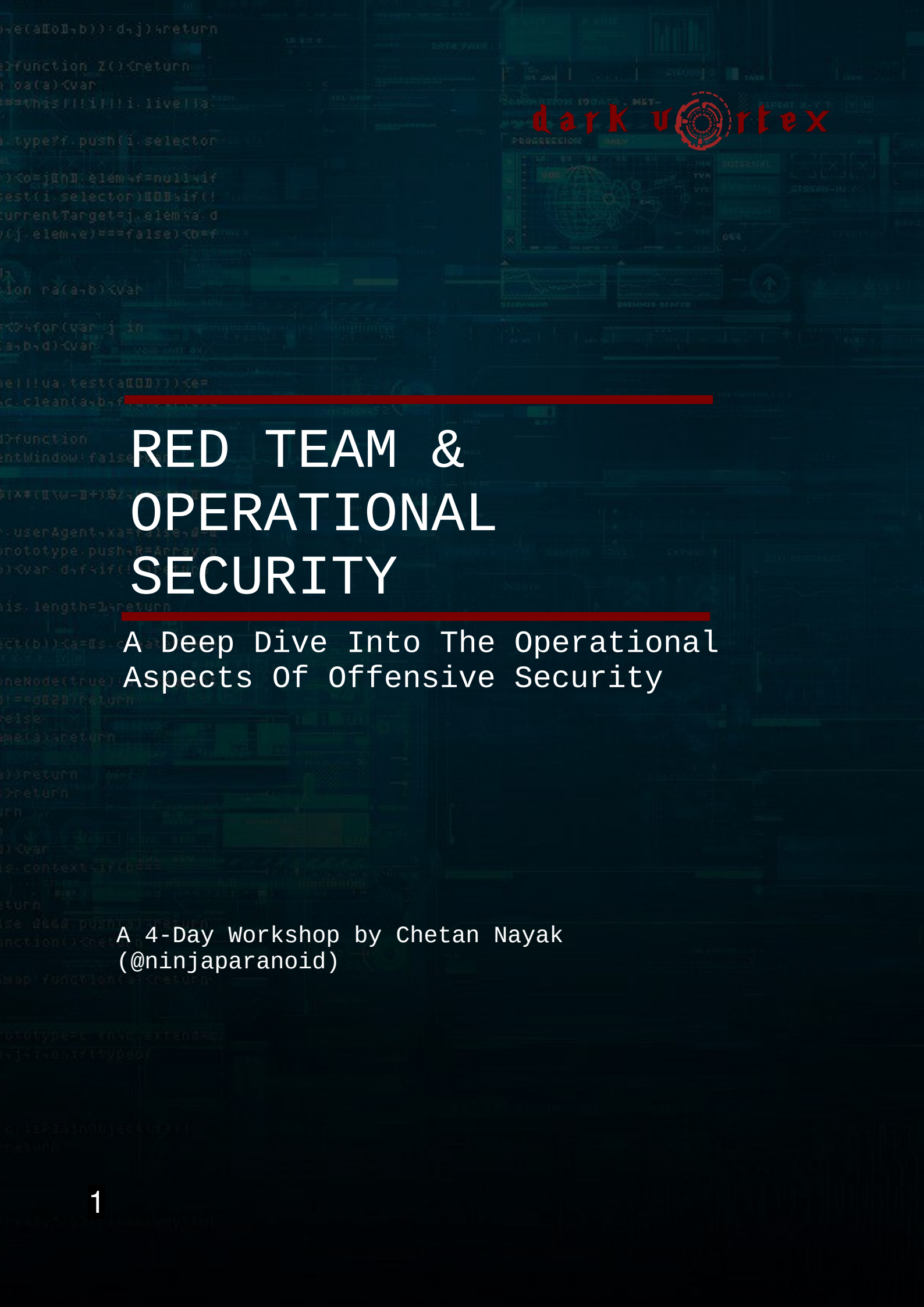

RED TEAM & OPERATIONAL SECURITY

A Deep Dive Into The Operational Aspects Of Offensive Security

A 4-Day Workshop by Chetan Nayak (@ninjaparanoid)

Table Of Contents

Day 1

- Enabling Event Audit Logging
- Configuring Sysmon for Analyzing Incident Events

