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

Objective

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.

Get the Free Pentesting Active Directory Environments E-Book

This site uses cookies to provide you with a better browsing experience. To learn more about the different cookies we're using, please see our privacy policy.

Accept Decline

I agree to receive communications from Varonis.*

You can unsubscribe from these communications at any time. For more information on our privacy practices, and how we're committed to protecting your information, please review our privacy policy.

Download Now

What is NTLM?

NTLM or "New Technology LAN Manager" is a protocol developed by Microsoft to authenticate 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.

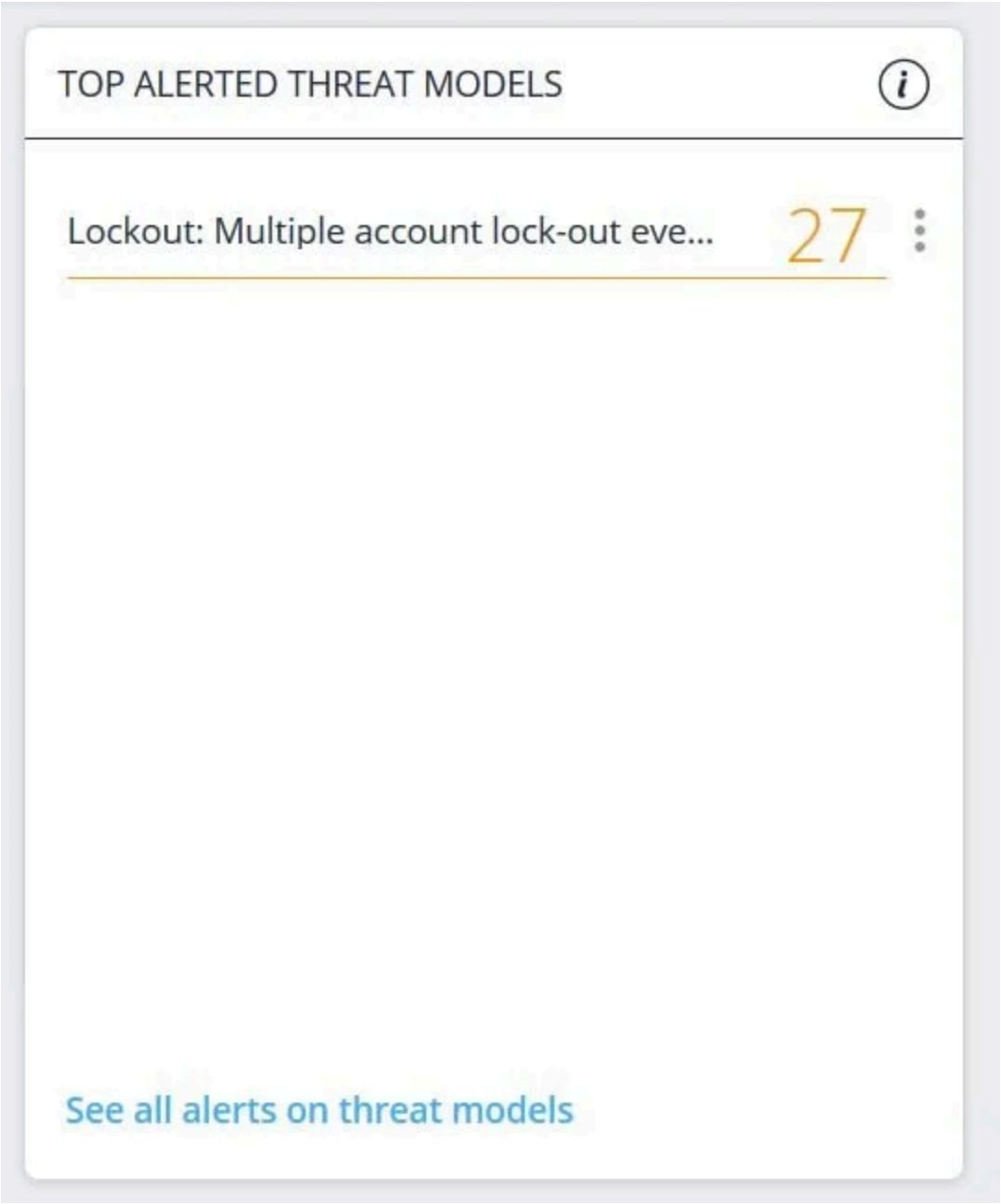
Detecting NTLM Brute Force Attacks with Varonis

There are several types of alerts that you can see in the **Varonis Alert Dashboard** or via **email** that may indicate that there is an ongoing **NTLM Brute Force Attack**.

