Advanced Persistent Threats as Case Studies for Cybersecurity Education

Li-Chiou Chen and Joseph Acampora

Seidenberg School of Computer Science and Information Systems

Cybersecurity Education and Research Lab

Pace University

CAE Community Symposium, Seattle

June 2023

Source:

Agenda

- Advanced Persistent Threat (APT) Definition
- Stages and Techniques of APT
- APT Experiments and Case Studies
- APT Topics in Cybersecurity Curriculum
- Cyber Range for Research, Training and Education
- Discussion

What is an APT

- a class of network attacks;
- attackers utilize malware or stealthy tools to hide their actions;
- the threat typically presents in a network and systems over a prolonged period;
- attackers aim to achieve strategic goals;
- for example, causing substantial damage to the victim organization by data exfiltration.

Comparison between APT and Traditional Attacks

Traditional Attacks

- Single attacker
- Targeting at individual systems
- Aims for financial gains or demonstrating abilities
- Short time frame

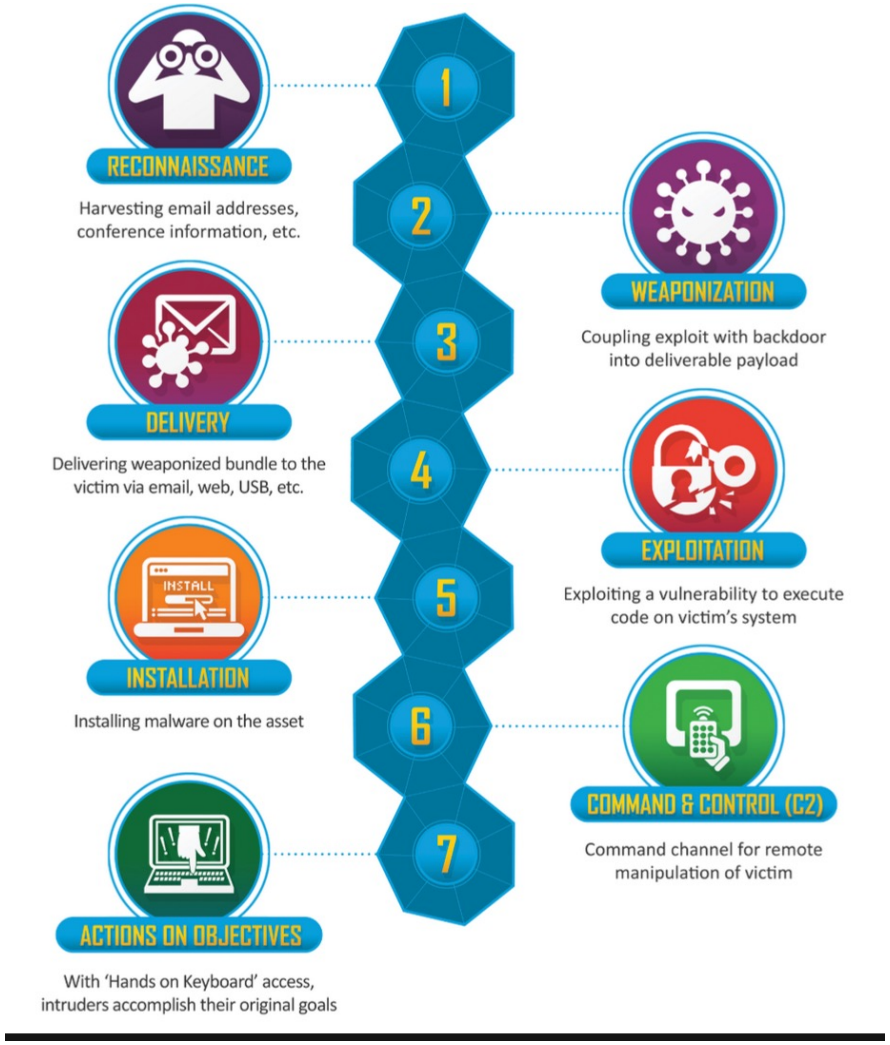
APT Attacks

- Organized groups with sophisticated skills
- Targeting at organizations, government
- Aims for strategic goals
- Long term acts, stay stealthy

Origins and History

- **Initial Use** : Around 2007-2008, the terminology APT appeared in the news to describe state-sponsored cyber attacks and DoD used to refer to specific threat actors.
- **Addressing Organizational Risk** : In 2011, NIST published 800-39 Managing Information Security Risk in which APT was defined and the organizational risk associated with APT was identified.
- **APT Detection Research** : Since 2010, many research studies have focused on APT detection.
- **Industry Practice**: Tools and solutions have been developed by industry from companies such as CrowdStrike, FireEye, Symantec, etc.

