
# GALAXIA,

## CYBERSECURITY TRAINING

Detailed description of scenarios

Nexova

IDELUX DÉVELOPPEMENT

# TABLE OF CONTENTS

# DURATION OF THE SCENARIOS

The durations below are very subjective depending on the proficiency of the participants and the orientation level provided by the trainer.

| Scenario | Estimated duration (min) |
|---|---|
| 1. Password Cracking | 60’ |
| 2. SQL Injection | 90’ |
| 3. Firewall and Network Filtering | 90’ |
| 4. Privilege Escalation | 90’ |
| 5. Network & Vulnerability Scan | 9’ |
| 6. Log4j Exploitation Apache Solr | 120’ |
| 7. MitM and Poissonning | 90’ |
| 8. Malicious Macros and YARA Detection | 120’ |
| 9. Defensive | 180’ |
| 10. Cross-Site Scripting (XSS) | 90’ |
| 11. Fortified Castle | 90’ |
| 12. Capture The Flag (CTF) | 180’ |
| 13. Energy | 180’ |
| 14. Railway | 180’ |
| 15. Phishing | 90’ |

# 1. PASSWORD CRACKING

This scenario is divided into three modules, each designed to helps the learners to progressively develop their proficiency in password piracy using different techniques and tools.

At the end of the scenario, the learners will have a solid understanding of the different methods of password cracking and the way to use them efficiently in controlled environments.

In each module, the learners will concentrate on the execution of the different techniques of password cracking to find out the user's identification information. They will start with offline password cracking, then online attacks and will finish by learning how to apply password manipulation techniques to improve their success rate.

For the basic level, the environment consists of two virtual machines: a KALI VM and a Windows 7 VM. The learners will use the KALI virtual machine to carry out password cracking attacks, as the Windows 7 virtual machine is configurated with a document protected with a password that the learners must try to unlock.

For the intermediary and advanced levels, the environment includes the VM KALI and an VM WEB. The VM WEB hosts a web application with a connection page that the learners must attack using online password cracking techniques. As the difficulty increases, the security of the web application is reinforced, which means that more advanced methods will be required to compromise the login information.

This scenario was designed to give learners practical experience in password cracking, from breaking into a document protected by a password to compromising login details on a web application. This training course will help to better understand the vulnerabilities of passwords and the way they can be exploited.

