Phriendly Phishing

PODCASTS

BYTES

WITH BEC & BENJI

Episode 3

Day in the Life of an Ethical Hacker

How weak is your security *really*?

Our guest...

Liam O'Shannessy

Executive Director
Security Testing & Assurance (STA)
CyberCX

Phriendly Phishing

PODCASTS

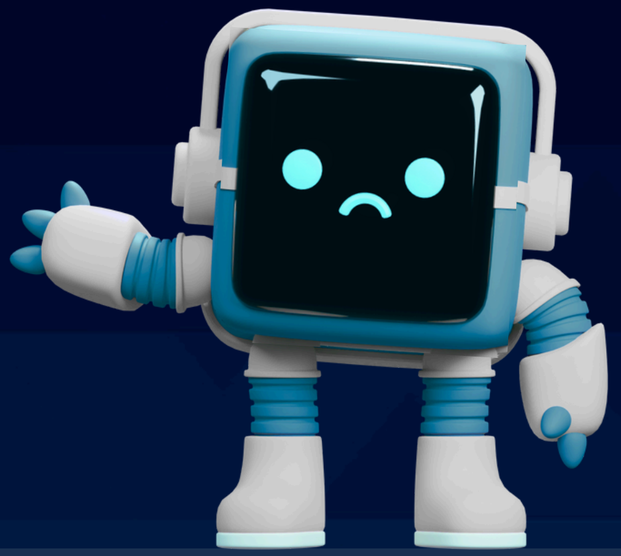
THE BYTES

- **Fundamentals of pentesting and evolution**
  - While the goals of ethical hacking remain the same, the landscape of vulnerabilities has evolved.
- **Skills Matrix & Purple Teaming**
  - Playing the world's biggest game of Tetris to coordinates engagements, particularly when matching red teams to collaborate with blue teams (Purple Teaming).
- **Knowledge transfer and specialisation**
  - Quickly becoming experts in new areas due to the need for rapid adaptation & deep understanding of specific technologies.
- **Human factor in security**
  - Human behaviour is crucial in security. Technical solutions are often accompanied by necessary changes in governance and user behaviour to be effective.
- **Security maturity & organisational readiness**
  - Staged approaches from blue teams to red teams highlights the importance of maturity in cyber security practices.

and much more!

Adversarial Nature

Adversaries are always innovating, finding new vulnerabilities and exploiting them, which keeps ethical hackers in a perpetual state of **defense** and **countermeasure development**.



This relationship is akin to a high-stakes game of chess where each move by the defender is met with a **counter-move** by the attacker.

Fundamentals & Evolution of Penetration Testing

The Fundamentals

The fundamental goals of ethical hacking remain the same: identifying vulnerabilities before adversaries do.

Evolution

Traditional pen testing focused on on-premises systems, but with the advent of cloud computing and AI, the scope has expanded.

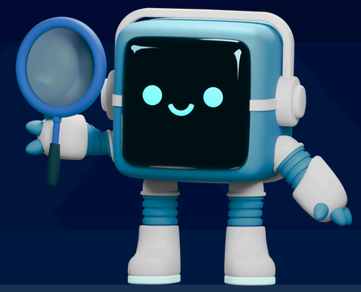
The technologies and environments in which vulnerabilities are found have evolved, and thus the landscape of vulnerabilities has evolved, particularly with the rise of cloud computing and generative AI.

External Risks & Cybercriminals

Cybercriminals have embraced the malicious use of AI as these tools can be used to **significantly increase** the sophistication of social engineering attacks and other email threats, with no technical knowledge required.

Cybercriminals are drawn to the:

- Low barrier to entry for generative AI tools.
- Ability to rapidly create high volumes of malicious content.
- Increased sophistication of existing attacks (phishing, vishing, smishing, etc).
- Little technical understanding required.



Ethical hackers must stay ahead by understanding and mitigating these advanced threats.

Skills Matrix & Coordination

The analogy of building a **giant jigsaw puzzle** or playing the world's **biggest game of Tetris** to describe how the team coordinates personnel and projects.

A **specialist team** matches the right personnel with the right job based on a **detailed skills matrix**.

