NÚKIB

National Cyber
and Information
Security Agency
of the Czech Republic

RED TEAM/BLUE TEAM EXERCISE

WHAT MUST BE CONSIDERED
BEFORE A TECHNICAL EXERCISE ENVIRONMENT IS BUILT

www.ncisa.cz

CONTENT

1. DESCRIPTION OF THE EXERCISE CONCEPT, ROLES AND TEAMS DISTINCTION

Technical exercises developed and executed in simulated virtualized environment allow for testing individual and collective skills. Thanks to their practical and interactive character, they represent very effective and attractive forms of education. One of the best and most used hands-on concept of technical exercise is Red team/Blue team model. It is a concept where Blue teams are responsible for the protection of a dedicated infrastructure that is under real-time attacks performed by an adversary - the Red team. Aside from the defending aspect, exercise players must report to leadership, react to company user's problems, and assess the potential legal and media impacts of the incidents. Such exercise is usually designed for security experts, incident responders, ICT administrators, and teams responsible for the protection of critical information infrastructure (CII), important information systems (IIS), or any kind of high-value assets.

Different teams with different roles are involved in the planning and execution stage. Each team is assigned with a generally accepted colour that describes its activities and responsibilities.

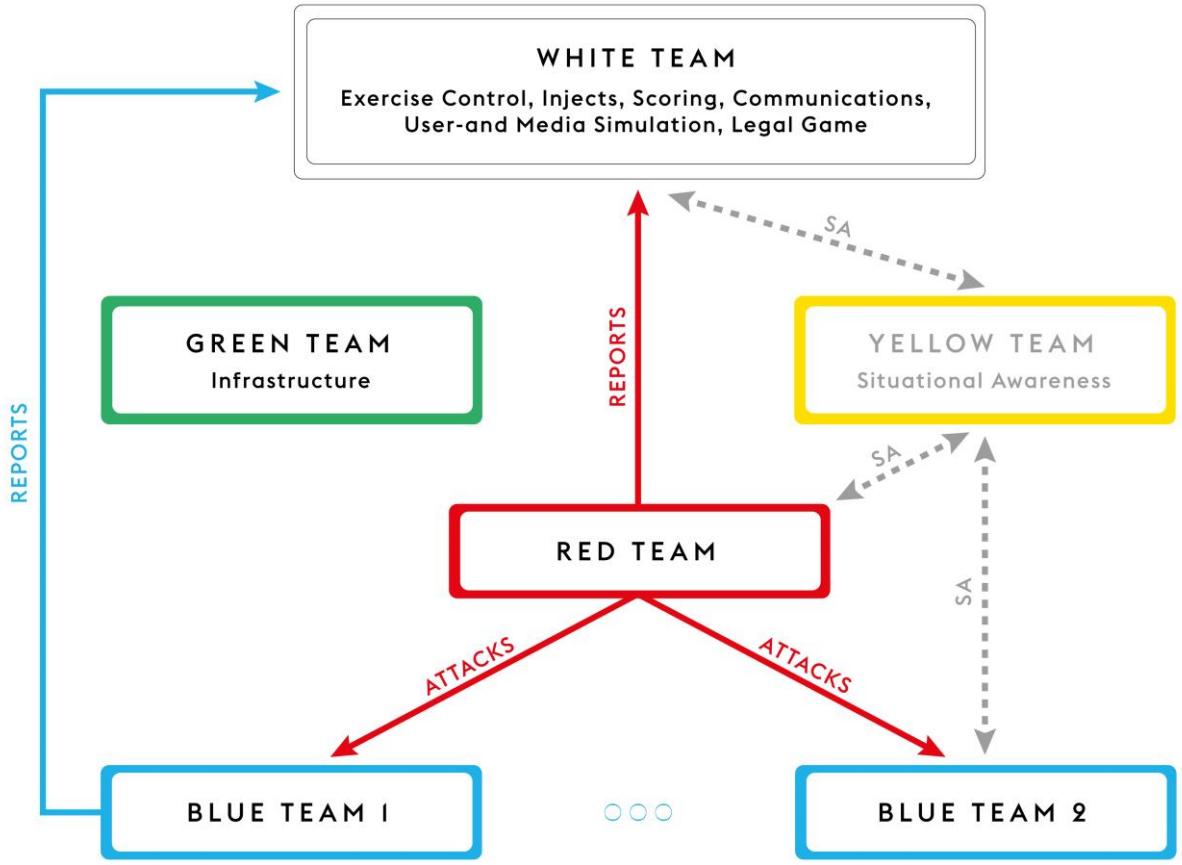

Figure 1: In the exercise each team has its own responsibilities and colour-based codenames that are commonly used in the ICT sector.

