Book of Accomplishment

About Me

Experienced Penetration Testing Professional with expertise in identifying and addressing security vulnerabilities across IT infrastructures. Proficient in executing simulated cyber-attacks, conducting vulnerability assessments, and mitigating risks. Skilled in compliance with industry standards like PCI DSS, ISO 27001, and NIST. Utilizes a systematic methodology, combining manual testing and automated tools, to analyze security controls and threat vectors. Committed to fostering a proactive security culture, providing actionable recommendations, and staying abreast of the latest security trends. Dedicated to empowering organizations to defend against emerging cyber threats and elevate their overall security posture.

Aenosh Rajora

Table of Content

Internship

➢ Corizo (Network Security)

Internship at Corizo focused on network security, providing hands-on experience and insights. Engaged in tasks like network monitoring, vulnerability assessments, and security protocol implementation. Collaborated with professionals, acquiring practical knowledge in configuring and maintaining security systems. Analyzed network traffic for potential threats, contributing to the development of robust security policies. Gained skills in fortifying digital networks against cyber threats in a dynamic environment. Overall, the internship at Corizo deepened understanding and expertise in network security

practices.

Software Development

- **Python for Absolute Beginners**

It covers fundamental topics such as Python installation, script execution, and PyCharm IDE setup. Additionally, the course delves into key programming concepts including data types, variables, functions, loops, and modules. The culmination of the course involves a final project to apply the knowledge gained throughout the program, making it an ideal starting point for beginners venturing into the world of programming.

Vulnerability Assessment and Pentesting

➢ Ethical Hacking Essentials (EHE)

The "Ethical Hacking Essentials" (EHE) is an introductory cybersecurity course designed to teach fundamental concepts in ethical hacking and penetration testing. Covering topics like threats, vulnerabilities, password cracking, web application attacks, IoT and OT attacks, cloud computing, and pentesting fundamentals, the course provides hands-on practical experience to equip learners with essential skills for a cybersecurity career. EHE certification offers formal recognition, enhancing learners' resumes and showcasing their expertise to potential employers. Certified individuals are likely to experience improved job prospects, higher salaries, and increased job satisfaction.

- **Hacking WEP/WPA/WPA2 Wi-Fi Networks Using Kali Linux 2.0**

This course was designed for individuals with no prior hacking knowledge, focusing on both practical and theoretical aspects. It begins by instructing on setting up Kali Linux 2.0, the latest version from Offensive Security Organization. Learners explore the communication between devices and delve into the theory behind WEP and WPA2 encryption cracking methods. The course covers multiple techniques for cracking WiFi encryption keys, allowing learners to try alternative methods if needed. Following successful key cracking, participants engage in advanced attacks against network clients. The course concludes by educating learners on self-protection and safeguarding Wi-Fi Access Points from potential attacks. It caters to both beginners and professionals, guiding novices from the basics to becoming professionals and enhancing the knowledge of those already experienced in hacking.

➢ Web Application Security Testing with Google Hacking

This course focuses on exposing sensitive data in web applications through Google indexing. Participants learn Google Hacking techniques, uncovering vulnerabilities like directory listings, SQL errors, and more. Real-world scenarios and demonstrations encourage practical application in penetration testing. The course highlights the Google Hacking Database and a case involving a critical vulnerability in Microsoft Yammer. The final part guides participants in preventing Google indexing for enhanced security.

➢ Foundations of Hacking and Pentesting Android Apps

This course focuses on hacking and penetration testing as vital components of application security, with a specific emphasis on Android applications. Organizations often employ penetration testers to assess the security of various systems. The course serves as a foundational guide for anyone interested in learning more about computer security and Android application hacking. Participants will gain knowledge on setting up a test environment, decompiling APKs, detecting common vulnerabilities, and utilizing Drozer for penetration testing in Android

applications. By the end of the course, learners will have acquired practical skills in Android hacking and pentesting.

