INSTITUTE OF
advanced
cyber defence

THE RANGE SIMULATOR

Hyper-realistic, cutting-edge cyber simulation

The Range Simulator enables top-tier organisations to train their teams with some of the world's most advanced cyber security training technology. It allows participants to experience real-world cyber scenarios, threats and attacks in a simulated environment.

> *Tell me, I forget . Show me, I remember. Involve me, I understand.*
> *Chinese Proverb*

Simulated learning for real-life success

Training via the Range Simulator is as close to reality it gets. Simulations engage students in "deep learning" that empowers understanding. Airlines require pilots to log flight simulator hours, the military uses 'war games' to undertake realistic drills, electrical engineers conduct regular simulations to check load requirements, and so on. Given the success in industry and government - we recognise the value of simulated cyber resilience training, and bring it to your teams.

The Institute of Advanced Cyber Defence's Range simulates networks, traffic and attack scenarios, as well as trains and tests individual procedures and technologies without harming your organisation's network.

Brought to you by The Institute of Advanced Cyber Defence

The Institute of Advanced Cyber Defence aims to advance both the quantity and quality of knowledge and skills in the domain of cyber intelligence and security. Our mission is to bridge the global skills gap and address the dearth of cyber defence competencies.

We offer our training in partnership with Cybint Cyber Solutions. Cybint was founded as a collaboration between military-trained cyber security and intelligence experts, industry professionals and well-seasoned educators. The Cybint training solution is currently used by businesses, higher-education institutions and government agencies worldwide. The aim of the partnership is to enhance awareness, expand education and bolster the capacity of those involved to prevent, investigate and respond to cyber threats and cyber crime.

Cybint Cyber Solutions

Who Should Attend?

The Range is for your team members who have a background and experience in one of the following:

- the SOC department in your organisation or as part of an analysis, incident response or forensics group
- operation and support in your IT department, such as system IT, system administrator, engineer or consultant
- developer or integrator of software systems/applications in your organisation.

The Benefits of the Range Simulator

Each delegate will have the opportunity to do the following:

- work in a computational environment and network that characterises the full organisational network
- experience events in real-time, executed and operated by malicious programs (everything is real, including viruses, malware, exploitation of weaknesses, break-ins, etc.)
- work in operating systems, such as Windows, Linux and others
- work in a replica of the full organisational environment, including different kinds of servers, such as FTP, WEB, Apache, SMTP, DC, IIS, SQL and more
- train teams and individuals to improve and advance their abilities to the fullest to increase their profession skill sets
- strengthen the communication expertise within the team to prepare for coping with stressful situations
- understand work methodologies, including the subjects of ethics, decision-making and escalation.

Range Scenarios

Select scenarios that suit the challenges facing your organisation to customise your Range experience.

1. Ransomware

Trainees will be faced with an actual ransomware attack, which will target the organisational network that they are responsible for defending during training. Trainees will construct a complete and accurate chain of events by conducting a full technical forensic investigation on the infected stations, the network and the C&C Server. In addition, trainees will encounter and discuss the challenges of responding to the ransomware event; therefore, they will also focus on different prevention methods rather than detection.

2. DDoS SYN Flood

In this scenario, the attacker uses many Internet bots to generate a large amount of traffic on one of the organisation's web sites. The traffic floods, and eventually overloads the bandwidth and resources of the target, crippling the server and causing a denial-of-service (DoS) to the web server.

3. DDoS DNS Amplification

In this scenario, the attacker is using the organisation's DNS server to conduct a much wider DNS amplification attack, which is a reflection-based distributed denial of service (DDoS) attack on a target. The attacker sends DNS lookup queries with spoofed IP address of the target to vulnerable DNS servers that support open recursive relays, such as our DMZ-DNS server. The large number of DNS responses are sent "back" to the target as if it requested them, flooding the bandwidth and resources of the target, crippling the server and causing a denial-of-service (DoS).

4. SQL Injection (Intermediate)

In this scenario, the organisation is being directly targeted by an attacker. A series of security flaws in the implementation of the environment enables the attacker to utilise externally accessible services to gain access to internal systems, extract privileged information and interfere with business processes. With this attack, the trainees experience how various "simple" misconfigurations can be used by an experienced attacker and have critical business impact.

5. WMI Worm (Advanced)

In this scenario, the trainees face a worm outbreak firsthand in the internal network. They are required to analyse the attack flow, utilise forensic tools and perform basic malware analysis/reverse engineering to mitigate the threat. The attack simulates the characteristics of a modern Bot-Net and focuses on developing the real-time response capabilities of the trainees.

6. Apache Shutdown (Novice)

This scenario emulates an attack on the organisation's publicly accessible service. The attack disrupts the operation of the service and utilises basic methods to strengthen the attacker's foothold in the system. In this scenario, the trainees are confronted with a disruption to business-critical components and must act swiftly in order to maintain as much uptime as possible and still mitigate the attack. They are also witnessing basic levels of other parts of the attack chain, such as housekeeping and persistence.