# 2. SQL INJECTION

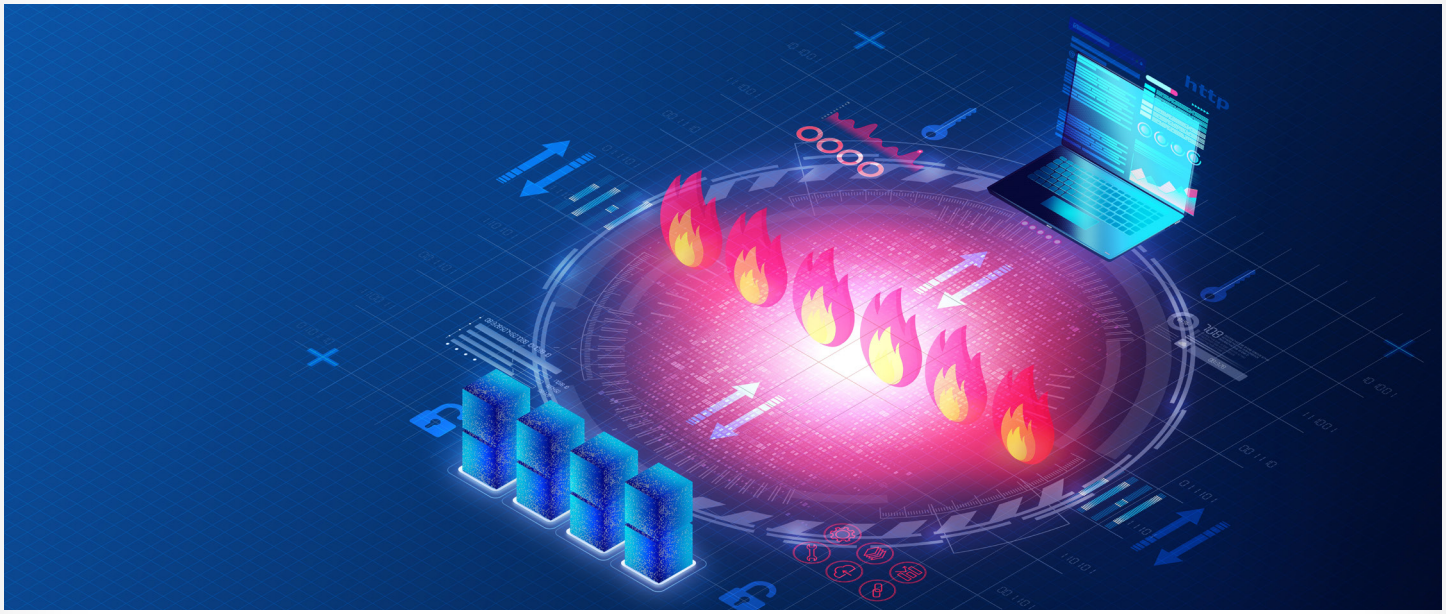

The scenario is designed with three levels of difficulty: basic, intermediary and advanced. Each level has its own challenges and its complexity increases progressively to help the learners develop and affine their proficiency.

The challenge is greater at the intermediary level. The learners will have to face an input filtering designed to block SQL injections. The have to get around these filters to access the login page and extract data from the table of users, avoiding the protection measures. This level highlights the need to understand and bypass common security defences. The advanced level combines all the learning points, demanding a strategic approach. The learners will manually carry out a blind SQL injection attack, where feedback from the server is minimal, requiring precise techniques. They also have to bypass filters specifically designed to block the blind SQL injection. This level tests their profound understanding of SQL injection and their capacity to manage the most restrictive conditions.

In addition to understanding the SQL vulnerabilities and web security, the learners must also be familiar with the basic methods of entry filtering. This additional layer of knowledge will be essential when confronting more sophisticated security measures designed to block the SQL injection attempts.

This scenario is designed to give learners practical experience with SQL injection attacks, from bypassing a login page to extracting sensitive data from a database. This training course will help to better understand the potential risks and the way these vulnerabilities can be exploited.

# 3. FIREWALL AND NETWORK FILTERING




This scenario provides the infrastructure necessary to carry out a basic configuration of a Palo Alto firewall. Through practical exercises in firewall configuration and network filtering, the learners will acquire a fundamental understanding of firewall configuration specifically focused on the Palo Alto platform. In this laboratory, the objectives are firstly to familiarise the learners with network key concepts, essential to understand the behaviour of firewalls. They will then learn how to configure a firewall to manage the traffic specific models, which will help them to control the data flow of the network.

In addition, they will explore the management interface of Palo Alto's web applications, where these configurations will be applied. At the end of the training course, the learners will be able to reproduce and reconfigure the basic rules of a firewall, explain the fundamental concepts of a firewall and the segmentation of the network, and monitor and solve basic problems for a Palo Alto firewall.

The scenario includes four network zones: IT LAN, Office LAN, DMZ and Intranet LAN, which helps them acquire practical experience in the management and segmentation of network traffic between different zones. The learners will have access to the IT-PC, which will be their main work station to interact with the network. From the IT-PC, the learner will access the Palo Alto firewall web interface, where they will configure different settings. The objective is to manage and secure the network by adjusting the configuration, by creating policies and defining the rules to control the traffic between different zones of the network.

This scenario is designed to give learners a practical experience in the configuration of a firewall and the filtering of network traffic, from the implementation of basic firewall rules to the management of traffic between different network zones. This training course will allow them to better understand how firewalls can be used to secure and segment networks.

# 4. PRIVILEGE ESCALATION

This scenario is designed to help the learners develop their proficiency in privilege escalation on a target system using diverse tools and techniques, which will allow them to understand how attackers obtain administrator access to a system. The objective of this scenario is to show learners the risks linked to weak identification information, combined with a poorly configured system that is not up to date.

