GIAC Penetration Tester Certification

Zetlan Technologies

ZETLAN TECHNOLOGIES

www.zetlantech.com

Online Course

Learn Without leaving Home!!

Course Modules

1. **Advanced Password Attacks**
   Additional methods to attack password hashes and authenticate.

2. **Attacking Password Hashes**
   Obtain and attack password hashes and other password representations.

3. **Azure Applications and Attack Strategies**
   Understanding of Azure applications and the attacks against them including federated and single sign-on environments and Azure AD authentication protocols

4. **Azure Overview, Attacks, and AD Integration**
   Understanding of Azure Active Directry implemntatn fundamentals, common Azure AD attacks, and Azure authentication techniques

Zetlan Technologies

5. Domain Escalation and Persistence Attacks

Understanding of common Windows privilege escalation attacks and Kerberos attack techniques that are used to consolidate and persist administrative access to Active Directory.

6. Escalation and Exploitation

Fundamental concepts of exploitation, data exfiltration from compromised hosts and pivoting to exploit other hosts within a target network.

7. Exploitation Fundamentals

Fundamental concepts associated with the exploitation phase of a pentest.

8. Kerberos Attacks

Zetlan Technologies

Understanding of attacks against Active Directory including Kerberos attacks.

9. Metasploit

Configure the Metasploit Framework at an intermediate level.

10. Moving Files with Exploits

Exploits to move files between remote systems.

11. Password Attacks

Understand types of password attacks, formats, defenses, and the circumstances under which to use each password attack variation. The candidate will be able to conduct password guessing attacks.

12. Password Formats and Hashes

Understanding of common password hashes and formats for storng password data.

13. Penetration Test Planning

Fundamental concepts associated with pen-testing, and utilize a process-oriented approach to penetration testing and reporting.

Zetlan Technologies

14. Penetratn Testng with PowerShell & the Windows Command Line

Understandg of the use of advanced Windows command line skills during a penetration test, and demonstrate an understanding of the use of advanced Windows Power Shell skills during a penetration test.

15. Reconnaissance

Fundamental concepts of reconnaissance and will understand how to obtain basic, high level information about the target organization and network, often considered information leakage, including but not limited to technical and non-technical public contacts, IP address ranges, document formats, and supported systems.

16. Scanning and Host Discovery

Appropriate technique to scan a network for potential targets, and to conduct port, operating system & service version scans & analyze the results.

17. Vulnerability Scanning

Conduct vulnerability scans and analyze the results.

Zetlan Technologies

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474