RANGEFORCE

Certificate of Continuing Education Completion

THIS CERTIFICATE IS AWARDED TO

Nazar Sakhnii

For successfully completing 192 modules, from 09/04/2022 to 09/04/2023, equivalent to 62 hours and 50 minutes of study, provided by the RangeForce Platform

Modules completed are shown in Annexes

09/08/2023

Date

Taavi Must, President of RangeForce

Annex 1

- Email URL Analysis
- Email Header Analysis Exercise
- Malware Analysis: VirusTotal
- Recorded Future: Browser Extension
- Malware Analysis: Introduction to Basic Tools
- QRadar: Network Activity
- QRadar: Basics
- QRadar Overview
- OSINT: Mapping Target Infrastructure
- Introduction to SIEM and SOAR
- Linux Syslog
- Windows - Procmon
- PowerShell Remoting
- PowerShell Filtering and Formatting
- PowerShell Objects and Data Piping
- PowerShell Commands
- PowerShell Modules
- Introduction to PowerShell
- SOC Level 1 Assessment
- Linux Networking Fundamentals Challenge
- PCAP Forensics: TShark
- IDS/IPS Overview
- NAT Concepts
- Layer 4 Networking
- Layer 3 Networking: Routing
- Layer 3 Networking: Overview
- Layer 2 Networking
- Introduction to OSI Networking Model
- Linux CLI Fundamentals Challenge
- Linux Tmux Introduction
- Linux System Info Gathering
- Linux Log Management: Systemd
- Basic Shell Scripting
- Linux Execution Context
- Linux Software Management
- Linux Environment Variables
- SSH Basics
- Linux User Management
- Active Information Gathering
- Passive Information Gathering
- Linux Authentication
- Linux File Permissions and Ownership
- Linux File Management
- Basic Linux File Editing
- Linux CLI Introduction
- Remote Code Execution Introduction
- Privilege Escalation: Introduction
- Understanding the Threat Landscape
- Introduction to the SOC
- Introduction to Active Directory
- Preparing Your Pentest Environment
- Legal Considerations for a Pentest
- Scoping and Budgeting for a Pentest
- Offensive Security Assessments
- Prepare for Forensic Investigation as a CSIRT
- Contain and Mitigate Incidents (Part 2)
- Contain and Mitigate Incidents (Part 1)
- Deploy an Incident Handling and Response Architecture (Part 3)
- Deploy an Incident Handling and Response Architecture (Part 2)
- Deploy an Incident Handling and Response Architecture (Part 1)
- Command Injection: Fix (PHP)
- Command Injection: Find & Exploit (PHP)
- XSS Overview
- Introduction to Injection Attacks
- Broken Access Control Overview
- SQL Injection: Authentication Bypass
- SQL Injection: Prelude
- SQL Injection: Overview
- x86 Calling Conventions - Microsoft x64
- x86 Calling Conventions - cdecl
- x86 Calling Conventions - System V ABI
- Stack Frames
- Debugger Usage: Cutter
- Anatomy of an ELF Executable
- Stack and Heap Basics
- x86 Instructions
- x86 Registers
- x86 Architecture Primer
- Introduction to Ryuk Ransomware
- The Evolution of Ransomware
- Ransomware Overview
- Fully Automated Analysis - Exercise
- Fully Automated Analysis - Case Study
- Introduction to Fully Automated Analysis
- Sandbox Evasion Techniques
- Malware Sandboxing
- Introduction to Email Based Threats
- Exploit Database
- Visual Spoofing
- Advanced Bruteforcing Tactics
- Known vs. Unknown Malware
- Introduction to Cybersecurity Terminology
- Introduction to Malware Analysis Stages
- Microsoft Sentinel: Log Analytics
- Microsoft Sentinel: Detection Rules
- Microsoft Sentinel: Threat Management
- Microsoft Sentinel: Introduction
- Burp Suite: Advanced
- Physical Media
- Clean Desk
- Stakeout
- Tailgating 2
- Valuables in Car
- Privacy Screens
- Unattended Computers
- Tailgating
- Same Passwords
- Password Handling
- Password Managers
- Multi-factor Authentication
- Passphrases
- Passwords
- Microsoft Office Risk
- Dumpster Diving
- USB Key Drops
- Printouts
- Unnecessary Data
- Keeping Data Safe
- Think Twice Before You Post
- Handling Confidential Material
- GDPR
- Data Leaks
- Burp Suite: Basics

Annex 2

- Conducting a Risk Assessment
- Integrating Documentation into Risk Management (Part 2)
- Integrating Documentation into Risk Management (Part 1)
- The Importance of Risk Management
- Blind XML External Entities
- Nmap Challenge
- Nmap: SNMP Enumeration
- XXE RCE Using PHP Expect
- Introduction to SSRF
- XML External Entities: Fix
- XML External Entities: Find & Exploit
- XML External Entities Overview
- Snort: Basics
- Introduction to Security Onion
- Testing With OWASP ZAP
- OWASP Zed Attack Proxy Overview
- OWASP ZAP: Basics
- Burp Suite Overview
- Password Cracking 2
- Nmap: SSH Enumeration
- Nmap: Basics
- Nmap: Overview
- Wfuzz
- API Security: Exposed Tokens
- HTTPS Security: Introduction
- Wireshark Basics
- JSON Web Token Security Challenge 1
- JSON Web Token Security
- Password Cracking
- Web Application Exploit Challenge Alpha 1
- Unrestricted File Upload: Find & Exploit (PHP)
- Path Traversal: Fix (PHP)
- Path Traversal: Find & Exploit (PHP)
- NoSQL Injection 1: Fix
- NoSQL Injection 1: Exploit
- NoSQL Injection 1: Find
- Reverse Shells
- Metasploit Basics
- Metasploit Overview
- Learner Onboarding Video
- Ransomware Attack
- Update Your Software
- Keylogger
- Suricata Challenge
- Suricata: Rule Management
- Suricata: IPS Rules
- Suricata: IDS Rules
- Suricata: Basics
- Conference Risk
- Sharing Information
- Correct Links
- Doublecheck Before You Trust
- Vishing
- Shoulder Surfing
- Social Engineering
- Password Security In-Depth
- Spreading Viruses
- Software Installs
- Spyware
- Ransomware
- Introduction to Malware Analysis
- Network Printer
- Free WiFi
- VPN
- Regular Expressions: Advanced
- Regular Expressions: Intermediate
- Regular Expressions: Basic
- Introduction to Regular Expressions
- Module Tutorial