Blue Team Exercises

Overview

As reports of major data breaches continue to fill the headlines, it has become impossible for any business, large or small, to ignore the importance of cybersecurity.

This course strikes the perfect balance of theory and practice. making it equally useful to those in IT or management positions across a variety of industries. It takes a simple and strategic look at best practices and tools available to both cybersecurity management and hands-on professionals, whether they be new to the field or looking to expand their expertise.

Audience

Security professionals, penetration testers, developers looking to secure their code

Skill Level

Intermediate to advanced

Duration

Five days

Format

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

Prerequisites

- Recommended: Cybersecurity awareness, IT Security experience
- Nice to have: Linux command line experience, common TCP/IP network protocols

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

Fundamental Networking and Security Tools

- Ping
- IPConfig
- NSLookup
- Tracert
- NetStat
- PuTTY

Troubleshooting Microsoft Windows

- RELI
- PSR
- PathPing
- MTR
- Sysinternals
- The Legendary God Mode

Nmap—The Network Mapper

- Network Mapping
- Port Scanning
- Services Running
- Operating Systems
- Zenmap

Vulnerability Management

- Managing Vulnerabilities
- OpenVAS
- Nexpose Community

Monitoring with OSSEC

- Log-Based Intrusion Detection Systems
- Agents
- Log Analysis

Protecting Wireless Communication

- 802.11
- inSSIDer
- Wireless Network Watcher
- Hamachi
- Tor

Wireshark

- Wireshark
- OSI Model
- Capture
- Filters and Colors
- Inspection

Access Management

- AAA
- Least Privilege
- Single Sign-On
- JumpCloud

Managing Logs

- Windows Event Viewer
- Windows PowerShell
- BareTail
- Syslog
- SolarWinds Kiwi

Metasploit

- Reconnaissance
- Installation
- Gaining Access
- Metasploitable2
- Vulnerable Web Services
- Meterpreter

Web Application Security

- Web Development
- Information Gathering
- DNS
- Defense in Depth
- Burp Suite

Patch and Configuration Management

- Patch Management
- Configuration Management
- Clonezilla Live

Securing OSI Layer 8

- Human Nature

- Human Attacks
- Education
- The Social Engineer Toolkit

Kali Linux

- Virtualization
- Optimizing Kali Linux
- Using Kali Linux Tools

CISv7 Controls and Best Practices

- CIS Basic Controls—The Top Six

What's Next?