PsExec Hunt Lab
Reveal Lab
Analyst: Ruslan
Date: 2026-01-25

Executive Summary

Network evidence indicates lateral movement consistent with PsExec tradecraft: SMB2 over TCP/445 from 10.0.0.130 to 10.0.0.133, NTLM authentication using the account ssales, remote service binary drop PSEXESVC.exe via ADMIN$, and inter-process communication via IPC$. A subsequent pivot attempt toward 10.0.0.131 (MARKETING-PC) failed with STATUS_LOGON_FAILURE.

Scope and Data Basis

This report is based on analyzed SMB/SMB2 and NTLM session activity captured in the investigation material, showing negotiated SMB sessions and share access patterns associated with remote execution.

Confirmed Observations

Category	Observation	Evidence
Initial source	10.0.0.130 initiated SMB negotiation to 10.0.0.133	
Protocol/port	SMB2 over TCP/445 in the observed flows	
First lateral target	Target hostname identified as SALES-PC	
Authentication	Username used for authentication: ssales	
Remote execution artifact	Service executable created/copied: PSEXESVC.exe	
Installation share	ADMIN$ used to install/copy PsExec service executable	
Communication share	IPC$ used for communication between machines	
Second lateral attempt	10.0.0.130 attempted SMB to 10.0.0.131; hostname MARKETING-PC; logon failure	

Activity Narrative (Condensed)

Phase	What happened	Key artifacts
Establish foothold-to-target session	SMB2 session initiated from 10.0.0.130 to 10.0.0.133 over TCP/445	
Identify and access first pivot host	NTLM metadata reveals hostname SALES-PC	
Authenticate using valid credentials	Account ssales used in SMB2 Session Setup/NTLM	
Deploy PsExec service component	PSEXESVC.exe created/copied via ADMIN$ (administrative share mapped to Windows directory)	
Maintain remote control channel	IPC$ used as the communication channel	
Attempt further lateral movement	10.0.0.130 → 10.0.0.131 (MARKETING-PC) failed with STATUS_LOGON_FAILURE	

Impact Assessment

Confirmed remote execution capability on the first lateral target is strongly implied by the creation/copy of PSEXESVC.exe through ADMIN$, a standard PsExec mechanism for remote command execution.
Credential abuse risk is present due to the authenticated use of ssales for SMB/NTLM activity across hosts.
Additional spread was attempted but not achieved on the second target due to STATUS_LOGON_FAILURE, indicating missing/invalid credentials or insufficient access to that host at the time of the attempt.

Indicators for Detection and Hunting

Type	Value
Source IP	10.0.0.130
Target IPs	10.0.0.133; 10.0.0.131
Hostnames	SALES-PC; MARKETING-PC
Account	ssales
File/service artifact	PSEXESVC.exe
Shares	ADMIN$; IPC$
Failure signal	STATUS_LOGON_FAILURE
Protocol/port	SMB2 / TCP 445

