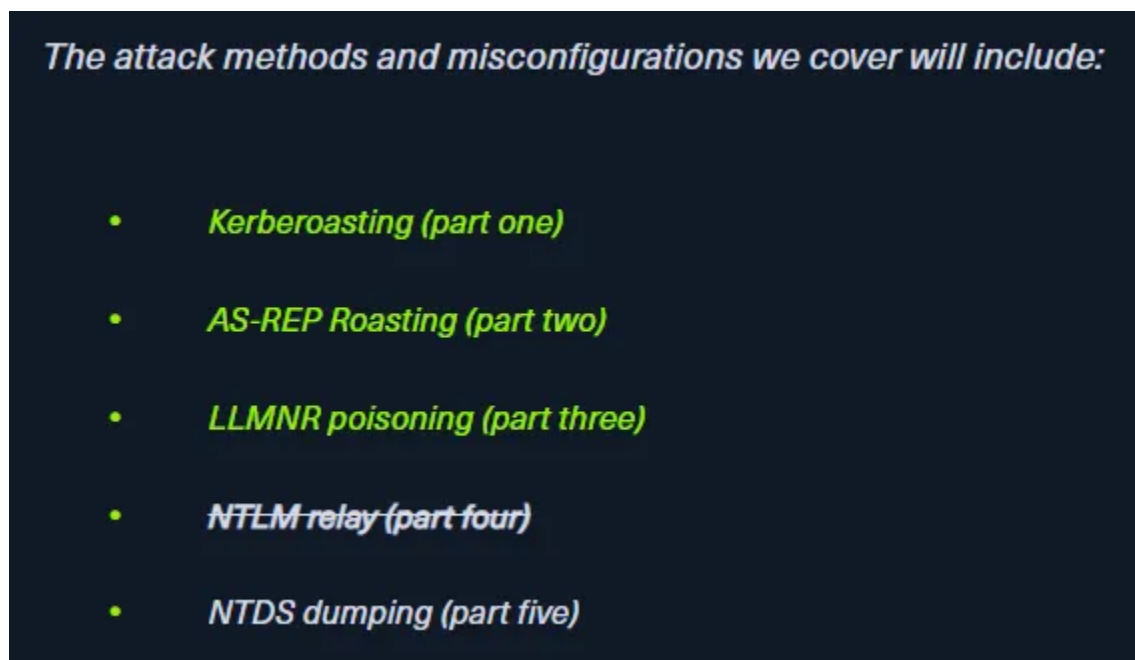


Scenario: Our SIEM alerted us to a suspicious logon event which needs to be looked at immediately . The alert details were that the IP Address and the Source Workstation name were a mismatch .You are provided a network capture and event logs from the surrounding time around the incident timeframe. Corelate the given evidence and report back to your SOC Manager.

This sherlock was launched with a new [blog](#) to teach us about NTLM Relay attack and how to investigate it with Wireshark and logon audit log, treat it like a walkthrough then you can solve this sherlock easily



*This sherlock is also the 4th AD investigation sherlock after Campfire-1 and 2 and Noxious so the last part of this series, NTDS dumping will be coming soon in the future ([CrownJewel-1](#) and [CrownJewel-2](#))

Task 1: What is the IP Address for Forela-Wkstn001?

We can also see other IP address jumped in on NBNS protocol to query status of a NetBIOS name or machine, including a list of all NetBIOS names from 172.17.79.1 and as the blog says that the IP address that sent this request could be an unknown device / threat actor device so we can use this IP address to filter for SMB traffic and see if the threat actor has accessed to any file share.

No.	Time	Source	Src P	Destination	Dst P	Protocol	Length	Info	Left
584	2024-07-31 04:53:40.0545768...	172.17.79.135	51476	172.17.79.1	445	SMB2	250	Negotiate Protocol Request	
587	2024-07-31 04:53:40.0554651...	172.17.79.1	445	172.17.79.135	51476	SMB2	306	Negotiate Protocol Response	
595	2024-07-31 04:53:40.0566275...	172.17.79.135	43532	172.17.79.129	445	SMB2	238	Negotiate Protocol Request	
598	2024-07-31 04:53:40.0571334...	172.17.79.129	445	172.17.79.135	43532	SMB2	366	Negotiate Protocol Response	
606	2024-07-31 04:53:40.0582350...	172.17.79.135	40090	172.17.79.4	445	SMB2	250	Negotiate Protocol Request	
607	2024-07-31 04:53:40.0592186...	172.17.79.4	445	172.17.79.135	40090	SMB2	378	Negotiate Protocol Response	
1185	2024-07-31 04:55:13.5542414...	172.17.79.135	445	172.17.79.136	50145	SMB2	228	Negotiate Protocol Response	
1195	2024-07-31 04:55:13.5569347...	172.17.79.136	50145	172.17.79.135	445	SMB2	220	Session Setup Request, NTLMSSP_NEGOTIATE	
1196	2024-07-31 04:55:13.5580399...	172.17.79.135	445	172.17.79.136	50145	SMB2	347	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED	
1197	2024-07-31 04:55:13.5585530...	172.17.79.136	50145	172.17.79.135	445	SMB2	635	Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle	
1198	2024-07-31 04:55:13.5595388...	172.17.79.135	445	172.17.79.136	50145	SMB2	139	Session Setup Response	