➢ Ethical Hacking with Ruby for Beginners

This course is designed for those aiming to become ethical hackers or enhance their hacking skills, with a specific focus on using Ruby for ethical hacking of corporate systems and web applications. Emphasizing the efficiency gained through mastering Ruby, the course covers vulnerability scanning and reverse engineering of Ruby on Rails applications. Participants learn to exploit common vulnerabilities, hack web services and APIs using Ruby, and use Metasploit for Ruby on Rails apps. The course concludes with guidance on documenting findings and best security practices for Ruby apps, making it accessible to learners with

varying expertise levels. The goal is to equip participants with the skills for ethical hacking using Ruby code, creating an exciting hacking journey.

- **Applied Attack Surface Analysis and Reduction for Vulnerability Assessment**

This course on Applied Attack Surface Analysis and Reduction is designed for cybersecurity professionals, covering the strategic aspects of analyzing and reducing an organization's attack surfaces. It explores attack surface analysis methodologies, metrics, and practical demonstrations to uncover weaknesses. Participants learn to apply these techniques across various business sectors, prioritize risks, and adapt to the dynamic nature of attack surfaces. The course also

delves into strategies for reducing attack surfaces, including strong controls and the principles of Zero Trust. It concludes with an overview of free and open-source attack surface analysis tools and provides a roadmap for further education, specifically EC-Council's Certified Chief Information Security Officer (CCISO) Program. Completing the course equips participants with skills to enhance an organization's cybersecurity posture.

➢ Digital Forensics Essentials (DFE)

The Digital Forensics Essentials course enhances learners' competence in digital forensics and information security, contributing value to their workplace. It covers Computer Forensics Fundamentals, the Investigation Process, Dark Web, Windows, Linux, Malware Forensics, and more. The interactive labs provide hands-on experience crucial for a future in digital forensics. Certification as DFE assures formal recognition for learners, improving their resumes and showcasing

expertise to prospective employers. This certification enhances prospects for employment advancement, higher salaries, and increased job satisfaction.

DevSecOps

➢ Practical DevSecOps with GitHub Actions

This course on DevSecOps focuses on integrating security practices into DevOps processes, ensuring that security considerations are not addressed only at the end of the delivery pipeline. DevSecOps, or Developer Security Operations, emphasizes incorporating a security mindset throughout the software development life cycle, aligning with the continuous processes of DevOps. The course advocates treating "Security as Code" and underscores its

importance as a coding requirement. The curriculum guides learners through the process of building an automated DevSecOps pipeline using GitHub actions. It begins with an introduction to Git/GitHub actions basics and YAML file syntax. The course then delves into understanding security concepts and proceeds to implement DevSecOps tools for Static Application Security Testing (SAST), Software Composition Analysis (SCA), and Dynamic Application Security Testing (DAST) through the YAML workflow file.

➢ Code Security with SonarQube

This course emphasizes the critical importance of code security and addresses the challenges by implementing SonarQube as a comprehensive solution. SonarQube stands out due to its real-time code scanning, allowing proactive identification and resolution of vulnerabilities throughout the development process. Its user-friendly interface and integration with various tools facilitate collaboration and

efficient issue resolution within development teams. Additionally, SonarQube's reporting and compliance features ensure that code meets industry standards and regulations, crucial for trust and legal adherence. The course promises a comprehensive and accessible approach to proactive code security through SonarQube, promoting collaboration, compliance, and long-term support.

