RANGEFORCE

Certificate of Continuing Education Completion

THIS CERTIFICATE IS AWARDED TO

Sameal Con-Roma

For successfully completing 106 modules, from 08/28/2023 to 08/29/2024, equivalent to 39 hours and 45 minutes of study, provided by the RangeForce Platform

Modules completed are shown in Annexes

08/28/2024

Date

Taavi Must, President of RangeForce

Annex 1

- Cybersecurity Kill Chain
- Handover Procedures
- Blue Team Functions and Tasks
- Overview of Logging and Monitoring in AWS
- Networking Security Services in Azure
- Azure Security Management
- Azure Security Monitoring
- Azure Security for the SOC
- Crypto-mining Attacks in the Cloud
- Isolating Cloud Attacks
- Containing Lateral Movement in the Cloud
- Cloud Security - Access Control
- IAM - Principle of Least Privilege
- Cloud Access Security Broker Introduction
- IAM - Creating Strong Passwords
- IAM Roles
- IAM: Managing User Accounts
- Phantom Overview
- Cryptography Overview
- Prevent Unvalidated Redirects and Forwards
- Prevent Cross-Site Request Forgery Flaws
- Prevent Cross-Site Scripting Flaws
- Prevent Session Management Flaws
- Prevent Injection Flaws
- Web Attack Overview
- Request/Response Model
- Web Protocols Overview
- Build in Security by Design
- IAM Overview
- SASE Overview
- Introduction to Governance, Risk, and Compliance
- Map the IoT Attack Surface
- Introduction to PowerShell
- Passive Information Gathering
- Introduction to Active Directory
- Preparing Your Pentest Environment
- Legal Considerations for a Pentest
- Scoping and Budgeting for a Pentest
- Offensive Security Assessments
- Cybersecurity Teams
- Cybersecurity Terminology
- Elastic: Introduction to Fleet and Elastic Agent
- Elastic: Introduction to Elastic Stack
- Hybrid Cloud Overview
- Cloud Security - Shared Responsibility
- Cloud Security Overview
- Forwarding Logs to Splunk
- Microsoft Sentinel: Introduction
- Regular Expressions In Splunk
- Splunk Webapp IR: Brute Force Detection
- Splunk: Lookups
- SQL Injection: Authentication Bypass
- Keys to Useful Threat Intelligence
- Yextend
- Suricata Challenge
- Windows - Active Directory GPO
- Windows - NTLM
- Weak and Reused Domain Credentials
- Linux Log Management: Systemd Journal
- Firewall Policies: FortiOS
- Investigations with Wireshark
- Windows - Process Injection IR (Splunk)
- Linux Security Investigation Exercise
- LOKI IOC Scanner
- Identifying Linux IOCs
- Visual Spoofing
- OpenSCAP
- Sudo Killer
- Lateral Movement Overview
- Greenbone Vulnerability Management
- Nikto
- CVE-2019-15107 WebMin 1.890 Exploit Unauthorized RCE
- Introduction to Vulnerability Management
- PCAP Forensics - HTTPS/TLS Decryption and Analysis
- Suricata: IPS Rules
- PCAP Forensics: Wireshark
- Traffic Light Protocol Overview
- Windows Active Directory Rights Management
- Splunk: API
- Splunk: Input Configuration
- PowerShell Logging
- Windows - CMD Basics
- PowerShell Objects and Data Piping
- PowerShell Commands
- PowerShell Modules
- Basic Shell Scripting
- Threat Intel Challenge
- Blue Team Challenge
- Pass the Hash
- PowerShell Filtering and Formatting
- Linux Syslog
- Linux System Info Gathering
- YARA Rule Writing
- YARA Rule Generation
- YARA Rule Management
- Email Challenge
- Splunk: Alerts
- Suricata: Rule Management
- Suricata: IDS Rules
- Suricata: Basics
- Wireshark Basics
- YARA Overview
- Regular Expressions in YARA
- Introduction to Regular Expressions
- Email URL Analysis
- Email Header Analysis Exercise