Blog Data Security

How to Investigate NTLM Brute Force Attacks

This post explains the process the Varonis IR team follows to investigate NTLM Brute Force attacks, which are common incidents reported by customers.

Ed Lin | 6 min read | Last updated November 2, 2022

Malicious actors routinely use the NTLM authentication protocol to carry out account enumeration and brute force-styled attacks to compromise accounts within a victim's network. Once inside, an attacker can gain persistence, exfiltrate sensitive data, and unleash ransomware.

In this post, we will cover the fundamentals of NTLM and its security flaws, as well as the workflow the Varonis IR Team uses to investigate these NTLM brute force attacks.

users and computers on the network. It uses a challenge/response mechanism for authentication which allows users to prove their identities without sending a password over the network.

Despite being replaced by more secure authentication protocols and having multiple known vulnerabilities, NTLM is still widely deployed today because of its compatibility with legacy systems and applications.

What are Account Enumeration and Brute Force?

In general, brute force attacks involve using trial and error to work through possible user name and password combinations in order to compromise an account.

Account enumeration is a more specific type of brute force attack where the attacker is attempting to guess the valid usernames of users within a network. These attacks are typically done when the malicious actor has limited information about their victim’s network.

Depending on the complexity of the attack, the guessed username attempts could be something basic like “Admin” or “Guest” or more sophisticated like using the naming convention that is currently being utilized at the organization, e.g. “JSmith3”.

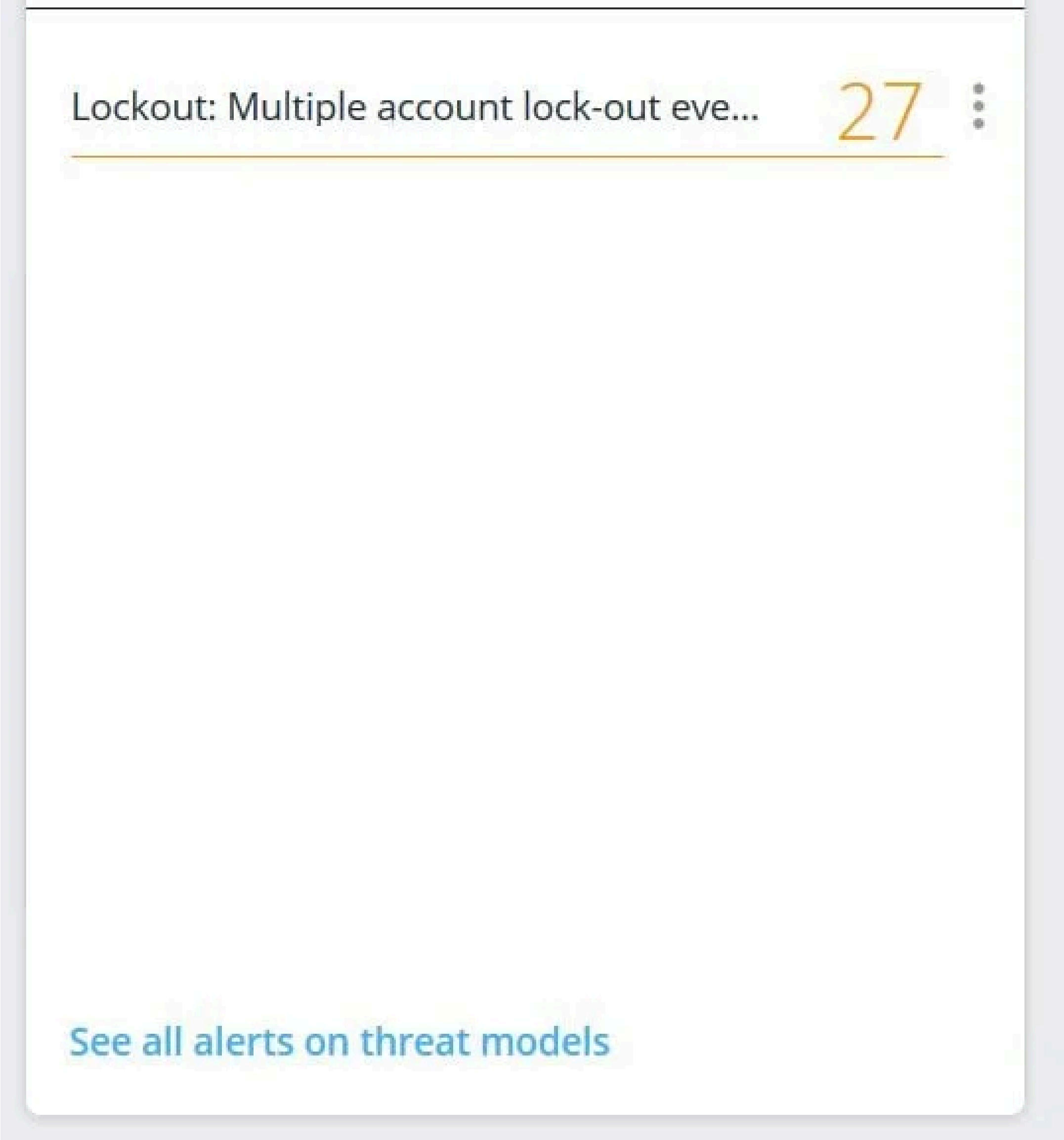
Additionally, if you or your organization has experienced a similar scenario, we recommend additional scrutiny when investigating as you may be more susceptible to future attacks.

