Table of Contents

Background

The absence of institutional structures to deal with cyber incidents and attacks is a genuine problem in responding to cyber threats. ITU is helping countries to establish their National Computer Incident Response Team (CIRT), which serves as a national focal point for coordinating cybersecurity incident response to cyber attacks in the country.

A three pronged modular approach is proposed. Either component can be undertaken independently or can be aggregated to cater for the country's needs.

Assessment: The objective of the CIRT Assessment is to define the readiness to implement a national CIRT.

Implementation: After the assessment, the initiative assists with planning, implementation, and operation of the CIRT. Continued collaboration with the newly established CIRT ensures that support remains available.

Cyberdrill: Cyberdrills are conducted with teams from around ten national CIRTs where our experts study and evaluate the core functions of established CIRTS, to ensure that CIRTs are effective in managing incidents as well as ensuring proper inter-CIRT cooperation, consistent with international standards and good practice.

ITU strongly advocates fostering international cooperation through specific programmes such as coordinated cyber drill exercises between countries in ensuring continued collective effort against cyber threats.

In view of this, ITU will be organising a two-day cyber drill. The purpose of this simulation is to enhance the communication and participating CIRT/CERT teams' incident response capabilities and improve overall cybersecurity readiness in the region.

This exercise is undertaken with IMPACT as our key partner with unique expertise in deploying the drill and elaborating scenarios.

Drill Execution

The cyber drill will be based on fictitious scenarios to gauge the national CIRT incident handling capabilities. The exercise is structured around scenarios that included several incidents involving the most common types of attacks. The scenarios will be communicated simultaneously to all the participating teams via the communications channel provided. All resources including logs for the scenario will be made available to the teams. The drill facilitator explains and guides the team throughout the scenario analysis. The teams submit the solution in the form of an advisory report back to the organising team.

Sample Scenarios

- Web defacement
- Spam
- Malware analysis

Steps

1. The drill scenario commences with all participating teams receiving an email from the **organiser** on an incident
2. The email will contain:
    a. Scenario
    b. Advisory report template
3. **Participants** need to perform analysis on the incident and come out with ways to mitigate the threat
4. Drill **observers** in the team can assist the main drill player in performing the incident analysis
5. **Participants** need to submit the mitigation or recommendation based on the given advisory report template back to the organiser

