AfricaCERT
United in promoting cyber security in Africa

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency Response Team

Designing and Running Cyber-exercises for CSIRTs

Haythem EL MIR, CISSP

CEO, Keystone & CSIRT.tn

Haythem.elmir@keystone.tn

About me

- Haythem EL MIR,
- 20 years in cybersecurity,
- CEO Keystone (Cybersecurity company covering MEA Region),
- Head of CSIRT.tn (member of FIRST and AfricaCERT),
- ANSI Technical Manager (from 2002 to 2012),
- Head of IRT at tunCERT from 2005 to 2012,
- CISSP since 2009,
- Active in Africa and Middle East since 2006.
- More than 50 cyber-Exercises.

Agenda

- Cyber-Exercises introduction
- Cyber-Exercises benefits
- Types of Cyber-Exercises
- Techniques used for Cyber-Exercises
- Cyber-Exercises target audience
- Planning Cyber-Exercises
- Use case : Data Breach

Objective of the session

- This training will help CSIRT to:
  - Understand the concept of cyber Exercise as a very powerful tool to develop their capacities and their community's,
  - Discover types of cyber-Exercises and different techniques,
  - Plan a cyber-Exercise,
  - Prepare and design a cyber-Exercise,
  - Run the Exercise,
  - Evaluate Exercise outcomes.

Cyber-Exercises

- Cybersecurity exercises are useful simulations of cyber attack scenarios to help CSIRTs evaluate their capacities in term of real-world response.
- Evaluate the defensive strategy and identify weaknesses that require improvements and further training.
- Prepare the CISRT and its constituency to respond to cyber-attacks and to manage major cyber-crisis: Malware infection, DDoS, Ransomware, Data leak, financial fraud, attack against critical systems, etc.

Cyber-Exercises

Cyber-Exercises

Organizer

Preparation team

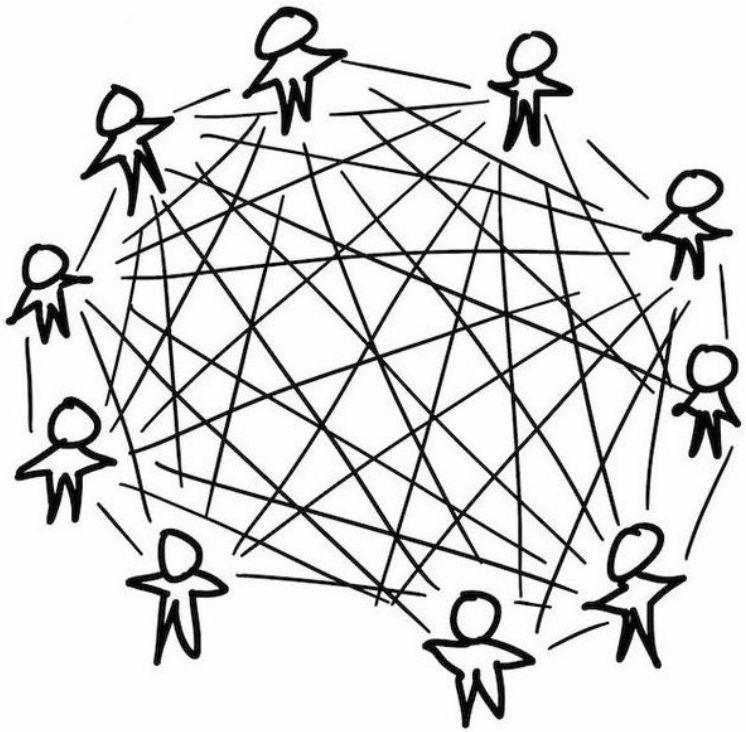
Evaluator

Cyber-Exercises

Teams

Individual

Cyber-Exercises



Remote players

A mix of both

Onsite players

Cyber-Exercises

Same organization (simple to complex)

Multiple organizations / wide scale

Cyber-Exercise benefits

- Improve cyber-resilience,
- Evaluate team readiness to respond to specific cyber-attacks,
- Evaluate technical and management skills,
- Practice incident response procedures,
- Identify weaknesses in term of skill, procedures and organization,
- Raise awareness about threat among security teams, decisions makers and managers, and clarify responsibilities,
- Train the team of response procedures, crisis management and technical procedures and tools,
- Improve collaboration with external parties,
- Improve communication,
- Collect metrics.

Cyber-Exercise benefits

- Help CSIRT to raise awareness within their constituency/community about their role in incident management and the importance to have all stakeholders involved.
- Example: In a bank the involvement of:
  - **CEO**: the main person accountable in case of emergency,
  - **CISO**: the key player in the response process,
  - **CIO**: in charge of IT systems to help in artifact gathering and the implementation of remediation,
  - **HR**: to be involved if one of the employees is related to the attack,
  - **Compliance**,: in case of major fraud or regulatory non-compliance,
  - **Risk**: to evaluate the impact and provide recommendations based on risk evaluation,
  - **Physical Security**: in case of physical intrusion or if video surveillance records are needed in case of ATM fraud,
  - **Legal**: to assist the whole process if a legal procedure is launched against cybercriminals,
  - **Communication/PR**: to ensure communication with customers, partners, regulators, etc.

