Engineers 3D

IT & ENGINEERING SERVICES

TRAINING PROJECTS PLACEMEMNTS

CYBER SECURITY SYLLUBUS

Linux Essentials For Pentesting

- -History and Features of Linux
- -Architecture of Linux OS
- -Linux Distributions
- -Linux Commands (System & Networking)
- -File Systems and its Types
- -Software Package Management
- -Users and Groups Administration
- -File/Folder Permissions
- -Special Permissions
- -Service and Process Management
- -Linux Security(PAM, SSH & SSH Security, IPTABLES and SELinux)
- -Shell Scripting Basics

Networking Essentials for Pentesting

- - Computer Networks and Types of Networks
- - Network Devices
- - Network Topologies
- - IP and MAC Address
- - OSI Model and TCP/IP Model
- - Addressing and Subnetting
- - IPv4 Packet Structure
- - Network Protocols(TCP, UDP, ICMP, ARP, RARP..)
- - IPv6 Packet Structure
- - Network Services(DNS, DHCP, SNMP, FTP, etc..)
- - Packet Analysis With Wireshark

Introduction to Cyber Security

- - What is Cyber Security?
- - Importance of Cyber Security
- - Cyber Security Domains

- - CIA Triad
- - Vulnerability, Threat and Risk
- - Risk Governance & Risk Management
- - Cyber Crime & Classification of Cyber Crimes
- - NIST Cybersecurity Framework
- - Cyber Security Compliance (GDPR,HIPAA, FISMA,SOC-1 & 2 and SOX)
- - ISO IEC 27001/ISO 27002
- - PCI-DSS
- - Industry Best Penetration Testing Standards (OWASP,WASC,SANS25, PTES, OSSTMM)
- - Case Studies

Network Security

- - Internet, Intranet, and Extranet
- - DMZ
- - DNSSEC
- - Firewalls
- - IDS and IDPS
- - VPN and tunneling
- - Network Address Translation (NAT) and PAT
- - Honeypots & Deception Technology

Vulnerability Assessment and Management

- - Fundamentals of Vulnerability Assessment and Management
- - Vulnerability Assessment Tool Deployment Strategy(Nessus, Qualys & Nexpose)
- - Scanning Methodologies
- - Authenticated vs Non-Authenticated Scanning
- - Planning and Performing Infrastructure Security Assessment
- - Web Application Vulnerability Assessment
- - Interpreting and Calculating CVSS Score
- - Risk Identification and Categorization
- - Reporting
- - Patches and Updates

Penetration Testing

- - Introduction to Penetration Testing
- - Types of Penetration Testing
- - Pentesting Services
- - Best Linux Distributions for Hacking and Penetration Testing
- - Penetration Testing Phases
- - Pre-Engagement Actions
- - OSINT
- - Threat Modeling & Vulnerability Identification
- - Exploitation (Using Metasploit & Manual, Password Cracking, Buffer Overflows, etc..)
- - Post-Exploitation (Privilege Escalation of Linux & Windows and Pivoting, etc...)
- - Reporting
- - Resolution & Re-Testing

Active Directory Attacking and Defending

- - Introduction Active Directory
- - Active Directory Setup
- - Active Directory Enumeration
- - Active Directory Attack Vectors

- - Active Directory Post Enumeration
- - Active Directory Post Attacks
- - AD Defense- Detection
- - AD Remediation
- - Kerberos Authentication

Cryptography

- - Introduction to Cryptography
- - Symmetric Ciphers
- - Asymmetric Ciphers
- - Pseudo-Random Number Generation
- - Steganography
- - Building SSL certificates
- - Digital Certificates and Digital Signatures
- - Hashes
- - Encoding

Application Penetration Testing

- - Web application Architecture and Technologies.
- - Web application offensive & Defensive
- - Information Gathering
- - Authentication & Authorization
- - Session Management
- - File Security
- - Database Security
- - Other Attacks
- - OWASP Top 10 Vulnerabilities 2017
- - OWASP Penetration Testing Check List
- - Secure Development Methodologies and Threat Modeling
- - WAF
- - Automated tools (Burpsuite,Owasp-zap, Paros Proxy, Netsparker, Charles Proxy, Webscarab)

Mobile Application & Wifi Penetration Testing

- - Android OS structure
- - IOS structure
- - Android app structure
- - Rooting Concept
- - Compromising Android os with malware
- - Communication channel Penetration Testing
- - Android app reverse engineering
- - Android app penetration testing
- - Core Concepts of Wifi and Checking Wifi adapter Compatibility
- - WIFI(WEP,WPA,WPA2) password cracking

Cloud Security

- - Architectural Concept and Design Requirements
- - Cloud Data Security
- - Cloud Platform and Infrastructure Security
- - Cloud Application Security
- - Operations
- - Legal and Compliance

Security Operations

- **- Understanding Events, Incidents and log mechanisms**
- **- Security Information & Event Management (SIEM) Basics**
- **- Introduction to QRADAR SIEM**
- **- Explore the user interface**
- **- Components and Architecture of QRADAR SIEM**
- **- Event collector & Flow Processor**
- **- Flow collector & Flow Processor**
- **- Magistrate & Aerial Database**
- **- Understanding LogActivity in QRADAR SIEM**
- **- Real-Time streaming and Searching**
- **- Quick Filters**
- **- AQL**
- **- Network Activity**
- **- Rules configuration in QRADAR SIEM**
- **- Locate Rules and Building Blocks**
- **- Inspect actions and responses of rules**

Python For Pentesting

- **- Introduction and Environment Setup**
- **- Basics of Python Programming**
- **- Building Tools With Python(N/W Scanner, Port Scanner, Password Cracker)**
- **- Building Tools With Python(Web Crawler, Packet Sniffer)**
- **- Building Tools With Python(Simple Malware, Python Backdoor)**