Students' Application of the MITRE ATT&CK® Framework via a real-time Cybersecurity Exercise

Aunshul Rege [1], Jamie Williams [2], Rachel Bleiman [1] and Katorah Williams [1]
[1] Criminal Justice, Temple University, Philadelphia, USA
[2] The MITRE Corporation, USA

rege@temple.edu
jcwilliams@mitre.org
Rachel.bleiman@temple.edu
Katorah.williams@temple.edu

Abstract: The MITRE ATT&CK framework enables practitioners to understand and track cyber adversary behaviors. Concepts such as social engineering (SE) are not directly captured in current version of ATT&CK as an individual technique, though the application of SE is relevant to many technical behaviors. Utilizing the ATT&CK framework in an educational setting, specifically within a competition focused on SE, allows students to explore adversarial behavior through experiential learning and understand how SE is relevant within cybersecurity. The structure of the framework allows students to see and describe each behavior from the perspective of the adversary, motivating them to compile and question "why" and "how" each individual action contributes to the operational objectives. This paper shares students' mappings of the ATT&CK framework to playbooks they developed during a real-time SE penetration testing competition. Students were given numerous flags to pursue during the competition and this paper will share their playbooks and mappings to the ATT&CK framework. This paper demonstrates that while someone with more knowledge and experience using the framework may map a SE case study differently than multidisciplinary students who are experiencing it for the first time, there is not a single correct way to map onto the matrix. Having students experience this mapping process allows them to understand the breakdown of an adversary's behavior and interpret key tactics and techniques in a way that fits their mapping needs. This paper also demonstrates how a SE case study can be mapped onto the ATT&CK framework despite SE not being the focus of the framework, and that SE uses tactics and techniques that are also relevant to technical cyberattacks. The authors hope to encourage more interdisciplinary cybersecurity education by sharing this experiential learning event.

Keywords: social engineering; pentesting; education; ATT&CK; attack playbooks

1. Introduction

A penetration test is a simulated cyberattack that is authorized by a company or organization to evaluate the security of the company's system. Traditionally, penetration tests are often technical in nature, utilizing such skills as network and application security, scripting, various operating system environments, cryptography, and remote access technologies, among a multitude of others. However, there also exist penetration tests that instead, or in part, rely on social engineering (SE) to evaluate the security of a company's system.

Social engineering is a technique where psychological persuasion of humans is used to "conduct reconnaissance (identify systems operating at target facilities), obtain information intended to secure electronic systems (passwords), or to encourage targets to inadvertently provide access to electronic systems and information (downloading and executing malicious files that are disguised as familiar or benign)" (Rege & Bleiman 2022). Because humans are often exploited in cyberattacks, a social engineering pentest can show how technical security measures can be bypassed without any technical expertise. Further, without the reliance on technical skills, social engineering penetration tests offer students and professionals from multiple disciplines an avenue into cybersecurity.

To promote interdisciplinary engagement in cybersecurity, the authors designed and implemented a social engineering pentesting competition in the summer of 2021. During this competition teams of students used SE to capture a series of flags, created adversarial playbooks, and mapped their playbooks to the ATT&CK framework. The framework, discussed in greater detail in the next section, organizes and describes cyber adversary behaviors and serves as a resource for threat mapping.

The following section describes the ATT&CK framework, including its tactics, techniques, and procedures as well as its various uses in education and competition spaces. Next, the paper describes the 2021 social engineering pen test competition, outlining the various flags that students were tasked with capturing. Then, the results include a deeper dive into five specific flags, discussing each's use regarding the flag and comparing its application across the different teams. The paper ends with a discussion of how ATT&CK applies to social

engineering, key takeaways from student mappings, implications for mitigation, and a consideration of the value of mapping exercises to students.

2. ATT&CK Framework

The MITRE ATT&CK framework enables practitioners to understand and track cyber adversary behaviors. The globally-accessible knowledge base (attack.mitre.org/matrices/enterprise) is maintained by the MITRE Corporation as a means of organizing and analyzing the tactics, techniques, and procedures (TTPs) used by real adversaries. The content within ATT&CK is informed by real-world observations and is continuously maintained via analysis of publicly available cyber threat intelligence (CTI) as well as contributions from the community of ATT&CK users.