After this training course, the learners will be able to articulate the acquired knowledge to better protect identification information, explain why a strong password policy is essential to protect the systems, as well as understand and generalise the importance of updating and patching systems.

The scenario aims to present the learners with web attacks targeting vulnerable and poorly secured web applications, with default identification information. It underlines the importance of modifying the default identification information and guides the learners through the challenges caused by unpatched and vulnerable exploitation systems with known CVE, the exploitation of poorly protected files and the security of files. The learners will study how an initial trust anchor can be exploited and spread to other vulnerabilities, to finally gain a root access to a server.

Throughout the scenario, the learners will have access to the VM ATK that they will use to carry out attacks and work on each step of the process.

This scenario is designed to give the learners a practical experience in privilege escalation, from exploiting initial vulnerabilities to obtaining a higher level access on a target system. This training course will allow them to better understand how privilege escalation can be done and the techniques used to exploit the weaknesses in a system.

# 5. NETWORK & VULNERABILITY SCAN

This scenario is designed to help the learners develop their proficiency in analysing networks and identifying vulnerabilities using diverse tools and techniques. In this scenario, the learners will focus on several key objectives. Firstly, they will learn the basics of network analysis through identifying and mapping the structures of the network. Then, they will receive practical experience by carrying out analyses on real networks, applying the techniques that they have learned. They will also learn to count off the exposed services, which is essential to identify the potential entry points in a network. Finally, they will be introduced to the fundamental principles of vulnerability analysis, which will help them to recognise potential weaknesses in the systems they analyse.

The learners have access to a laboratory that allows them to carry out network analyses on a number of different hosts, carrying out different services. The first objective of the learners is to discover the available hosts on the network. Then they have to identify the open ports of the hosts from the first step and carry out network analyses using different "nmap" options. Finally, they will have to try and find vulnerabilities on the hosts. If there is time, the learners can try and exploit the vulnerabilities that they have found.

This scenario is designed to give learners a practical experience in network and vulnerability analysis from mapping network structures to identifying the exposed services and potential vulnerabilities. This training course will allow them to acquire a solid base in network security and vulnerability evaluation.

# 6. LOG4J EXPLOITATION APACHE SOIR

In this laboratory, the learners will be confronted by real scenarios with the critical “Log4Shell” vulnerability, which has affected numerous systems worldwide. The learners will have access to a attacking machine, which will simulate the exploitation of vulnerable applications. They will also use a target server that executes a Java application using the Log4j logging framework.

This configuration simulates a realistic environment to exploit and understand how attackers exploit this vulnerability, providing practical experience in detection and attenuation of the problem. In this session, the learners will work on three difficulty levels: basic, intermediary and advanced.

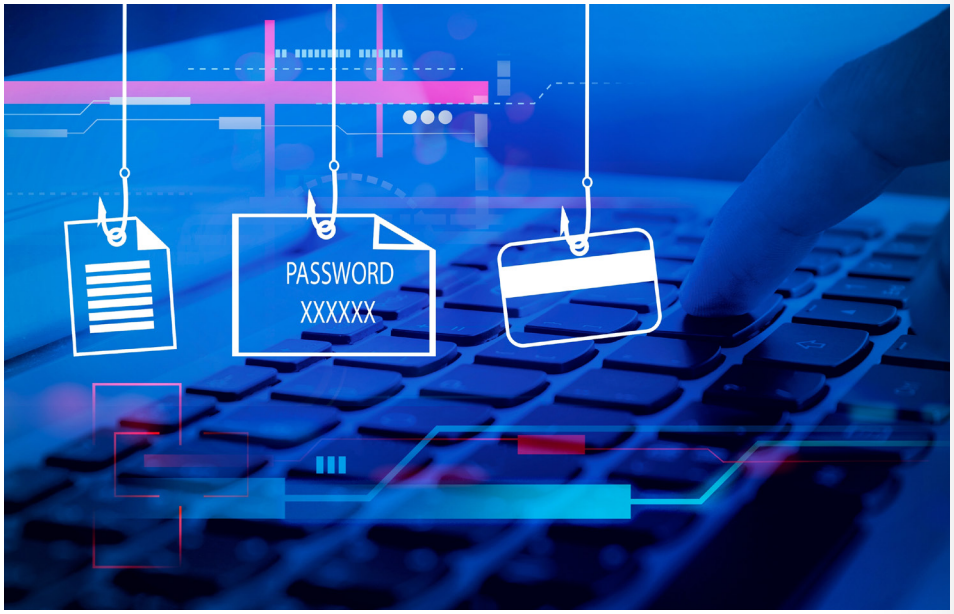
At the advanced level, they will learn how to bypass standard security measures designed to block exploitation, and to apply the manual attenuation strategies to secure the system against more sophisticated attacks. For the basic level, they have to have a fundamental understanding of penetration tests, Java and TCP/IP protocol. Knowledge of server architecture and of the client is also essential. The learners must have a solid knowledge of the offensive and defensive security, as well as the capacity to bypass security measures linked to web applications, such as those used in Apache2 servers.