Cyber Security

➢ Cyber Warfare - Défense Against Nation-State Threats

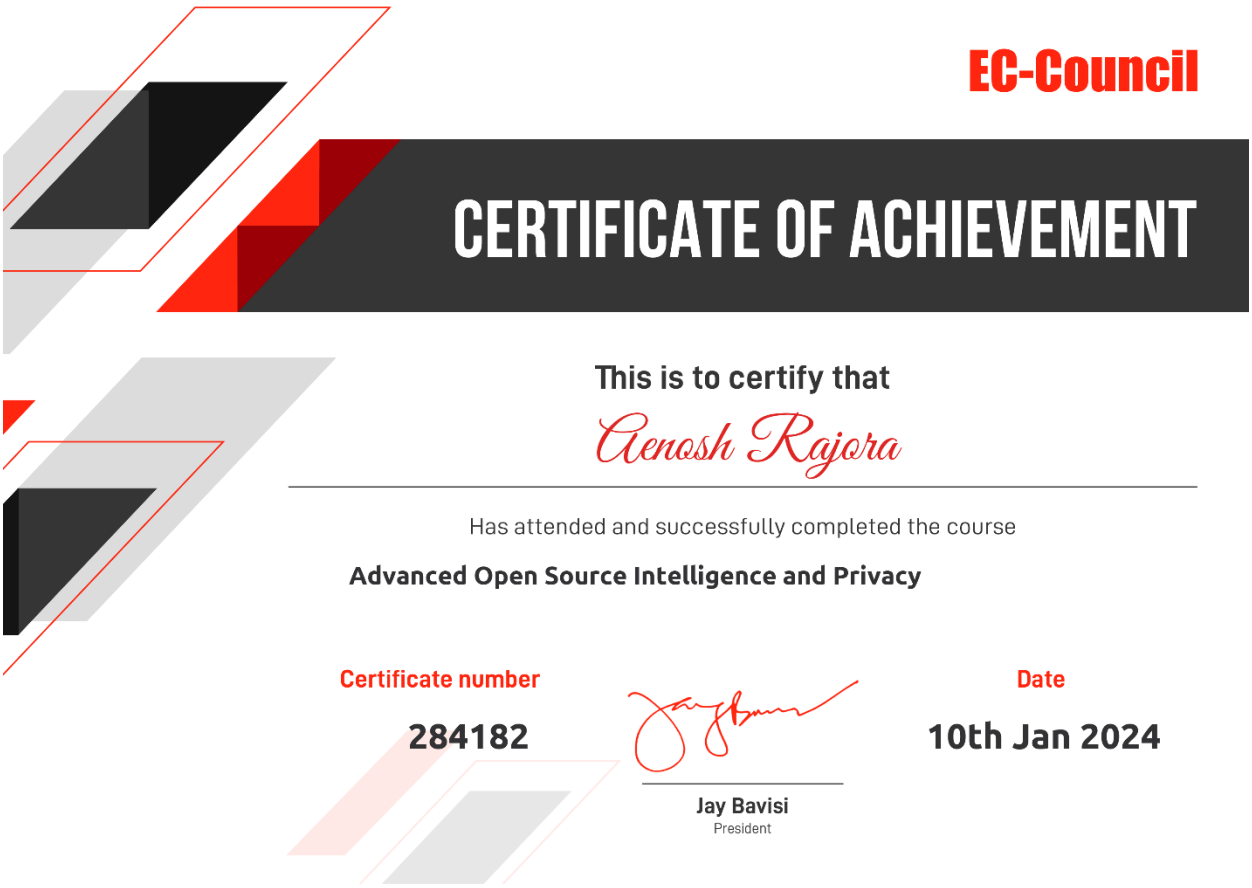
This course addresses the evolving landscape of global security, emphasizing the increasing threat of cyber warfare in modern geopolitical scenarios. As governments and organizations worldwide rely heavily on technology, the potential for rogue states to disrupt and interfere with critical infrastructure poses unprecedented risks. Cybersecurity and IT professionals, along with senior leaders in critical sectors, must be equipped to detect and respond to cyber

espionage and sabotage attempts promptly. The course targets professionals in critical infrastructure, finance, and government, aiming to enhance their ability to recognize and defend against cyber warfare threats. Given the potential impact on national security, corporate security teams must be adept at withstanding and recovering from large-scale cyberattacks. Government officials, military members, and cyber planners must also be well-versed in cyber warfare threats to formulate effective offensive and defensive cybersecurity strategies.

