Cyber Range The Future of Cyber Security Training

Carlos Perez Gonzalez

Cyber Range – The future of Cyber Security training

GIAC (GPEN) Gold Certification

Author: Carlos Pérez, cperezgonzalez@gmail.com
Advisor: Rajat Ravinder Varuni
Accepted: May 5th 2020

Abstract

Both the private and government sectors are looking for talent. Thousands of vacancies are going unfilled as the industry struggles with a shortage of adequately trained professionals. According to the latest forecasts, there will be 3.5 million unfilled cybersecurity jobs by 2021. The challenges related to finding talent are not new, and this problem has grown in the last years with an increase in cyber-attacks.

Professionals need to be able to train on a real battlefield; the bad guys do not play by the rules and have all the time to attack the systems or critical infrastructures. The use of Cyber Range has been instrumental in the last three years to improve government defenses and is now very relevant for the private sector too.

This new technology and the implementation of real simulation attack scenarios, besides its benefit as a threat intelligence tool to automatically collect data, is allowing to improve the defenses and the threat response . Cyber Range enables companies and governments to be in the ideal position to defend themselves against cyber-attacks. This article will explain what a Cyber Range is, what it can do, and how it can be useful to improve the training of professionals that work in the cybersecurity field.

1. Introduction

Why should we be looking for a place to practice hacking techniques? Why are companies offering training environments to their staff? Why would the company be performing a real cyber exercise within a hyper-realistic environment? These are some of the questions that are often heard in the meeting rooms of a cybersecurity company.

This document is intended to cover an aspects of what a Cyber Range is and its key components.

It is increasingly common to find solutions known as the Cyber Range, companies with a high level of cybersecurity experience that replicate real scenarios through a platform, that is occurring in the day to day of an organization.

A Cyber Range provides a controlled environment in which organizations execute cyber exercises without any live impact to the network systems. The Cyber Range, in general, is based on the business process model and technology to using for penetration testing or incident response involving a red team and a blue team.

Reference: (Definition.What Is a Cyber Range?.2018 Cloudshare.)

The companies are using this technology to improve strategic business decision points, also corresponding technical concerns that should be considered when implementing defensive technology and deployment compliance to reduce risk.

It is agreed that in-depth knowledge in cybersecurity allows us to offer a service for customers to support them to improve and provide insight the activity, this allows us to reduce the risk through the training. These exercises involve a realistic and repeatable simulation to allow a company to identify any weaknesses and points of improvement.

The scenarios can provide a realistic simulation of the impacts that a cyber threat may have on a business. This environment reproduces a scenario by combining risk factors as "what-if."

These cyber exercises are held on virtual learning environments that simulate with full fidelity networks and resources. They are habitually used for testing red team & incident response capacities and offer an accurate analysis of threat's knowledge and assess

competencies accurately. Doing so, companies can improve their response processes and test their team's readiness.

Reference: (Government Technology. Cyber Range: Who, What, When, Where, How and Why?. Dan Lohrmann 10/03/2018 LOHRMANN ON CYBERSECURITY & INFRASTRUCTURE. Govteh.com)

1.1. Goals and benefits

The Cyber Range provides a method of examining human performance and reactions as well as the decisions taken, in order to compare them with the outcomes expected in the context of an enterprise under a cyber-attack scenario.

A Cyber Range involves multiple entities and conducts an exercise of cyber-attacks where the enterprise needs to defend against them while the business continues to operate as usual, whilst ensuring that information systems and networks are fully operational, minimizing the impact.

Below we can find some key features of a Cyber Range.

- Assess the effectiveness of the organization's exercise through exhaustive incident reporting and analysis guidelines for remedying deficiencies
- Assess the organization's capability to determine operational impacts of cyber-attacks and implement proper recovery procedures during the exercise
- Understand the implications of losing trust in IT systems and create workarounds for such losses
- Assess the ability of the technical team to detect and adequately react to hostile activity during the exercise
- Expose and correct weaknesses in cybersecurity systems
- Expose and correct weaknesses in cyber operations policies and procedures
- Enhance cyber awareness, readiness, and coordination
- Determine the effectiveness of the cyber education provided to the training audience before the start of the exercise

- Develop contingency plans for surviving the loss of some or all IT systems

2. Technology

A Cyber Range is developed using and integrating different technologies such as JAVA, Python, PowerShell, or VMware. These programming languages and the availability of the technology VMware on Cloud such as Amazon, Azure or even dedicated servers in OVH, allows us the creation a Cyber Range that could be used in the worldwide proving of different access to the platform (HTML5, VPN) and involving different locations or countries of an organization in a same cyber exercise.