BLUE TEAMS:

- represent the main training audience,
- tasked to defend given infrastructure.

Depending on the exercise size, the number of teams and participants could range from e.g. small exercise of 5 teams of 4 people each to large exercise of 25 teams of 10 to 100 people each.

Two different approaches can be implemented to assemble a blue team.
It is the responsibility of:

- participating organization, that should choose the most suitable employees,

or

- planning team to create skills-balanced teams. To do so, each attendee must fill out an extensive questionnaire about his or her technical capabilities and skills. To ensure skills-balanced teams, there should usually be at least one person with following areas of experience – network protection, Microsoft environment and UNIX-like systems, and team coordinator.

RED TEAM:

- develops attacking techniques,
- launches cyber attacks against the Blue team's infrastructure in real-time.

The more the Red Team uses real-world attacking techniques to compromise the environment, the more authentic and beneficial an exercise is. The Red team usually consists of penetration testers or individuals responsible for active defense. Based on the size of the exercise, there are usually several sub-teams. Two basic types of approaches come into consideration:

- Each sub-team is responsible for executing the whole array of attacks. Each sub-team is responsible for one or several Blue teams.
- Each sub-team has a different focus and executes the subset of attacks against all Blue teams. The focus of teams could be end user attacks, network layer attacks, special infrastructure type attacks (e.g., attacks on industrial control systems, train operation system, nuclear power plant systems, drone command and control, etc.).

Usually, it is not a competition between Blue teams and the Red team, rather than between the Blue teams. The Red team is familiar with the infrastructure. On the other hand, the exercise can be used to educate Red team members as well, e.g. by requiring them to find some hidden flags in the machines and report their content to the leader/initiator of this task.

GREEN TEAM:

- designs and prepares the technical environment,
- strives to keep infrastructure running and operational during the exercise,
- manages all resources for virtualised systems,
- deals with all the issues reported by Blue or Red teams.

The Green team cooperates closely with the Red team to be able to distinguish the difference between a system being attacked and system not working correctly. The Green team checks the availability of legitimate services as the availability is part of scoring.

WHITE TEAM

- consists of exercise managers and planners (with project management skills rather than technical skills),
- is responsible for whole planning process and coordination with other teams including Red team,
- creates exercise scenario, geopolitical synopsis, and provides other supporting materials,
- is responsible for media and legal game by simulating it, or better by inviting legal advisors and professional journalists,
- simulates standard users alias blondies,
- ensures communication with training audience and other teams,
- represents the top authority for final scoring and any kind of decision.

YELLOW TEAM

- evaluates and scores reporting activities of Blue teams.

There are different types of reporting:

- Threat reporting includes indicators of compromise (IP addresses, malware files, URLs, or domain names) used by the Red team.
- Situation reporting that is designed to be forwarded to the coordinating body in line with the exercise scenario, e.g. security board. The situation report should provide an overall perspective and use the language accordingly.

The Yellow team is present mostly in bigger exercises. In smaller ones, the activities are usually covered by the White team.

EXERCISE OBSERVERS AND VISITORS

Exercise event poses a good opportunity for inviting partners and other stakeholders to establish and strengthen relationships. In that case, a special briefing for observers should be prepared to provide them with basic information.

2. EXERCISE COMPONENTS

THE RED/BLUE TEAM EXERCISE CONSISTS OF SEVERAL DIFFERENT COMPONENTS:

- exercise scenario,
- technical infrastructure[1],
- scenario injects (tasks from leadership, media requests, legal questions, status reporting),
- standard user simulation,
- scoring mechanism,
- and the Red team attack scenario.

An **EXERCISE SCENARIO** provides Blue teams with background story, current and overall situation, and all necessary information on the adversary group. It should be clear whether the exercise participants deal with a hacktivist group (with less sophisticated skills) or they face a state-sponsored group (with an almost unlimited budget, sophisticated skills and tools). Compared to non-technical exercise, the scripted scenario cannot go into the details.

