**Operating System Commands**

What is the Windows command to create a service on a remote machine?

sc.exe (ServerName) create (ServiceName)

**Networking**

What is port address translation and how is it different than network address translation? Which one is typically used in an enterprise environment and why?

PAT allows multiple users withing a private network to use minimal number of IP addresses. The difference between NAT and PAT is that NAT is used to map public IP addresses to private IP addresses. Whereas PAT is where multiple private IP addresses are mapped into a single public IP.

**Security Principles**

What are the three primary cloud deployment models and what are their differences?

* Public Cloud : cloud resources are owned, maintained and managed by a third-party provider
* Private Cloud: company itself is responsible for and bears the costs of the acquisition, deployment and maintenance of the cloud
* Hybrid Cloud: combination of both public and private cloud and allows companies to be more flexible and use more services

**Cyber Threat Intelligence**

Using information from this relatively recent advisory, provide examples for each of the four points of the Diamond Model (e.g. essentially putting last week’s research to work).

Adversary: Russia

Capabilities: Malware [Drovorub]; (capability for direct communications with actor- controlled C2 infrastructure; file download and upload capabilities; “root” command access; port forwarding of network traffic to other host.)

Victim: United States/Linux Operating Systems

Infrastructure: Linux Kernel

<https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF>