**Operating System Commands**

**What is the default PowerShell execution policy? How do you get the current execution policy? How do you set it to a policy that will require all scripts and configuration files be signed by a trusted publisher?**

The PowerShell Execution Policy is the setting that determines which type of PowerShell scripts (if any) can be run on the system.

The AllSigned Policy enables only scripts or configuration files that are digitally signed by a publisher you trust.

**Networking**

**What's the difference between DoT and DoH?**

DoH or DoT encrypts the queries which are disguised as regular HTTPS traffic. DoT only uses port 853, while DoH uses port 443, which is the port that all other HTTPS traffic uses as well.

**Security Principles**

**As it relates to cloud computing, what is the difference between single-tenant and multi-tenant infrastructure? Which poses more risk and why?**

Single tenant is a single instance of the software and supporting infrastructure serve a single customer, each customer has his or her own independent database and instance of the software.

Multi-tenancy means that a single instance of the software and its supporting infrastructure serves multiple customers. Each customer shares the software application and also shares a single database.

Multi tenancy poses more risk because everyone is sharing one software application and database, therefore information can be stolen.

**Cyber Threat Intelligence**

**Using information from this recent CTI report, provide examples for each of the four points of the Diamond Model.**

<https://www.clearskysec.com/wp-content/uploads/2020/08/The-Kittens-are-Back-in-Town-3.pdf>

Adversary: Iran

Capabilities: Malware; impersonating “Deutsche Welle” and the “Jewish Journal” using emails alongside WhatsApp messages as their main platform to approach the target and convince them to open a malicious link; attackers utilize fake LinkedIn profiles as well.

Victim: LinkedIn Users

Infrastructure: command and control trying to victim to click on malicious link as well attempts to send over malicious zip file to victim.