Full-Force Red Team Training

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
- and more...

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"*

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, RedTeam's experiences, techniques, tactics and procedures will be integrated and make up the core foundation of the entire course.

Lots of FREE gear, taught by a great experienced team. Register here now!

Full-Force Red Team Training

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

RedTeam 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 (ie: lock picking, evasion, diversions, physical pretexting) are simulated against surrounding and cooperating offices and/or buildings.

For more information, please email us at: training@redteamsecure.com

Full-Force Red Team Training

Day 1
Overview, Planning & Mission Delivery

Red Team Scoping, Planning & Execution

- 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

Day 2
Technical Attacks & Execution

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

Full-Training Exercise(s)

- Exploit systems/apps in the lab of various complexities
- Acquire sensitive information (flags) to be leveraged for Day 3 and Day 4 exercises

Day 3
Social Attacks & Execution

Social Engineering Pretexting & Execution

- 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

Full-Training Exercise(s)

- Spear phish targets for intel
- Telephone phish targets for intel
- Clone badges from target people to be used for Day 4

Day 4
Physical Attacks & Execution

Physical Security Infil Planning & Execution

- 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

Full-Training Exercise(s)

- Pick locks and bypass physical security controls
- Execute a covert physical intrusion on real office

Day 5
Remediation, Reporting & Presentation

Report Development & Delivery – Half Day

- Technical writing for red team operation reports
- Remediation development
- Presentation techniques

Full-Training Exercise(s)

- 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 1, Link 2, Link 3, Link 4, Link 5, Link 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 in an effort 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 in order to achieve physical access to the final objective.