Cyber-Exercise Topics

- IR:
  - Incident management,
  - Incident response,
  - Computer Investigation,
  - Malware investigation,
  - Intrusion,
  - Etc.
- Assessment:
  - Penetration testing,
  - Configuration assessment,
  - Architecture assessment,
  - Application security assessment,
  - Banking system assessment,
  - Etc.
- System protection:
  - Applying security control,
  - Security management,
  - Implementing security solutions,
  - Hardening systems,
  - Etc.
- Communication:
  - Crisis communication,
  - Communication with media,
  - Internal communication,
  - Etc.
- Legal procedure:
  - Evidence gathering,
  - Writing reports,
  - Chain of custody,
  - Etc.

Types of Cyber-Exercises

- The selection depends on the objective and on the audience:
  - Crisis management : for decision makers and for mangers,
    - 2 hours
  - Technical/Live: CSIRT, IT teams, SOC Teams,
    - 4 hours to a couple of days,
  - Incident management: CISO, IT managers, SOC Manager, CSIRTs,
    - 2 to 3 hours
  - It can be a combination (but not recommended),
  - Capture the Flag,
    - 4 to 24 hours,
  - Card Game,
    - 3 hours.
  - Attack/Defense – Blue Team/Red Team,
    - 4 to 24 hours.

Types of Cyber-Exercises

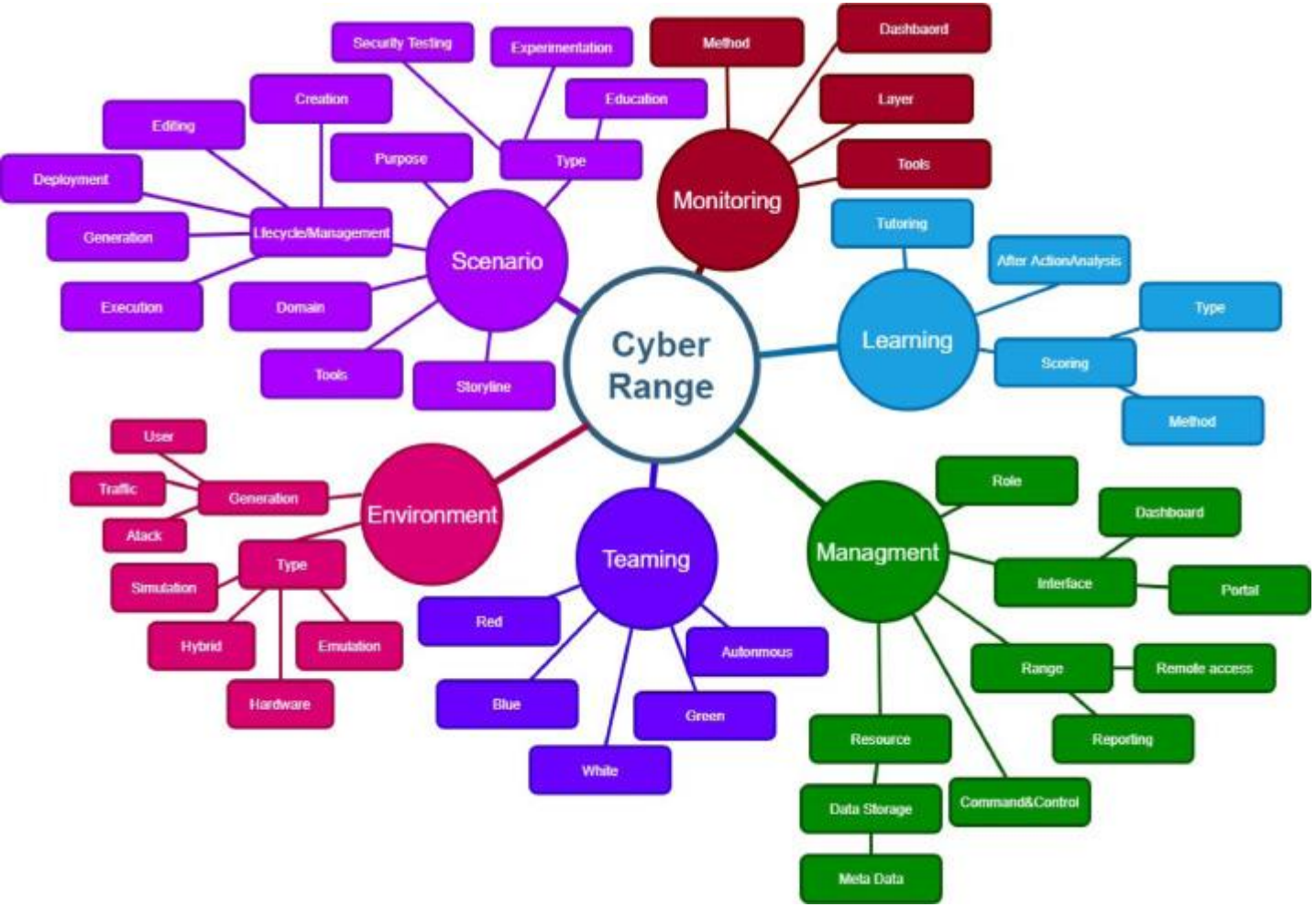
- Table Top: participants are around a table, a moderator is conducting the exercise, by injecting events in relation with the scenarios and participants have to think of ways to solve different situations.
  - Open discussions can be moderated by the moderator.
- Participants can answer some questions in a paper form or through web/mobile application,
- The TableTop exercise can involve all participants in the same discussion or can simulate a crisis cell who will be in charge of handling the crisis with interaction with other participants.
  - Role have to be assigned to each player (CEO, RM, PR, CISO, Legal, CIO),
  - Participants can be assisted with scripts and guides,
- The TableTop can organize participants in groups.
  - Groups can work on the same scenario or on different ones.
- Card Games can be used for TableTop exercises.