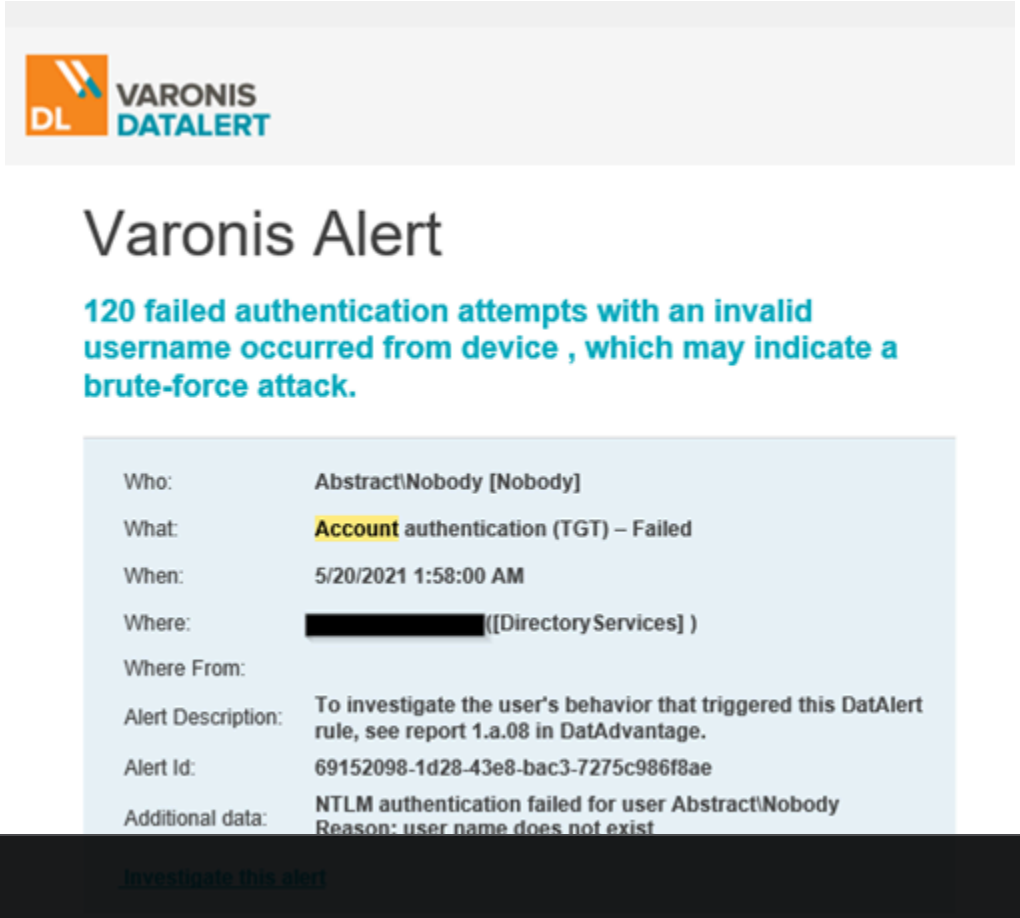
Some of which include:

+ Password spray [illegible]
+ Account Enumeration Attack from a single source (using NTLM)
+ Lockout: Multiple account lockouts

This site uses cookies to provide you with a better browsing experience. To learn more about the different cookies we're using, please see our privacy policy.



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



This site uses cookies to provide you with a better browsing experience. To learn more about the different cookies we're using, please see our privacy policy.

1. Preparing the Investigation in Varonis via the WebUI

Click "**Analytics**" in the Varonis Dashboard.

Select "**DirectoryServices**" in the Servers dropdown.

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**"

Varonis uses "**Abstract/Nobody**" as a placeholder in the User Name column for usernames that do not exist in AD. By searching for events with "**Abstract/Nobody**," you are effectively 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**"

This will bring you to an audit log of all the related authentication attempts related to this specific alert.

