Red Team Exercises

Overview

This course will teach Red Team Exercises - theory and practice

Audience

Hackers, Attackers

Skill Level

Introductory - Intermediate

Duration

Five days

Format

Lectures and hands on labs. (50% 50%)

Prerequisites

- Recommended: Cybersecurity awareness
- Nice to have: Comfortable in Linux environment (be able to navigate Linux command line, run commands)

Lab environment

- Zero Install: There is no need to install software on students' machines!
- A lab environment in the cloud will be provided for students.

Students will need the following

- A reasonably modern laptop with unrestricted connection to the Internet. Laptops with overly restrictive VPNs or firewalls may not work properly
- Chrome browser
- SSH client for your platform

Detailed outline

Red Teams in Cyberspace

- Why Human Hackers

- Innovation and Automation
- Modeling Technology
- Nonpivot Technology
- Pivoting and Exploiting Technology
- Automation Advantages and Disadvantages
- Example Scenarios
- Threat Hunting

The State of Modern Offensive Security

- The Challenge of Advanced Persistent Threats
- No Rules of Engagement
- Environmental Challenges
- Regulatory Standards
- Adversarial Customers
- Technical Personnel
- Effective Red Team Staffing

Shaping

- Who
  - Customer Technical Personnel
  - Customer Operational Personnel
  - Provider Technical Personnel
  - Provider Operational Personnel
- When
  - Preventing Incidents
  - Balancing Scope Attributes
- What
  - Motivation of the Assessment
  - Prior Testing
  - Existing Security
  - Scope Footprint
  - Inorganic Constraints

Rules of Engagement

- Activity Types
- Physical
- Social Engineering
- External Network
- Internal Network

- Pivoting
- Wireless Network
- Category
- Escalation of Force
- Incident Handling
- Tools
- Certification Requirements
- Personnel Information

Reporting

- Necessary Inclusions
- Types of Findings
- Exploited Vulnerabilities
- Nonexploited Vulnerabilities
- Technical Vulnerabilities
- Nontechnical Vulnerabilities
- Documenting Findings
- Findings Summaries
- Individual Findings
- Briefing
- The No-Results Assessment

What is Next?