Some points to consider when building a Cyber Range:

Flexibility: The platform must support the creation of different instances and network topologies, from networks with a single host to multiple interconnected networks and hosts. Installed operating systems must support a wide range of versions (including updated or less updated packages, unpatched versions, or the installation of deliberately vulnerable systems).

Scenarios: All scenarios must be built and design by experts to develop real and unique environments. The scenarios will be integrated into the platform, where the instructors can deploy scenarios automatically. They must be built with a high level of authenticity, recreating real-life situations like generating news or public information leakages.

Scalability: The solution must be scalable, increasing the number of resources. It is essential to use reliable virtualization technology such as VMware 6.7, Azure o AWS.

Secure: Users should be able to use and access the platform without impediments. Access to the environment of the exercise into the Cyber Range can be performed through a web browser HTML5, with Apache Guacamole technology, for example. VPN access is another way of accessing the environment.

APIs and Sandbox: All environments must be managed from the portal. The API allows us to obtain real information on the status of Cyber Range assets, restart or return

the environment's previous stage before a new cyber training session. The environment must be isolated and sandboxed to launch controlled attacks and run real threats.

Management Portal: The portal of the Cyber Range should include an admin panel (WebGUI). The language can be JAVA, Python, Angular with Go, for example. This area is used to show the information of the participants, such as keeping track of the training, showing the metrics and progress of the training sessions.

Dedicated Environment: The Cyber Range should be designed with the premise of being dedicated and provide isolated environments for each of the groups or participants to avoid a situation in which two teams of different sessions overlap.

User Management: A Cyber Range should have a management portal to allow users and groups management, tracking of previous sessions, and in general, create a robust and reliable database of results and sessions to track the evolution of the participants. A Cyber Range must also provide access to users, providing all their information and progress of the training, which will be registered by the Cyber Range metric tools. Also, the access must be done through HTTPS with a web browser. All the login accesses must be registered and tracked.

Logs and Monitoring: The Cyber Range must have a historical record and store the logs during a minimum period to check and analyze the techniques used during the live sessions. It is also mandatory to have a monitoring and tracking system for operational services used in each session. The platform should be designed to be fault-tolerant and provide backup or contingency plans to keep the training sessions active.

2.1. Hardware

The design and implementation of the Cyber Range on a virtualized infrastructure allows us to deploy and adopt different features such as the number of participants, the difficulty of the challenges, the diversity of the challenges, the number of servers o virtual machines or operating systems to mention a few. All kinds of participants (Red Team, Blue Team, and Instructors) have a dedicated area in the platform to use.

It is recommendable to use physical servers where it can be possible to virtualize real environments and host the scenarios that will be implemented. The use of a virtualization infrastructure makes the platform deploy a real training environment.

An example of infrastructure deployed and managed and deployed on cloud

- Dedicated server with 512 GB RAM - Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz
- VMware Center 6.7 with standard license.
- SSD Hard Drive with 8 Terabytes

Reference: (Training and simulation environments at scale breadth and speed to out maneuver bad actors. Cyber range Solution. 2019 VMware)

2.2. Software

If we wish to install other network elements such as routers or firewalls, we need to make sure during the design phase that they can be deployed in our network correctly.

Below we can see an example of some operating systems, appliances or software usually deployed in a cyber range scenario.

- Web Application Firewalls (WAFs)
- Security Information and Event Management (SIEM)
- Mail Transfer Agents (MTAs)
- Microsoft Windows Operating Systems
- Linux / Unix Operating Systems
- Network Firewalls
- Routers and Switches
- Antivirus Software

2.3. Documentation

All features integrated into the Cyber Range should be in English, as well as the complimentary user manuals and guides.

