INTRODUCTION
TO CYBER WARFARE

Overview

When exactly did information security become cyber warfare? What changed? How do modern attacks against information systems differ from what hacking was 5-10 years ago? Old defence doctrines are ineffective against modern APT-like scenarios. Successful attacks are no longer measured by whether the perimeter was breached. The student learns to understand that the breach is inevitable and true defences are organic, highly iterative, mixed approached and heavily dependent on human resource. Effective security operations have to correspond to the modern kill-chain, so before security can be implemented, specific attack scenarios should be carefully examined. The student will understand the concepts of reactive vs. proactive security.

What you will learn:

- What is cyber and the digital universe?
- What is denial of service and how it is performed?
- How is information gathering performed?
- How to gain privileges (with brute-forcing and without)?
- How to inject code into interpreted context?
- How to exploit vulnerable code?
- Security truisms
- What are blacklists and how are they implemented?
- What are whitelists and how are they implemented?
- How to improve authentication mechanisms?
- How to better manage your current assets?
- How to create baselines and detect anomalies?
- How to use and improve the human factor?
- What are APTs?
- What is the anatomy of a modern breach?
- How do mitigation strategies compare?
- How is security a process?
- What is security by design?

Who should be attending?

Our public course targets entry level participants – no prior technical knowledge is required: sales, pre-sales, customer support, product, business development and management personnel.

This course can also be adapted for junior level technically-oriented audiences with prior technical experience: IT, NOC, SOC, Dev-ops, SW developers, SW QA, and others with technical skills.

This option is available only for groups or organizations ordering this course as tailor made.

Prerequisites

- **Entry level (Public course):** Technical/scientific mind-set, very good English (reading), search skills (google).
- **Junior level (Tailor made course, for groups/organizations only):** MS technologies, Networking (TCP/IP), Linux/Unix OS & Shell.

Course Contents

Part 1: Threat Landscape

- **Agenda etc.**

- **What is cyber and the digital universe**

- **Damage 1: denying service**
  - Flooding
  - Spoofing
  - Protocol malformations
  - Reflections and amplifications

- **Damage 2: information gathering**
  - Scanning, fingerprinting and enumeration
  - Manual vs. Automated spidering
  - Credential harvesting
  - Resource mapping
  - Error based information disclosure

- **Damage 3: gaining privileges**
    - Brute-force logins and passwords
    - Password hashes and password dictionaries
    - Custom dictionaries and password complexity
    - Bypass authentication mechanisms
    - Bypass session management
    - Bypass OS user and fs permissions
    - Bypass security software

- **Damage 4: injecting code**
    - cmd OS injections
    - data-store injections
    - file injections (XML, json, etc)
    - remote file and resource inclusion
    - injecting web clients (browsers)
    - injecting client applications (office, pdf, etc)

- **Damage 5: binary exploitation**
    - Buffer, stack and heap overflows
    - Browser and plugin exploitation
    - Memory corruptions
    - Code execution

Part-2: Mitigation strategies

- **What is defence all about**

- **Mitigation 1: blacklists**

  - IP blacklists
  - Anti-malware defences
  - URL filtering (... and ad blocking too)
  - Block mail SPAM and spoofs
  - Application firewalls (proxies and reverse-proxies, WAFs, DB-fw)
  - IDS/IPS/HIPS

- **Mitigation 2: whitelists**

  - NAC
  - Firewalls and access-lists
  - Application whitelisting
  - Application firewalls (positive proxies and reverse-proxies)
  - Web content filtering (WAFs and application-layer filtering)

- **Mitigation 3: better authentication**

  - strong passphrases
  - certificates
  - cryptography
  - multi-factor authentication
  - permissions and the 'need to know' rule
  - admins (locale & domain) and roots
  - audit

- **Mitigation 4: manage your assets**

    - patch operating systems and applications
    - perform vulnerability scans
    - harden OS and application configurations
    - maintain a 'master' system image bank
    - backup and disaster recovery
    - keep detailed logs and network traffic captures

- **Mitigation 5: misbehave is the new malware**

    - New rule: do not block
    - Sandboxes and dynamic analysis
    - Honeypots and decoys
    - Exploit mitigation tools
    - Centralized log collection and analysis (aka SIEM)
    - Network/host-based anomaly detection
    - Heuristic A/V and HIPS

- **Mitigation 6: it's all about the people**

    - New profession: security analyst
    - User education
    - Skill assessment and training (of security teams)
    - Secure coding for developers
    - Penetration test

Part-3: Putting it all together (optional)

- Worst case scenarios (APT breach case study)
- APT kill-chains
- Security truisms
- Mitigation strategies compared (ASD mitigations)
- Security as a process (SANS 20 CSC)
- What is security by design?
- Final project: Security by design

Your first step into the Cyber Security Community.

Next Course