The learners will always use the attacking machine, but the vulnerable Apache “Solr” server is only accessible by the intermediary of an inverse proxy. This adds an additional layer of complexity as the learners must bypass the proxy to exploit the Log4j vulnerability. In addition, they will have to bypass the inverse proxy security measures, all the while applying the attenuation strategies on the target server.

# 7. MITM AND POISSONNING

This scenario is divided into three modules, each designed to help the learners to progressively develop their proficiency in Man-in-the-Middle type attacks.

In each module, the learners will focus on the execution of a Man-in-the-Middle attacked to intercept and compromise user identification information. They will learn to manipulate the network traffic, to capture sensitive data and take advantage of poor configurations. At the end of the scenario they will have a solid understanding of MitM attack techniques and the way to effectively execute them in controlled environments.




At the intermediary level, the learners will carry out the same attack, but on a more secured website, which will require a more profound understanding of the security measures in place and they ways to bypass them.

Before being immerged in the scenario, it is important that the learners have a solid understanding of the basics of web applications, such as the functioning of web sites, HTTP/HTTPS protocols and the role of cookies and the authentication sessions of the user.

In addition, it is essential to master the basic principals of networks, especially IP addressing, DNS, TCP/IP and packet flow.

These prerequisites will enable the learners to understand the mechanisms of traffic interception and the execution of Man-in-the-Middle attacks in diverse environments. The training environment is made up of two main elements. Firstly, there is the virtual attacking machine, to which the learners will have full access. This virtual machine is equipped with all the necessary tools to carry out Man-in-the-Middle attacks, capture network traffic and exploit vulnerabilities.

There is also the user work station, which simulates the target victim. This machine is used by the victim to navigate on a web application hosted in the environment. The objective of the learners is to intercept and compromise the identification information when the user interacts with the web application.

This scenario was designed to give learners practical experience in Man-in-the-Middle attacks, from the interception of network traffic to the compromise of user identification information during a web session. This training course will allow them to better understand how network vulnerabilities can be exploited to steal sensitive information.

# 8. MALICIOUS MACROS AND YARA DETECTION

This scenario is divided into three modules, each designed to helps the learners to progressively develop their proficiency in creating YARA rules.

In each module, the learners will focus on the development of a simple YARA rule to match chains of specific characters in a document containing macros. At the end of the scenario, they will have acquired a good mastery of the fundamental principals of YARA rules.

In the intermediary scenario, the learners have access to a Windows executable file and an ODT document. They have to identify the malicious payload in the provided document and understand its function. Then, they have to construct YARA rules based on the properties of the provided files.

The learners will have to understand the encryption process and decrypt one of the ODT files to collect the information, update their YARA rule from the previous section and finally, execute the YARA rule on all the files.
Next, we will discuss the prerequisites for the exercise.

For the intermediary level, in addition to having basic proficiency, knowledge of macros, Metasploit and chain of command tools is essential. The learners will also have be proficient in Python programming to write scripts and automate tasks.


The scenario is made up of two virtual machines. The first is a virtual Windows machine on which OpenOffice and YARA CLI are installed. The learners can use this machine to demonstrate the attack of a malicious document and test their YARA rules.

