Bien sûr, je peux vous fournir des exemples concrets et des détails complémentaires pour les commandes netstat mentionnées. Voici quelques précisions :

1. **Lister toutes les connexions réseau actives** Commande : netstat -a Cela affiche une liste complète des connexions actives, y compris celles en écoute.
2. **Identifier les connexions établies** Commande : netstat -n Ajoutez l'option -p tcp pour ne voir que les connexions TCP établies : netstat -n -p tcp.
3. **Identifier les ports en écoute** Commande : netstat -an | find "LISTENING" Cela montre uniquement les ports en attente de connexions entrantes.
4. **Afficher les connexions avec les noms des processus** Commande : netstat -ano Cela associe chaque connexion réseau à l'ID de processus correspondant. Vous pouvez ensuite utiliser le gestionnaire de tâches pour identifier le processus spécifique.
5. **Afficher les statistiques réseau** Commande : netstat -e Cela fournit des statistiques sur les paquets envoyés, reçus, erreurs, etc.
6. **Afficher la table de routage** Commande : netstat -r Cela montre la table de routage, y compris les passerelles et interfaces réseau.
7. **Actualiser l’affichage en temps réel** Commande : netstat -an 1 Ajoutez un intervalle (en secondes) pour voir les connexions mises à jour en temps réel.
8. **Lister les connexions réseau et exporter les résultats** Commande : netstat -an > connections.txt Cela enregistre les connexions actives dans un fichier connections.txt.
9. **Trouver la connexion réseau la plus active** Commande : netstat -o Pour analyser ensuite les données, vous pouvez utiliser des outils comme Wireshark pour identifier les connexions les plus sollicitées.
10. **Trouver si une machine du réseau envoie trop de requêtes** Commande : netstat -an | find "SYN\_SENT" Analysez si une IP envoie trop de requêtes SYN simultanément, ce qui peut indiquer une activité suspecte.

Ces commandes vous offrent un contrôle détaillé sur les connexions réseau et facilitent l'analyse proactive des risques. Si vous souhaitez explorer une commande spécifique ou simuler un exercice, faites-le-moi savoir !