**Equipe: Paulo Henrique Araujo Nobre, Matheus Holanda Matos e Moises Moura Rabelo**

**Instituto Federal de Educação, Ciência e Tecnologia do Ceará**

**Disciplina: Redes de Computadores Prof. Nídia S. Campos**

**Usando o netstat**

**Material de apoio:**

* Redes de Computadores e a Internet – uma abordagem top-down, 5ª edição, autores: James F. Kurose, Keith W. Ross, editora Pearson.
* Cisco CCNA 1 - Introdução às Redes

**Objetivo:**

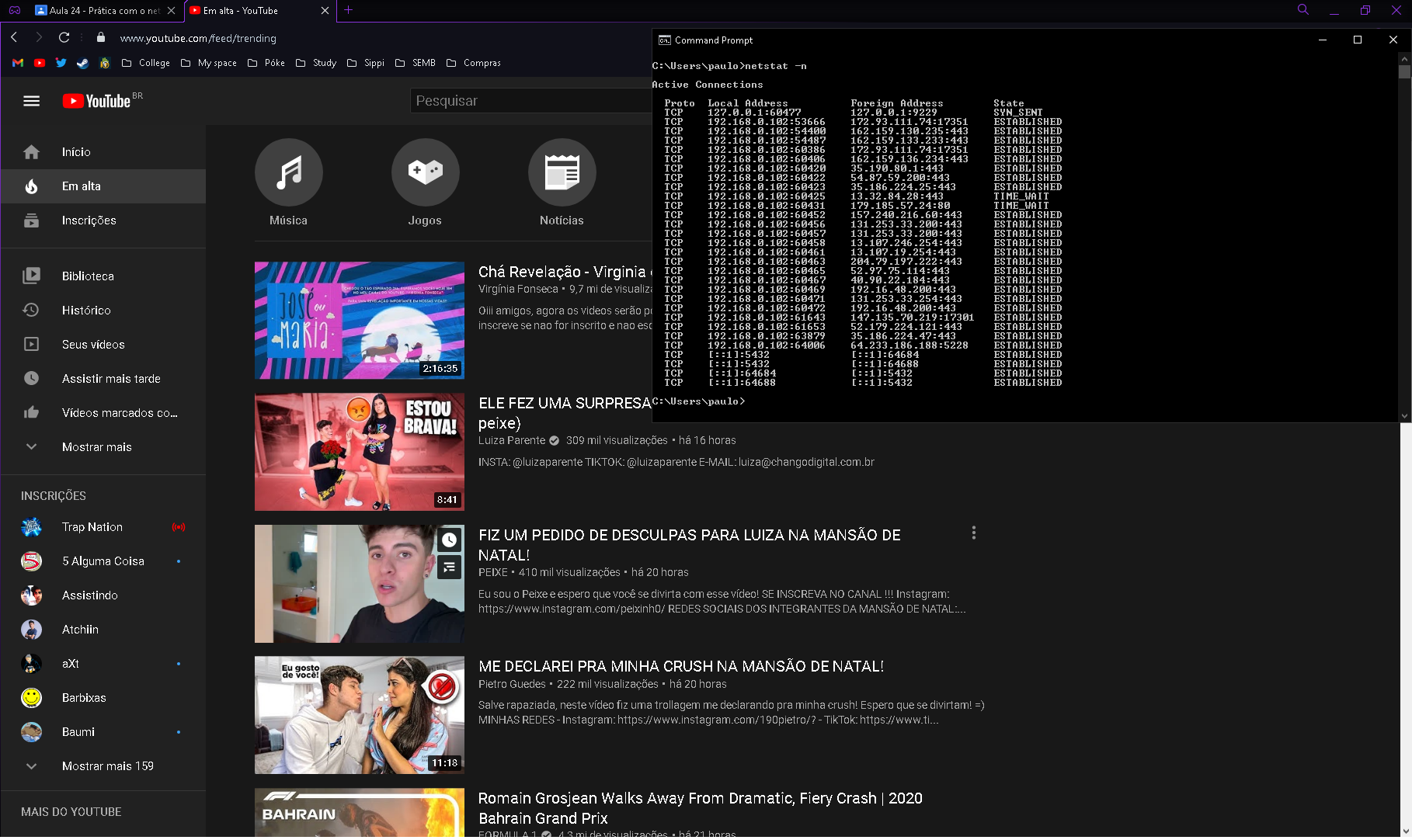
* Visualizar portas origem e destino da camada de transporte com o programa **netstat**.