After filtered with smb2 && ip.addr == 172.17.79.135 , we can see that this unknown device successfully authenticated as arthur.kyle and tried to access other file shares.

Information 7/31/2024 4:54:49 AM Microsoft Windows security auditing 4702 Other Object Access Events

Information 7/31/2024 4:55:16 AM Microsoft Windows security auditing 4624 Logon

Information 7/31/2024 4:55:16 AM Microsoft Windows security auditing 5140 File Share

Information 7/31/2024 4:55:39 AM Microsoft Windows security auditing 4624 Logon

Information 7/31/2024 4:55:39 AM Microsoft Windows security auditing 4624 Logon

Information 7/31/2024 4:55:39 AM Microsoft Windows security auditing 4702 Other Object Access Events

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

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

Logon Information:

- Logon Type: 3
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: No

Impersonation Level: Impersonation

New Logon:

- Security ID: S-1-5-21-3239415629-1862073780-2394361899-1601
- Account Name: arthur.kyle

Security_1 Number of events: 51				
Level	Date and Time	Source	Event ID	Task Category
Information	7/31/2024 4:54:48 AM	Microsoft Windows security audi...	4624	Logon
Information	7/31/2024 4:54:49 AM	Microsoft Windows security audi...	4624	Logon
Information	7/31/2024 4:54:49 AM	Microsoft Windows security audi...	4702	Other Object Access Events
Information	7/31/2024 4:55:16 AM	Microsoft Windows security audi...	4624	Logon
Information	7/31/2024 4:55:16 AM	Microsoft Windows security audi...	5140	File Share
Information	7/31/2024 4:55:39 AM	Microsoft Windows security audi...	4624	Logon
Information	7/31/2024 4:55:39 AM	Microsoft Windows security audi...	4624	Logon
Information	7/31/2024 4:55:39 AM	Microsoft Windows security audi...	4702	Other Object Access Events

Event 4624, Microsoft Windows security auditing.	
General	Details
<div> <div> Account Name: arthur.kyle Account Domain: FORELA Logon ID: 0x64A799 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} </div> <div> Process Information: Process ID: 0x0 Process Name: - </div> <div> Network Information: Workstation Name: FORELA-WKSTN002 Source Network Address: 172.17.79.135 Source Port: 40252 </div> <div> Detailed Authentication Information: Logon Process: NtLmSsp </div> </div>	
Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4624
Level:	Information
User:	N/A
OpCode:	Info
More Information:	Event Log Online Help

Its time to open audit log to see that there is one login event that look very suspicious since there is no Logon ID (NULL SID) and it was authenticated via NTLM and the source IP address is the suspicious device we are after.

arthur kyle

Task 4: What is the IP Address of Unknown Device used by the attacker to intercept credentials?

172.17.79.135

Task 5: What was the fileshare navigated by the victim user account?

ntlmrelay.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smb2

Packet list Narrow & Wide Case sensitive String Bad

No.	Time	Source	Src P	Destination	Dst P	Protocol	Length	Info	Left
1412	2024-07-31 04:55:28.1387490...	172.17.79.4	445	172.17.79.136	50152	SMB2	138	Tree Connect Response	
1413	2024-07-31 04:55:28.1389204...	172.17.79.136	50152	172.17.79.4	445	SMB2	178	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO	
1414	2024-07-31 04:55:28.1390159...	172.17.79.136	50152	172.17.79.4	445	SMB2	202	Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \DC01\Trip	
1415	2024-07-31 04:55:28.1390160...	172.17.79.4	445	172.17.79.136	50152	SMB2	474	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO	
1416	2024-07-31 04:55:28.1474338...	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Ioctl Response, Error: STATUS_NOT_FOUND	
1418	2024-07-31 04:55:28.1477711...	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip	
1419	2024-07-31 04:55:28.1480176...	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME	
1420	2024-07-31 04:55:28.1481850...	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip	
1421	2024-07-31 04:55:28.1482938...	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME	
1422	2024-07-31 04:55:28.1484778...	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip	
1423	2024-07-31 04:55:28.1485869...	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME	
1424	2024-07-31 04:55:28.1487687...	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip	
1425	2024-07-31 04:55:28.1488544...	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME	
1426	2024-07-31 04:55:28.1492142...	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip	
1427	2024-07-31 04:55:28.1492902...	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME	
1428	2024-07-31 04:55:28.1494701...	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip	
1429	2024-07-31 04:55:28.1495480...	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME	
1430	2024-07-31 04:55:28.1497476...	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip	
1431	2024-07-31 04:55:28.1498559...	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME	
1432	2024-07-31 04:55:28.1500447...	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip	

