

]Hacking**Team**[

Remote Control System Training Schedules

Schedule 1 (mandatory)	<i>Welcome and introduction</i>	<ul style="list-style-type: none"> ○ Field of application (active interception, spyware based interception systems), ○ Core concepts (Da Vinci client-server model, Da Vinci interaction diagrams, System Actors) ○ Architectural model (block diagram, processes)
	<i>Console basics</i>	<ul style="list-style-type: none"> ○ Navigation and Buttons ○ Recent Items ○ Quick Launch Buttons ○ Basic configurations ○ Search forms
	<i>Architecture</i>	<ul style="list-style-type: none"> ○ Core components (collectors, master db server, shard db servers, consoles) ○ Network components (Network Injectors, Anonymizers), ○ Additional modules (Alerting system, RMI modems) ○ Running processes and data flow model

Schedule 2 (mandatory)	<i>Operation & User Management</i>	<ul style="list-style-type: none"> ○ Lesson: Accounting: Operations, Groups, Users, Targets, Agents ○ Lesson: Administrators, System Admins, Technicians, Analysts ○ Hands-on: Accounting ,Operation, Auditing
	<i>Agents Factory : creating and configuring Da Vinci agents</i>	<ul style="list-style-type: none"> ○ Lesson: What to know before: Consciousness and Awareness of Intention ○ Hands-on: Basic configuration ○ Lesson: Event driven logic and how to approach ○ Hands-on: Advanced Configuration: Events, Actions, Modules ○ Things you should never do
	<i>Application building (cross Platform)</i>	<ul style="list-style-type: none"> ○ Windows Executable ○ Mac Application ○ Blackberry's COD ○ Iphone's App ○ Android's APK ○ Windows Mobile's CAB ○ Symbian's SYS
	<i>Evidence analysis</i>	<ul style="list-style-type: none"> ○ Browsing and marking evidences ○ The dashboard ○ Filtering ○ Exporting

Schedule 3 – Infection Vectors (based on what purchased)	<i>Native Applications</i>	<ul style="list-style-type: none"> ○ Melting with native applications ○ Optional modules
	<i>Offline tools</i>	<ul style="list-style-type: none"> ○ Bootable CD ○ Bootable USB ○ U3
	<i>Mobile Infection</i>	<ul style="list-style-type: none"> ○ SD Card Infection ○ Infection from PC ○ QR Code
	<i>Infection Module</i>	<ul style="list-style-type: none"> ○ Local users ○ USB Drives ○ VMWare virtual machines
	<i>Exploits</i>	<ul style="list-style-type: none"> ○ Using social exploits ○ Leveraging on Zeroday exploits
	<i>Remote Mobile Infection</i>	<ul style="list-style-type: none"> ○ Wap Push messages ○ Service Loading ○ Service Indication

Schedule 4 – Network Injector	<i>Installation</i>	<ul style="list-style-type: none"> ○ Appliance Injector ○ Tactical Injector ○ Update
	<i>WiFi Options</i>	<ul style="list-style-type: none"> ○ Cracking capabilities
	<i>Target Recognition</i>	<ul style="list-style-type: none"> ○ IP Address ○ RADIUS ○ DHCP ○ String matching
	<i>Resource Infection</i>	<ul style="list-style-type: none"> ○ Identifying the resource to infect
	<i>Infection Types</i>	<ul style="list-style-type: none"> ○ Downloaded Application ○ Web page injection ○ Fake upgrade

Schedule 5 – System	<i>Network setup</i>	<ul style="list-style-type: none"> ○ Frontend ○ Backend
	<i>Anonymizers</i>	<ul style="list-style-type: none"> ○ Installation ○ Configuration ○ Upgrade
	<i>Monitoring</i>	<ul style="list-style-type: none"> ○ System Health
	<i>Backup</i>	<ul style="list-style-type: none"> ○ Scheduling ○ Restoring
	<i>Troubleshooting</i>	<ul style="list-style-type: none"> ○ Audit logs ○ Application logs ○ System logs ○ Script usage

HowTos	<i>Obtaining a bootable USB drive</i>
	<i>Symbian Signing</i>
	<i>Delivering on Iphone</i>