The documentation should include the following points:

- Hardware User Manual
- Administrator User Manual
- Quick Scenario Generation Guide
- Technical Guides (maintenance, updates, management)
- Frequent questions – FAQ

2.4. Management

The instructor may be able to build and manipulate the scenarios that will be used for the simulation. The configuration panel allows us to create new scenarios, reuse existing scenarios, or make changes in the topology and configuration of the network, for example the removal or inclusion of new assets.

In the admin panel, it is possible to register new users, enable or disable scenarios, keep track of the number of flags achieved by the users, and the number of points and skills learned in the Cyber Range, among others.

2.5. Participants

The Cyber Range is designed to be utilized by different users with different roles. The admin role enables designing, managing, and scenario configuration to prepare offensive operations and defensive operations and to evaluate the participants and the teams.

Usually, the Cyber Range has three leading roles.

- **White Team:** created for instructors, moderators, and administrators; it allows content management, monitoring of the members in training scenarios, and overall evaluations.

- **Red Team: m**embers of the red team play the role of attacker, pentesters, security consultants, and ethical hackers that want to train their attack techniques to use this role.
- **Blue Team:** it plays the role of a defensive team member that allows improving and learning about attack techniques that are being used by hackers to improve their defensive capacity and sharpen their skills.

3. Methodology

Although there is no formal framework for the development of Cyber Range scenarios, we can use, implement, and rely on recognized frameworks such as MITRE or NIST.

These frameworks allow the development of the challenges and training scenarios of a Cyber Range. The use cases, based on an impact point of view, should be balanced between defensive technology vs cyber-attacks, depending if they are used and implemented in a corporate or a government environment.

The process and design of the use cases and challenges are based on different approaches maintaining the following priorities:

- Develop and expand cybersecurity skills
- Measure knowledge and capabilities of CyberSec teams
- Raise awareness on companies and c-suite executives
- Improve overall cybersecurity education

Cyber Range should be designed to implement challenges with the objective that the participants can develop, improve their capabilities, develop their skills, or build new ones based on experiences acquired on their own Cyber Security experiences.

The main categories that can be deployed on a Cyber Range, adding a differential value on participants are some of the following categories:

Cryptography	Networking
Operating Systems	Employee/Human Errors
Web Application	Mobile
Internet of Things (IoT)	SCADA
Malware Analysis	Digital Forensics

All scenarios should be designed with a gradual progression starting from more fundamental challenges towards more difficult challenges, categorized on the following levels:

- **Low:** different aspects of Cyber Security are contemplated for participants with an elementary knowledge of the subject.
- **Medium:** amateur level challenges, it is a level suitable for computer security enthusiasts with specific knowledge on the subject, but with a little experience in solving cybersecurity incidents.
- **High:** the challenges require a strong knowledge of cybersecurity to face them. Challenges of high complexity may be oriented to train cybersecurity teams of public and private organizations, forensic investigators, incident response teams, and similar participants with expert knowledge in the field.
- **Extreme:** this level of difficulty will require the participant to have exceptional knowledge, a deep understanding of unusual techniques, and substantial experience working on the field.

The present methodology and scenario design require cybersecurity understanding of the following definitions:

- **Scenario:** cybersecurity exercise that is performed on the Cyber Range platform and has a set of different challenges and threats.
- **Platform:** the hardware and software infrastructure necessary.

- **Challenges:** there is a vast number of cybersecurity challenges around us. The main task is to train the teams to understand the threats and be fully prepared to face these challenges of different levels and categories.

The following describes the low-level phases that are considered when building or designing a challenge for a Cyber Range.

3.1. Design and Deployment

The knowledge base of cybersecurity experts is based on their experience and is also acknowledged by certifications of relevant accreditation bodies from the industry, such as GPEN (SANS), OSCP (Offensive Security), CEH (EC-Council) or other certifications. It is also essential to have extensive experience developing current techniques and procedures, using the MITRE ATT&CK or NIST framework as a reference framework.