Stages of APT- Lockheed Martin Cyber Kill Chain

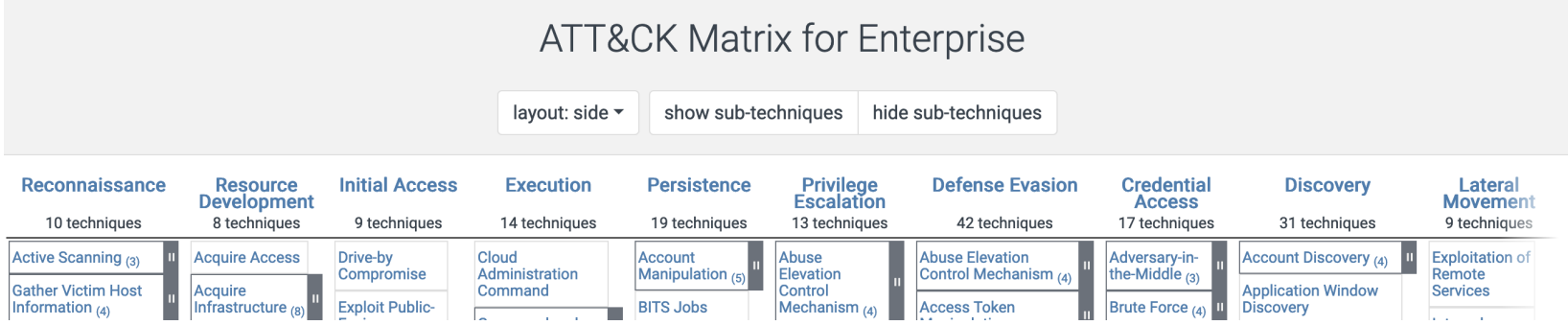


- Described APT in 7 stages
- A step-by-step approach to identify attack techniques

Source: The Cyber Kill Chain, Lockheed Martin, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Stages of APT - MITRE Att&ck

- A taxonomy of techniques, tactics and procedures utilized by APT
- Described APT in 10 stages and each stage is a collection of techniques



Source: MITRE Att&ck Matrix for Enterprise, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