The second virtual machine works using Kali Linux and is for development purposes. The learners can use it to generate useful charges, create automation tools and experiment.

This scenario is designed to give the learners a practical experience in YARA rules and the identification of malicious documents, from the detection of specific character chains to the analysis of potentially dangerous files. This training course will give them a better understanding of how YARA rules can be used to detect malicious software and prevent threats.

# 9. DEFENSIVE

Throughout this session, the learners will develop their proficiency in detecting and identifying active threats and by reinforcing the defence of the network using adapted rules.

The main objectives of this exercise is to allow the learners to detect in progress cyberattacks by emphasising the importance of real time detection capacities. During the attack, the learners will identify the compromise indicators and will use this information to develop a robust rule that improves the posture of the network security. In addition, the participants will have to produce and present a detailed report documenting their conclusions.

Before starting the laboratory, it is necessary to ensure that the learners meet the required prerequisites. They must have a solid understanding of the fundamental principals of networks, including TCP/IP, DNS, HTTP/HTTPS, as well as experience with routers, network switches and firewalls. They must be familiar with the fundamental concepts of cybersecurity, such as threat vectors, attack methods and defence strategies.

In addition, the learners must master Windows and Linux systems and have some experience in programming or in scripting languages such as Python or Bash.

Advanced understanding in security tools such as SIEM or IDS/IDS systems and firewalls, as well as the ability to create personalised rules, is necessary. A thorough understanding of the incident response process, from identification to post-incident analysis, is also essential.

In this laboratory, the learners will work in a simulation SOC environment. They will use the Analyst machine to supervise the network in real time, by detecting and analysing the threats as and when they occur. The trainer will carry out the attack using the Attacker machine, simulating a real cyberattack. Throughout the session, the learners have to identify, document and respond to the attack as it occurs. The emphasis will be on vigilance, real-time detection and rapid reaction.

The attack in this exercise follows a several step approach, starting by the initial compromise by phishing.

*Note: For the requirements of this laboratory, we will suppose that the external recognition has already been done and that the attacker has gathered the email addresses and domains.*

The attack will begin by recognition, listing web applications using an active scan. Then, initial access will be obtained by phishing, where malicious emails incite users to execute a payload. Once the payload has been activated, execution occurs by user interaction, leading to the establishment of Command & Control via widely used network ports.

The attacker will then escalate privileges and evade defences by increasing their access and disabling essential security tools. The system remains persistent by modifying the boot or login process, ensuring that the attacker remains inside the system. As the attack progresses, discovery and lateral movement are carried out when the attacker scans the network services and uses remote services to navigate the network.

Then, the attacker will collect data, taking information from the local system. The Command & Control is facilitated by the intermediary of a multi-hop proxy to keep control of the compromised systems. The persistence and privilege escalation will be reinforced by the creation or the modification of the system processes, which allow continuous access and even higher privileges within the network.

The attack will peak at impact, when the attacker finalises the compromise by defacing the system, in other words, by modifying web pages or visual elements to highlight the breach.

Once the attack simulation is finished, the learners must write a complete report. This report must describe the nature of the attack, the moment that it happened and the results obtained, all the while presenting the recommended actions to attenuate each identified threat. This report will then be sent to the respective intervention teams.

# 10. CROSS-SITE SCRIPTING (XSS)

This exercise is designed to introduce the learners to one of the most widespread risks in terms of web application security and help them to develop the necessary expertise to identify and exploit XSS vulnerabilities. The objective of this scenario is to train learners on the identification and exploitation of different XSS vulnerability levels (Cross-Site Scripting). The scenario presents an activity with three levels of difficulty: basic, intermediary and advanced.

In the basic level, the learners face the simplest challenges to understand the fundamental XSS principles. Clues are available but will lead to a 20% reduction in points. The intermediary level presents more complex challenges, guiding the learners in the right direction using clues that reduce points by 40%. At the advanced level, the challenges are more difficult, with clues suggesting specific actions, but their use leads to a 60% reduction in points.

The main objective is to help the learners to progressively master the XSS vulnerabilities while balancing the use of clues with their problem solving skills.

