AM	Compiled HTML		25 KE			
	Av	toruns.exe			10/20/2021 2:08 AM	Application		2.440 KE			
	- Au	touns64.exe			10/20/2021 2:08 AM	Application		2.853 KE			
	tus 🖭	torunscike	Open			Application		695 KE			
	🗇 aut	torunsc64.ex	Run a	s administrator		Application		769 KE			
	🛄 Bgi	info.exe	Share	with Skype		Application		3,275 KE			
	🛄 Bgi	info64.exe	Troub	leshoot compatib	ility	Application		4,494 KE			
	🔦 Car	cheset.exe	Pinto	Start		Application		415 KE			
	🔦 Car	cheset64.exe	Gan Scan	with Windows De	tender	Application		544 KE			
	Clo	ockres.exe	16 Share			Application		331 KE			
	Clo	ockres64.exe				Application		430 KE			
	Con	ntig.exe	Give a	eccess to	~	Application		439 KE			
159 items 1 item se	elected 2.78 MB		Pin to	taskbar							
			Resto	re previous versio	ns						
			Send	to	>						
			Cut								
			Сору								
			Creat	a chort cut							
			Delete								
			Renar								
			Prope	erties							

Hands on 4 – Combatting Persistence

Categories of persistence

Autoruns - Sysinte	ernals: www.sysinternals.com	n (Administrator) [DESKTOP-7A15TS1\sysade	min]										- 0 ×
File Search Entry	y User Options Categ	ory Help												
6000	<u>२</u> २ 🕻 🤊		P Quick Filter											
		Network	Providers			👛 v	VMI							
Everything	🖻 Logon 🐂	Explorer	🥭 Internet Explorer	Scheduled Tasks	Services	Drivers	Codecs	o [©] Boot Execute	Image Hijacks	C AppInit	🚯 Known DLLs	🍫 WinLogon	Winsock Providers	Print Monitors
Autoruns Entry			Description		Publisher		Image Path					Timestamp	Virus Total	
✓ WicrosoftEd	dgeUpdateTaskMachineCor	e	Keeps your Micr	rosoft software up to date	(Verified) Microsoft Co	rporation	C:\Program Files (x86)\	Microsoft\EdgeUpdate\Mi	icrosoftEdgeUpdate.exe			Thu Apr 1 12:17:37	2021	
✓ [™] \MicrosoftE	dgeUpdateTaskMachineUA		Keeps your Micr	rosoft software up to date	(Verified) Microsoft Co	rporation	C:\Program Files (x86)\	Microsoft\EdgeUpdate\Mi	icrosoftEdgeUpdate.exe			Thu Apr 1 12:17:37	2021	
🗹 🖭 \npcapwatcl	hdog				(Not Verified)		C:\Program Files\Npca	p\CheckStatus.bat				Wed Apr 21 13:46:46	5 2021	
OneDrive St	tandalone Update Task-S-1-	5-21-1961932216-	26321 Standalone Upda	ater	(Verified) Microsoft Co	rporation	C:\Users\sysadmin\Ap	pData\Local\Microsoft\On	eDrive\OneDriveStandalor	neUpdater.exe		Thu Nov 18 13:58:11	2021	
✓ (○) \Opera GX set	cheduled assistant Autoupd	late 1637272882	Keeps Opera Bro	owser Assistant up to date	(Verified) Opera Softw	ire AS	C:\Users\sysadmin\Ap	pData\Local\Programs\Op	era GX\launcher.exe			Thu Nov 4 10:00:11	2021	
✓(()\Opera GX set	cheduled Autoupdate 16347	717190	Keeps Opera up	to date.	(Verified) Opera Softw	ire AS	C:\Users\sysadmin\Ap	pData\Local\Programs\Op	era GX\launcher.exe			Thu Nov 4 10:00:11	2021	
VMwareToo	olsUpdater		Windows Power	Shell	(Verified) Microsoft W	ndows	C:\Windows\System32	\WindowsPowerShell\v1.0	powershell.exe			Mon Mar 18 21:46:5	6 2019	-
Services														
HKLM\System\Cu	urrentControlSet\Services											Thu Nov 18 16:41:54	2021	
✓ O edgeupdate			Microsoft Edge	Update Service (edgeupd	(Verified) Microsoft Co	rporation	C:\Program Files (x86)\	Microsoft\EdgeUpdate\M	crosoftEdgeUpdate.exe			Thu Apr 1 12:17:37 a	2021	
edgeupdate	im Institution Constant		Microsoft Edge	Update Service (edgeupd	(ventied) Microsoft Co	rporation	C:\Program Files (x86)\	Microsoft\EdgeUpdate\M	crosoftEdgeUpdate.exe			Thu Apr 1 12:17:37 a	2021	
	genevationservice		Microsoft Edge t	er lust-in-time compliati	(Venned) Microsoft Co	rporation	C: (Program Files (x86))	Microsoft NET/RedictLict/	MSDuild eve	service.exe		Wed Oct 20 01/22/21	12021	
NetTroPortS	Sharing		Net Tco Port Sha	ving Senice Provider shi	(Notified) Microsoft Co	moration	C\Windows\Microsoft	NET) Framework 640 vr4 0.20	210/SMSuchost eve			Fri Dec. 6 22:02:02 2	019	
