

Training:

Hacking Bureaucracy

Date of the online training: **October 26-27, 2021**

Overview

Bureaucracies didn't start out as soul-crushing obstructions to innovation and agility, but you can't escape them today. Whether you're in government, industry, school, or an independent practitioner, you face relentless bureaucracies that impede progress, destroy morale, and frustrate security. Not taught in schools or other institutional learning facilities, this course plays to the puzzle-solving superpowers of the hacker mindset. Come learn how to achieve your personal and organizational goals effectively and legally, by hacking the system.

In theory, bureaucracy isn't a bad thing. Really. Bureaucracy allows large organizations to scale and accomplish complex missions that would otherwise be impossible. In practice however, bureaucracies easily become their own worst enemy. Particularly vulnerable are the innovative people, new missions, and agile organizations essential for success in information security and cyber operations. You can't escape the bureaucracy, but you can hack it.

If navigated appropriately, success is possible despite the bureaucracy, and sometimes even because of it. Hackers are adept at bending complex systems to their will, and bureaucracies are nothing if not complex systems. The techniques, tactics, and rules of the game are a bit different in the bureaucratic domain, but the hacker mindset is the same.

This course provides strategies for hacking bureaucracy that everyone can apply. To be clear, we are not suggesting anything illegal, but instead offering ways to accomplish legitimate objectives using legitimate means despite the mountains of TPS reports you may have to face.

We'll cover:

- Understanding bureaucracies as complex systems.

- Knowing when to fight, when to route around, and when to socially engineer.
- Reverse engineering the stated and actual power networks in organizations.
- Operating from the outside-in, from the inside-out, and from within organizations.
- Applying OSINT and HUMINT methodologies to gather intelligence.
- Threat analysis and risk assessment.
- Planning, wargaming, actions, and intended and unintended effects.
- Working within legal and ethical constraints.
- Case studies of real world examples.
- Most importantly, hundreds of offensive and defensive bureaucracy hacking TTPs: for the individual, the leader, and the organization.

This interesting and fast-moving class will include hands-on exercises to apply and reinforce the skills learned. You'll leave this course with a fresh perspective and a toolkit of techniques to better accomplish your mission.

The views expressed in course are those of the author(s) and do not reflect the official policy or position of their current or past employers, the Department of Defense, or the United States Government.

Who should attend this training and why?

All professionals in information security and those in complementary disciplines would enjoy and benefit from this class. The course is designed to address hacking all types of bureaucracies, whether government, corporate, military, or academic, so participants from all areas will find this course valuable. English-speaking international students are also welcome. Bureaucracies exist everywhere and the lessons we'll provide will be generally applicable to all.

Prerequisites

No formal prerequisites. Students at all levels would gain from this course, but experience with bureaucracies is a plus :)

About the Trainers

Greg Conti is a Co-Founder and Principal at Kopidion, a cyber security training and professional services firm. Formerly he served as Director of Security Research at IronNet. He served on the West Point faculty for more than a decade where he led their cybersecurity research and education efforts. During his career in the Army he served in a variety of Signals Intelligence and Cyber Operations assignments, deploying to Iraq as Officer-in-Charge of U.S. Cyber Command's Expeditionary Cyber Support Team and as a Senior Advisor in the U.S. Cyber Command Commander's Action Group where he co-developed the Joint Advanced Cyber Warfare Course. Gregory is the co-author of the recently published book, *On Cyber: Towards an Operational Art for Cyber Operations* (Kopidion Press), as well as approximately 100 articles and papers covering online privacy, usable security, cyber conflict, and security visualization. He has spoken at numerous security conferences, including Black Hat, DEFCON, RSA, ShmooCon, BSides Delhi, Google Ideas, and the NATO Conference on Cyber Conflict. Greg holds a B.S. from West Point, an M.S. from Johns Hopkins University, and a Ph.D. from the Georgia Institute of Technology, all in computer science. He may be found at www.gregconti.com, on Twitter as @cyberbgone and at @kopidion_llc.

Booking

Recommended online booking of trainings through:

<https://tickets.ernw.de/troopers/tr21training/>

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German.
+49 6221 480390 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hm-ts.de

+49 6022 5089999 / <https://www.hm-ts.de>