

Vu Nguyen

UID: u1483046

Assignment 15 - Processes, Handles and Windows Registry (Lab and Quiz)

3.0.3 Lab

1. Part 2, Step a

David Eccles School of Business
THE UNIVERSITY OF UTAH

MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 69290 > 3.0.3 Lab - Identify Running Processes

Time Remaining: 2 47

Topology Content Status WinClient

Recycle Bin

Tools

TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
lsass.exe	588	TCP	*.*.*.*	1540	*.*.*.*	0	LISTENING
lsass.exe	588	TCPv6	:::.	1540	:::.	0	LISTENING
services.exe	576	TCP	*.*.*.*	1540	*.*.*.*	0	LISTENING
services.exe	576	TCPv6	:::.	1540	:::.	0	LISTENING
spoolsv.exe	1564	TCP	*.*.*.*	1539	*.*.*.*	0	LISTENING
spoolsv.exe	1564	TCPv6	:::.	1539	:::.	0	LISTENING
echohost.exe	716	TCP	*.*.*.*	1537	*.*.*.*	0	LISTENING
echohost.exe	908	TCP	*.*.*.*	1537	*.*.*.*	0	LISTENING
echohost.exe	676	TCP	*.*.*.*	1538	*.*.*.*	0	LISTENING
echohost.exe	1460	TCP	*.*.*.*	1541	*.*.*.*	0	LISTENING
echohost.exe	396	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	676	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	676	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	396	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	1072	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	1072	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	676	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	716	TCPv6	:::.	1537	:::.	0	LISTENING
echohost.exe	908	TCPv6	:::.	1537	:::.	0	LISTENING
echohost.exe	676	TCPv6	:::.	1538	:::.	0	LISTENING
echohost.exe	1460	TCPv6	:::.	1541	:::.	0	LISTENING
echohost.exe	396	UDPv6	:::.	5003	:::.	0	LISTENING
echohost.exe	676	UDPv6	:::.	5003	:::.	0	LISTENING
echohost.exe	1072	UDPv6	:::.	5003	:::.	0	LISTENING
echohost.exe	1072	UDPv6	:::.	5003	:::.	0	LISTENING

Endpoints: 40 Established: 0 Listening: 24 Time Wait: 0 Close Wait: 0

2. Part 3, Step c

David Eccles School of Business
THE UNIVERSITY OF UTAH

MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 69290 > 3.0.3 Lab - Identify Running Processes

Time Remaining: 2 46

Topology Content Status WinClient

Mozilla Firefox Start Page

Firefox Search or enter address

mozilla

TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
firefox.exe	2784	TCP	*.*.*.*	1543	localhost	1544	ESTABLISHED
firefox.exe	2784	TCP	*.*.*.*	1544	localhost	1543	ESTABLISHED
firefox.exe	3112	TCP	*.*.*.*	1546	localhost	1546	ESTABLISHED
firefox.exe	3112	TCP	*.*.*.*	1546	localhost	1545	ESTABLISHED
lsass.exe	588	TCP	*.*.*.*	1540	*.*.*.*	0	LISTENING
services.exe	576	TCP	*.*.*.*	1540	*.*.*.*	0	LISTENING
services.exe	576	TCPv6	:::.	1540	:::.	0	LISTENING
spoolsv.exe	1564	TCP	*.*.*.*	1539	*.*.*.*	0	LISTENING
spoolsv.exe	1564	TCPv6	:::.	1539	:::.	0	LISTENING
echohost.exe	716	TCP	*.*.*.*	1537	*.*.*.*	0	LISTENING
echohost.exe	908	TCP	*.*.*.*	1537	*.*.*.*	0	LISTENING
echohost.exe	676	TCP	*.*.*.*	1538	*.*.*.*	0	LISTENING
echohost.exe	1460	TCP	*.*.*.*	1541	*.*.*.*	0	LISTENING
echohost.exe	396	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	676	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	676	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	396	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	1072	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	1072	UDP	*.*.*.*	5003	*.*.*.*	0	LISTENING
echohost.exe	676	UDPv6	:::.	5003	:::.	0	LISTENING
echohost.exe	716	TCPv6	:::.	1537	:::.	0	LISTENING
echohost.exe	908	TCPv6	:::.	1537	:::.	0	LISTENING
echohost.exe	676	TCPv6	:::.	1538	:::.	0	LISTENING
echohost.exe	1460	TCPv6	:::.	1541	:::.	0	LISTENING

Endpoints: 44 Established: 4 Listening: 24 Time Wait: 0 Close Wait: 0

Sorry, I could not screenshot the tcp of firefox turning red since it will disappear immediately after I closed the browser. So, I will answer the question related to the screenshot that I supposed to took a screenshot. After closing the browser in step c Part 3. The TCP view window will show us the red highlighted firefox.exe which notify us that the application lost connection with the browser.

3.2.11 Lab

3. Part 1, Step 1f

The screenshot shows a virtual machine environment with the following components:

- Process Explorer:** A window titled "Process Explorer - Sysinternals: www.sysinternals.com [WINCLIENT\CyberOpsUser]" displaying a list of running processes. The list includes columns for CPU, Private Bytes, Working Set, PID, Description, and Company Name. Processes like iexplore.exe, chrome.exe, and firefox.exe are visible.
- Mozilla Firefox:** A browser window titled "Mozilla Firefox Start Page" is open, showing the Firefox logo and search bar.
- Taskbar:** The Windows taskbar at the bottom shows the Start button, task view, and several pinned applications including Firefox, Chrome, and File Explorer.
- System Tray:** The system tray on the right shows the time as 6:11 PM on 2/5/2024.

4. Part 2, Step 1b

The screenshot shows a virtual machine environment with the following components:

- Process Explorer:** A window titled "Process Explorer - Sysinternals: www.sysinternals.com [WINCLIENT\CyberOpsUser]" displaying a list of running processes. The list includes columns for CPU, Private Bytes, Working Set, PID, Description, and Company Name. Processes like iexplore.exe, chrome.exe, and firefox.exe are visible.
- Windows Command Prompt:** A window titled "cmd" is open, showing the output of the command "ipconfig /all". The output displays network configuration details for the adapter "Ethernet0", including IP address, subnet mask, and default gateway.
- Taskbar:** The Windows taskbar at the bottom shows the Start button, task view, and several pinned applications including Firefox, Chrome, and File Explorer.
- System Tray:** The system tray on the right shows the time as 6:13 PM on 2/5/2024.

5. Part 3, Step b

