Security Training Program

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l.

The systems described in this document are furnished under a license agreement or non-disclosure agreement.

Table Of Contents

Security Training Program 4
Purpose of the program 4
Instructors and training orientation 5
Participants selection and groups formation 5
Continuous assessment 6
Equipment and additional material 7
Overview of the three stages 8
Stage 1 8
Courses details 8
Stage 1 Completion 11
What's next 11
Stage 2 11
Stage 3 12
Appendix A – Questionnaire examples 13
Low level 13
Networking 14

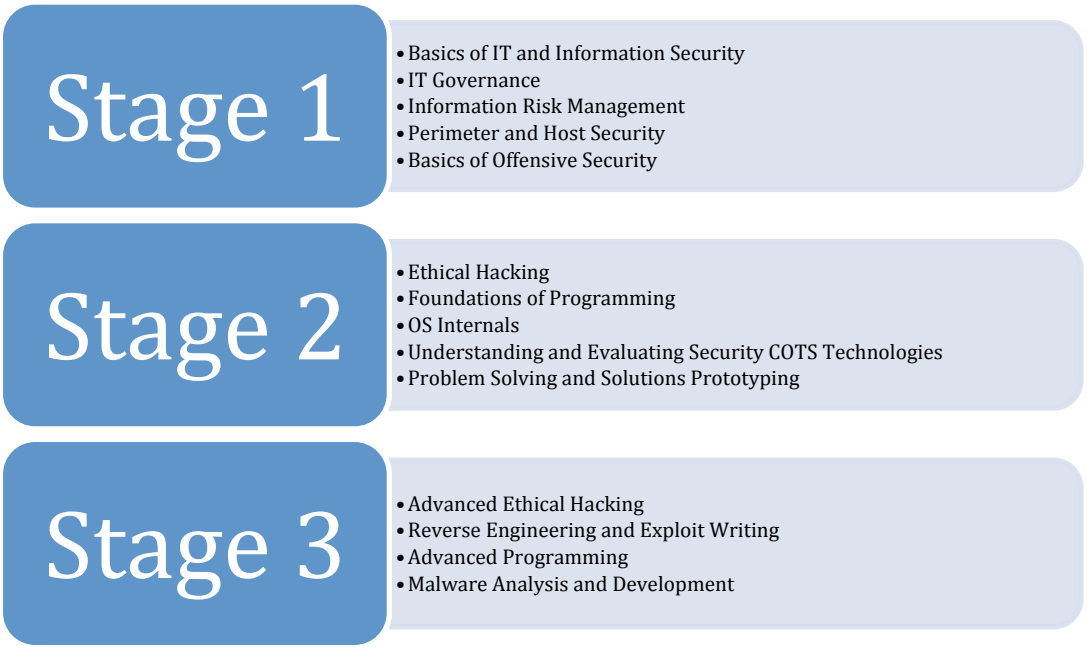
Security Training Program

In today cyber warfare a government must have hacking capabilities and the skills to defend from external threats. While it remains important to be able to correctly setup defensive measures to protect a cyber-infrastructure, it becomes more and more fundamental the acquisition of offensive skills.

An highly skilled Security Team is the only option to secure and actively protect your own resources and critical infrastructure.

In order to build such a team, we propose a graduate level training program, with a strong bias towards practical skills, that turns a trainee into a world-class expert able to independently and successfully orienteer and lead in the field of IT security.

The program is divided into **three stages**, each with specific and peculiar objectives.



The program includes training of **three independent groups**, each composed of 15 people. A **management figure to lead each group** is identified within each group and required to acquire a particular set of skills. Such figure will be chosen according to **preliminary screening** conducted by HT, and can be changed if necessary.

Purpose of the program

Purpose of the training program is to create a world-class team of IT security experts.
By the end of the program, each member will be able to:

- deeply understand complex security scenarios;
- independently assess and elaborate on issues and possible solutions;
- prototype and realize customized tools.

The training covers different aspects of hacking and imparts the necessary skills to take on every aspect of defensive and offensive IT security.

The program empowers the student to plan and implement complex network and system security solutions and actively assess and intrude the security of infrastructure through state of the art penetration techniques. The trainee will also be able to independently analyze, engineer and develop the solutions and tools needed for operating in IT security.