➢ Advanced Open Source Intelligence and Privacy

This advanced Open Source Intelligence (OSINT) course builds upon the foundation established in the previous OSINT course, assuming participants have a familiarity with basic search operators, generic OSINT processes, and a solid working knowledge of major web services and social media platforms. It is recommended to have completed the introductory Open Source Intelligence course before enrolling in this advanced program. The course delves into more advanced topics concerning OSINT and emphasizes the privacy perspective of one's digital life. Recognizing the unprecedented accessibility of information and data in contemporary times, the

course navigates through the intricacies of conducting online investigations. It introduces different approaches and tools, providing insights into privacy considerations. Participants will gain an understanding of advanced OSINT perspectives, enhance their privacy practices in the digital realm, and explore tools such as Recon-ng and Spiderfoot. The course covers techniques like profiling a LinkedIn contact and searching for information on the deep web. As participants uncover the extensive information exposed on the internet, the course aims to equip them with the skills needed to navigate this abundance of data effectively.



➢ Reverse Engineering, Memory Hacking, and Software Protection

This course is designed for individuals eager to learn the intricacies of reversing and patching packed programs without the need for unpacking. It challenges the common belief that packing and anti-debugging are sufficient to prevent reverse engineering, and participants will explore the effectiveness of various popular packers by packing crackmes and then reversing them, all without unpacking.

Traditionally, packed programs are unpacked before debugging, but this course takes a different approach. The analysis is performed using Cheat Engine, a tool widely used by game hackers, to study and analyze the processes of packed programs running in memory. Participants will learn debugging techniques despite the implementation of anti-debugging measures, eliminating the need to unpack and dump memory.

Rather than unpacking and patching dumped files, participants will delve into writing scripts to hack memory using advanced techniques like Array-Of-Bytes (AOB) Injection, injecting code into code caves through inline memory patching. The course covers various practical exercises using crackmes, exploring packing with popular packers and hacking them using Cheat Engine.

➢ Hands-on Cryptography with C++

This course is tailored to empower participants with the knowledge and skills required to design and build contemporary cryptographic solutions using C++. In an era where data privacy and ownership are paramount, the course explores the symbiotic relationship between C++ and cryptography, unraveling the complexities of cryptographic algorithms like AES and RSA.

The significance of this course is heightened in the digital age, where safeguarding data privacy is critical. C++ plays a pivotal role in this domain, making it essential to understand and master symmetric cryptographic algorithms. The course offers practical implementations of basic cryptographic tasks using C++, involving hands-on experiences with Caesar ciphers and RSA ciphers. As participants progress through the course, they will gain proficiency in utilizing essential cryptographic resources, including the Crypto++ and Botan libraries. The goal is to equip participants with the skills needed to address evolving challenges in the cryptography field. By the course's conclusion, participants will have the knowledge and practical experience to contribute effectively to the dynamic landscape of data security.

Security Architecture and Operations

➢ Network Defense Essentials (NDE)

Network Defense Essentials is an introductory cybersecurity course that covers fundamental concepts in information security and network defense. Tailored for entry-level information security and cybersecurity careers, it is well-suited for individuals aspiring to enter the cybersecurity field. The course provides a

comprehensive overview of key information security components, including Identification, Authentication, Authorization, Virtualization and Cloud Computing, Wireless Networks, Mobile and IoT Devices, and Data Security. Interactive labs are incorporated to ensure learners gain hands-on, practical experience crucial for a future in cybersecurity. Certification as NDE provides formal recognition for learners, enhancing their resumes and showcasing their expertise to prospective employers.

