Microsoft Sysinternals

For the contest, I'm recommending three of the tools from Microsoft Sysinternals. The Sysinternals web site was created in 1996 by Mark Russinovich to host his advanced system utilities and technical information

TCPView

I want to show you how to use TCPView to identify programs that are using ports that are commonly used for cyberattacks.

Commonly used port

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as

TCP:80 (HTTP)

TCP:443 (HTTPS)

TCP:25 (SMTP)

TCP/UDP:53 (DNS)

They may use the protocol associated with the port or a completely different protocol.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), examples of common ports are

TCP/UDP:135 (RPC)

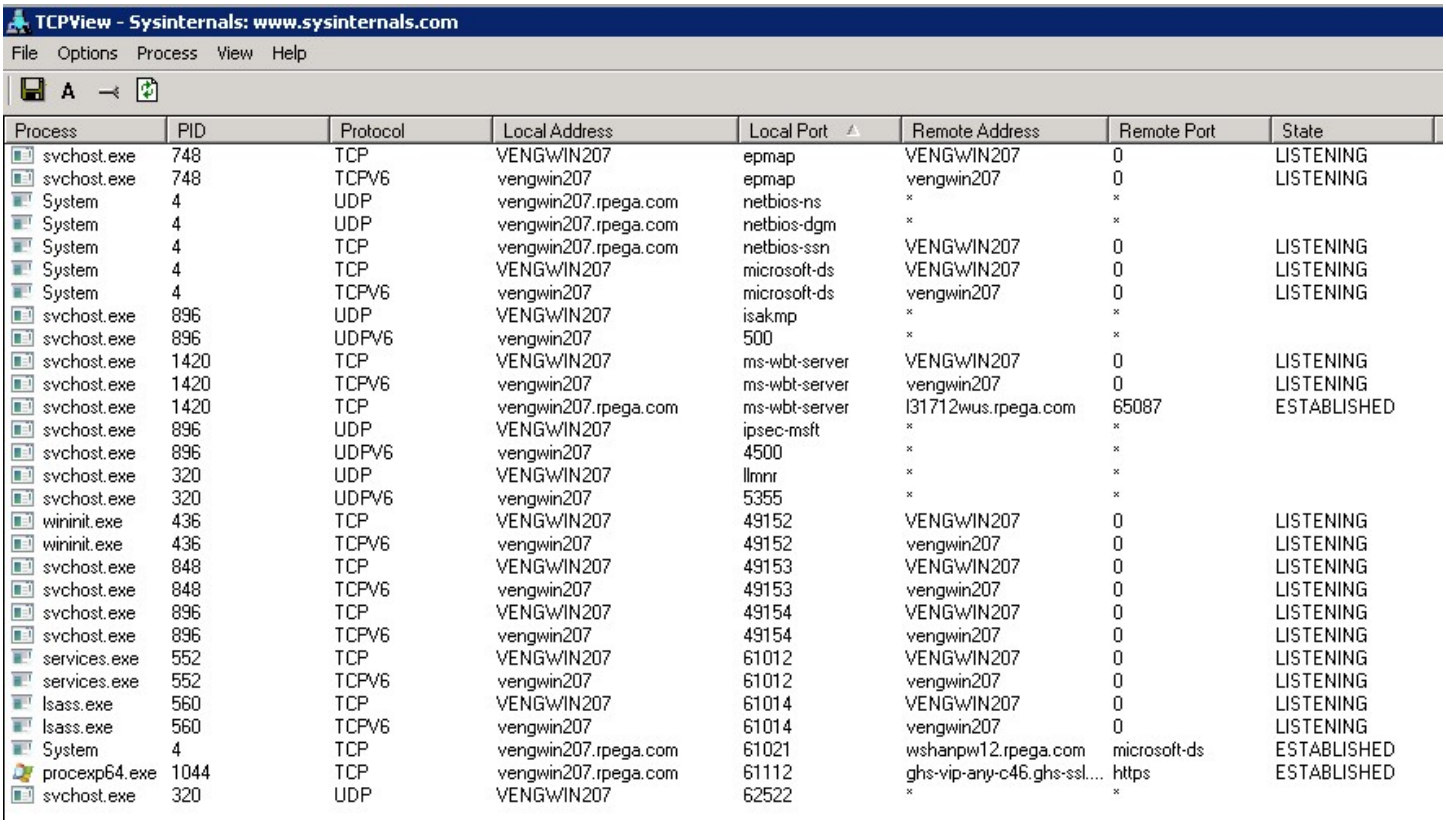
TCP/UDP:22 (SSH)