VGAuthServi	ice		VMware Alias M	anager and Ticket Service	(Verified) VMware Inc	poration	C:\Program Files\VMw	are\VMware Tools\VMware	VGAuth\VGAuthService e			Sat Any 14 09:40:22 2	2018	
VM3DService			VMware SVGA H	telper Service: Helps VMw	(Verified) VMware. Inc		C:\Windows\system32	vm3dservice.exe				Mon Feb 22 02:55:33	2 2021	
VMTools	-		VMware Tools: P	Provides support for sync	(Verified) VMware. Inc		C:\Program Files\VMw	are\VMware Tools\vmtool	id.exe			Sat Apr 14 09:58:52 2	2018	
VMware Phy	vsical Disk Helper Service		VMware Physica	I Disk Helper Service: Ena	(Verified) VMware, Inc		C:\Program Files\VMw	are\VMware Tools\vmacth	lo.exe			Sat Apr 14 09:54:36 2	2018	
VMwareCAF	FCommAmapListener		VMware CAF AN	MOP Communication Ser	(Not Verified)		C:\Program Files\VMw	are\VMware Tools\VMware	CAF\pme\bin\CommAm	apListener.exe		Sat Apr 14 09:32:46 2	2018	
VMwareCAF	FManagementAgentHost		VMware CAF Ma	anagement Agent Service	(Not Verified)		C:\Program Files\VMw	are\VMware Tools\VMware	CAF\pme\bin\Managem	entAgentHost.exe		Sat Apr 14 09:32:14 2	2018	
VMwareCap	oture		VMwareCapture	Enables optional screen	(Not Verified) VMware	Inc	C:\Program Files\VMw	are\VMware Tools\VMWar	eCapture.exe			Sat Apr 14 09:58:58 2	2018	
Drivers														
HKLM\System\Cu	urrentControlSet\Services											Thu Nov 18 16:41:54	2021	
iaLPSSi_GPIC	0		Intel(R) Serial IO	GPIO Controller Driver: I	(Verified) Intel Corpora	tion - Clien	C:\Windows\System32	\drivers\iaLPSSi_GPIO.sys				Mon Mar 18 21:43:3	8 2019	
🗹 🖻 npcap			Npcap Packet D	river (NPCAP): Npcap Pa	(Verified) Insecure.Cor	n LLC	C:\Windows\system32	\DRIVERS\npcap.sys				Wed Apr 21 11:59:48	3 2021	
vm3dmp			vm3dmp: VMwa	are SVGA 3D Miniport	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vm3dmp.sys				Sat Apr 14 10:02:02 2	2018	
vm3dmp-de	ebug		vm3dmp-debug	g: VMware SVGA 3D Minip	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vm3dmp-debug	.sys			Sat Apr 14 10:02:02 2	2018	
vm3dmp-sta	ats		vm3dmp-stats: \	VMware SVGA 3D Miniport	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vm3dmp-stats.s	ys			Sat Apr 14 10:02:02 2	2018	
vm3dmp_lo	ader		vm3dmp_loader	r: VMware SVGA 3D Minip	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vm3dmp_loader	-sys			Sat Apr 14 10:02:02 2	2018	
Vmci			VMware VMCI B	us Driver: VMware PCI V	(Verified) VMware, Inc		C:\Windows\System32	\drivers\vmci.sys				Wed Nov 29 00:10:3	2 2017	
Vmhgts			VMware Host Gu	uest Client Redirector: Im	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vmhgts.sys				Sat Apr 14 09:55:46 2	2018	
VMMemcti			Memory Contro	Driver: Univer to provide	(verified) VMware, Inc		C:\Windows\system32	URIVERS/Vmmemcti.sys				Sat Apr 14 09:50:10 /	2018	
V wmmouse			VMware Pointin	g Device: VMware Pointin	(ventied) viviware, inc		C:\Windows\System32	\drivers\vmmouse.sys				Sat Apr 14 09:50:42 /	2018	
Vmrawusk			Viviware Priysica	in Disk Heiper: VMware Ph	(verified) viviware, inc		C:\Windows\systems2	(DRIVERS)(VIIIrawusk.sys				Sat Apr 14 09:33:04 2	2010	
VinetWED	26		unetWED: Guest	Introspection Network Eil	(Verified) VMware, Inc		C\Windows\systems2	DRIVERS\vnetWEP.cm				Sat Apr 14 09:57:52 2	2018	
View view fit			viewire, duest	trospection Driver	(Verified) VMware Inc		C\Windows\system32	DRIVERS\usenfit sus				Sat Apr 14 (0.0044 2	2018	
M in vsock			Sockets Virtual	Machine Communicatio	(Verified) VMware Inc		C\Windows\system32	DRIVERS\vsock svs				Wed Nov 29 00:10:3	2 2017	
HKLM\SOFTWARE	E\Microsoft\Windows NT\C	urrentVersion\Font	t Drivers		,							Mon Mar 18 21:55:43	3 2019	
MS8uld	Size	:: 62,080 K												
MSBuild: Pro	ovides Just-in-time compli Time	e: Wed Oct 20 0	01:22:21 2021											