Once a threat actor has successfully identified existing usernames, they will begin brute forcing those users to compromise their passwords and gain access to the network. As a result, it is imperative to identify and remediate these account enumeration attacks in order to prevent a cyber attack in its beginning stages.

Detecting NTLM Brute Force Attacks with Varonis

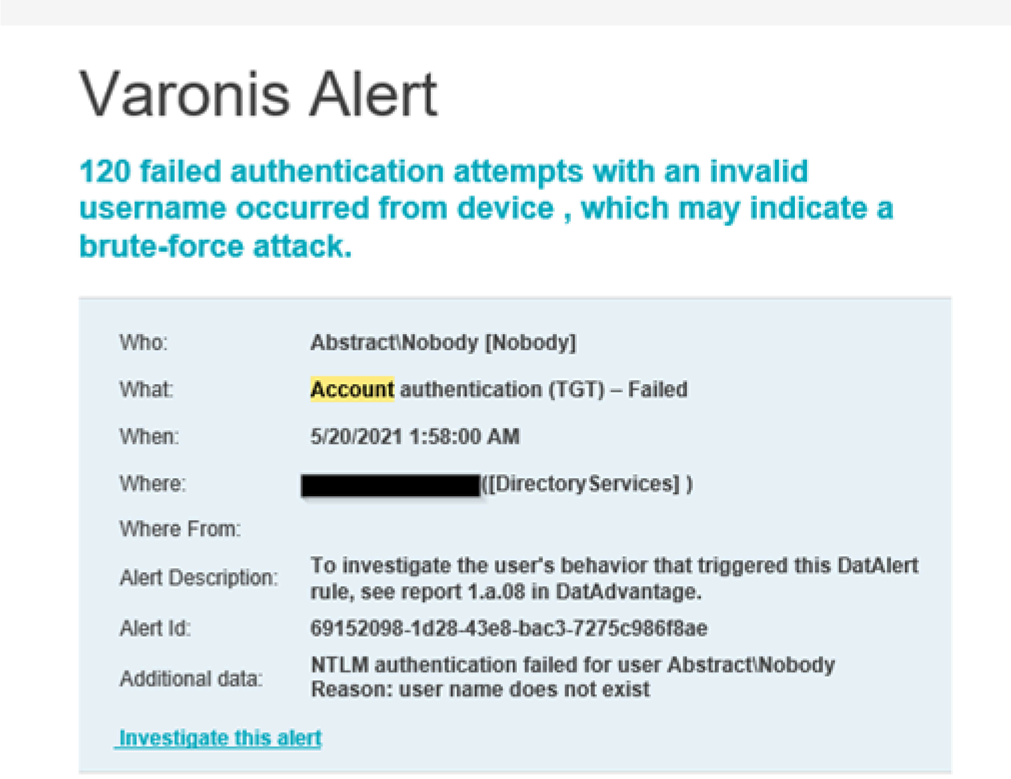
Some of which include:

- Password spraying attack from a single source
- Account Enumeration Attack from a single source (using NTLM)
- Lockout: Multiple account lockouts
- Abnormal Behavior: an unusual amount of lockouts across end-user/service/admin accounts



Lockout: Multiple account lock-out eve... 27

You can also search for all failed authentication behavior in the Varonis Dashboard to look for suspicious activity that you want to investigate.