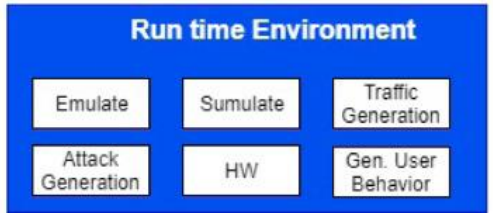
Techniques used for Cyber-Exercises

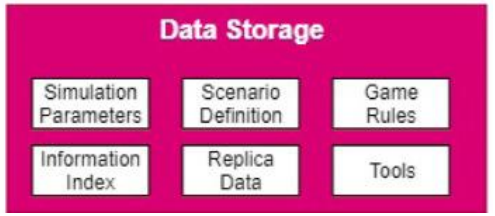
- Live play: a realistic technical environment, with simulated attacks,
- Cyber Range: a controlled environment where trainees can practice exercises without harming real systems.
- Commercial Cyber Range have ready scenarios,
- Hybrid Cyber Range,
- Scripted and automated injects,
- VM,
- Technical exercises can be played remotely or on site.

Shooting Range

Techniques used for Cyber-Exercises







Cyber-Exercises target audiance

- CSIRT Team,
- It can be used by CSIRT team to target:
  - Top management,
  - Managers,
  - Business units,
  - IT administrators,

- For National CSIRT:
  - Decision makers,
  - CIIP,
  - Security team,
  - Sectorial CSIRTs,
  - General training.

Planning Cyber-Exercises

- Define the objective,
- Identify the target audience,
- Identify the type of the exercise and the technique to be used,
- Prepare a project plan with timeframes,
- Identify needed resources,
- Design the scenarios,
- Prepare the infrastructure,
- Prepare guides,
- Prepare the facility,
- Run the exercise,
- Evaluate.

Planning a Cyber-Exercises

- Define the objective

Train on specific procedures	Test collaboration between teams	Test incident and crisis management process and procedures (BCP, Escalation, Triage, etc.)
Evaluate team skills	Raise awareness on specific threats	Raise awareness among managers and business units
Test communication strategy	Test new tools	Evaluate the security program

Planning a Cyber-Exercises

- Identify the target audience:

Top-management	IT Teams	Security forces
Managers	CSIRTs	CIIP
Ministers	Business Unit	Gouvernment

Planning a Cyber-Exercises

- Identify the type of the exercise and the technique to be used:

Tabletop	Local	CTF
Cyber Range	Remote	Team vs individual
Card Game	Complex vs simple	Offensive vs defensive

Planning a Cyber-Exercises

- Identify needed resources:

Internet	Server	Room
Projector	VMs	Audio
LAN	Paper & Pen	Email communications (Hard copies)

Scenario selection

New threat	Observed attack in similar environment	Involving internal stakeholders
Most critical systems	Most relevant attack	Practice specific procedure
Most critical process	Involving external parties	Test DRP

Evaluation

Participants involvement	Time spent to solve tasks	Taken decisions
Participants feedback	Ability to follow-up procedures	Action effectiveness
Solved tasks	Communication effectiveness	Recommendations to update procedure

Mistakes to avoid

Boring scenario	Lack of resources to host VMs	Mixed audience (presence of the CEO)
Wrong technical details	Network/Internet failure	Incoherent scenarios
Scary scenarios	Installing tools on participants corporate laptop	Vey easy technical scenarios

Recommandations to consider

- Make it pleasant and entertaining
- Make sure participants are engaged
- Have a team to assist participants
- Moderate and stimulate open discussions
- Use realistic scenarios
- Make it a competition between mixed teams
- Start from simple situations to more complex
- Learn from observed real attacks
- Avoid competition between organizations

Prepare the facility

- Table top:
  - Meeting room / Training room,
  - Printing guides,
  - Projector / PPT,
  - Microphone / speaker
  - White board,
  - Paper and pens,
  - Team names,
  - Water and coffee.
- Remote:
  - Email communication,
  - Instant messaging.