Recommended Actions

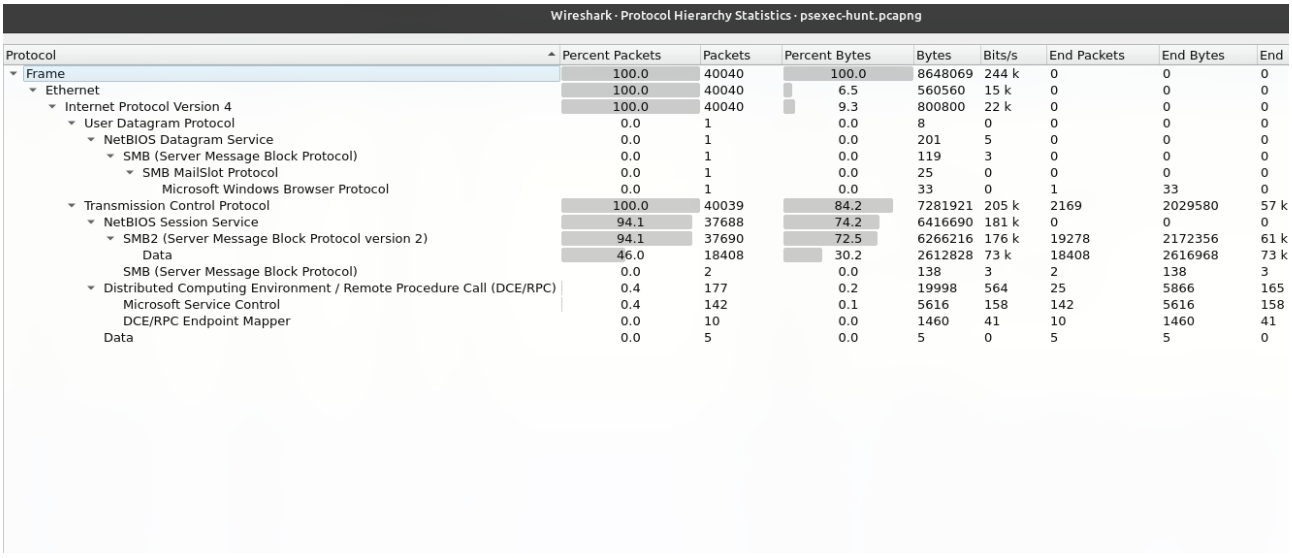
Priority	Action	Rationale
High	Isolate 10.0.0.130 and SALES-PC from lateral paths (SMB/RPC) pending triage	Confirmed SMB pivot behavior and PsExec service artifact deployment
High	Reset and review **ssales** (password, active sessions, group memberships, recent logons)	Account used to authenticate for lateral activity
High	On SALES-PC, search for and preserve evidence of PsExec service activity (PSEXESVC.exe, service creation, execution traces)	Direct indicator of remote execution setup
Medium	Hunt for ADMIN$/IPC$ access spikes and PSEXESVC.exe writes from non-admin endpoints	ADMIN$ used for service deployment; IPC$ used for communication
Medium	Validate why MARKETING-PC rejected authentication (policy, credential scope, local admin rights)	Failed pivot attempt confirms intent to expand
Medium	Restrict/segment SMB administrative shares exposure; enforce least privilege for remote admin	Reduces feasibility of PsExec-style lateral movement
Medium	Reduce NTLM usage where feasible; strengthen credential protections	Observed NTLM in session setup for lateral movement

Conclusion

The observed SMB2/NTLM activity matches a PsExec lateral movement pattern: authenticated access using ssales, deployment of PSEXESVC.exe via ADMIN$, and control channel use of IPC$, followed by an unsuccessful second pivot to MARKETING-PC (10.0.0.131) due to STATUS_LOGON_FAILURE.

1. To effectively trace the attacker's activities within our network, can you identify the IP address of the machine from which the attacker initially gained access?

Statistics → Protocol Hierarchy



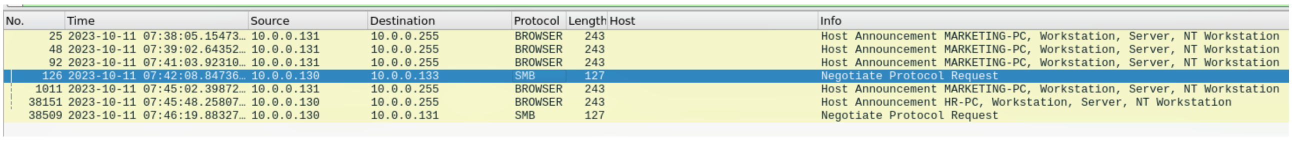
Wireshark · Protocol Hierarchy Statistics · psexec-hunt.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End
Frame	100.0	40040	100.0	8648069	244 k	0	0	0
Ethernet	100.0	40040	6.5	560560	15 k	0	0	0
Internet Protocol Version 4	100.0	40040	9.3	800800	22 k	0	0	0
User Datagram Protocol	0.0	1	0.0	8	0	0	0	0
NetBIOS Datagram Service	0.0	1	0.0	201	5	0	0	0
SMB (Server Message Block Protocol)	0.0	1	0.0	119	3	0	0	0
SMB MailSlot Protocol	0.0	1	0.0	25	0	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.0	33	0	1	33	0
Transmission Control Protocol	100.0	40039	84.2	7281921	205 k	2169	2029580	57 k
NetBIOS Session Service	94.1	37688	74.2	6416690	181 k	0	0	0
SMB2 (Server Message Block Protocol version 2)	94.1	37690	72.5	6266216	176 k	19278	2172356	61 k
Data	46.0	18408	30.2	2612828	73 k	18408	2616968	73 k
SMB (Server Message Block Protocol)	0.0	2	0.0	138	3	2	138	3
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.4	177	0.2	19998	564	25	5866	165
Microsoft Service Control	0.4	142	0.1	5616	158	142	5616	158
DCE/RPC Endpoint Mapper	0.0	10	0.0	1460	41	10	1460	41
Data	0.0	5	0.0	5	0	5	5	0

The screenshot above show a clear presence of the SMB (Server Message Block) protocol, which is often associated with file-sharing and network resource access on Windows networks. SMB operates over both UDP and TCP, though TCP is the more common transport protocol due to its reliability and connection-oriented nature, while UDP is typically used in less demanding, connectionless scenarios.

