Detecting password spraying attacks within Active Directory environments

Data required

- Data: Azure Active Directory audit data
- Data: Windows event logs

To optimize the searches shown below, you should specify an index and a time range.

Scenario

In a password spraying attack, attackers use one or a small list of commonly used or popular passwords against a large volume of usernames to acquire valid account credentials. This tactic can be used to obtain an initial access to an environment, and can also be used to escalate privileges when access has been already achieved.

In some scenarios, password spraying capitalizes on the password rotation security policies implemented by most organizations. As users change their passwords, it is possible that some pick predictable or seasonal passwords that match commonly used passwords on the attacker's password lists.

These searches detect possible password spraying attacks against Active Directory environments, using Windows Event Logs in the Account Logon and Logon/Logoff Advanced Audit Policy categories. The searches help identify instances where one source user, source host, or source process attempts to authenticate against a target or targets using an unusually high number of unique users, which is not common behavior for legitimate systems.

Detection searches

- Multiple disabled or invalid users failing to authenticate from host using Kerberos protocol

To successfully implement this search, your deployment needs to ingest domain controller and Kerberos events. The Advanced Security Audit policy setting Audit Kerberos Authentication Service within the Account Logon settings needs to be enabled.

This search is designed to identify a source endpoint failing to authenticate with multiple disabled or invalid users using the Kerberos protocol. This behavior could be indicative of an adversary performing a password spraying attack against an Active Directory environment using Kerberos to obtain initial access or elevate privileges. A host failing to authenticate with multiple disabled domain users is not a common behavior for legitimate systems.

The search looks for for event 4768, which is generated every time the Key Distribution Center issues a Kerberos
Ticket Granting Ticket.

The search calculates the standard deviation for each host and uses a 3-sigma statistical rule to identify an unusual number of users. It only triggers on domain controllers, not on member servers or workstations.

To customize the search, you can try different combinations of the bucket span time and the calculation of the upper bound field. You can also investigate returned events further by adding in fields such as source IP and attempted user accounts.

| search (Account_Name!="*$" EventCode=4768 Result_Code=<failure code> eventtype=wineventlog_security) | bucket span=2m _time | stats dc(Account_Name) AS unique_accounts values(Account_Name) AS tried_accounts BY _time, Client_Address | eventstats avg(unique_accounts) AS comp_avg , stdev(unique_accounts) AS comp_std BY Client_Address | eval upperBound=(comp_avg + (comp_std * 3)), isOutlier=if(((unique_accounts > 10) AND (unique_accounts >= upperBound)),1,0) | search isOutlier=1

Enter one of the following failure code in the search above to filter to either disabled or invalid users:

<table>
<thead>
<tr>
<th>User type</th>
<th>Search lines to use</th>
<th>Failure code explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled users</td>
<td></td>
<td>search (Account_Name!=&quot;*$&quot; EventCode=4768 Result_Code=0x12 eventtype=wineventlog_security)</td>
</tr>
<tr>
<td>Invalid users</td>
<td></td>
<td>search (Account_Name!=&quot;*$&quot; EventCode=4768 Result_Code=0x6 eventtype=wineventlog_security)</td>
</tr>
</tbody>
</table>

Multiple valid users failing to authenticate from host using Kerberos protocol

To successfully implement this search, your deployment needs to ingest domain controller and Kerberos events. The Advanced Security Audit policy setting Audit Kerberos Authentication Service within the Account Logon settings needs to be enabled.

This search is designed to identify a source endpoint failing to authenticate with multiple valid users using the Kerberos protocol. This behavior could be indicative of an adversary performing a password spraying attack against an Active Directory environment using Kerberos to obtain initial access or elevate privileges.

This search looks for event 4771, which is generated when the Key Distribution Center fails to issue a Kerberos Ticket Granting Ticket (TGT). Failure code 0x18 indicates that the wrong password has been provided for a legitimate domain user.

The search calculates the standard deviation for each host and uses a 3-sigma statistical rule to identify an unusual number of users. It only triggers on domain controllers, not on member servers or workstations.

To customize the search, you can try different combinations of the bucket span time and the calculation of the upper bound field. You can also investigate returned events further by adding in fields such as source IP and attempted user accounts.
user accounts.

A host failing to authenticate with multiple valid domain users is not a common behavior for legitimate systems. Possible false positive scenarios include vulnerability scanners, misconfigured systems, and multi-user systems like Citrix farms.

| search (Account_Name!="*" EventCode=4771 Failure_Code=0x18 eventtype=wineventlog_security) | bucket span=2m_time | stats dc(Account_Name) AS unique_accounts values(Account_Name) AS tried_accounts BY _time, Client_Address | eventstats avg(unique_accounts) AS comp_avg, stdev(unique_accounts) AS comp_std BY Client_Address | eval upperBound=(comp_avg + (comp_std * 3)), isOutlier=if(((unique_accounts > 10) AND (unique_accounts >= upperBound)),1,0) | search isOutlier=1

▶ Multiple disabled or invalid users failing to authenticate from host using NTLM protocol

To successfully implement this search, your deployment needs to ingest domain controller events. The Advanced Security Audit policy setting Audit Credential Validation within the Account Logon settings needs to be enabled.

This search is designed to identify a source endpoint failing to authenticate with multiple valid or invalid users using the NTLM protocol. This behavior could be indicative of an adversary performing a password spraying attack against an Active Directory environment using NTLM to obtain initial access or elevate privileges.

The search looks for event 4776, which is generated on the computer that is authoritative for the provided credentials.

- For domain accounts, the domain controller is authoritative.
- For local accounts, the local computer is authoritative.

