Capture the Flag in ICS

Kaspersky Lab ICS CERT

Contents

What is CTF?

General idea

A capture the flag (CTF) contest is a competition for cybersecurity experts organized in the form of a game, in which the participants solve computer security problems. They must either capture (attack/bring down) or defend computer systems in a CTF environment. Typically, these competitions are team-based and attract a diverse range of participants, including students, enthusiasts and professionals. A CTF competition can take from a few hours to several days.

The winner is usually the team or individual scoring the most points at the end of the game. As in many sporting events, prizes are commonly awarded for first, second and third places. In the interest of contest integrity and respect for the game platform, CTF ground rules are shared with participants prior to the event. Violation of these rules may result in restrictions or even elimination from the competition.

CTF environment

Depending on the format of the competition and other preferences and restrictions, different types of infrastructure can be chosen as the CTF environment. It can be fully virtualized, entirely physical or a combination of both. Normally, it is designed to emulate both the IT and OT networks of a real-world industrial infrastructure.

Demo stand at the GeekPWN conference in Shanghai. October 24, 2017

The monitoring and control level of the ICS systems used in CTF contests approximates that of similar systems in real-world industrial facilities, such as electrical substations, oil refineries, factories, etc. It may include networking devices, SCADA, HMI, engineering workstations, PLCs, RTUs, sensors and actuators used by real-world industrial enterprises. It may also include modern IoT/IIoT assets/technologies, as well as safety and physical security systems. The physical level of an industrial facility is normally emulated using physical or digital models.

The ICS infrastructure is typically assembled on a logically isolated network, using a configuration analogous to that found in real-world facilities.

CTF Format

There are several variations on the capture the flag format. The most popular styles are jeopardy, attack-defense and a mix of the two.

In a jeopardy style CTF, teams must complete as many cybersecurity challenges as they can from a given selection, applying their skills and knowledge to a diverse range of computer security categories in novel and creative ways. Task categories typically include networking, programming, applications, mobile, forensics, reverse engineering and cryptography. A team is awarded a specific number of points for each challenge it completes.

In an attack-defense CTF competition, teams must capture and defend vulnerable IT and OT systems. To gain points, a team must retain control of as many systems as possible while denying access to other competing teams. More points can be earned when a team can demonstrate the physical consequences of attacks on a system, such as the shutdown of an industrial process or unsafe conditions, including short circuits, fluid leakages, an incorrect sequence of operations, etc. Watch a video from the demo stand at Kaspersky Industrial CTF, October 2016: https://youtu.be/WQy6qJyQ8MA.

Short circuit at the demo stand at Kaspersky Industrial CTF, October 2015

Finally, a mixed CTF is arguably the most challenging for the participants. Combining jeopardy and attack-defense styles, successful teams must strategically divide their efforts and play to the strengths of each of their members by completing security challenges while simultaneously hacking into target vulnerable systems, maintaining access to these machines and defending them against their competitors.

CTF goals

There are many reasons for organizing a CTF contest, including general awareness and education of an industrial enterprise's management and technical staff about cyberthreats before the company experiences them first-hand.

The attack-defense scenario can be used both to train OT specialists in responding to cyberattacks and to test the IT/OT security staff's skills in near-real-world attack scenarios.

A CTF offers a good chance to introduce security specialists to modern attack vectors, kill chains and advanced tactics and technologies used by different cyber security expert teams from around the world.

Another objective of a CTF could be to test of ICS equipment and system configurations already used at an enterprise's facilities or being considered for installation / upgrade. This is also a good chance to test ICS security products and solutions used at the enterprise or considered for installation on its IT and OT networks.

One more interesting objective might be to find new cybersecurity talent either inside or outside the organization. Holding a CTF can be a great way of identifying people who have the aptitude and skills to perform ICS penetration testing and general ICS cybersecurity tasks and activities.

A CTF can be also used as a team-building and security-awareness exercise for an enterprise's employees. The one- or two-day event would be split into two parts: a morning educational session to train the attendees to use offensive and defensive cybersecurity techniques and an afternoon session where they compete against each other in small groups. As a result of the event, each participant will acquire skills that will enhance the team's overall security capabilities.

Questions to answer before running a CTF

What are your objectives in running a CTF?

Running your own CTF contest can help build up security skills and find new internal and external talent.

What type of CTF contest do you want to run?

As mentioned above, it can be jeopardy, attack-defense or a mix of the two.

Will the CTF be open to the public?

Some CTFs are public events, in which the teams have to travel to a physical location where the CTF environment is set up. Some are online-only events (see our resource list), where all the participants need is an internet connection and a set of tools. Some CTFs are corporate or invitation-only events.