Instructors and training orientation

All the classes are held by **top-class instructors** selected among the best professionals in the computer security field.

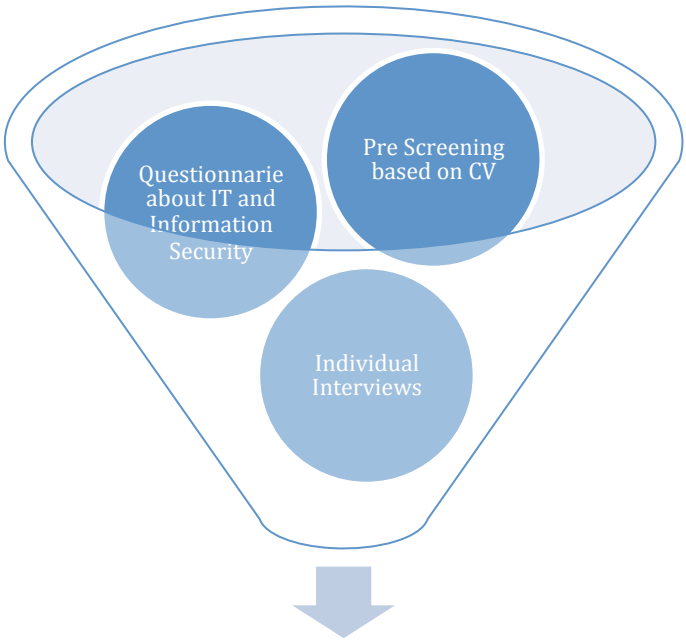
Our instructors are involved daily in real-world computer security, and most of them being are active professionals at respected security firms all over the world. This guarantees a **training program oriented towards practical skills** and rich with knowledge and experience coming from the real world and not only from academic studies.

Participants selection and groups formation

Participant selection is done in three stages:

1. Curriculum Vitae screening;
2. Questionnaire to evaluate the general preparation of the candidates Individual interview (refer to *Appendix A* for examples of questionnaire);
3. Individual interviews to assess the skills and the motivation of the candidates.

Out of the selection process, **45 trainees are chosen** and enlisted in the training program.



Minimum requirement for all participants is a bachelor degree in computer science. Exceptions can be considered for participants who prove to be self-taught in computer security and well versed in computer science.

All the participants need to be personally interested in security in general and IT Security in particular, committed and with high need for achievement, as **the program is very demanding and comparable to a graduate level university course**.
Any individual who doesn't have these characteristics won't be able to take the best out of this very advanced training program.

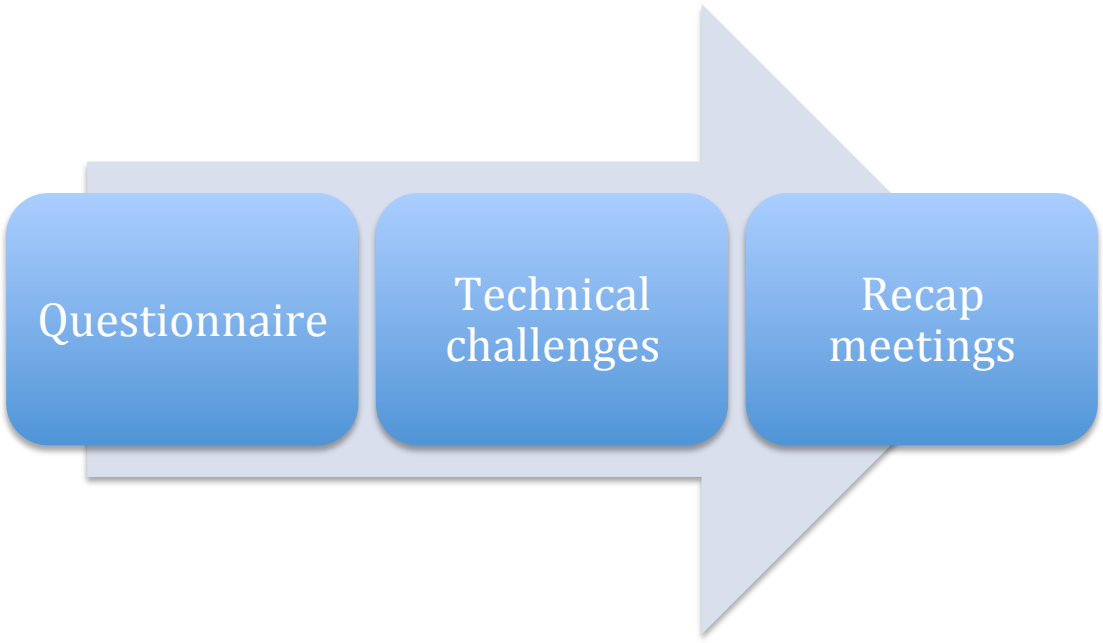
Selection is further done according to specific requirements and characteristics, such as ability to work in a multi-disciplinary team and willingness to learn and improve.