➢ Shell Scripting with Z Shell

This course is tailored for individuals who are new to Linux and want to enhance their command line skills or automate tasks on Linux using the Z shell. Whether you need to perform automated testing or wish to unlock the hidden power of Linux, this course provides a comprehensive journey through the various features of Linux and Z shell, which are among the most popular shells in Linux distributions. The course covers essential features, ranging from

fundamental to advanced, guiding participants on how to harness these features in shell scripts for automated tasks. It caters to both beginners, aiming to cultivate their command line and scripting skills, and power users seeking to elevate their proficiency in command line and scripting using Z shell. Throughout the course, participants will gain insights into Linux fundamentals and advanced scripting, with a focus on automation using the Z shell. Whether you are starting your Linux journey or looking to take your skills to the next level, this course provides a comprehensive and practical exploration of Linux and Z shell capabilities.

➢ Recon for Pentesting & Bug Bounties

This course is designed to provide comprehensive coverage of Recon and Bug Bounty Hunting, progressing from fundamentals to advanced exploitation techniques. Starting with the basics, participants will learn about the working of web servers, DNS, and distinctions between URL, URN, and URI. The course covers essential concepts such as Target Expansion, Content Discovery,

Fuzzing, CMS Identification, Certificate Transparency, Visual Recon, GitHub Recon, Custom Wordlists, Mind maps, Bug Bounty Automation, and Bug Bounty Platforms. Key topics covered in the course include Target Selection Techniques, Host and Subnet Scans, Host Discovery, Content Discovery, Subdomain Enumeration (Horizontal & Vertical), CMS Identification, Fuzzing for web vulnerabilities (e.g., XSS, Open Redirect, SSRF, SQL Injection), and using Shodan for bug bounties. The course emphasizes GitHub Recon to find sensitive information, automation for daily tasks, report writing for Bug Bounty & pen-testing, and the utilization of mind maps for a strategic approach.

➢ Applied HTML5 Security

This course delves into the realm of HTML5, which serves as the backbone for modern web applications, being utilized in 90% of websites and web applications. As HTML5 becomes integral to web development, understanding its security implications is paramount. Despite being designed with inherent security improvements, HTML5 is not immune to vulnerabilities, making it

crucial for developers and application security professionals to grasp HTML5 security concepts. The course begins with an overview of HTML5 fundamentals and then explores common vulnerabilities associated with HTML5, including potential attack vectors and built-in security features. Participants will gain insights into HTML5 attack vectors, understanding the security features embedded in HTML5, and explore defensive programming techniques to secure HTML5 code. Special attention will be given to addressing security issues related to HTML5 Forms.