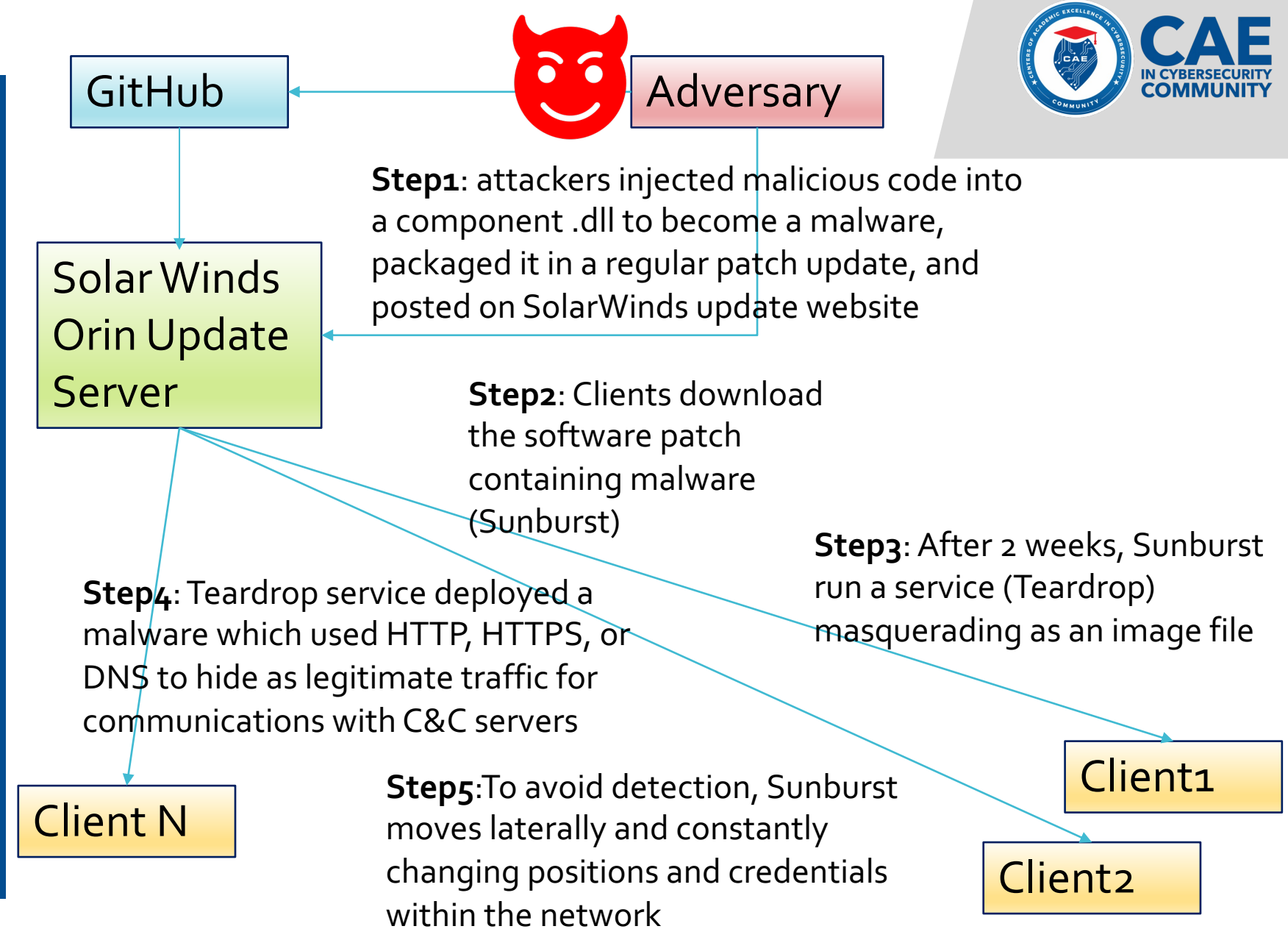
DARPA APT Experiments

- **Purpose**: For development of experimental prototype to provide forensic and real-time detection of APT
- **Datasets**
  - DARPA Operationally Transparent Cyber (OpTC) Program
  - DARPA Transparent Computing (TC) Program
- Used by many APT detection research
- Provide potential contents for APT techniques for case studies
- Finding needles in the hay – unbalanced dataset for machine learning

Case Study: SolarWinds

- The Story:
  - Solarwinds Orion infrastructure monitoring software is a popular cybersecurity monitoring software used by multiple organizations including US government
- Vulnerabilities
  - Solarwinds update server credentials were insecure
  - Solarwinds Orion advised clients to bypass EDR to avoid false positives
  - Vulnerabilities in authentication processes in software supply chain
  - Code integrity in software update
- Time Frame:
  - August 2019 : earliest recorded malicious domain registration
  - September 2019: Attackers accessed SolarWinds
  - December 2020: FireEye reported potential compromise

Case Study: SolarWinds



Case Study: SolarWinds

- Techniques used
  - more than 70 types of techniques are used such as Account Discovery, Account Manipulation, Forge Web Credentials, Use Alternate Authentication Material, …, etc.
  - Domain Generation Algorithm was used to establish a Command & Control server as a communication backdoor
  - Attackers setup valid digital signature and encryption infrastructure to spoof authentication of malware
- APT groups:
  - US and UK governments attributed it to APT29, Cozy Bear, and The Dukes;
  - Industry reporting referred to UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm

Knowledge Areas Needed for APT Defenses, Detection and Responses

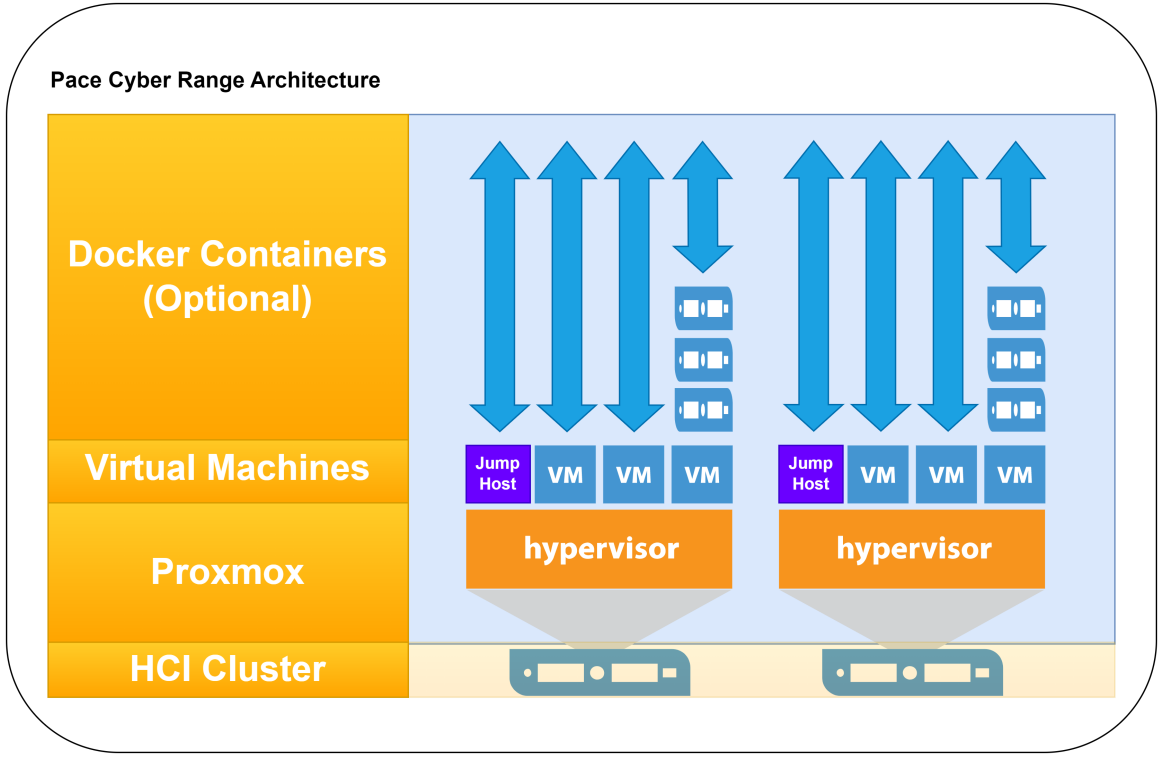
- Defenses
  - Host Hardening
  - Access Controls
  - Vulnerability Management
  - Security Policy Management
  - Trust Management
- Detect and Analysis
  - Log Analysis
  - Penetration Testing
  - Host based intrusion detection (end-point detection and response)
  - Malware Analysis
- Response
  - Risk Management
  - Incidence Handling and Response
- Mostly Importantly, APT stories that connects them all!

