# Pen Test Diary

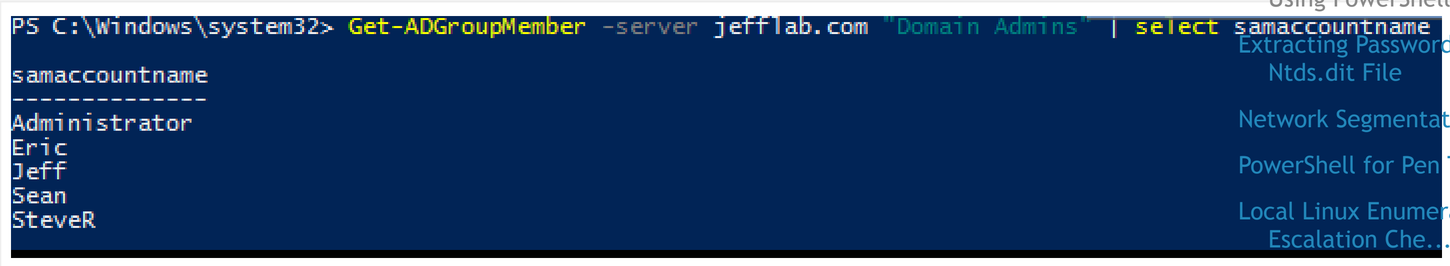
Minggu, 27 Agustus 2017

## Performing Domain Reconnaissance Using PowerShell

The first thing any attacker will do once he gains a foothold within an Active Directory domain is to try to elevate his access. It is surprisingly easy to perform domain reconnaissance using PowerShell, and often without any elevated privileges required. In this post, we will cover a few of the different ways that PowerShell can be used by attackers to map out your environment and chose their targets.

### The Basics of Reconnaissance using PowerShell

First, let’s look at how PowerShell can be used for discovering some of the most basic, high-value assets. The end-goal for any attacker is to compromise a member of Domain Admins or Enterprise Admins. To build out a list of targets, some basic PowerShell will show you what accounts are members of those groups.



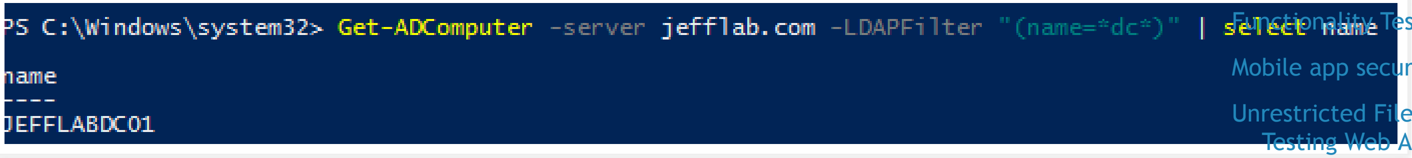
```
PS C:\Windows\system32> Get-ADGroupMember -server jefflab.com "Domain Admins" | select samaccountname

samaccountname
--------------
Administrator
Eric
Jeff
Sean
SteveR
```

Also of interest is building out a list of high-value servers such as Domain Controllers, file servers and database servers. We will explore some more advanced ways to do this shortly, but some basic queries can give you some quick insight into these systems. With simple filters on computer names, computer descriptions, group membership and OU location, you

Arsip Blog

▼ 2017 (57)
- ► Desember (1)
- ► November (1)
- ► Oktober (1)
- ► September (8)
- ▼ Agustus (46)
  - Citrix Desktop Breakout
  - NFS, no_root_squash and SUID - Basic NFS Security
  - Web Protocols
  - Performing Domain Reconnaissance Using PowerShell
  - Extracting Password Hashes from the Ntds.dit File
  - Network Segmentation
  - PowerShell for Pen Testers
  - Local Linux Enumeration & Privilege Escalation Che...
  - Penetration testing methodologies
  - Public Vulnerability Database Resources
  - Active Directory Roles

can quickly build a list of target computers to compromise.

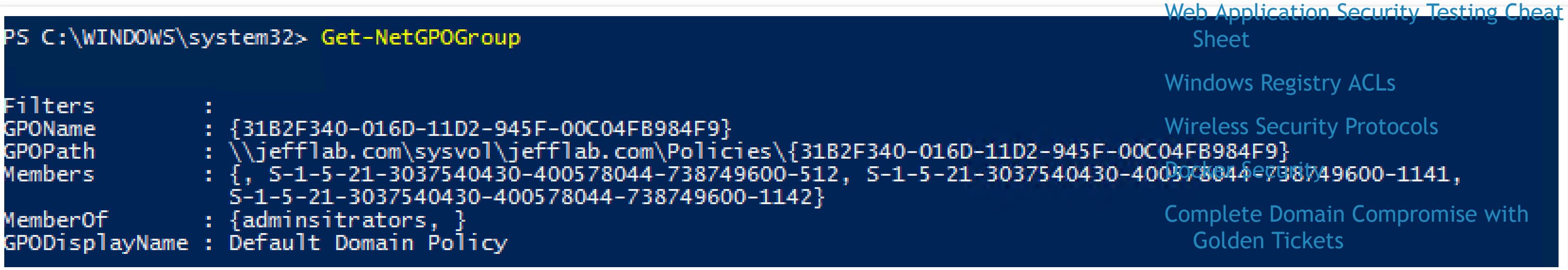


```
PS C:\Windows\system32> Get-ADComputer -server jefflab.com -LDAPFilter "(name=*dc*)" | select name

name
----
JEFFLABDC01
```

## Performing Reconnaissance with PowerSploit

PowerSploit is a PowerShell-based penetration-testing platform that offers several useful modules for performing domain recon. These modules allow attackers to quickly traverse the network and gather valuable intelligence to formulate an attack plan.

