Panel: Actions with Impact. Lessons Learnt from Schools Conducting Ethical Hacks

12:20pm - 12:50pm

Maurice Cummins, CIO, AISNSW

Seth Mayo, ICT Operations Manager, Toongabbie Christian College

Mark Sullivan, Chief Operating Officer, The PARED Foundation

Stuart Frederick, Director of ICT, Warakirri College

What Is An Ethical Hack?

What is Ethical Hacking?

- Proactive security practice
- Pre-approved
- Defined scope
- Professionals simulating cyber-attacks on a network, system or application
- Seeking to identify and exploit vulnerabilities before malicious actors
- Report of vulnerabilities and rectification guidance is provided
- Usually an NDA is signed
- Also known as ‘Penetration Testing’

Essential to:

- uncover security weaknesses
- assess systems configuration and defense mechanisms
- ensure resilient cybersecurity posture
- heighten your cyber security defences

What should Ethical Hacking achieve?

Ethical hackers:

- prevent malicious hackers from breaching an organization's network
- identify system vulnerabilities that others may exploit
- analyze and enhance an organisation’s security policies
- help protect customer data

Ethical Hacking Skills

- Knowledge of operating environments such as Windows, Linux, Unix, OSX/iOS
- Familiarity with programming languages such as HTML, PHP, Python, etc.
- In-depth understanding of networking
- Awareness of local security laws and standards
- Understanding the architecture of the operating system
- Can analyse malware and reverse engineer

Types Of Ethical Hackers

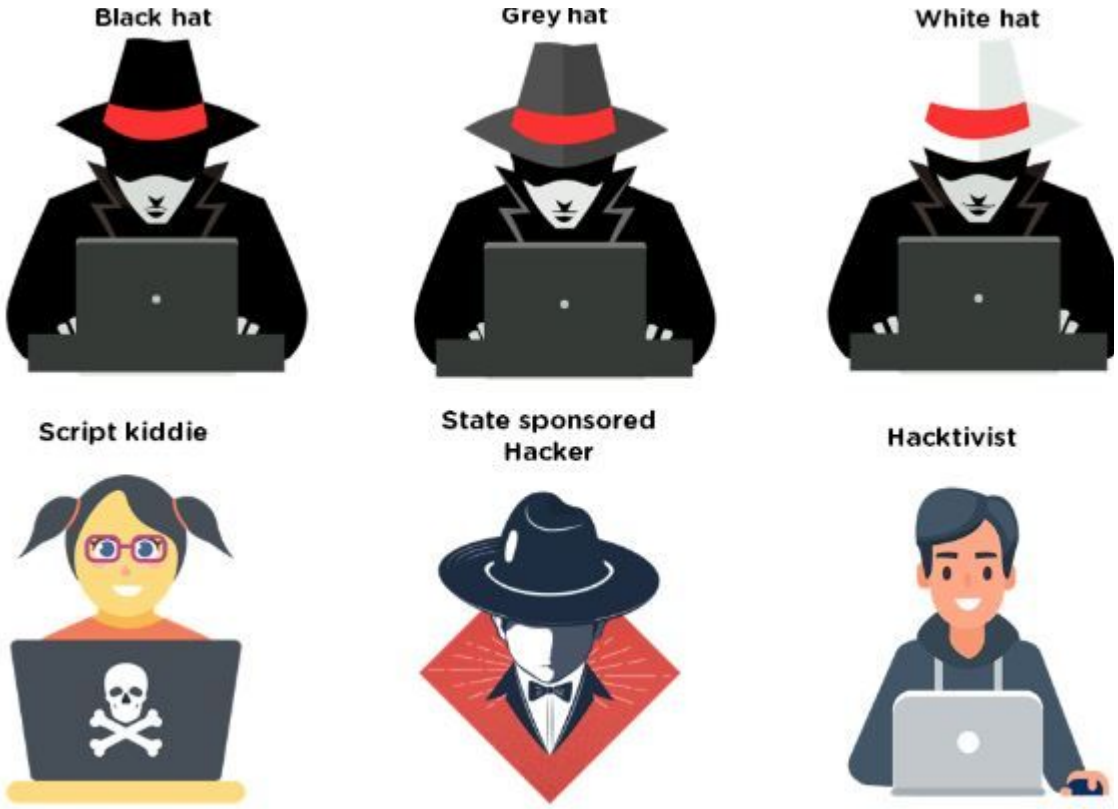


Image source: https://www.simplilearn.com/ethical-hacking-tutorial-article

Strategies Ethical Hackers Commonly Deploy

Wireless Network Testing

Physical Testing

Social Engineering

Vulnerability Scanning

The Ethical Hack Process

1: Statement of Work

- Quote
- Agreed scope and timeframe
- Formal approval process
- NDA

2: External Pen Testing

- Remotely testing school's IP addresses etc
- Best practice is to start with external testing

3: Internal Pen Testing

- Remote engineer
- Using organisation provisioned device
- With basic user privileges

4: Report

- Results of testing
- With evidence
- Vulnerabilities categorised into critical, high, medium and low risk

5: Remediation

- Steps to remediate exposed vulnerabilities
- Often requires significant time and resources

6: Retest

- At an agreed upon time
- Included in original scope
- Used to test the effectiveness of remediation steps

Participants In Ethical Hacking

Red Team

- Simulates a real-world attack
- Uses the same tactics, techniques and procedures that a cybercriminal would
- Objective to attack the school's systems and exploit vulnerabilities to gain unauthorised access

Blue Team

- Is responsible for defending against the simulated attacks
- Assess how well the school's cybersecurity team can respond to attacks and detect intrusions in real-time

Purple Team

- A more collaborative approach
- Combines the strengths of both the Red and Blue Teams
- The two teams work together to improve the school's security posture
- Also known as "Red Team/Blue Team"

Purpose

AISNSW partial grants provided to:

Activate Ethical Hacking

Promote Member Schools' cyber resilience

Awarded 53 Schools CAF Grant totaling : $213,850

Why the traditional approach does not work for schools

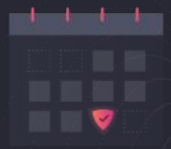
Traditional framework-based assessments assume there's only one way to reach maturity, but reality is more complex…

Oversimplification

- Frameworks assume minimum security foundations
- Schools need flexible, adaptable approaches

Knowledge Gap

- Assumes security expertise exists
- Most schools lack dedicated security teams



Implementation Guidance

- Too many generic recommendations at once
- Need prioritisation with achievable steps