Prepare the facility

- Technical:
  - Internet connection,
  - LAN (Wifi/Cable/Switch),
  - Scenario hosting environment : Local/Remote Server,
  - Workstation,
  - Score board projection,
  - Music and food,

Cyber-Exercises

- National Exercise:
  - Hacktivist Attack,
  - State-sponsored attack,
  - Massive banking fraud,
  - Attack against critical infrastructure (Telecom, Electricity, Banks, etc.)
  - Attack against popular media,
  - Government data leak,
  - Combined attacks against the government,
  - Attack on an ISP,
  - Privacy breach against health sector,
  - Ransomware attack against public administration,
  - Massive exploitation of a zero-day vulnerability,
  - Etc.

Present the scenarios: tell the story

- Mira Group, is a big industrial group active in many economic sectors (Energy, food, Agriculture, textile, tourism, etc.), they hold 83 branches.
- To manage all the IT systems, the group had created its own private cloud with centralized AD, centralized ERP system, web hosting, MS Exchange server, Security systems,
- All branches are connected via an IP MPLS network to the main datacenter, and they connect to Internet via the main link in the datacenter.
- The central IT team is composed by 20 engineers,
- A CISO was nominated 1 year ago and he started to develop the security policy and BCP, the SoC project did not start yet,
- Each branch has an IT team of 1 to 5 people to support their companies.
- The industrial group is listed on the stock exchange.

Injects

- To start the exercise, a set of injects should be prepared to drive participants through a realistic simulation,
- Injects are information and updates to be provided to participants,
- Injects should be interrelated to conduct the attack scenarios,
- Through the sequence of injects, participants should feel very involved and concerned by the attack, to get them engaged to find solutions and give recommendations,
- This involvement will push participants to think and to provide recommendations and solutions.

Injects

- Inject 1: 8th of November, 7:52, an employee opened his computer and found all his files corrupted, they identified a text file talking about a ransom. The employee reported the issue to the help desk. The helps desk received 12 reports in less than 7 min about the same behavior. The incident was escalated to the CISO.
- Inject 2: All servers are encrypted by the ransomware.
- Inject 3: All logs were wiped.
- Inject 4: The attacker is claiming he copied all databases.
- Inject 5: All the backups are encrypted too.
- Inject 6: All branches are unable to run their operations. Some customers are talking about the attack on social media.
- Inject 7: The media are talking about the attack.
- Inject 8: The stock market share falls.

Preparing technical scenario

- Prepare a virtual environment (One or multiple VMs),
- The environment can simulate a whole infrastructure (Bank, Telco, SCADA, etc.),
- Design the attack scenario and prepare evidences and artefacts,
- Prepare guidance to help participants to go through the exercise step by step,
- Prepare an evaluation quiz per task (if needed),
- Prepare hints (if needed),
- Host the scenarios (Local server, VM copied on Participants' laptops, Cyber Range),
- Prepare the access (Local IP, Cabling, Wifi, VPN, Credentials, etc.).

