← My new blog is XINTRA.ORG/BLOG

Successful 4624 Anonymous Logons to Windows Server from External IPs?

April 30, 2020

If you see successful 4624 event logs that look a little something like this in your Event Viewer showing an ANONYMOUS LOGON, an external IP (usually from Russia, Asia, USA, Ukraine) with an authentication package of NTLM, NTLMSSP, don't be alarmed - this is not an indication of a successful logon+access of your system even though it's logged as a 4624.

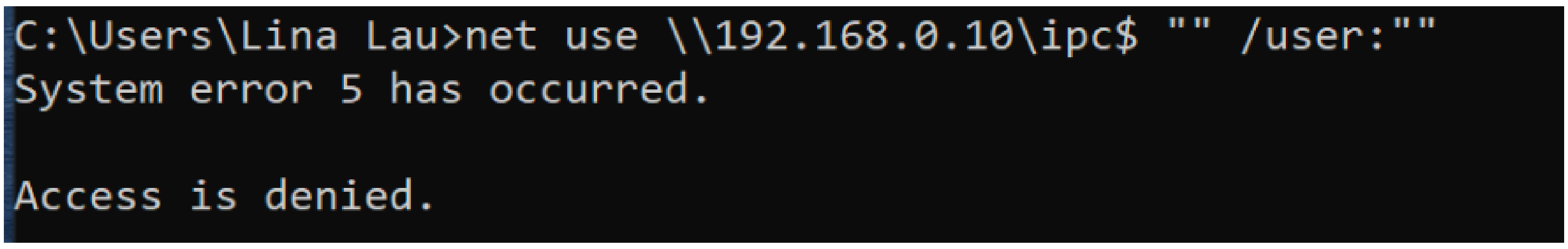
```
An account was successfully logged on.

Subject:
    Security ID:        NULL SID
    Account Name:       -
    Account Domain:     -
    Logon ID:       0x0

Logon Type:         3

New Logon:
    Security ID:        ANONYMOUS LOGON
    Account Name:       ANONYMOUS LOGON
    Account Domain:     NT AUTHORITY
    Logon ID:       0x7863af9a
    Logon GUID:     {00000000-0000-0000-0000-000000000000}

Process Information:
    Process ID:     0x0
    Process Name:       -

Network Information:
    Workstation Name:   ZZC-01309261645
    Source Network Address: 111.xxx.xxx.134
    Source Port:        55xxx

Detailed Authentication Information:
    Logon Process:      NtLmSsp
    Authentication Package: NTLM
    Transited Services: -
    Package Name (NTLM only):   NTLM V1
    Key Length:     128
```

If your server has RDP or SMB open publicly to the internet you may see a suite of these logs on your server's event viewer. Although these are showing up as Event ID 4624 (which generally correlates to successful logon events), these are NOT successful access to the system without a correlating Event ID 4624 showing up with an Account Name \\domain\username and a type 10 logon code for RDP or a type 3 for SMB. You can double check this by looking at 4625 events for a failure, within a similar time range to the logon event for confirmation.

The reason for this is because when a user initiates an RDP or SMB connection, the connection via RDP/SMB will be logged as a successful connection, BEFORE the user is prompted to enter their password. This means a successful 4624 will be logged for type 3 as an anonymous logon. When the user enters their credentials, this will either fail (if incorrect with 4625) or succeed showing up as another 4624 with the appropriate logon type and a username.