The protocol hierarchy details reveal the use of NetBIOS Session Service and SMB2 (Server Message Block Protocol version 2) over TCP. This indicates a deliberate communication flow likely initiated for lateral movement or file transfer.

By investigating the specific traffic patterns associated with SMB, it becomes evident that an SMB negotiation occurred between two IP addresses, 10.0.0.130 and 10.0.0.133.



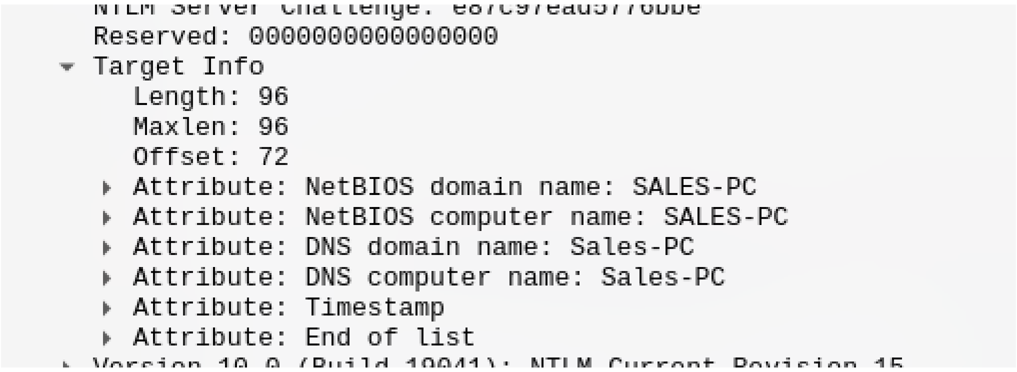
No.	Time	Source	Destination	Protocol	Length	Host	Info
25	2023-10-11 07:38:05.15473…	10.0.0.131	10.0.0.255	BROWSER	243		Host Announcement MARKETING-PC, Workstation, Server, NT Workstation
48	2023-10-11 07:39:02.64352…	10.0.0.131	10.0.0.255	BROWSER	243		Host Announcement MARKETING-PC, Workstation, Server, NT Workstation
92	2023-10-11 07:41:03.92310…	10.0.0.131	10.0.0.255	BROWSER	243		Host Announcement MARKETING-PC, Workstation, Server, NT Workstation
126	2023-10-11 07:42:08.84736…	10.0.0.130	10.0.0.133	SMB	127		Negotiate Protocol Request
1011	2023-10-11 07:45:02.39872…	10.0.0.131	10.0.0.255	BROWSER	243		Host Announcement MARKETING-PC, Workstation, Server, NT Workstation
38151	2023-10-11 07:45:48.25807…	10.0.0.130	10.0.0.255	BROWSER	243		Host Announcement HR-PC, Workstation, Server, NT Workstation
38509	2023-10-11 07:46:19.88327…	10.0.0.130	10.0.0.131	SMB	127		Negotiate Protocol Request

During this process, the client, originating from 10.0.0.130, sent a Negotiate Protocol Request to 10.0.0.133. This request is a fundamental step in establishing communication between a client and a server, where the SMB protocol version is agreed upon to ensure compatibility for further operations. The use of TCP port 445 confirms this as standard SMB communication.

Answer: 10.0.0.130

2. To fully understand the extent of the breach, can you determine the machine's hostname to which the attacker first pivoted?