The environment is made up of a web server executing the vulnerable application as well as the learners' work stations. The application itself functions with a Docker container and is accessible via the 1337 port, under the webrealm domain.

# 11. FORTIFED CASTLE

In this exercise, we are going to explore how unsecured communication protocols of ICS (Industrial Controller Systems) systems can be exploited.

Industrial Controller Systems, ICS, SCADA servers and programmable logic controllers are essential to operations. However, without a secured communication protocol, these systems are vulnerable to certain attacks. In this laboratory, we will focus on the Modbus protocol. It is commonly used, but does not have security function such as encryption or authentication.

By exploiting the Modbus vulnerabilities, cyber pirates can disrupt operations in an OT environment. The interconnected nature of ICS and IT systems has very often eliminated their isolation, and so they are more exposed to unauthorised access.

The objective of this exercise is to raise awareness of the exploitation of unsecured ICS protocols. They will learn how attackers gain unauthorised access to industrial systems and how they can manipulate the commands and system statuses.

The learner must have basic skills in IT and internet browsing. They should also understand the TCP/IP protocol, SCADA communication models and understand the basics of Modbus protocol. An introduction to network structures, data transmission, and the basics of connectivity is also required.

In this virtual laboratory, the learner will work with several key elements. The castle simulates an industrial device controlling a flag. The controller controls the flag by following the commands from the SCADA server and reports its status. The SCADA server sends commands to raise or lower it, and also receives updates on the status of the controller.

The attacker machine will be used to simulate unauthorised access attempts on the ICS environment, including the SCADA server and the Programmable Logic Controller, PLC.

# 12. CAPTURE THE FLAG (CTF)

The Capture the Flag competition includes challenges ranging from basic to advanced. In a CTF competition, participants must complete different challenges to uncover hidden pieces of information, known as flags. These flags are the proof that the learner has succeeded in completing the challenge, and each captured flag wins them points. The aim is to have as many points as possible by capturing as many flags as possible.

The CTF competition includes four different categories: Full Pwn, Web, Forensics et Reversing.

Each category focuses on different aspects of cybersecurity and together, they cover a wide range of skills. There is something for everyone, whether it's offensive tactics, web security, in-depth code analysis, or digital forensics.

How to complete the challenges?

The CTF competition is made up of a multi-scenario environment. The first is used to host the competition platform, where the challenge information and the display table are found.

The second is used as a playground for the learners and has a Kali Linux virtual machine, Docker containers and virtual machines linked to the challenges. The competition platform is accessible via the OPNsense firewall, which acts as a transition for learners.

As a trainer, the deployment of the CTF competition has several steps that are, of course, documented in the trainer guide.

# 13. ENERGY

This scenario is divided into three modules, each designed to help the learners to progressively strengthen their proficiency in detecting and attenuating sophistication cyberattacks that target IT and OT environments.

The aim of this exercise is to help the learners understand how a complex cyberattack targeting the IT systems of a business in the energy sector can cause serious disruptions and risks for the businesses.

The objective of this exercise is to simulate a realistic cyberattack on a business in the energy sector. They will first learn to bypass initial security defences, then to carry out recognition and move laterally within the OT network.

They will also have to scan and map the infrastructure to understand the layout. The exercise consists in exploiting the vulnerabilities of the OT infrastructure by perpetrating an attack that will cause a city wide power cut. The aim is to understand the techniques the attackers could use and how to defend against them.

Before beginning this exercise, the learners must have a good command of several key domains. Understanding HTTP and SSH protocols is essential for network communication and secured connections. Understanding proxy and reverse proxy functions will be useful to learn how attackers bypass security checks.

The learners also have to master the use of Linux for system management and have a good understanding of network concepts. Experience using Metasploit is important to simulate attacks and exploit vulnerabilities. In addition, skills in programming will be useful for script writing and task automation.

In this exercise, the learners will start by a Water Hole attack on a climbing web site frequently visited by an IT employee. By compromising this website, the learner aims to incite users to download malware.