ATT&CK is appropriately structured around organizing adversary behaviors into TTPs. Specifically, for each included behavior ATT&CK captures and contextualizes the adversary's:

1. Tactic(s), or "why" the behavior was performed
2. Technique, or "how" the adversary attempted to achieve their tactical goal by performing the behavior. ATT&CK also includes sub-techniques, which are functional equivalents to techniques but describe the specific behavior at a lower level than a technique (where applicable).
3. Procedure, or "what" the adversary specifically did to implement the technique

The organization provided by ATT&CK not only captures the adversary perspective of malicious cyber operations, but also facilitates the creation of a common, shared language for tracking these behaviors. This enables users to apply ATT&CK towards many operational use cases, including (but not limited to):

- Tracking and organizing new as well as known behaviors observed in threat intelligence/case studies
- Developing and aligning defensive countermeasures for specific behaviors
- Prioritizing and communicating behaviors used by a red or other form of offensive assessment team
- Engineering and documenting an organization's current defensive posture, including strengths and potential gaps relative to specific adversary behaviors

Though ATT&CK is selectively scoped to cyber activities (i.e., those directly involving victimized systems modeled into the framework as platforms), the structure and way of organizing TTPs is applicable to wider domains. This structure -- specifically modeling behaviors into why (tactics), how (techniques), and what (procedures) -- is conducive towards modeling and connecting behaviors to defensive countermeasures. Researchers have explored and used the blueprint of ATT&CK to create similar ATT&CK-like representations of differing adversary behaviors.

Concepts such as social engineering are not directly captured in current versions of ATT&CK as an individual technique/object, though the application of social engineering is relevant to many technical behaviors. For example, T1566 Phishing as well as many other behaviors exist where the "human-element" associated with the targeted system is exaggerated. These techniques specifically incorporate or even rely-on elements of persuasion, manipulation, elicitation, and impersonation for successful execution.

2.1 Uses of ATT&CK Framework

The ATT&CK framework has been used to introduce and expose various learners to security concepts, specifically the practice of modeling the cyber behaviors of threats (mitrecorp 2018). ATT&CK provides a structured process and prototype for tracking and understanding malicious activity within the context of analyzing why and how an adversary makes certain decisions and takes corresponding actions. An "ATT&CK-like" approach to modeling threats also lends towards exploring many different domains as well as use cases regarding defensive operations (Nickels et al 2019). The context provided by ATT&CK can also provide focus and a storyline to accommodate competition participants (Spunk 2019). For instance, groups of students mapped a social engineering case study onto the MITRE ATT&CK framework to understand the adversarial mindset for a course project. Having students experience this mapping project allowed them to understand the breakdown of an adversary's behavior and interpret key tactics and techniques in a way that fits their mapping needs (Bleiman et al. 2022).

3. Cybersecurity Competition

The ATT&CK framework was used in the Social Engineering (SE) Penetration Test Competition (SE-PTC) in the summer of 2021. The context of the SE-PTC was to conduct a SE pen test of the cybersecurity lab run by the

authors. Student teams would pose as pen testing firms the authors hired to test their (lab employees') vulnerability to SE attacks (Rege & Bleiman 2022). A total of 16 teams engaged in the competition: 1 high school team, 9 undergraduate teams, and 6 graduate teams (Rege & Bleiman 2022).

Each team had to accomplish a set of predetermined flags (tasks), such as acquiring information about lab employees' mail client and browser, obtaining copies of datasets and publications, convincing lab employees to change information on the lab's website, trying to get hired, and attempting to develop collaborations. Students had to use three SE tactics: OSINT, phishing, and vishing to pursue these flags.

OSINT or Open Source INTelligence involves gathering information from publicly available sources (Nickels et al 2019). Phishing occurs when a target is contacted via email by a cybercriminal who poses as a legitimate organization to lure the target into providing sensitive data, such as intellectual property, user accounts and passwords, or obtain confidential information (Nickels et al 2019). Vishing, or voice solicitation, has the same objectives as phishing (acquire sensitive information), but uses the phone or other voice over IP technologies (Rege & Bleiman 2022). More information about the competition structure and logistics is available in (Rege & Bleiman 2022).

Students then had to develop corresponding playbooks that documented their various strategies for each flag (Rege & Bleiman 2022). More specifically, students had to map their playbook strategies to the ATT&CK framework. For a more thorough discussion of the competition structure, logistics, and student experiences, please see the Rege & Bleiman (2022) paper.

3.1 Flags

Students were given numerous flags to pursue during the competition, which are displayed in Table 1 below. This paper will focus on flags 2, 3, 6, 10, and 12 to show student playbooks and mappings to the ATT&CK framework (marked with * in Table 1); these details for the remaining flags can be found in Appendix 1.