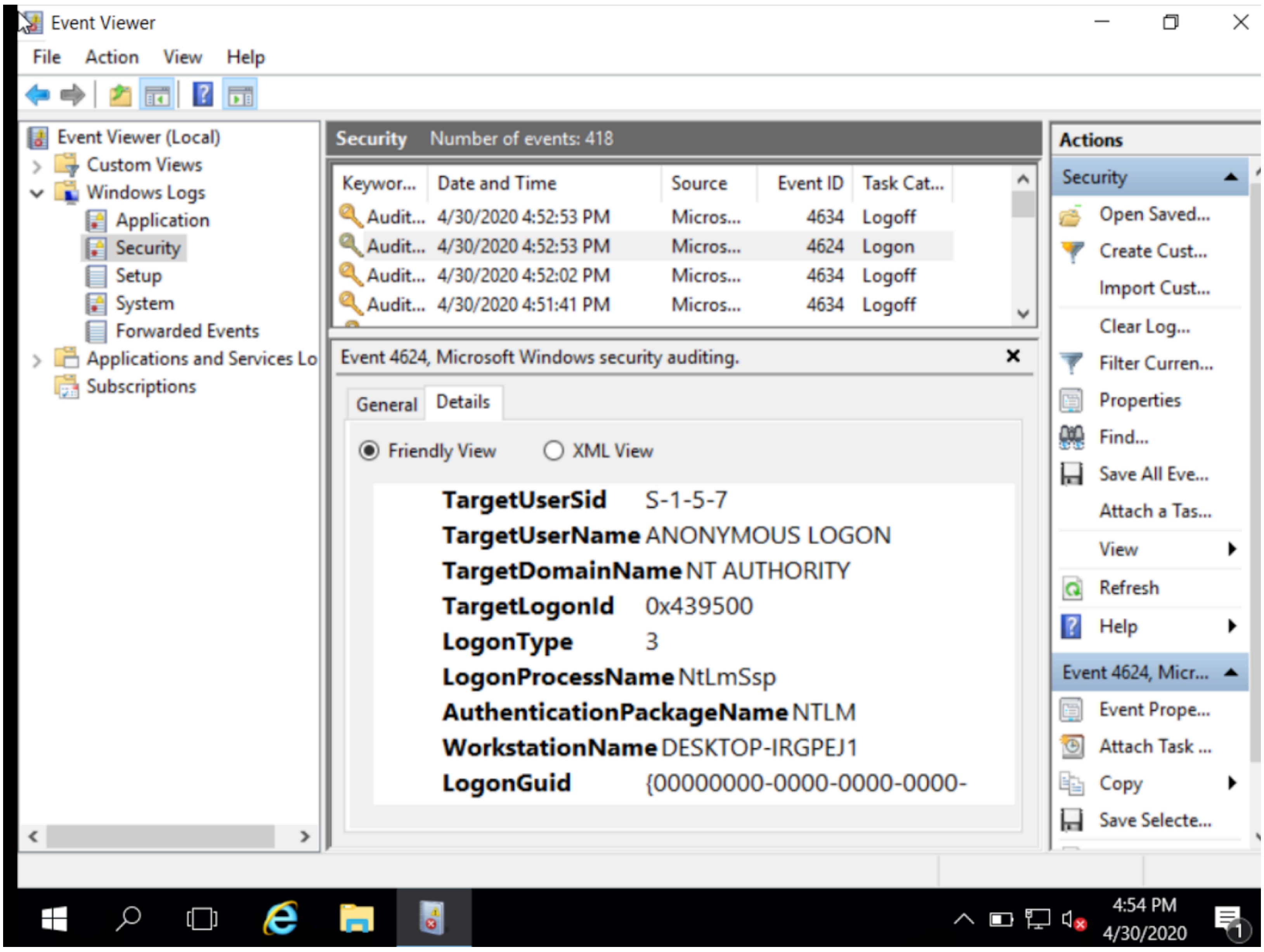
EXAMPLE: 4624 Type 3 - ANONYMOUS LOGON - SMB

To simulate this, I set up two virtual machines - one Windows 10, and one Windows Server 2016.



```
C:\Users\Lina Lau>net use \\192.168.0.10\ipc$ "" /user:""
System error 5 has occurred.

Access is denied.
```

You can see this has been denied. I log into the Server 2016 to check out the event logs and can see it's appearing as a 4624 SUCCESSFUL logon type 3.

