LAPORAN PENETRATION TESTING: CICADA HTB

INFORMASI PROYEK

Nama Target: Cicada HTB
Alamat IP: 10.10.11.35
Tipe Environment: Windows Active Directory
Tingkat Kesulitan: Medium
Tanggal Testing: [Tanggal Pelaksanaan]

RINGKASAN EKSEKUTIF

Penetration testing terhadap lingkungan Windows Active Directory Cicada HTB berhasil mengkompromi domain secara penuh melalui serangkaian teknik enumerasi, eksploitasi kredensial, dan eskalasi hak akses. Testing dimulai dari external reconnaissance hingga berhasil mendapatkan akses sebagai Domain Administrator. Proses ini menunjukkan beberapa kelemahan keamanan kritis dalam konfigurasi Active Directory dan manajemen hak akses.

METODOLOGI PENGETESAN

1. Reconnaissance - Pemindaian jaringan dan enumerasi layanan
2. Initial Access - Akses awal melalui SMB share
3. Lateral Movement - Perpindahan antar akun pengguna
4. Privilege Escalation - Eskalasi hak akses ke Domain Admin
5. Post-Exploitation - Pengumpulan kredensial dan bukti kompromi

TEMUAN DETAIL

1. Enumerasi Jaringan Awal

Tools: Nmap
Command: nmap -sV -sO 10.10.11.35
Hasil: Teridentifikasi beberapa port terbuka termasuk layanan SMB, LDAP, dan WinRM yang menjadi initial attack vector.

2. Kelemahan SMB Share Configuration

Tools: smbclient, NetExec
Temuan: Share HR dapat diakses tanpa autentikasi
Dampak: Ekspos dokumen internal berisi kredensial default
Kredensial yang Ditemukan: Cicada$M6Corpb*@Lp#nZp!8

Command yang Digunakan:
smbclient -L //10.10.11.35/
smbclient //10.10.11.35/HR

3. User Enumeration via RID Brute-force

Tools: NetExec
Teknik: RID brute-forcing untuk enumerasi user domain
Hasil: Teridentifikasi multiple user accounts termasuk michael.wrightson

Command:
netexec smb cicada.htb -u -p "" --rid-brute

4. Credential Validation dan Lateral Movement

Proses: Validasi kredensial yang ditemukan terhadap user yang terenumerasi
Hasil: User michael.wrightson menggunakan kredensial yang ditemukan di SMB share

Command:
netexec smb cicada.htb -u michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8' --shares

5. LDAP Information Disclosure

Tools: ldapsearch, NetExec
Temuan: Ekspos kredensial user tambahan melalui query LDAP
Kredensial Baru: aRt$Lp#7t*VQ!3 untuk user david.orelious

6. Backup Script Analysis

Akses: SMB share DEV menggunakan kredensial david.orelious
Temuan: File Backup_script.ps1 berisi kredensial plaintext
Kredensial: Cicada123! untuk user Cicada

7. Initial Compromise via WinRM

Tools: Evil-WinRM
Akses: Remote system access menggunakan kredensial yang ditemukan
Hasil: Berhasil mendapatkan user flag dari desktop user

8. Privilege Escalation via SeBackupPrivilege

Vulnerability: Misuse of SeBackupPrivilege
Teknik: Abuse backup privileges untuk membaca file SAM/SYSTEM
Proses:

- Verifikasi privileges dengan whoami /priv
- Ekstraksi SAM dan SYSTEM registry hives
- Credential dumping menggunakan pypykatz

Commands:
reg save hklm\sam C:\Temp\sam
reg save hklm\system C:\Temp\system
pypykatz registry --sam sam system

9. Domain Administrator Access

Hasil: Berhasil mendapatkan kredensial Administrator domain
Akses: Full domain compromise melalui Evil-WinRM
Bukti: Root flag berhasil diambil dari administrator desktop

TOOLS YANG DIGUNAKAN

- Nmap - Network scanning dan service detection
- smbclient - SMB share enumeration dan access
- NetExec - SMB/LDAP enumeration dan credential spraying
- ldapsearch - LDAP directory querying
- Evil-WinRM - Windows Remote Management access
- pypykatz - Credential extraction dari registry hives

SKILLS YANG DITUNJUKKAN

Technical Skills

- Network reconnaissance dan service enumeration
- Active Directory reconnaissance (SMB, LDAP, user enumeration)
- Credential hunting dan password reuse attacks
- Lateral movement across user accounts
- Windows privilege escalation techniques
- Credential dumping dan hash extraction
- Windows Remote Management utilization

Analytical Skills

- Attack path mapping dan vulnerability chain analysis
- Systematic approach to penetration testing
- Documentation dan reporting capabilities

REKOMENDASI KEAMANAN

1. Access Control Hardening

- Implementasi autentikasi untuk semua SMB shares

- Review dan restriksi share permissions berdasarkan principle of least privilege
- Implementasi network segmentation untuk sensitive shares

2. Password Security Improvements

- Eliminasi hardcoded credentials dalam scripts dan dokumentasi
- Implementasi strong password policy dengan complexity requirements
- Enable account lockout policies setelah multiple failed attempts
- Regular password rotation dan audit

3. Privilege Management

- Review user privileges khususnya SeBackupPrivilege
- Implementasi principle of least privilege untuk semua service accounts
- Regular privilege access reviews dan audits

4. Monitoring dan Detection

- Implementasi monitoring pada SMB access logs
- Alert mechanisms untuk multiple failed authentication attempts
- Monitoring untuk unusual LDAP query patterns
- Detection untuk credential dumping activities

PENCAPAIAN

- User Flag Captured - Bukti kompromi user-level access
- Root Flag Captured - Bukti full domain compromise
- Complete Attack Chain Demonstration - External to domain admin compromise
- Multiple Attack Vectors - Demonstrasi berbagai teknik penetration testing

KESIMPULAN

Penetration testing terhadap environment Cicada HTB berhasil mengdemonstrasikan kompleksitas attack chains dalam environment Windows Active Directory. Serangkaian miskonfigurasi dan kelemahan keamanan memungkinkan attacker dari external network untuk mencapai full domain compromise melalui methodical approach yang mencakup enumerasi, credential exploitation, dan privilege escalation.

Project ini memberikan valuable insights tentang pentingnya defense-in-depth strategy dalam environment Windows Active Directory dan menunjukkan kemampuan praktikal dalam identifying, exploiting, dan documenting security vulnerabilities.