Cyber Threat Assessment Fortinet

Inside Network Security Assessment
Nse 7
Network Security Assessment
Network Vulnerability Assessment
UTM Security with Fortinet
Network Security Assessment: From Vulnerability to Patch
Information assurance trends in vulnerabilities, threats, and technologies
Cyber Forensics
The Rise of Politically Motivated Cyber Attacks
Blue Team Operations
Managing A Network Vulnerability Assessment
Decision Making and Security Risk Management for IoT Environments
Fortigate Security Pocket Guide
Fortinet NSE8 - Network Security Expert Written Exam – New version (NSE8_812)
NSE4 Study Guide Part-II Infrastructure
Scalable Framework for Cyber Threat Situational Awareness
Nse 4
Introduction to FortiGate Part-II Infrastructure
Fortinet Certified Network Security Professional
The Art of Cyber Defense
Understanding Cybersecurity Management in FinTech
Fortinet NSE4 6.2 Actual Exam Actual Questions 2021 Fortinet Network Security Expert 4 - NSE 4
Cyber Security on Azure
Security and Organization within IoT and Smart Cities
Nse 4
Strategic Cyber Deterrence
ITNG 2022 19th International Conference on Information Technology-New Generations
Common Cyber Attack Or Cyber Warfare
Introduction to FortiGate Part-1 Infrastructure
Guide to Cyber Threat Information Sharing
Fortinet Certified Network Security Administrator
Fortinet Network Security Expert 4 (NSE4 FGT 6.2) Exam Practice Questions & Dumps
Guide to Vulnerability Analysis for Computer Networks and Systems
Cyber-Security Threats, Actors, and Dynamic Mitigation
Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications
Models for Threat Assessment in Networks
Introduction to FortiGate Part-1 Infrastructure
Threat Analyst Critical Questions Skills Assessment
Assessing Cyber Security
Fight Fire with Fire

KOLE DEON

Inside Network Security Assessment Createspace Independent Publishing Platform
Traditionally, network security (firewalls to block unauthorized users, Intrusion Prevention Systems (IPS) to keep attackers out, Web filters to avoid misuse of Internet browsing, and antivirus software to block malicious programs) required separate boxes with increased cost and complexity. Unified Threat Management (UTM) makes network security less complex, cheaper, and more effective by consolidating all these components. This book explains the advantages of using UTM and how it works, presents best practices on deployment, and is a hands-on, step-by-step guide to deploying Fortinet's FortiGate in the enterprise. - Provides tips, tricks, and proven suggestions and guidelines to set up FortiGate implementations - Presents topics that are not covered (or are not covered in detail) by Fortinet's documentation - Discusses hands-on troubleshooting techniques at both the project deployment level and technical implementation area
Nse 7 Springer
This book aims to provide the latest research developments and results in the domain of AI techniques for smart cyber ecosystems. It presents a holistic insight into AI-enabled theoretic approaches and methodology in IoT networking, security analytics using AI tools and network automation, which ultimately enable intelligent cyber space. This book will be a valuable resource for students, researchers, engineers and policy makers working in various areas related to cybersecurity and privacy for Smart Cities. This book includes chapters titled "An Overview of the Artificial Intelligence Evolution and Its Fundamental Concepts, and Their Relationship with IoT Security", "Smart City: Evolution and Fundamental Concepts", "Advances in AI-Based Security for Internet of Things in Wireless Virtualization Environment", "A Conceptual Model for Optimal Resource Sharing of Networked Microgrids Focusing Uncertainty: Paving Path to Eco-friendly Smart Cities", "A Novel Framework for a Cyber Secure Smart City", "Contemplating Security Challenges and Threats for Smart Cities", "Self-Monitoring Obfuscated IoT Network", "Introduction to Side Channel Attacks and Investigation of Power Analysis and Fault Injection Attack Techniques", "Collaborative Digital Forensic Investigations Model for Law Enforcement: Oman as a Case Study", "Understanding Security Requirements and Challenges in the Industrial Internet of Things: A Review", "5G Security and the Internet of Things", "The Problem of Deepfake Videos and How to Counteract Them in Smart Cities", "The Rise of Ransomware Aided by Vulnerable IoT Devices", "Security Issues in Self-Driving Cars within Smart Cities", and "Trust-Aware Crowd Associated Network-Based Approach for Optimal Waste Management in Smart Cities". This book provides state-of-the-art research results and discusses current issues, challenges, solutions and recent trends related to

security and organization within IoT and Smart Cities. We expect this book to be of significant importance not only to researchers and practitioners in academia, government agencies and industries, but also for policy makers and system managers. We anticipate this book to be a valuable resource for all those working in this new and exciting area, and a "must have" for all university libraries.