Incorporating APT Topics in Cybersecurity Curriculum

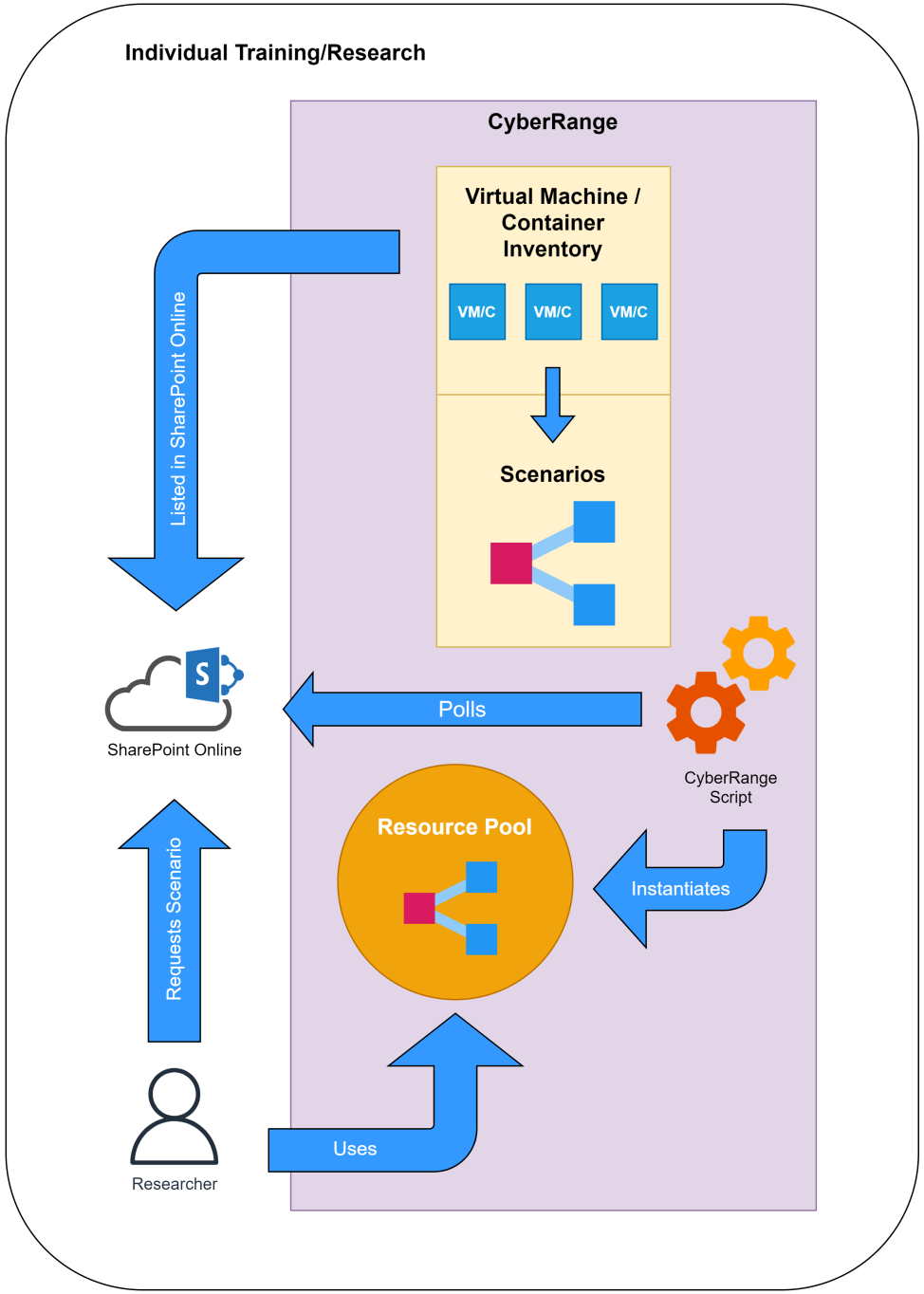
Response	Information Security Management (Security Policy Management, Risk Management, Incidence Handling and Response)
Detection	Penetration Testing and Ethical Hacking (Pen Testing, Vulnerability Management), Malware Analysis and Reverse Engineering (Malware Analysis)
Defense	Network Security (Intrusion Detection, Log Analysis), Introduction to Cybersecurity (Host Hardening, Access Controls, Trust Management)
Foundation	Computer Networking, Programming, Operating Systems