Varonis Alert

120 failed authentication attempts with an invalid username occurred from device , which may indicate a brute-force attack.

Who:	Abstract\Nobody [Nobody]
What:	Account authentication (TGT) – Failed
When:	5/20/2021 1:58:00 AM
Where:	[redacted]([DirectoryServices])
Where From:	
Alert Description:	To investigate the user's behavior that triggered this DatAlert rule, see report 1.a.08 in DatAdvantage.
Alert Id:	69152098-1d28-43e8-bac3-7275c986f8ae
Additional data:	NTLM authentication failed for user Abstract\Nobody Reason: user name does not exist

Investigate this alert

1. Preparing the Investigation in Varonis via the WebUI

Click “**Analytics**” in the Varonis Dashboard.

Select “**DirectoryServices”** in the Servers dropdown.

Filter for Authentication Events by typing “**Account Authentication (TGT)**” This will give you all the events related to attempted logins for the specified time.

Now search for all NTLM authentications that failed due to a bad username by adding “**User Name (Event By) = Nobody (Abstract)**,” and “**Authentication Protocol = NTLM**” drilling down on all NTLM attempts that failed due to having an incorrect username.

Additionally, if you are seeing any of the previously mentioned alerts such as “**Account Enumeration Attack from a single source (using NTLM)**,” you can view directly the related events that triggered this alert.

If you are not seeing any relevant alerts, please continue onto **Step 2**.

Click and open a new tab for alerts by clicking on the plus sign and selecting “**Alerts**”. Run a query searching for “**Account Enumeration Attack from a single source (using NTLM)**” or any of the related brute force alerts and click “**Run Search**”.

Hover over “**Actions**” beneath the search bar and click “**View all Related Events**”

2. Investigating the Events in Varonis via the WebUI

Now that you have the relevant events, there will be four columns that will be helpful during the investigation:

+ Event Description
+ Device Name
+ Event Time
+ Collection Device Hostname

Make sure they are present by clicking on “**Attributes**” and by searching for each of the column tiles in the newly opened window and selecting them

Within the event view, you are looking for failed logins for usernames that do not match your naming convention by using the “Event Description” column. Generic account names like “administrator,” “admin,” “root,” or “service,” can indicate a dictionary-style NTLM brute force attack.

Other examples of generic account names may be other simple names like “john,” “aaa,” and “test.” You may even see usernames from foreign languages as well.

your corporate naming conventions.

Attackers commonly use device names like “Windows10” or “mstsc” in an attempt to obfuscate their activity. Sometimes they’ll leave the device name entirely empty. Some of the most commonly spoofed device names include:

- Rdesktop
- Remmina
- Freerdp
- Windows7
- Windows8
- Windows2012
- Windows2016
- Windows2019

If you are seeing generic account names that do not match your naming convention in combination with spoofed or null device names, it is likely that your organization is being targeted by an account enumeration attack.

Add the spoofed device names to the search bar and select all monitored resources in the Server dropdown.

By looking at all activity from the spoofed devices, you can determine if there are immediate signs of account compromise such as successful authentications.

You can also filter by all successful events from this suspicious device by clicking on the "**Status**" hyperlink on the left and selecting "**Success**" in the window that pops up. For example, account lockout events would be considered a successful event while the underlying failed authentications would not.

Moreover, if there are lockouts from these devices or if there are multiple attempts to authenticate to actual usernames, it is highly likely that the attacker has successfully identified valid usernames and is now attempting to log in via password brute forcing.

Above: We can assume that this admin account has been successfully enumerated by the attacker as a valid user since it has been locked out.

pivoting a search to look for all activity from these locked-out accounts could be a useful query as well.

Finally, take note of the "**Collection Device Hostname**" for these authentication attempts. This is the Domain Controller (DC) we need to prioritize during the next phase of the investigation. Since the device name is often spoofed or null, we will need to enable additional logging to identify the actual device being attacked.