Network Security Assessment

Independently Published

Do you assess cybersecurity vulnerabilities according to the role of the affected device? Does your organization collect cybersecurity related information in a systematic order? How do you share information cyber threat intelligence between public and private sectors? How you will find people with the right aptitude for the different cybersecurity skills? Is it possible to calculate the likelihood of a threat exploiting a given vulnerability? Should it be considered an immediate threat to be addressed through direct remediation? What are the current exploitable vulnerabilities in your business that are more common? What cyber threats are there and how do you prepare for, and minimize potential attacks? What is the most challenging aspect of cybersecurity management across your organization? When will the threat of a cyberattack be enough to spark real organizational resilience? This Threat Analyst Guide is unlike books you're used to. If you're looking for a textbook, this might not be for you. This book and its included digital components is for you who understands the importance of asking great questions. This gives you the questions to uncover the Threat Analyst challenges you're facing and generate better solutions to solve those problems. Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you're talking a one-time, single-use project, there should be a process. That process needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Threat Analyst investments work better. This Threat Analyst All-Inclusive Self-Assessment enables You to be that person. INCLUDES all the tools you need to an in-depth Threat Analyst Self-Assessment. Featuring new and updated case-based questions, organized into seven core levels of Threat Analyst maturity, this Self-Assessment will help you identify areas in which Threat Analyst improvements can be made. In using the questions you will be better able to: Diagnose Threat Analyst projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices. Implement evidence-based best practice strategies aligned with

overall goals. Integrate recent advances in Threat Analyst and process design strategies into practice according to best practice guidelines. Using the Self-Assessment tool gives you the Threat Analyst Scorecard, enabling you to develop a clear picture of which Threat Analyst areas need attention. Your purchase includes access to the Threat Analyst self-assessment digital components which gives you your dynamically prioritized projects-ready tool that enables you to define, show and lead your organization exactly with what's important.

Network Vulnerability Assessment

Independently Published There are hundreds--if not thousands--of techniques used to compromise both Windows and Unix-based systems. Malicious code and new exploit scripts are released on a daily basis, and each evolution becomes more and more sophisticated. Keeping up with the myriad of systems used by hackers in the wild is a formidable task, and scrambling to patch each potential vulnerability or address each new attack one-by-one is a bit like emptying the Atlantic with paper cup.If you're a network administrator, the pressure is on you to defend your systems from attack. But short of devoting your life to becoming a security expert, what can you do to ensure the safety of your mission critical systems? Where do you start?Using the steps laid out by professional security analysts and consultants to identify and assess risks, Network Security Assessment offers an efficient testing model that an administrator can adopt, refine, and reuse to create proactive defensive strategies to protect their systems from the threats that are out there, as well as those still being developed.This thorough and insightful guide covers offensive technologies by grouping and analyzing them at a higher level--from both an offensive and defensive standpoint--helping administrators design and deploy networks that are immune to offensive exploits, tools, and scripts. Network administrators who need to develop and implement a security assessment program will find everything they're looking for--a proven, expert-tested methodology on which to base their own comprehensive program--in this time-saving new book.