Pace Cyber Range: Use Cases and Architecture

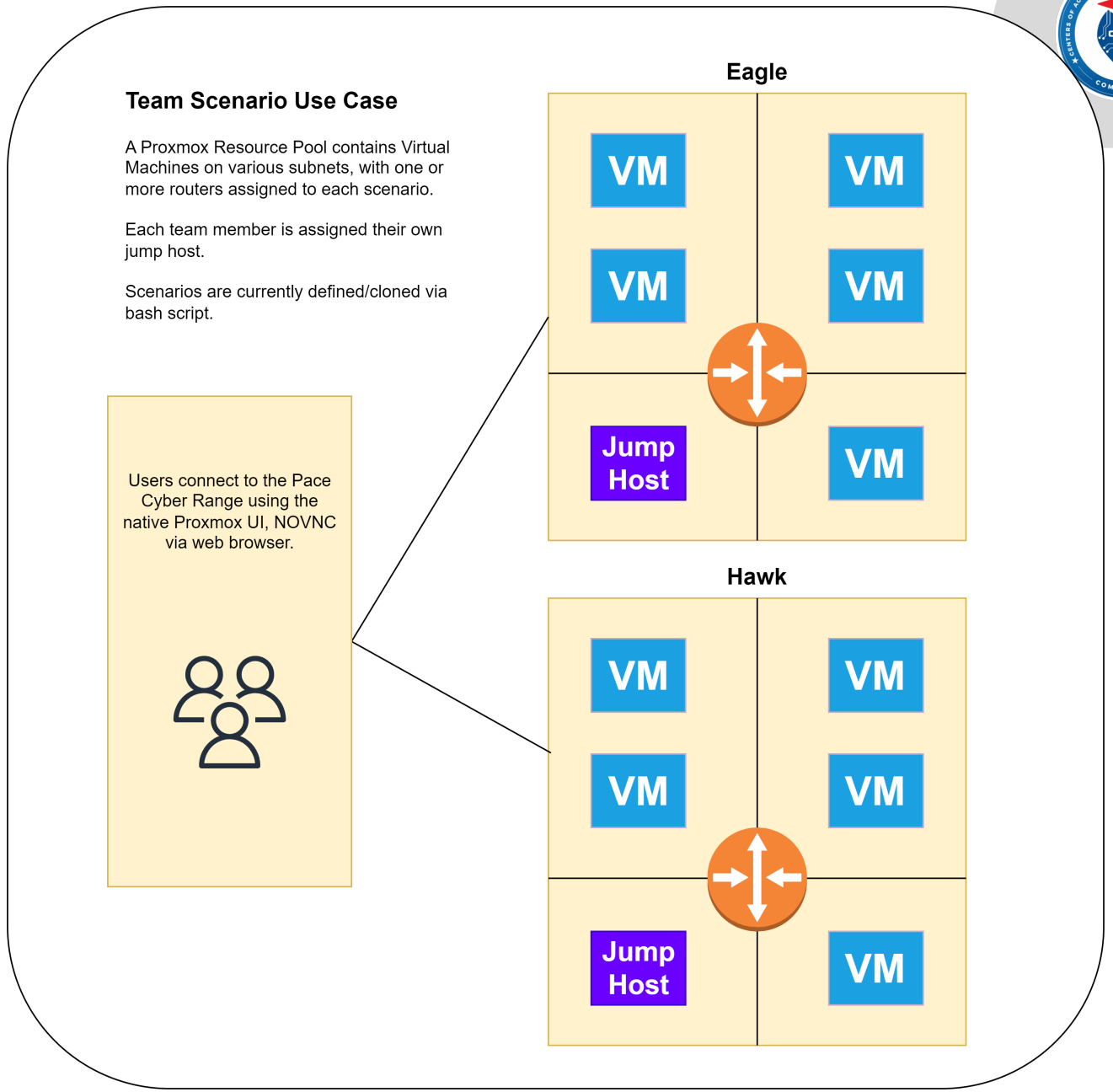
- **Use cases:**
  - APT simulations and data collection
  - Team competition scenario training
  - Cybersecurity class Labs
  - Individual attack/defend training



