ADVERSARY EMULATION CAMPAIGN HINT

1.Understand Your Objectives: Your primary aim is to mimic the tactics, techniques, and procedures (TTPs) of real-life adversaries to test and strengthen your organization's defenses. Make sure your objectives align with this.
2. Scope Appropriately: Define what is within the scope of your operation and stick to it. This includes systems, networks, and physical spaces.
3.Leverage Threat Intelligence: Use up-to-date threat intelligence to make your emulation as realistic as possible. Choose an adversary whose TTPs you will emulate.
4.Follow the ATT&CK Framework: The MITRE ATT&CK framework is a great guide for emulating adversary behavior. It provides comprehensive information about different TTPs.
5.Multi-Vector Attacks: Real adversaries won't limit themselves to just one vector. Consider including multiple attack vectors in your emulation.
6.Emphasize Stealth: Adversaries will typically try to avoid detection. Your red team should emulate this by using stealthy techniques and avoiding unnecessary noise.
7.Use Tools Wisely: Use a blend of off-the-shelf tools, custom software, and manual techniques. Remember, it's about emulating the adversary, not the tools they use.
8.Practice Safe Operations: Make sure you're not causing actual harm to your organization. Always have a rollback plan in case something goes wrong.
9.Include Social Engineering: Many adversaries use social engineering techniques. Including these in your emulation can make it more realistic and test your human defenses.
10.Regularly Update Skills: The cybersecurity landscape is continually evolving, and so are adversaries. Regular training and education, like the courses offered by SANS, Zero Point, SpecterOps and Others, can help you keep up.
11.Test Incident Response: Your emulation should not only test your defenses but also your response capabilities. How quickly and effectively can your organization respond to a breach?
12.Use Deception: Plant false flags or deceptive information to emulate sophisticated adversaries and test your blue team's analytical capabilities.
13.Real-Time Adjustments: Monitor the operation and make real-time adjustments as necessary. A real adversary would change their tactics if they were not working, and so should you.
14.Post-Operation Analysis: After the operation, conduct a thorough analysis. What worked, what didn't, and why?
15.Share Knowledge: Lessons learned should be shared across your organization to improve overall security. Use the red team operation as a learning tool, not just a test.

Tools: Atomic Red Team, Cobalt Strike, Caldera, RTA, Infect Monkey, Covenant or SliverC2

https://www.linkedin.com/in/joas-antonio-dos-santos