UTM Security with Fortinet IGI Global Looking to step into the Network Security field with the Fortigate firewall? Or are you required to manage a FortiGate NGFW for your organization? Then this is the right book for you! The FortiGate is an amazing device with many cybersecurity features to protect your network. If you are new to FortiGate's then this is the perfect book for you! This book will cover general overview of working with Fortinet. Also, you will gain a solid understanding on day to day administrative tasks. Next, you will learn how FortiGate interacts with various layer-2 protocol. Also you will get a chance how to filter network traffic and apply security policies which is very exciting. Lastly, you will learn about the session table and how Fortigate handles traffic. Below is a full list of what this book covers: Chapter One - Introduction to FortiGate-Identify platform features of FortiGate-Describe Security Processor Unit SPU-Identify factory defaults-Understand the different operational

modes-Understand FortiGate and FortiGuard Relationship-Manage administrator profiles-Manage administrative profiles-Manage network interfaces-Manage basic services-backup and restore config file-upgrade and downgrade firmware-Understand CLI structure-Understand GUI navigation-Initial ConfigurationChapter - 2 - Layer two technologies-Configuration of layer-2 VLANs-Describe VLANs and VLAN tagging process-Describe FortiOS Transparent Mode-Configure FortiOS Transparent Mode settings-Describe Transparent Mode Bridge Table-Describe MAC forwarding-Describe how to find MAC address on FortiOS-Describe Forwarding Domains-Describe and configure Virtual Switches-Describe Spanning Tree Protocol-Describe and Configure various NAT Mode layer-2 protocols-Describe and configure Layer-3 VLAN interface-Describe Virtual Wire Pairing-Describe and Configure VXLANChapter-3 Layer Three Technologies: -Configuration of Static Routes-implementation of Policy-Based Routes-Control traffic for well-known Internet Services-Interpret the FortiOS Routing Table-Understand FortiOS anti-spoofing mechanism-Implement route failover and floating route-Understand ECMP-Recognize active route vs standby route vs inactive routes-Use built in sniffer and diagnose flow debug tools, -Understand Session Table Entry.Chapter 4 - Firewall Policy and NAT-Identify components in Firewall Policy-Describe how traffic matches Firewall Policy Entries-Configure Firewall Policy Logging-Describe Policy GUI list views-Describe Policy ID's vs Policy Sequence numbers-Described where objects are referenced-Explain Name restrictions on Firewall Policies-Perform Firewall Policy re-ordering-Describe NAT and PAT-Explain different configuration modes for NAT-Configure and Describe SNAT and DNAT VIPs-Troubleshoot NAT issues

Network Security Assessment: From Vulnerability to Patch

John Wiley & Sons

This guide only contains practice questions and answers to the Fortinet Certified Network Security Professional exam.

Information assurance trends in vulnerabilities, threats, and technologies Routledge

Over the years, a plethora of reports has emerged that assess the causes, dynamics, and effects of cyber threats. This proliferation of reports is an important sign of the increasing prominence of cyber attacks for organizations, both public and private, and citizens all over the world. In addition, cyber attacks are drawing more and more attention in the media. Such efforts can help to better awareness and understanding of cyber threats and pave the way to improved prevention, mitigation, and resilience. This report aims to help in this task by assessing what we know about cyber security threats based on a review of 70 studies published by public authorities, companies, and research organizations from about 15 countries over the last few years. It answers the following questions: what do we know about the number, origin, and impact of cyber attacks? What are the current and emerging cyber security trends? And how well are we prepared to face these threats?

Cyber Forensics CRC Press

This book will take readers from the

discovery of vulnerabilities and the creation of the corresponding exploits, through a complete security assessment, all the way through deploying patches against these vulnerabilities to protect their networks. This is unique in that it details both the management and technical skill and tools required to develop an effective vulnerability management system. Business case studies and real world vulnerabilities are used through the book. It starts by introducing the reader to the concepts of a vulnerability management system. Readers will be provided detailed timelines of exploit development, vendors' time to patch, and corporate path installations. Next, the differences between security assessment s and penetration tests will be clearly explained along with best practices for conducting both. Next, several case studies from different industries will illustrate the effectiveness of varying vulnerability assessment methodologies. The next several chapters will define the steps of a vulnerability assessment including: defining objectives, identifying and classifying assets, defining rules of engagement, scanning hosts, and identifying operating systems and applications. The next several chapters provide detailed instructions and examples for differentiating vulnerabilities from configuration problems, validating vulnerabilities through penetration testing. The last section of the book provides best practices for vulnerability management and remediation.* Unique coverage detailing both the management and technical skill and tools required to develop an effective vulnerability management system* Vulnerability management is rated the #2 most pressing concern for security professionals in a poll conducted by Information Security Magazine* Covers in the detail the vulnerability management lifecycle from discovery through patch.

