REMOTE CONTROL SYSTEM

GALILEO

THE HACKING SUITE FOR GOVERNMENTAL INTERCEPTION

Trainings

]HackingTeam[

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.

Document Approval

Revision	Author(s)	Release Date
1.0	FAE Team	June 2014

Table Of Contents

1 Why you need training

In an age of constant increase of cyber-crime activities, you need to keep the pace. It is increasingly necessary to constantly deepen and broaden your understanding of the techniques used for attacking and defending, as those are the same technique that you have to apply to keep the world a safe place.

HackingTeam offers a suite of training courses at all levels, from the basics of networks and operating systems to advanced exploitation of software vulnerabilities. You can select the courses that you deem more useful or ask for custom training to be designed especially for you.

Our instructors are experts in their field, with a solid background and real-life experience. You will confront yourself with people that apply every day the topics they teach.

All of the courses lean toward **giving practical knowledge and working experience**, with many hours spent on simulations, hands-on exercises and challenges.

2 The Courses

In this section we present the courses we offer, explaining the scope and target of each course and to what type of audience they are intended for.

2.1 HT101: Network Penetration Testing

Level: Intermediate
Duration: 5 days
Prerequisites: Basic knowledge of networking

In this course you learn the elements necessary to gain access to an infrastructure, attack its Internet-facing elements and compromise wireless networks. You then move on to use different tools to identify network weaknesses, exploit them and compromise your target, to acquire critical information and maintain access, all without being noticed.

Agenda:

- Module Introduction
- Introduction to IT Security
    - The CIA Paradigm
    - Terminology
- Network Fundamentals
    - ISO/OSI Stack
    - Network Topologies
    - Network Devices
    - Network Protocols
    - DNS
- Perimeter Protections
    - VPN
    - NAC
    - Firewall
    - Intrusion Detection System (IDS)
    - Intrusion Prevention System (IPS)
- Network Penetration Testing Methodology
    - Step 1 - Planning
    - Step 2 - Verification and Scanning
    - Step 3 - Exploitation
    - Step 4 - Data Collection
    - Step 5 - Maintaining Access
    - Step 6 - Covering Tracks
- Accessing the Infrastructure
    - Internet-facing Targets
    - Attacking the Local Network
    - Attacking the Wireless Network
- Network Host Intrusion
    - Services Enumeration (Step 1)
    - Vulnerability Scanning (Step 2)
    - Exploitation (Step 3)
    - Data Collection (Step 4)
    - Maintaining Access (Step 5)
    - Covering Tracks (Step 6)

2.2 HT102: Web Application Penetration Testing

Level: Intermediate
Duration: 5 days
Prerequisites: Basic knowledge of operating systems and web protocols

The course is focused on web application security, teaching you how to analyze an application, gather public information on the target site, identify vulnerabilities and exploit them, both manually and with automatic tools.

Agenda:

- Module Introduction
- Web Applications Basics
    - Introduction to Applications
    - Client-Server Model
    - Web Application Architecture
    - Web Protocols
    - Sessions and Cookies
    - Same Origin Policy
    - Encoding Basics
- Application Penetration Testing Methodology
    - Step 1 - Planning
    - Step 2 - Information Gathering
    - Step 3 - Application Enumeration
    - Step 4 - Vulnerability Identification
    - Step 5 - Exploitation
    - Step 6 - Data Collection
- Information Gathering (Step 2)
    - Virtual Hosting
    - Search Engine Hacking
- Application Enumeration (Step 3)
    - Server Banners
    - Triggering Errors
    - Default Resources
    - Third-Party Plugins
- Spidering a Web Application (Step 3)
    - Introduction
    - Entry Points
    - Static vs. Dynamic Resources
    - Comments
    - Introduction to Burp Suite Spider
- Vulnerability Identification (Step 4)
    - Automatic Approach
    - Manual Approach
- OWASP Top 10 2013
    - Introduction to OWASP
    - Introduction to OWASP Top 10
    - A01 - Injection
    - A02 - Broken Authentication and Session Management
    - A03 - Cross-Site Scripting (XSS)
    - A04 - Insecure Direct Object References
    - A05 - Security Misconfiguration
    - A06 - Sensitive Data Exposure
    - A07 - Missing Function Level Access Control
    - A08 - Cross-Site Request Forgery (CSRF)
    - A09 - Using Components with Known Vulnerabilities
    - A10 - Invalidated Redirects and Forwards
- Web Application CTF

- Students will be challenged with a series of custom web application affected by real-world security issues
- During the CTF the students will be asked to impersonate a cyber cops team involved in the investigation of a criminal network

2.3 HT103: Reverse Engineering

Level: Intermediate/Advanced
Duration: 4 days
Prerequisites: Advanced knowledge of operating systems and basic understanding of software development and object oriented programming

The course gives you the foundation on reverse-engineering techniques and tools, showing a variety of systems and network monitoring utilities, a disassembler, a debugger and others, that are essential in understanding the inner working of the software under analysis. You also learn how to understand key characteristics of a malware sample found during the examination.

