SANS EMEA

cyberstart essentials

#cyberdisc

cyberstart essentials

What is it?

CyberStart Essentials is an online learning platform with over one hundred hours of content and labs, designed to teach computer, hardware, network and security fundamentals. The platform, which is a part of the CyberDiscovery programme, features text, video, mini podcasts and virtualised lab exercises, resulting in a fun and captivating student experience. Every module ends with a quiz, designed to test students' comprehension of the content, but also their ability to research and apply their knowledge of the topic beyond what is covered in CyberStart Essentials.

What problem does it solve?

As has been widely reported, there is currently a significant global shortage of cyber security practitioners. For many governments, it is therefore a top priority to develop new talent through retraining and encouraging young adults to engage with the profession. There are, however, numerous challenges in achieving this on a large scale, including talent identification and delivering the right foundational knowledge for students to study.

What does it teach?

Cyber security has a vast number of disciplines, with many different specialist skill areas underneath the high-level banners of offensive, defensive and forensic. SANS, as the world's largest trainer of technical cyber security skills in both breadth and depth, consistently observes that certain foundation knowledge makes grasping security concepts and skills significantly easier. In order to grasp how to forensically unpick modern technology to reconstruct a crime, or to find flaws in software that attackers might exploit, the components on which this technology runs must be understood. CyberStart Essentials focuses on this challenge.

During CyberStart Essentials students learn the role of a CPU, how it executes code, its relationship with memory and the fundamentals of how attackers disrupt intended behaviours. Protocols and constructs behind networks are also taught, including the inner workings of packets and protocols that allow the internet to function. CyberStart Essentials covers key concepts and terms, dramatically increasing students' rapid and successful progression to deeper cyber security study.

How does it work?

Many of the concepts that need to be learnt before pursuing the more 'fun' aspects of cyber security can involve moderately in-depth learning and seemingly arbitrary study to newcomers. CyberStart Essentials provides this crucial content but always with relevance to current cyber security, weaving fun security tasks and concepts into the theory. Modules are stacked so that concepts are progressively built up and detailed understanding is developed. Students study a diverse set of topics that slowly increase in difficulty until they grasp that concept, rather than overloading them with information on a single topic. The platform also features web-based access to virtualised labs, enabling students to get hands on with new Linux commands or security problems without the difficulty of setting up infrastructure. This significantly reduces the barrier to entry and allows for transition between theory and hands-on exercises for a more engaging student experience.

Find out more

www.joincyberdiscovery.com

@CyberDiscUK

The curriculum

Computer Hardware

Motherboard / Processor / RAM / Storage / GPU / Input Devices / Output Devices / Heatsink / Power Supply / CPU Components / CPU Registers / Fetch, Decode & Execute / The Stack & The Heap / File Systems / Fat32 & ExFAT / NTFS / Ext3 & Ext4 / HFS & APFS

Data

Bits / Alternate Number Bases / Binary / Hexadecimal / ASCII / File headers / Logic / Logical Concepts - AND/ OR/NOT/NAND/NOR/XOR / Applied Logic

Encryption

Concepts / Encryption vs encoding / Symmetric encryption / Asymmetric encryption / How HTTPS works / Hashing

Exploitation

Command Injection / Cross Site Scripting / File Inclusion / SQL Injection / Session Guessing / ClickJacking / CSRF / Directory Traversal / File Upload Flaws / Concept: Vulnerability scanners / GDB & Debugging / Debugging Concepts / Integer Overflow / Buffer Overflows / Buffer Overflows with Shellcode / Buffer Overflow Mitigations / Existing Exploits / Walkthrough: Exploiting an FTP service / Exploiting a Web Application / Metasploit / Patch Cycles & Support, How They Connect To Exploitation / Social Engineering / Phishing / Drive by Download / Credential Harvesting / High Value Target Phishing

Google

How Search Works / Commands & Colons / Wildcards & Quotes / Calculator / Troubleshooting / Alternative Search Mechanisms

Kali

Kali Introduction / Installing Kali / Wordlists / Kali-SSH / Finding Tools

Linux

What is Linux / Installing Linux / Navigating the GUI / Linux Networking GUI / The Terminal / The Superuser / Navigating in the terminal / Folder structure / File Permissions / Hidden Files / Environment Variables / Tab Completion / Previous Commands / History / Parameters / Interrupts / Clearing the terminal / The cp command / The mkdir command / The mv command / The rm command / The cat command / The less command / The find command / Grep / Which / Apropos / Nano / Vim / File / Strings / Wget / Processes / Pipes & Redirects / The Passed File / Scheduled Tasks / Package Managers / Packages / Source / SSH

Networking

Types of Networks / Network Hardware / IP Addresses / MAC Addresses / Packets / Protocols / TCP Protocol / UDP Protocol / IP Addresses / Subnets / TCP Protocol / UDP Protocol / Web servers / HTTP Protocol / HTML / Javascript / PHP / Cookies & Localstorage / Email / SMTP Protocol / POP3, IMAP & Exchange / Email Spoofing - DKIM & SPF / DNS / TLD / Forward & Recursive Lookup / Recursive & Iterative Lookup / DNS Records / ICMP / DHCP / OSI / TCPIP / Packet Headers / ARP

Operating Systems

What is an Operating System / What is the Kernel / What is a Process / What is an Interrupt / What is the BIOS / Boot Loaders

Privilege Escalation

Why Privelege Escalation / Exploiting Services / Kernel Exploits / Wildcard Injection / SUID Files / Sudo / Windows Permissions / Bypass UAC / Kernel Exploits / Stored Credentials / Unquoted Service Paths / The Registry / Folder Permissions / Always Install Elevated

Programming

What is a computer program / Programming languages / Running python programs / Printing in Python / What are Variables / Variables in Python / Maths in Python / Functions in Python / Comments in Python / Type Conversion in Python / Character sequence and escapes in Python / User input in Python / Conditionals in Python / Arrays in Python / Loops in Python / Writing files in Python / Sockets in Python / Threads in Python / Portscanner in Python / Function documentation / Program structure / Procedural programming in Python / Object oriented programming in Python / Defensive programming in Python / What is C / Running C programs / Printing in C / Variables in C / Maths in C / Functions in C / Comments in C / Conditionals in C / Loops in C / Arrays in C / User input in C / Pointers and memory in C / Object oriented programming in C

Reconnaissance

Google & Robots / Maltego / Job Postings / Wordlists & CeWL / Prior Breaches / Whois / DNSRecon & DIRB / Nmap

Security

The Law / Getting Caught / Ethics / Redteam vs Blueteam / Defence in Depth / Risk Management / Critical Security Controls / Stages of Attack

Virtualisation

What is Virtualisation? / What are the types of virtual machines? / What are the users of virtual machines? / How to set up your own virtual machine

Windows

What is Windows / Installing Windows 10 / Networking - Windows / Windows Defender / Registry / Logfiles

www.joincyberdiscovery.com
#cyberdisc