TECHNICAL HANDBOOK

CYBER SECURITY COMPETITION

Kevin Maclean
Cyber Security Competitions Manager

kmaclean@glasgowclyde.ac.uk

CONTENTS

We would like to thank our industry and educational partners that are passionate about finding the top talented people and help make this competition possible:

paloalto® NETWORKS

GLASGOW CLYDE COLLEGE

EC-COUNCIL|ACADEMIA

Balfour Beatty

OVERVIEW

This competition focuses on all the essential requirements for a successful career as a Cyber Security Analyst within any industry. This competition tests your abilities in Reconnaissance, Scanning, Vulnerability Testing, Exploitation of Systems, System Hardening, and Technical Analysis.

CAREER PATHWAY

A Cybersecurity Professional is responsible for providing security during the development stages of software systems, networks and data centres. The professionals will have to search for vulnerabilities and risks in hardware and software. They manage and monitor any attacks and intrusions. The Security Specialist must recognize the potential threat or attempted breach by closing off the security vulnerability.

Cybersecurity Professionals may be tasked with anything from installing, administering and troubleshooting security solutions to writing up security policies and training documents for colleagues.

While other job roles are responsible for a specific part of the overall system, Cybersecurity Professionals must be able to take a step back and see the big picture to keep it secure from threats.

SKILLS REQUIRED

AT A BEGINNER LEVEL - Job Titles would include – System Administrator / Network Engineer / Systems Engineer / Cyber Security Technician (CompTIA, 2020)

- Scan and assess network for vulnerabilities
- Monitor network traffic for unusual activity
- Investigate a violation when a breach occurs
- Install and use software to protect sensitive information
- Prepare reports that document security breaches
- Research new security technology

- Help end-users when they need to install or learn about new products and procedures:

AT AN INTERMEDIATE LEVEL – Job Titles would include – Security Analyst / Security Engineer / Pen Tester (CompTIA, 2020)

- Manage and configure tools to monitor network activity
- Conduct penetration testing
- Analyse reports from tools to identify unusual network behaviour
- Plan and recommend changes to increase the security of the network
- Apply security patches to protect the network
- Help end-users when they need to install or learn about new products and procedures
- Train beginner cybersecurity professionals

AT AN ADVANCE LEVEL – Job titles would include – Senior Security Engineer / Senior Security Analyst / CISO (CompTIA, 2020)

- Manage and configure tools to monitor network activity
- Research the latest IT security trends
- Develop security standards and best practices for the organization
- Recommend security enhancements to management or senior staff
- Develop and update business continuity and disaster recovery protocols
- Help end-users when they need to install or learn about new products and procedures
- Manage and train team

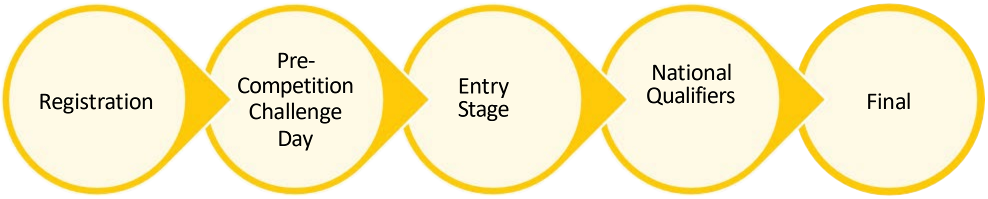
SALARY RANGES

- Beginner
  - £35,000
- Intermediate
  - £50,000
- Advance
  - £75,000 – 80,000

RESOURCES AND REGISTRATION

Registration can be found at the following link, World Skills UK Cyber Security Registration and Resource Link, you will need to be in a team of two. You should currently be in education, training, employment, or be enrolled in a program of study or otherwise, you must have completed the equivalent to a level 4 qualification.

COMPETITION STRUCTURE



The competition process will start by getting your team together and registering your interest in the competition. Once completed you will be invited to a Cyber Challenge Day where you can test your skills and have a sneak peek into the types of tasks that you will face during the heats and the final.

Once you have taken part in the Cyber Challenge Day, the Entry Stage is the next step forward, this will be a test of your theoretical knowledge of all things cyber security.

Passing the Entry Stage gives you access to the National Qualifier – the Skills Challenge Heat. This is a one-day event that will task you and your partner's skills in practical activities to do with cyber security and are detailed a little later.

The top ten highest scoring teams from across the UK will be invited to the WorldSkills UK National.

