Mile2 Certified Penetration Testing Engineer

Windows Server 2019 wurde für den praktischen Einsatz in modernen Computernetzwerken entwickelt. Damit Sie sich umgehend mit dem neuen Betriebssystem vertraut machen können, finden Sie in diesem Buch einen kompakten Überblick zu den wichtigsten, in Windows Server 2019 enthaltenen Rollen und Features einschließlich der praxisrelevanten Neuerungen und Verbesserungen. Neben der Installation des Betriebssystems erhalten Sie zudem einen leichten Einstieg in Themen wie die Active Directory-Domänendienste, die Virtualisierung mit Hyper-V, die Datei- und Speicherdienste - mitsamt der neuen Speichermigrationsdienste - oder auch die Windows PowerShell. Windows Server 2019 als Server Core wird hierin ebenso detailliert vorgestellt, wie auch das neue Windows Admin Center (WAC) als zentrale Konsole für die Verwaltung selbst hybrider Serverfarmen. Das Buch ist die 5. - erweiterte - Ausgabe des zu Beginn noch von Addison-Wesley veröffentlichten, erfolgreichen Fachbuches zu den Windows-Serverbetriebssystemen von Carlo Westbrook. Die im Buch enthaltenen Schritt-für-Schritt-Anleitungen rund um die Installation, Aktualisierung, Migration, Verwaltung und Wartung von Windows Server 2019 ermöglichen einen schnellen und praktischen Einstieg. Aus dem Inhalt - Einführung und Neuerungen in Windows Server 2019 - Installation, Aktualisierung und Migration - Navigation und (Remote-)Verwaltung - Einführung in die Verwaltung mit Windows PowerShell - Bereitstellen und Verwalten von Rollen und Features - Windows Server 2019 im Netzwerk - Netzwerkinfrastrukturdienste in Windows Server 2019 - Windows Server 2019 und die Active Directory-Domänendienste - Druck- und Dokumentdienste unter Windows Server 2019 - Einführung in die Virtualisierung mit Hyper-V - Windows Server 2019 als Server Core und Nano-Server - Windows Subsystem for Linux (WSL) unter Windows Server 2019 - Systemüberwachung und Fehlerbehebung - Sichern und Wiederherstellen Buch+ - Erweiterte Inhalte zum Buch (u. a. die Liste aller im Buch verwendeten Links, Beispiel-Skripts, usw.) stehen Online zum kostenfreien Abruf bereit!
????????????,????Windows??????????,?????Windows????????????????????????????,?????Windows????????????????? ????????,??Rootkits????

CPTE: Certified Penetration Testing Engineer hard copy workbook and e-course materials

"The Certified Penetration Testing Engineer (CPTE) is a vendor-neutral certification offered by Mile2 for aspiring penetration testing engineers who are looking to enhance their hands-on experience regarding the penetration testing methodologies used by the industry professionals. The course also covers the five key elements of penetration testing, namely; information gathering, scanning, enumeration, exploitation and reporting. These five key elements form a basis of discovering the vulnerabilities in a given system. The Certified Penetration Testing Engineer (CPTE) course enhances the business skills needed to identify protection opportunities, justify testing activities and optimize security controls to reduce risk associated with working with the internet. The course utilizes the latest tools, such as Saint, Metasploit through Kali Linux and Microsoft PowerShell. "--Resource description page.

????????????????????????????????,?????????,????????????????????

Get hands-on experience on concepts of Bug Bounty Hunting Key Features Get well-versed with the fundamentals of Bug Bounty Hunting Hands-on experience on using different tools for bug hunting Learn to write a bug bounty report according to the different vulnerabilities and its analysis Book Description Bug bounty programs are the deals offered by prominent companies where-in any white-hat hacker can find bugs in the applications and they will have a recognition for the same. The number of prominent organizations having this program has increased gradually leading to a lot of opportunity for Ethical Hackers. This book will initially start with introducing you to the concept of Bug Bounty hunting. Then we will dig deeper into concepts of vulnerabilities and analysis such as HTML injection, CRLF injection and so on. Towards the end of the book, we will get hands-on experience working with different tools used for bug hunting and various blogs and communities to be followed. This book will get you started with bug bounty hunting and its fundamentals. What you will learn Learn the basics of bug bounty hunting Hunt bugs in web applications Hunt bugs in Android applications Analyze the top 300 bug reports Discover bug bounty hunting research methodologies Explore different tools used for Bug Hunting Who this book is for This book is targeted towards white-hat hackers, or anyone who wants to understand the concept behind bug bounty hunting and understand this brilliant way of penetration testing. This book does not require any knowledge on bug bounty hunting.

?? ????????????????? ?? ?????????????????????????? ???