# Exercise 2: Attack Models/Attack Modelling Techniques

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criteria** | **Lockheed Martin's Cyber Kill Chain Framework** | **MITRE ATT&CK Framework** | **Diamond Model** | **Attack Tree Model** |
| Year (in which year the model is created/introduced) | 2011 | 2013 | 2013 | 1999 |
| Developer (who created/introduced the model) | Lockheed-Martin | MITRE | the US Department of Defense | Bruce Schneier |
| Type of Model (what type of model is, e.g., intelligence driven/knowledge base/mathematical/graphical/hierarchical) | phase-based | a knowledge base of adversarial techniques | the diamond structure | systematic and illustrative method |
| Type of Usage (the model can be used for threat or attack detection, modelling, analysis, mitigation or something else) | Analysis、mitigation | analysis, mitigation | Threat、modelling,analysis | Modelling、analysis |
| Key Features (what are the main features of the model) | The Cyber Kill Chain framework is part of the Intelligence Driven  Defense model for the identification and prevention of cyber  intrusions activity. The model identifies what the adversaries  must complete in order to achieve their objective | document common tactics, techniques, and procedures (TTPs) that advanced persistent threats use against Windows enterprise networks | The model establishes the basic atomic element of any intrusion activity,  the event, composed of four core features: adversary, infrastructure, capability, and victim. | Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks. Basically, you represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes. |
| Operational Mode/ Stages/Phases/Structure (what are the different stages/phases of the model) | seven steps | 14 different tactics | the diamond structure  contains events, four core features, six meta features, and confidence values of features. | Tree structure |
| Complexity (how easy to apply/use for an attack modelling/analysis) | middle | high | high | High |
| Mitigations/ Countermeasures (whether the model provide mitigations and what mitigations) | a defender is required to only disrupt one attacking stage in the chain to stop that attack.  RECONNAISSANCE：  Collect website visitor logs for  alerting and historical searching.  Collaborate with web administrators to  utilize their existing browser analytics.  Build detections for browsing  behaviors unique to reconnaissance.  Prioritize defenses around  particular technologies or people  based on recon activity  WEAPONIZATION：  Conduct full malware analysis –  not just what payload it drops,  but how it was made.  Build detections for weaponizers  – find new campaigns and new  payloads only because they reused a weaponizer toolkit.  Analyze timeline of when malware  was created relative to when it was  used. Old malware is “malware off  the shelf” but new malware might  mean active, tailored operations.  Collect files and metadata  for future analysis.  f Determine which weaponizer artifacts  are common to which APT campaigns.  Are they widely shared or closely held?  DELIVERY：  Analyze delivery medium – understand  upstream infrastructure.  Understand targeted servers and  people, their roles and responsibilities,  what information is available.  Infer intent of adversary  based on targeting.  Leverage weaponizer artifacts to  detect new malicious payloads  at the point of Delivery.  Analyze time of day of when  operation began.  Collect email and web logs for  forensic reconstruction. Even if an  intrusion is detected late, defenders  must be able to determine when  and how delivery began.  EXPLOITATION：  User awareness training and  email testing for employees.  Secure coding training for  web developers.  Regular vulnerability scanning  and penetration testing.  Endpoint hardening measures:  Restrict admin privileges  Use Microsoft EMET  Custom endpoint rules to  block shellcode execution  Endpoint process auditing to forensically  determine origin of exploit.  INSTALLATION：  HIPS to alert or block on common  installation paths, e.g. RECYCLER.  Understand if malware requires  administrator privileges or only user.  Endpoint process auditing to  discover abnormal file creations.  Extract certificates of any  signed executables.  Understand compile time of malware  to determine if it is old or new.  COMMAND & CONTROL：  Discover C2 infrastructure  thorough malware analysis.  Harden network:  Consolidate number of  internet points of presence  Require proxies for all types  of traffic (HTTP, DNS)  Customize blocks of C2  protocols on web proxies.  Proxy category blocks, including  “none” or “uncategorized” domains.  DNS sink holing and name  server poisoning.  Conduct open source research  to discover new adversary  C2 infrastructure.  ACTIONS ON OBJECTIVES：  Establish incident response playbook,  including executive engagement  and communications plan.  Detect data exfiltration, lateral  movement, unauthorized  credential usage.  Immediate analyst response  to all CKC7 alerts.  f Forensic agents pre-deployed to  endpoints for rapid triage.  Network package capture  to recreate activity.  Conduct damage assessment  with subject matter experts. | it provides an appropriate level of categorization for adversary action and specific mechanisms of defending against it.  ATT&CK documents adversary group behavior profiles.  individual reports are used to document one particular incident or group, but this makes it difficult to compare what happened across incidents or groups and come to a conclusion on what types of defenses were most effective. With ATT&CK, analysts can look across groups of activity by focusing on the technique itself. When deciding how to focus defensive resources, analysts might want to start with techniques that have the highest group usage. | Establish a formal method applying scientific principles to intrusion analysis: those of  measurement, test ability, and repeatability – providing a simple, formal, and comprehensive  method of activity documentation, synthesis, and correlation. This scientific approach and  simplicity produces improvements in analytic effectiveness, efficiency, and accuracy. | In any real attack tree, nodes will have many different values corresponding to many different variables, both Boolean and continuous. Different node values can be combined to learn even more about a system’s vulnerabilities. Figure 6, for instance, determines the cheapest attack requiring no special equipment. You can also find the cheapest low-risk attack, most likely nonintrusive attack, best low-skill attack, cheapest attack with the highest probability of success, most likely legal attack, and so on. Every time you query the attack tree about a certain characteristic of attack, you learn more about the system’s security. |
