Exam Objectives that do NOT Exist in Security+ SY0-401 but ARE in SY0-501

OBJ/Sub-OBJ	NEW in 501
1.0 Threats, Attacks and Vulnerabilities	
1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.	
· **Crypto-malware**	NEW
· **Keylogger**	NEW
· **RAT**	NEW
1.2 Compare and contrast types of attacks.	
· **Application/service attacks**	
o Amplification	NEW
o Domain hijacking	NEW
o Man-in-the-browser	NEW
o Pass the hash	NEW
§ Shimming	NEW
§ Refactoring	NEW
· **Wireless attacks**	
o RFID	NEW
o NFC	NEW
o Disassociation	NEW
· **Cryptographic attacks**	
o Known plain text/cipher text	NEW
· **Online vs. offline**	*Offline = NEW
o Collision	NEW
o Downgrade	NEW
o Weak implementations	NEW
1.3 Explain threat actor types and attributes.	
· **Types of actors**	

o Script kiddies	NEW
o Hacktivist	NEW
o Organized crime	NEW
o Nation states/APT	NEW
o Competitors	NEW
· **Attributes of actors**	
o Internal/external	NEW
o Level of sophistication	NEW
o Resources/funding	NEW
o Intent/motivation	NEW
· **Use of open-source intelligence**	NEW
1.4 Explain penetration testing concepts.	
· Passive reconnaissance	NEW
· Pivot	NEW
· Persistence	NEW
1.6 Explain the impact associated with types of vulnerabilities.	
· Race conditions	NEW
· Vulnerabilities due to:	
o End-of-life systems	NEW
· Improper input handling	NEW
· Improper error handling	NEW
· Resource exhaustion	NEW
· Untrained users	NEW
· Vulnerable business processes	NEW
· Memory/buffer vulnerability	
o Memory leak	NEW
o Pointer dereference	NEW
o DLL injection	NEW
· System sprawl/undocumented assets	NEW