The Rise of Politically Motivated Cyber Attacks

Independently Published

The Art of Cyber Defense: From Risk Assessment to Threat Intelligence offers a comprehensive exploration of cybersecurity principles, strategies, and technologies essential for safeguarding digital assets and mitigating evolving cyber threats. This book provides invaluable insights into the intricacies of cyber defense, guiding readers through a journey from understanding risk assessment methodologies to leveraging threat intelligence for proactive defense measures. Delving into the nuances of modern cyber threats, this book equips readers with the knowledge and tools necessary to navigate the complex landscape of cybersecurity. Through a multidisciplinary approach, it addresses the pressing challenges organizations face in securing their digital infrastructure and sensitive data from cyber-attacks. This book offers comprehensive coverage of the most essential topics, including: Advanced malware detection and prevention strategies leveraging artificial intelligence (AI) Hybrid deep learning techniques for malware classification Machine learning solutions and research perspectives on Internet of Services (IoT)

security Comprehensive analysis of blockchain techniques for enhancing IoT security and privacy Practical approaches to integrating security analysis modules for proactive threat intelligence This book is an essential reference for students, researchers, cybersecurity professionals, and anyone interested in understanding and addressing contemporary cyber defense and risk assessment challenges. It provides a valuable resource for enhancing cybersecurity awareness, knowledge, and practical skills.

Blue Team Operations CRC Press

The instant access that hackers have to the latest tools and techniques demands that companies become more aggressive in defending the security of their networks. Conducting a network vulnerability assessment, a self-induced hack attack, identifies the network components and faults in policies, and procedures that expose a company to the damage caused by malicious network intruders. Managing a Network Vulnerability Assessment provides a formal framework for finding and eliminating network security threats, ensuring that no vulnerabilities are overlooked. This thorough overview focuses on the steps necessary to successfully manage an assessment, including the development of a scope statement, the understanding and proper use of assessment methodology, the creation of an expert assessment team, and the production of a valuable response report. The book also details what commercial, freeware, and shareware tools are available, how they work, and how to use them. By following the procedures outlined in this guide, a company can pinpoint what individual parts of their network need to be hardened, and avoid expensive and unnecessary purchases.

Managing A Network Vulnerability Assessment Independently Published

The NSE 7 Network Security Architect designation recognizes your advanced skills and ability to deploy, administer, and troubleshoot Fortinet security solutions. We recommend this course for network and security professionals who are involved in the design, administration, and support of security infrastructures using Fortinet solutions.

Decision Making and Security Risk Management for IoT Environments Packt Publishing Ltd

Threat actors, be they cyber criminals, terrorists, hacktivists or disgruntled employees, are employing sophisticated attack techniques and anti-forensics tools to cover their attacks and breach attempts. As emerging and hybrid technologies continue to influence daily business decisions, the proactive use of cyber forensics to better assess the risks that the exploitation of these technologies pose to enterprise-wide operations is rapidly becoming a strategic business objective. This book moves beyond the typical, technical approach to discussing cyber forensics processes and procedures. Instead, the authors examine how cyber forensics can be applied to identifying, collecting, and examining evidential data from emerging and hybrid technologies, while taking steps to proactively manage the influence and impact, as well as the policy and governance aspects of these technologies and their

effect on business operations. A world-class team of cyber forensics researchers, investigators, practitioners and law enforcement professionals have come together to provide the reader with insights and recommendations into the proactive application of cyber forensic methodologies and procedures to both protect data and to identify digital evidence related to the misuse of these data. This book is an essential guide for both the technical and non-technical executive, manager, attorney, auditor, and general practitioner who is seeking an authoritative source on how cyber forensics may be applied to both evidential data collection and to proactively managing today’s and tomorrow’s emerging and hybrid technologies. The book will also serve as a primary or supplemental text in both under- and post-graduate academic programs addressing information, operational and emerging technologies, cyber forensics, networks, cloud computing and cybersecurity.

