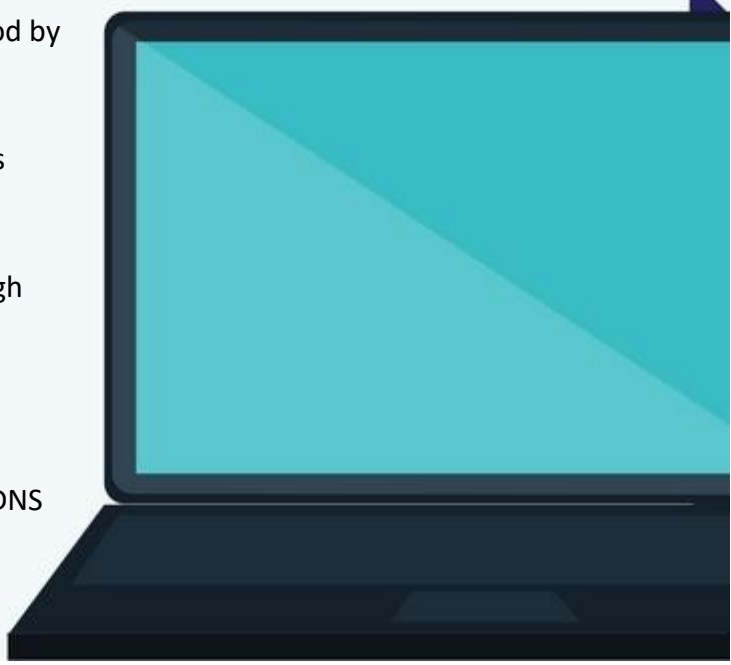
LEARNING SECURITY BASICS

For the best experience with our competitions, we advise CyberCenturion teams to get to grips with a few basics of how computers and security works. This page has a list of resources and terms that teams may find useful for the competition rounds. This is not intended to be an extensive list; teams are encouraged to use the expertise of their Team Leaders, plus some independent research and learning to find out more.

HOW THE INTERNET WORKS

Internet security is a key part of the CyberCenturion competition. We highly recommend possessing technical knowledge of how the Internet works. Some important concepts include:

- Protocol - a set of rules for handling communications at the physical or logical level.
- Internet Protocol (IP) - a set of rules governing the format of data sent over the Internet or other network.
- Transmission Control Protocol (TCP) - TCP is one of the main protocols in TCP/IP networks. TCP guarantees delivery of data and guarantees that packets will be delivered in the same order in which they were sent.
- Domain Names / Hostnames - the part of a network address which identifies it as belonging to a particular domain.
- Domain Name System (DNS) - the hierarchical method by which Internet addresses are constructed.
- Domain Name Resolution - the way these hostnames are resolved to their mapped IP address.
- Ports - data is transmitted between processes through ports (or sockets). Each port provides queues for sending and receiving data.
- IANA Ports Registry - the Internet Assigned Numbers Authority looks after the global coordination of the DNS Root, IP addressing, and other Internet protocol resources



THREATS AND BASIC DEFENCES

The National Cyber Security Centre UK [NCSC] issue alerts and advisories to address cyber security issues detected in the UK. They also produce in-depth analysis on cyber threats and vulnerabilities. Here are some names you should become familiar with. The NCSC glossary can be found here, but the list contains some other sites of interest too.

Threats

Botnets - a network of infected devices, connected to the Internet, used to commit coordinated cyber attacks without their owner's knowledge.

Buffer Overflows - an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations.

Denial of Service (DoS) - when legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

Malware - software which is specifically designed to disrupt, damage, or gain authorised access to a computer system.

Phishing - untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Rootkits - a set of software tools that enable an unauthorised user to gain control of a computer system without being detected.

Spyware and trojans - software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

Defence

Antivirus Software - software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Firewalls - hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to or from a network.

OTHER RESOURCES

The following resources have been shared by CyberPatriot and CyberCenturion teams and our own team.

- Splunk: offers a monitoring and reporting program that helps thwart attacks as they happen and provides insight into past attacks
- FutureLearn online course: Cyber Security for SMEs, Identifying Threats & Preventing Attacks
- FutureLearn online course: Introduction to Cyber Security
- Dash: online course an introduction to HTML, CSS and JavaScript
- SANS: free and fee-based training and resources for cyber professionals
- Have I Been Pawned: a free secure site where you can check if your email account has been compromised
- Centre for Internet Security: provides numerous resources on internet security and cyber security standards
- CNET: the latest cybersecurity news and thousands of open-source software programs for download

Good luck Centurions!