ENTRY STAGE

The entry stage will test your theoretical knowledge of being a cyber security professional, you will be tested on subjects such as Digital Forensics, Penetration Testing Methodologies, Malware Analysis, Data Security, Security Legislation, and a basic understanding of common tools and techniques.

This may consist of a small presentation of information in the form of short answer questions, multiple-choice questions, or a demonstration of techniques used.

NATIONAL QUALIFIERS

The national qualifier heats consist of two sessions in a single day competition that concentrates on some of the core skills of a Cyber Security Professional.

The heat may be done on-site, or remotely depending on circumstances. Both will follow a similar structure.

The heat will be based on a capture the flag type competition where competitors will have access to a set of pre-configured systems that have been designed to test a specific skillset.

The skills tested during the heats will usually consist of the following:

- Social Engineering Techniques
- Vulnerability Scanning Techniques
- Web Application Exploitation
- Client System Exploitation
- System Hardening

NATIONAL FINAL

The final will be held in November and will be a two-day event that consists of 4 sessions. The individual sessions will cover the following topics:

Capture the Flag (CTF) Sessions:

- Social Engineering Techniques
- Vulnerability Scanning Techniques
- Web Application Exploitation
- Client System Exploitation
- Server Systems Exploitation
- Network Monitoring

System / Application Analysis Session

- Network Traffic Analysis
- Web Application Code Analysis
- Malware Analysis

System Hardening Session

- Network Infrastructure Securing
- Securing Web Application
- Securing Databases
- Securing Servers

During the finals your overall mark will consist of the following:

- ➢ 50% Capture the flag session
- ➢ 25% System / Application Analysis Session
- ➢ 25% System Hardening Session

WHAT TO EXPECT DURING THE COMPETITION

During each of these competitions, you will be required to bring pre-existing knowledge to an unknown situation. It is best to prepare well in all aspects of the competition as a team. The CTF session will last for two sessions over a single day, the System Hardening and System / Application Analysis will be in separate sessions over the second day.

During the heats and final there will be lots going on, as you are on a public platform where aspiring students and potential employers can come and see the fantastic work you are doing.

MARKING

The skills competition is marked by three Judges from Glasgow Clyde College, the judges' decision will be independently moderated and quality assured before being confirmed at the end of the heats or the closing ceremony. Judges are looking for technical competency but are also looking for excellence amongst competitor. Judges will therefore take into account skills such as time management, working under pressure, and communication skills. All marking is objective and based on agreed criteria.

The tasks at the WorldSkills UK national final follow a similar format to those in the qualifier but are more complex requiring in-depth knowledge of the specific areas.

Judges will also be looking for other skills expected of a cyber security professional, such as:

- Time management
- Communication Skills
- Working under Pressure
- Planning
- Methodical Approaches
- Problem Solving

JUDGES TOP TIPS

Preparation and Planning

Ensure you have looked over this document and taken on board the resources available to you, cyber security is a huge topic with lots of fun and fantastic resources out on the internet. Make full use of them and prepare for what is to come. Practising as much as your spare time will allow you to and ensuring you have a good understanding of the target systems you may be presented with. A home lab is a great way to do this, it ensures you not only have experience of analysing these systems but also the set up of the systems.

Time Management

Manage your time effectively when completing tasks, divide your tasks up between your team, ensure the right person is doing the right job.

Planning

Plan out what you are going to tackle first, and who is assigned to a particular task. Planning out what tools you are going to use, what techniques you use and who is going to do these tasks is key to ensuring you complete all tasks in the given time

Understanding

Study the technologies that are likely to come up in the Briefs, all the systems that are to be used will be detailed before the competition, ensure you have a good understanding of them and potential vulnerabilities. Along with how to work with t eh systems, understand how to configure and set them up this is a key part of the defence / securing section of the competition.

Don’t Worry

If a task hasn’t gone as well as you thought it should have, don’t dwell on it, just draw a line under it and move on to the next task. Always look forward to the marks you can gain and not the ones you think you may have lost.

Enjoy!

Enjoy your WorldSkills UK experience, gaining access to the heats and the final is a huge achievement in itself, and one you should be immensely proud of. This competition is designed to be challenging but fun at the same time.

TRAINING FOR THE COMPETITION

In preparation for the competition you could look at some of the following recognised qualification and see what is involved how to go about gathering the required knowledge.

