ATTESTATO DI PARTECIPAZIONE

Codice Progetto: 040PROTD2104656

Si certifica che

PULVIRENTI MARCO

Ha partecipato al **Corso di Formazione Professionale**

"Academy Cybersecurity "

Durata totale: h 213 Teoria: h 178 Pratica: h 35

Periodo di svolgimento: dal 01/02/2021 al 19/03/2021

Ore frequentate: 212

Torino li 26/04/2021

Il Responsabile del Progetto

ATTESTATO DI PARTECIPAZIONE

Moduli

SALUTE E SICUREZZA GENERALE
Quadro normativo in materia di sicurezza dei lavoratori. Elementi innovativi del D. Lgs. 81/2008. Riferimenti storico legislativi. La storia della prevenzione. L'igiene del lavoro. Esempi di esperienze pratiche. Elementi di tecnica della comunicazione interpersonale. Prevenire, informare, formare. Valutazione del rischio, criteri. Figure primarie della struttura. Organizzazione della sicurezza in azienda. Obblighi e responsabilità civili e penali. Compiti e attribuzioni.
DIRITTI E DOVERI
Lg. 276/03. il CCNL. Competenze e obblighi dell'agenzia per il lavoro e dell'impresa utilizzatrice. Il contratto di somministrazione.
MODULO TECNICO
Introduction: Course Overview and Goals; Setting Up a Personal Lab. What is Virtualization? Virtualization Software Overview; Creating a Virtual Machine; Creating and Using Snapshots; Installing Kali as a Virtual Machine; Installing Windows as a Virtual Machine; Creating a Linux Cloud Server. Linux Administration and Security: Introduction to UNIX/Linux; The Kernel; The Shell; The Terminal; Linux Distributions; Command Line Basics; man pages; Directories; Files; Bonus: Problem Solving Methodology; File Contents; Linux File Tree; Shell Expansion; Commands and Arguments; Control Operators; Shell variables; Shell Embedding and Options; Shell History; File Globbing; Pipes and Commands; I/O Redirection; Filters; Basic Unix Tools; Command Line Challenge; Regular Expressions. Regular Expressions Challenge: Command-Line Environment; tmux; vim; Bonus: Touch Typing; Bonus: Mouseless Computer Control; Bash Scripting; Introduction; Loops; Parameters. Local User Management: Introduction to Users; User Management; User Passwords; User Profiles; Groups. File Security: Standard File Permissions; Advanced File Permissions; Access Control Lists; File Links; Processes; Introduction; Process Priorities; Background Jobs; Linux System Administration; Scheduling; Logging; Memory Management; Resource Monitoring; Package Management. Computer Networking Fundamentals: Introduction to Networking; The OSI Model; Key Networking Terms; Packet Sniffing with Wireshark; Advanced Wireshark Filtering and Analysis; Identifying Malicious Content and Streams; Extracting and Repairing Content from PCAP files; Physical Layer; Data Link Layer; MAC; ARP; Ethernet; Network Layer; Network Addresses. IP (IPv4, IPv6); Network Masks; Routing; ICMP; Transport Layer; TCP; UDP; Session and Presentation Layer; Logical Ports; Application Layer; Socket Programming - TCP/UDP Client and Server; DHCP, DNS, FTP, HTTP, HTTPS, SNMP, SSH, Telnet, TLS/SSL; Networking Conclusion - A Journey of a Packet. Python Programming for Security: OWASP Python Security Project; Implementing 'ps' using Python and /proc; Creating a Port Scanner. Attacking and Defending Networks; Introduction; MITRE ATT&CK Framework; Network Anonymity; Proxy Servers; proxychains; Tor; Network Attack Detection and Prevention; Denial-of-Service Attacks; MITM Attacks; IP Spoofing; ARP Spoofing; DNS Spoofing; Bypassing HTTPS (Protocol Downgrade Attacks); JavaScript Code Injection; Detecting ARP Poisoning Attacks; Detecting Suspicious Network Activity; Preventing MITM Attacks; Firewalls; Next-Generation Firewalls; Web Application Firewalls; iptables Fundamentals; IDS/IPS; SNORT; Suricata; Techniques for Evading IDS/IPS. Incident Response: SOC (Security Operations Center); SOC Components: People, Processes, and Technology; SOC Implementation; Preparing for an Incident; Incident Response Lifecycle; Security Logging and Monitoring; Local and Centralized Logging; Security Information and Event Management (SIEM); Installing and Configuring Splunk on a Windows Server; Transformation Commands; Reports, Dashboards, and Alerts; Detecting Ransomware with Splunk. Real-World Project: Building an Intrusion Detection System from Scratch. Working with Scapy (Packet manipulation tool). Penetration Testing: Introduction to Penetration Testing; Terminology; The Phases of a Penetration Test; Information