(Not Verified) @Microsoft Corporati Version: 16.9.0.19

C: Program Files (x86) Wicrosoft.NET/RedistList/MSBuild.exe

Hands on 4 – Combatting Persistence

📧 Autoruns - Sysintern	als: www.sysintern	als.com (Administrator)	[DESKTOP-7A15TS1\sysad	min]										- 0 >
File Search Entry	User Options	Category Help												
d 🔚 🖒 🗋	Р 🔓 🖊	🛍 💾 🎫 🛛	P Quick Filter											
	Q Network	📿 Network Providers 💼 WMI							① Office					
Everything	Logon	Replorer	🥭 Internet Explorer	Scheduled Tasks	Services	Drivers	Codecs	o [©] Boot Execute	Image Hijacks	C AppInit	Known DLLs	🍫 WinLogon	Winsock Providers	Print Monitor
Autoruns Entry			Description		Publisher		Image Path					Timestamp	Virus Total	
✓ ➡\MicrosoftEdg	geUpdateTaskMachi	ineCore	Keeps your Micr	rosoft software up to date	(Verified) Microsoft C	orporation	C:\Program Files (x86)	\Microsoft\EdgeUpdate\M	licrosoftEdgeUpdate.exe			Thu Apr 1 12:17:37 2	021	
✓ ₿\/MicrosoftEdg	geUpdateTaskMachi	ineUA	Keeps your Micr	rosoft software up to date	(Verified) Microsoft C	orporation	C:\Program Files (x86)	\Microsoft\EdgeUpdate\M	licrosoftEdgeUpdate.exe			Thu Apr 1 12:17:37 2	2021	
npcapwatchd	dog				(Not Verified)		C:\Program Files\Npca	ap\CheckStatus.bat				Wed Apr 21 13:46:46	2021	
✓ ■ \OneDrive Star	ndalone Update Ta:	sk-S-1-5-21-1961932216	-26321 Standalone Upd	ater	(Verified) Microsoft C	orporation	C:\Users\sysadmin\Ap	pData\Local\Microsoft\On	neDrive\OneDriveStandalo	neUpdater.exe		Thu Nov 18 13:58:11	2021	
MO\Opera GX sch	neduled assistant Au	utoupdate 163/2/2882	Keeps Opera Bro	owser Assistant up to date	(Venfied) Opera Softw	/are AS	C:\Users\sysadmin\Ap	pData\Local\Programs\Op	bera GX\launcher.exe			Thu Nov 4 10:00:11	2021	
VMwaraToold	Indater	te 1034/17190	Windows Power	to date.	(ventied) Opera Softw (Verified) Microroft W	/are AS	C:\Users\sysadmin\Ap	/WindowsPowerShell/v10	oera GX launcher.exe			Mon Mar 18 21-46-56	2021	
Services	iopuster		This down in other	Junear .	(veniled) increaser in	110043	c.(mindows(systemsz		powersmentexe			10011021.48.3	2013	
HKLM\System\Curre	entControlSet\Servi	ices										Thu Nov 18 16:41:54	2021	
☑ ➡ edgeupdate			Microsoft Edge	Update Service (edgeupd	(Verified) Microsoft C	orporation	C:\Program Files (x86)	\Microsoft\EdgeUpdate\M	licrosoftEdgeUpdate.exe			Thu Apr 1 12:17:37 2	021	
🗹 🔯 edgeupdatem			Microsoft Edge	Update Service (edgeupd	(Verified) Microsoft C	orporation	C:\Program Files (x86)	\Microsoft\EdgeUpdate\M	licrosoftEdgeUpdate.exe			Thu Apr 1 12:17:37 2	2021	
MicrosoftEdge	eElevationService		Microsoft Edge	Elevation Service (Micros	(Verified) Microsoft C	orporation	C:\Program Files (x86)	Microsoft\Edge\Applicati	on\95.0.1020.53\elevation	service.exe		Thu Nov 18 15:29:29	2021	