Table 1: Flags for the 2021 Summer SE Pen Test Competition

Flag #	Flag Description	# pursuing teams
1	Get the CARE Lab's Twitter account to Like a tweet posted by a competing team	10; 4
2*	Get the CARE Lab's Twitter account to Retweet a tweet posted by a competing team	8; 5
3*	Get the CARE Lab to disclose its office location and/or phone number	14; 5
4	Get the CARE Lab to disclose its mail client	7; 5
5	Get the CARE Lab to disclose its browser information	8; 4
6*	Get the CARE Lab to share its critical infrastructure ransomware incident dataset	11; 6
7	Get the CARE Lab to share its publications	9; 4
8	Get the CARE Lab to share its conference powerpoints	9; 4
9	Convince the CARE Lab to hire the team to host the CARE Pod	5; 5
10*	Convince the CARE Lab to update the lab website	7; 5
11	Convince the CARE Lab to update a rival team's page on the lab website	12; 5
12*	Collaborate with the CARE Lab to develop education projects	5; 4
13	Collaborate with the CARE Lab to be a guest on the CARE Pod	10; 4

3.1.1 Flag 2: Get the CARE Lab's Twitter account to Retweet a tweet posted by a competing team

For this flag, teams had to convince the CARE Lab employees to 'Retweet' one of their tweets. Overall, eight teams pursued this flag; five of the teams' playbooks are shared here (Figures 1-5).