Fortigate Security Pocket Guide Independently Published

Looking to step into the Network Security field with the Fortigate firewall? Or are you required to manage a FortiGate NGFW for your organization? Then this is the right book for you! The FortiGate is an amazing device with many cybersecurity features to protect your network. If you are new to FortiGate's then this is the perfect book for you! This book will cover general overview of working with Fortinet. Also, you will gain a solid understanding on day to day administrative tasks. Next, you will learn how FortiGate interacts with various layer-2 protocol. Also you will get a chance how to filter network traffic and apply security policies which is very exciting. Lastly, you will learn about the session table and how Fortigate handles traffic. Below is a full list of what this book covers: Chapter One - Introduction to FortiGate-Identify platform features of FortiGate-Describe Security Processor Unit SPU-Identify factory defaults-Understand the different operational modes-Understand FortiGate and FortiGuard Relationship-Manage administrator profiles-Manage administrative profiles-Manage network interfaces-Manage basic services-backup and restore config file-upgrade and downgrade firmware-Understand CLI structure-Understand GUI navigation-Initial ConfigurationChapter - 2 - Layer two technologies-Configuration of layer-2 VLANs-Describe VLANs and VLAN tagging process-Describe FortiOS Transparent Mode-Configure FortiOS Transparent Mode settings-Describe Transparent Mode Bridge Table-Describe MAC forwarding-Describe how to find MAC address on FortiOS-Describe Forwarding Domains-Describe and configure Virtual Switches-Describe Spanning Tree Protocol-Describe and Configure various NAT Mode layer-2 protocols-Describe and configure Layer-3 VLAN interface-Describe Virtual Wire Pairing-Describe and Configure VXLANChapter-3 Layer Three Technologies: -Configuration of Static Routes-implementation of Policy-Based Routes-Control traffic for well-known Internet Services-Interpret the FortiOS Routing Table-Understand FortiOS anti-spoofing

mechanism-Implement route failover and floating route-Understand ECMP-Recognize active route vs standby route vs inactive routes-Use built in sniffer and diagnose flow debug tools, -Understand Session Table Entry.Chapter 4 - Firewall Policy and NAT-Identify components in Firewall Policy-Describe how traffic matches Firewall Policy Entries-Configure Firewall Policy Logging-Describe Policy GUI list views-Describe Policy ID's vs Policy Sequence numbers-Described where objects are referenced-Explain Name restrictions on Firewall Policies-Perform Firewall Policy re-ordering-Describe NAT and PAT-Explain different configuration modes for NAT-Configure and Describe SNAT and DNAT VIPs-Troubleshoot NAT issues

Fortinet NSE8 - Network Security Expert Written Exam – New version (NSE8_812) G Skills

The purpose of this capstone project was to identify and understand gaps and weaknesses that hinder U.S. corporations' and government agencies' abilities to accurately analyze and characterize cyber threats. In order to achieve the purpose of this capstone project, the study focused on identifying common foundational characteristics, unique categorical differences between cybercrime and cyber warfare types of attacks, and analysis of modern vulnerability and threat assessment models. The research question posed was whether or not current vulnerability and threat assessment models can facilitate and accommodate for nation state types of cyber-attack assessments. Through examination of the literature it is concluded that while both common foundational and unique characteristic attributes do exist and can be identified, there's no formal legal framework the government has developed to truly address cybercrime and cyber warfare types of cyber threats. Additionally, this capstone project highlights the different approaches corporate and governmental security personnel undertake to assess their respective levels of threat and vulnerabilities demonstrate a lack of common cohesion. Therefore, readers can further deduce neither U.S. corporations, nor government agencies possess an adequate capability to accurately determine their respective levels of risk for experiencing either a cybercrime or cyber warfare type of attack. Keywords: Cybersecurity, Professor Albert Orbinati, computer, network, crime, war, law.

NSE4 Study Guide Part-II Infrastructure Rowman & Littlefield

The Network Security Professional designation recognizes your ability to install and manage the day-to-day configuration, monitoring, and operation of a FortiGate device to support specific corporate network security policies.Fortinet's NSE4 actual exam material brought to you by group of certification experts.