What about logistics?

When planning the contest, treat logistics as one of the key factors. The key points to check on the logistics plan are delivering and assembling the CTF environment and participants' travel arrangements.

What prizes and entry fees will you have?

Depending on the audience, different participant motivation schemes can be used. When appropriate, consider prizes for the winning teams as one of the motivators.

How will you staff your contest?

Organizing a CTF event involves a number of different roles. At the very least, you will need IT/OT cyber security experts to work in the capacity of judges and scorekeepers, IT and OT engineers to set up the CTF environment, as well as field staff to maintain the facilities at the CTF venue.

Why not share the CTF costs with a public event like a conference, exhibition etc.?

If you want to attract the attention of a security-expert audience and to invite the press to make news, you can run your CTF as part of a conference or other public event. This can also help to reduce the budget by sharing some of the costs with the main event. Of course, you'll need to make sure the audience of the conference will benefit from your CTF and enjoy it.

What's your CTF budget?

Normally, the following main aspects should be considered when planning the budget:

- CTF infrastructure designing / building / delivering / hosting costs
  In addition to the servers, workstations, network infrastructure, OT hardware (PLCs, sensors, actuators etc.) and software (SCADA, HMI, Historian etc.), and physical models, you need to budget for designing, building, programming, configuring, assembling, delivering and hosting a complete environment that simulates an industrial object.
  The infrastructure will be provided by Kaspersky Lab or a subcontractor.

- Finding participants
  To make the CTF competition an exciting show and to achieve your other goals, you will probably need to find experts competent enough not only to gain access to a restricted ICS environment but also to develop a successful attack scenario that will affect the industrial process, possibly with "physical consequences". Since experts in this domain are few, we usually run an open online "qualifications" round, selecting the teams with the best achievements for the final competition, where the qualified participants apply their skills to a real CTF environment.
  Kaspersky Lab will provide a set of services, including planning, preparation, support and reporting for the qualifications and the finals.

- Participant travel and accommodation
- Venue costs
- Personnel to organize and support the event
- The show
- Marketing materials
- Prizes
- Catering
- PR and media coverage

CTF timeline

A successful CTF event consists of several stages

Initiation stage

The Kaspersky Lab team will conduct a workshop to agree on the format of the CTF and other general aspects of the event. During the workshop, Kaspersky Lab experts will provide all the necessary information and will help to define the goals and agree on the type and scope of the CTF. As a result of the workshop, an initial plan and a budget estimate will be developed. To achieve this, the Customer will need to involve managers, sponsors and specialists with the relevant roles and expertise, such as IT, Information Security, HR, PR, etc.

Workshop preparation usually takes up to 1 week.

Planning stage

At this stage, the Kaspersky Lab team and the Customer will plan all the required resources and budget in accordance with the initial plan. This stage usually takes about 2 weeks.

Based on the raw time and budget estimates, the final plan will be prepared, detailing all the required resources, budget items and logistics. The final plan will be reviewed and agreed by the Customer and the Kaspersky Lab team.

In the case of a public CTF, when planning the dates of CTF qualifications and finals, it is important to take into account all other public CTFs planned in the region and worldwide.

At this stage, the CTF working group will also be created. The Customer and the Kaspersky Lab team will assign specialists with the appropriate roles and responsibilities to the working group. A kick-off meeting will be conducted.

Preparation stage

At this stage, the working group will design and create the contest environment and infrastructure to run the qualifications and the finals. The duration of this stage depends on the type and scope of the CTF contest and is typically at least 1 month.

The Kaspersky Lab team will prepare the CTF qualifications tasks and infrastructure, do CTF promotion (in the case of a public CTF), and run the qualifications to select the teams that will take part in the finals.

This, along with preparing the virtual environment for the qualifications, will take 3 to 4 weeks. In addition, Kaspersky lab will host and run the CTF qualifications score tracking environment.

In parallel, the Customer will start activities to prepare the venue and infrastructure to conduct the finals and the awards ceremony. That work must be finished before the finals.

Qualifications stage

At this stage, all teams registered for the contest will attempt to solve tasks in the qualifications in order to make it to the finals.

The qualifications will take 2 days.

The Customer should make all the necessary announcements to launch the qualifications. The Kaspersky Lab team will monitor all activities and maintain the qualifications environment to ensure its availability throughout the qualifications, providing participants with assistance to ensure that the contest runs smoothly and that all participants have equal opportunities to win.

The qualifications results will be communicated to all participants. The winners will be granted access to the CTF finals. Any PR activities that are necessary will be performed.