Use case : Data Breach

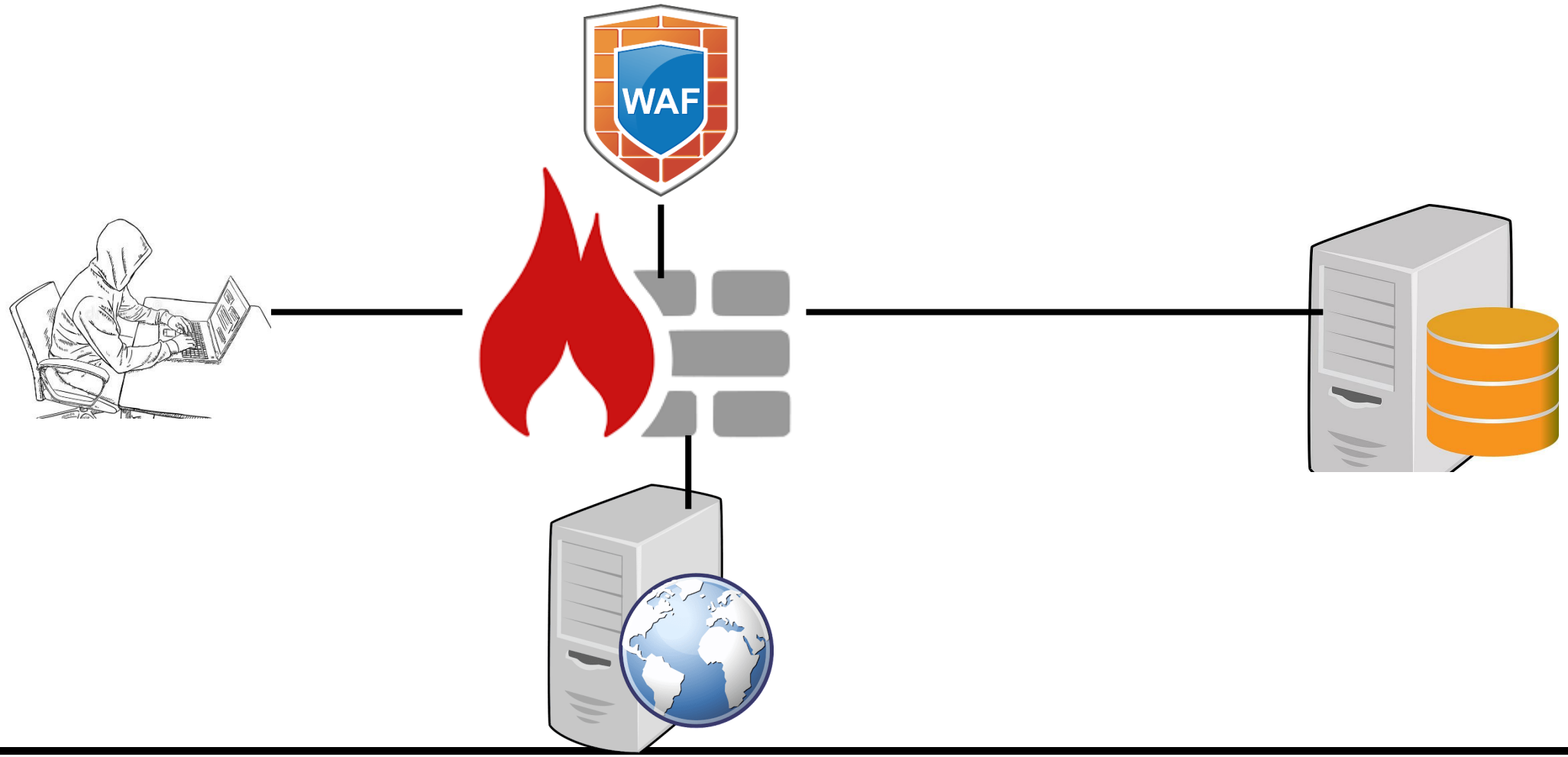
SOCIAL-LEAK21

The scenario presentation

- The social security company was informed abut a data breach, millions of citizens records are being sold on the dark web. It seems that these records are stolen from the main database.
- The company have a main datacenter hosting key IT services, among them the core application to manage 5 millions citizen records,
- They have 30 branches.
- They have a back-up center at 120 KM from the HQ.
- The application is offering online services, to pay pension and to manage all citizens private data,
- To protect the online service, they deployed a Firewall and a WAF,
- A CISO was nominated 2 years ago, working on developing an ISMS,
- No monitoring system is deployed,
- The protection system is considered very basic,
- The internal information system is composed by 200 servers and 1200 workstations,

Attack scenario

- The exercise design can start from the creation of an attack scenario.



