

About this learning path

- Learning path objectives
 - Develop custom Python scripts to automate cybersecurity tasks
 - Apply Python to meet objectives throughout the cybersecurity attack life cycle
 - Automate common cyberattack and defense activities with Python
- Course format
 - Course mapped to the MITRE ATT&CK and Shield frameworks
 - Python code for achieving MITRE ATT&CK and Shield techniques
 - Live demonstrations of Python applications



INFOSEC Skills

Course 1: Introduction to Python

Hello and welcome to this python for cybersecurity learning path.



Why Python?



Popularity

Python is currently among the most popular programming languages and one of the fastest-growing



Simplicity

Python's simple, readable syntax makes it easy to learn and use, perfect for quick scripts



Capability

Python includes a number of libraries, providing a massive amount of built-in functionality



Preparing for this learning path

- This learning path is designed to be interactive and driven by demonstrations
 - Creating Python scripts to solve real-world use cases
- All Python code will be completely explained
 - Prior Python experience is useful but not required
- The ability to create and run Python code is essential
 - Demos will use a combination of both Windows and Linux (many are platform agnostic)
 - Sample Python code will be written in Python 3

INFOSEC Skills

will be designed to achieve the objectives of specific attack and shield techniques.



Section 1: Introduction to MITRE ATT&CK and Shield



INFOSEC Skills

Hello, and welcome to this learning path for Python for cybersecurity.



What is MITRE ATT&CK?

- MITRE ATT&CK is a tool developed by the MITRE Corporation to improve cybersecurity understanding
- It maps different attacker techniques and procedures to the cyberattack life cycle and an adversary's goals

ATT&CK Matrix for Enterprise

layouts * show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 12 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 13 techniques
<ul style="list-style-type: none"> Active Scanning (1) Defect: Victim Host Information (1) Defect: Victim Identity Information (1) Defect: Victim Network Information (1) Defect: Victim Org Information (1) Phishing for Information (1) Search Closed Sources (1) Search Open Technical Databases (1) Search Open Websites/Domains (1) Search Victim-Owned Websites 	<ul style="list-style-type: none"> Acquire Infrastructure (1) Compromise Accounts (1) Compromise Infrastructure (1) Develop Capabilities (1) Establish Accounts (1) Obtain Capabilities (1) 	<ul style="list-style-type: none"> Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (1) Registration Through Removable Media Supply Chain Compromise (1) Trusted Relationship Valid Accounts (1) 	<ul style="list-style-type: none"> Command and Scripting Interpreter (1) Exploitation for Client Execution Inter-Process Communication (1) Native API Scheduled Task/Job (1) Shared Modules Software Deployment Tools System Services (1) User Execution (1) Windows Management Instrumentation 	<ul style="list-style-type: none"> Account Manipulation (1) BITS Jobs Boot or Logon Autostart Execution (1) Boot or Logon Initialization Scripts (1) Browser Extensions Compromise Client Software Binary Create Account (1) Create or Modify System Process (1) Event Triggered Execution (1) External Remote Services Hyack Execution Flow (1) Implant Container Image Office Application Startup (1) Pre-OS Boot (1) Scheduled Task/Job (1) Server Software Component (1) 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism (1) Access Token Manipulation (1) Boot or Logon Autostart Execution (1) Boot or Logon Initialization Scripts (1) Browser Extensions Create or Modify System Process (1) Event Triggered Execution (1) Group Policy Modification Hide Artifacts (1) Hijack Execution Flow (1) Process Injection (1) Scheduled Task/Job (1) Valid Accounts (1) 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism (1) Access Token Manipulation (1) BITS Jobs Client Update/Device File or Information Direct Volume Access Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (1) Group Policy Modification Hide Artifacts (1) Hijack Execution Flow (1) Impair Defenses (1) Indicator Removal on Host (1) Indirect Command Execution Masking (1) Modify Authentication Process (1) Modify Cloud Compute Infrastructure (1) 	<ul style="list-style-type: none"> Brute Force (1) Credentials from Password Stores (1) Exploitation for Credential Access Forced Authentication Input Capture (1) Man-in-the-Middle (1) Modify Authentication Process (1) Network Sniffing OS Credential Dumping (1) Steal Application Access Token Steal or Forge Kerberos Tickets (1) Steal Web Session Cookies Two-Factor Authentication Interception Unapproved Credentials (1) 	<ul style="list-style-type: none"> Account Discovery (1) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Process Discovery Query Registry Remote System Discovery Software Discovery (1) System Information Discovery System Network Tools/Scripts 	<ul style="list-style-type: none"> Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (1) Remote Services (1) Registration Through Removable Media Software Deployment Tools Tarred Shared Content Use Alternate Authentication Material (1) 	<ul style="list-style-type: none"> Archive Collected Data (1) Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Configuration Repository (1) Data from Information Repository (1) Data from Local System Data from Network Shared Drive Data from Removable Media Data Trapped (1) Email Collection (1) Input Capture (1) Man-in-the-Middle (1) Screen Capture Video Capture 	<ul style="list-style-type: none"> Application Layer Protocol (1) Communication Through Removable Media Data Encoding (1) Data Obfuscation (1) Dynamic Reservation (1) Encrypted Channel (1) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (1) Remote Access Software Traffic Signaling (1) Web Service (1) 	<ul style="list-style-type: none"> Automated Exfiltration (1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (1) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (1) Scheduled Transfer Transfer Data to Cloud Account 	<ul style="list-style-type: none"> Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (1) Defacement (1) Disk Wipe (1) Endpoint Denial of Service (1) Firmware Corruption Inhibit System Recovery Network Denial of Service (1) Resource Hijacking Service Stop System Shutdown/Reboot

So, let's start out by
talking about MITRE ATT&CK.

INFOSEC Skills



What is MITRE Shield?

- MITRE Shield was developed by MITRE to promote active defense
- It identifies different goals that an active defender may have and outlines methods for achieving those goals

[illegible]

Important terms

- The MITRE ATT&CK and Shield frameworks have several unique terms:
 - **Tactic**: The tactical goal at a particular stage of a cyberattack or a goal in active defense
 - **Technique**: A mechanism by which an attacker can achieve the goal outlined in a particular Tactic
 - **Sub-Technique**: A method for carrying out a particular Technique
 - **Procedure**: A specific implementation of a particular Technique or Sub-Technique

Credential Access

14 techniques

Brute Force (4)

Password Guessing

Password Cracking

Password Spraying

Credential Stuffing

INFOSEC Skills

etc that have been observed to
implement a particular technique.



MITRE ATT&CK Tactics

1. PRE-ATT&CK: Reconnaissance and Resource Development
2. Initial Access
3. Execution
4. Persistence
5. Privilege Escalation
6. Defense Evasion
7. Credential Access
8. Discovery
9. Lateral Movement
10. Collection
11. Command and Control
12. Exfiltration
13. Impact



MITRE Shield Tactics

1. Channel
2. Collect
3. Contain
4. Detect
5. Disrupt
6. Facilitate
7. Legitimize
8. Test

INFOSEC Skills

And so all of these are actions that an active defender can take to help



Structure of this learning path

- The purpose of this learning path is to demonstrate how Python can be applied to cybersecurity
- Each course focuses on an area of the MITRE ATT&CK or Shield frameworks
 - Tactics from MITRE ATT&CK
 - Specific applications from MITRE Shield
 - Decoys
 - Network-level active defense
 - Monitoring for active defense
- Each course will discuss some Techniques and Sub-Techniques in detail
 - Introduction to Technique
 - Python demonstration of applying a Technique or Sub-Technique