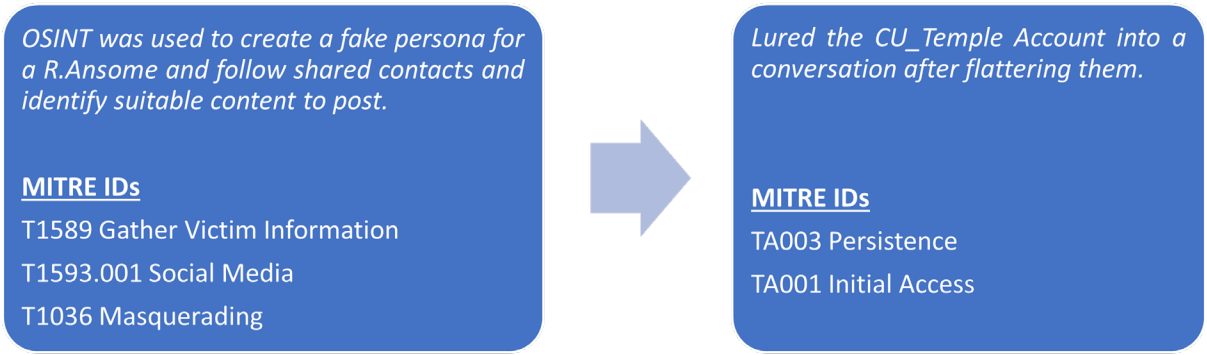

Figure 1: G1 playbook

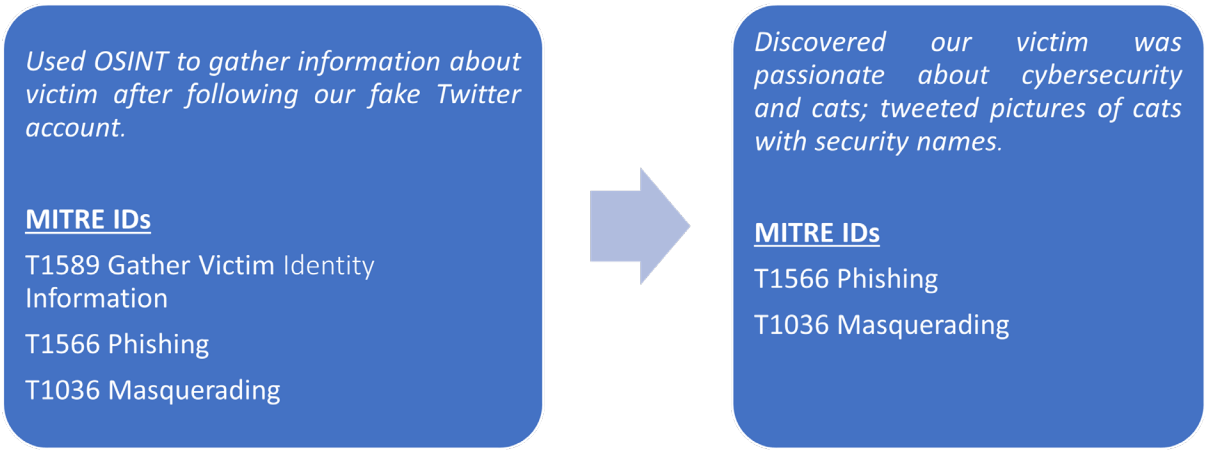

Figure 2: G2 playbook

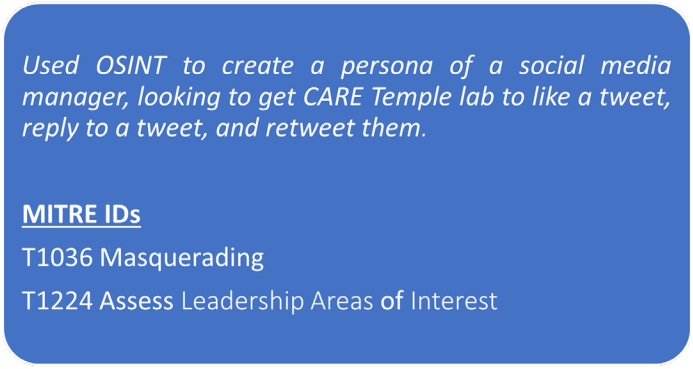

Figure 3: UG2 playbook

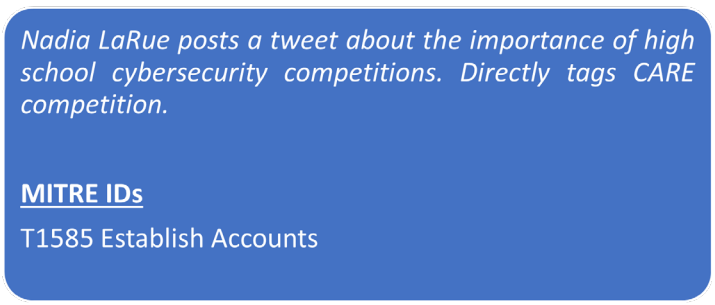

Figure 4: UG3 playbook

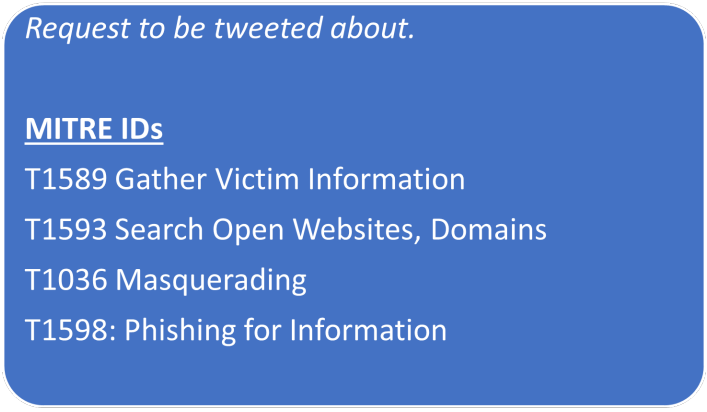

Figure 5: HS playbook

3.1.2 Flag 2 Analysis

The playbooks above indicate that the most commonly used technique was T1036: Masquerading, followed by T1589: Gather Victim Information. These are understandable given the objective; students had to collect OSINT on the Lab employees and correspondingly use that to masquerade and take on an identity. Interestingly, there were some techniques that were only used once across the various teams. Consider the tactics TA0001: Initial Access and TA0003: Persistence. While all teams did engage in both these techniques, only a few actually documented it. Furthermore, one team used a sub-technique, namely T1593.001: Social Media, while other groups primarily used the broader technique T1593: Search Open Websites/Domains. Thus, while many students did use social media in their OSINT, they may have just chosen to use the broader technique instead of the specific one.

Table 2: ATT&CK techniques identified by student teams for Flag 2

Technique ID	Tactic ID	Total	G1	G2	UG2	UG3	HS
T1036: Masquerading	TA0005: Defense Evasion	4	X	X	X		X
T1566: Phishing	TA0001: Initial Access	2		X			X
T1585: Establish Accounts	TA0042: Resource Development	1				X	
T1589: Gather Victim Information	TA0043: Reconnaissance	3	X	X			X
T1593: Search Open Websites/Domains	TA0043: Reconnaissance	2	X				X
N/A	TA0003: Persistence	1	X				

Majority of the playbooks above demonstrate that T1589: Gather Victim Information and T1593: Search Open Websites/Domains, which both belong to TA0043: Reconnaissance, were part of the first stage and thus aligned with the ATT&CK framework. Interestingly, T1036: Masquerading, which is part of TA0005: Defense Evasion (stage 7), is also listed as part of the first stage. The framework defines this technique as "the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names". However, students may have understood this technique as part of developing pretexts and personas, i.e., 'masquerading' as someone else.