TCP/UDP:3389 (RDP)

From *MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) which is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected*

https://attack.mitre.org/wiki/Technique/T1043

Exit any/all other programs. Launch TCPView



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
svchost.exe	748	TCP	VENGWIN207	epmap	VENGWIN207	0	LISTENING
svchost.exe	748	TCPV6	vengwin207	epmap	vengwin207	0	LISTENING
System	4	UDP	vengwin207.rpega.com	netbios-ns	*	*	
System	4	UDP	vengwin207.rpega.com	netbios-dgm	*	*	
System	4	TCP	vengwin207.rpega.com	netbios-ssn	VENGWIN207	0	LISTENING
System	4	TCP	VENGWIN207	microsoft-ds	VENGWIN207	0	LISTENING
System	4	TCPV6	vengwin207	microsoft-ds	vengwin207	0	LISTENING
svchost.exe	896	UDP	VENGWIN207	isakmp	*	*	
svchost.exe	896	UDPV6	vengwin207	500	*	*	
svchost.exe	1420	TCP	VENGWIN207	ms-wbt-server	VENGWIN207	0	LISTENING
svchost.exe	1420	TCPV6	vengwin207	ms-wbt-server	vengwin207	0	LISTENING
svchost.exe	1420	TCP	vengwin207.rpega.com	ms-wbt-server	l31712wus.rpega.com	65087	ESTABLISHED
svchost.exe	896	UDP	VENGWIN207	ipsec-msft	*	*	
svchost.exe	896	UDPV6	vengwin207	4500	*	*	
svchost.exe	320	UDP	VENGWIN207	llmnr	*	*	
svchost.exe	320	UDPV6	vengwin207	5355	*	*	
wininit.exe	436	TCP	VENGWIN207	49152	VENGWIN207	0	LISTENING
wininit.exe	436	TCPV6	vengwin207	49152	vengwin207	0	LISTENING
svchost.exe	848	TCP	VENGWIN207	49153	VENGWIN207	0	LISTENING
svchost.exe	848	TCPV6	vengwin207	49153	vengwin207	0	LISTENING
svchost.exe	896	TCP	VENGWIN207	49154	VENGWIN207	0	LISTENING
svchost.exe	896	TCPV6	vengwin207	49154	vengwin207	0	LISTENING
services.exe	552	TCP	VENGWIN207	61012	VENGWIN207	0	LISTENING
services.exe	552	TCPV6	vengwin207	61012	vengwin207	0	LISTENING
lsass.exe	560	TCP	VENGWIN207	61014	VENGWIN207	0	LISTENING
lsass.exe	560	TCPV6	vengwin207	61014	vengwin207	0	LISTENING
System	4	TCP	vengwin207.rpega.com	61021	wshanpw12.rpega.com	microsoft-ds	ESTABLISHED
procexp64.exe	1044	TCP	vengwin207.rpega.com	61112	ghs-vip-any-c46.ghs-ssl....	https	ESTABLISHED
svchost.exe	320	UDP	VENGWIN207	62522	*	*	

Sort by Local Port. If you see anything using ports 80, 8080, 443, 22, 25, 53, 135, or 3389 then you need to research these programs with Process Explorer

Autoruns

Process Explorer

I reached out to Mr. Russinovich who gave approval for us to view a 12-minute excerpt from his September 2017 presentation called "Case of the unexplained", from the Microsoft Ignite Conference. Here he demonstrates how to use Autoruns and Process Explorer to identify and remove malware: https://youtu.be/qouxznNC2XU?t=51m03s

These tools really are the best out there for troubleshooting problems on Windows computers, I use them all the time. And have been now for decades. So I suggest that any students interested in this type of thing, watch more video, and/or download his complete presentations.

Additional information (Homework) the following 3 presentations provide similar but more depth of information on this:

License to Kill: Malware Hunting with the Sysinternals Tools (a PDF download is available)

Malware Hunting with Mark Russinovich and the Sysinternals Tools (A Powerpoint download is available)

Microsoft Security Intelligence Report volume 11 Book chapter on Malware cleaning techniques download the file named Microsoft_Security_Intelligence_Report_volume_11_Advanced_Malware_Cleaning_Techniques_for_the_IT_Professional_English.pdf

Anyone that is interested in learning more about Troubleshooting Windows issues, I recommend Mark's book *Troubleshooting with the Windows Sysinternals Tools* more info here https://docs.microsoft.com/en-us/sysinternals/learn/troubleshooting-book