Once the malware has been installed, the learner will analyse the work station and the compromised network. The next step is to exploit the Grafana server by using a path traversal vulnerability to access its database, crack passwords, and gain root access via SSH.

From there, the learner will place a malicious document on an FTP server that transfers data between the IT and OT networks. When the document is open, it will exploit the engineers work station.

Finally, the learner will use a Python script to stop the power station's generator, which will cause a blackout.

The power station has four generators that produce the electricity for the city. The electricity produced is sent to a step-up transformer, which increases the voltage for transmission. Two circuit breakers, one before and one after the transformer, control the flow of electricity.

A closed circuit breaker lets electricity flow, whereas an open breaker stops the flow. The power station functions automatically, adjusting the number of active generators depending on the city's consumption of electricity, which it receives from the substation. When the energy produced equals the consumption, the system is stable and the frequency remains at 50 hertz. If the frequency is unstable for more than one minute, the station crashes, which causes a blackout.

The generators and the circuit breakers are controlled by a programmable controller and the engineers can manage them by the local HMI or the SCADA HMI. The substation, located near the city, uses a step-down transformer to reduce the distribution voltage.

Like the power station, it uses circuit breakers to control the input and output lines. These circuit breakers are also managed by a programmable controller and can be controlled locally or remotely by the SCADA system. The substation communicates with the power station to determine if the electricity has been produced and transmitted.

This scenario is designed to give the learner a practical experience of the simulation and analysis of a cyberattack on an energy infrastructure, from exploiting the vulnerabilities to the blackout. This training course will help the learner to understand how the attackers target both IT and OT environments and how these threats can be attenuated.

# 14. RAILWAY

In this session, they will learn to obtain unauthorised access to industrial control system and manipulate the commands that supervise rail components. The scenario covers three difficulty levels. For the most advanced, the learners will firstly focus on the infiltration and privilege escalation in the railway's IT infrastructure. They will use this access to explore and spread their control of the network.

Then, they will move on to the OT environment to access and manipulate critical systems such as OPC UA servers and programmable controllers. The objective is to understand the impact of cyberattacks on operational technology where these attacks can disrupt railway operations.

For this exercise, the participants must have solid bases in several key domains. They must have a good understanding of web application security, including the capacity to recognise and exploit common attacks, and have experience in script writing for task automation and the development of personalised tools.

A detailed understanding of Active Directory attacks and of OT protocols, such as Modbus and OPC UA, is essential to navigate and exploit the industrial control systems. In addition, a good understanding of HTTP and SSH protocols, as well as proxy and reverse proxy functions, network traffic analysis will be crucial to analyse and secure the communications network.

In this scenario, the learners will take part in a railway simulation infrastructure, implicating both IT and OT components.

Access to the attacking machine and kiosk is provided. They start by exploiting the ticket sale kiosk's vulnerabilities to obtain an initial access to the network. From there, they will proceed to a privilege escalation, to a recognition and system pivot to infiltrate the IT and technical networks.

The main activities are to carry out ART MITM attacks, capture network traffic to obtain identification information and exploit unsecured server configurations. The final objective is to access the critical OT systems, such as the OPC UA servers and the programmable controller to understand and simulate the impact of cyberattacks on railway operations. The controller is a physical device that controls railway components.

The railway infrastructure is made up of several essential elements: two signal lights, two points, two locomotives and two infrared sensors. The signal lights are green when the points are in different directions and red when they are aligned.

The points allow trains to move between two itineraries: a main itinerary and a divergent itinerary. The locomotives represent the trains, and the infrared sensors are installed at the ends of the tracks in tunnels to detect when trains reach the end of the line. Once detected, the sensors automatically reverse the direction of the trains, simulating a real operation.

The infrastructure is controlled and fed by an electrical box, which consists of two independent elements. The first is a controller that manages the railway infrastructure, including the signal lights and the points. The controller can be accessed via the Ethernet using an Ethernet shield. The second component is an Arduino, used to control the locomotives. This configuration reflects a real environment, where multiple control systems are integration to manage complex railway operations.