Day 2

- Initial Access Payloads
  - Finding DLL Sideloads
  - Caveats of DLL Sideloading
  - HTA – HTML Applications
    - Executing Shellcode from Jscript
  - AppLocker Bypasses
    - C-Sharp Weaponization
    - Process Injections in C-Sharp
    - Bitflipping Lolbins
  - Packaging Payloads with MSI for Initial Access
  - Code Signing Payload Packages
  - Packaging Payloads in ISO
  - Callback Shellcode in C
- Initial Access Lab
- Post-Exploitation
  - C-Sharp Toolkit
    - Walking through various C-Sharp Open Source Tools
    - OpSec Considerations with C-Sharp Tooling
    - C-Sharp v/s Badger Object Files (BOFs)
  - Internal Reconnaissance with WinAPI (BRC4)

        - Host Enumeration
        - User Enumeration
        - Local Group Policy Enumeration
        - In-Memory WMI Enumeration
        - User and Host Monitoring
    - Writing BOFs for Brute Ratel C4
    - Bring Your Own Injections with BOFs
    - Fork & Run (Process Injections) v/s BOF

Day 3

- Privilege Enumeration and Escalation
    - Vulnerable Services
    - Unquoted Service Path
    - Sysvol and Microsoft LAPS
    - Service Hijacking
- Local Persistence (BRC4)
    - Service and Service Triggers
    - Task Scheduler
    - Registry
    - DLL Sideloads
    - Autoruns
    - COM Object Model
    - COM Interactions
    - COM Hijacking
    - COM Backdoors and Persistence
- Active Directory Situational Awareness

- Forests, Domains, Sites and Trusts
- Computers and Users
- Group Policy & Active Directory Objects
- Machine Account v/s User Account
- Password Hashing
- Active Directory Certificates

- Domain Reconnaissance
  - Group Policy Analysis
  - User Sessions
  - Service Accounts
  - Password Policies
  - PowerView and SharpView
  - AD Explorer: Local v/s Socks
  - LDAP Sentinel (BRC4)
  - Writing RAW LDAP Queries for User and System Enumeration
- Windows Credentials
  - Windows Access Tokens
  - Token Impersonation
  - Hot-Swapping Tokens
  - Security Accounts Manager
  - Mimikatz
    - Password Extraction
    - Memory Dumping
    - Kerberos Ticket Enumeration
    - Data Protection API (DPAPI)
      - Google Chrome and Credential Manager

- Manual DPAPI Key Decryption

Day 4

- Domain Lateral Movement
  - SMB and RPC Pivoting
  - BRC4 PsExec Pivoting
  - TCP Pivoting
  - WinRM and PowerShell Pivoting
  - Fileless WMI Queries and WMI Execution
  - Service Diversion
  - Socks Tunneling
    - Remote Desktop
    - SSH Tunneling
    - Windows Attack Tool Proxying
- Advanced Active Directory Domain Attacks
  - The Kerberos Realm
  - Kerberoasting and S4U2self Abuse
  - AS-REP Roasting
  - Golden Tickets
  - Silver Tickets Attacks
  - Pass The Hash
  - Pass The Ticket
  - Password Cracking for Tickets
  - DCSync
  - ACL, SACL, DACL and GPO Abuse
    - Exploiting Group Policy Creator Owners

        - Exploiting Group Permissions with Recursive LDAP Queries
        - SID Hunting For Privileged Active Directory Rights
    - Trust Abuse in Domain Environment
        - Trust Abuse Privilege Escalation
        - Pivoting Across Domains in a Forest
        - DnsAdmins Exploitation
    - Constrained and Unconstrained Delegation
    - Active Directory Certificate Abuse (ADCS)
        - SAN Enrollment
        - Vulnerable Certificate Templates
        - SAN Abuse and Requesting Authentication Certificates
        - Privilege Escalation and Lateral Movement

Target Audience

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

This intense 4-day workshop is designed for security professionals who want to enhance their skills by digging more deeper than the usual Red Team. This course will give you a deep dive towards various Operational tasks and issues and how to overcome them during a Red Team.

Requirements

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

What all do you get in the end

- 4 days of rigorous workshop
- Course PDF, and content materials
- Multiple Virtual Machines to practice the lab offline in the candidate’s own environment.

For any queries, contact paranoidninja@0xdarkvortex.dev