- CompTIA PenTest+
- CompTIA Network+
- CompTIA Security+
- CompTIA Server +
- Cisco CCNA
- Cisco CCNA Security
- EC Councils Latest Ethical Hacker Course
- Kali Linux Training by Offensive Security
- SANS Cyber Security Training
- pfSense Familiarisation Training
- PaloAlto EDU 210 Firewall Essentials: Configuration and Management
- Immersive Labs

SANS Cyber Security Skills Roadmap

CompTIA Cyber Security Skills Roadmap

HOME-LAB TRAINING

For training purposes towards this competition, it is strongly recommended you set up your own lab environment.

A guide for this is below, but is in no way an exhaustive list, this is only a recommendation on how to set up a basic testing environment.

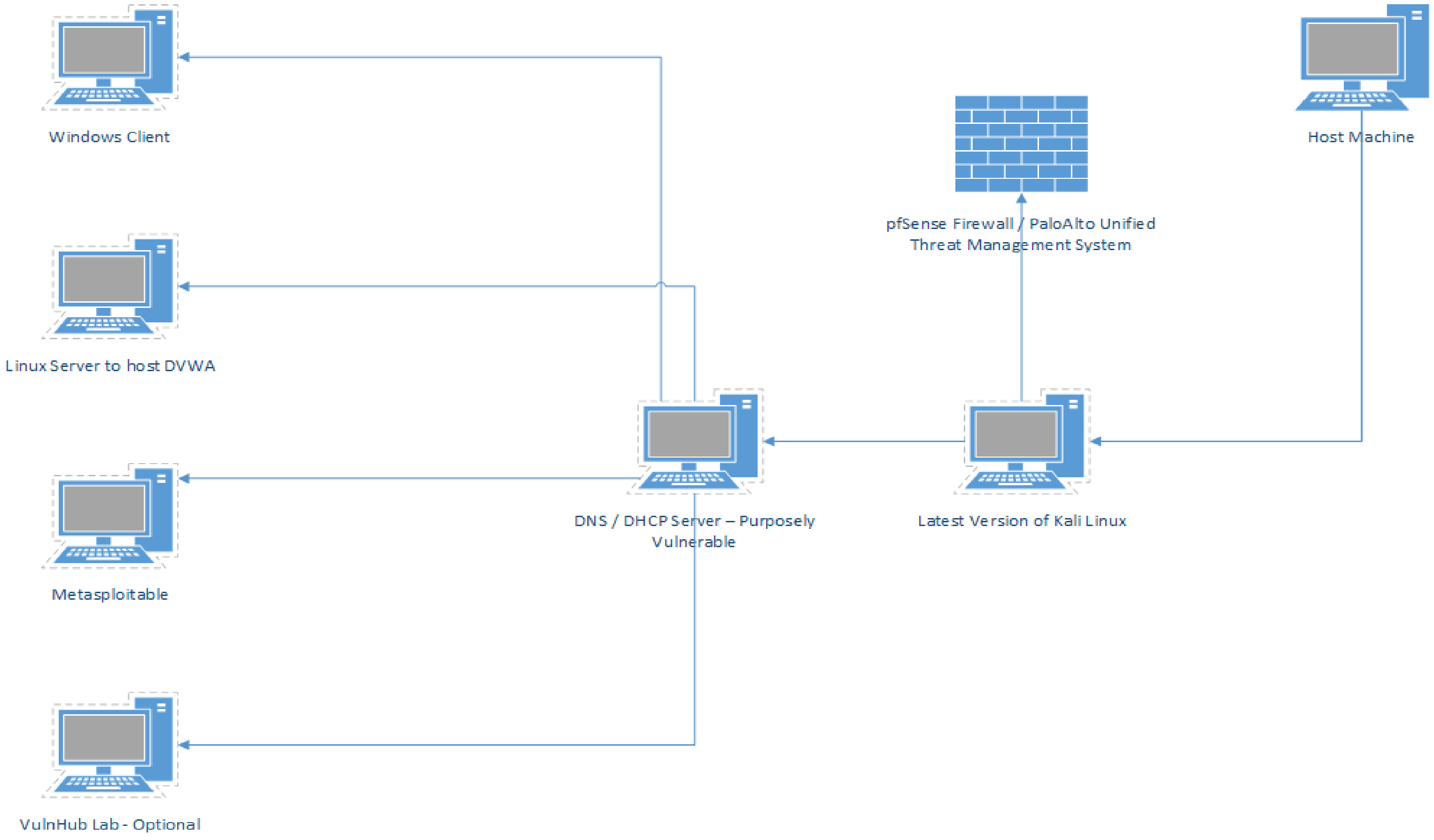
Always adhere to your establishments computing policies when creating these environments within a learning environment, and always test responsibility and with prior authorisation to do so.