The attack scenario

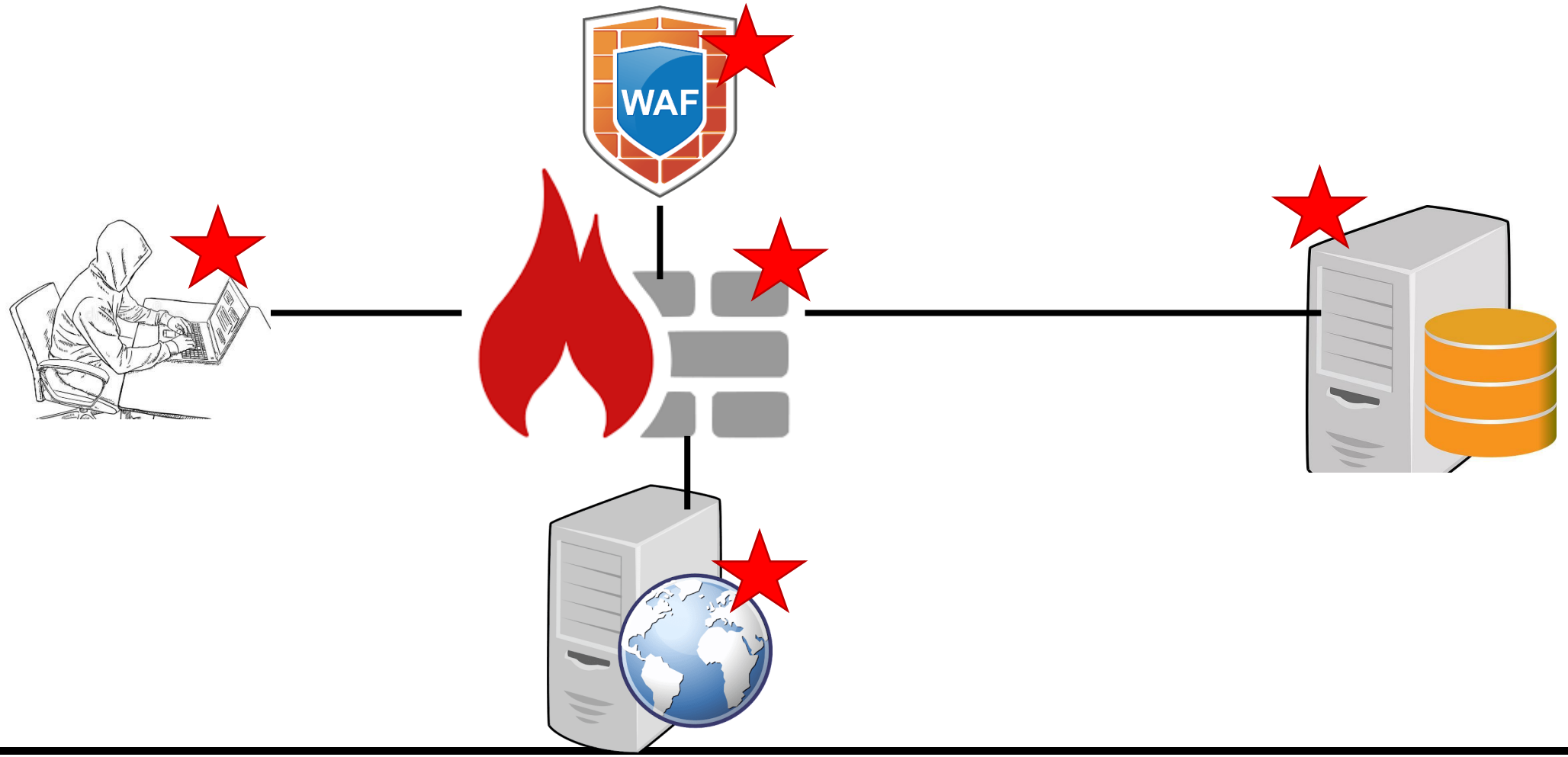
- An attacker found an upload vulnerability on the web server hosted by the social security company,
- He succeeded in exploiting it by bypassing the WAF,
- Once exploited, he succeeded in uploading a web shell,
- Once uploaded the attacker succeeded in performing a privilege escalation in order to gain a full control of the web server,
- From the web server he was able to locate the database server, the used database account in the web application was identified, but its usage was very limited,
- From the web sever he ran a brute force attack on SSH server on the database server,
- Once the root account was compromised, the attacker took full control of the database server.

The attack scenario

- On the database server, the attacker managed to find the SYSDBA account,
- With the SYSDBA account, the attacker managed to run a script to dump all the database,
- The dump was sent directly to the attacker's server by establishing a reverse shell,
- The attacker left the reverse shell (as a backdoor) to maintain access on the server.

Attack scenario

- What traces can be left by the attacker and where ?

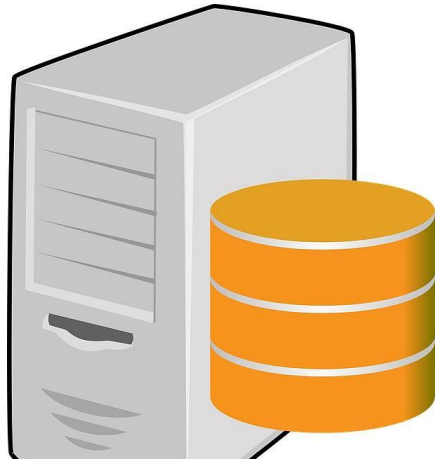


Preparing the technical Exercise

- After presenting the scenario, participants will be in charge of doing the investigation:
  - What is the first system to analyze?
  - What information needs to be collected?
  - Where to find evidence and artefacts?
- Participants need to be guided through the investigation step by step and each step will be a task,
- For each step, we need to provide traces and artefacts, inside which some information needs to be identified by participants,

Preparing the technical Exercise

- Analyzing the database server:
  - Identify traces related to:
    - Database dumping,
    - Dump exfiltration,
    - Exfiltration destination IP,
    - Reverse shell,
    - SSH brute force,
    - IP used to access via SSH
    - Identification of the SYSDBA account,
    - Date and time of all the attacks.



Preparing the technical Exercise

- Analyzing the web server:
  - Identify traces related to
    - The web shell,
    - The upload vulnerability,
    - The privilege escalation,
    - The SSH brute force attack,
    - The IP used to attack the web server (WAF IP),
    - The access to the database server,
    - Date and time of all the attacks.

Preparing the technical Exercise

- Analyzing the WAF:
  - Identify traces related to
    - Vulnerability exploitataion,
    - Bypass technique,
    - IP used to attack the web server,
    - Date and time of all the attacks.