Scalable Framework for Cyber Threat Situational Awareness CRC Press

"Scalable Framework for Cyber Threat Situational Awareness" is a comprehensive and practical guide that explores the development and implementation of a scalable framework for achieving effective cyber threat situational awareness. Authored by cybersecurity experts and researchers, this book serves as a valuable resource for security

professionals, analysts, and decision-makers seeking to enhance their understanding of cyber threats and improve their response capabilities. In this book, the authors address the critical need for organizations to establish robust situational awareness capabilities to detect, analyze, and respond to cyber threats in real-time. They present a scalable framework that integrates various data sources, analysis techniques, and visualization tools to provide a holistic view of the evolving threat landscape. Key topics covered in this book include: Introduction to cyber threat situational awareness: The authors provide an overview of the concept of cyber threat situational awareness, its importance in modern cybersecurity, and the challenges faced in achieving comprehensive awareness in dynamic and complex environments. Scalable framework architecture: The book presents the architecture of a scalable framework for cyber threat situational awareness. It covers the integration of diverse data sources, including network logs, intrusion detection systems, threat intelligence feeds, and user behavior data. The authors discuss the design principles and components necessary for building a scalable and adaptable framework. Data collection and aggregation: The authors delve into the process of collecting and aggregating data from various sources within the organization and external feeds. They explore techniques for data normalization, filtering, and enrichment to ensure the availability of high-quality data for analysis. Threat detection and analysis: The book covers advanced analytics techniques and algorithms for detecting and analyzing cyber threats. It explores anomaly detection, machine learning, and behavioral analysis approaches to identify patterns, indicators, and potential threats within the data. Visualization and reporting: The authors discuss visualization tools and techniques for presenting cyber threat information in a meaningful and intuitive manner. They highlight the importance of visualizing complex data to aid in decision-making, incident response, and collaboration among security teams. Incident response and mitigation: The book explores strategies for incident response and mitigation based on the insights gained from the cyber threat situational awareness framework. It covers incident triage, prioritization, and response coordination to ensure timely and effective actions against identified threats. Scalability and adaptability: The authors address the scalability and adaptability considerations of the framework, enabling organizations to handle large volumes of data, accommodate evolving threats, and integrate new data sources and analysis techniques. Integration with existing security systems: The book provides guidance on integrating the cyber threat situational awareness framework with existing security systems, such as security information and event management (SIEM) platforms, intrusion detection systems (IDS), and security orchestration, automation, and response (SOAR) tools. Emerging trends and future directions: The authors

discuss emerging trends and technologies in cyber threat situational awareness, including threat intelligence sharing, collaborative defense, and leveraging artificial intelligence (AI) and machine learning (ML) for automated threat analysis.

Nse 4 Createspace Independent Publishing Platform

According to the FBI, about 4000 ransomware attacks happen every day. In the United States alone, victims lost $209 million to ransomware in the first quarter of 2016. Even worse is the threat to critical infrastructure, as seen by the malware infections at electrical distribution companies in Ukraine that caused outages to 225,000 customers in late 2015. Further, recent reports on the Russian hacks into the Democratic National Committee and subsequent release of emails in a coercive campaign to apparently influence the U.S. Presidential Election have brought national attention to the inadequacy of cyber deterrence. The U.S. government seems incapable of creating an adequate strategy to alter the behavior of the wide variety of malicious actors seeking to inflict harm or damage through cyberspace. This book offers a systematic analysis of the various existing strategic cyber deterrence options and introduces the alternative strategy of active cyber defense. It examines the array of malicious actors operating in the domain, their methods of attack, and their motivations. It also provides answers on what is being done, and what could be done, by the government and industry to convince malicious actors that their attacks will not succeed and that risk of repercussions exists. Traditional deterrence strategies of retaliation, denial and entanglement appear to lack the necessary conditions of capability, credibly, and communications due to these malicious actors' advantages in cyberspace. In response, the book offers the option of adopting a strategy of active cyber defense that combines internal systemic resilience to halt cyber attack progress with external disruption capacities to thwart malicious actors' objectives. It shows how active cyber defense is technically capable and legally viable as an alternative strategy for the deterrence of cyber attacks.

