Evil Corp Challenge

GROUP 1:

Hemanth Bojja	11702675
Vamsi Pavan Krishna Dasineni	11658186
Aryanth Reddy Kondreddy	11696947
Sushmitha Inapakuthika	11696399

Introduction

The "Evil Corp" challenge is a pwn (exploitation) category challenge in cybersecurity competitions.

It is designed to assess participants' skills in identifying and exploiting vulnerabilities in a simulated environment.

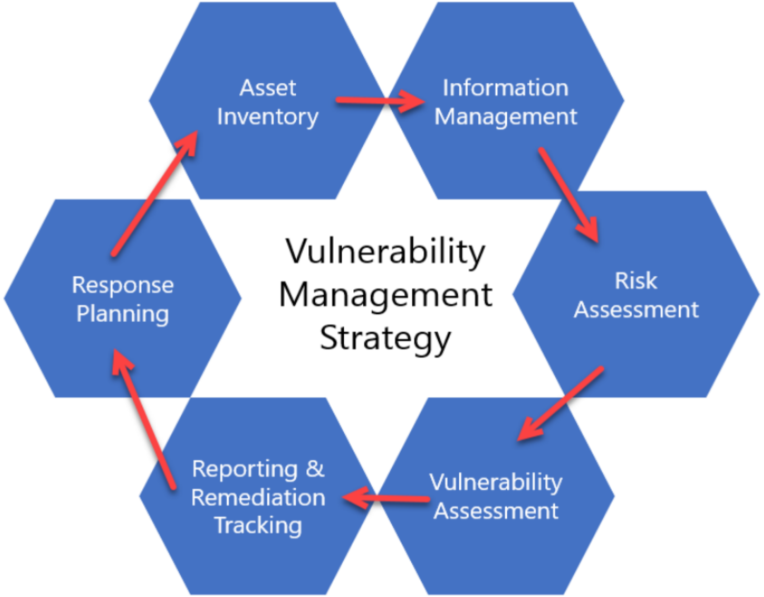
Participants are required to find and exploit vulnerabilities within the challenge to gain control or access to specific resources.

Understanding the Challenge

Pwn challenges typically involve finding security vulnerabilities in software or systems.

Participants need to analyze the given scenario, understand the vulnerabilities present, and devise an exploit.

The goal is to demonstrate the ability to think like a hacker and exploit weaknesses for educational purposes.

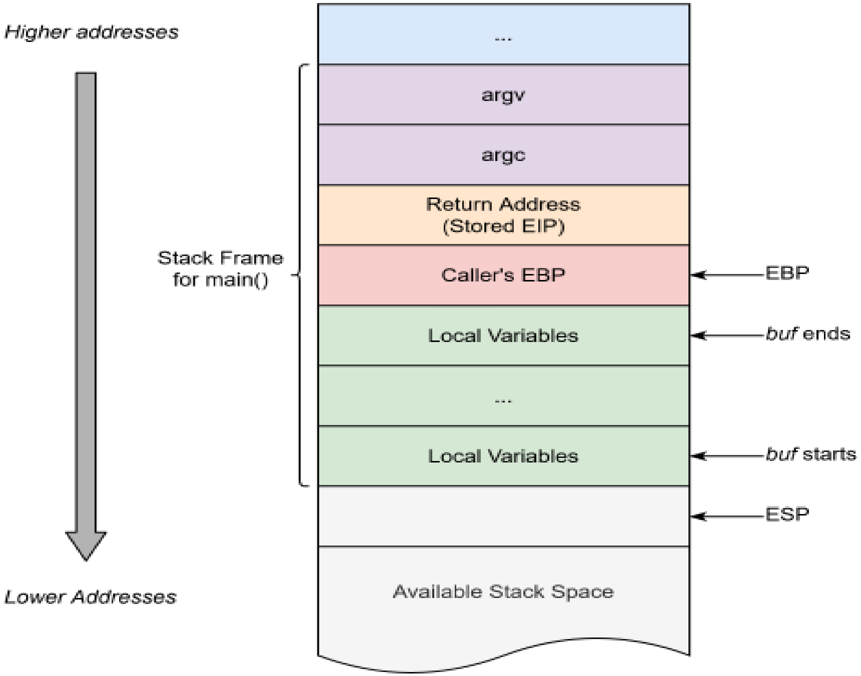


Types of Exploitation

Common exploitation techniques in pwn challenges include buffer overflows, format string vulnerabilities, and use-after-free exploits.

Participants may need to write or modify exploit code to gain control over the target system.

Understanding memory management, assembly language, and debugging techniques are essential for success.

