

Atividade de Classe - O que está acontecendo?

Objetivos

Identifique os processos em execução em um computador, o protocolo que eles estão usando e seus endereços de porta local e remota.

Parte 1: Baixe e instale o software TCPView.

Parte 2: Responda às seguintes perguntas.

Parte 3: Use um navegador e observe a janela TCPView.

Histórico/Cenário

Para que um hacker estabeleça uma conexão com um computador remoto, uma porta deve estar escutando nesse dispositivo. Isso pode ser devido a infecção por malware ou a uma vulnerabilidade em um software legítimo. Um utilitário, como o TCPView, pode ser usado para detectar portas abertas, monitorá-las em tempo real e fechar portas e processos ativos que as utilizam.

Recursos necessários

- PC com acesso à Internet
- Software TCPView

Instruções

Parte 1: Baixe e instale o software TCPView.

- a. Clique no link abaixo para acessar a página de download do TCPView.

Atividade de Classe - O que está acontecendo?

<http://technet.microsoft.com/en-us/sysinternals/tcpview.aspx>

The screenshot shows the Windows Sysinternals TCPView v3.05 download page. The page includes a navigation menu with links to Home, Learn, Downloads, and Community. The main content area features the product name 'TCPView v3.05' by Mark Russinovich, published on July 25, 2011. A 'Download TCPView (285 KB)' button is prominently displayed. Below this, there is a 'Run TcpView now from Live.Sysinternals.com' button and a list of supported operating systems: Client: Windows Vista and higher; Server: Windows Server 2008 and higher. The page also includes a sidebar with 'Utilities' and 'Additional Resources' links, and an 'Introduction' section describing the tool's functionality.

- Crie uma pasta na área de trabalho chamada **TCPView**.
- Extraia o conteúdo do zip para esta nova pasta.
- Inicie o aplicativo Tcpview.
- Finalmente, concorde com os termos de licença de software.

The screenshot shows the TCPView application window. The window title is 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes File, Options, Process, View, and Help. The main display area is a table of network connections. The table has columns for Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, State, Sent Packets, Sent Bytes, Rcvd Packets, and Rcvd Bytes. The table lists various processes and their network activity, including listening ports and established connections.

| Process | PID | Protocol | Local Address | Local Port | Remote Address | Remote Port | State | Sent Packets | Sent Bytes | Rcvd Packets | Rcvd Bytes |
|--------------|------|----------|-----------------|--------------|----------------|-------------|-----------|--------------|------------|--------------|------------|
| lsass.exe | 476 | TCP | pi | 58702 | pi | 0 | LISTENING | | | | |
| lsass.exe | 476 | TCPV6 | pi | 58702 | pi | 0 | LISTENING | | | | |
| services.exe | 468 | TCP | pi | 49155 | pi | 0 | LISTENING | | | | |
| services.exe | 468 | TCPV6 | pi | 49155 | pi | 0 | LISTENING | | | | |
| svchost.exe | 716 | TCP | pi | epmap | pi | 0 | LISTENING | | | | |
| svchost.exe | 768 | TCP | pi | 49153 | pi | 0 | LISTENING | | | | |
| svchost.exe | 924 | TCP | pi | 49154 | pi | 0 | LISTENING | | | | |
| svchost.exe | 1408 | UDP | pi.cisco.com | ssdp | * | * | | 36 | 17,142 | 462 | 91,080 |
| svchost.exe | 1408 | UDP | pi | ssdp | * | * | | | | | |
| svchost.exe | 312 | UDP | pi | ws-discovery | * | * | | | | | |
| svchost.exe | 1408 | UDP | pi | ws-discovery | * | * | | | | | |
| svchost.exe | 1408 | UDP | pi | ws-discovery | * | * | | | | | |
| svchost.exe | 312 | UDP | pi | ws-discovery | * | * | | | | | |
| svchost.exe | 972 | UDP | pi | llmnr | * | * | | | | | |
| svchost.exe | 972 | UDP | pi | 54649 | * | * | | | | | |
| svchost.exe | 1408 | UDP | pi | 61427 | * | * | | | | | |
| svchost.exe | 312 | UDP | pi | 61464 | * | * | | | | | |
| svchost.exe | 1408 | UDP | pi.cisco.com | 63677 | * | * | | | | | |
| svchost.exe | 1408 | UDP | pi | 63678 | * | * | | | | | |
| svchost.exe | 716 | TCPV6 | pi | epmap | pi | 0 | LISTENING | | | | |
| svchost.exe | 2300 | TCPV6 | pi | 3587 | pi | 0 | LISTENING | | | | |
| svchost.exe | 768 | TCPV6 | pi | 49153 | pi | 0 | LISTENING | | | | |
| svchost.exe | 924 | TCPV6 | pi | 49154 | pi | 0 | LISTENING | | | | |
| svchost.exe | 1408 | UDPV6 | [0:0:0:0:0:0:1] | 1900 | * | * | | | | | |
| svchost.exe | 1408 | UDPV6 | pi.cisco.com | 1900 | * | * | | | | | |

Endpoints: 55 Established: 1 Listening: 24 Time Wait: 0 Close Wait: 0

Parte 2: Responda às perguntas a seguir.

- a. Quantos Endpoints estão listados?
- b. Quantos estão escutando?
- c. Quantos endpoints são estabelecidos?

Parte 3: Use um navegador e observe a janela TCPView.

- a. Abra o menu Opções e clique em “Sempre no topo”.
Observação: Use a seção Ajuda do programa para ajudá-lo a responder às perguntas a seguir.

- b. Abra qualquer navegador.

O que acontece na janela do TCPView?

- c. Navegue até cisco.com.

O que acontece na janela do TCPView?

- d. Feche o navegador.

O que acontece na janela do TCPView?

O que você acha que as cores significam?

Observação: Para fechar um processo diretamente, clique com o botão direito do mouse no processo e escolha **Finalizar Processo**. Usar esse método pode fazer com que um programa ou o sistema operacional se torne instável. Apenas termine os processos que você sabe que são seguros para terminar. Este método pode ser usado para impedir a comunicação de malware.