Flyer College: Types of Hackers and Ethical Hacking Plan

Daniel Monbrod

Lewis University

INSY 46000-001: Cybercrime Prevention Tools

Dr. Mathias Plass

February 16, 2025

Flyer College: Types of Hackers and Ethical Hacking Plan

Cybersecurity is a growing concern in the digital age, especially for higher education institutions like Flyer College. Academic institutions store a vast amount of sensitive information, including student records and financial aid data, making them prime targets for cyberattacks. My duties involve assessing the cybersecurity environment and offering recommendations for risk mitigation.

This report outlines the distinct types of hackers, identifies the greatest threats to Flyer College, and defines the essential requirements for hiring a penetration testing team. By aligning our security strategy with best practices in ethical hacking, Flyer College can strengthen its defenses and protect against cyber threats.

Types of Hackers

Hackers come in various forms, each with different motives and techniques. Below is a breakdown of the main types of hackers and their roles:

- **Ethical Hackers (White Hat Hackers)** – Organizations legally contract these professionals to find and resolve security vulnerabilities within an organization's systems. They conduct in-depth testing to simulate attacks, helping pinpoint areas of the organization's role that enhance its overall security posture and ensure that sensitive data and assets are not available from potential threats.
- **Nuisance Hackers (Amateurs)** – These individuals engage in hacking with limited skill and often act out of curiosity rather than malicious intent. However, their activities can still cause damage.
- **Activist Hackers (Hacktivists)** – These hackers use cyberattacks to promote political or social causes. They may target institutions to expose perceived injustices.

- **Criminal Hackers (Black Hat Hackers)** – These hackers operate illegally for financial gain, stealing data, committing fraud, or deploying ransomware.
- **Nation-State Actors** – Government-sponsored hackers that conduct cyber espionage, disrupt services, or steal intellectual property for geopolitical advantage.

The Greatest Cyber Threat to Flyer College

Flyer College faces multiple cybersecurity threats, but criminal hackers and nation-state actors pose the most significant risks. Criminal hackers are likely to target student data and financial records for identity theft and fraud, while nation-state actors may exploit vulnerabilities to gain unauthorized access for espionage or disruption. Given the sensitive nature of Flyer College's data, the primary focus should be defending against these threats through defensive security measures and ethical hacking assessments.

Penetration Testing Team Requirements

Flyer College must engage a professional and ethical penetration testing team to strengthen security. The following are the key requirements for the team:

Professionalism and Integrity

- The team must have a proven history of ethical behavior and expertise in penetration testing.
- They should possess recognized cybersecurity certifications (e.g., CEH, OSCP, CISSP).

Background Checks

- All penetration testers must undergo a comprehensive background check to verify their credibility and ensure they have no history of unethical hacking or criminal activities.

Defined Scope and Limitations

To mitigate potential risks, the penetration testing engagement must establish stringent limitations, which include:

1. Strictly restricted to pre-approved systems (student and financial aid records databases).
2. No access to faculty or student personal devices.
3. Testing must occur outside peak operational hours to avoid disruptions.
4. No social engineering tactics (e.g., phishing) on staff or students.
5. All vulnerabilities must be communicated and reported but never exploited.

Data Handling Protocols

- All data accessed during testing must be appropriately managed and encrypted.
- No penetration tester can copy or store sensitive data beyond the testing scope.

Incident Response and Reporting

In case of discovering a breach during testing, the following steps must be taken:

1. Immediately stop testing to prevent further exposure.
2. Notify the IT director (Joe Williams) and security team.
3. Document the vulnerability and provide a risk assessment.
4. Recommend immediate mitigation steps.
5. Continue monitoring for signs of exploitation post-assessment.

Accountability Measures

To ensure compliance, the contract must include penalties for any violation, such as:

- Financial penalties for exceeding the testing scope.
- Termination of the contract if ethical standards are violated.
- Mandatory reporting of any misconduct to the appropriate authorities.

Conclusion

Flyer College must proactively address cyber threats by methodically classifying potential adversaries and identifying high-risk ones. Contracting a qualified penetration testing team is essential for this initiative. The institution can effectively enhance its defenses and safeguard its digital assets by implementing rigorous security protocols and ethical hacking practices. By carefully selecting a penetration testing team and adhering to established cybersecurity best practices, Flyer College will strengthen its security posture and fulfill its duty to protect the sensitive data of all stakeholders.

References

Bellaby, R. W. (2021, February 12). *An ethical framework for hacking operations - ethical theory and moral practice*. SpringerLink. https://link.springer.com/article/10.1007/s10677-021-10166-8

Madnick, B., Huang, K., & Madnick, S. (2023). The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process. *Information Security Journal: A Global Perspective*, *33*(3), 204–225. https://doi.org/10.1080/19393555.2023.2201482

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015, June 10). *The classification of hackers by Knowledge Exchange Behaviors - Information Systems Frontiers*. SpringerLink. https://link.springer.com/article/10.1007/s10796-015-9567-0