| User Skill Level (what level of expertise required to apply/use the model) | middle | high | high | High |
| Knowledge Base – Database of Important Information (whether it provides knowledgebase and what level of knowledgebase) | none | The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community | providing a simple, formal, and comprehensive  method of activity documentation, synthesis, and correlation. | none |
| Documentation – Description of Model and its Operations (whether it provides documentation and what level of documentation) | <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf>  The site mentions the use of ckc，Above is the link | <https://attack.mitre.org/resources/getting-started/>  Blog | There's a paper about diamond models called Hello  “The Diamond Model of Intrusion Analysis” | None |
| Human Risk (whether it covers the human risk in the attack modelling/analysis) | Yes | Yes | Yes | No |
| Collaboration (who can collaborate in the attack modelling/analysis, e.g., only security experts or most stakeholders or anyone) | security experts | red team or penetration tester | most stakeholders | most stakeholders |
| Reusability (whether the developed model can be used for other similar attack modelling/analysis, e.g., fully or partially or some part of it) | Kill Chain is important,ATT&CK and The diamond are all borrowed and supplemented kill chain | PRE-ATT&CK covers the first two phases of the Kill Chain model, including tactics and technologies related to attackers' attempts to exploit specific target networks or system vulnerabilities for related operations.  ATT&CK for Enterprise covers the last five phases of Kill Chain | The diamond model and the kill chain are highly complementary. The kill chain analysis allows analysts to "target and attract an opponent to create the desired effect". The diamond model allows analysts to develop intelligence analysis tools and understand them, so as to build and organize the knowledge necessary for the execution of kill chain analysis | 1. Consequence Driven AttackTrees  2. Threat Analysis and Risk Assessment  3. Mitigation Trees |
| Use Cases (example scenarios where a written/graphical description of how users will perform an attack modelling/analysis using this model, e.g., Strategic and Tactical use cases) | 1.RECONNAISSANCE:  In this step, Intruder will try to select some potential victims, and they will try their best to find messages form victims.  2.WEAPONIZATION:  In this step, intruder will carefully design a special tool such as malware ,backdoor implant, and so on in order to make itself successfully hide in target’s structure.  3.DELIVERY:  In this step, the adversaries convey the malware to the target and launch their operations.  4.EXPLOITATION:  The adversaries will exploit a vulnerability to gain access.  5.INSTALLATION:  The adversaries will install a persistent backdoor or implant in the victim environment to maintain access for an extended period of time.  6.COMMAND&&CONTROL:  Intruders open a command channel to enable the adversaries to remotely manipulate the victims.  7.ACTIONS ON OBJECTS:  In this stage, the intruder will accomplish his goal, and gain full control of victim’s system. | 1.RECONNAISSANCE:  The attacker is trying to gather information to plan future operations to accomplish an attack. 2. Resource Development:  The attacker is trying to establish resources to support future operations to accomplish an attack.  3. Initial access: The attacker is trying to gain an initial access to the target system.  4. Execution: The attacker is trying to run malicious code on the local system or the remote system.  5. Persistence: The attacker is trying to maintain continuous access to the target system across restarts, changed credentials, and other interruptions that could terminate their access.  6. Privilege escalation: The attacker is trying to gain higher-level permissions and elevate access on the target system.  7. Defence evasion: The attacker is trying to avoid detection throughout their compromise of the target system.  8.Credential access: The attacker is trying to steal credentials to access the target system.  9. Discovery: The attacker is trying to gain more knowledge about the target system and its internal environment.  10. Lateral movement: The attacker is trying to enter and move through the internal environment of the target system.  11. Collection: The attacker is trying to gather information relevant to the attacker’s aim.  12. Command and Control: The attacker is trying to communicate with the compromised system to control and operate that system.  13. Exfiltration: The attacker is trying to steal data from the compromised system.  14. Impact: The attacker is trying to manipulate, interrupt, or destroy the compromised system and its data. | The diamond model is a cognitive model in addition to a set of mathematical techniques. The cognitive model allows security experts to organize large amounts of interrelated logic, whereas a set of mathematical techniques enables them to enhance strategic decision-making and analytical workflow against the adversary. | The AND relationship represents that all child nodes must need to perform their actions in order to achieve the action of the parent node.  and the OR relationship represents that any one child node needs to perform their action in order to achieve the action of the parent node. |
| Applications (Type of Computer Networks/Systems/IT Infrastructure, where the model can be effectively used) | CND.Identify patterns | Threat intelligence, detection and analysis, simulated attack, evaluation and improvement | intrusion analysis | Attack tree generation algorithm |

**Question:** Compare Attack Models/Attack Modelling Techniques in DETAIL.