MSBuild			MSBuild: Provid	es Just-in-time compliati	(Not Verified) ©Micro	soft Corpor	C:\Program Files (x86)	\Microsoft.NET\RedistList\	MSBuild.exe			Wed Oct 20 01:22:21	2021	
Net IcpPortSha	aring		Net. Icp Port Sha	aring Service: Provides abi	(Venified) Microsoft C	orporation	C:\Windows\Microsoft	t.NET\Frameworkb4\v4.0.3	U319\SMSvcHost.exe			Fri Dec 6 22:03:03 20	019	
VM3DSen ce	e		VMware SVGA H	lanager and Ticket Service	(verified) VMware, Inc (Verified) VMware, Inc		C:\Program Files\Viviv	vare\viviware loois\viviwar	e vGAuth\vGAuthService.	exe		Sat Apr 14 09:40:22 2 Mon Feb 22 02:55:32	2021	
VMTools			VMware Tools: P	rovides support for sync	(Verified) VMware, Inc.		C:\Program Files\VMw	are\VMware Tools\vmtool	sd.exe			Sat Apr 14 09:58:52 2	018	
VMware Physic	ical Disk Helper Sen	vice	VMware Physica	I Disk Helper Service: Ena	(Verified) VMware, Inc		C:\Program Files\VMw	vare\VMware Tools\vmacth	lp.exe	Sat Apr 14 09:54:36 2				
VMwareC FC	ommAmqpListene	a.	VMware CAF AM	MQP Communication Ser	(Not Verified)	(Not Verified) C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\CommAmqpListener.exe 5					Sat Apr 14 09:32:46 2			
VMwareC FM	lanagementAgentH	Host	VMware CAF Ma	anagement Agent Service	(Not Verified)	(Not Verified) C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\ManagementAgentHost.exe Sat Apr 14					Sat Apr 14 09:32:14 2	Sat Apr 14 09:32:14 2018		
VMwareC ptu	ire		VMwareCapture	Enables optional screen	(Not Verified) VMware	e, Inc	C:\Program Files\VMw	vare\VMware Tools\VMWar	eCapture.exe			Sat Apr 14 09:58:58 2		
Drivers														
HKLM\System\Curre	entControlSet\Servi	rices	1-1-1/D) 0-1-110	(0)0 C	01-17-10 I-1-1 C	and an and an	C1005-1					Thu Nov 18 16:41:54	2021	
			Intel(K) Serial IO	GPIO Controller Driver: I	(Verified) Intel Corpor	ation - Clien	C:\Windows\System32	ConversitaLPSSI_GPIO.sys				Mon Mar 18 21:43:38	2019	
vm3dmp			vm3dmn: VMw	are SVGA 3D Miniport	(Verified) VMware Inc		C:\Windows\system32	\DRIVERS\vm3dmp.svs				Sat Apr 14 10:02:02 2	018	
vm3dmp-debu	ua		vm3dmp-debug	x: VMware SVGA 3D Minip	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vm3dmp-debug	1.5V5			Sat Apr 14 10:02:02 2	018	
vm3dmp-tats	s		vm3dmp-stats:	VMware SVGA 3D Miniport	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vm3dmp-stats.s	ys.			Sat Apr 14 10:02:02 2	018	
vm3dmp_oad	ler		vm3dmp_loader	r: VMware SVGA 3D Minip	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vm3dmp_loader	r.sys			Sat Apr 14 10:02:02 2	018	
🗹 🖻 vmci			VMware VMCI B	lus Driver: VMware PCI V	(Verified) VMware, Inc		C:\Windows\System32	\\drivers\vmci.sys				Wed Nov 29 00:10:32	2 2017	