**Tarefa 1 - Visualizar conexões Web**

**PASSO 1 -** Abra apenas uma janela de um navegador Web.

**PASSO 2 -** No browser, entre com a URL de sua preferência.

**PASSO 3 -** No prompt, digite **netstat –n.**

****

**PASSO 4** – Escolha apenas uma linha da resposta do netstat que corresponde a uma conexão web e responda analisando a linha escolhida:

* 1. Qual a porta origem (source port) do cliente web? E a porta destino (destination port)?

**Local Address: 192.168.0.102:64006**

**Foreing Address: 64.233.186.188:5228**

* 1. O que poderia ser a porta origem do servidor web? E sua porta destino?

**Local Address: 64.233.186.188:5228**

**Foreing Address: 192.168.0.102:64006**

* 1. Qual é o protocolo da camada de aplicação usado nessa conexão?

**TCP**

* 1. Qual é o protocolo da camada de transporte usado nessa conexão?

**TCP**

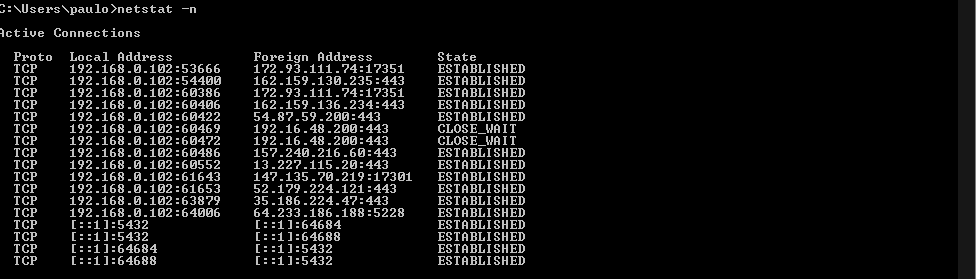
**Tarefa 2 - Opções do help do netstat**

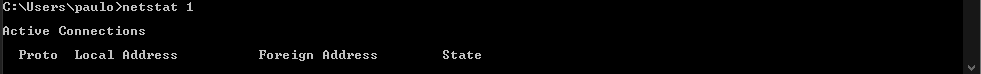
**PASSO 1 - No prompt de comando, digite netstat /? e complete a tabela abaixo:**

|  |  |
| --- | --- |
| Opção | Descrição |
| -a | Exibir todas as conexões e portas de monitoramento. |
| -n | Exibir endereços e números de porta em forma numérica. |
| [interval] (1) | Re-exibir estatísticas a cada cinco segundos. Pressione CTRL+C para parar a re-exibição das estatísticas. |
| -p [proto] (TCP) | Mostra conexões para o protocolo especificadas por proto; proto pode qualquer um dos seguintes: TCP, UDP, TCPv6 ou UDPv6. Se usado com a opção –s exibi estatística por protocolo, proto pode ser qualquer um dos seguintes:  IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP ou UDPv6. |

**PASSO 2 -** Execute o netstat com para cada uma das opções da tabela anterior.

****

****

****

****

**PASSO 3** - Compare as saídas dos comandos abaixo escrevendo 3 linhas de saída de cada um:

1. **netstat** –**a**

****

2. **netstat** –**an**

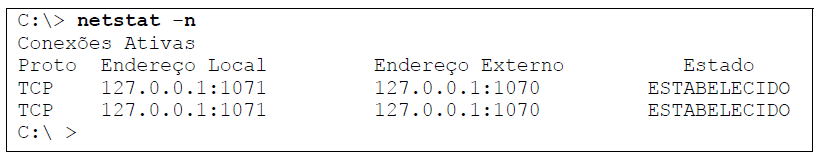
****

**Tarefa 3 - Computador hackeado?**

**PASSO 1 - Os endereços IP exibidos pelo netstat entram em várias categorias:**

|  |  |
| --- | --- |
| **Endereço IP** | **Descrição** |
| 127.0.0.1 | Este endereço se refere ao host local, ou a este computador. |
| 0.0.0.0 | Um endereço global, significando “QUALQUER”. |
| Endereço Remoto | O endereço do dispositivo remoto que tem uma conexão com este computador. |

Sabendo disto, consulte a saída do netstat abaixo. Um novo engenheiro de rede suspeita que seu computador foi comprometido por um ataque externo contra as portas 1070 e 1071. Como você responderia?



**Não é um ataque externo pois a endereço 127.0.0.1 é destinado para um endereço local.**