Introduction to FortiGate Part-II Infrastructure Springer Nature

This professional guide and reference examines the challenges of assessing security vulnerabilities in computing infrastructure. Various aspects of vulnerability assessment are covered in detail, including recent advancements in reducing the requirement for expert knowledge through novel applications of artificial intelligence. The work also offers a series of case studies on how to develop and perform vulnerability assessment techniques using start-of-the-art intelligent mechanisms. Topics and features: provides tutorial activities and thought-provoking questions in each chapter, together with numerous case studies; introduces the fundamentals of vulnerability assessment, and reviews the state of the art of research in this area; discusses vulnerability assessment frameworks, including frameworks for industrial control and cloud systems; examines a range of applications that make use of artificial

intelligence to enhance the vulnerability assessment processes; presents visualisation techniques that can be used to assist the vulnerability assessment process. In addition to serving the needs of security practitioners and researchers, this accessible volume is also ideal for students and instructors seeking a primer on artificial intelligence for vulnerability assessment, or a supplementary text for courses on computer security, networking, and artificial intelligence.

Fortinet Certified Network Security Professional

Apress

Welcome to our Exclusive Fortinet NSE 8 - Network Security Expert Written Exam preparation book, designed to help you ace the real NSE 8 exam on your first attempt. This book is your ultimate resource for testing your knowledge, practicing with actual exam questions, and saving both time and money. Our book offers the latest questions, comprehensive explanations, and valuable references for all the topics covered in the Fortinet NSE 8 - Network Security Expert Written Exam (NSE8_812). By enrolling in this book, you'll boost your confidence and readiness to tackle the actual exam, as you'll be thoroughly assessing your skills across the required subjects. To pass the official Fortinet NSE 8 - Network Security Expert Written Exam on your first try, it's essential to put in the hard work, and our book provides updated information aligned with the entire exam syllabus. Achieving the NSE 8 Certification signifies your in-depth knowledge of network security design, configuration, and troubleshooting for complex networks. However, please note that to attempt the exam, candidates must possess relevant industry experience. We recommend completing the necessary Professional, Analyst, Specialist, and Architect designation training and gaining extensive hands-on experience with Fortinet products in a production environment. The written exam consists of questions related to design scenarios with exhibits, configuration extracts, and troubleshooting situations, all designed to evaluate your expertise in security networking and Fortinet solutions. Remember that reference materials are not allowed in the exam room. Key details about the NSE 8 - Network Security Expert 8 Written Exam (NSE8_812) include: Number of questions: 60 Time allowed: 120 minutes Scoring: Answers must be 100% correct for credit; there's no partial credit or deduction for incorrect answers. You'll receive a document indicating pass or fail, along with your performance in each exam section. Question types: Multiple choice and multiple select Time required between exam retakes: 15 days Retesting: You cannot retake an exam version you've already passed. Recertification: If you're seeking to renew your NSE 8 certification, schedule the written exam no more than six months before your current certification's expiration date. Keep in mind that passing both the written and practical exams is necessary to obtain NSE 8 certification. Welcome aboard, and let's work together to help you succeed in the Fortinet NSE 8 - Network Security Expert Written Exam!

The Art of Cyber Defense

DIANE Publishing

Central to computer

security are detecting attacks against systems and managing computer systems to mitigate threats to the system. Attacks exploit vulnerabilities in the system such as a programming flaw. Threats are vulnerabilities which could lead to an attack under certain circumstances. The key to the detection of attacks is discovering an ongoing attack against the system. Mitigating threats involves a continuous assessment of the vulnerabilities in the system and of the risk these vulnerabilities pose with respects to a security policy. Intrusion detection systems (IDS) are programs which detect attacks. The goal is to issue alerts only when an actual attack occurs, but also to not miss any attacks. The biological immune system provides a compelling model on which to base an IDS. This work adds the biological concepts of positive selection and collaboration to artificial immune systems to achieve a better attack detection rate without unduly raising the false alarm rate. Attack graphs assess the threat to the system by showing the composition of vulnerabilities in the system. The key issues with attack graphs are to large networks, ease of coding new attacks into the model, incomplete network information, visualization of the graph and automatic analysis of the graph. This work presents an abstract class model that aggregates individual attacks into abstract classes. Through these abstractions, scalability is greatly increased and the codification of new attacks into the model is made easier when compared to the current approach that models each attack. Clustering of identical machines is used to reduce the visual complexity of the graph and also to increase scalability. Incomplete network information is handled by allowing "what if" evaluations where an administrator can hypothesize about the existence of certain vulnerabilities in the system and investigate their consequences.