SecureNinja
The Cybersecurity Experts

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Advanced Systems & Applications Attack & Defense

COURSE DESCRIPTION

SecureNinja's (5) five-day Advanced Systems & Applications Attack & Defense boot camp was created for Network/Web Application Penetration testers that are looking for the little tips and tricks that will help them better attack high-security environments. Students that are Network/System Administrators with three or more years' experience working in environments such as financial institutions, DoD networks, or similar high-security environments will benefit greatly from this course. You choose the delivery format. Either in one of our public training centers or Live Online from work or your home computer.

TOPICS COVERED

- Attacking From the Outside
- Bypassing Anti-Virus & HIPS
- DLL Injection & Process Injection
- Advanced Post-Exploitation
- Capture the Flag Team Hacking

WHO WOULD BENEFIT

IT System Administrators, IT Security Professionals, Windows Developers

PREREQUISITES

Familiarity with Windows System Administration, familiarity with programming

COURSE LENGTH

- 5 Days

FOLLOW ON COURSES

- Cyber War
- Hands-on Malware Analysis
- Hands-on Mobile Application Security

COURSE DETAILS

Day 1: Attacking From the Outside

- Attacking Hardened Web Applications
    - Advanced Methods of identifying SQLI/XSS
- Bypassing Common Web Application Security Mechanisms
    - Client-Side Filtering
    - Alphanumeric Filtering

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

    - Magic Quotes
    - ASP.NET Request Validate
- Bypassing Common Security Products
    - IDS Signature Evasion
    - Dealing with Web Application Firewalls

Day 1's Mission:
Attack a mock company's heavily protected external web applications from the outside

Day 2: Bypassing Anti-Virus & HIPS

- Bypassing Popular Anti-Virus
    - AVG
    - McAfee
    - Symantec
    - Windows Defender

- Bypassing Popular HIPS
    - McAfee HIPS
    - Symantec Endpoint Protection
    - Forefront

Day 2's Mission: Bypass the most common host-based security products

Day 3: DLL Injection & Process Injection

- DLL Injection
    - Advanced Post-Exploitation
    - Data-Mining

- Process Injection
    - Advanced Network Enumeration
    - Data-Mining 2008 Active Directory with security settings enabled

Day 3's Mission: Bypass Group Policy Objects, Software Restriction Policy, and HIPS

Day 4: Advanced Post-Exploitation

- Attacking Windows 7
    - Advanced Post-Exploitation
    - Data-Mining

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Attacking 2008 Active Directory
    - Advanced Network Enumeration
    - Data-Mining 2008 Active Directory with security settings enabled

Day 4’s Mission: Finding all of a company's intellectual property and stealing it

Day 5: Mother of All Capture the Flags

- Putting everything together in a team hacking competition