1. Record Nr. UNINA9910338004803321

Autore	Hosmer Chet
Titolo	PowerShell and Python Together : Targeting Digital Investigations / / by Chet Hosmer
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2019
ISBN	1-4842-4504-0
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (223 pages)
Disciplina	005.282
Soggetti	Data protection Python (Computer program language) Data and Information Security Python
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Chapter 1: An Introduction to PowerShell for Investigators -- Chapter 2: PowerShell Pipelining -- Chapter 3: PowerShell Scripting Targeting Investigation -- Chapter 4: Python and Live Investigation/Acquisition -- Chapter 5: PowerShell / Python Investigation Example -- Chapter 6: Launching Python from PowerShell -- Chapter 7: Loose Ends and Future Considerations -- Appendix: Challenge Problem Solutions -- .
Sommario/riassunto	Bring together the Python programming language and Microsoft’s PowerShell to address digital investigations and create state-of-the-art solutions for administrators, IT personnel, cyber response teams, and forensic investigators. You will learn how to join PowerShell's robust set of commands and access to the internals of both the MS Windows desktop and enterprise devices and Python's rich scripting environment allowing for the rapid development of new tools for investigation, automation, and deep analysis. PowerShell and Python Together takes a practical approach that provides an entry point and level playing field for a wide range of individuals, small companies, researchers, academics, students, and hobbyists to participate. What You’ll Learn: Leverage the internals of PowerShell for: digital investigation, incident response, and forensics Leverage Python to exploit already existing PowerShell CmdLets and aliases to build new automation and analysis

capabilities Create combined PowerShell and Python applications that provide: rapid response capabilities to cybersecurity events, assistance in the precipitous collection of critical evidence (from the desktop and enterprise), and the ability to analyze, reason about, and respond to events and evidence collected across the enterprise.