Operating System Commands

What is the command to get the processes running on another machine using WMIC?

**Tasklist command**

Networking

What is a DDOS attack and how can it be mitigated?

**-A DDOS attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. It can be mitigated by detection, response, routing and adaptation.**

Security Principles

Why is hardware and software inventory management critical to an organization's information security program?

**Hardware and software inventory is critical because a company must identify all the hardware devices and software applications that process their data. Most companies create lists in order to have insight into the components that may compromise an organizations infrastructure.**

Cyber Threat Intelligence

What does TTP stand for? Provide examples of each. BONUS: What framework provides a reference for TTPs that have been observed being used by real-world actors?

**TTP stands for tactics, techniques, and Procedures. TTP is a pattern of activities  or methods associated with a specific threat actor or group of threat actors.**

**Bonus : the MITRE att&ck frameork**