The tactic placement of the techniques highlighted by the students also potentially sheds light on their perceived process for completing this flag. Despite the breadth of their actions (techniques), almost all of the playbooks included tactical decisions based on the shared goals of gathering information (TA0043: Reconnaissance) and/or avoiding detection (TA005: Defense Evasion). Finally, while some students listed TA0003: Persistence, they did not identify a specific framework technique.

3.1.3 Flag 3: Get the CARE Lab to disclose its office location and/or phone number

For this flag, teams had to get information about the CARE Lab, specifically to get employees to share their office location and/or phone numbers. Overall, 14 teams pursued this flag; five of the teams' playbooks are analyzed here.

3.1.4 Flag 3 Analysis

The majority of techniques identified in the playbooks were part of the TA0043: Reconnaissance tactic. A noteworthy observation is the variety of techniques that were used in this tactic: T1589: Gather Victim Information, T1591: Gather Victim Org Information, T1591.001: Determine Physical Location (the actual flag in this case), T1593: Search Open Websites/Domains, T1593.001: Social Media, T1594: Search Victim Owned Websites, and T1598: Phishing for Information. This demonstrates that students utilized an assortment of techniques to find information about the CARE Lab. Interestingly, some techniques such as T1036: Masquerading and T1113: Screen Capture, which appear in later stages of the enterprise matrix, TA0005: Defense Evasion and TA0009: Collection respectively, were used in the initial stages of the playbooks. The possible use of T1036 has been discussed above (see Flag 2 analysis).

Table 3: ATT&CK techniques identified by student teams for Flag 3

Technique ID	Tactic ID	Total	G1	G2	UG2	UG3	HS
T1036: Masquerading	TA0005: Defense Evasion	4	X	X	X		X
T1113: Screen Capture	TA0009: Collection	1					X
T1199: Trusted Relationship	TA0001: Initial Access	1		X			
T1585: Establish Accounts	TA0042: Resource Development	1		X			
T1589: Gather Victim Information	TA0043: Reconnaissance	1					X
T1591: Gather Victim Org Information	TA0043: Reconnaissance	2		X			X
T1591.001: Determine Physical Location	TA0043: Reconnaissance	1					X
T1593: Search Open Websites/Domains	TA0043: Reconnaissance	2			X		X
T1593.001: Social Media	TA0043: Reconnaissance	1	X				
T1594: Search Victim Owned Websites	TA0043: Reconnaissance	1		X			
T1598: Phishing for Information	TA0043: Reconnaissance	2		X			X
N/A	TA0003: Persistence	1			X		

3.1.5 Flag 6: Get the CARE Lab to share its critical infrastructure ransomware incident dataset

For this flag, teams had to convince the CARE Lab employees to 'Retweet' one of their tweets. Overall, 11 teams pursued this flag; five of the teams' playbooks are analyzed here.

3.1.6 Flag 6 Analysis

The playbooks above and Table 4 below show fewer techniques being used for TA0043: Reconnaissance compared to flag 3, which tried to get the Lab employees' office location. This may be related to what students envisioned an adversary would have to achieve in order to complete the flag (i.e., collecting or gathering information from a victim system, particularly the data from a specific website). The specific scope of the flag and resulting limited breadth of observed techniques mapped by the student playbooks can be used as valuable inputs to preemptively model and defend against this type of threat. A real adversary may vary their actions (techniques), yet potentially rely on successful completion of specific identified tactics and techniques central to completing this objective.

However, an interesting observation can be seen in UG3's playbook, which is the only one that captured technique T1005: Data from Local System and thereby captures the very essence of this flag (to exfiltrate the ransomware dataset). However, it is listed as the only technique throughout the playbook, which does not identify any reconnaissance (TA0042) techniques. Another interesting observation is the absence of TA0042: Resource Development, a tactic that was applied in Flags 2 and 3 above.

Table 4: ATT&CK techniques identified by student teams for Flag 6

Technique ID	Tactic ID	Total	G1	G2	UG2	UG3	HS
T1005: Data from Local System	TA0009: Collection	1				X	
T1036: Masquerading	TA0005: Defense Evasion	4	X	X	X		X
T1589: Gather Victim Information	TA0043: Reconnaissance	1					X
T1593: Search Open Websites/Domains	TA0043: Reconnaissance	4	X	X	X		X
T1598: Phishing for Information	TA0043: Reconnaissance	1					X
N/A	TA0003: Persistence	2		X	X		

3.1.7 Flag 10: Convince the CARE Lab to update the lab website

For this flag, teams had to convince the CARE Lab employees to 'Retweet' one of their tweets. Overall, seven teams pursued this flag; four of the teams' playbooks are analyzed here.

