Course Title:

Offense For Defense

INSTRUCTORS:

Security Consultant Jason Downey

Description: Welcome to "Offense for Defense," a specialized course tailored for information security blue teamers, or defenders, aiming to fortify their skills in offensive security strategies. Throughout this program, participants will delve into the fundamentals of offensive security, gaining insight into the tactics, techniques, and procedures employed by adversaries. By understanding the attacker's mindset and methodologies, defenders will be better equipped to anticipate and defend against common cyber threats effectively. Through practical exercises and real-world scenarios, participants will learn to proactively identify vulnerabilities, assess risks, and implement robust defensive measures to safeguard against potential attacks. Join us as we empower defenders with the knowledge and tools needed to strengthen their cybersecurity posture and protect critical assets from evolving threats.

COURSE OUTLINE	
Introduction	Learn the value of offensive knowledge in strengthening defensive strategies. Understand the psychology and tactics of attackers to better defend against them.

Implementing Defensive Speedbumps	Discover techniques to slow down attackers, making it harder for them to navigate your systems undetected.
Utilizing Simulation Tools	Gain hands-on experience with Atomic Red Team and the MITRE ATT&CK framework to simulate attacks and test defenses.
Attack Methodologies	Dive into various attack vectors such as password attacks, phishing, and exploitation tactics to understand how attackers gain access.
Password Security and Persistence Mechanisms	Explore how attackers guess passwords and implement persistence, and learn strategies for securing credentials and detecting persistence.
Lateral Movement and Advanced Persistence	Learn to identify and block lateral movement within networks and understand advanced persistence techniques used by attackers.
Securing Service Accounts and Delegation	Understand the risks associated with service accounts and delegation and learn how to secure them against exploitation.
Active Directory and AD Certificate Services Security	Delve into securing Active Directory, identifying common misconfigurations, and understanding AD Certificate Services' vulnerabilities.
Hands-On Workshops	Each key section includes practical exercises, allowing participants to apply what they've learned in simulated

	environments to reinforce their understanding and skills.
Course Conclusion	Summarize key takeaways, engage in an open Q&A to clarify doubts, and discuss strategies for continued learning in cybersecurity defense.