Full-Force Red Team Training

**Overview**

Penetration Testing, Social Engineering and Physical Intrusion for the first time ever in a training program. From the team who brought you, [*“Hacking the Grid*](https://youtu.be/pL9q2lOZ1Fw)*”*

For the first time ever, there is a training course that is more like an actual live Red Team Operation. The training converges Physical Infiltration/Security, Social Engineering and Penetration testing for full-training exercises with students breaking into actual offices/buildings (legally, of course), hacking systems/apps, and social engineering real people, face to face. There are no actors and there is no other information security training like this today.

The goal of the training is to immerse the student in as much of a real Red Team Operation as possible. Soup to nuts, the instructors will guide students as they undergo a full-cycle Red Team Operation from the planning phase to the reporting phase. At every step, Red Team’s experiences, techniques, tactics and procedures will be integrated and make up the core foundation of the entire course.

**Full-Training Exercises**

* Covertly break into a target office and plant a hardware backdoor on LAN
* Clone an RFID badge from a specified target in a public area
* Exploit system vulnerabilities on target's network
* Use telephone social engineering to acquire information from a target and more…

**Sampling of Tools**

* Lock picks, Shove-it, Under Door Tool
* Bump Keys, Practice Locks
* USB Rubber Ducky, LAN Turtle, LAN Star
* RFID Card Cloner
* Kali Linux Tools, Metasploit, PyPhishing, etc.
* PlugBot on Raspberry Pi

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **What You Will Learn** | |  | **What You Will Do** | |
|  |  |  |  |  |  |
|  | Full-cycle Red Teaming from |  |  | Full-Training Exercises (FTX) |  |
|  | Operational Planning to Reporting |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  | |
|  | How to converge Technical, Physical and | |  | Plan, execute and report on a full-training | |
|  |  | Red Team Operation | |
|  | Social Engineering vulnerabilities | |  |
|  |  |  |  |
|  |  |  |  |  | |
|  | Covert and overt methods of entry into |  |  | Conduct target reconnaissance both offline |  |
|  |  |  | and online |  |
|  | a target location |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | Social engineering tactics, from | |  | Clone RFID badges, pick locks, steal keys | |
|  |  | and/or bypass physical security controls | |
|  | telephone to face-to-face | |  |
|  |  |  |  |
|  |  |  |  |  | |
|  |  |  |  | Exploit network and application |  |
|  | Physical security scouting and recon |  |  | vulnerabilities on target network |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | Penetration testing for Red Team | |  | Make overt and covert entry into a target | |
|  | Operations | |  | location and establish APT persistence | |
|  |  |  |  |  |  |

Red Team Security has developed a unique training program that includes paid, but unknowing participants, as real-life targets. The students will exercise their newly acquired skills and tactics by carrying out social engineering attacks in-person, by phone and over email. Covert entry skills and other physical security attacks (i.e., lock picking, evasion, diversions, physical pretexting) are simulated against surrounding and cooperating offices and/or buildings.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Day 1**  **Overview,**  **Planning &** **Mission**  **Delivery** | **Day 2**  **Technical Attacks & Execution** | **Day 3**  **Social Attacks &**  **Execution** | **Day 4**  **Physical Attacks &**  **Execution** | **Day 5**  **Remediation, Reporting** **& Presentation** |
| **Red Team Scoping,**  **Planning & Execution** | **Penetration Testing for Red Team Operations** | **Social Engineering**  **Pretexting & Execution** | **Physical Security Infill** **Planning & Execution** | **Report Development &**  **Delivery** |
| Course introduction and overview   * Red team methodology * Scoping for red team operations * Red team operations resource planning and roles * Red team operations execution * Inter-team communications * Client communication and evidence management * Training mission assignment * Team break out * Ready the technical environment * Introduction to Penetration Testing for Red Team Operations | * Introduction (cont.) * Testing methodology and objectives * Tools * Passive/active Info gathering * Vulnerability analysis * Exploitation, pivoting and post-exploitation * Sensitive data collection for red team operations * Crafting attack plans for adjacent attack surfaces * Exploit systems/app in the lab of various complexities | * Introduction to SE * Information gathering * Influencing tactics * Elicitation techniques * Pretexting * SE methods of delivery (email, telephone, physical) * Campaign planning and metrics * Props and costumes * SE tools * Spear phish targets for intel * Telephone phish targets for intel * Clone badges from target people to be used for Day 4 | * Introduction * Online, long-range and short-range recon tactics * Identification of physical security controls * Camera/IDS evasion and bypass * Lock picking * Physical bypass and entry tools * Covert and overt entry tactics, planning and execution * Pick locks and bypass physical security controls * Execute a covert physical intrusion on real office | * Technical writing for red team operation reports * Remediation development * Presentation techniques * Create the red team operation report * Present the findings report to the panel |

# **Objectives & Approach**

We’ve meticulously crafted a training simulation unlike any other, that mirrors a full Red Team Operation as close to real life as possible- lifted from our own professional exploits ( [**Link**](https://youtu.be/pL9q2lOZ1Fw?__hstc=213954056.e794bfa0934a98641af8454cf7bb0ffb.1486660510520.1488988302272.1489002673570.101&__hssc=213954056.4.1489002673570&__hsfp=3807016949) **1**,  [**Link**](https://youtu.be/r0jBLzmrH9w?__hstc=213954056.e794bfa0934a98641af8454cf7bb0ffb.1486660510520.1488988302272.1489002673570.101&__hssc=213954056.4.1489002673570&__hsfp=3807016949) **2**,  [**Link**](https://youtu.be/cxxnuofREcM?__hstc=213954056.e794bfa0934a98641af8454cf7bb0ffb.1486660510520.1488988302272.1489002673570.101&__hssc=213954056.4.1489002673570&__hsfp=3807016949) **3**,  [**Link**](https://youtu.be/YIV0xvatX0M?__hstc=213954056.e794bfa0934a98641af8454cf7bb0ffb.1486660510520.1488988302272.1489002673570.101&__hssc=213954056.4.1489002673570&__hsfp=3807016949) **4**,  [**Link**](http://www.businessinsider.com/red-team-security-hacking-power-company-2016-4?__hstc=213954056.e794bfa0934a98641af8454cf7bb0ffb.1486660510520.1488988302272.1489002673570.101&__hssc=213954056.4.1489002673570&__hsfp=3807016949) **5**,  [**Link**](http://www.businessinsider.com/red-team-security-hacking-power-company-2016-4) **6**). The training simulation centers around a (fake) target company complete with employee profiles, phone numbers, email addresses, social media accounts, real human targets and actual physical offices. The students’ goal is to put their knowledge into action by performing a simulated Red Team Operation to identify and compromise the target company via three (3) domains: **Technical**, **Social** and **Physical**.

Successful completion of one domain, in a capture-the-flag themed approach, will provide enough information to advance to the next domain. If students successfully reach the final domain, Physical, they must covertly break into a secure office and act quickly to solve physical security challenges to achieve physical access to the final objective.

****