Python Security Multi-Tool Project

This document is to show which tools from this project map out to the different tactics in the MITRE ATT&CK Framework. Use this as a guide, so that you know which tool to use for a certain situation, and when to use it. End goal is to combine all these functions into one large offensive framework, and one large defensive framework.

Reconaissance and Resource Development

Offensive Operations	Defensive Countermeasures
PortScan.py – Active Scanning	**HoneyScan.py**
DNSExploration.py – Passive Scanning	**HoneyResolver.py**

Initial Access

Offensive Operations	Defensive Countermeasures
TestDefaultCredentials.py – Valid Accounts	**ValidAccountDetection.py**
AutorunSetup.py - Autoruns	**AutorunDetection.py**

Code Execution

Offensive Operations	Defensive Countermeasures
WMIExecution.py – Windows Management Interface	**WMIDetection.py**
TaskScheduler.py – Scheduled Task	**ScheduleTracker.py**

Persistence

Offensive Operations	Defensive Countermeasures
RegAutorun.py – Autostart and Autoruns	**DetectRegistryAutorun.py**
ChangePath.py – Hijack Execution	**DetectPathModificationRegistry.py**
	DetectPathModificationEvent.py

Privilege Escalation

Offensive Operations	Defensive Countermeasures
LogonScript.py – Logon Scripts	**DetectLogonScript.py**
	PythonLibraryMismatch.py

Defense Evasion

Offensive Operations	Defensive Countermeasures
DetectAntivirus.py – Impair Defenses	**DecoyProcess.py**
TerminateAntivirus.py	
AlternateDataStream.py - Hide Artifacts	**DetectADS.py**

Credential Access

Offensive Operations	Defensive Countermeasures
ChromeDump.py – Impair Defenses	**DetectLocalStateAccess.py**
NetworkCredentialSniffing.py	**DecoyCredentials.py**

Discovery

Offensive Operations	Defensive Countermeasures
UserDiscovery.py – Accounts	**LastLogin.py**
	DetectAdminLogin.py
FileDiscovery.py – File Discovery	**MonitorDecoyContent.py**
	CreateDecoyContent.py

Lateral Movement

Offensive Operations	Defensive Countermeasures
RemoteServices.py – Remote Services	**DetectSMB.py**
WebSessionCookieHijack.py - HTTP Cookies	**CreateFakeCookies.py**
	DetectDecoyCookies.py

Collect Intelligence

Offensive Operations	Defensive Countermeasures
ModifyClipboard.py – Clipboard Data	**MonitorClipboard.py**
LocalEmailFiles.py - Email	**FindEmailArchives.py**

Command and Control

Offensive Operations	Defensive Countermeasures
EncryptedChannelClient.py – Encrypted Channel	**DetectEncryptedTraffic.py**
EncryptedChannelServer.py	

ProtocolTunnelingClient.py – Protocol Tunneling	**ProtocolDecoder.py**
ProtocolTunnelingServer.py	

Data Exfiltration

Offensive Operations	Defensive Countermeasures
DNSExfiltrationClient.py – over DNS	**DetectAlternativeProtocol.py**
DNSExfiltrationServer.py	
NonApplicationClient.py – Non-Application Layer Protocols	**DetectNonApplicationProtocol.py**
NonApplicationServer.py	

Impact – Achieving Impact

Offensive Operations	Defensive Countermeasures
DataEncryption.py – Data Encryption	**CheckFileEntropies.py**
AccountAccessRemoval.py – Account Removal	**DetectPasswordChange.py**