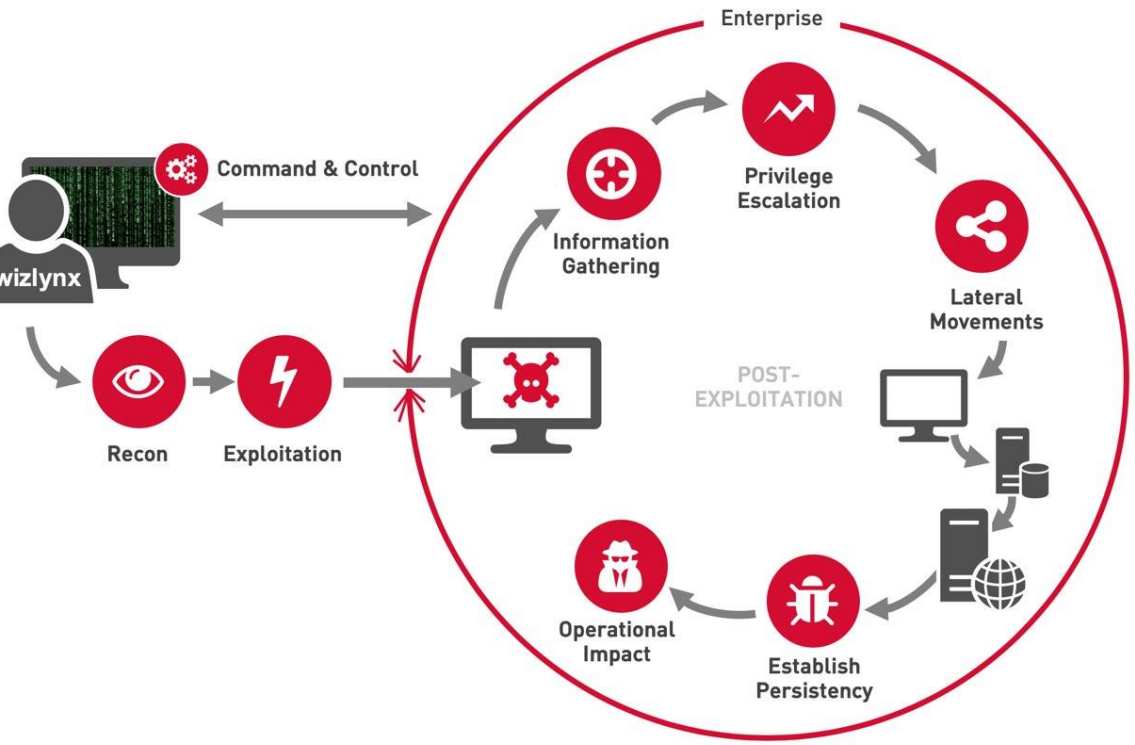
Preparing the technical Exercise

- Analyzing the Firewall:
  - Identify traces related to
    - Attack activity,
    - When the first event occurred,
    - All events related to the identified IP (the IP was used previously to access a specific account),

