Master Class

PAULA
Januszkiewicz,
CQURE

Hacking and Securing Windows Infrastructure

span | Arena

AGENDA:

Day 1 – May 17, 2025 (Saturday)

Work hours: 9am – 5pm

Registration, coffee and snack

Module 1: Understanding Windows Platform

1. Introduction to the Windows 10/11 and Windows Server security concepts
2. Architecture overview
3. Key System Components
    a. Processes, Threads and Jobs
    b. Services, Functions and Routines
    c. Sessions
    d. Objects and Handles
    e. Registry
4. Rights, permissions and privileges
5. Access Tokens
6. Win32 API

Module 2: Modern Attack Techniques

1. Discussion: Top attack techniques
2. Advanced Persistent Threats
3. Initial access vectors
    a. Phishing – rev shell mail phishing blob
    b. Valid Credentials – password spray exc.
    c. Spoofing – DNS Twist
    d. Vulnerable components (drive by download)
    e. Weak defaults
    f. Other vectors

Module 3: Local Privilege Escalation Techniques

1. Escalation through Windows Services
    a. Unquoted service path
    b. Image and DLL manipulation
2. Schedule Tasks
3. Access Token Manipulation
    a. Selmpersonate
    b. SeTcb
    c. Create User Token
4. Process Injection
5. DLL Injection and Reflective DLL Injection
6. Create Remote Thread
7. Process memory (powerpick/psinject)
8. Memory injection
9. Other techniques

Lunch

Module 4: Securing Offline Access

1. Offline Access techniques
2. TPM Architecture
3. Implementing BitLocker
4. Discussing Bit Locker

Module 5: Windows Authentication

1. Architecture & cryptography
    a. Windows Logon
    b. Windows Logon Types
    c. LSASS Architecture
    d. NTLM
    e. Kerberos
    f. Token Based Authentication – PRT
2. SAM Database
3. NTDS.dit
4. LSA Secrets & gMSA accounts
5. Secrets, credentials and Logon Data
6. SSP Providers
7. Data Protection API

Coffee break

Module 6: Attacks on Identity Infrastructure

1. Pass- the- Hash, OverPTH attacks
    a. Pass the ticket
    b. Golden and silver ticket
    c. Pass the PRT
    d. Shadow Credentials/ NGC
2. NBNS/LLMNR spoofing, NTLM Relay, Kerberoasting
3. DCSync and DCShadow
4. AdminSDholder
5. Other identity attack techniques

Day 2, May 18, 2025 (Sunday)

Work hours: 9am – 5pm

Coffee and snack

Module 7: Protecting Identity in the Modern Infrastructure

1. Credential Guard
2. LAPS
3. LSA Protection
4. SMB Signing and Encryption
5. Managing Krbtgt
6. Detection of the identity attacks
7. Monitoring AD Infrastructure
8. Analyzing complex AD infrastructure (Bloodhound, Pingcastle, etc.)

Module 8: Hybrid Deployment

1. Hybrid Identity
2. Account synchronization using Azure AD Connect
3. Password Hash Synchronization
4. Pass-through Authentication
5. Seamless SSO
6. Federation with Active Directory Federation Services

Module 9: Attack and protection of MSSQL

1. Offline access
2. TDS Injection
3. Weak Authentication Schema
4. Securing MSSQL server instance
5. TDE Encryption
6. Extracting credentials

Lunch

Module 10: Secure Active Directory Certificate Services (PKI)

1. Reviewing misconfigurations
2. Misusing certificates
3. Implementing best practices
4. Kill- Chain with certificates

Module 11: Windows Infrastructure Services

1. Securing and monitoring DNS Service
2. Securing and monitoring Internet Information Services
3. Securing the File Server

Coffee break

Module 12: Securing Windows Platform

1. Malware protection approach
2. Implementing Application Whitelisting
3. Configuring Exploit Guard
4. Attack Surface Reduction Rules
5. Controlled Folder Access
6. Reviewing security benchmarks

Summary: Top 50 tools: the attacker's and defender's best friends

1. Practical walkthrough through tools
2. Tools for Red Team/ Pentesters
3. Tools for Blue Team