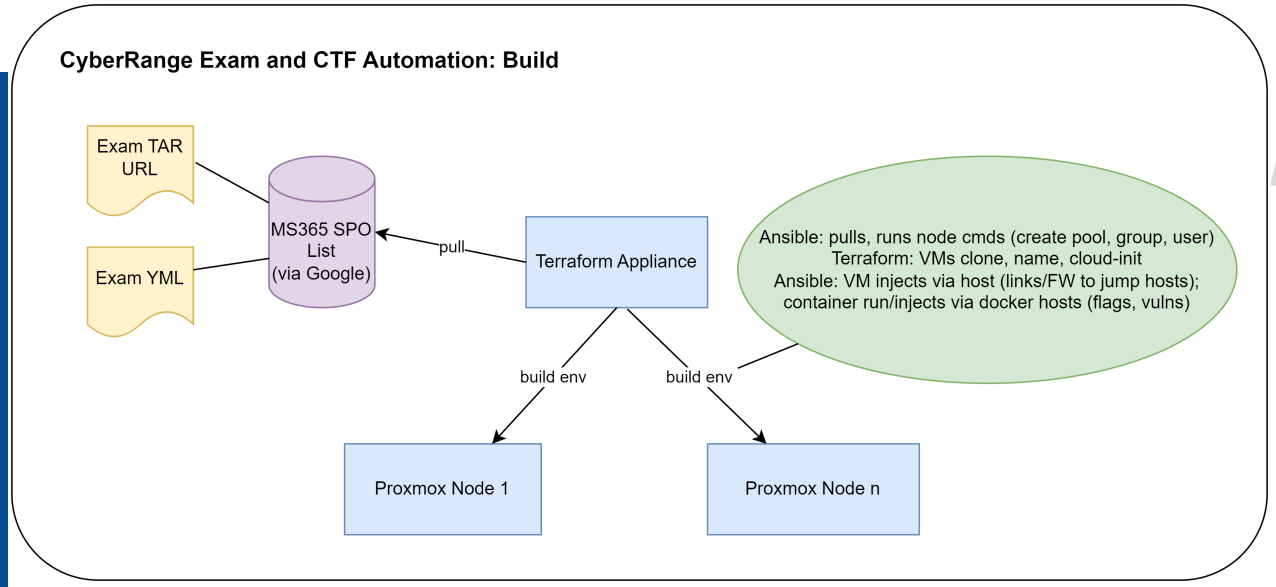
Individual Attack/ Defend Training

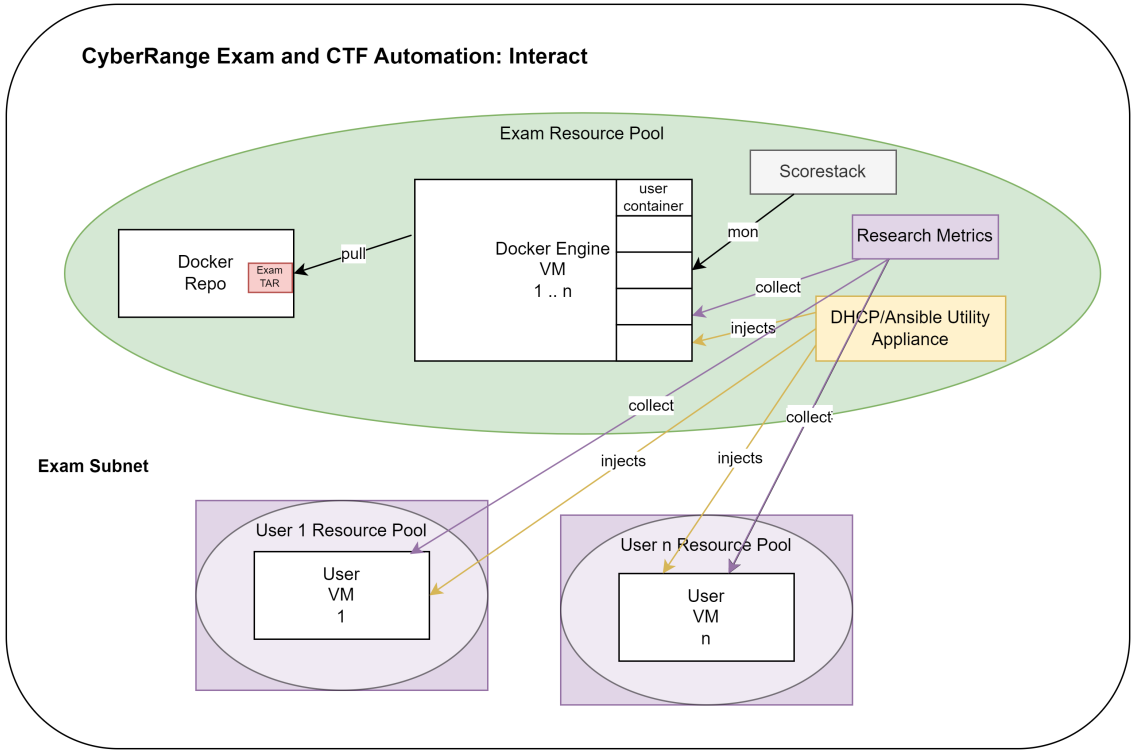


Team Competition Training

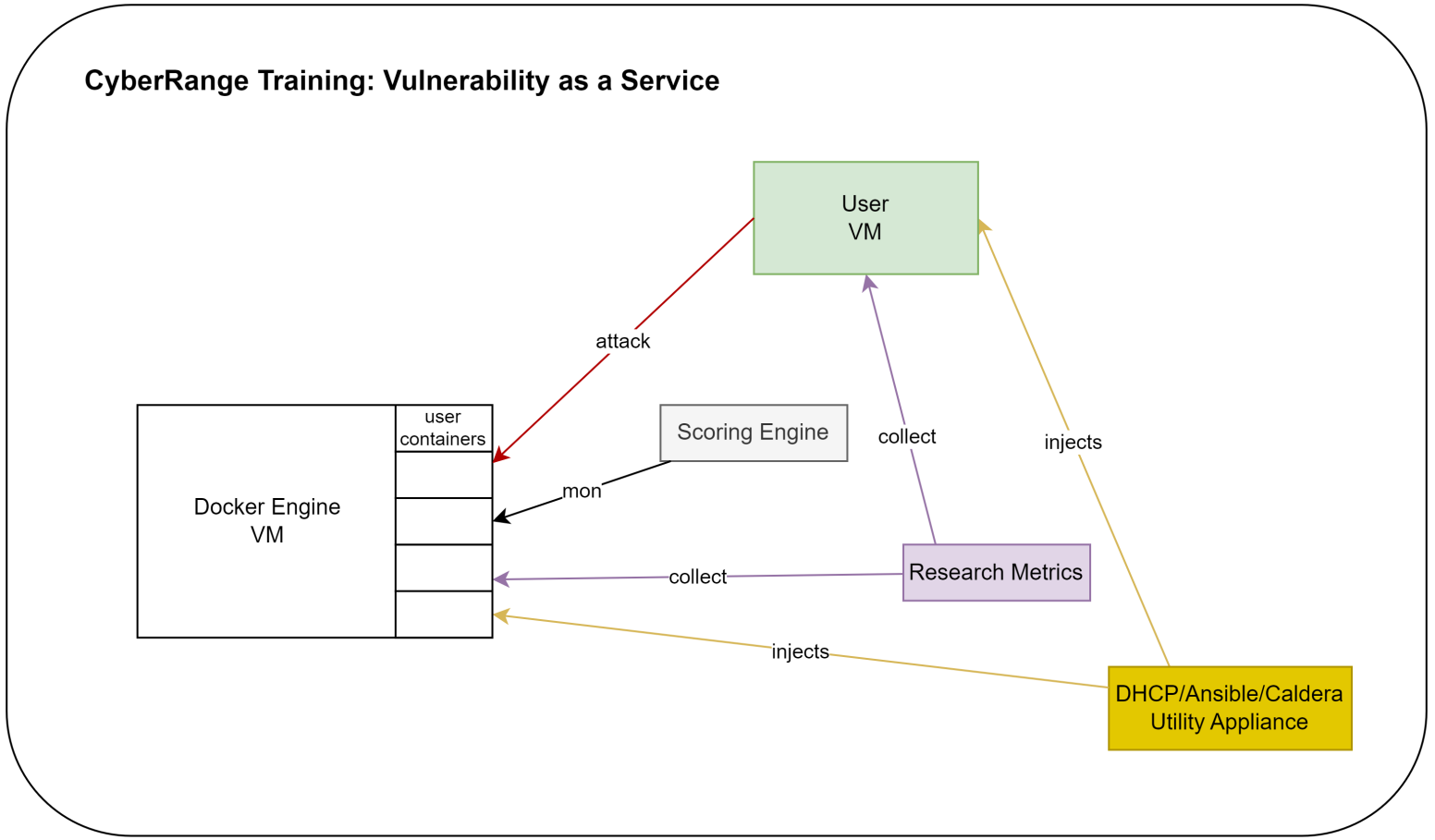


Automation for Building and Interactivity





Vulnerability as a Service for users, instructors or AI



Examples: Misconfigure conf file, registry key ● Downgrade version, auth level ● Edit firewall rule ● Adjust file permission ● Add/enable user

Discussion

- APT cases to connect the dots for students
- Scenario based exercises to consider APT defenses as a whole
- Team based exercises for interactions, communications and responses
- APT simulations on a cyber range for data collection or analyses utilizing machine learning

References

- Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. Computers & Security, 86, 402-418.
- Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851-1877.
- NIST, SP800-39(2011). Managing Information Security Risk—Organization, Mission, and Information System View, USA. Available at http://csrc.nist.gov/publications/PubsSPs.html#SP 800.
- MITRE, “SolarWinds Compromise,” available at https://attack.mitre.org/campaigns/C0024/
- Datta, P. (2022). Hannibal at the gates: Cyberwarfare & the Solarwinds sunburst hack. Journal of Information Technology Teaching Cases, 12(2), 115-120.

Acknowledgement

- The authors would like to acknowledge the support from the CyberCorps: Scholarship for Service Program of the National Science Foundation under Grant No. 2043095. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or the US government.

Contact Information

- Li-Chiou Chen, lchen@pace.edu
- Joseph Acampora, jacampora@pace.edu

- Cybersecurity Education and Research Lab (CERL), Pace University
  - https://www.pace.edu/seidenberg/faculty-and-research/centers-and-labs/cybersecurity-education-and-research-lab
- Pace University Cyber Range
  - https://cerl.seidenberg.pace.edu/cyber-range/