The 45 selected trainees are divided into three groups of 15 each.
The members of each group are aggregated according to diversity criteria, in order to **promote innovation and confrontation**, essential skills to a group that must lead new research into the security field.

For each group, **one trainee is selected to become the group manager**, and trained to acquire the skills needed to lead a team involved in IT Security operations.

Continuous assessment

During the training program, newly learnt skills are c**ontinuously assessed to verify a steady and proficient learning experience**. The assessments include tests and questionnaires, the results of which are used in order to better plan the following courses and Stage participation.



Technical challenges are part of the assessment process; challenges give the students a way to practice and improve their technical skills on the field, at the same time letting the instructor understand the rate of absorption of the imparted training.

Frequent **recap meetings** are periodically held during the program to align all the attendees: managers, students, instructors.

Equipment and additional material

Each trainee will be provided with one laptop, software required for the courses and training material.

To complete the formation, additional books will be given to the students, together with an extended bibliography and reference URLs.

Overview of the three stages

The training program is divided in three stages, each composed of:

- 8 courses of 6 days each (total of 24 sessions for three groups);
- 1 course held approximately every 45 days;
- 2 months of leave are planned during each stage;
- courses located in Italy, London and in Saudi Arabia.

Stage 1

During Stage 1 of the program, each trainee acquires **foundational skills in IT**; a common base level assures homogeneity and guarantees maximum effectiveness in the following Stages.
According to the results obtained in the selection process, the schedule can be adapted and **preliminary courses will be held if necessary**.

A great effort will be made to make all the participants to the program able to flawlessly move in the world of Information Security, which will be considered both from a technical and a managerial point of view.

Courses details

(HT101) IT Security introduction
This course introduces the main concepts of Information Security and covers a wide spectrum of topics, with a strong component inspired to real life examples. The course covers both technical and managerial issues, and makes the attendee able to understand the practical issues behind security information and correctly take care of the process of risk management. Part of the program is basic terminology and concepts, basics of computers and networking including Internet Protocol, routing, Domain Name Service, and network devices, basics of cryptography, security management, and wireless networking; policy as part of risk management is presented as well.
At the end, the practical sides will be experimented with an implementation of defense in-depth.

- Information Security Frameworks
- Secure Infrastructures
- Fundamentals of Cryptography
- Policies for Information Security

(HT102) Defensive Security Essentials
Defensive Security Essentials is focused on the defensive aspects of IT security and provides training on how to keep an IT infrastructure secure. It imparts all the skills needed to protect the sensitive information stored in the organization's network. The course provides techniques immediately usable to determine and implement a security roadmap.
Up-to-the-minute knowledge and skills required for effective security will be in the hands of every trainee at the end of the course.

- Networking Fundamentals
- Network Security
- IT Security Technologies
- Windows hosts Security
- Linux hosts Security

(HT103) Management in IT Security

This course covers the basics of IT security seen from a management point of view. While clarifying the relations between the different aspects and the need for a clear direction in security management, the course walks through the main topics of IT security, including Access Control, Network Security, IT Governance, Risk Management, Business Continuity and Disaster Recovery, Cryptography, Regulations and Physical Security.
At the end of the course, the students are able to effectively organize and manage the organization of the security within a complex reality.