# 15. PHISHING

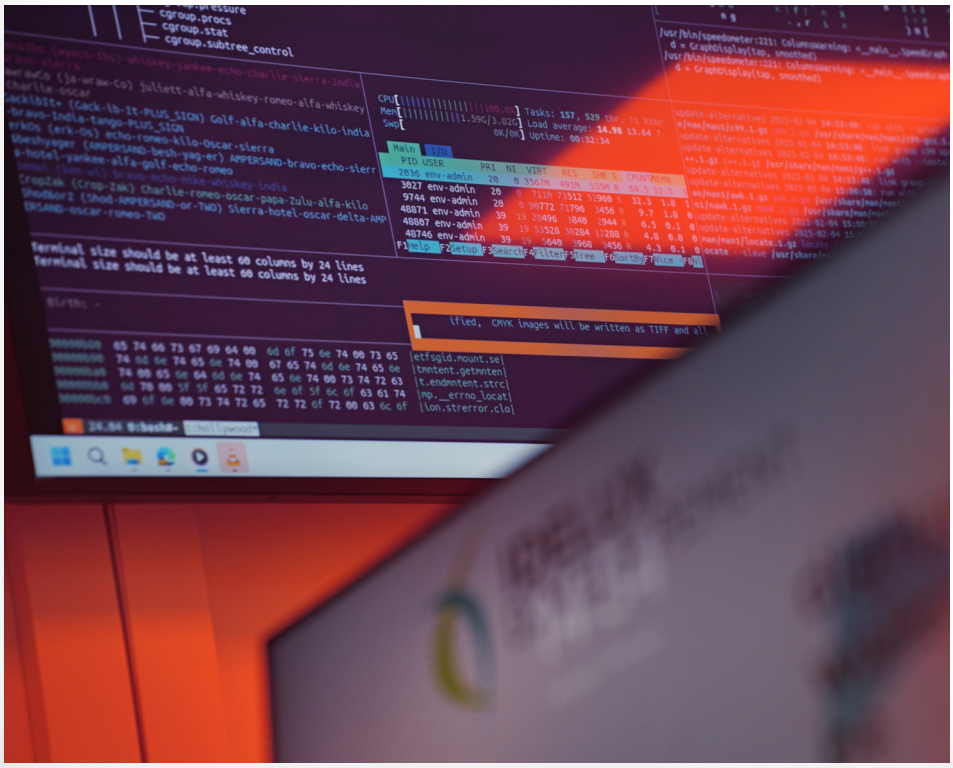
There are two objectives. How to identify “classic” identifiers of a phishing email and how to react when face with such an email?

Participants should be able to use a desktop computer and web-based email account.

The task is to open every email in their inbox and determine whether it is a phishing attempt.

If the email is legitimate, they have to open it and click on the link or open the attachment to win points. Of course, if the legitimate emails are not identified, points will be deducted. In the case of phishing emails, if the right actions have been taken, the participant will earn more or less points.

The participants scores will be displayed on the dashboard to make the activity even more dynamic.



The IDELUX Group, founded in 1962, is the sustainable economic development agency for the province of Luxembourg. With over 60 years' experience, it is structured into five intercommunales (organisations providing services) and employs 500 people. Its public-interest mission is to help to improve the well-being of the inhabitants within its territory through four main areas of activity: economic development, support for community projects, water management and waste management.

In terms of economic development, IDELUX is particularly active in strategic sectors such as space, biotech, logistics, wood, agrifood and tourism. Cybersecurity is also a priority for IDELUX, which is committed to promoting cybersecurity initiatives such as Cyberwal and supporting companies in their efforts. In close collaboration with public and private players, IDELUX works towards the harmonious and sustainable development of the province of Luxembourg, serving its communities and businesses.


**Contact**

Pierre-Yves DEFOSSE
Business Developer

Tel. +32 476 34 93 40

pierre-yves.defosse@idelux.be

www.investinluxembourg.be



Publisher in charge: Fabian COLLARD - Drève de l'Arc-en-Ciel, 98 - B – 6700 ARLON


Nexova

IDELUX DÉVELOPPEMENT

digital wallonia .be

Wallonie Relance

Avec le soutien de la Wallonie