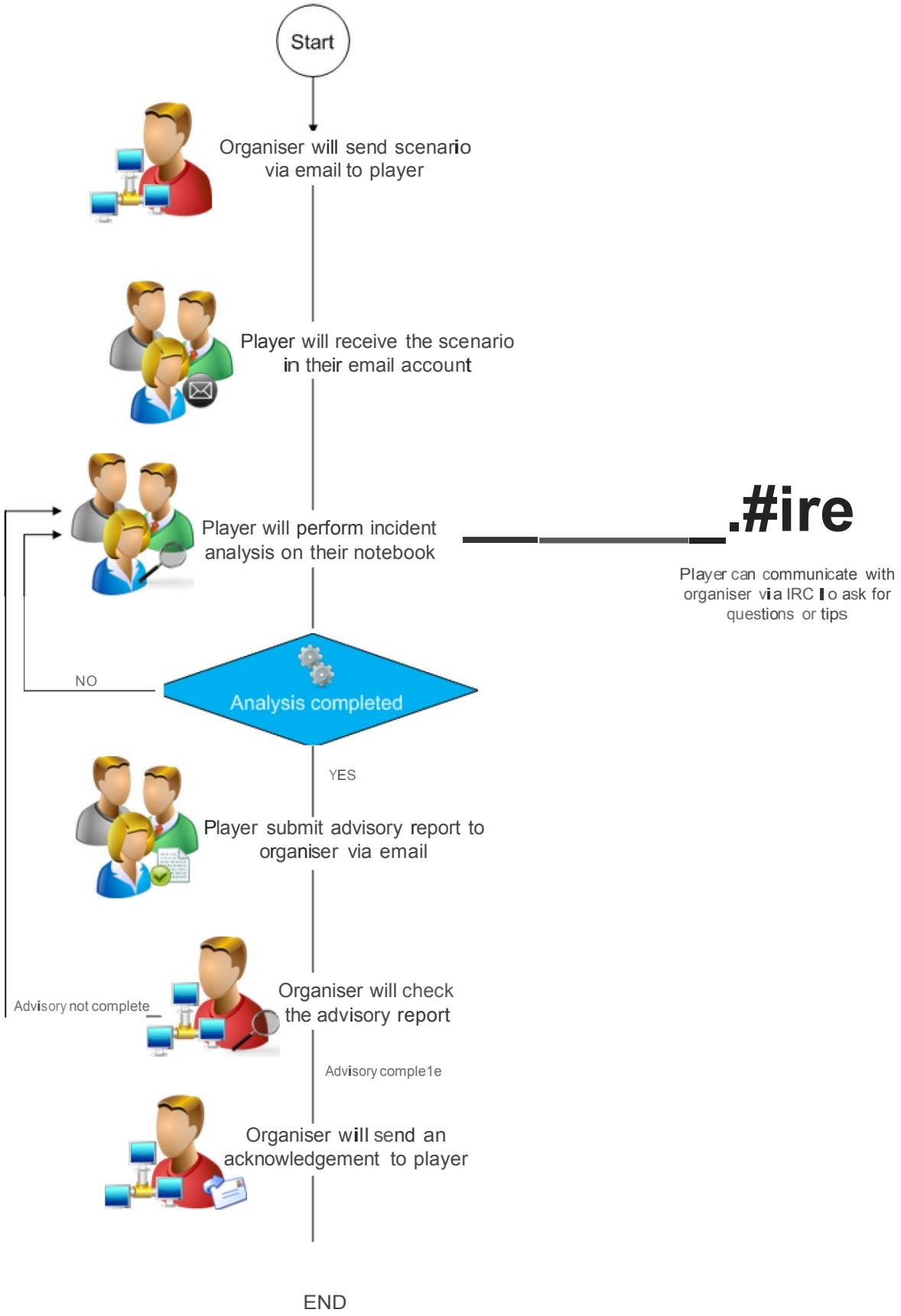


Figure 1 : Scenario Execution Flowchart

Drill Communications

Mail Server	All formal communications between the organiser and participants will go through this mail server
IRC Server	Will be used for: • Informal communication between organiser, participants and observers • Channel for participants to ask questions or tips on the scenarios • Ad-hoc alerts from the organiser • Collaborate with other participating CIRT as well as the organiser
DNS Server	Local DNS server for IMPACT-ALERT.NET domain
Scenario Server	This server hosts images for the cyber drill scenarios