Given the concept of tactics, an attacker chooses to carry out his attack from the beginning to the end. An attacker keeps in mind that the tactics used must obtain intermediate results during the attack. The trainer must define the procedures needed to design scenarios that test the participants' knowledge of an internationally recognized framework.

MITRE ATT&CK Enterprise describes the actions that an adversary could take to compromise and operate within a corporation's network. This frame of reference can also be used to describe the behavior of an attacker during post-exploitation.

MITRE ATT&CK Enterprise has 11 tactics:

MITRE ATT&CK Enterprise Tactics		
1. Initial Access	5. Defense Evasion	9. Collection
2. Execution	6. Credential Access	10. Exfiltration
3. Persistence	7. Discovery	11. Impact
4. Privilege Escalation	8. Lateral Movement	

While there are only 11 tactics in the Enterprise ATT&CK framework, there are scores of techniques, too many to be listed here.

They can be found in https://mitre-attack.github.io/attack-navigator/enterprise/

Reference: (APT Groups and Operations. Spreadsheet.2019 Google)

On the other hand, NIST is based on the NICE Framework for measuring the degree of talent and skills acquired by each profile category. NIST has 7 Categories with 33 Specialty Areas and 52 Work Roles.

NICE Framework Components and Relationships	
Categories	Categories provide the overarching organizational structure of the NICE Framework. There are seven categories, and all are composed of Specialty Areas and work roles.
Specialty Areas	Each specialty area represents an area of concentrated work, or function, within cybersecurity and related work.
Work Roles	Work roles are the most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role.
Knowledge, Skills, and Abilities (KSAs)	KSAs are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training.
Source: NIST Special Publication 800-181	

Therefore, MITRE and NIST allow us to design challenges for a Cyber Range with a wide range of categories and knowledge pools, allowing us to build realistic scenarios and encompassed in a known frame of reference for Windows, Linux, and Mac operating systems. When creating scenarios based on mobile devices, we rely on the MITRE ATT & CK Mobile framework.

However, the MITRE ATT&CK framework is based exclusively on offensive techniques, so when designing digital forensics scenarios, the methodology changes.

The ISO/IEC 27037 standard guides on identifying, gathering / collecting / acquiring, handling, and protecting or preserving digital forensic evidence.

As an example, the target is compromised first thanks to the TTPs, and then the forensic artifacts are collected for the investigation of digital evidence. In this way, the participant has a forensic practice field based on realistic scenarios.

Not all digital forensics scenarios are always based on the discovery of forensic artifacts that demonstrate compromise. There are also forensic scenarios where the participant must search and profile the evidence provided, analyzing several forensic devices, which are discovered every day. In this way the investigation is effective, linking and correlating evidence to gather specific data on Windows, Linux, mobile devices, IoT devices, routers or network traffic scenarios.

For web applications, the Open Web Application Security Project (OWASP) is the best support for the development of complex challenges in web applications.

Reference: (The Open Web Application Security Project (OWASP). OWASP)

3.2. Phase 1: Scenario planning

We need to be creative, and in this phase, we spend a great amount of time and resources to translate the scenario from the creator's mind and illustrate it in a structured way in order to make it usable in a powerful learning tool.

Here we have some of the basic requirements that are necessary to design the challenges:

Scenario Overview

- Goals and Objectives
- Scenario Scope
- Categorization (level, complexity)

Cyber Exercise Phases

- Infrastructure design
- Network topology
- Virtualization

- Middleware and system integration
- Troubleshooting and contingency plans

Outcome

- Analysis and categorization of results
- Abilities acquired
- Knowledge acquired
- Reports and deliverables
- Lessons learned

3.3. Phase 2: QA of scenarios

During this phase, an expert team will test the agreed scenarios, replicate the session, perform a final rehearsal, and verify that they meet the established requirements.

If the scenarios do not have the quality level expected or the level of the challenges is not appropriated, this is the time to step back, review, and start over.

3.4. Phase 3: Deployment

In this last phase, the scenarios are integrated into the Cyber Range solution. The simulator configuration options are outlined; in this way, the instructor has the necessary information and previous validations to execute the scenario.