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:

This site uses cookies to provide you with a better browsing experience. To learn more about the different cookies we're using, please see our privacy policy.

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

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.

The “Device Name” may also be a spoofed device name from the attacker’s authentication requests. Most likely, you won’t recognize these device names as these also will not follow 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.

This site uses cookies to provide you with a better browsing experience. To learn more about the different cookies we're using, please see our privacy policy.

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.

When an account is locked out due to an account enumeration attack, we highly recommend disabling this enumerated account and changing its password for a stronger one. Additionally, 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.

This site uses cookies to provide you with a better browsing experience. To learn more about the different cookies we're using, please see our privacy policy.

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.

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.

This site uses cookies to provide you with a better browsing experience. To learn more about the different cookies we're using, please see our privacy policy.

4. Investigating NTLM logs in Event Viewer

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

Open Event Viewer and go to **Application and Services Logs>Microsoft>Windows>NTLM>Operational**.

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.

In this screenshot, we see that the attacker's device name was spoofed to be WINDOWS7 and that the destination device for these malicious authentications is DESKTOP2.

5. Remediation

Once we identify the victim device, we can identify how the attacker is sending these authentications. To do so, we can use the following techniques to 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!)**

This site uses cookies to provide you with a better browsing experience. To learn more about the different cookies we're using, please see our privacy policy.

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.

After connecting to this targeting machine and running Netstat, we can see multiple established connections to the victim's device by suspicious IPs over port 3389.

Once you have this information, you can take remediation actions such as blocking specific IPs from the firewall or closing certain ports.

For devices that are required to remain exposed to the internet, we recommend reducing the attack surface for malicious actors by:

+ Enabling MFA for all users
+ Disabling pre-built usernames like "**Guest**" and "**Admin**"
+ Enforcing a strong password policy

However, it is important to note that if given enough attempts, threat actors can eventually make their way into a network as they narrow down their brute force attempts.

Finally, we recommend reviewing Varonis and NTLM logs to confirm these authentication attempts have stopped and continue to be on guard for new NTLM brute force attack activity.

Special thanks to Ian McIntyre, Ian Levy, and Raphael Kelly of the Varonis Incident Response Team for their contributions to this guide.

The Varonis IR Team provides free cybersecurity analysis and remediation to Varonis customers. Contact your Varonis Sales Team for details!

What should I do now?

Below are three ways you can continue your journey to reduce data risk at your company:

1. **Schedule a demo with us** to see Varonis in action. We'll personalize the session to your org's data security needs and answer any questions.
2. **See a sample of our Data Risk Assessment** and learn the risks that could be lingering in your environment. **Varonis' DRA** is completely free and offers a clear path to automated remediation.
3. Follow us on **LinkedIn**, **YouTube**, and **X (Twitter)** for bite-sized insights on all things data security, including DSPM, threat detection, AI security, and more.

This site uses cookies to provide you with a better browsing experience. To learn more about the different cookies we're using, please see our privacy policy.

Try Varonis free.

Get a detailed data risk report based on your company's data.
Deploys in minutes.

Get started | View sample

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.

This site uses cookies to provide you with a better browsing experience. To learn more about the different cookies we're using, please see our privacy policy.

GDPR: The Right to Be Forgotten and AI

Michael Buckbee

What is a Brute Force Attack? Definition

Michael Buckbee

VARONIS

Protection Regulation (GDPR) is its “right to be forgotten”. It’s related to the right to erasure but takes in far...

cyberattack equivalent of trying every key on your key ring, and eventually finding the right one.

Platform

Overview
DSPM
AI Security
Data Discovery & Classification
Cloud DLP
Policy Automation
UEBA
MDDR
SSPM
Compliance Management
Email Security
Identity Security
Athena AI
Data Access Governance

Coverage

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

Resources

Support
Community
Blog
Webinars
Events
Varonis Threat Labs
State of Cybercrime

Company

About Varonis
Careers
Investor Relations
Public Sector
Partner Program
Newsroom
Contact Us
Brand

English

Trust Center | Privacy Policy

© 2024 Varonis

This site uses cookies to provide you with a better browsing experience. To learn more about the different cookies we're using, please see our privacy policy.