Scenario Setup

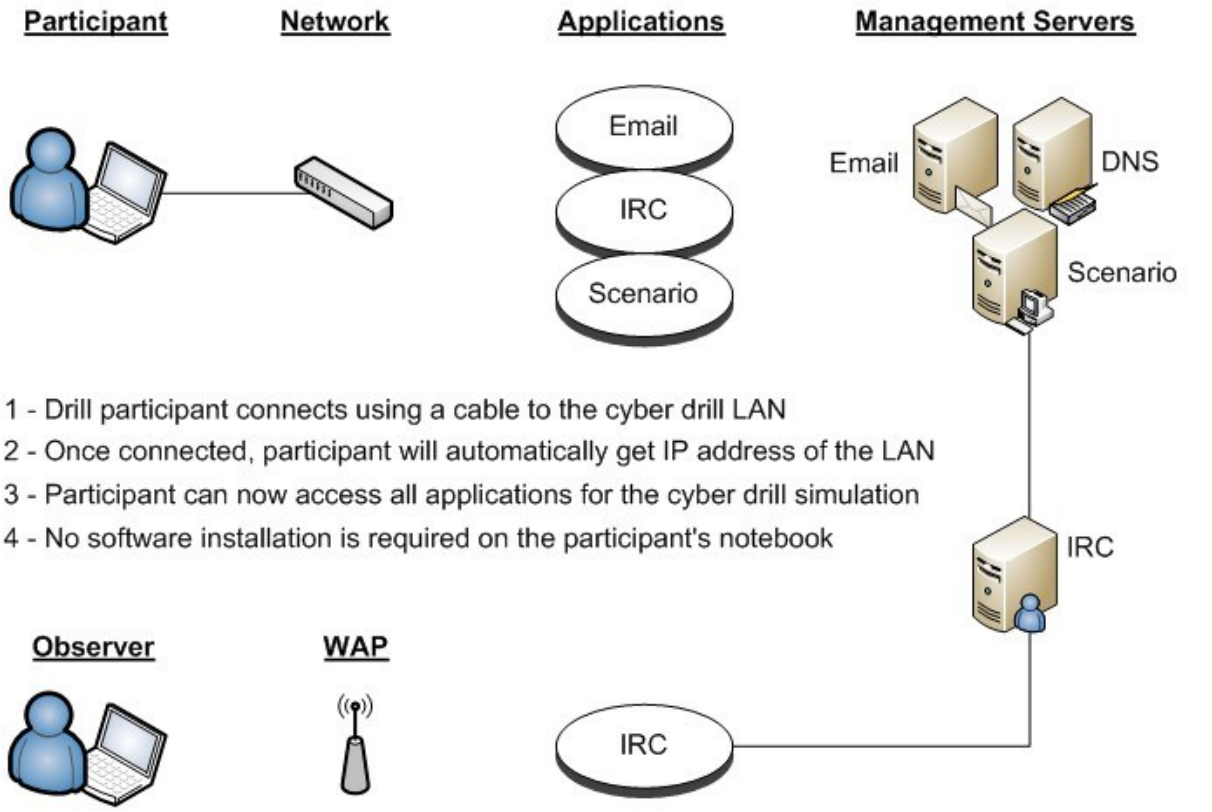


Figure 2 : Scenario Setup

Drill Setup

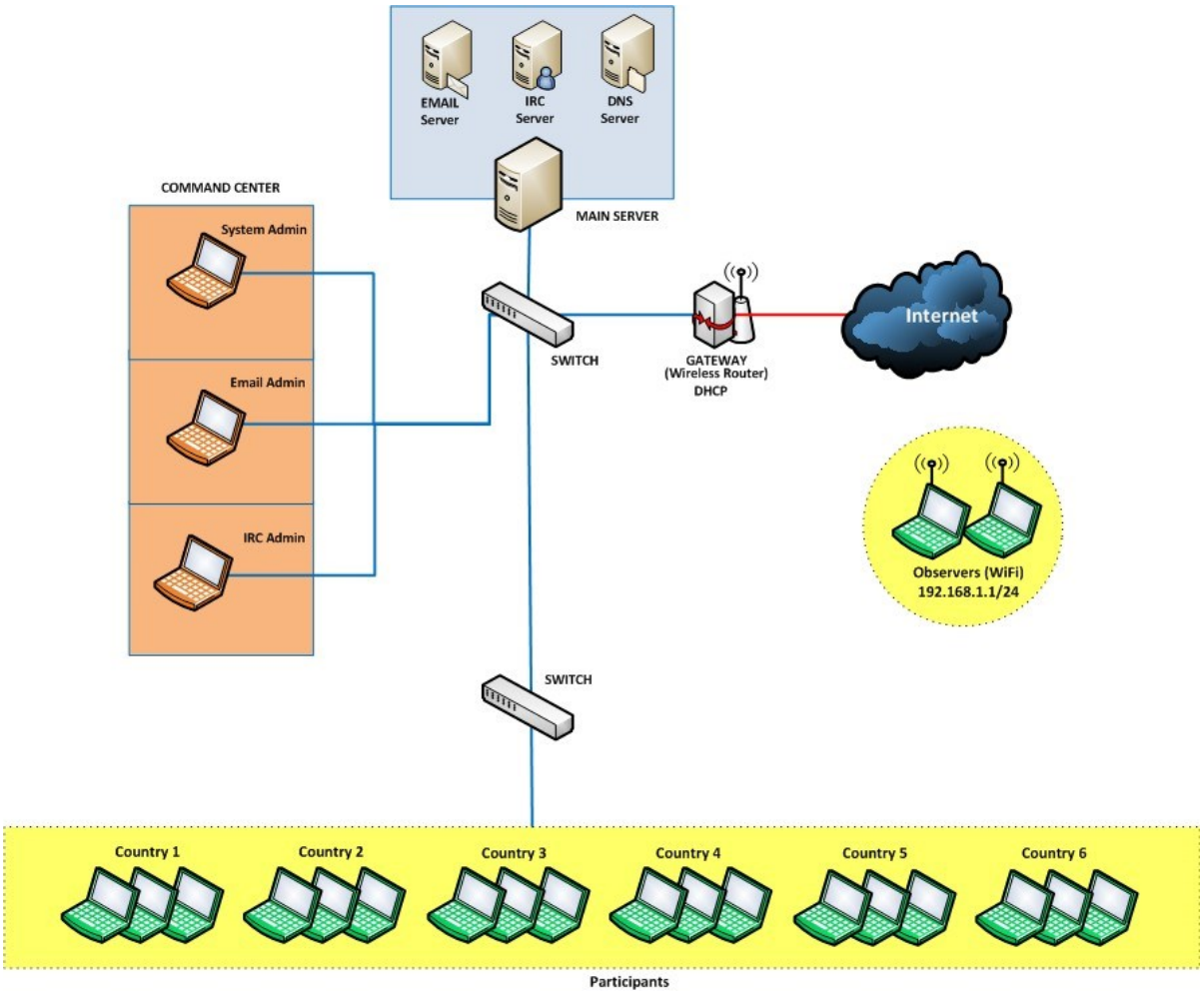


Figure 3 : Drill Setup

Participants – Roles & Responsibilities

Player	• Perform incident analysis on the scenario and send solution or recommendation based on the given advisory report template back to the organiser
Observer	• Observe and assist the players in his team during the drill

Participating External Observers

External Observers: They will be able to communicate with the participating teams' observer to understand the status as well as the process for threat mitigation.

