GIAC Exploit Researcher and Advanced Penetration Tester

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1. **Accessing the Network**

   Understanding of how to bypass network access control systems.

2. **Advanced Fuzzing Techniques**

   Able to develop custom fuzzing test sequences using the Sulley framework, measure code coverage in fuzzing, identfy the limitations of fuzzing, and identify ways to improve a fuzzer.

3. **Advanced Stack Smashing**

   Demonstrate an understanding of how to write advanced stack overflow exploits against canary-protected programs and ASLR.

4. **Client Exploitation and Escape**

   Demonstrate an understandg of bypassing or exploiting restricted Windows or Linux client environments, and exploiting or interacting with client environments using tools like Powershell.

GIAC Exploit Researcher and Advanced Penetration Tester

5. Crypto for Pen Testers

Able to attack and exploit common weaknesses in cryptographic implementations.

6. Exploiting the Network

Demonstrate an understanding of how to exploit common vulnerabilities in modern networks attacking client systems and common network protocols.

7. Fuzzing Introduction and Operation

Demonstrate an understanding of the benefits and practical app of protocol fuzzing to identify flaws in target software systems.

8. Introduction to Memory and Dynamic Linux Memory

Demonstrate a basic understanding of X86 processor architecture, Linux memory management, assembly and the linking and loading process.

9. Introduction to Windows Exploitation

Demonstrate an understandg of Windows constructs required for exploitation and the most common OS and Compile-Time Controls.

10. Manipulating the Network

Demonstrate an understanding of how to manipulate common network systems to gain escalated privileges and the opportunity to exploit systems.

11. Python and Scapy For Pen Testers

Demonstrate an understanding of the ability to read and modify Python scripts & packet crafting using Scapy to enhance functionality as required during a penetration test.

12. Shellcode

Demonstrate the ability to write shellcode on the Linux operating system, & demonstrate an understanding of the Windows shellcode methodology.

13. Smashing the Stack

Demonstrate an understanding of how to write basic exploits against stack overflow vulnerabilities.

14. Windows Overflows

Demonstrate an understanding of how to exploit Windows vulnerabilities on the stack, and bypass memory protections.

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