According to the scenario, the Blue team is, in most cases, the Rapid Reaction Team (RRT) that is sent to assist to a fictitious organisation (e.g., power plant, train dispatch, military air base, etc.) that is under cyber attacks and is not able to handle the situation by itself.

Preparation of the **TECHNICAL INFRASTRUCTURE** includes:

- configuration of the legitimate servers, services, endpoint workstations, and network devices,
- developing vulnerabilities and attack vectors (e.g. outdated and unpatched systems and applications, vulnerable services and weak user passwords, default configurations and many unwanted or not needed applications, malware, logic bombs, etc.)

The size should be suitable for the expected Blue team size. It usually contains different network segments – demilitarized zone (DMZ), client segment, server segment, and industrial control system (ICS) segment and a central firewall. Basic logging and monitoring tools should be configured for Blue teams. The infrastructure should be as realistic as possible.

SCENARIO INJECTS cover several areas including:

- Specific tasks from leadership (anything from publishing an article on the web server running in DMZ segment, up to providing a description of security measures applied to the workstation in ICS segment),
- media requests,
- legal questions,
- and status reporting.

[1] The technical platform usually provides means for effective management of infrastructure virtualization, tools to check the availability of defined services, network traffic generation, scoring application, etc.

The goal is to show that the technical problems are not handled in isolation and the decisions made by the Blue team may have non-technical consequences. In addition, these kind of injects teach technicians to cooperate and communicate (and how) with executive management, legal advisors, and spokesperson in real life. The teams are forced to prioritize activities taking into account injects, systems patching, securing and monitoring.

STANDARD USER SIMULATION covers activities performed by employees of a fictitious entity where the Blue team is sent. The users must be able to perform standard activities without interruptions, e.g. browse the Internet, access corporate servers, operate the ICS systems, run applications, log into the machines in the infrastructure with legitimate credentials etc. From the Red team perspective, those users could be asked to run a malicious application simulating the phishing attack. As a defence, the Blue teams are required to apply suitable group policy, installing an antivirus software, or using any software restriction tool.

The **SCORING MECHANISM** covers 5 areas:

- Services availability,
- successful attacks,
- media and legal injects,
- reporting,
- communication with the entity´s employees.

The purpose of scoring is to motivate participants and to provide them with immediate feedback identifying strong and weak areas of the Blue team.

Extra points can be given or taken for machine revert to the initial state (restoring a previously saved state of the virtual machine) or the extraordinary team performance. Service availability category is based on an automated check of required services as they are defined in the rules. Team loses its points in case the service is unreachable, either due to the misconfiguration or an ongoing attack. Team is scored with negative points for successful Red team attacks. The number of lost points depends on the severity of at the attack, the difficulty of protection against such an attack, and also on the difficulty of execution of the attack

The Red team follows a **RED TEAM ATTACK SCENARIO** during the whole exercise. The scenario must be developed in advance. It defines clear Red team objectives. The main purpose of the Red team is to keep Blue teams entertained even in the case of a very good, knowledgeable, and experienced Blue team. The Red team needs to have enough attack vectors prepared with a different level of sophistication.

Basic attack vectors may include (sorted from the simple attacks to more sophisticated ones):

- non-patched applications and systems,
- well-known vulnerabilities and well-known malware,
- default configuration and password,
- users with wrong rights,
- wrongly configured services,
- non-required services,
- custom developed malware,
- rootkits,
- non-educated (malicious) users,
- logic bombs,
- self-developed applications,
- maliciously altered firmware,
- etc.

Red team activities should be in line with real-world techniques. They can include:

- network reconnaissance,
- scanning active systems,
- opening ports and applications listening on respective ports,
- defacements,
- denial of service (DoS),
- compromising machines to have access point to respective network segments,
- gathering data from users' computers,
- compromising system server, ICS segment etc.,
- disruption of the whole infrastructure by focusing on the firewall, domain controllers, or domain name service (final stage). *(see Figure 2)*

Keep in mind, there must exist an effective defence strategy for the Blue team for every attack launched by the Red team. Even for the Red team, it is necessary to plan the attack scenario in a way to keep Blue teams motivated. There should be visible consequences of attacks on Blue teams (e.g., defaced website, some important data deletion, stopping some necessary applications of services). Moreover, the standard user simulation team or the media should pinpoint those issues to Blue teams and ask them for resolution (in the case of users) or statement (in the case of media).