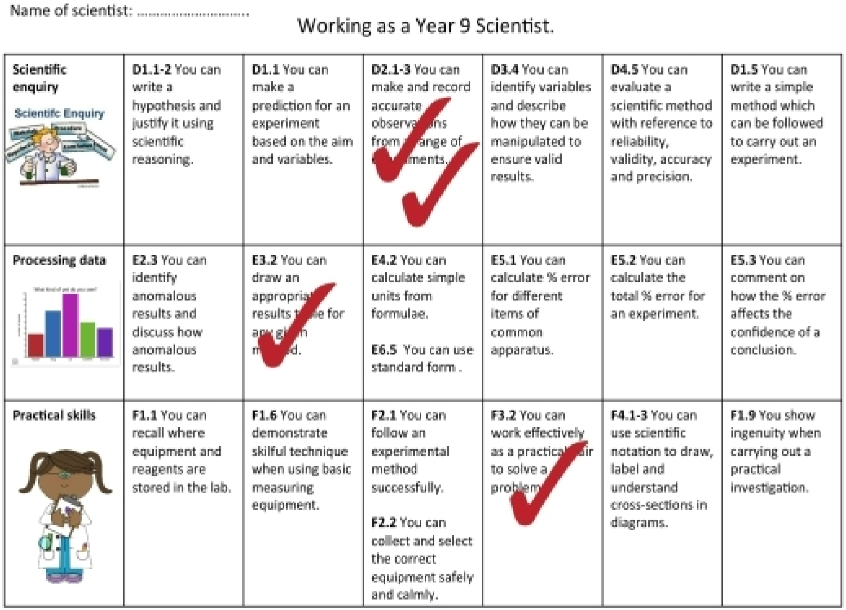


Importance of Skills Assessment

The "Evil Corp" challenge allows participants to showcase their technical skills in a competitive environment.

It helps assess participants' proficiency in reverse engineering, exploit development, and vulnerability analysis.

Competing in such challenges can enhance participants' knowledge and practical skills in cybersecurity.



Name of scientist: ……………………………

Working as a Year 9 Scientist.

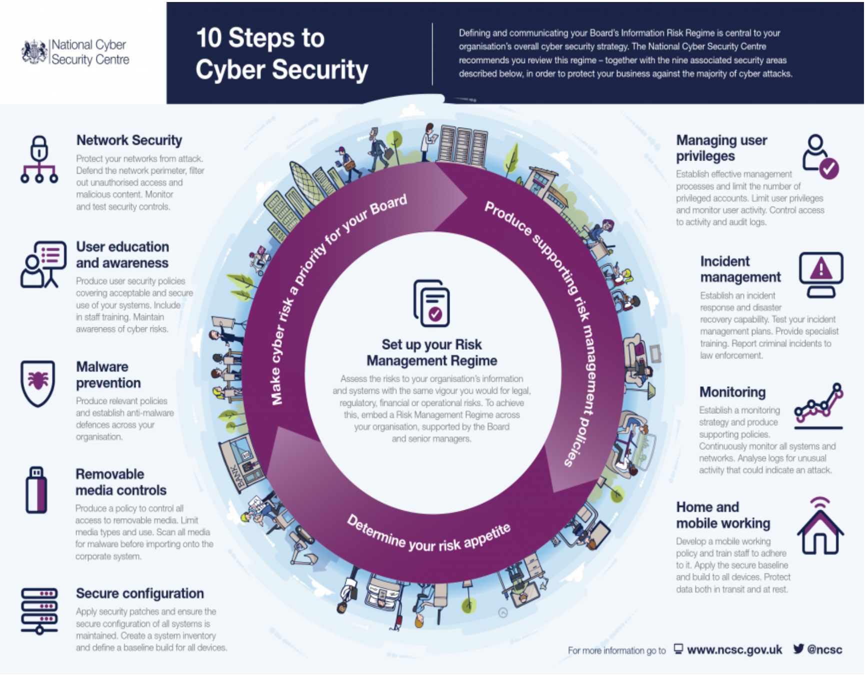
Scientific enquiry Scientifc Enquiry	**D1.1-2** You can write a hypothesis and justify it using scientific reasoning.	**D1.1** You can make a prediction for an experiment based on the aim and variables.	**D2.1-3** You can make and record accurate observations from a range of experiments. ✓ ✓	**D3.4** You can identify variables and describe how they can be manipulated to ensure valid results.	**D4.5** You can evaluate a scientific method with reference to reliability, validity, accuracy and precision.	**D1.5** You can write a simple method which can be followed to carry out an experiment.
Processing data	**E2.3** You can identify anomalous results and discuss how anomalous results.	**E3.2** You can draw an appropriate results table for any given method. ✓	**E4.2** You can calculate simple units from formulae. **E6.5** You can use standard form .	**E5.1** You can calculate % error for different items of common apparatus.	**E5.2** You can calculate the total % error for an experiment.	**E5.3** You can comment on how the % error affects the confidence of a conclusion.
Practical skills	**F1.1** You can recall where equipment and reagents are stored in the lab.	**F1.6** You can demonstrate skilful technique when using basic measuring equipment.	**F2.1** You can follow an experimental method successfully. **F2.2** You can collect and select the correct equipment safely and calmly.	**F3.2** You can work effectively as a practical pair to solve a problem. ✓	**F4.1-3** You can use scientific notation to draw, label and understand cross-sections in diagrams.	**F1.9** You show ingenuity when carrying out a practical investigation.

