RED TEAM & OPERATIONAL SECURITY

It's The Little Things That Matter

Dark Vortex LLP

© 2021 Dark Vortex LLP

Table of Contents

Day 1

Day 2

- Antivirus and Sandbox evasion
- Internal Reconnaissance
- Local Privilege Escalation
- Local Persistence
- Active Directory Situational Awareness
- Domain Reconnaissance
- Kerberos Overview
- Active Directory and Kerberos Attacks
    - Kerberoasting
    - Golden Tickets
    - Silver Tickets Attacks
    - Pass The Hash
    - Pass The Ticket
    - DCSync
    - LDAP Sentinel
    - Bloodhound - Visualizing Attack Paths
    - Domain Privilege Escalation
- Day 2 - Lab

© 2021 Dark Vortex LLP

Day 3

- Security Token Manipulation
- Advanced Domain Tactics and Techniques
  - Lateral Movement with SMB, RPC, COM Objects
  - ACL and GPO Abuse
  - Trust Abuse in domain environment
  - Constraint and Unconstrained delegation
- Mission Completion and Data Exfiltration
- OPSEC Considerations
  - Reflective DLLs
  - PowerShell and C# weaponization
  - Phishing Campaigns and Sandboxes
  - Unhooking EDRs
- Day 3 – Lab

© 2021 Dark Vortex LLP

Target Audience

- Red Team members
- Penetration Testers
- Blue Teamers
- Threat Hunters

All security engineers/professionals wanting to learn advanced offensive tactics and procedures (TTPs) and information security professionals looking to advance their skillsets.

Requirements

- A laptop with 16GB RAM to support 2 VMs running at the same time.
- Understanding of operating system architecture
- Basic understanding of development
- Strong will to learn and creative mindset.

What all do you get in the end

- 3 days of rigorous training program
- 3 days of Red Team simulation lab access
- Course PDF and content materials
- Brute Ratel Trial License during the Course

For any queries, contact paranoidninja@0xdarkvortex.dev

© 2021 Dark Vortex LLP