

**Information Security COMP 451 A**

**Project Phase 1: Project Proposal**

Ayesha Wajid (22-10070)

Mutahara Salman (21-11447)

Menahil Zafar (22-10476)

**Domain PasswordSpray**

Domain PasswordSpray is a tool which is written in PowerShell to perfrom a password spray attack against the users of a domain. Password spraying attacks attempt to authenticate into multiple user accounts using the same password. And so, because of this coorporate networks are frequently under attack as tracking down usernames from a company is easy task with the help of OSINIT techniques, by using simple networks such as Facebook or Linkedin.

This tool will automatically create the userlist from the domain whether a user delivers username(s) at runtime or not. If runtime userlist is delivered, then it would be matched against the auto-generated list and all user-provided usernames that meet the following criteria will be omitted from the final spray list:

* Locked out
* Disabled
* Expired
* Nonexistent
* Within 1 bad password attempt of a lockout

**Steps:**

The steps to conduct an password spraying attacks are

* Acquire a list of usernames:

It starts with a list of accounts. This is easier than it sounds. Most organizations have a formal convention for emails, such as **firstname.lastname@company.com**. This allows adversaries to construct usernames from a list of employees. If the bad actor has already compromised an account, they may try to enumerate usernames against the domain controller. Or, they find or buy usernames online.

* Spray passwords:

Finding a list of common passwords is even easier. A Bing search reveals that publications list the most common passwords each year. **123456**, **password**, and **qwerty** are typically near the top.

* Gain Access:

Eventually one of the passwords works against one of the accounts. Attacker only needs password and username and after that they can have access of the account.

**Outcomes:**

After following the steps above mentioned attacker can have hold of the account.

This attack can be found commonly where the application or admin sets a default password for the new users.

**Our Input:**

There are several password spraying programs available for use with many different sorts of additional fascilities. In order to make the domainpassword spray more efficient and popular. We would add the feature of attacking from multiple domains rather than a single one. These attempts would be randomized between the domain controllers and services such as (LDAP).

**References**

1. <https://resources.infosecinstitute.com/topic/top-tools-for-password-spraying-attacks-in-active-directory-networks/>
2. <https://github.com/sbinsaleem/DomainPasswordSpray>
3. <https://buaq.net/go-10107.html>