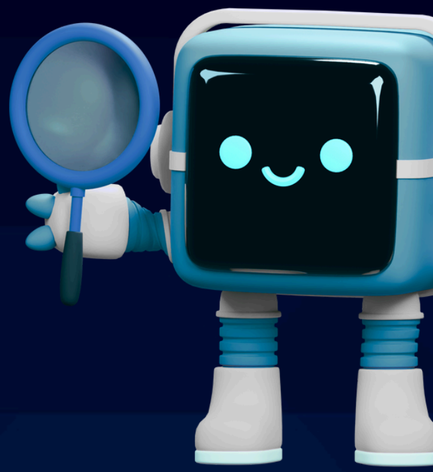
Continuous training is vital to keep up with the **evolving technology**. Ethical hackers must be adaptable, often becoming experts in new technologies quickly due to the **ever-changing nature of cyber security**.

Purple Teaming

Purple teaming is a collaborative approach that combines the efforts of the red team (attackers) and the blue team (defenders).

The goal is to improve the organisation's defense mechanisms by having both teams work together.

The red team simulates attacks, while the blue team tries to detect and respond to these attacks in real-time.

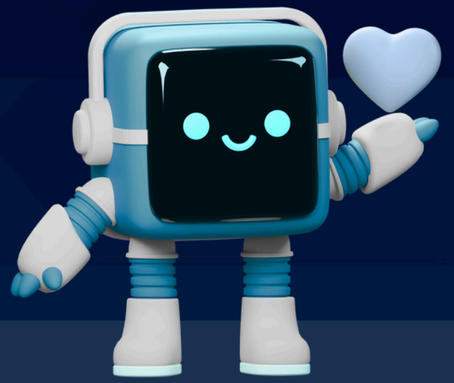


This exercise helps identify gaps in the defense strategy and improves the overall security posture by creating a more resilient system through continuous feedback and improvement.

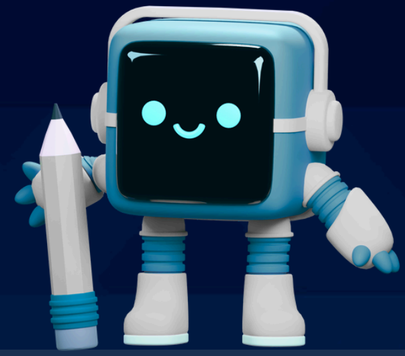
Knowledge Transfer and Specialisation

Ethical hackers can quickly become subject matter experts in new areas due to the need for rapid adaptation and deep dives into specific technologies during projects.

- Continuous training is vital to keep up with the evolving technology.



- Must be adaptable, often becoming experts in new technologies quickly.



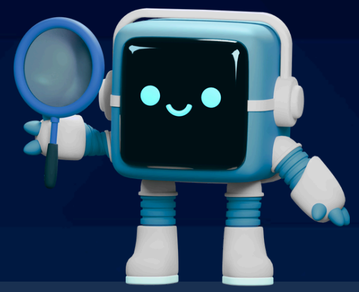
The hacker community is highly collaborative, with a strong culture of sharing knowledge and techniques to improve overall security.

Human Factor in Security

Effective cyber security strategies must include:

- Training and awareness programs to educate employees.
- Governance policies to enforce those practices.
- A culture that supports and promotes security.

By addressing the human factor, organisations can reduce the risk of security incidents and create a culture of security awareness and responsibility.



Governance and human behaviour are crucial in security. Technical solutions are often accompanied by necessary changes in governance and user behaviour to be effective.

Security Maturity & Organisational Readiness

Organisational readiness for pen testing, including the staged approach from blue teams to red teams, highlights the importance of maturity in cyber security practices.

The Essential 8 Maturity Model

The purpose of the Essential 8 Maturity Framework is to provide organisations with a baseline of eight essential mitigation strategies to help protect their systems against cyber threats. The framework provides guidance on protecting Windows networks.

Maturity Model assessments should be conducted based on the organisation's current and desired level of maturity.

Achieving higher maturity levels requires continuous improvement, monitoring, and adaptation to the evolving threat landscape.

Organisational readiness for pen testing, including the staged approach from blue teams to red teams, highlights the importance of maturity in cyber security practices.

Phriendly Phishing

PODCASTS

www.phriendlyphishing.com

Stay tuned for more!

BYTES

WITH BEC & BENJI

https://linktr.ee/BytesBB