3. Preparing NTLM auditing

In this section, we will focus on ensuring that the proper configurations are in place to capture the most helpful events for the investigation.

More specifically, you will need to use **Event ID 8004** in Event Viewer to identify the actual device that is on the receiving end of these NTLM brute force attack attempts. Locating the victim device will be the first step in the remediation process.

8004 events are typically not enabled by default and may require configuration changes in specific Domain Controller group policies to enable logging.

Log in to a Domain Controller and open Group Policy Management Editor

Navigate to the Default Domain Controllers Policy and Right-Click to select Edit.

The Group Policy Management Editor will open. Navigate to **Policies>Windows Settings>Security Settings>Local Policies**" and select "**Security Options**."

There are three security policies that we will need to configure:

- Network security: Restrict NTLM: Audit Incoming Traffic = Enable auditing for all accounts
- Network security: Restrict NTLM: Audit NTLM authentication in this domain = Enable all
- Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers = Audit all

Change these values by right-clicking and selecting “**Properties**” and then define the policy settings. Click Apply when finished.

Run “**gpupdate /force**” to apply these changes and begin collecting these events.

4. Investigating NTLM logs in Event Viewer

Navigate to the DC that you identified based on “**Collection Device Hostname**” in step 1.

Right-click and select “**Properties**”.

Expand the storage size of this log from the default 1MB to a larger size (we recommend 20MB as a starting point).

You can now use **Event ID 8004** events to investigate malicious authentication activity.

Use the **Find** function to search for the device name or user names we saw the attacker using in **Step 1**.

Once you are able to find an 8004 event that matches one of the malicious authentications events in the WebUI, use the “**Secure Channel Name**” field to identify the device the attacker is targeting.

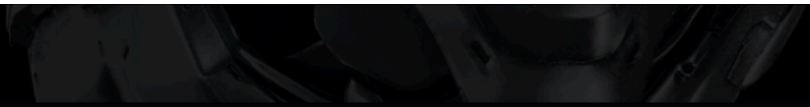
5. Remediation

Once we identify the victim device, we can identify how the attacker is sending these authentication attempts. There are a few different sources of data that you can investigate:

- Check firewall logs for connection activity that occurred at the same time as the authentication attempts.
- Log on to the victim device and use tools such as Netstat or Wireshark **(only do this if you see no indications of a successful suspicious authentication on that device!)**

Attackers will use tools like Shodan to search for devices with publicly exposed ports, which is likely how they found this victim device in the first place.

You should identify the IP address and port the attacker is using to send the authentication requests. One port, in particular, **RDP** or **port 3389** has been one of the most commonly targeted ports by threat actors, especially given the recent rise of remote workers.



Keep reading

Varonis tackles hundreds of use cases, making it the ultimate platform to stop data breaches and ensure compliance.

Identify and Investigate Business Email Compromise (BEC) Scams

Ed Lin

February 10, 2022

In this post, we'll review how to spot Business Email Compromise Scams and walk you through an investigation with Varonis.

Addressing New Federal IT Work From Home Risks

David Harrington

March 24, 2021

This federal IT working from home guide will cover the risks involved and potential solutions.

GDPR: The Right to Be Forgotten and AI

Michael Buckbee
March 29, 2020

One (of the many) confusing aspects of the EU General Data Protection Regulation (GDPR) is its “right to be forgotten”. It’s related to the...

What is a Brute Force Attack? Definition

Michael Buckbee
December 8, 2021

A brute force attack (also known as brute force cracking) is the cyberattack equivalent of trying every key on your key ring, and eventually...

Platform

Overview
DSPM
AI Security
Data Discovery & Classification
Cloud DLP
Policy Automation

Coverage

Microsoft 365 & Entra ID
File Shares & NAS
SaaS
IaaS
Databases
View all coverage

Resources

Support
Community
Blog
Webinars
Events
Varonis Threat Labs

Company

About Varonis
Careers
Investor Relations
Public Sector
Partner Program
Newsroom

CSPM

Compliance Management

Email Security

Identity Security

Athena AI

Data Access Governance

English

Trust Center | Privacy Policy