3.1.8 Flag 10 Analysis

The objective of this flag was to get the Lab to update its website. The student's mappings suggest a broader interpretation of how (tactics) and what (techniques) could be done to complete this objective. This suggests that the flag provided a wider possibility for adversary creativity, which widens the defenders attack surface while also creating opportunities to identify, track, and potential attribute threats based on their patterns.

In addition to the usual tactics and techniques seen thus far, one interesting tactic/technique used was TA0009: Collection/T1113: Screen Capture. The description for T1113 states that "the next goal after collecting data is to steal (exfiltrate) the data" (and therefore might appear a technique for the last tactic). However, it also states "Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives", which may explain that (in this specific context) students took a screenshot to further their objective for changing the website. Another interesting tactic choice was TA0040: Impact, which is the last tactic in the framework's chain. Interestingly, the technique used here is T1565: Data Manipulation, which aligns with this flag's objective. However, only one instance of this tactic/technique combination was found in the playbooks.

Table 5: ATT&CK techniques identified by student teams for Flag 10

Technique ID	Tactic ID	Total	G1	G2	UG3	HS
T1036: Masquerading	TA0005: Defense Evasion	3	X	X		X
T1113: Screen Capture	TA0009: Collection	1				X
T1199: Trusted Relationship	TA0001: Initial Access	1		X		
T1565: Data Manipulation	TA0040: Impact	1			X	
T1589: Gather Victim Information	TA0043: Reconnaissance	1				X
T1593: Search Open Websites/Domains	TA0043: Reconnaissance	2	X	X		
T1593.001: Social Media	TA0043: Reconnaissance	1				X
T1594: Search Victim Owned Websites	TA0043: Reconnaissance	1	X			
T1598: Phishing for Information	TA0043: Reconnaissance	2	X			X
N/A	TA0003: Persistence	2	X	X		

3.1.9 Flag 12: Collaborate with the CARE Lab to develop education projects

For this flag, teams had to convince the CARE Lab employees to 'Retweet' one of their tweets. Overall, five teams pursued this flag; three of the teams' playbooks are analyzed here.

3.1.10 Flag 12 Analysis

Given the broader nature of the objective of this flag (collaboration), it was interesting that few tactics/techniques were used. Students once again conducted OSINT (TA0043) on the Lab, developed a

pretext/persona (TA0005), and kept trying (TA0003) to secure collaboration. The student's mapping again suggests that pretext (knowing the victim) as well as evasion of scrutiny were central to this objective. This observation can be used by defenders against these types of threats, particularly by understanding what types of OSINT adversaries may seek and how they could acquire it.

Table 6: ATT&CK techniques identified by student teams for Flag 12

Technique ID	Tactic ID	Total	G1	G2	HS
T1036: Masquerading	TA0005: Defense Evasion	2	X	X	X
T1589: Gather Victim Information	TA0043: Reconnaissance	1			X
T1593: Search Open Websites/Domains	TA0043: Reconnaissance	2	X	X	X
T1598: Phishing for Information	TA0043: Reconnaissance	1			X
N/A	TA0003: Persistence	1	X	X	

4. Discussion

4.1 Limitations

Perhaps the biggest limitation is the low number of competing students, which affects the generalizability of these findings. Another noteworthy point is that students might use techniques they are most comfortable with. This is compounded by the temporal constraints of the competition that may limit a more thorough exploration of the tactics and techniques. However, this exploratory effort still offers a good abstraction of how social engineering techniques can be mapped to the tactics and techniques in the framework, which are discussed below.

4.2 ATT&CK tactics, techniques, and social engineering

This paper attempted to map social engineering strategies used by students during a real-time cybersecurity exercise to the ATT&CK framework. Table 7 provides a summary of the tactics and techniques used by students in the social engineering pen testing competition.

Table 7: Overview of tactics and techniques used by students in the competition

1. TA0043: Reconnaissance	2. TA0042: Resource Development	3. TA0001: Initial Access	5. TA0003: Persistence	7. TA0005: Defense Evasion	11. TA0009: Collection	12. TA0040: Impact
Gather Victim Identity Information	Acquire Infrastructure	Phishing	Create Account	Masquerading	Data from Local System	Data Manipulation
Gather Victim Org Information	Establish Accounts	Trusted Relationship			Screen Capture	
Phishing for Information	Stage Capabilities	Valid Accounts				
Search Open Websites/Domains						
Search Victim-Owned Websites						

Table 8 provides a summary of the most popular tactics identified by students. Given the theme of social engineering, it is not surprising to see the extensive use of TA0043: Reconnaissance, TA0042: Resource Development, TA001: Initial Access, and TA0003: Persistence, as they are essentially the preparatory work of OSINT, pretext and persona development, and studying the target.