Organiser – Roles & Responsibilities

Drill Director	• Overall co-ordination with the drill experts and participating countries
Drill Facilitator	• Manage the cyber drill by co-ordinating the activities of the drill experts and participating countries • Assist participants during the cyber drill • Guide the teams through the scenarios during deployment for the cyber drill • Present summary of the cyber drill to participants
Drill Manager	• Administration and coordination for the cyber drill • Assist participants during the cyber drill
System Administrator	• In charge of servers and virtual machines for the cyber drill • Manage the deployment of scenarios to all the participants • Manage and contain the drill activities on the infrastructure provided to the participants
Mail Administrator	• In charge of email communications for the cyber drill • Help co-ordinate the activities of the participants for the duration of the drill through e-mail communications • Introduce additional scenario elements through e-mail communications during the entire drill • Capture salient points for post drill summation and analysis. • Assist participants during the cyber drill
IRC Administrator	• In charge of IRC communications channel for the cyber drill • Communicate and co-ordinate the activities of the drill participants to reach a conclusion on the scenarios provided • Manage scenarios presented during the drill • Capture salient points for post drill summation and analysis • Assist participants during the cyber drill
IT and Technical Support	• To develop and support IT infrastructure which involves setting up and dismantling the cyber drill environment for the hardware, software and operating systems • Provide troubleshooting, security and management of all network devices, servers and infrastructure • Assist participants during the cyber drill

Prerequisites for Participants

The cyber drill participants are required to bring their own notebook computers.

Minimum Hardware and Software Requirements

- Notebook computer with minimum 2GB RAM, a wireless card and a US layout keyboard
- Operating system running on Windows XP and above
- Latest web browser (IE, Firefox or Chrome) with flash and Java installed
- Word processing application (MS Words, OpenOffice or AbiWord etc.)

Knowledge Areas

It is recommended that the participants should have knowledge in the following areas:

- Incident handling
- Reverse Engineering
- Information gathering
- Log analysis
- Packet analysis
- Malware analysis
- Familiarity of the Unix/Linux OS

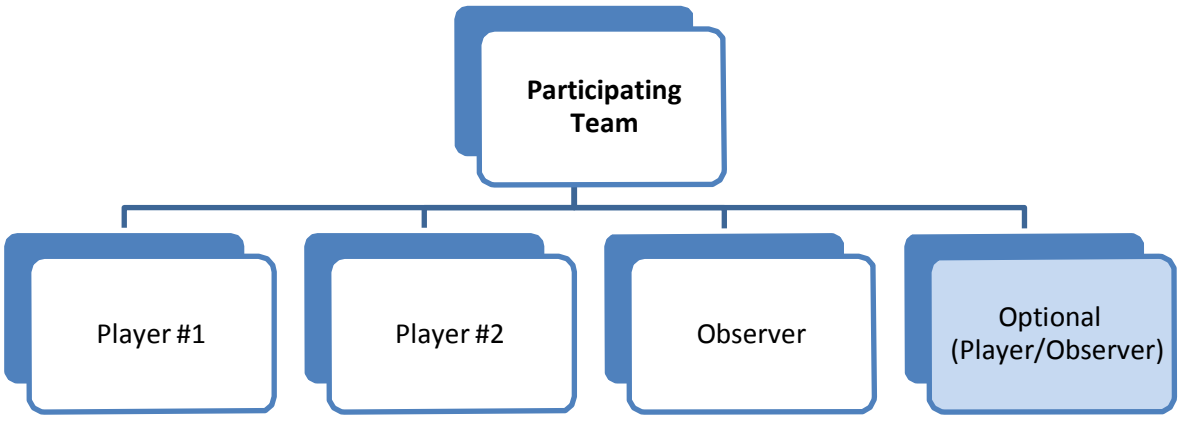
The participants can use their own software tools however; it is recommended that they should also be familiar with the following tools:

- Wireshark
- OllyDbg

Team Structure

Each participating country's CIRT/CERT team will be divided into 2 roles, representing "*player*" and "*observer*". The player will execute the incident handling process, analyse the threats and mitigate the simulated attacks while observer will execute the communication roles and assist the player to mitigate the simulated attacks.

Each participating team must have a minimum of three (3) or a maximum of four (4) representatives to participate in the drill:



Drill – Do's and Don'ts

Do's

- Participants can use their own software tools
- Participants can use any reference websites to search for information
- Participants can communicate with other participating teams via IRC channel made available for this purpose
- Participants can seek assistance from the organiser via IRC channel

Don'ts

- No malicious activity is allowed that can cause harm to the network such as Scanning, Sniffing, DOS or any attempt to attack the drill infrastructure (e.g. IRC Server, Web Server)
- No misuse of internet is allowed

Post Drill Activities

All participating teams are to submit a feedback of the drill to the organiser. The feedback form will be provided by the organiser.

The organiser will consolidate the feedback and prepare a post-mortem report. An executive summary report by the organising drill team will also be submitted to ITU.