



ویستا فن آوری فردا

مشاوره، اجرا، تامین و ارائه تجهیزات
آموزش دوره های تخصصی IT، مخابرات، مدیریت
شناسه ملی: ۱۴۰۰۷۲۹۶۴۲۹

مقدمه:

پایتون یک زبان برنامه نویسی سطح بالا است که در تمامی زمینه های کامپیوتری بسیار محبوب شده و شرکت هایی مثل گوگل سرمایه گذاری های عظیمی روی توسعه این زبان برنامه نویسی کرده اند به طور مثال بخش هایی از موتور جستجو شرکت گوگل با این زبان توسعه یافته است.

پایتون از قدرت فوق العاده ای برخوردار است و با توجه به اینکه به زبان گفتاری انسان شبیه است این امکان را فراهم می کند تا به سرعت سناریو ای که در ذهن داریم را تست کنیم و کد کمتری بزنییم و نتیجه سریع تری داشته باشیم و به جای اینکه زمان را بر روی توسعه برنامه و کد زدن هدر دهیم روی ایده های بیشتری کار کنیم.

این ویژگی زبان پایتون بسیار مورد توجه کارشناسان امنیتی قرار گرفته زیرا امکان توسعه سریع و تست سریع حملات سایبری را می دهد و زمان انجام کار را کاهش می دهد. به همین دلیل بسیاری از اکسپلویت هایی که این روز های توسط کارشناسان امنیت نوشته می شود به زبان پایتون هستند.

پایتون تعداد زیادی ماژول و ابزارهای قدرتمند آماده برای بحث امنیت شبکه، تست نفوذ، تست وب اپلیکیشن ها ، مهندسی معکوس و ... دارد و با استفاده از این ابزارها می توانیم تحقیقات امنیتی ، تست نفوذ و حملات سایبری را با سرعت بیشتر و بسیار بی دردسر تر انجام داد.

پایتون بسیار آسان است و چه برنامه نویسی بدانید و چه ندانید در مدت زمان کوتاهی می توانید برنامه نویس با این زبان فوق العاده جالب را یاد بگیرید. در این دوره ما سعی می کنیم شما را با این زبان فوق العاده آشنا کنیم تا لذت کار با یک زبان فوق مدرن را تجربه کنید.

در کار ما فلسفه این است که کارهای تکراری انجام نشود و به جای اینکه تمرکز روی نوشتن کد های بهتر باشد تمرکز روی انجام کار و ایده های جدید باشد. در این دوره ما ابتدا از پایه زبان پایتون را شناخته و سپس از آن برای بحث های امنیت شبکه و برنامه نویسی سیستم در محیط لینوکس و یونیکس استفاده خواهیم کرد.



ویستا فن آوری فردا

مشاوره، اجرا، تامین و ارائه تجهیزات
آموزش دوره های تخصصی IT، مخابرات، مدیریت
شناسه ملی: ۱۴۰۰۷۲۹۶۴۲۹

پیشنیاز:

آشنایی با مفاهیم شبکه های کامپیوتری و TCP/IP

آشنایی مختصر با سیستم عامل Linux

CEH

سرفصل ها:

Module 1: Python Scripting – Language Essentials

- Introduction to Interpreted Languages and Python
- Data Types and variables
- Operators and Expressions
- Program Structure and Control
- Functions and Functional Programming
- Classes, Objects and other OOPS concepts
- Modules, Packages and Distribution
- Python in Linux and Unixes
- Python in Windows
- Python in Mobiles: iPhone and Androids
- Python in Embedded Devices: Routers
- Program Portability
- Lab Exercises

Module 2: System Programming and Security



ویستا فن آوری فردا

مشاوره، اجرا، تامین و ارائه تجهیزات
آموزش دوره های تخصصی IT، مخابرات، مدیریت
شناسه ملی: ۱۴۰۰۷۲۹۶۴۲۹

- I/O in Python
- File and Directory Access
- Multithreading and Concurrency
- Inter Process Communication (IPC)
- Permissions and Controls
- Case Studies
- Lab Exercises

Module 3: Network Security Programming – Sniffers and Packet Injectors

- Raw Socket basics
- Socket Libraries and Functionality
- Programming Servers and Clients
- Programming Wired and Wireless Sniffers
- Programming arbitrary packet injectors
- PCAP file parsing and analysis
- Case Studies
- Lab Exercises

Module 4: Web Application Security

- Web Servers and Client scripting
- Web Application Fuzzers
- Scraping Web Applications – HTML and XML file analysis
- Web Browser Emulation
- Attacking Web Services
- Application Proxies and Data Mangling
- Automation of attacks such as SQL Injection, XSS etc.
- Case Studies
- Lab Exercises

Module 5: Exploitation Techniques



ویستا فن آوری فردا

مشاوره، اجرا، تامین و ارائه تجهیزات
آموزش دوره های تخصصی IT، مخابرات، مدیریت
شناسه ملی: ۱۴۰۰۷۲۹۶۴۲۹

- Exploit Development techniques
- Immunity Debuggers and Libs
- Writing plugins in Python
- Binary data analysis
- Exploit analysis Automation
- Case Studies
- Lab Exercises

Module 6: Malware Analysis and Reverse Engineering

- Process Debugging basics
- Pydbg and its applications
- Analyzing live applications
- Setting breakpoints, reading memory etc.
- In-memory modifications and patching
- Case Studies
- Lab Exercises