3.5. Phase 4: Updates

As a security consultant or pentester, you know that new vulnerabilities are discovered every day. A Cyber Range environment is perfect for deploying these new threats and learning about them.

The Cyber Range should have an interface since where we can load or design new scenarios. This interface allows implementing physical and logical connectivity,

For example, in the case of physical connectivity was necessary, it would implement the addition of a new functional element to the Cyber Range.

Reference: (European Union Agency for Cyber Security.Cyber Good Practice Guide for Incident Management 2019-ENISA

3.6. Sample: Designing a scenario

An exercise must be performed as a real live case where the organization will put its coordination ability to the test, different schedules between countries, or even the internal escalation process. An exercise cloud requires great coordination on the part of the participants and different teams involved. This environment stimulates training and assessment of current business processes associated with planning, executing, and training during an exercise.

Scope:

- Planning: 3 months
- Build-up: 1 -1 month
- Execution: 4 hours

Requirements: Define the objectives with the client and plan the organization. The organizations need to validate the process and train personnel in-between other exercises. Required resources include the people involved in the project, also need time to plan, create, and develop real scenarios.

- The environment must be familiar with the organization and requires an in-depth knowledge of the client and its objectives
- The exercise involves more countries and people travelling for meetings.

Baseline:

- **Objectives:** Train the organization and staff; validate procedures; determine the ability to detect, respond, and recover from simulated real events.
- **Lessons Learned:** Focus on what went well and what needs improvement, assess capability for detecting, responding and recovering from certain simulated and realistic events. In all cases, we use real events to facilitate exercise control evaluation. Allow to build a plan to address the issues areas and increase Red Team capabilities.

4. Offensive Scenarios– Penetration Testers

The scenarios deployed through the Cyber Range must allow for real training on different technologies. This module is focused on the Red Team to improve the area of detection and exploitation of unknown vulnerabilities.

4.1. Web Applications

Web application challenges must cover the principal vulnerabilities. The exercises developed should provide answers to the following points of OWASP 2017.

- A1: Injection
- A2: Broken Authentication and Session Management
- A3: Cross-Site Scripting (XSS)
- A4: Unsafe direct object references
- A5: Incorrect security configuration
- A6: Sensitive data exposed
- A7: Function level access control is missing
- A8: Cross-Site Request Forgery (CSRF)
- A9: Use of known vulnerable components
- A10: Redirects and forwarding not validated

During the training in web applications, the purpose of the evaluation is to identify any vulnerability that could be exploited to attack the server-side, client-side, avoid controls, increase privileges, or extract confidential data.

During the evaluation, participants will use proven invasive test techniques to identify any weaknesses quickly. The application is viewed and manipulated from various perspectives, even without credentials, user credentials, and privileged user credentials.

Some free products that can be introduced as vulnerable frameworks for testing are the following refereces:

1. **Error! Reference source not found.**)
2. The Open Web Application Security Project. 2018 OWASP. WebGoat https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project)

3. The Open Web Application Security Project. 2019 OWASP RailsGoat https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

4. The Open Web Application Security Project. 2017 OWASP.WebGoat.NET: (https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project)

5. The Open Web Application Security Project. 2018 OWASP Mutillidae 2012 Reference: https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

4.2. Infrastructure

Infrastructure scenarios make it possible to improve offensive attack capacity and, in the same way, improve defensive techniques.

This environment should be interconnected in different interrelated networks. The number of networks and the number of equipment will depend on the requirements of a customer. Training in this environment guarantees the passing of the necessary tests to pass the certification. The Cyber Range should be able to withstand the following configurations.

- Domain Controllers - Windows 2012, 2016 and 2019 and Windows 7 and 10 clients
- Web servers
- Database Servers
- Application servers
- Backup Servers
- Servers with software vulnerable to a buffer overflow
- Outdated equipment or third-party software without updating

The scenarios should allow the following actions by instructors and participants

- The analysis focused on critical systems, such as domain controllers and databases.
- Top-level review of a more significant number of systems on the LAN or DMZ
- Oriented to critical vulnerabilities that could lead to a commitment to the network.
- Pivoting
- Elevate privileges
- Execute public or private exploits

All hosts are analyzed in the most used protocols (TCP, UDP, and ICMP) to identify hosts in production.