Follow → TCP Stream



```
    NTLM Server Challenge: e87c97ead577bbbe
    Reserved: 0000000000000000
  ▾ Target Info
      Length: 96
      Maxlen: 96
      Offset: 72
    ▸ Attribute: NetBIOS domain name: SALES-PC
    ▸ Attribute: NetBIOS computer name: SALES-PC
    ▸ Attribute: DNS domain name: Sales-PC
    ▸ Attribute: DNS computer name: Sales-PC
    ▸ Attribute: Timestamp
    ▸ Attribute: End of list
  ▸ Version 10.0 (Build 19041): NTLM Current Revision 15
```

The SMB traffic reveals the use of NTLM (NT LAN Manager) authentication as part of the session setup process. NTLM is a challenge-response authentication protocol commonly used in Windows environments. It involves the exchange of negotiation messages, challenges, and responses between the client and the server. This protocol is often exploited by attackers during lateral movement attempts.

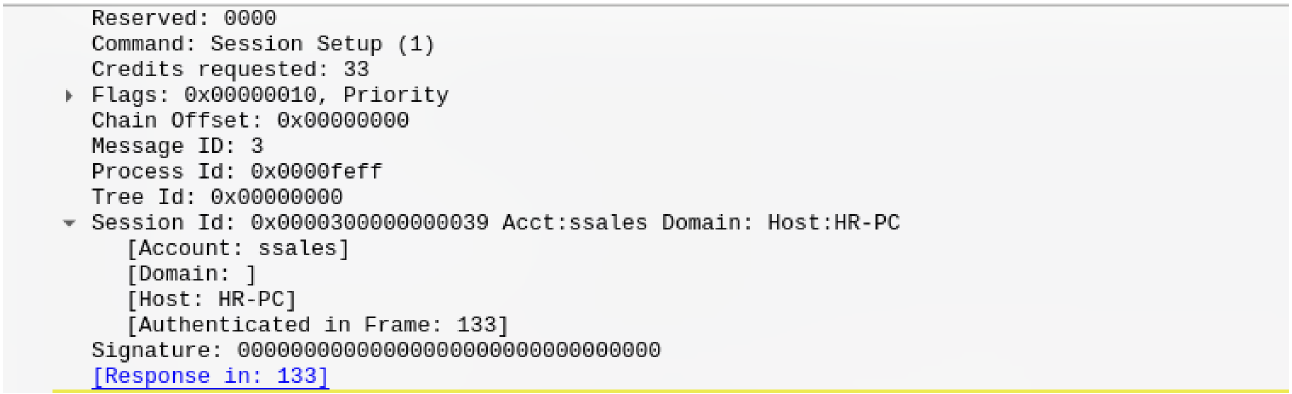
In the detailed breakdown of the NTLM authentication exchange, we can see that the server responds to the client with a message containing metadata about the target machine. This includes key attributes such as the NetBIOS domain name, NetBIOS computer name, and DNS domain/computer name. From the extracted information, the target machine's hostname is identified as SALES-PC. This data is crucial as it confirms the pivot point in the attack, where the attacker transitioned from their initial foothold to a new target machine within the network.

The attributes also confirm that the attacker's activity leveraged SMB2 over TCP port 445 to establish a connection to SALES-PC. This interaction is a hallmark of lateral movement tactics, where the attacker attempts to expand their reach and establish control over additional resources in the compromised environment. Identifying the compromised hostname provides valuable insight into the attack's progression and sets the stage for further investigation into the compromise's depth and scope.

Answer: SALES-PC

3. Knowing the username of the account the attacker used for authentication will give us insights into the extent of the breach. What is the username utilized by the attacker for authentication?

To identify the username utilized by the attacker for authentication, we trace back to the session initiation within the SMB traffic observed in the TCP stream. The SMB2 Session Setup Request packet reveals the critical details related to the authentication process. This step in the SMB communication sequence is where the client attempts to establish a session with the server using provided credentials.



```
    Reserved: 0000
    Command: Session Setup (1)
    Credits requested: 33
  ▸ Flags: 0x00000010, Priority
    Chain Offset: 0x00000000
    Message ID: 3
    Process Id: 0x0000feff
    Tree Id: 0x00000000
  ▾ Session Id: 0x0000300000000039 Acct:ssales Domain: Host:HR-PC
       [Account: ssales]
       [Domain: ]
       [Host: HR-PC]
       [Authenticated in Frame: 133]
    Signature: 00000000000000000000000000000000
    [Response in: 133]
```

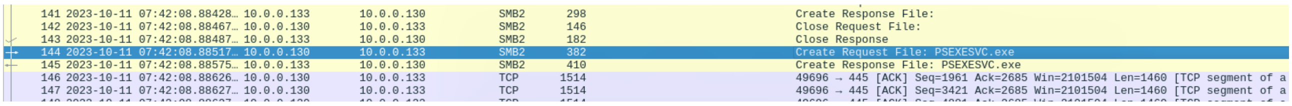
Upon inspecting the session setup request, the NTLM authentication information is displayed. This includes the session identifier and the account name used during the authentication. The captured information indicates that the username ssales was employed for authentication. This username belongs to the host HR-PC, as observed in the metadata within the packet. The NTLM authentication process leverages challenge-response mechanisms, where the client provides a response token based on a server-generated challenge.