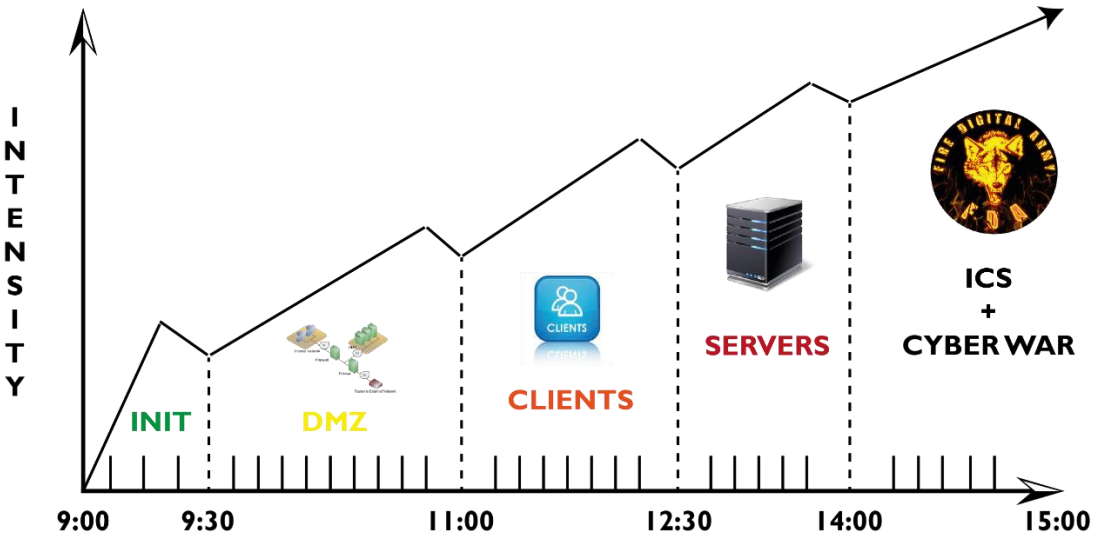

Figure 2: An example of Red team focus on different network segments (with different objectives) during the Cyber Czech 2016 exercise with the attacks timing and increasing attack intensity.

3. LIFECYCLE OF THE EXERCISE

There are several stages during the whole lifecycle of the exercise:

- **PREPARATION**
- **HACKATHON**

It is a several hours long dry run of the Red team attack scenario that is conducted about 4-6 weeks before the execution to verify that all attacks including scripts and automation are working properly.

- **TEST RUN**

It is the full exercise execution for few Blue teams conducted already on the prepared infrastructure to verify all parts of exercise are working together correctly. Blue teams usually consist of students or co-workers that did not participate in the exercise preparation. The suitable timing is 3 weeks before the execution to have time to fix discovered issues.

- **EXECUTION**

Its duration could vary from 2 up to 5 days for various exercises. It must include a familiarization period - Blue teams get access to the infrastructure and have several hours to analyse the infrastructure, find and fix any issues, configure the firewall, and take any defensive countermeasures.

- **FEEDBACK**

It might be in the form of structured questionnaire that covers all parts of the exercise. This is the most valuable input for the exercise evaluation and for the preparation of next iteration of exercise.

- **AFTER ACTION SEMINAR**

It is held roughly one month after the exercise and all members of Blue teams should participate. A detailed evaluation of all parts is provided together with a description of Red team attacks and scenario.

- **LESSONS LEARNED**

The best practices and lessons learned from the exercise are prepared and provided to the participants to allow them to incorporate those best practices into standard operations.

4. RESOURCES REQUIREMENTS

We use the national technical Cyber Czech exercise as a reference to share our own experiences with Red/Blue team exercise preparation and to summarize the exercise enter resources.

The Cyber Czech exercise has been regularly held since 2015 as a project of the National Cyber Security Center (currently within NCISA) of the Czech Republic together with the Masaryk University, Brno. The training audience of the exercise consists of 5-6 teams of 4 people each (24 participants maximum) responsible for the protection of CII and IIS from both public and private sector.

