1400 - Hacking the Cloud

Thursday at 14:00 in 101 Track
45 minutes | Demo
Gerald Steere*Cloud Wrecker, Microsoft*

Sean Metcalf*CTO, Trimarc*

You know the ins and outs of pivoting through your target's domains. You've had the KRBTGT hash for months and laid everything bare. Or have you?

More targets today have some or all of their infrastructure in the cloud. Do you know how to follow once the path leads there? Red teams and penetration testers need to think beyond the traditional network boundaries and follow the data and services they are after. This talk will focus on how to take domain access and leverage internal access as a ticket to your target's cloud deployments.

We will also discuss round trip flights from cloud to on-premises targets and what authorizations are required to access your target's cloud deployments. While this talk is largely focused on Microsoft Azure implementations, the concepts can be applied to most cloud providers.
Gerald Steere
Gerald Steere has been a member of the C+E Red Team since joining Microsoft in June 2014. He regularly dives into the deepest corners of Azure looking for vulnerabilities unique to the cloud scale environment and collecting all the creds. Prior to that, he was a security auditor and penetration tester for three civilian Federal agencies, where he acquired a love for obtaining and cracking as many passwords as possible. He has spoken on cloud security topics at multiple BlueHat events and most recently at BSides Seattle.

@darkpawh
Sean Metcalf
Sean Metcalf is founder and principal consultant at Trimarc Security, LLC (www.TrimarcSecurity.com), which focuses on mitigating, detecting, and when possible, preventing modern attack techniques. He is one of about 100 people in the world who holds the Microsoft Certified Master Directory Services (MCM) certification, is a Microsoft MVP, and has presented on Active Directory attack and defense at BSides, Shakacon, Black Hat, DEF CON, and DerbyCon security conferences.

Sean has provided Active Directory and security expertise to government, corporate, and educational entities since Active Directory was released. He currently provides security consulting services to customers and regularly posts interesting Active Directory security information on his blog, ADSecurity.org.

@pyrotek3

#defcon25/by_track/101/thursday #defcon25/By_Day/_thursday