The use of the ssales account suggests the attacker either compromised this user account or leveraged stolen credentials to authenticate and gain access to the target system. This is a critical indicator of compromise IoC as it reveals the identity being exploited in the breach. The account name provides valuable context for incident response teams to assess the permissions and roles associated with this user, helping them determine the extent of the attacker's capabilities and privileges within the compromised environment.

Anwer: ssales

4. After figuring out how the attacker moved within our network, we need to know what they did on the target machine. What's the name of the service executable the attacker set up on the target?

To uncover what the attacker did on the target machine, we analyze the SMB requests further down in the TCP stream. The communication reveals that the attacker issued a Create Request via SMB to set up a service executable on the target machine. This step is a critical indicator of their activity and provides insight into the tools they used to maintain persistence or execute commands.



```
141 2023-10-11 07:42:08.88428… 10.0.0.133      10.0.0.130      SMB2    298        Create Response File:
142 2023-10-11 07:42:08.88467… 10.0.0.130      10.0.0.133      SMB2    146        Close Request File:
143 2023-10-11 07:42:08.88487… 10.0.0.133      10.0.0.130      SMB2    182        Close Response
144 2023-10-11 07:42:08.88517… 10.0.0.130      10.0.0.133      SMB2    382        Create Request File: PSEXESVC.exe
145 2023-10-11 07:42:08.88575… 10.0.0.133      10.0.0.130      SMB2    410        Create Response File: PSEXESVC.exe
146 2023-10-11 07:42:08.88626… 10.0.0.130      10.0.0.133      TCP     1514       49696 → 445 [ACK] Seq=1961 Ack=2685 Win=2101504 Len=1460 [TCP segment of a
147 2023-10-11 07:42:08.88627… 10.0.0.130      10.0.0.133      TCP     1514       49696 → 445 [ACK] Seq=3421 Ack=2685 Win=2101504 Len=1460 [TCP segment of a
```

The captured packet details show that the attacker created a file named PSEXESVC.exe on the target machine. This executable is a service component of PsExec, a legitimate tool often misused by attackers for lateral movement. PsExec operates by copying its service executable, PSEXESVC.exe, to the target system's ADMIN$ share, which is a hidden administrative share commonly used for remote administration on Windows systems. Once transferred, the service is executed, providing the attacker with remote access and execution capabilities on the compromised host.

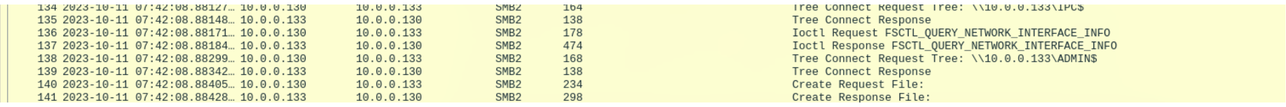
The SMB2 Create Request packet includes details such as the tree ID pointing to the target's ADMIN$ share and the account used for this operation, which, as established earlier, is ssales. The session identifier and the domain context confirm the connection was made using the credentials of the compromised account, further demonstrating how the attacker leveraged valid user privileges to conduct their malicious actions.

By creating the PSEXESVC.exe service on the target machine, the attacker gained the ability to execute commands remotely, effectively compromising the host. This action highlights the need to monitor administrative shares and user activity, particularly when tools like PsExec are detected in network traffic, as they often signal unauthorized or malicious operations.

Answer: PSEXESVC

5. We need to know how the attacker installed the service on the compromised machine to understand the attacker's lateral movement tactics. This can help identify other affected systems. Which network share was used by PsExec to install the service on the target machine?