- IT Governance
- Basics of Risk Management
- Business Continuity & Disaster Recovery
- Legal Aspects of IT Security
- Compliance in IT Security

(HT104) Computer Forensics Basics - Windows

This course covers computer forensic and media exploitation methodology from the basics up to in-depth view and understanding of the topic. At the end of the course the students will be able to autonomously work as computer forensic investigators. During classes, in-depth technical digital forensic knowledge on Windows Digital Forensics (Windows XP through Windows 7 and Server 2008) is explained, together with practical use of top of the market tools such as Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more.

- Basics of Forensics
- Evidence Acquisition
- Windows Forensics

(HT105) Advanced Defensive IT Security

Organizations have to consider threats both from external and internal attacks. Therefore a key focus must be on data protection and the ability to secure critical information, no matter whether it resides on a server, on a private network or on a portable device.
For an infrastructure to be secure, the security team has to be able to detect attacks in time, and this requires deep understanding of the traffic on the network. Penetration testing and vulnerability analysis are mandatory skill to identify problems and issues to assess the impact of external threats and devise the necessary countermeasures. Furthermore, when an attack is detected, a quick reaction and adequate forensic analysis has to be performed.
This course makes the trainee able to effectively cover all the steps in the security lifecycle of a complex infrastructure: planning the security measures to be taken, test them and analyze footprints of attacks.

- Defending a Network
- Packet Analysis
- Introduction to Pentesting

- Incident Handling
- Malware
- Data Loss Prevention

(HT106) Perimeter Security

Securing the perimeter of an infrastructure means effectively setting up multiple layers. *Perimeter Security* covers the details of the Internet Protocol, with notions on how to secure a network through correct configuration of firewalls and how to spot abnormal patterns caused by external and internal attacks. OS lockdown techniques are covered as well to secure the exposed servers; part of the course teaches how to sandbox insecure applications and enforce full application policies.

This course gives great attention to problem solving and root cause analysis, essentials in order to effectively implement a secure perimeter.

- Firewalls Understanding and Configuration
- IDS and IPS
- COTS Products Evaluation
- Security of the Host
- Perimeter Security Configuration

(HT107) Offensive IT Security

Understanding the attackers' tactics and techniques is fundamental in order to be able to protect an IT infrastructure. This course gives all the knowledge necessary to find vulnerabilities and discover intrusions and equips the trainee with a comprehensive incident handling plan.

During this course the latest cutting-edge attack vectors, as wells as the old ones, are taught. A comprehensive methodology for Ethical Hacking is given, making the trainee able to perform and document a penetration test. Additionally, the course explores the legal issues bound to all the activities of Information Security.

- Advanced Incident Handling and Investigation
- Network Penetration Testing
- Wifi Penetration Testing
- Protocols Security
- Application and Web Security
- Backdoor deployment

(HT108) Securing Windows Platforms

This course covers the skills necessary to secure Windows platforms, including Windows Desktop and Server versions.

Part of securing a Windows host is screening the code executed and avoiding the infection from malwares: this course includes notions on how to prevent a malware infection, how to identify the behavior of a malware and how to clean an infected host.

- Windows OS Hardening
- Privileges Configuration on Windows
- FDE for Windows
- Windows Firewalling
- Windows Server Applications

Certifications

Each trainee must obtain at least three certifications out of the eight courses attended.
Two stages of certification are available:

- **Silver**: acquired by completing a time-limited questionnaire that covers all the topics of the course.
- **Gold**: acquired by completing a research or development project comparable to a graduate thesis work.

The trainee elected to be the manager for his group has the mandatory requirement to take certification for the course *HT103 – Management in IT Security*.

Stage 1 Completion

Stage 1 gives **foundational knowledge common to all participants**, necessary to successfully achieve a more advanced knowledge taught in the following steps. It covers topics of defensive and offensive security, including securing of network and hosts, malware analysis, incident handling and forensics.

At the end of the 8 courses, the trainee will be able to understand and elaborate on complex issues that involve IT Security, besides leading the risk management process within a complex IT organization.

In order to be admitted to the following stages, **each trainee has to complete Stage 1**.
Stage 1 is considered completed when:

- All 8 courses have been successfully completed;
- Each participant achieves at least 3 certifications;
- One person per each group achieves an IT Security Management certification.