It is recommended that you start practicing on prebuilt vulnerable systems. Some of these include:

- Damn Vulnerable Web Application
- Metasploitable
- Windows Server 2008 – unpatched and firewall off.
- Windows 7 SP1 – unpatched and firewall off.
- Any of the Vulnerable by Design virtual machines from http://www.vulnHub.com

It is recommended that all machines run on an internal network within VirtualBox (or any other virtualisation software you have) as this is what is used within the competition.

It is recommended that the host machine have at least 16 GB ram with a quad-core processor to run all machines at once, the operating system for the host machine is not relevant.


Windows Client
Linux Server to host DVWA
Metasploitable
VulnHub Lab - Optional
DNS / DHCP Server – Purposely Vulnerable
pfSense Firewall / PaloAlto Unified Threat Management System
Latest Version of Kali Linux
Host Machine

This is a logical diagram of the proposed set up. The DHCP/DNS server should be the gateway to the rest of the network hosting DNS records for any web-based application you are hosting.

All five machines should have their IP address statically assigned for ease of use and reliability for DNS.

The latest version of Kali Linux should be used and set to dynamically gather its DHCP settings from the server. This should be fully updated with a form of vulnerability scanner installed, as this is not done by default (OpenVAS). While updating and installing the vulnerability scanner this is the only time your Kali machine should be on an internet facing network adapter if you are inside a controlled network. You should also consider installing the Wireshark package to monitor all of your internal network traffic.

The Windows client should not be updated, and have its firewall turned off, it should be joined to a domain

The Server should be set up as a domain controller, it should have DNS, DHCP enabled, and all security removed. This will make it purposely vulnerable, so you can test different tools.

Metasploitable can be acquired from here and should be set up according to the instructions, ensuring when setting IP addressing that it is within the network you are working with.

DVWA can be acquired here as source files which will require you to set up a web server. The live version can be acquired here, but will not retain any information once powered down. It is under the Download section and download the ISO for DVWA v1.0.7 Live CD. Instructions on how to set up a persistent copy are here.

VulnHub has lots of community created resources, they will have explanations on how to attach the machines to a virtual network and some have walkthroughs to enable you to complete the tasks. https://www.vulnhub.com/. There is no recommendation as to what virtual machines to acquire form VulnHub, as it would be personal preference on what you wish to test your skills on.

The firewall is to be connected to a different network through the use of an internal network inside your virtualisation software, ring-fence this off so it does not interfere with the rest of the lab set up. You can incorporate it into the set up once you are comfortable with the software you are using and its impact on your virtual network. Having the firewall included is for set up and testing purposes.

DIGITAL RESOURCES

- HackTheBox
- HackThisSite
- Over the Wire War Games
- Vulnhub
- OWASP
- PaloAlto EDU 210

COMPETITION RULES

These competition rules apply to all parts of the competition, from entry stage to the final. Stage-specific rules will be given on the day of that part of the competition.

- If at any point you feel you are finished and you leave your station, you may not come back and continue work.
- If you feel that you require assistance, possibly due to a suspected hardware/software failure, please put your hand up and inform a judge.
- It is your responsibility to save your work on a regular basis.
- No personal storage devices or mobile phones are allowed in or around your workstation during the competition.
- Only the virtual machines provided are eligible for use. Access to the point's server is PROHIBITED unless submitting your captured tokens.
- Access to the Internet is PROHIBITED from any device.
- No collaboration with other competing teams.

BEYOND THE NATIONAL FINALS

The Cyber Security Competition national finals also form part of the selection process for Team UK at the WorldSkills International competitions where you will compete against aspiring security professionals from across the globe. Training managers will be onsite during the competitions, monitoring the performance of those who are age-eligible and who show the highest skills, passion and drive to compete at the highest level could be invited to train for Team UK.

Those who are not eligible for Team UK may join the Campions Programme, which allows continued involvement, including the opportunity to work with WorldSkills UK and visit schools, colleges, and events to inspire the next generation of competitors.

Alternatively, if training is of interest to you, you could consider supporting WorldSkills UK with organising and training, and even helping run the National Finals.

Get inspired and become part of Team UK today!