Real-World Relevance

The skills tested in pwn challenges are directly applicable to real-world scenarios in cybersecurity.

Identifying and exploiting vulnerabilities is crucial for securing systems and applications.

Professionals with expertise in exploitation techniques are in high demand in the cybersecurity industry.



National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Set up your Risk Management Regime
Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite
BANK

Managing user privileges
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

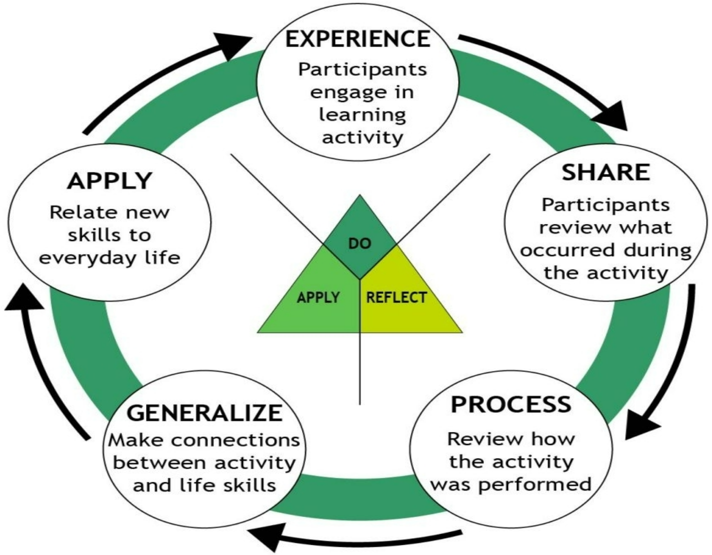
For more information go to www.ncsc.gov.uk @ncsc

Learning Opportunities

Participating in pwn challenges like "Evil Corp" provides hands-on experience in offensive security techniques.

Participants can learn new exploit development skills, enhance their problem-solving abilities, and expand their knowledge of security concepts.

Feedback from challenges can help participants improve their skills and techniques for future engagements.


EXPERIENCE
Participants engage in learning activity
SHARE
Participants review what occurred during the activity
PROCESS
Review how the activity was performed
GENERALIZE
Make connections between activity and life skills
APPLY
Relate new skills to everyday life
DO
APPLY
REFLECT

Collaboration and Networking

Pwn challenges often encourage collaboration among participants to solve complex problems.

Networking with other cybersecurity enthusiasts and professionals in the field can lead to valuable learning opportunities and career connections.

Sharing knowledge and experiences with peers can foster a supportive community of like-minded individuals.

Ethical Considerations

It is crucial for participants in pwn challenges to adhere to ethical guidelines and rules of engagement.

Engaging in ethical hacking practices, respecting privacy and confidentiality, and obtaining proper authorization are essential.

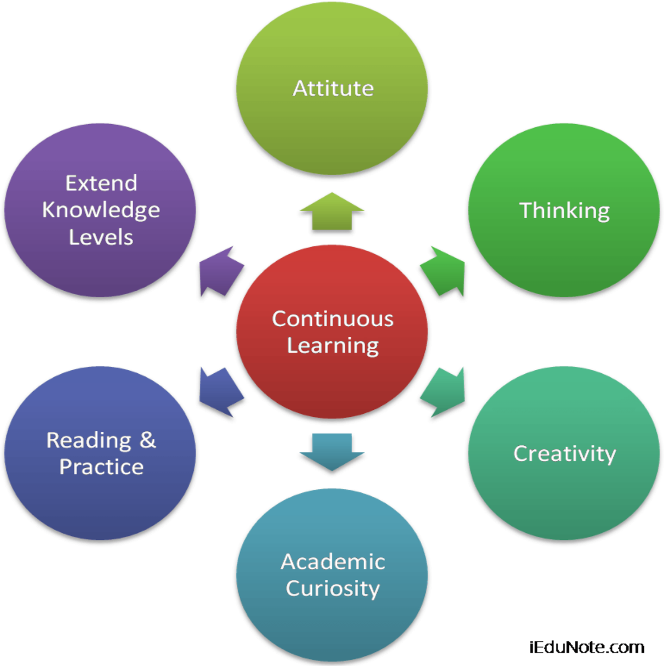
Upholding ethical standards in cybersecurity competitions reflects professionalism and integrity in the industry.