vmhgfs			VMware Host G	uest Client Redirector: Im	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vmhgfs.sys				Sat Apr 14 09:55:46 2	018	
VMMemCt			Memory Contro	I Driver: Driver to provide	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vmmemctl.sys				Sat Apr 14 09:56:16 2	018	
Vmmouse			VMware Pointin	g Device: VMware Pointin	(Verified) VMware, Inc		C:\Windows\System32	\\drivers\vmmouse.sys				Sat Apr 14 09:56:42 2	018	
V vmrawdsk			VMware Physica VMware USP De	a Disk Helper: VMware Ph	(Verified) VMware, Inc		C:\Windows\system32	URIVERS\vmrawdsk.sys				Sat Apr 14 09:55:04 2	018	
Vinusbinduse			viniware 036 Po	Inting Device: Viviware Po	(verified) VMware, Inc		C:\Windows\systems2	DRIVERS\vmusbmouse.sys				Sat Apr 14 09:57:52 2 Sat Apr 14 10:00:44 2	018	
vsepfit			vsenfit: Guest In	trospection Driver	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vsenfit.svs				Sat Apr 14 09:59:58 2	018	
vsock			vSockets Virtual	Machine Communicatio	(Verified) VMware, Inc		C:\Windows\system32	\DRIVERS\vsock.sys				Wed Nov 29 00:10:32	2 2017	
HKLM\SOFTWARE\N	Microsoft\Windows	s NT\CurrentVersion\For	nt Drivers									Mon Mar 18 21:55:43	2019	
(kik) MSBuild		Size: 62,080 K												
MSBuild: Provi	ides Just-in-time com	pli Time: Wed Oct 20	01:22:21 2021											
(Not Verified)	@Microsoft Corporat	ti Version: 16.9.0.195												
C:\Program Fi	les (x86) Microsoft.N	NET\Dedict ist\MSB.ild.eve												

Hands on 4 – Combatting Persistence

- Find and remove the item that is allowing the <REDACTED> to persist
 - Hint: It is not a GroupPolicy, PowerShell Profile, Driver, Image File Execution Option or Startup Object

After you have removed the persistence

- Stop the service using task manager
- Delete the <REDACTED> using <REDACTED>
- Restart the computer
 - Is the service gone?

Homework Links

- Persistence Image File Execution Options Injection
 - <u>https://pentestlab.blog/2020/01/13/persistence-image-file-execution-options-injection/</u>
- Windows Security Log Event IDs
 - <u>https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx</u>
 - Windows Sysinternals
 - <u>https://docs.microsoft.com/en-us/sysinternals/</u>

Netnef

Additional Resources

- Abusing Windows Management Instrumentation (Black Hat)
 - <u>https://tinyurl.com/a7jpzmsc</u>
 - <u>https://www.youtube.com/watch?v=0SjMgnGwpq8</u>
- Revoke-Obfuscation: PowerShell Obfuscation Detection (Black hat)
 - <u>https://www.youtube.com/watch?v=x97ejtv56xw</u>
- PowerShell Documentation
 - <u>https://docs.microsoft.com/en-us/powershell/</u>



Questions?