11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

Defending Your Systems & Networks When Attacked

(Customized Course)

DAY ONE

- Introduction to Network Defense
- Security Model
  - Authentication
  - Confidentiality
  - Integrity
  - Availability
  - Authorization

LAB: Security Model

- Security Posture
  - Promiscuous
  - Paranoid
  - Permissive
  - Prudent
- Risk management
- Risk Assessment
  - Information Security Policy
  - Information Security Management
- Pre-assessment
- Assessment
- Post-assessment
  Defining types of risk
- Security policy
  - Identifying services and allowing them

LAB: Allowing a Service

- TCP/IP 101
  - Introduction and Overview
    Introducing TCP/IP networks
  - What TCP/IP provides: key application services and multivendor capabilities TCP/IP and the Internet
  - Internet RFCs and STDs
  - TCP/IP protocol architecture
  - Protocol layering concepts
  - TCP/IP layering
  - Components of TCP/IP networks

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

LAB: TCP/IP
DAY TWO

- Network protocols
  - IP
  - TCP
  - UDP
  - ICMP

LAB: Network Protocols

- Review of the hacking process
  - Hacking methodology
    - Surveillance
    - Footprinting
    - Scanning
    - Vulnerability assessment
    - Exploitation
    - Covering tracks
    - Evasion

LAB: Hacking Review

- Defining vulnerability
- Need for vulnerability assessment
- Challenges of vulnerability assessment
- System vulnerabilities
- Desktop vulnerabilities
  - Browsers
  - Client applications
- Interpreting advisory notices
- CVE
- Vulnerability sites
  - Responsible disclosure
  - Full disclosure
- Lifecycle of a vulnerability and exploit
- Challenges of zero-day vulnerability
- Exploitation of a vulnerability
- Vulnerability scanners
  - Strengths and weaknesses of a vulnerability scanner
  - Scanning methods

LAB: Vulnerability Assessment

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

DAY THREE

- Perimeter configuration and security
  - Router hardening
  - Turning off services not required
  - Routing protocol weaknesses
    - Router packet filtering (stateless)
      - Sanity Checking
        - Ingress and Egress filtering

LAB Perimeter Security

- Firewall Deployment
  - Why is a firewall needed?
    - What does a firewall provide?
    - What does a firewall not provide?
  - Providing services
    - Common services
- Firewalls and the security policy
  - Firewall architecture
    - Outgoing access
    - Incoming access
    - Layered defence
    - Fortress mentality

LAB: Firewall Deployment

- Firewall Configuration
    - Four main firewall types
      - Stateless
      - Stateful
      - Circuit level gateway
      - Application proxies
      - Comparison of the firewall types
      - Advantages and disadvantages

LAB: Firewall Configuration

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

DAY FOUR

- Selecting an Operating System
  - Hardening the Operating System
    - Center for Internet Security
      - Benchmarks
  - Scanning the bastion host for vulnerabilities

LAB: Hardening the OS

- Firewall Architecture
    - Combining components to give defence in depth
    - Types
      - Classic
      - Belt and braces
      - Belt and braces with separate services subnet
    - Selecting an architecture
      - Organization requirements and needs

LAB: Firewall Architecture

- Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
  - What IDS can and cannot do
  - Types IDS
    - Network
    - Host
    - Network Node
  - Advantages of IDS
  - Limitations of IDS
  - Stealthing the IDS

  - Need for IPS
    - Types of IPS
    - Network
    - Host
  - Mechanics of how an IPS does its job
  - Effective deployment strategies of IDS and IPS
  - Detecting intrusions

LAB: Intrusion Detection and Intrusion Prevention

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

DAY FIVE

- Defending Against Web Applications and Web Servers
    - Deploying web application firewalls
    - Writing Secure Web Applications

LAB: Web Applications

- Combating the Advances in Malware
    - Live memory fornesics
    - Tools
        - Open source
        - Commercial

LAB: Malware

- Fighting the Zero Day Threat
    - Endpoint protection
    - Network access control

LAB: Endpoint Protection and NAC

- Building Secure Network Architectures
    - Balancing services with risk
    - Proven methods to secure the network
- Deploying Robust and Secure Wireless Networks
- Challenges of staying current
    - References
        - Books
        - Mailing lists
        - Videos
        - Professional organizations