**Operating System Commands**

What is the command to set a registry key value using PowerShell?

* Set-ItemProperty-Path

**Networking**

Why would a company use a network proxy? BONUS: When are reverse proxies used?

* Companies could utilize proxy servers as firewalls and web filters. Good proxies keep users and the internal network safe.
* Bonus: Reverse proxies are used typically implemented for increased security and performance. Compress inbound and outbound data. Distribute client request.

**Security Principles**

How are vulnerability assessments different from penetration tests? Why is it important to do both?

* Vulnerability assessments scans for known vulnerabilities within your system and reports potential exposures.
* Penetration test are intended to exploit weaknesses in the architecture of your network and determine the degree to which a malicious attacker can gain.

**Cyber Threat Intelligence**

DIFFICULT: Malware is described as being "Stage A", "Stage B", etc. malware (NOTE: The actual stages are numbers, so "Stage <#>"). How many stages are there, and what makes them different? (No more than a sentence per stage...no reason to go into detail. I'm just trying to orient you as understanding malware and what is meant by something when it is stated in a CTI report is critical in our field.)

Stage 1 (Entry)- Accessing a hijacked website. Malware downloads silently and you have no idea that you are being infected.

Stage 2(Traffic distribution)- The malware redirects to an exploit server using techniques based on what computer you’re working with.

Stage 3(Exploit)- Available and supported exploit packs will attempt to leverage vulnerabilities in the browser.

Stage 4 (Infection)- The successful exploitation results in download of payload.

Stage 5 (Execution)-The malware will call home with sensitive data