One tactic, TA0005: Defense Evasion, specifically technique T1036: Masquerading was used extensively by students. This technique is described as occurring "when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation." The description also states that the technique "may include manipulating file metadata, tricking users into misidentifying the file

type, and giving legitimate task or service names." Students may not have considered this latter portion of the description and may have interpreted the first part of the description as applicable to the development of pretexts and personas, which were manipulative and helped evade defenses and observation.

There were a few tactics that appear later in the framework, namely TA0009: Collection and TA0040: Impact. Interestingly, Collection was used for flags 6 (get the dataset) and 10 (change website). In the first case, the specific technique of T1005: Data from Local System was used, which is expected given the objective of getting the dataset from the Lab. In the second case, students used T1113: Screen Capture to take a photo of the page that needed updating. Given that this tactic is often used before 'exfiltration', which applies to obtaining the dataset, but it could also precede the Impact, which was the Lab website posting incorrect (mis) information.

Table 8: Seven most popular tactics used by students

ATT&CK Tactic ID	Total
TA0043: Reconnaissance	66
TA0005: Defense Evasion	35
TA0003: Persistence	19
TA0042: Resource Development	13
TA0001: Initial Access	11
TA0009: Collection	3
TA0040: Impact	1

Table 9 provides details on the most popular techniques identified by students in their playbooks. Currently, the framework has 10 techniques for TA0043: Reconnaissance. Students used 50% of the techniques in this tactic. There are 7 techniques for TA00042: Resource Development and students used 43% of these. Students used 33% of the 9 techniques in TA0001: Initial Access. For the remaining tactics/techniques, students only used 1 or 2 techniques. However, it is interesting to note that the frequency of technique usage did not necessarily align with the number of techniques used. For instance, T1036: Masquerading (TA005: Defense Evasion) was the most used technique even though it was just one of 40 (2.5%) available techniques for this tactic.

Table 9: Nineteen most popular techniques used by students

AT&CK Technique ID	Total
T1036: Masquerading	35
T1593: Search Open Websites/Domains	28
T1598: Phishing for Information	16
T1589: Gather Victim Information	11
T1199: Trusted Relationship	8
T1585: Establish Accounts	6
T1583: Acquire Infrastructure	5
T1591: Gather Victim Org Information	5
T1594: Search Victim Owned Websites	5
T1224: Access leadership areas of interest	4
T1593.001: Social Media	3
T1113: Screen Capture	2
T1566: Phishing	2
T1608: Stage Capabilities	2
T1005: Data from Local System	1
T1078: Valid Accounts	1
T1136: Create Account	1

AT&CK Technique ID	Total
T1565: Data Manipulation	1
T1591.001: Determine Physical Location	1

4.3 A deeper dive into student mappings

The competition allowed for a glimpse into how students were mapping their playbooks to the framework. A few observations can be made:

1. The same flag can be accomplished through similar tactics and techniques despite variations in the pretexts/personas and OSINT gathered. This is expected given the nature of the flags, which required students to do OSINT and develop pretexts and personas. It also highlighted the creativity and human aspects of cybersecurity.
2. Some students may have converged several techniques that may have an overlapping meaning. For instance, when creating personas, students may have used T1036: Masquerading, T1585: Establish Accounts, or T1136: Create Accounts.
3. On several occasions, students used a Tactic but did not identify the specific technique that was used. This was mostly the case for TA0003: Persistence. Furthermore, there were also some occasions when students were clearly using specific tactics and techniques but failed to identify them in their playbooks.
4. Tables 15-17 demonstrate that the majority of the tactics and techniques used were part of the preparation work needed to start the various flags/objectives. Thus, students mostly used social engineering related tactics and techniques, which aligns with the competition theme and emphasizes the human-social-behavioral aspects of cyberattacks.
5. Some tactics and techniques were rarely listed in playbooks. Of particular interest are the tactics and techniques that appear later in the chain. For instance, TA0009: Collection (T1005: Data from Local System and T1113: Screen Capture) and TA0040: Impact (T1565: Data Manipulation) were hardly used. This may be an indication that students did not get far enough in their attempts to pursue the flags and hence did not list them in their playbooks.