CTF finalists' travel and accommodation will be planned, arranged and communicated to the Finals participants. This normally takes up 1 to 4 weeks, depending the participants' needs and venue requirements.

Finals

At this stage, the teams selected will travel to the CTF venue to participate in the finals.

The Kaspersky Lab team and the Customer will prepare the venue and the CTF Finals infrastructure.

Kaspersky lab will host and run the CTF Finals score tracking environment.

The Kaspersky Lab team will monitor all activities of the participants and will provide them with help and support during the finals.

During the contest, Kaspersky Lab will ensure that all the participants have access to the CTF Finals environment.

In addition, all of the participants' attack-related activity, including their successful attacks, will be tracked and logged, with network traffic backed up for further analysis.

The awards ceremony will take place when the finals are over and all the scores have been calculated.

Finally the CTF infrastructure will be shut down and disconnected. After this, only the Kaspersky Lab team and selected specialists of the Customer will have access to the data collected for the purposes of analyzing the CTF results.

Analyzing the results and reporting.

At this stage, Kaspersky Lab will analyze the data inside the CTF infrastructure and prepare a report. This stage usually takes about 1-2 weeks.

During a CTF contest, the participants generate vast amounts of network traffic and make numerous changes to the ICS environment model. The purpose of these activities is to gain control of the ICS infrastructure and make destructive changes. It is very important to analyze all the artifacts to potentially find new vulnerabilities (in some cases, 0-days) and new attack vectors. If a new vulnerability is found, the Kaspersky Lad ISC CERT team will perform coordinated vulnerability disclosure, enabling the respective vendor to fix it.

The Kaspersky Lab team will prepare the CTF technical report for the customer. The Customer can use it in accordance with the goals agreed at the initial stage.

Scope of service

To sum up, the CTF organization service may include:

- An initial workshop, planning, preparation, and project Kick-off.
- Renting or building, delivering and hosting the custom ICS infrastructure with an industrial process simulation environment
- Running qualifications
- Conducting PR activities
- Travel and accommodations for the CTF organization crew, the venue crew, CTF Finals participants, journalists and other attendees – as agreed with the Customer
- Renting a venue (if required)
- Running the CTF Finals
- Prizes
- Collecting all digital artifacts for analysis (network traffic, attack PoCs, memory dumps, disk images)
- Performing coordinated vulnerability disclosure for any 0-days identified
- Preparing CTF technical and executive reports

Our CTFs

Kaspersky Lab team regularly organizes and conducts CTF contests. A few of the latest CTFs organized by our team are listed below.

On January 23-26, 2018, the Massachusetts Institute of Technology (MIT), in collaboration with Kaspersky Lab, hosted its second annual “Think Security” seminar devoted to protecting industrial automation systems from cyberattacks. The event was organized jointly with MIT Cybersecurity at MIT Sloan (formerly (IC)^3) and the Sloan School of Management, with the participation of Kaspersky Lab’s Department of Educational Programs.

The seminar also featured an industrial Capture the Flag (CTF) contest, a shortened version of the annual contest organized by the Kaspersky Lab ICS CERT team. The competition included a variety of tasks ranging from Application Security, Binary Exploitation and Reverse Engineering to Digital Forensics, Fun, Cryptography and Networking. The most successful participants were awarded prizes.

Read the full story at https://ics-cert.kaspersky.com/events/2018/02/19/think-security/

The finals of the last Kaspersky Industrial CTF 2017, an industrial cybersecurity contest, were held on October 24, at the GeekPWN conference in Shanghai. This was the third CTF (Capture the Flag) tournament organized by Kaspersky Lab and the first to have the international status. Earlier, 696 teams from different countries had taken part in the qualifications. The three teams that competed in the finals were CyKor (Korea), TokyoWesterns (Japan), and Flappy Pig (China). The CTF environment consisted of a power distribution substation and an oil refinery facility

Finalist teams at the GeekPWN conference in Shanghai, October 24, 2017

Read the full story at https://ics-cert.kaspersky.com/events/2017/10/27/ctf_finals/

Video: https://news.cgtn.com/news/3d3d414d7a63545a326c4754/share_p.html

In October 2016, Kaspersky Lab hosted a cyber security event in which the RTDS Simulator was used to simulate a Micro Grid power and energy generation / delivery environment.

Demo stand at the conference in Kazan (Russia). October 2016

Read the full story at https://ics.kaspersky.com/conference-2016/

Video: https://www.youtube.com/watch?v=qf5u1TenxtM

Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT) is a global project of Kaspersky Lab aimed to coordinate the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky Lab ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the Industrial Internet of Things.

Kaspersky Lab ICS CERT Ics-cert@kaspersky.com