- Active Directory AD domains and forests will be identified, as will independent servers. Whenever possible, account information will be listed.
- UNIX servers will be analyzed to run services such as Telnet, SSH, X11, r-services, SNMP, and NFS.
- Web services will be identified.
- Database services will be listed.
- Network Recognition
- Recognition of installed applications
- Malicious Domain Recognition
- Malicious Website Recognition

It is possible to use all the desired tools in the Cyber Range to detect all services and list specific details to identify potential vulnerabilities and exploit them.

4.3. Windows Environment

Windows environments are the most expanded among organizations. The development of these scenarios which allow us to learn how to compromise domain controllers, allow us to assess the risks of our possible organization network

All the exposed vulnerabilities must correspond to real cases, which are implemented and tested during the design and implementation phases. The objective is to be the domain administrator of each one of them.

These exercises have integrated clients within the domain controller to simulate external and internal attacks, in case a successful attacker could extract the user accounts and thus compromise the entire organization.

- Some vulnerabilities detected would be the following.
- Common Windows Vulnerabilities
- Lack of protection against external attacks
- Excessive permissions on shares and files
- Lack of protection against viruses/malware
- Weak or non-existent encryption
- Do not comply with the minimum security policy
- Weak security policies
- Weak or default passwords
- Other vulnerabilities and most common configuration errors in an active directory can be found in our mini labs.
- Active Directory Settings by default
- Too many domain administrator accounts
- Insufficient patching on servers / Workstation
- Do not keep an inventory of accounts/users with delegated access

- Service accounts with excess privileges
- Do not keep access control of privileged users to the AD
- Use of the same password on different servers
- Obsolete authentication methods (LM / NTLMv1)
- Access from systems without a trust relationship
- Execution of non-essential services on domain controllers
- Do not correctly isolate network resources, such as critical servers
- Do not keep security updates up to date
- Incorrect credential management

Through these vulnerabilities and scenarios, a participant could understand and achieve a total commitment of the system, allowing him to advance and understand from a defensive point, the techniques necessary to stop the attack.

4.4. Networking

Poorly configured firewalls and underlying network devices may allow an attacker to compromise the network. Ambiguous or poorly designed rules often create attack vectors. Unrestricted exit access can exacerbate data loss or allow malicious users to design attacks against other devices. During the cyber exercises, poorly configured Firewall devices would be available, which will allow the participant to practice in real environments.

The analysis will show the security status of the network perimeter against a potentially unsecured network such as the Internet and that there is a dedicated DMZ and adequate segmentation. Generally, excessive access to a particular system or range of systems is given, often the network administrator asks that all ports be opened to a particular device, perhaps during the implementation period and then it is not indicated that the cycle of implementation is complete and the access rule must be removed.

Sometimes outgoing access is not well defined, allowing superfluous access to services such as FTP, ICMP, and DNS.

The student reviews the firewall configuration to ensure that its policy is appropriate and adequately documented, considering the context of the environment.

During the scenario, it will be possible to perform the checks on the integrity of the firewall and the device:

- Ensure that global rules and properties are consistent with the security policy of the device and the firewall
- Ensure that no additional or inappropriate rules have been configured. This includes the identification of inactive rules
- Ensure that the rules consider bidirectional filtering (input and output), capturing control of outgoing connections
- Ensure that proper and proper storage of logs is being performed and that a well-defined method has been established to retain this information for enough period.
- Scan the underlying device to locate unnecessary and unnecessary services, default access credentials, obsolete operating system, missing patches, management services (such as Telnet and SSH) and general settings
- Ensure that routing methodology, authentication schemes, and VPN settings conform to the best practices recommended

References: (Cyber Threat Map. Top 5 Reported Industries – 2020 FireEye)

5. Defensive Scenarios– Incident Responders

The defensive scenarios are aimed at training, perfecting, and increasing the capabilities of the teams in the defensive area of Cyber Security. Teams will face attacks live, and for a limited time, which will challenge and test all their knowledge and skills.