4.4 Implications for mitigation

Currently, mitigation techniques identified in the ATT&CK framework do not offer much insight into solutions for social engineering techniques. Given the above analysis, an important point for discussion is what these mappings imply for mitigations against social engineering attacks. Given the detailed use of TA0043: Reconnaissance, TA0042: Resource Development, TA0001: Initial Access, and TA0003: Persistence, employee security training programs might spend more time on these specific tactics. The variety of techniques used in these preliminary tactics in the intrusion chain might further help in designing the training programs. For instance, if T1589: Gather Victim Information and T1591: Gather Victim Org Information are extensively used, training programs may emphasize limiting information that employees and companies make available publicly to limit OSINT findings. Consider for instance this excerpt from G3's report, which aligned their mitigation recommendations with specific techniques:

> The mitigation for Search Open Websites/Domains, Technique (T1593) has no easy mitigation other than control the information that individual can control outside of the organization such as social media privacy settings (e.g., public, private, friends only) and webpage settings (e.g., password protected). The masquerading technique (T1036) by tricking users into misidentifying the file type and giving legitimate task or service names can be mitigated by assigning an authentication code or number to the legitimate task, service, or persona (e.g., social security number). Phishing for Information using a spearphishing link (T1598.003) can be mitigated using anti-spoofing, email authentication, and cyber threat intelligence (CTI) mechanisms along with training to detect malicious links. Establish accounts, techniques (T1585) where adversaries create accounts (e.g., social media) has no easy mitigation other than threat intelligence of these accounts are potentially linked to bad actors.

These suggestions from students could be worked into training programs to make them more effective.

4.5 Value of mapping exercise to students and next steps

One of the biggest advantages the mapping exercise provides is that students can use it as an aid; it allows them to understand where they are in the intrusion chain and how their techniques have helped them move from (or not) one tactic to another to get closer to their objectives. These insights are invaluable to organizations working towards understanding and defending adversary campaigns. Mapping exercises (as well as real threat intelligence) provide insights into the tactics and techniques utilized by adversaries, which can be paired with defensive countermeasures that inform security decisions and operations.

Another important finding is that some of the flags' objectives/impacts may not be represented in the framework as they are intangible or do not align with the philosophy of how ATT&CK techniques are built. Consider for instance, flag 9 (getting hired - insider threat). This flag was accomplished by a few teams and is a legitimate threat for almost all organizations, but the concept of insider threats is not explicitly modeled into the current ATT&CK tactics and techniques. In this case, augmenting ATT&CK or using a use-case specific framework (such as the CTID Insider Threat TTP Knowledge Base) could help capture the nuances highlighted by the various student adversary playbooks. Similarly, flag 2 required the CARE Lab's Twitter account to Retweet a tweet posted by a team (who is posing as someone else). Retweeting a post from a bad actor could damage a company's reputation, which is another intangible harm.

This competition case study offered a first step into understanding how social engineering techniques could be mapped to the ATT&CK framework. For future competitions, the authors could implement the following changes. The competition theme could vary to test out how this influences the mapping process. Students could be given thorough mapping examples during the competition orientation, which would allow them to map more effectively. Students could also receive cheat sheets to make the mapping process easier and more efficient.

The authors hope other educators find this competition case study useful and a template for how to design their own unique and creative course projects that teach students about the wonderful ATT&CK framework and the mapping process.

5. Acknowledgements

This work was supported by the National Science Foundation Award # 2032292. The authors thank their university's ethics board for guiding us to ensure that this workshop was be safe, ethical, and fun for all those involved. The authors also thank their university's Risk Management Unit for preparing all the forms necessary for this workshop.

References

Bleiman, R., Williams, J., Rege, A. & Williams, K. (2022). "Exploring the MITRE ATT&CK® Matrix in SE Education". Proceedings from the IEEE Cyber Science Conference.

Mitrecorp. (2018). MITRE ATT&CKcon 2018: ATT&CK as a Teacher. Available at: https://youtu.be/4s3pZirFCPk).

Nickels, K. et al. (2019). "Getting Started with ATT&CK," ATT&CK. Available at: https://medium.com/mitre-attack/getting-started/home.

Rege, A. & Bleiman, R. (2022). 'Collegiate Social Engineering Capture the Flag Competition', *Proceedings of the 2021 APWG eCrime conference*.

Splunk (2019).. Boss of the SOC (bots) advanced apt hunting companion app: Now available on splunkbase, Splunk. Available at: https://www.splunk.com/en_us/blog/security/boss-of-the-soc-bots-advanced-apt-hunting-companion-app-now-available-on-splunkbase.html (Accessed: February 14, 2023).