BLACKHAT
ETHICAL HACKING

www.blackhatethicalhacking.com

PROGRAMMING LANGUAGES FOR OFFENSIVE SECURITY

Offensive Security is a field that requires a wide range of technical skills, including programming. Knowing how to code using variety of programming languages can be incredibly useful for identifying and exploiting vulnerabilities, developing custom tools, and automating tasks.

SWIPE →

BASH LANGUAGE

(Unix Shell)

Bash is a powerful shell scripting language that is commonly used on Unix-like systems. It is well-suited for automating tasks such as file manipulation, text processing, and system administration. Bash is also a popular language for offensive security, as it can be used to write shellcode and execute system commands.

THE GO LANGUAGE

(A Compiled Language for
Scalable Applications)

Go is a compiled programming language designed for building scalable and efficient applications. It is known for its built-in concurrency support, making it ideal for building highly parallel systems. Go is a good choice for offensive security when developing high-performance tools such as network scanners or password cracking applications.

PYTHON LANGUAGE

(A High-level, Interpreted Language for General-purpose Programming)

Python is a popular interpreted language that is often used for general-purpose programming, scientific computing, and data analysis. Its syntax is easy to learn, and it has a large community of users and libraries available. Python is well-suited for offensive security, as it can be used to write tools for password cracking, network scanning, and other security-related tasks.

LUA LANGUAGE

(A Lightweight Scripting Language for Embedding)

Lua is a lightweight, fast, and powerful scripting language designed for embedding in apps. It is known for its simplicity, ease of use, and flexibility, making it a popular choice for game development, scripting in various applications, and other embedded use cases. Lua is a good choice for offensive security when developing custom scripts for network scanning, malware analysis, or other security tasks. Nmap is a great example that uses NSE scripts written in Lua.

C/C++ LANGUAGE

C and C++ are low-level languages that provide fine-grained control over system resources and hardware. These languages are often used in the development of exploits and custom malware, as well as in the reverse engineering of binaries and firmware.

ASSEMBLY LANGUAGE

Assembly language is the lowest-level language that can be used to write code for a computer. While it is less commonly used than higher-level languages like Python and C, it is an essential tool for offensive security professionals who need to understand how a system works at the hardware level.

POWERSHELL LANGUAGE

PowerShell is a command-line shell and scripting language developed by Microsoft. It is particularly well-suited for offensive security on Windows systems, as it provides easy access to system resources and can be used to automate tasks such as lateral movement and privilege escalation.

CONCLUSION

A solid understanding of programming languages is essential for success in offensive security. While the languages we've covered in this example are by no means the only ones used in offensive security, they are certainly among the most popular and versatile, also used by us. By learning these languages and understanding their strengths and weaknesses, you can build a powerful toolkit for identifying and exploiting vulnerabilities, developing custom tools and scripts, and automating tasks in your offensive security operations.