Enter costs for various resources:

1. **MANPOWER**
    - **GREEN TEAM**
        - Approx. 5 people responsible for designing core infrastructure and maintaining virtualised platform, installing and configuring operating system, setting up computing nodes, core-networking, deploying software and system configuration, storage etc.
    - **RED TEAM**
        - Approx. 5 people responsible for network infrastructure, building and implementing workstations and service exploits, implementing vulnerabilities, maintaining access against active defenders, penetration activity etc.
    - **WHITE TEAM**
        - Approx. 3 people responsible for sending/receiving injects, scoring, simulating media, publishing exercise news, users simulation etc.
        - Project management skills are required rather than technical skill.

2. TECHNOLOGY[2]

- Hardware including a physical central processing unit that is assigned to a virtual machine (720 vCPU), a computer memory (640 GB RAM) etc.
- Virtualization, choice of two basic options
    - VmWare that provides cloud computing and platform virtualization software and services

    PROS: enable to freely set up virtual machines, support service ensured by virtualization provider

    CONS: higher initial cost - approx. 120,000 EUR

    - KVM (Kernel-based Virtual Machine)/Virtualbox that is an open source virtualization architecture

    PROS: freeware, possibility to implement other functionalities

    CONS: no provider service support, additional work with functionalities implementation
- Computer licenses
- Project management/collaborating tool – e.g. Redmine (a free and open source web-based project management tool)
- Automation
    - Automation tools (e.g. Ansible, Teraform), requires knowing programming and scripting language (e.g. Yml, Python, Bash, Powershell)
    - Tools for traffic generation (self-written option)
- Monitoring
    - Software application for monitoring systems, networks and infrastructure (e.g. Nagios, Icinga2), requires writing own scripts for service monitoring
    - Logging tools
    - Scoring application, prepared by using HTML, JavaScript, CSS, Database

[2] The range of systems and services should be limited to suitable number allowing Blue teams reasonable management on one hand, yet it must allow incorporation of a sufficient number of vulnerabilities and attack vectors on the other. The development of infrastructure is an iterative process and it is not easy to keep track of current state of all machines as different machines are prepared by different people. The simple way to keep different versions of machines during the development is to use virtual machine snapshots.

3. FUNDING

- Hardware - approx. 320,000 EUR
- Virtualization - approx. 120,000 EUR
- Tools - mostly open source option
- Organization of the exercise including catering, rent of premises, social event, providing support services etc. – approx. 8,000 EUR

4. TIME

- A complete process from a first meeting up to the after-action seminar takes several months (usually from 8 to 12, depending on the exercise scope).
- Most of that time is spent on preparation of the infrastructure together with Red team attack scenario planning. One exercise could be executed repeatedly for different training audiences[3].

Keep in mind, the bigger the scope of the exercise is, the more human resources you need. If it is your first time you develop such technical exercise, allocate more time for preparatory phases to have the option to check and double check everything. If you want to imitate infrastructure you are not familiar with, consult/visit the experts from the field.

[3] There are several challenges connected with multiple exercise executions, especially when the time between them is several months long. In this case, it is usually necessary to repeat the hackathon before the exercise execution.

5. PRE-EXERCISE ANALYSIS

As the preparation of such exercise is money and time demanding, the return of such investment should be considered before the exercise environment is built.

Start with addressing several questions:

- **CONSTITUENCY -** Is your constituency/training audience wide enough so the exercise can be further offered/repeated?

  Do pre-analysis whether the cyber community is interested in such exercises (national or governmental CERT teams, others CSIRT/CSIRC teams and similar institutions). Alternatively, can the exercise be further commercialized and offered to private companies?

  If the exercise is tailor-made directly for one particular organization with the infrastructure mirroring the real infrastructure, keep in mind it is rather impossible to reuse it for any other organization.

- **COMPETITIVE PRODUCT –** Is there any similar product (custom made exercise/virtualized environment) on your domestic market?

  Do the market research to find out what similar products are offered on the market. Is it worthwhile to build your own infrastructure or buy custom built exercise? Consider total investment of both options.

- **FURTHER USE –** How can the technical infrastructure be further used?

  The training environment must be designed and built to maximize its benefit from the beginning. Consider its learning, research, and development use (e.g. preparing fully automated instructional scenarios, testing of technical skills for both red teaming and defending activities etc.)

- **SCOPE OF THE EXERCISE –** What will be to scope of the exercise? Will it be held remotely or do you need any special facility/equipment?

Make your decision whether to develop or buy technical platform/exercise based on the rationality and proper cost-benefit analysis, not because it is well-presented/good-looking and attractive.