APT & Zero Day Exploits Quiz

Directions: Chose the best answer to each question.

1. What does APT stand for?
	1. Advanced Phishing Template
	2. Abstract Patching Threats
	3. Advanced Persistent Threats
	4. Allowing Penetration Tests
2. APT is different from malware.
	1. True
	2. False
3. If malware and APT are different, what is the difference?
	1. Nothing
	2. APT is a manually executed and a highly researched attack
	3. APT is done on mobile devices only
	4. APT is always detectable while Malware is not.
4. What are the 3 stages to an APT?
	1. Infiltration; Lateral Movement; Extraction
	2. Import; Expand; Elude
	3. Steal; Organize; Abuse
	4. Attack; Pretend; Turn
5. What is a Zero Day Attack?
	1. An attack where hackers destroy a system in one day
	2. An attack that uses zero networking tools to infiltrate a system.
	3. An attack on an existing flaw in a system that had just been discovered but was always there
	4. A specific type of worm that encrypts a systems data
6. Which of the following is NOT a likely target for a Zero Day Attack?
	1. CEO
	2. A Bank Manager
	3. Wendy’s Cashier
	4. United States Government
7. What is a WAF?
	1. Web Allocating Fear
	2. Wired Attack Foundation
	3. Web Application Firewall
	4. Weak Application Flaw
8. What is Lateral Movement in Cybersecurity?
	1. Exploring and mapping a network while broadening presence in the network
	2. Initial movement to infiltrate a system
	3. Leaving a network with no trace of infiltration
	4. Hackers moving on to a new target with a new set of goals
9. Who is Wicked Panda (APT41)?
	1. A notorious APT group that took down power to large cities in China
	2. A individual who is responsible for stealing covid payment plans in America
	3. An notorious APT group who is believed to be tied to the Chinese Communist Party
	4. A group of Swedish APT hackers who broke into the US Government
10. Security professionals often beat hackers to patching a newly discovered security vulnerability.
	1. True
	2. False