> Frame 1419: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface eth0, id 0

0000 00 0c 29 f7 7d 94 00 0c 29 56 44 f9 08 00 45 00

For this one, we have to find for Tree Connect that response with Error like this which mean file share could not be found or was not recognized by the server. This could happen if the share doesn't exist, is offline, or the client doesn't have access rights.

\\DC01\Trip

Task 6: What is the source port used to logon to target workstation using the compromised account?

Security_1 Number of events: 51				
Level	Date and Time	Source	Event ID	Task Category
Information	7/31/2024 4:54:48 AM	Microsoft Windows security audi...	4624	Logon
Information	7/31/2024 4:54:49 AM	Microsoft Windows security audi...	4624	Logon
Information	7/31/2024 4:54:49 AM	Microsoft Windows security audi...	4702	Other Object Access Events
Information	7/31/2024 4:55:16 AM	Microsoft Windows security audi...	4624	Logon
Information	7/31/2024 4:55:16 AM	Microsoft Windows security audi...	5140	File Share
Information	7/31/2024 4:55:39 AM	Microsoft Windows security audi...	4624	Logon
Information	7/31/2024 4:55:39 AM	Microsoft Windows security audi...	4624	Logon
Information	7/31/2024 4:55:39 AM	Microsoft Windows security audi...	4702	Other Object Access Events

Event 4624, Microsoft Windows security auditing.	
General Details	
Account Name:	arthur.kyle
Account Domain:	FORELA
Logon ID:	0x64A799
Linked Logon ID:	0x0
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	{00000000-0000-0000-0000-000000000000}
Process Information:	
Process ID:	0x0
Process Name:	-
Network Information:	
Workstation Name:	FORELA-WKSTN002
Source Network Address:	172.17.79.135
Source Port:	40252
Detailed Authentication Information:	
Logon Process:	NtLmSsp
Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4624
Level:	Information
User:	N/A
OpCode:	Info
More Information:	Event Log Online Help
Logged:	7/31/2024 4:55:16 AM
Task Category:	Logon
Keywords:	Audit Success
Computer:	Forela-Wkstn001.forela.local

40252

Task 7: What is the Logon ID for the malicious session?

0x64A799

Task 8: The detection was based on the mismatch of hostname and the assigned IP Address. What is the workstation name and the source IP Address from which the malicious logon occur?

FORELA-WKSTN002, 172.17.79.135

Task 9: When did the malicious logon happened. Please make sure the timestamp is in UTC?

2024-07-31 04:55:16

Task 10: What is the share Name accessed as part of the authentication process by the malicious tool used by the attacker?

The screenshot shows the Windows Security Event Viewer. The top pane displays a list of events. The bottom pane shows the details for Event 5140, 'Microsoft Windows security auditing'.

Level	Date and Time	Source	Event ID	Task Category
Information	7/31/2024 4:54:48 AM	Microsoft Windows security auditing	4624	Logon
Information	7/31/2024 4:54:49 AM	Microsoft Windows security auditing	4624	Logon
Information	7/31/2024 4:54:49 AM	Microsoft Windows security auditing	4702	Other Object Access Events
Information	7/31/2024 4:55:16 AM	Microsoft Windows security auditing	4624	Logon
Information	7/31/2024 4:55:16 AM	Microsoft Windows security auditing	5140	File Share
Information	7/31/2024 4:55:39 AM	Microsoft Windows security auditing	4624	Logon
Information	7/31/2024 4:55:39 AM	Microsoft Windows security auditing	4624	Logon
Information	7/31/2024 4:55:39 AM	Microsoft Windows security auditing	4702	Other Object Access Events

Event 5140, Microsoft Windows security auditing.	
General	Details
A network share object was accessed.	
Subject:	
Security ID:	S-1-5-21-3239415629-1862073780-2394361899-1601
Account Name:	arthur.kyle
Account Domain:	FORELA
Logon ID:	0x64A799
Network Information:	
Object Type:	File
Source Address:	172.17.79.135
Source Port:	40252
Share Information:	
Share Name:	*\VPCS
Share Path:	
Access Request Information:	
Access Mask:	0x1

For this, we have to inspect EventID 5140 (network share accessed) that happened after the threat actor authenticated as arthur

*\IPC\$