A host failing to authenticate with multiple valid or invalid domain users is not a common behavior for legitimate systems. Possible false positive scenarios include vulnerability scanners and misconfigured systems.

The search calculates the standard deviation for each host and uses a 3-sigma statistical rule to identify an unusual number of users. It only triggers on domain controllers, not on member servers or workstations.

To customize the search, you can try different combinations of the bucket span time and the calculation of the upper bound field. You can also investigate returned events further by adding in fields such as source workstation name and attempted user accounts.

| search (Logon_Account!="*" <error code> EventCode=4776 action=failure eventtype=wineventlog_security) | bucket span=2m_time | stats dc(Logon_Account) AS unique_accounts values(Logon_Account) AS tried_accounts BY _time, Source_Workstation | eventstats avg(unique_accounts) AS comp_avg, stdev(unique_accounts) AS comp_std BY Source_Workstation | eval upperBound=(comp_avg + (comp_std * 3)), isOutlier=if(((unique_accounts > 10) AND (unique_accounts >= upperBound)),1,0) | search isOutlier=1

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Enter one of the following error code in the search above to filter to either valid or invalid users:

<table>
<thead>
<tr>
<th>User type</th>
<th>Search lines to use</th>
<th>Error code explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid users</td>
<td></td>
<td>search (Logon_Account!=&quot;*$&quot; 0xC000006A EventCode=4776 action=failure eventtype=wineventlog_security)</td>
</tr>
<tr>
<td>Invalid users</td>
<td></td>
<td>search (Logon_Account!=&quot;*$&quot; 0xC0000064 EventCode=4776 action=failure eventtype=wineventlog_security)</td>
</tr>
</tbody>
</table>

**Multiple users attempting to authenticate using explicit credentials**

To successfully implement this search, your deployment needs to ingest Windows Event Logs from domain controllers, member servers, and workstations. The Advanced Security Audit policy setting Audit Logon within the Logon/Logoff settings needs to be enabled.

This search identifies a source user failing to authenticate with multiple users using explicit credentials on a host. This behavior could be indicative of an adversary performing a password spraying attack against an Active Directory environment to obtain initial access or elevate privileges.

This search looks for event 4648, which is generated when a process attempts an account logon by explicitly specifying that accounts credentials.

The search calculates the standard deviation for each host and uses a 3-sigma statistical rule to identify an unusual number of users. This event generates on domain controllers, member servers, and workstations. The search triggers on the potentially malicious host which may be being controlled via a Trojan or operated by a malicious insider.

To customize the search, you can try different combinations of the bucket span time and the calculation of the upper bound field. You can also investigate returned events further by adding in fields such as source account, attempted user accounts and the endpoint where the behavior was identified.

A source user failing attempting to authenticate multiple users on a host is not a common behavior for regular systems. Some applications, however, may exhibit this behavior in which case sets of users hosts can be added to an allow list. Possible false positive scenarios include systems where several users connect to, such as mail servers, identity providers, remote desktop services, and Citrix.
To successfully implement this search, your deployment needs to ingest Windows Event Logs from domain controllers, member servers, and workstations. The Advanced Security Audit policy setting Audit Logon within Logon/Logoff settings needs to be enabled.

This search is designed to identify a source process name failing to authenticate with multiple users. This behavior could be indicative of an adversary performing a password spraying attack against an Active Directory environment to obtain initial access or elevate privileges.

This search looks for event 4625, which generates on domain controllers, member servers, and workstations when an account fails to log on. It also searches for Log On Type 2, which describes an interactive log on attempt.

The search calculates the standard deviation for each host and uses a 3-sigma statistical rule to identify an unusual number of users. The search triggers on the potentially malicious host which may be being controlled via a Trojan or operated by a malicious insider. This could be a domain controller, member server, or workstation.

To customize the search, you can try different combinations of the bucket span time and the calculation of the upper bound field. You can also investigate returned events further by adding in fields such as source process name, source account, and attempted user accounts.

A process failing to authenticate with multiple users is not a common behavior for legitimate user sessions. Possible false positive scenarios include vulnerability scanners and misconfigured systems.
Multiple users remotely failing to authenticate from host

To successfully implement this search, your deployment needs to ingest domain controller events. The Advanced Security Audit policy setting **Audit Logon** within Logon/Logoff settings needs to be enabled.

This search is designed to identify a source host failing to authenticate against a remote host with multiple users. This behavior could be indicative of an adversary performing a password spraying attack against an Active Directory environment to obtain initial access or elevate privileges.

This search looks for event 4625, which indicates every failed attempt to log on to a local computer. The event generates on domain controllers, member servers, and workstations. It also looks for log on Type 3 which describes an remote authentication attempt.

The search calculates the standard deviation for each host and uses a 3-sigma statistical rule to identify an unusual number of users. The search triggers on the host that is the target of the password spraying attack. This could be a domain controller as well as a member server or workstation.

To customize the search, you can try different combinations of the bucket span time and the calculation of the upper bound field. You can also investigate returned events further by adding in fields such as source process name, source account, and attempted user accounts.

A host failing to authenticate with multiple valid users against a remote host is not a common behavior for legitimate systems. Possible false positive scenarios include vulnerability scanners, remote administration tools, and misconfigured systems.

Additional resources

The searches in this guide are also included in Enterprise Security, which provides more information about how to implement them successfully in your security maturity journey. If you have questions about this use case, see the Security Research team's support options on GitHub. In addition, these Splunk resources might help you understand and implement this use case:

- Newly added Active Directory credentials
• Detecting lateral movement with Active Directory data
• Managing Azure cloud infrastructure
• Conducting an Azure new user census