To understand how the attacker installed the service on the compromised machine, we need to analyze the specific network share utilized during the PsExec operation. PsExec, a popular tool for remote administration, typically leverages administrative shares on target systems to copy its service executable and perform its operations. In this case, the network traffic captured in the TCP stream provides clear evidence of the share used.



```
134 2023-10-11 07:42:08.88127… 10.0.0.130      10.0.0.133      SMB2     164                    Tree Connect Request Tree: \\10.0.0.133\IPC$
135 2023-10-11 07:42:08.88148… 10.0.0.133      10.0.0.130      SMB2     138                    Tree Connect Response
136 2023-10-11 07:42:08.88171… 10.0.0.130      10.0.0.133      SMB2     178                    Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
137 2023-10-11 07:42:08.88184… 10.0.0.133      10.0.0.130      SMB2     474                    Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
138 2023-10-11 07:42:08.88299… 10.0.0.130      10.0.0.133      SMB2     168                    Tree Connect Request Tree: \\10.0.0.133\ADMIN$
139 2023-10-11 07:42:08.88342… 10.0.0.133      10.0.0.130      SMB2     138                    Tree Connect Response
140 2023-10-11 07:42:08.88405… 10.0.0.130      10.0.0.133      SMB2     234                    Create Request File:
141 2023-10-11 07:42:08.88428… 10.0.0.133      10.0.0.130      SMB2     298                    Create Response File:
```

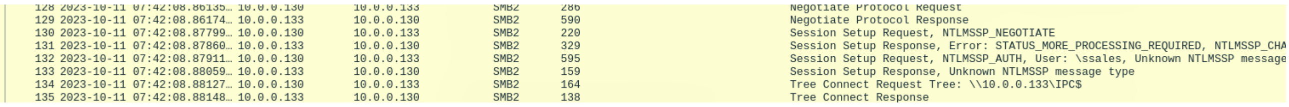
The SMB2 Create Request packet, which was used to create the service executable PSEXESVC.exe, indicates that the service was installed on the ADMIN$ share of the target machine. The ADMIN$ share is a hidden administrative share mapped to the Windows system directory, usually C:\Windows. It is used for administrative tasks such as remote file transfers and execution. The presence of the tree ID pointing to \\10.0.0.133\ADMIN$ confirms this share was targeted by PsExec.

Using the ADMIN$ share allowed the attacker to remotely copy the PsExec service executable to the target machine, initiate its execution, and gain remote access. This tactic is an indicator of lateral movement, as it relies on accessing privileged shares and leveraging valid credentials, such as the compromised ssales account, to execute commands on other systems.

Understanding the use of the ADMIN$ share in this context provides critical insights into the attacker's methods. It highlights the need for robust monitoring and auditing of administrative shares and user account activities to detect and prevent unauthorized access and lateral movement across the network.

6. We must identify the network share used to communicate between the two machines. Which network share did PsExec use for communication?

To identify the network share used for communication between the two machines, we analyze the SMB Tree Connect Requests made earlier in the captured traffic.



```
128 2023-10-11 07:42:08.86135… 10.0.0.130      10.0.0.133      SMB2     286                    Negotiate Protocol Request
129 2023-10-11 07:42:08.86174… 10.0.0.133      10.0.0.130      SMB2     590                    Negotiate Protocol Response
130 2023-10-11 07:42:08.87799… 10.0.0.130      10.0.0.133      SMB2     220                    Session Setup Request, NTLMSSP_NEGOTIATE
131 2023-10-11 07:42:08.87860… 10.0.0.133      10.0.0.130      SMB2     329                    Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHA
132 2023-10-11 07:42:08.87911… 10.0.0.130      10.0.0.133      SMB2     595                    Session Setup Request, NTLMSSP_AUTH, User: \ssales, Unknown NTLMSSP message
133 2023-10-11 07:42:08.88059… 10.0.0.133      10.0.0.130      SMB2     159                    Session Setup Response, Unknown NTLMSSP message type
134 2023-10-11 07:42:08.88127… 10.0.0.130      10.0.0.133      SMB2     164                    Tree Connect Request Tree: \\10.0.0.133\IPC$
135 2023-10-11 07:42:08.88148… 10.0.0.133      10.0.0.130      SMB2     138                    Tree Connect Response
```

The request, shown in the screenshot above, indicates that the attacker used the IPC$ share for communication. The IPC$ share, short for Inter-Process Communication, is a special administrative share on Windows systems that facilitates communication between processes, especially for remote management and control operations. Unlike typical shares for file storage, IPC$ is used to exchange data related to administrative tasks, such as managing network connections or accessing system services.

