HT101 - Network Vulnerability Assessment

Proactive vulnerability assessment training is the key to any organization's security posture. Constant assessment for potential weakness is required to maintain a security edge as new vulnerabilities in operating systems, software, hardware, and even human elements are identified and exploited every day. This course is designed to provide the fundamental knowledge necessary to comprehend the overall host & network security posture and the basic practices in vulnerability assessment course.

Course Agenda:

DAY 01

- **Module introduction**
  - Overview of the first day
    - Theory, tools and technologies as a starting point
    - Students must have a clear idea of what we'll teach during the day
- **IT Security**
  - Abstract
    - CIA triad
- **Terminology**
  - Security Assessment Typologies and Objectives
    - Different technologies but the same goals
    - The role of the security assessments in a modern organizations
  - Vulnerability Assessment (VA)
  - Penetration Testing (PT)
- **Network Fundamentals**
  - ISO/OSI stack
  - Network Topologies
    - Bus Topology
    - Star Topology
    - Ring Topology
    - Tree Topology
    - Mesh Topology
  - Network Devices
    - Repeater/Hub
    - Bridge/Switch
    - Router
  - TCP/IP
    - IP protocol
      - **LAB - IP packet analysis with WireShark (IP_TCP_HTTP.pcapng)**
    - TCP
      - **LAB - 3-way-handshake analysis with WireShark (IP_TCP_HTTP.pcapng)**
    - UDP
      - **LAB - UDP packet analysis with WireShark (IP_UDP.pcapng)**

        - **LAB - introduction to network traffic sniffing**
            - How to set up and run WireShark sniffer
            - How to intercept network traffic
            - How to filter network packets
        - **LAB - packets forging with Scapy**
            - Introduction to the Scapy framework
            - How to forge IP and TCP packets
    - Routing
        - Basics of Routing
        - Static Routing
        - Dynamic Routing
        - **LAB - Routing table**
            - Print routing table
            - Delete/add routes
            - Traceroute with different paths
- **Common Perimeter Protections**
    - VPN
    - NAC (agent and agent-less solutions)
    - Firewall
        - **LAB - introduction to firewall rules**
        - **LAB - Configuring IPTABLES with fwbuilder**
        - **LAB - The role of fw rules reviewing during a security engagement**
    - IDS
    - IPS

DAY 02

- **Recap of the previous day**
- **Module Introduction**
    - Overview of the day
- **Wireless Assessment & Weakness**
    - Standard **802.11**
    - WEP
    - WPA/WPA2
    - WPS
    - Putting all together: Wireless Architecture Vulnerability Assessment
        - Tools and hardware
        - Identify legitim APs and rogue APs
        - Mapping the signal coverage on Google Earth
        - Encryption protocol evaluation
    - **LAB - Introducing wireless network identification and encryption evaluation**
        - Introduction to Kismet
        - Traffic sniffing on a wireless network
- **Introduction to VA Methodology**
    - Defining the macro step of the proposed method
    - OSSTMM and other testing standards (cenni)

        - Il nostro è derivato , basato su esperienza
- **Step 1 - Assessment Planning**
    - Initial phases of a security assessment
- **Step 2 - Information Collection**
    - Infrastructure Information Gathering
        - Whois
            - **LAB - Whois of a domain, analyzing output to retrieve useful information**
        - DNS
        - Metadata
            - **LAB - Using FOCA to obtain corporate information**
        - SHODAN Search Engine
            - **LAB - Using SHODAN to collect target information**
- **Step 3 - Enumeration**
    - O.S. Fingerprinting and Footprinting
        - How to
        - Accuracy
        - **LAB - Information gathering via Unix command line utilities**
    - Introduction to port scanning
        - Port scanning theory (e.g., scanning typologie such as tcp connect, syn scan, etc..)
        - **LAB - NMAP help page analysis**
        - **LAB - How to specify a target or a set of targets to scan**
        - **LAB - How to select a specific or range of ports**
        - **LAB - How to select a specific port scanning technique**
        - **LAB - Understanding NMAP output**
        - **LAB - OS and services fingerprinting**
        - **LAB - How to use NMap Scripting Engine (NSE)**

DAY 03

- **Recap of the previous day**
- **Module Introduction**
    - Overview of the day
- **Step 4, part I - Testing System & Network Services**
    - Manual Services Testing and Interaction
        - System & Network services (Linux & Windows platform)
            - **LAB - Intercepting a real world FTP client session (FileZilla)**
            - **LAB - Open a telnet session and connect to both FTP and HTTP server**
        - Enterprise services
            - Microsoft (NetBios)
            - Microsoft (Active Directory)
            - **LAB - Analyzing and accessing a NETBIOS service**
    - Active System & Network Vulnerability Scanning
        - Introduction to vulnerability scanning
            - Inner workings of a vulnerability scanner
            - Commercial vulnerability scanners
            - **LAB - Introduction and scanning of a vulnerable target**
                - How to run Tenable Nessus scanner
                - How to configure a scanning policy

        - Scanning a target or a range of targets
        - Understanding and exporting the output of the scanner
    - Metasploit
        - **LAB - Running the Metasploit framework**
        - **LAB - Search and run modules**
        - **LAB - How to configure and run and exploit**
        - **LAB - Using NMAP with Metasploit**
- User Credential Gathering
    - Social Engineering
    - Brute force attacks
        - Direct brute forcing
        - Reverse brute forcing
        - **LAB - Authentication Attack with THC Hydra (SSH server)**
    - Password Guessing
    - Authentication Mechanism Attacks
        - Weak transmission
            - **LAB – Intercepting passwords with WireShark**

DAY 04

- **Recap of the previous day**
- **Module Introduction**
    - Overview of the day
- **Step 4, part II - Analysis**
    - Identify False Positive and Noise
        - Definition of false positive and false negative and why they occur
        - Defining a modus operandi in order to identify a false positive
            - **LAB - Analysis of a Nessus' plugin**
- **Step 5 - Reporting**
    - Vulnerability Impact Evaluation and Prioritization
        - Defining risk in information security
        - Risk evaluation with CVSS v.2
            - **LAB - Evaluation of Nessus findings and how to recalculate the real risk**
    - Vulnerabilities Reporting
    - Enterprise Vulnerabilities Management
- **References & Tools**