Industrial Security Controls

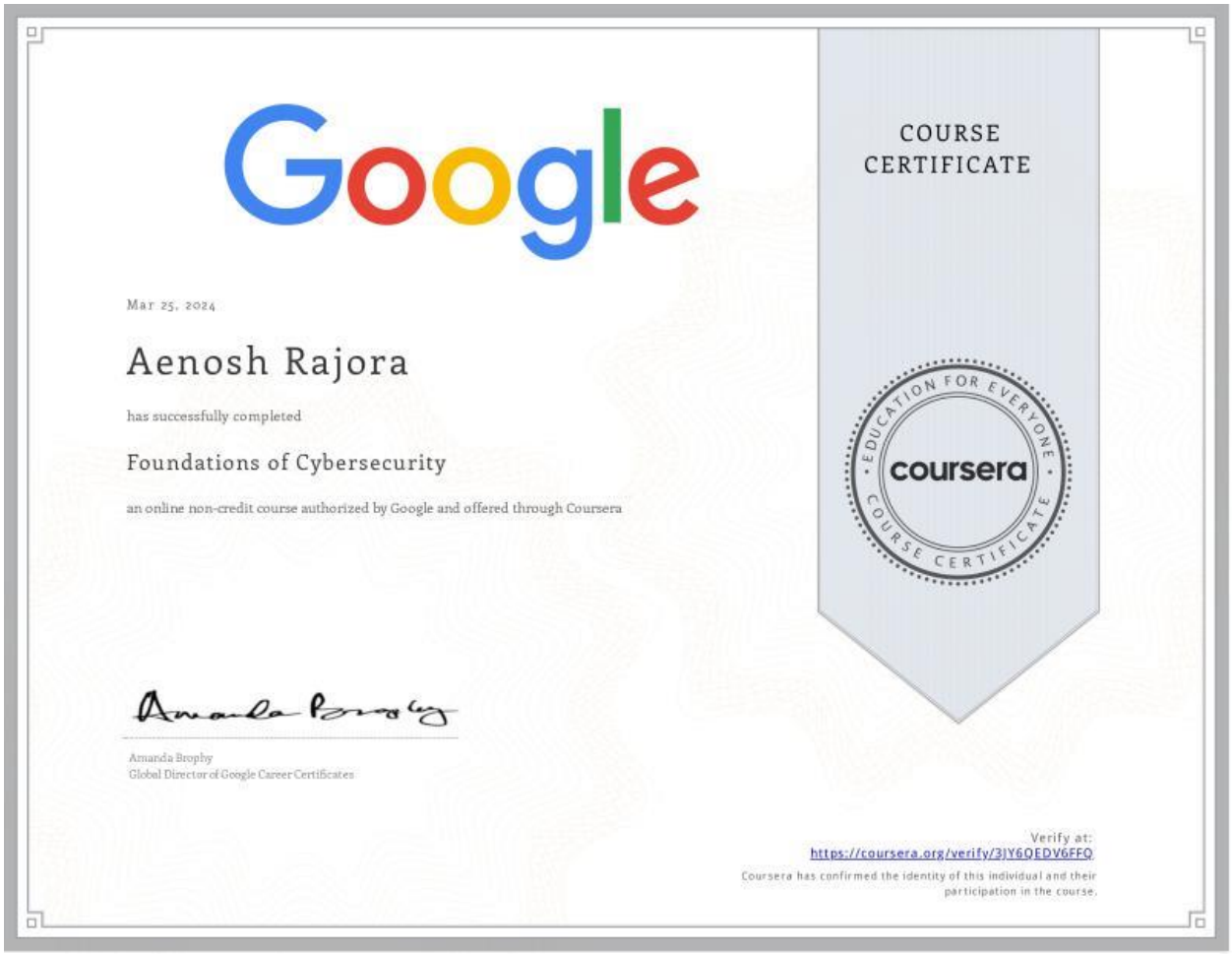
➢ Practical Internet of Things Hacking

This IoT Firmware Hacking course is designed for individuals keen on understanding and exploiting the vulnerabilities present in IoT devices. With the proliferation of Internet-connected devices, the security implications become