Continuous Learning and Improvement

The "Evil Corp" challenge and similar pwn challenges serve as a platform for continuous learning and skill development.

Participants can leverage feedback, engage in post-challenge analysis, and seek further training to enhance their capabilities.

Embracing a growth mindset and a commitment to ongoing improvement are key to succeeding in cybersecurity challenges.

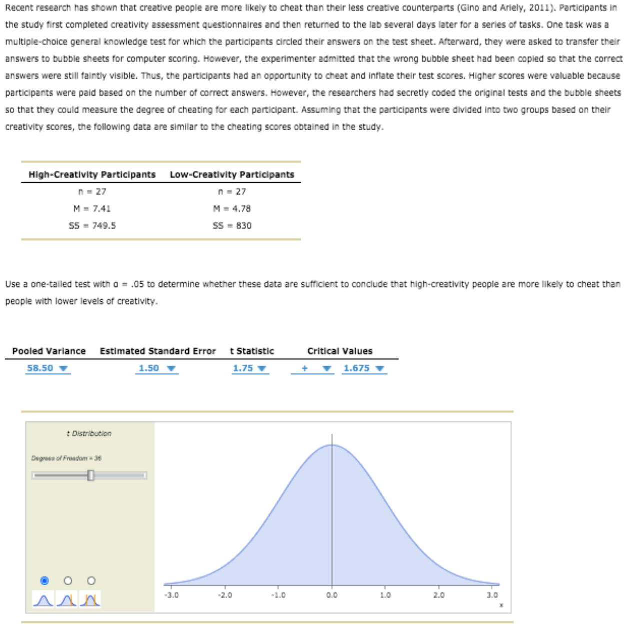


Conclusion

The "Evil Corp" challenge is a valuable opportunity for participants to test their pwn (exploitation) skills in a controlled environment.

By engaging in such challenges, participants can sharpen their technical abilities, gain practical experience, and demonstrate their expertise in offensive security.

Embracing the challenge, learning from experiences, and staying curious are essential for personal and professional growth in the field of cybersecurity.



Recent research has shown that creative people are more likely to cheat than their less creative counterparts (Gino and Ariely, 2011). Participants in the study first completed creativity assessment questionnaires and then returned to the lab several days later for a series of tasks. One task was a multiple-choice general knowledge test for which the participants circled their answers on the test sheet. Afterward, they were asked to transfer their answers to bubble sheets for computer scoring. However, the experimenter admitted that the wrong bubble sheet had been copied so that the correct answers were still faintly visible. Thus, the participants had an opportunity to cheat and inflate their test scores. Higher scores were valuable because participants were paid based on the number of correct answers. However, the researchers had secretly coded the original tests and the bubble sheets so that they could measure the degree of cheating for each participant. Assuming that the participants were divided into two groups based on their creativity scores, the following data are similar to the cheating scores obtained in the study.

High-Creativity Participants	Low-Creativity Participants
$n = 27$	$n = 27$
$M = 7.41$	$M = 4.78$
$SS = 749.5$	$SS = 830$

Use a one-tailed test with $\alpha = .05$ to determine whether these data are sufficient to conclude that high-creativity people are more likely to cheat than people with lower levels of creativity.

Pooled Variance	Estimated Standard Error	t Statistic	Critical Values	
58.50 ▼	1.50 ▼	1.75 ▼	+ ▼	1.675 ▼

References

1. Cybersecurity Competitions: Benefits and Best Practices. (n.d.). Retrieved from https://www.nist.gov/cyberframework/cybersecurity-competitions-benefits-and-best-practices
2. Aboagye, E., Yawson, J. A., & Appiah, K. N. (2021). COVID-19 and E-learning: The challenges of students in tertiary institutions. Social Education Research, 1-8.
3. https://app.hackthebox.com/login?redirect=%2Fchallenges%2FEvil%2520Corp