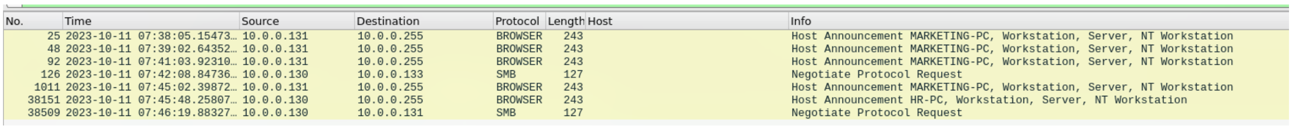
The captured Tree Connect Request shows a connection to \\10.0.0.133\IPC$, confirming that the IPC$ share was leveraged during the attack. This share is commonly used in SMB communications, particularly for operations that involve authentication, remote service management, or command execution, as seen in this scenario with PsExec. The connection attributes in the packet indicate the session was established using the previously compromised ssales account, and the communication proceeded over SMB2 on TCP port 445.

By using the IPC$ share, PsExec established a channel for remote procedure calls (RPC) and other inter-process communications necessary for its functionality.

Answer: IPC$

7. Now that we have a clearer picture of the attacker's activities on the compromised machine, it's important to identify any further lateral movement. What is the hostname of the second machine the attacker targeted to pivot within our network?

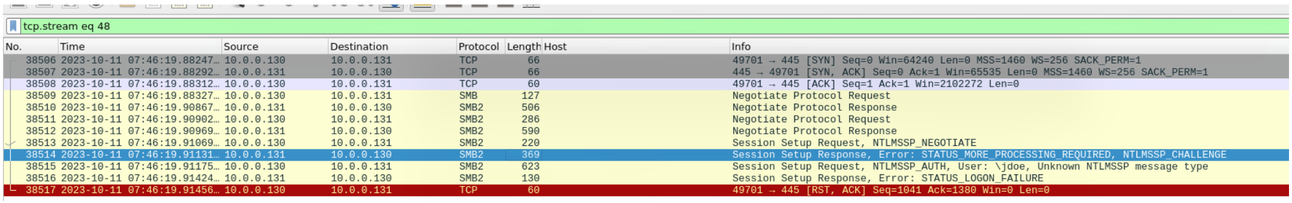
To identify the hostname of the second machine the attacker targeted for lateral movement, we examine the network traffic to locate another SMB session initiated from the attacker's initial foothold. The captured traffic reveals that the attacker attempted to communicate with a different target within the network.



No.	Time	Source	Destination	Protocol	Length	Host	Info
25	2023-10-11 07:38:05.15473…	10.0.0.131	10.0.0.255	BROWSER	243		Host Announcement MARKETING-PC, Workstation, Server, NT Workstation
48	2023-10-11 07:39:02.64352…	10.0.0.131	10.0.0.255	BROWSER	243		Host Announcement MARKETING-PC, Workstation, Server, NT Workstation
92	2023-10-11 07:41:03.92310…	10.0.0.131	10.0.0.255	BROWSER	243		Host Announcement MARKETING-PC, Workstation, Server, NT Workstation
126	2023-10-11 07:42:08.84736…	10.0.0.130	10.0.0.133	SMB	127		Negotiate Protocol Request
1011	2023-10-11 07:45:02.39872…	10.0.0.131	10.0.0.255	BROWSER	243		Host Announcement MARKETING-PC, Workstation, Server, NT Workstation
38151	2023-10-11 07:45:48.25807…	10.0.0.130	10.0.0.255	BROWSER	243		Host Announcement HR-PC, Workstation, Server, NT Workstation
38509	2023-10-11 07:46:19.88327…	10.0.0.130	10.0.0.131	SMB	127		Negotiate Protocol Request