Users will access isolated environments where they can practice real-life scenarios through challenges developed by the expert team. The scenarios are based on the NIST methodology and the NIST.SP.800-61r2.pdf document.

Reference: (US Department of Commerce. National Institute of Standard and Technology. NIST. (8/06/2012) Revision 2)

The exercises must address the following points:

- Specific events / metrics
- Determined Objects (Set of elements that make up a network)
- Threat Detection and Analysis
- Countermeasures and Risk Mitigation
- Attack's Impact Assessment
- Internal procedures

This technology tests the level of preparation, detection, eradication, and recovery after an incident. A cyber Range allows us to test not only the technical knowledge of the organization but also all the human resources and resources available to stop a security incident.

Reference: (6 new metrics for measuring incident response using automation. Andrew Bushby, UK director 2019 Information Age)

5.1. Infrastructure

In the Cyber Range, an Infrastructure is developed that contemplates all the security measures of an organization. In the same way, the probes of the detection of attacks and defensive measures are installed and deployed. Unlike an offensive infrastructure, the development of a defensive infrastructure is built with the maximum-security measures implemented, which are close to the reality of corporate environments

Each exercise should evaluate a possible point of attack. An example would be to assess the ability of participants to detect and mitigate a phishing attack. Moreover, in the same way in which administrative and technical steps must be followed if the phishing attack succeeds.

Usually, an attacker aims to compromise the corporate network entirely by successfully accessing the domain controller from an external server controlled by the attacker. The attack will be prepared to evade security measures such as antivirus or IDS (Intrusion Detection System)

The scenario is developed with the attack methodology based on the MITRE ATT&CK framework.

5.2. Goals

- Analysis of security measurements
- Forensic analysis of compromised teams
- Evaluation of information leaked
- Decision-making
- Fraudulent email analysis

Reference: Defining Metrics for Incident Management. 2018. Stuart Rance 23/09/2014. SysAid

5.3. Threat Hunting

This is the case when the defenders take a proactive defensive posture. In this way, they are not waiting for an internal system, such as an IDS, events log, or Firewall to flag an event. The blue team is actively searching the network for any indication of a threat or compromise. This task is essential to use tools that will assist the hunter.

The goals for this team would be

- Detect the intruder
- Prevent them from gaining a stronger foothold with the network
- Remove them from the network

An environment such as a cyber range allows exercises to be carried out where defensive teams will need to hunt down attackers or threats that they can proactively cause. Usually, the companies include threat hunting experts in their Incident Response. The goal for this is to learn about APT "Advance Persistent Threat" and prevent it. The threat hunting requires multiples skills and technical teams involved.

6. Reporting

6.1. Scoreboard

The scoreboard allows displaying the offensive and defensive aptitudes separately allowing the supervisors to always have control over the progress of the participants. The Cyber Range always shows the scoreboard and the data related to all the members, which generates a healthy competition environment allowing to improve in each step of the training.

6.2. Levels

- Basic
- Medium
- Advanced
- Extreme

6.3. Metrics

The metrics of these exercises are usually relative measures of the results within the scope of the test. The desired results differ for organizations and each domain, but they usually revolve around providing a realistic scenario where participants must solve real challenges.

Cyber Range uses platforms to support the assessment of current capabilities in companies. The organized and controlled competitions by Cyber Range present a unique opportunity to identify the strengths and weaknesses of each participant.

Reference (European Union Agency for Cyber Security.Leads a wide range of activities in the field of cyber exercises. 2019-ENISA)

6.4. Maturity

Organizations are at different levels of maturity and therefore require different exercises. This approach allows organizations to enter processes of awareness and discover the state of maturity of their internal processes. . Identify gaps within the organizational resources, identify what subprocess should be adopted to make improvements and of this way could design meaningful process to organization.

7. Benefits

Cyber exercises allow extracting conclusions based on the challenges that are delivered to the participants of each team. The response and presentation of the reports allow us to extract and create statistics that are accessible by the organizers in real-time. Similarly, through the Cyber Range, we could extract conclusions based on the questionnaires about the artifacts that are delivered to the participants, the flags found, or other metric systems that we have defined in each exercise and implemented in the Cyber Range.