7. Trojan Data Leakage (Intermediate)

Spear-phishing is one of the most widely used and notorious ways of infiltrating an organisation, taking advantage of the weakness of the human factor through social engineering. The trainees experience first-hand the entire chain of a successful spear-phishing attack that includes both breaking in, as well as exfiltration of sensitive information. Examples of high-profile spear-phishing attacks include RSA, HBGary Federal and Operation Aurora (attack on Google).

8. DB Dump via FTP Exploit (Advanced)

This scenario demonstrates a sophisticated attacker using multiple methods for pivoting within the system. The attacker circumvents multiple security mechanisms that allow him to reach segments of the network he otherwise couldn't have reached. The entry vector is a laptop being connected to the user's segment, emulating either a rogue employee, infected workstation or a "visitor" gaining access to a port in the wall within the company's premises.

9. Java Applet NMS Kill (Intermediate)

This attack emulates a Watering-Hole attack in which the attacker sits and waits for the victim to perform an action he is expected to perform, such as browsing a certain website. The second emphasis in this scenario is of the attacker blinding the " eyes" of the organisation by taking down the monitoring services while performing other malicious activities. Examples of high-profile watering-hole attacks include U.S Department of Labor, Syrian Electronic Army and some major gas and oil industry companies.

10. Java Applet Send Mail (Intermediate)

This starts as a watering-hole attack. The attacker is waiting for the target to get where he is expected to go. The emphasis in this scenario is on exfiltration of internal data by eavesdropping" all internal email communications in the company.

11. Web Defacement (Novice)

This scenario demonstrates one of the most common web attacks, in which the goal is not harming assets or stealing information. Instead, the goal is mainly to damage the organisation's reputation or send a psychological message. The attacker infiltrates the organisation's Internet-facing web server and mutilates it to display the attacker's message. Recent examples include anonymous attacks on Brazil's and Singapore's government websites.

12. Killer Trojan (Intermediate-Advanced)

The attack vector chosen by the attacker in this scenario is infecting a MIcrosoft Office installation CD. This could have been done by intervening in the supply chain or by replacing the disk inside the targeted company itself. Once inside, a Trojan connects back to the attacker who then sends commands to steal secret files and important user information. As a contingency move, that attacker also hijacks a nearby machine and plants a backdoor that will call home the next time the machine is rebooted. This enables him to maintain access after the current attack ends. To further compromise the organisation, the attacker attaches a malicious PDF file and sends it to other users in the organisation through the originally infected machine.

13. Trojan Share PE (Advanced)

This scenario begins with a phishing attack in which an employee receives an infected email. Because the targeted user has low privileges, the attacker needs to find a way to obtain high privileges. By scanning network shares, the attacker finds a script being run regularly by IT administrators in order to perform a certain backup operation. By modifying this script, the next time it is executed by an admin, the attacker's code is executed with high privileges. From there, the attack pivots to the database server being used for data exfiltration purposes. The attacker loads stolen files into the company's Internet accessible website, enabling him to download them all by accessing the website.

14. WPAD Man-in-the-Middle

In this scenario, the system performs a Man-in-the-Middle (MiTM) attack on the network. The attacker deceives hosts by impersonating a legitimate proxy in the segment. He does this by exploiting the Web Proxy Auto-Discovery (WPAD) Domain Name System (DNS) queries. Once all traffic from the user segment goes though the attacker, sensitive data are extracted and exfiltrated to the CNC server on theInternet using two different methods – ICMP packets and DNS queries.

SCADA protocol scenarios (Critical Infrastructure)

1. HMI - Overloading the Plant (Intermediate)

This scenario shows the dangers of attacks that originate from the internal network. In the scenario, the attacker initiates the attack on the SCADA network from the company's internal network. He exploits and compromises the management station of the SCADA system, the Human-machine interface (HMI). After a full compromise, the attacker uploads a malware designed to stay on the HMI and connect to the physical Programmable logic controllers (PLCs) in order to destroy the plant completely by overloading the turbines.

2. VPN - Shutting Down the Plant (Intermediate)

This scenario shows the dangers of attacks that originate from the Internet and by securing VPN access to the SCADA network. In the scenario, the attack starts by exploiting the well-known vulnerability, Heartbleed, on the VPN server which resides inside the SCADA network. After successful exploitation, the attacker is able to gain access to the SCADA network from the Internet using the VPN. The attacker continues to connect to the PLCs and shuts down the plant.

3. Field 2 Field - Silent Attack (Advanced)

This is an advanced scenario in which the trainees are required to investigate a 'silent' attack on the SCADA network by analysing the protocol that is being used in SCADA networks. The attacker infiltrates the network by taking over one of the physical locations of the SCADA network that is located outside of the plant itself (a remote 'field'). From there, he scans the network and attacks the PLCs that are located inside the factory. The attack is being done in a silent manner, without raising any physical red flags. To understand what the attack does exactly, the trainees will have to investigate the ModBus protocol which is being used in SCADA networks. The trainees will be given a cheatsheet containing references to the protocol and the PLCs.

Talk to the Institute today to schedule a date and select the scenarios that best suits your environment.