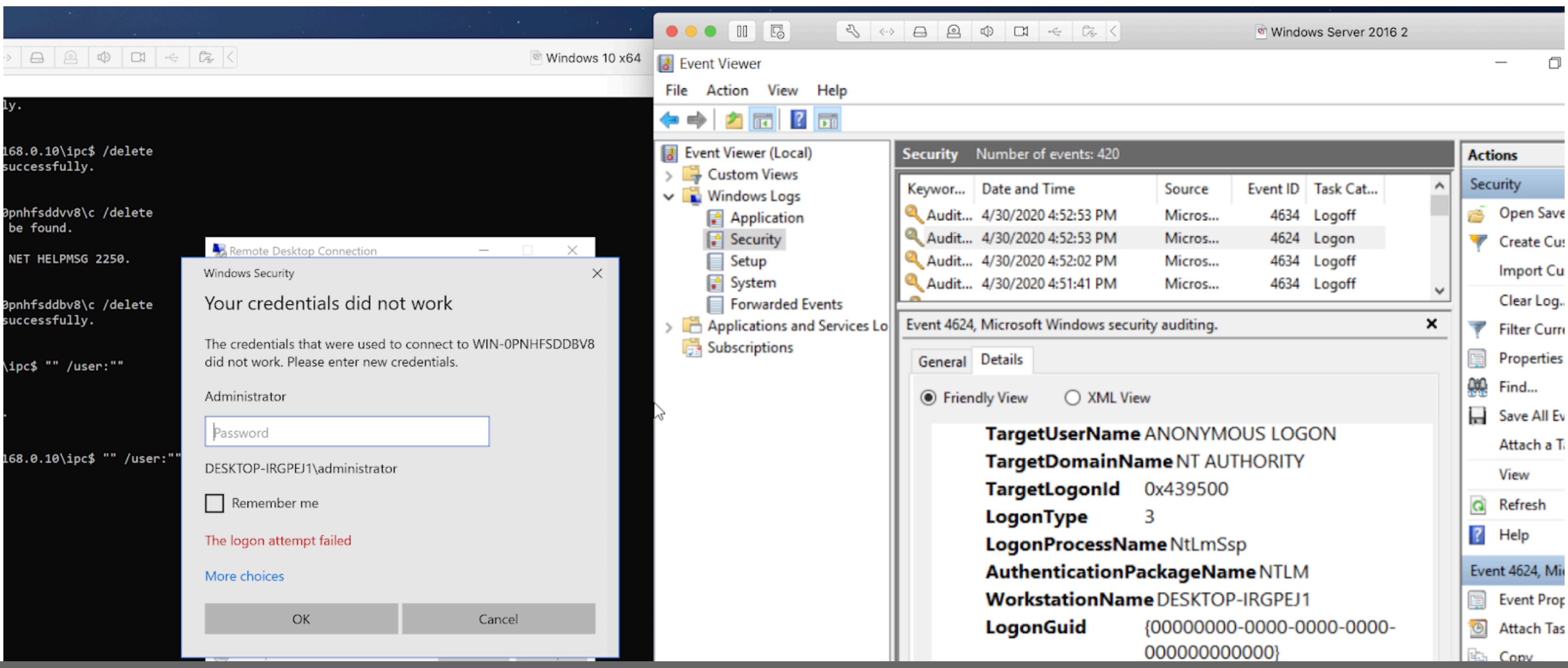


```
Security   Number of events: 418

Keywor...  Date and Time          Source     Event ID  Task Cat...
Audit...   4/30/2020 4:52:53 PM   Micros...  4634      Logoff
Audit...   4/30/2020 4:52:53 PM   Micros...  4624      Logon
Audit...   4/30/2020 4:52:02 PM   Micros...  4634      Logoff
Audit...   4/30/2020 4:51:41 PM   Micros...  4634      Logoff

Event 4624, Microsoft Windows security auditing.
General  Details
● Friendly View   ○ XML View

TargetUserSid              S-1-5-7
TargetUserName             ANONYMOUS LOGON
TargetDomainName           NT AUTHORITY
TargetLogonId              0x439500
LogonType                  3
LogonProcessName           NtLmSsp
AuthenticationPackageName  NTLM
WorkstationName            DESKTOP-IRGPEJ1
LogonGuid                  {00000000-0000-0000-0000-
```

EXAMPLE: 4624 Type 3 - ANONYMOUS LOGON - RDP

To simulate this, I set up two virtual machines - one Windows 10, and one Windows Server 2016.