The generation of environments and challenges based on real cases allows having the right balance of exercises on different challenges and degrees of difficulty, as well as the creation of a repository of knowledge within the organizer based on lessons learned.

Although the responses are measured quantitatively based on the maximum or minimum score by the level of difficulty, the objective of these answers allows having a knowledge base to significantly increase the results, providing a differential value to the organization that carries out the investment in a Cyber Range.

Next, we name some of the benefits of carrying out simulation exercises on a Cyber Range, which will be enhanced and improved in any of the cases.

- Vulnerability Detection
- Exploit development
- Development of non-harmful Malware for proof of concept
- The exploitation of Web vulnerabilities, operating systems, and applications
- Internal recognition of networks
- Privilege escalation
- Lateral movements
- Establishment of persistence
- Deletion of evidence
- Password breakage
- Actions of "Denials of Service" in web systems
- Forensic analysis
- Evidence Collection

References: (European Union Agency for Cyber Security.Cyber Europe Program.2019-ENISA and European Union Agency for Cyber Security.Cyber Good Practice Guide for Incident Management 2019-ENISA)

8. Conclusion

During the document, we have analyzed what a Cyber Range, which allows us to carry out and what benefits it provides is. In general, the technology implemented implies that the people behind it have a high degree of knowledge not only in cybersecurity but also in other facets such as IT or OT systems. A significant investment in the development and management of a Cyber Range is required. However, it is notable how this solution is being imposed on organizations that wish to carry out simulations of their incident response teams or wish to improve their pentesting teams.

The most valuable certifications in the market are beginning to use this technology to validate the aptitudes of the students, because they put into practice not only the technical ability, but also the human capacity of each student.

In the next few years, a good range of Cyber Range solutions is approaching, large corporations are investing much money in these solutions, due to the possible income that the integration of this technology can contribute in government or even military defense systems.

The benefits they bring are many and varied, from the recruitment of talent to have a fleet of personnel prepared to face day-to-day threats. In the same way, it serves as a place of investigation and support for the analysis of future threats.

9. References

1. Definition.What Is a Cyber Range?.2018 Cloudshare.

   https://www.cloudshare.com/virtual-it-labs-glossary/cyber-range

2. US Department of Commerce. National Institute of Standard and Technology. NIST. (8/06/2012) Revision 2

   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

3. European Union Agency for Cyber Security.Leads a wide range of activities in the field of cyber exercises. 2019-ENISA

   https://www.enisa.europa.eu/topics/cyber-exercises

4. European Union Agency for Cyber Security.Cyber Europe Program.2019-ENISA

   https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

5. European Union Agency for Cyber Security.Cyber Good Practice Guide for Incident Management 2019-ENISA

   https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

6. The Open Web Application Security Project (OWASP). OWASP

   https://owasp.org/www-project-top-ten/

7. Cyber Threat Map. Top 5 Reported Industries – 2020 FireEye

   https://www.fireeye.com/cyber-map/threat-map.html

8. APT Groups and Operations. Spreadsheet.2019 Google

   https://goo.gl/QEayyo

9. Government Technology. Cyber Range: Who, What, When, Where, How and Why?. Dan Lohrmann 10/03/2018 LOHRMANN ON CYBERSECURITY & INFRASTRUCTURE. Govteh.com

https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cyber-range-who-what-when-where-how-and-why.html

10. Training and simulation environments at scale breadth and speed to out maneuver bad actors. Cyber range Solution. 2019 VMware

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/ clearlyindustry/vmware-cyberrange-datasheet.pdf

11. 6 new metrics for measuring incident response using automation. Andrew Bushby, UK director 2019 Information Age

https://www.information-age.com/incident-response-automation-123471307/

12. Defining Metrics for Incident Management. 2018. Stuart Rance 23/09/2014. SysAid

https://www.sysaid.com/blog/entry/defining-metrics-for-incident-management

Last Updated: May 30th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Amsterdam August 2020	**Amsterdam, NL**	**Aug 03, 2020 - Aug 08, 2020**	**Live Event**
SANS FOR508 Canberra August 2020	**Canberra, AU**	**Aug 17, 2020 - Aug 22, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**