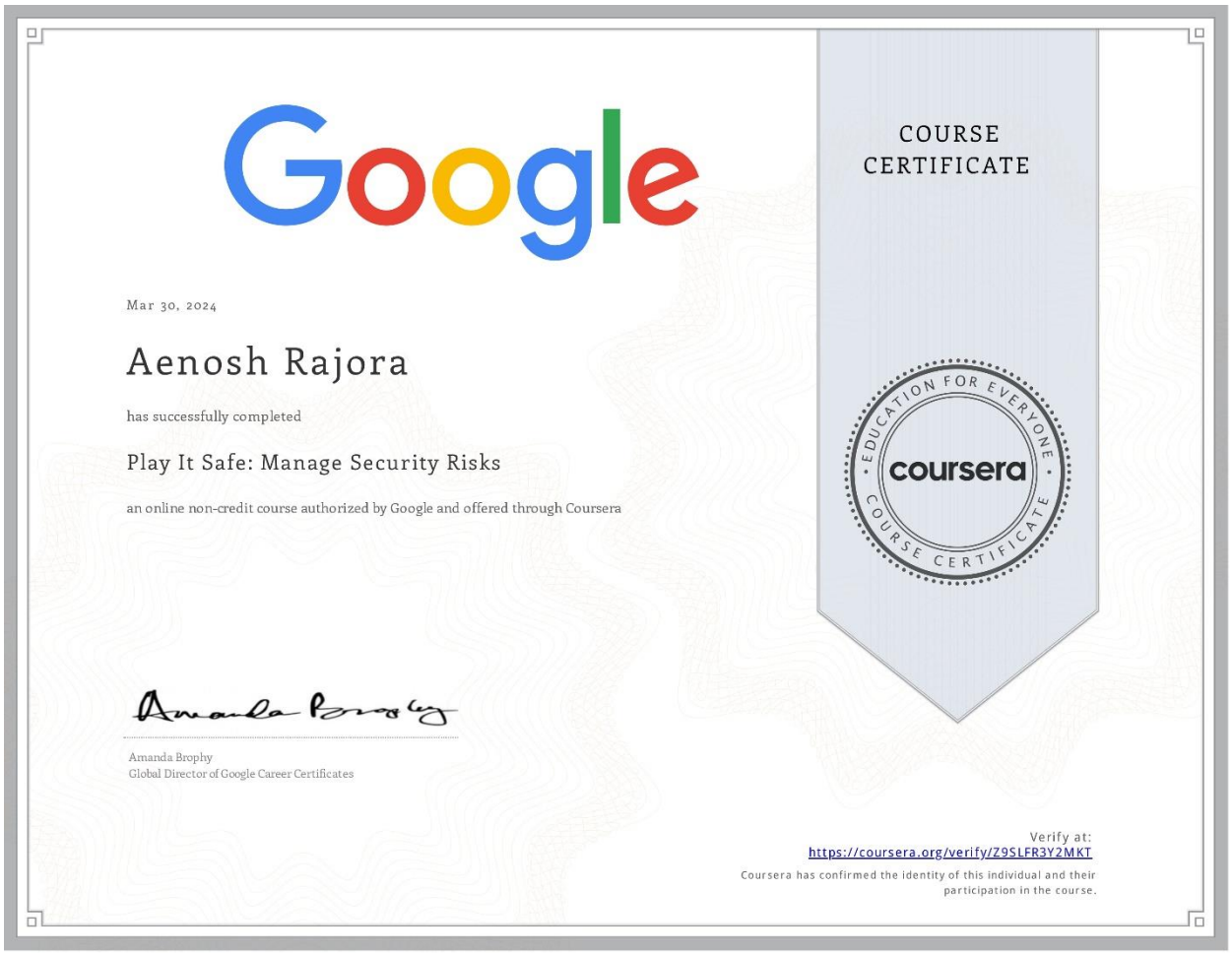
critical. This course provides a unique journey into the world of IoT firmware, covering topics such as extraction, reverse engineering, and exploitation. The course commences with foundational aspects, including tool installation and terminology. It then progresses into hands-on practice, using free and popular tools to ensure accessibility for participants without the need for additional purchases. The emphasis on ethical penetration testing underscores the responsible and authorized nature of the activities, ensuring compliance with legal and ethical standards. Ideal for penetration testers, security enthusiasts, and network administrators, this course equips participants with the skills to assess and secure IoT devices.