I attempted to connect to RDP via the desktop client to the server and you can see this failed, but a 4624 event has also been logged under type 3 ANONYMOUS LOGON. This is because even though it's over RDP, I was logging on over 'the internet' aka the network.



```
ly.

168.0.10\ipc$ /delete
successfully.

0pnhfsddvv8\c /delete
 be found.

 NET HELPMSG 2250.

0pnhfsddbv8\c /delete
successfully.

\ipc$ "" /user:""

.

168.0.10\ipc$ "" /user:""
```

Remote Desktop Connection

Windows Security

Your credentials did not work

The credentials that were used to connect to WIN-0PNHFSDDBV8 did not work. Please enter new credentials.

Administrator

Password

DESKTOP-IRGPEJ1\administrator

□ Remember me

The logon attempt failed

More choices

OK Cancel

```
Security   Number of events: 420

Keywor...  Date and Time          Source     Event ID  Task Cat...
Audit...   4/30/2020 4:52:53 PM   Micros...  4634      Logoff
Audit...   4/30/2020 4:52:53 PM   Micros...  4624      Logon
Audit...   4/30/2020 4:52:02 PM   Micros...  4634      Logoff
Audit...   4/30/2020 4:51:41 PM   Micros...  4634      Logoff

Event 4624, Microsoft Windows security auditing.
General  Details
● Friendly View   ○ XML View

TargetUserName             ANONYMOUS LOGON
TargetDomainName           NT AUTHORITY
TargetLogonId              0x439500
LogonType                  3
LogonProcessName           NtLmSsp
AuthenticationPackageName  NTLM
WorkstationName            DESKTOP-IRGPEJ1
LogonGuid                  {00000000-0000-0000-0000-
                           000000000000}
```

4624 anonymous logon anonymous logon from asia anonymous logon type 3 external ip connecting to server

Unknown *5 May 2021 at 02:20*

Hello, Thanks for great article.
I have a question I am not sure if it is related to the article.
I can see NTLM v1 used in this scenario. Do you think if we disable the NTLM v1 will somehow avoid such attacks?

Yiğit *9 November 2021 at 04:02*

This is not about the NTLM types or disabling, my friend.
This is about the open services which cause the vulnerability.

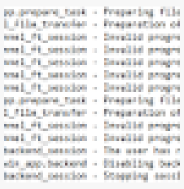
REPLY

Enter comment

Popular posts from this blog

Forensic Analysis of AnyDesk Logs

February 10, 2021

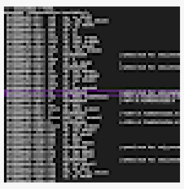


Most threat actors during ransomware incidents utilise some type of remote access tools - one of them being AnyDesk. This is a free remote access tool that threat actors download onto hosts to access them easily and also for bidirectional file transfer. There are two locations for where AnyDesk logs are stored on the Windows …

READ MORE

How to Reverse Engineer and Patch an iOS Application for Beginners: Part I

June 06, 2022



So you want to reverse and patch an iOS application? I got you >_< If you've missed the blogs in the series, check them out below ^_^ Part 1: How to Reverse Engineer and Patch an iOS Application for Beginners Part 2: Guide to Reversing and Exploiting iOS binaries: ARM64 ROP Chains Part 3: Heap Overflows on iOS ARM64: Heap …

READ MORE

Powered by Blogger

Report Abuse