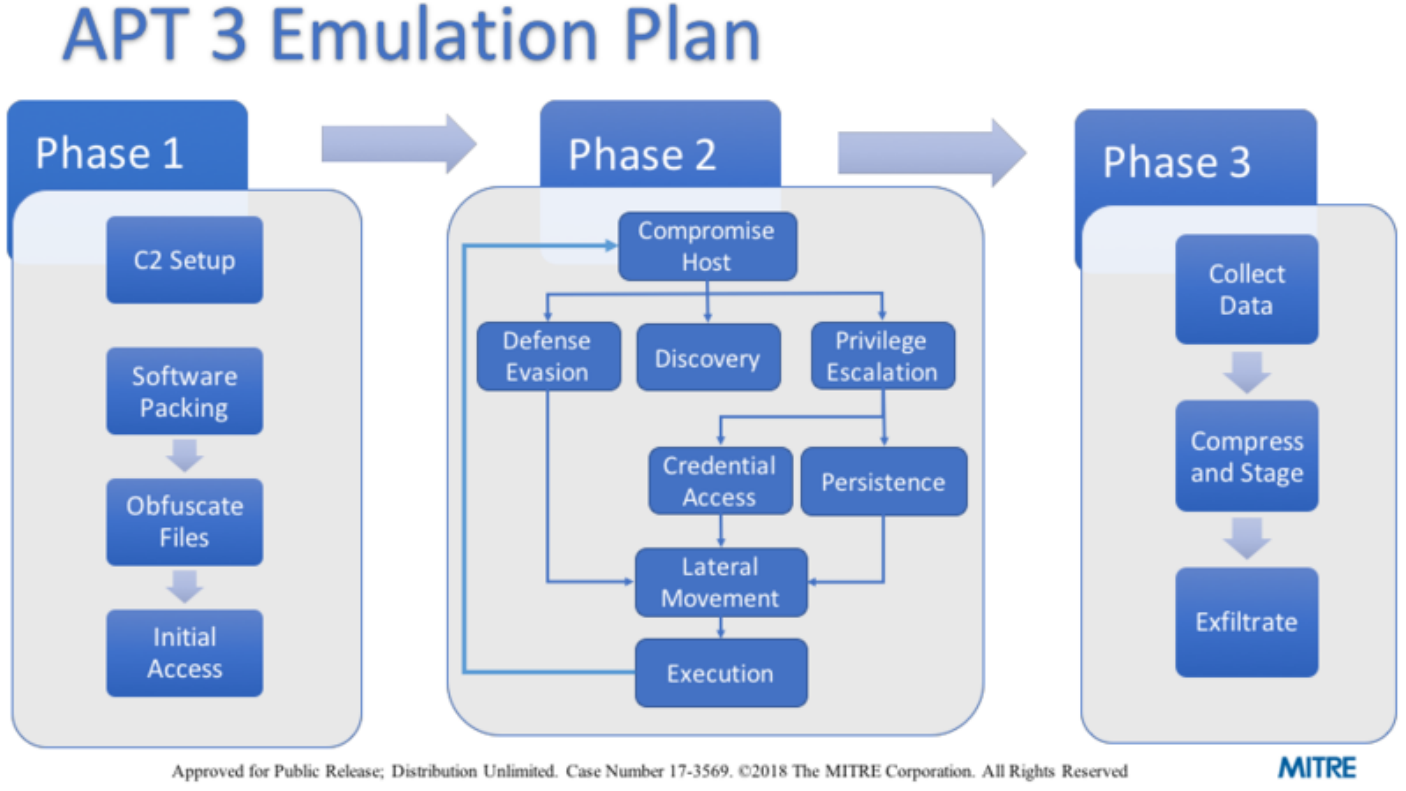
Preparing the technical Exercise

- Once the scenario is ready, we need to prepare the environment:
  - Install servers and applications,
  - Prepare the vulnerabilities,
  - Test services and vulnerabilities,
  - Connecting the network,
  - Run the attack and leave traces,
  - Check logs and traces,
  - Take a snapshot,
  - Prepare tasks (questions and answers),
  - Test the whole scenario.

Preparing the technical Exercise



THE CYBER KILL CHAIN



Preparing the Tabletop Exercise

Preparing the Tabletop Exercise

- Incident management:
  - How to check that the breach is real?
  - What to check in our system? Where to start?
  - Do we have expertise on how to handle such an attack?
  - Prepare a response plan?
  - Do we disconnect the system?
  - Do we have to communicate with the attackers?
  - What to do about stolen data?

Preparing the Tabletop Exercise

- Security plan:
  - What are the vulnerabilities exploited by the attacker,
  - How could these vulnerabilities be avoided?
  - What tools and procedures we need to have in place to avoid the occurrence of such vulnerabilities,
  - What problems do we have in relation with the security architecture?
  - How can WAF be bypassed?
  - How to make sure that we have all necessary traces?
  - How can we detect such attack?
  - What about the password policy?

Preparing the Tabletop Exercise

- Escalation process :
  - Do we need to inform the top management?
  - Who else to involve ?
  - Do we need to inform the authorities?
  - Do we need to call the police?
  - Are we able to identify the attacker if we involve the police?
  - With whom do we need to collaborate?

Preparing the Tabletop Exercise

- Communication plan:
  - Do we need to inform our employees?
  - Do we need to inform our customers?
  - Do we need a public annoucement?
  - What if the media are aware of the attack?
  - Do we need to prepare a press release or a press confernce?
  - What is our communication startegy?

Preparing the Tabletop Exercise

- Legal pursuit :
  - How to deal with such a breach from a legal perspective?
  - What kind of legal pursuit can we face?
  - How to conduct an investigation?
  - What kind of data we need to collect and preserve as evidence?
  - Is it possible to locate the attacker?
  - Is international collaboration efficient in such situation?

Preparing the Tabletop Exercise

- Once the scenario is ready, we need to prepare the environment:
  - Prepare the guide/script,
  - Prepare questions and discussion points,
  - Prepare a PPT.

Summary

- Define the objective,
- Identify the target audience,
- Identify the type of the exercise and the technique to be used,
- Prepare a project plan with timeframes,
- Identify needed resources,
- Design the scenarios,
- Prepare the infrastructure,
- Prepare guides,
- Prepare the facility,
- Run the exercise,
- Evaluate.

Additional references

- DELTA RISK: How to Design an Effective Cyber Exercise
- TRAFICOM : Instructions for organising cyber exercises - A manual for cyber exercise organisers
- ANSSI: ORGANISER UN Exercise DE GESTION DE CRISE CYBER
- ENISA: Good Practice Guide on National Exercises
- MITRE: Cyber Exercise Playbook
- CIS: Tabletop Exercises - Six Scenarios to Help Prepare Your Cybersecurity Team
- ENISA: The 2015 Report on National and International CyberSecurity Exercises Survey, Analysis and Recommendations

Haythem.elmir@keystone.tn