Agenda:

- Reverse Engineering Fundamentals
  - Windows Fundamentals
  - ASM description with 2 syntaxes : AT&T and Intel
  - Examples of instructions and how they work (mov, sum, int etc.)
  - Calling Convention
- Building an analysis environment (LAB)
  - A description of the provided VM and tools will be provided
  - Take a snapshot of the clean machine
- Forensics Methods and Techniques
  - Basic forensic procedures to get evidence of malware
  - How to analyze the collected evidence
- Network Traffic Analysis
  - Common protocols overview (TCP/UDP/HTTP/DNS)
  - Malware communicates with the rest of the world (e.g., Zeus)
- Memory Analysis
  - How malwares hide secrets (password, IP address, key, etc..)
  - How to leak and reuse secrets with memory analysis
- Carving executables out of RAM (LAB)
- Static Analysis
  - Static Analysis definition
  - LABs on Static Analysis
- Dynamic Analysis
  - Dynamic Analysis definition
  - Resume of everything with a guideline on how things should be done
- Dealing with Anti Reversing, Code Obfuscation and Encryption
  - Overview on different techniques
  - What to do when the code is obfuscated
  - Detection of the debugger

2.4 HT104: Vulnerability Detection and Exploitation

Level: Intermediate/Advanced
Duration: 4 days
Prerequisites: Advanced knowledge of operating systems and basic understanding of software development, object oriented programming and modern computer architectures.
Preparatory courses: HT103

Starting from topics taught in HT102, this course teaches how to audit software, dissect an application, discover security vulnerabilities and assess their level of danger. You run vulnerability scans and observe exploits to understand how to better secure networks, servers and workstations. The course is aimed at professionals involved in securing enterprise systems: network and system administrators, computer security personnel, officers with direct involvement in security and those involved in cyber security measures and implementation.

Agenda:

- Exploitation Techniques Fundamentals
  - A set of categories of software's vulnerabilities
- Public Vulnerabilities & 0-Days
  - Vulnerability Definition
  - Public and Private Vulnerabilities
  - Exploits
- Fuzzing bugs - how to write a simple fuzzer
  - The history of fuzz testing
  - What "to fuzz" means
  - Even a dumb fuzzer can give you a crash
  - How to create a fuzzer
  - Let's write a fuzzer
- OWASP Top 10 2013
  - Top 10 is a "concept" that can be extended to other contexts (e.g., mobile, cloud)
  - Security issues related to web application and technologies
  - Risk definition and adopted methodology
- Source code auditing
  - What source code auditing is?
  - Manual vs automated review
- Client-side vs Server-side attacks
  - Defining Server-side attacks
  - Defining client-side attacks
- Mobile Vulnerabilities and Weakness
  - OWASP TOP 10 for Mobile 2014
- Modify Exploit Code
  - Not always an exploit works out-of-the-box
- Web Application Exploit Development
  - Why exploiting web applications
  - Framework methods to develop a professional web exploit

2.5 HT201: Advanced Wireless Penetration Testing

Level: Intermediate
Duration: 4 days
Prerequisites: Basic knowledge of networking and operating systems. It is necessary to have a deep understanding of topics taught in HT101 before approaching this course

HT105 gives students a deep technical understanding of the security of WiFi networks. The students learn how to audit modern wireless networks for security vulnerabilities, and understand the best practices to set up a secure wireless environment along with an in-depth knowledge of WiFi protocols and features.

Agenda:

- Wireless Technology Introduction
  - Introduction
  - The 802.11 standard
  - WEP
  - WPA/WPA2 Personal
  - WPA/WPA2 Enterprise
  - WPS (PIN & Push-to-Connect)
- Wireless Infrastructure Penetration Testing
  - High-level methodology
  - Tools and hardware
  - Identify legitimate and rogue APs
  - Mapping the signal coverage on Google Earth
  - Encryption protocol evaluation
  - Identifying attack locations
- Basic Wireless Attacks
  - LAB – Wi-Fi identification
  - LAB – Sniffing Wi-Fi traffic (Open & Encrypted)
  - LAB – Brute-forcing WPS PIN
- Cracking Wireless Encryption Protocol
  - LAB - Attacking the WEP protocol
  - LAB - Attacking the WPA-Personal protocol
  - LAB - Attacking the WPA2-Personal protocol
- Attacking Public Hotspots
  - Introduction to Captive Portal
  - Attacking Hotel's AP and corporate guest network
- Client Attacks
  - Offline attacks (key recovery methods, direct access to the device)
  - LAB - Client attacks
- Enterprise Wireless Technology
  - Introduction to WPA Enterprise
  - Standard Enterprise Protocols
  - Enterprise Wireless Vulnerabilities
  - LAB – Attacking Enterprise Wireless Technologies

2.6 HT202: IT Intrusion – Desktop & Mobile

Level: Intermediate/Advanced
Duration: 4 days
Prerequisites: Advanced knowledge of Networking and Operating Systems

The ultimate goal when compromising security of desktop and mobile devices is to gain access to secret and valuable information without making the victim aware of it. This course will give you the information and methodology to gather information about targets, gaining access to target infrastructure, detecting vulnerable services and guiding you through the process of exploiting them in order to access target hosts.

Agenda:

- Preliminary topics recap
  - Network fundamentals
  - Wireless fundamentals
  - Common perimeter protection
  - Web application fundamentals
  - Vulnerabilities and exploits
- Testing Methodology Overview
  - Step 1 – Planning and Reconnaissance
  - Step 2 – Verification and Scanning
  - Step 3 – Exploitation
  - Step 4 – Data Collection
  - Step 5 – Maintaining Access
  - Step 6 – Covering Tracks
- Obtaining access the target's infrastructure
  - Attacking internet-facing targets
  - Attacking local network
  - Attacking wireless network
- Server-Side Attacks
  - Network PT vs. Web Application PT
  - Network Penetration Test
  - Network Host Intrusion
  - Web Application Penetration Test
- Client-Side Attacks
  - Attacking a Workstation
  - Attacking a Mobile Device