At the end of stage 1, a second round of written questionnaire and personal interviews will be held. The results of this appraisal are used to perfect the organization of the following Stage.

What's next

The following two Stages build on the knowledge acquired during Stage 1, to make the trainees able to evaluate existing technologies, devise their own ideas, develop them into usable software and make use of the most advanced intrusion techniques.

Stage 2

Stage 2 starts to build specialized knowledge; the topics covered during this stage include:

- Foundations of software development;
- Operating Systems internals;
- Advanced hacking techniques.

At the end of this Stage the attendees are security experts, able to understand any security issue, solve problems related to security and implement advanced security solutions.

Furthermore, they are able to deeply understand COTS security technologies, autonomously analyze a problem, devise the best solutions and prototype them in software.

A challenging appraisal session is held in order to detail the program for the next Stage.

Stage 3

Stage 3 builds in-depth vertical knowledge, to make the experts able to turn their ideas into reality, and tackle with ease even the most complex security problems (e.g. writing advanced 0day exploits, developing Stuxnet-like technology). In the 14 months of stage 3 the focus is on **advanced software development and reverse engineering**. The students are taught how to understand the behavior of a malware and how to replicate it in custom written code; from that point, it is expected from the trainee to evolve the functionalities of such software and customize it to own needs.
At the end of the full program any of the students involved will become a highly skilled and all rounded security experts, with skills rarely found on the market and that will enable him to effectively work in the world of IT Security and Offensive Security.

Appendix A – Questionnaire examples

Following is two examples of questionnaire that could be used to assess the initial knowledge and adequateness of the candidates.

Low level

Big vs Little Endian
In big endian, the most significant byte is stored at the memory address location with the lowest address This is akin to left-to-right reading order Little endian is the reverse: the most significant byte is stored at the address with the highest address.

Stack (Memory)
When a function calls another function which calls another function, this memory goes onto the stack An `int` (not a pointer to an `int`) that is created in a function is stored on the stack.

Heap (Memory)
When you allocate data with `new()` or `malloc()`, this data gets stored on the heap.

Malloc
Memory allocated using malloc is persistent—i.e. , it will exist until either the programmer frees the memory or the program is terminated `void *malloc(size_t sz)` Malloc takes as input sz bytes of memory and, if it is successful, returns a void pointer which indicates that it is a pointer to an unknown data type.

```
void free(void * p)
```

Free releases a block of memory previously allocated with malloc, calloc, or realloc.

---

1. Explain the following terms: virtual memory, page fault, thrashing
2. What is a Branch Target buffer? Explain how it can be used in reducing bubble cycles in cases of branch misprediction
3. Describe direct memory access (DMA) Can a user level buffer / pointer be used by kernel or drivers?
4. Write a step by step execution of things that happen after a user presses a key on the keyboard Use as much detail as possible
5. Write a program to find whether a machine is big endian or little endian
6. Discuss how would you make sure that a process doesn't access an unauthorized part of the stack
7. What are the best practices to prevent reverse engineering of DLLs?
8. Write an aligned malloc & free function that takes number of bytes and aligned byte (which is always power of 2)

   EXAMPLE

   `align_malloc(1000,128)` will return a memory address that is a multiple of 128 and that points to memory of size 1000 bytes

   `aligned_free()` will free memory allocated by `align_malloc`

OSI 7 Layer Model

Networking architecture can be divided into seven layers. Each layer provides services to the layer above it and receives services from the layer below it.
The seven layers, from top to bottom, are:

OSI 7 Layer Model	
Level 7	Application
Level 6	Presentation
Level 5	Session
Level 4	Transport
Level 3	Network
Level 2	Data Link
Level 1	Physical

---

1. Explain what happens, step by step, after you type a URL into a browser. Use as much detail as possible.
2. Explain any common routing protocol in detail For example: BGP, OSPF, RIP
3. Compare and contrast the IPv4 and IPv6 protocols.
4. What is a network / subnet mask? Explain how host A sends a message / packet to host B when: (a) both are on same network and (b) both are on different networks Explain which layer makes the routing decision and how.
5. What are the differences between TCP and UDP? Explain how TCP handles reliable delivery (explain ACK mechanism), flow control (explain TCP sender's / receiver's window) and congestion control.