11-Internal Password Spraying - from Windows

From a foothold on a domain-joined Windows host, the DomainPasswordSpray **tool is highly effective.** If we are authenticated to the domain, the **tool will automatically generate a user list from Active Directory, query the domain password policy, and exclude user accounts within one attempt of locking out**. Like how we ran the spraying attack from our Linux host, we can also supply a user list to the tool if we are on a Windows host but not authenticated to the domain. **We may run into a situation where the client wants us to perform testing from a managed Windows device in their network that we can load tools onto**. We may be **physically on-site in their offices and wish to test from a Windows VM, or we may gain an initial foothold through some other attack, authenticate to a host in the domain and perform password spraying in an attempt to obtain credentials for an account that has more rights in the domain.**

شرح العملية خطوة بخطوة:

DomainPasswordSpray : https://github.com/dafthack/DomainPasswordSpray

1. وجودك على جهاز متصل بالدومين:

- لو وصلت لجهاز ويندوز عضو في الدومين (Domain-Joined)، ده معناه إنك تقدر تتواصل مع Active Directory مباشرة.
- **DomainPasswordSpray** هي أداة بتساعدك في إجراء **Password Spraying** بطريقة ذكية.

---

2. الأداة بتعمل حاجات أوتوماتيكية:

- **استخراج قائمة المستخدمين (User List):**
  - لو انت متصل بالدومين ومُصادَق عليك (Authenticated)، الأداة هتستخرج قائمة بالحسابات من Active Directory.
- **سياسة كلمة المرور (Password Policy):**
  - الأداة بتقرأ سياسة كلمات المرور الخاصة بالدومين (زي عدد المحاولات المسموحة قبل ما الحساب يتقفل - Account Lockout Policy).
- **تجنب إغلاق الحسابات (Lockouts):**

- الأداة بتستثني الحسابات اللي قربت توصل للحد الأقصى من المحاولات الفاشلة (مثلاً لو باقي محاولة واحدة قبل القفل).

---

3. لو مش متصل بالدومين:

- لو مش معاك صلاحية مصادقة على الدومين:
  - ممكن توفر للأداة قائمة حسابات يدوياً (User List) وتحاول تعمل **Password Spraying** بنفس الطريقة.

سيناريوهات الاستخدام:

1. **اختبار من جهاز ويندوز مدار داخل شبكة العميل:**
   - لو العميل عايزك تنفذ الهجوم من جهاز ويندوز موجود في شبكته.
   - ممكن تكون في مكاتب العميل (On-Site) أو على جهاز افتراضي (VM) مخصص للاختبار.
2. **الوصول الأولي (Foothold):**
   - لو حصلت على جهاز ويندوز عضو في الدومين من خلال هجوم أولي (مثلاً عبر ثغرة).
   - تستخدم الجهاز ده عشان تحاول ترقى صلاحياتك بالحصول على بيانات حسابات أكتر.

هدف الهجوم:

- **الحصول على حساب بصلاحيات أعلى:**
  - الهدف الأساسي من الهجوم هو الوصول لحساب بصلاحيات عليا (زي **Domain Admin**).
- **التنقل الأفقي داخل الشبكة (Lateral Movement):**
  - بعد الحصول على حسابات أكتر، ممكن توسع نطاق وصولك للشبكة بالكامل.

---

use tool

There are several options available to us with the tool. Since the host is domain-joined, we will skip the `-UserList` flag and let the tool generate a list for us. We'll supply the `Password` flag and one single password and then use the `-OutFile` flag to write our output to a file for later use.

هنا ان مثلا مش بستخدم اي ip or domain علشان الاداة هي مش بتحتاج اي حاجة من دول هو بس لو انتا شخص علي domain ودي الميزة بتاعت الاداة

```
PS C:\htb> Import-Module .\DomainPasswordSpray.ps1
PS C:\htb> Invoke-DomainPasswordSpray -Password Welcome1 -OutFile
spray_success -ErrorAction SilentlyContinue

[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] The smallest lockout threshold discovered in the domain is 5 login
attempts.
[*] Removing disabled users from list.
[*] There are 2923 total users found.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 2923 users gathered from the current
user's domain
[*] The domain password policy observation window is set to  minutes.
[*] Setting a  minute wait in between sprays.

Confirm Password Spray
Are you sure you want to perform a password spray against 2923 accounts?
[Y] Yes  [N] No  [?] Help (default is "Y"): Y

[*] Password spraying has begun with  1  passwords
[*] This might take a while depending on the total number of users
[*] Now trying password Welcome1 against 2923 users. Current time is 2:57 PM
[*] Writing successes to spray_success
[*] SUCCESS! User:sgage Password:Welcome1
[*] SUCCESS! User:tjohnson Password:Welcome1

[*] Password spraying is complete
[*] Any passwords that were successfully sprayed have been output to
spray_success
```

Mitigations

Several steps can be taken to mitigate the risk of password spraying attacks. While no single solution will entirely prevent the attack, a defense-in-depth approach will render password spraying attacks extremely difficult.

Technique	Description
`Multi-factor Authentication`	Multi-factor authentication can greatly reduce the risk of password spraying attacks. Many types of multi-factor authentication exist, such as push notifications to a mobile device, a rotating One Time Password (OTP) such as Google Authenticator, RSA key, or text message confirmations. While this may prevent an attacker from gaining access to an account, certain multi-factor implementations still disclose if the username/password combination is valid. It may be possible to reuse this

Technique	Description
	credential against other exposed services or applications. It is important to implement multi-factor solutions with all external portals.
`Restricting Access`	It is often possible to log into applications with any domain user account, even if the user does not need to access it as part of their role. In line with the principle of least privilege, access to the application should be restricted to those who require it. نحط حدود مثلا للحاجة ااي هستخدمها ونمنع مثلا عنه تطبيقات معينة
`Reducing Impact of Successful Exploitation`	A quick win is to ensure that privileged users have a separate account for any administrative activities. Application-specific permission levels should also be implemented if possible. Network segmentation is also recommended because if an attacker is isolated to a compromised subnet, this may slow down or entirely stop lateral movement and further compromise. انه ينتشر في الشبكة **attacker** هنا مثلا تعزل الشبكة عن شبكة بحيث مينفعش
`Password Hygiene`	Educating users on selecting difficult to guess passwords such as passphrases can significantly reduce the efficacy of a password spraying attack. Also, using a password filter to restrict common dictionary words, names of months and seasons, and variations on the company's name will make it quite difficult for an attacker to choose a valid password for spraying attempts.