Google Cybersecurity Professional Certificate

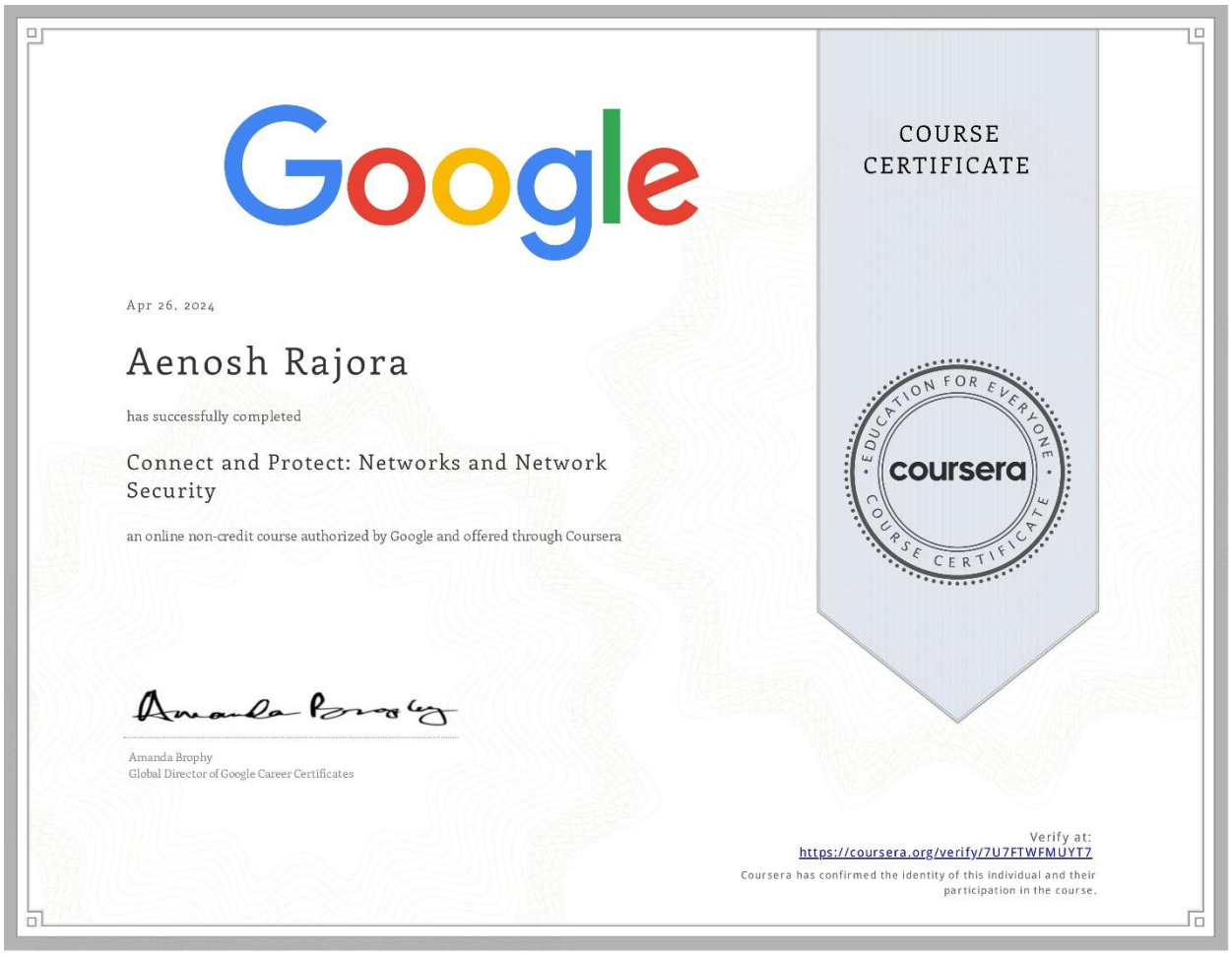
- **Foundations of Cybersecurity**
  This course helps to identify and recognize the skills and knowledge needed to become a cybersecurity analyst or security analyst. It helps to identify how security attacks or cybersecurity attacks impact on business operations, Explain Security ethics and Identify common tools used by cybersecurity analysts.



- **Play It Safe: Manage Security Risks**
  This course helps to identify the primary threads, risk and vulnerabilities to business operations, examine how organizations use security frameworks and controls to protect business operations. It also define commonly used Security Information and Event Management (SIEM) Tools and how to use a playbook to respond to threats, risk, and vulnerabilities.



- **Connect and Protect: Network and Network Security**
  This course defines the types of networks and components of networks. It also illustrate how data is send and receive over the network (3- way handshake). It helps to understand how to secure a network against intrusion tactics and describe system hardening techniques



Cisco Junior cybersecurity Analyst

- **Introduction to Cybersecurity**

  It explore th exciting world of cybersecurity and why the cybersecurity is essential and the importance of cybersecurity.

Introduction to Cybersecurity Badge

Introduction to Cybersecurity Certificate