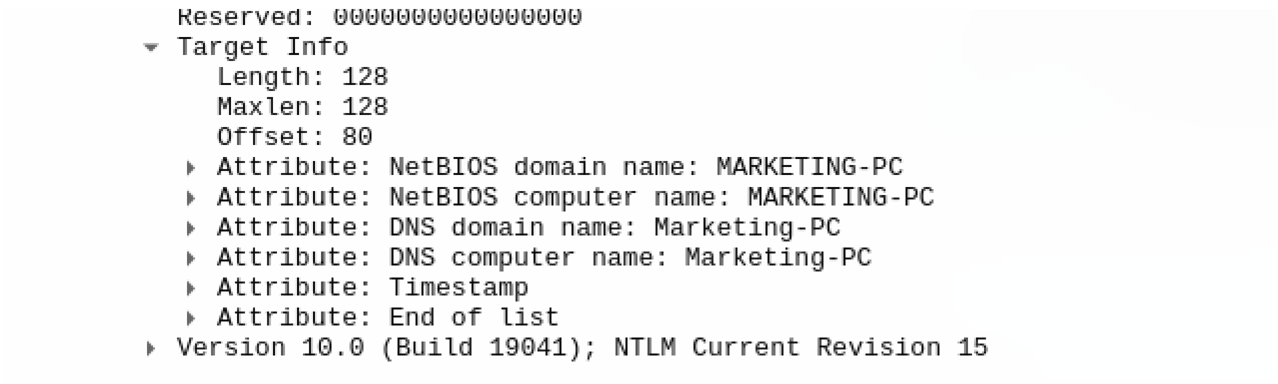
The packet analysis shows an SMB Negotiate Protocol Request from the attacker's IP, 10.0.0.130, to the destination IP, 10.0.0.131. The SMB session setup process includes NTLM negotiation details that reveal the identity of the target machine. Upon analyzing the NTLM Challenge response from the destination, the hostname is extracted from the session metadata.

Follow → TCP Stream



tcp.stream eq 48

No.	Time	Source	Destination	Protocol	Length	Host	Info
38506	2023-10-11 07:46:19.88247…	10.0.0.130	10.0.0.131	TCP	66		49701 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
38507	2023-10-11 07:46:19.88292…	10.0.0.131	10.0.0.130	TCP	66		445 → 49701 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
38508	2023-10-11 07:46:19.88312…	10.0.0.130	10.0.0.131	TCP	60		49701 → 445 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
38509	2023-10-11 07:46:19.88327…	10.0.0.130	10.0.0.131	SMB	127		Negotiate Protocol Request
38510	2023-10-11 07:46:19.90867…	10.0.0.131	10.0.0.130	SMB2	506		Negotiate Protocol Response
38511	2023-10-11 07:46:19.90902…	10.0.0.130	10.0.0.131	SMB2	286		Negotiate Protocol Request
38512	2023-10-11 07:46:19.90969…	10.0.0.131	10.0.0.130	SMB2	590		Negotiate Protocol Response
38513	2023-10-11 07:46:19.91069…	10.0.0.130	10.0.0.131	SMB2	220		Session Setup Request, NTLMSSP_NEGOTIATE
38514	2023-10-11 07:46:19.91131…	10.0.0.131	10.0.0.130	SMB2	369		Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
38515	2023-10-11 07:46:19.91175…	10.0.0.130	10.0.0.131	SMB2	623		Session Setup Request, NTLMSSP_AUTH, User: \jdoe, Unknown NTLMSSP message type
38516	2023-10-11 07:46:19.91424…	10.0.0.131	10.0.0.130	SMB2	130		Session Setup Response, Error: STATUS_LOGON_FAILURE
38517	2023-10-11 07:46:19.91456…	10.0.0.130	10.0.0.131	TCP	60		49701 → 445 [RST, ACK] Seq=1041 Ack=1380 Win=0 Len=0



```
      Reserved: 0000000000000000
    ▾ Target Info
        Length: 128
        Maxlen: 128
        Offset: 80
      ▸ Attribute: NetBIOS domain name: MARKETING-PC
      ▸ Attribute: NetBIOS computer name: MARKETING-PC
      ▸ Attribute: DNS domain name: Marketing-PC
      ▸ Attribute: DNS computer name: Marketing-PC
      ▸ Attribute: Timestamp
      ▸ Attribute: End of list
    ▸ Version 10.0 (Build 19041); NTLM Current Revision 15
```

The target hostname is identified as MARKETING-PC, as reflected in attributes such as the NetBIOS domain name, NetBIOS computer name, and DNS computer name. These attributes confirm that the attacker targeted this machine in their attempt to expand their reach within the network. However, further inspection of the session setup shows a STATUS_LOGON_FAILURE error, indicating that the attacker's attempt to authenticate and establish a session was unsuccessful.

Answer: MARKETING-PC