One example of the insight PowerSploit can provide by looking into Active Directory is the Get-NetGPOGroup command. This command enumerates all GPOs at the domain and expands the Restricted Groups settings to see where users have been granted local group memberships through GPOs. By running this, you can quickly get a full listing of all users that have been granted local privileges across the domain, providing a valuable list of target accounts that will surely have elevated privileges. Also, it requires no rights to the computers themselves because this information is all retrieved from GPOs on the Domain Controllers.



```
PS C:\WINDOWS\system32> Get-NetGPOGroup


Filters        :
GPOName        : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPOPath        : \\jefflab.com\sysvol\jefflab.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
Members        : {, S-1-5-21-3037540430-400578044-738749600-512, S-1-5-21-3037540430-400578044-738749600-1141,
                 S-1-5-21-3037540430-400578044-738749600-1142}
MemberOf       : {adminsitrators, }
GPODisplayName : Default Domain Policy
```

Additional modules such as Find-GPOLocation let you search for an individual user and find all of the computers to which she has been assigned local privileges through GPOs.

Some of the other interesting modules supported by PowerSploit include:

- **Invoke-FileFinder** – This command finds sensitive files on hosts by traversing shared folders looking for specified search criteria.
- **Invoke-ShareFinder** – This command will quickly build a list of non-standard shared folders, without investigating the files stored within them.
- **Find-LocalAdminAccess** – This will return a list of the members of the Adminsitrators group on specified systems.

Cryptography

Functionality Testing a IDS/IPS

Mobile app security testing checklist

Unrestricted File Upload Security Testing Web Appl...

Pre-Engagement Interactions

Network Security VAPT Checklist

Penetration Testing Guidelines

CVSS for Penetration Test Results

Active Directory Delegation Security Issues

Kerberos Working

Cisco Network Penetration Testing

Cisco Router Hardening

Mini Penetration Testing Framework

Web Application Security Testing Cheat Sheet

Windows Registry ACLs

Wireless Security Protocols

Docker Security

Complete Domain Compromise with Golden Tickets

PowerShell AMSI Bypass

Network Infrastructure Penetration Testing

Windows Privilege Escalation Scripts

Linux Privilege Escalation Scripts

MSSQL Database Penetration Testing

Oracle Database Penetration Testing

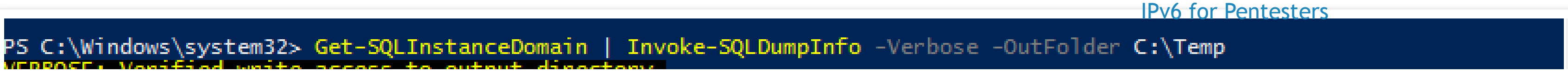
IPsec VPN Penetration Testing

VOIP Penetration Testing Cheat Sheets

## Targeting Databases with PowerUpSQL

PowerUpSQL is a PowerShell Toolkit that is geared towards attacking SQL Servers. Database servers are a highly-valued target due to the likelihood they contain sensitive information. The Get-SQLInstanceDomain command will retrieve information on all accounts with registered Service Principal Names (SPNs) from the domain, indicating where Microsoft SQL databases are installed. This is performed without requiring any rights to the database servers themselves, since this information is all registered in Active Directory.

By coupling this command with the Invoke-SQLDumpInfo command, it is possible to extract the vulnerabilities, privileges and other configurations from all domain-joined SQL databases with minimal effort.



```
PS C:\Windows\system32> Get-SQLInstanceDomain | Invoke-SQLDumpInfo -Verbose -OutFolder C:\Temp
VERBOSE: Verified write access to output directory.
```

## Protecting Against Reconnaissance

Domain reconnaissance is very difficult to prevent. Most of the information in Active Directory is readable to all domain user accounts by design, so any compromised account can be used to perform this level of discovery. Monitoring LDAP traffic and detecting abnormal queries is the most proactive way to respond to domain reconnaissance. Reducing the attack surface within your domain is the best course of prevention to be sure whatever is discovered cannot easily be used against you.

di 23.02

## Tidak ada komentar:

## Posting Komentar

- Metasploit Cheat Sheets
- Wireless Hacking WiFu
- Applocker Bypass Technique
- Packet Crafting
- CREST CCT Application Exam
- Windows Patch Management Strategies
- Persistence
- Lateral Movement
- IPv6 for Pentesters

Masukkan komentar Anda...

Beri komentar sebagai: Google Accoun ▼

Publikasikan Pratinjau

Posting Lebih Baru Beranda Posting Lama

Langganan: Posting Komentar (Atom)

Tema Sederhana. Diberdayakan oleh Blogger.