ABAIأباد
معهد شبكة أباد للتدريب
ABAD NETWORK FOR TRAINING

EJPT - JUNIOR PENETRATION TESTER

Assessment Methodologies: Information Gathering (1 Lab)
- -Introduction To Information Gathering
- -Passive Information Gathering
- -Active Information Gathering

Assessment Methodologies: Footprinting & Scanning (5 Labs)
- -Introduction
- -Mapping a Network , Port Scanning
- -Exercises
- -Challenges

Assessment Methodologies: Enumeration (18 Labs)
- -Introduction
- -Overview
- -SMB (7 Labs)
- -FTP (2 Labs)
- -SSH (2 Labs)
- -HTTP (3 Labs)
- -SQL (4 Labs)

Assessment Methodologies: Vulnerability Assessment (2 Labs)
- -Introduction
- -Vulnerability Overview
- -Vulnerability Case Studies
- -Nessus (1 Lab)
- -Vulnerability Research (1 Lab)

Assessment Methodologies: Auditing Fundamentals (No Lab)
- -Introduction
- -Auditing Fundamentals

Host & Network Penetration Testing: System/Host Based Attacks (16 Labs)
- -Introduction
- -Host Based Attacks
- -Windows Vulnerabilities
- -Exploiting Windows Vulnerabilities (5 Labs)
- -Windows Privilege Escalation (2 Labs)

-Windows File System Vulnerabilities
-Windows Credential Dumping (2 Labs)
-Linux Vulnerabilities
-Exploiting Linux Vulnerabilities (4 Labs)
-Linux Privilege Escalation (2 Labs)
-Linux Credential Dumping (1 Lab)

Host & Network Penetration Testing: Network-Based Attacks (5 Labs)
-Introduction
-Tshark
-Wifi-Security

Host & Network Penetration Testing: The Metasploit Framework (MSF) (36 Labs)
-Introduction
-Metasploit Framework Overview
-Metasploit Fundamentals
-Information Gathering & Enumeration (2 Labs)
-Enumeration (7 Labs)
-MSF Vulnerability Scanning (1 Lab)
-Nessus Vulnerability Scanning
-Web Apps (1 Lab)
-Client-Side Attacks
-Windows Exploitation (3 Labs)
-Linux Exploitation (4 Labs)
-Post Exploitation Fundamentals (2 Labs)
-Windows Post Exploitation (10 Labs)
-Linux Post Exploitation (4 Labs)
-Metasploit GUIs (2 Labs)

Host & Network Penetration Testing: Exploitation (16 Labs)
-Introduction
-Introduction To Exploitation
-Vulnerability Scanning (2 Labs)
-Searching For Exploits
-Fixing Exploits (1 Lab)
-Bind & Reverse Shells (3 Labs)
-Exploitation Frameworks (1 Lab)

ABAD NETWORK FOR TRAINING

-Windows Exploitation (5 Labs)
-Linux Exploitation (4 Labs)
-AV Evasion & Obfuscation

Host & Network Penetration Testing: Post-Exploitation (26 Labs)
-Introduction
-Post-Exploitation
-Windows Local Enumeration (5 Labs)
-Linux Local Enumeration (5 Labs)
-Transferring Files To Windows & Linux Targets (3 Labs)
-Upgrading Shells (1 Lab)
-Windows Privilege Escalation (1 Lab)
-Linux Privilege Escalation (2 Labs)
-Windows Persistence (2 Labs)
-Linux Persistence (2 Labs)
-Dumping & Cracking Windows Hashes (1 Lab)
-Dumping & Cracking Linux Hashes (1 Lab)
-Pivoting Overview (1 Lab)
-Clearing Your Tracks (2 Labs)

Host & Network Penetration Testing: Social Engineering (1 Lab)
-Introduction
-Social Engineering Overview
-Let's Go Phishing (1 Lab)

Web Application Penetration Testing: Introduction to the Web and HTTP Protocol (12 Labs)
-Introduction
-Intro to Web
-web and http protocols
-HTTP Methods
-Directory Enumeration
-Burp Suite
-Nikto , vulnerabiltiy scanning
-SQLi with SQLMap
-XSS Attack with XSSer
-Attacking HTTP Login Form