Gathering – Passive; Open Source Intelligence Gathering (OSINT); Google Hacking; Information Gathering – Active; Host discovery; Port and Service Scanning; Nmap and zenmap; Finding Unlisted Files and Directories; Social Engineering for Information Gathering; Maltego; SEToolkit; HiddenEye; Enumeration Vectors; Default Passwords; SNMP Enumeration; Threat Modeling and Vulnerability Analysis; Vulnerability Scanners; Nessus, Nexpose, OpenVAS; Password Cracking; Hashcat, Hydra; Server-Side Exploitation; Bind, Reverse, and Encrypted Shells; The Metasploit Framework; Client-Side Exploitation; Creating a Backdoor; Delivering a Backdoor; Protecting Against Delivery Methods; Exploiting a System Through a Malicious Update; Browser Exploitation; BeEF; Hiding Malware Inside Innocent Files;Trojan Detection; Post Exploitation and Reporting; Privilege Escalation Techniques (Linux and Windows); Pivoting; Maintaining Access. Windows Administration and Security: Introduction to Windows; Command Line Basics; Batch Scripting; Windows Registry; Permissions; Workgroup; Powershell for Hackers; Sysinternals Suite; Windows Domain and Active Directory; Creating a Windows Server 2019 Machine; Promoting a Server to a Domain Controller; Active Directory Attacks; Securing Windows Domain. Web Application Security: Introduction to Web Applications; Web Servers; Web Application Architecture; Web Application Technologies; Client-Side Development - HTML, CSS, and JavaScript; HTML5; Tags; Nesting Elements – Hierarchy; HTML Attributes; Forms; DOM - Document Object Model; CSS3; JavaScript; Manipulating the DOM; Ajax; jQuery; Server-Side Development; Common Server-Side Programming Languages; PHP; Variables, Loops, Functions, and Classes; Object Serialization; PHP and http; Exploitable PHP Functions; Sessions; Using PDOs to Connect to a Database; Databases Introduction; Relational / SQL; Non-Relational / NoSQL; Web Application Reconnaissance Tools; Finding and Exploiting the OWASP Top 10 and Common Web App Attacks; Burp Suite Fundamentals; SQL Injection; OS Command Injection; Path Traversal; Local File Inclusion; Remote File Inclusion; Cross-Site Request Forgery (CSRF); Broken Authentication; Sensitive Data Exposure; XXE - XML External Entities; Broken Access Contro; Security Misconfigurations; XSS - Cross-Site Scripting; Insecure Deserialization; Using Components with Known Vulnerabilities; OWASP Open SAMM; Discovering Vulnerabilities Automatically; ZAP, Nikto, w3af, sqlmap. Access Management, Fondamenti di Web Access Management (WAM), concetti di credenziale e digital identity protection. Benefici derivanti, Compliance normative ed esempi di applicabilità nelle Industry di riferimento. Introduzione alle architetture dei sistemi di WAM e Single Sign-On. Architetture WAM. Protocolli di comunicazione: Fondamenti di SSO (siteminder) Lab: installazione e configurazione ldap e http server, Lab: installazione componenti Siteminder, Lab: installazione Access gateway, Panoramica su certificati, Lab: Integrazione di web application con metodi di autenticazione e policy management, Single Sign-On, Strong Authentication (MFA, 2FA). Federation Based Authentication, Identity Provider, Credential Provider. Lab: Altri metodi di autenticazione Apache-mod, Lab: protezione con Webagent. Identity and Access Governance (IAG). Introduzione alle tematiche di Identity & Governance Management: Gestione e controllo dell'identità digitale, il concetto di identità digitale, ambiti disciplinari. Introduzione alle tematiche di Identity & Governance Management: Gestione e controllo dell'identità digitale, il concetto di identità digitale, ambiti disciplinari. Benefici derivanti dall'applicazione di un sistema di ID & Governance Management: perché utilizzare IDM, realtà aziendali, Come funziona un sistema di Identity Management: macroaree, l'identità pura, user access, servizi basati sui ruoli, come gestire i 3 aspetti dell'identità, Componenti, Workflow Federated Identity Management & Governance. Privileged Identity Management, Sfide e rischi nell'implementare un sistema di ID Governance MGMT. Componenti Tecnologiche. Overview del prodotto di Identity Governance. Concetti base applicati alla tecnologia. Laboratorio. Laboratorio, Connettori Standard, Connettori Custom, Integrazione con sistemi target. Identity Governance; Role Mining.

Azione formativa realizzata con il finanziamento di Forma. Temp