StealthCup 2025 – V1.1 – 2025-03-25 / stealth.ait.ac.at

Permission to attack

Violation of these rules will result in disqualification:

- All the networks and hosts you target are within the range 10.0.x.0/24, where x (teamX) is your team_id. **Do not try to attack any other networks**, the internet, or the management network 10.0.0.242.0/24. You are dealing with small subnets here.
- Do not (intentionally) overflow, overload or DoS the open-source detection components (Wazuh, Suricata).
- Attacks on the IDS themselves are tolerated, yet your score will be validated manually. If you've exploited any IDS (backend) directly, your score won't count. The idea is to use evasion techniques, not to fuck up the IDS (backend).
- If any system gets unresponsive, or the disk is filled up, you will lose the current run and must reset.
- Do not delete any log files or command history on purpose, do not block or stop any network service as this will alert the admins and blow your cover.
- We use ansible for deployment, so don't get confused by "weird" open SSH ports. We use them for maintenance reasons.
- Do not restart any machines, doing so might influence the Kill Chain.
- The machines are hosted in the AWS. Intense calculations might freeze some of the machines, depending on CPU coins. If you hit the limit, your machines will freeze.

Objectives

- Enterprise Cup: You need to create a user called "plumber", that has domain admin rights.
- OT Cup: You need to leak chemicals. This is achieved by bringing the PLC into an unsafe state. We will validate if the PLC PORV flag is set, meaning an unsafe operation alarm was triggered, the safety valve popped, and chemicals leak into the sewers. ☹

Scoring system

- You will have access to all current alarms that you've triggered via the "dashboard".
- Any alarm triggered will give you penalty points. When you validate your challenge, your current penalty points will be frozen, resulting in your score for that given objective. The team with the lowest score wins!

- There are multiple detection systems in place that trigger alerts in four severity levels: Critical, High, Medium, and Low. All alerts from all detectors contribute to the score, but more severe alerts will be weighted higher. If you want to get on top of the leaderboard, you should therefore try to generate as few alerts as possible and specifically avoid severe alerts! The sum of all weighted alerts is finally also multiplied with a multiplicator that increases every time the infrastructure is reset. The final score is computed as follows: $\sum_{IDS}(\#critical * w_{critical} + \#high * w_{high} + \#medium * w_{medium} + \#low * w_{low}) *$
- $(1 + 0.05 * \#resets)$
- For example, let’s assume you have triggered the following numbers of alerts in the respective IDS:
    - Wazuh: 2 critical, 10 high, 934 medium, and 5423 low
    - Suricata: 0 critical, 0 high, 2 medium, and 0 low
    - Moreover, you already have reset the infrastructure twice. Assuming the weights 50, 3, 1, and 0.05 for critical, high, medium, and low alerts from Wazuh as well as 500, 30, 20, and 10 for critical, high, medium, and low alerts from Suricata, the final score is computed via [Wazuh: 100 (2 critical alerts) + 30 (10 high alerts) + 934 (934 medium alerts) + 271.15 (5423 low alerts)] + [Suricata: 0 (0 critical alerts) + 0 (0 high alerts) + 40 (2 medium alerts) + 0 (0 low alerts)] * 1.1 (2 resets) = 1512.6
- You can reset the infrastructure at any time via the dashboard. A reset will reset both the infrastructure and your score. However, by doing so, you will lose access to the infrastructure for approximately 10–20 minutes.
- Each reset increases a multiplier value, meaning that with every additional reset, your subsequent score will be calculated as <score> * <reset_multiplier>, resulting in a higher score.
- If multiple teams reset at the same time—or worse, slightly offset in time—delays may increase, as manual steps and background scripts are involved. Therefore, we recommend that the last reset be initiated at least 60 minutes before the end of the event. Please note that resets only happen every 15 minutes, allowing us to handle multiple resets in batches.
- The dashboard and most timestamps are in GMT+0. Event start and end times are in Vienna time (CET/CEST).
- Validation of results is immediate but score locking can take up to 5 minutes (we need to give the cloud EDR some time to do its magic …).
- When you lock your current score, it must be reviewed by us to be finalized. That means you need to submit a short write-up explaining how you (think you) bypassed the IDS. You don’t need to validate every result, but keep in mind: only validated one’s count.

Infrastructure

- The infrastructure will consist of the following:
  - Multiple Windows 2022 Servers and multiple Ubuntu 22.04 Servers
  - Multiple Active Directories including AD trusts, including some default Windows Server Services
  - An open source “SCADA/HMI” solution
  - An open source “Historian” solution
  - An open-source NIDS, HIDS, SIEM solution (detect only mode)
  - A commercial EDR solution (detect only mode)
  - An PLC from Phoenix Contact
  - Network Firewall(s) between the subnets
- You will gain access to a KALI box that your team has deployed during an active physical engagement. The KALI box is in the client network of the Plumetech Organization. You will have direct access to it via SSH (only) with port -p2020 + <team_id>. There are no outgoing port limitations from the KALI box.

Data policy

- The commercial EDR might send out data to its servers in Europe by default when the EDR agent is installed. We did not contact them to collect and analyze data, but this might be a default behavior.
- We will collect network data (PCAP), system log files and command histories. Please make sure that you don’t leak any private or personal data. If you do, please contact our ethics team who immediately will take further actions to remove that data. The data we collect will be analyzed for the purpose of cyber security research and might be published in full or part following open science best practices.
- We will not publish any team names or names of individuals, unless you want us to do so. In that case, please reach out to us, we are happy to help ;)

Other onsite infos

- You will have separate war rooms, most of the teams will have their own room (first come, first serve). Please bring your gear. We will have a limited set of extra monitors for you. Wifi only!
- If you want to listen to music, please bring your own Bluetooth speakers.
- There are pictures being taken, if you don’t want pictures of you released anywhere, please ask the ethics team for a warning west and wear it throughout the event, this will help us to select photos for public release. ☺