CyberDefenders: PacketDetective Lab

The following writeup is for PacketDetective Lab on CyberDefenders, it involves investigating a pcap file.

Scenario: In September 2020, your SOC detected suspicious activity from a user device, flagged by unusual SMB protocol usage. Initial analysis indicates a possible compromise of a privileged account and remote access tool usage by an attacker.

Your task is to examine network traffic in the provided PCAP files to identify key indicators of compromise (IOCs) and gain insights into the attacker's methods, persistence tactics, and goals. Construct a timeline to better understand the progression of the attack by addressing the following questions.

The attacker's activity showed extensive SMB protocol usage, indicating a potential pattern of significant data transfer or file access. Calculating the total bytes used by SMB can help estimate the extent of file activity.

What is the total number of bytes used by the SMB protocol?

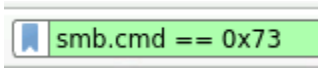
Start off by opening Traffic-1.pcapng with Wireshark. You can then navigate to Statics > Protocol Hierarchy to find the total number of bytes used by SMB:

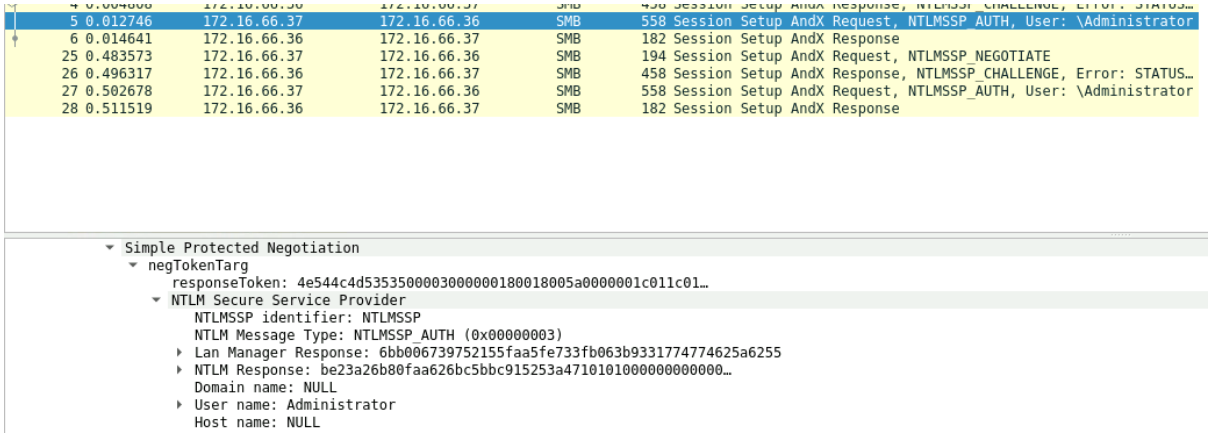
Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	32	100.0	6262
Ethernet	100.0	32	7.2	448
Internet Protocol Version 4	100.0	32	10.2	640
Transmission Control Protocol	100.0	32	82.6	5174
NetBIOS Session Service	100.0	32	72.4	4534
SMB (Server Message Block Protocol)	100.0	32	70.4	4406
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	15.6	5	5.3	332
Event Logger	9.4	3	1.9	116

As you can see, the total is 4406.

Authentication through SMB was a critical step in gaining access to the targeted system. Identifying the username for this authentication will help determine if a privileged account was compromised. Which username was utilised for authentication via SMB?

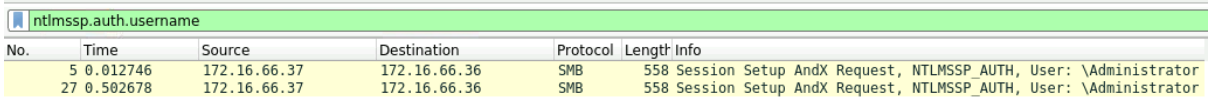
In the SMB protocol, usernames are typically transmitted during the Session Setup Request, we can use the following filter to search for Session Setup Andx Request:





We can that the username is Administrator.

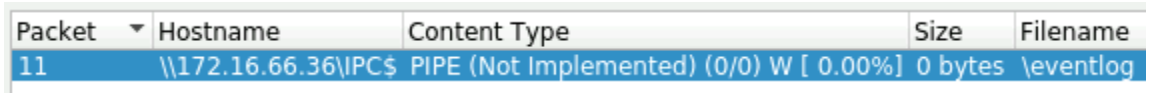
Alternatively, and as provided in the hint, you do use the following display filter:



During the attack, the adversary accessed certain files. Identifying which files were accessed can reveal the attacker's intent.

What is the name of the file that was opened by the attacker?

Navigate to File > Export Objects > SMB:

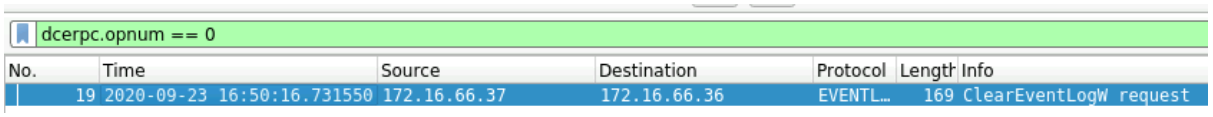


You can see that the file that was accessed is eventlog.

Clearing event logs is a common tactic to hide malicious actions and evade detection. Pinpointing the timestamp of this action is essential for building a timeline of the attacker's behaviour.

What is the timestamp of the attempt to clear the event log?

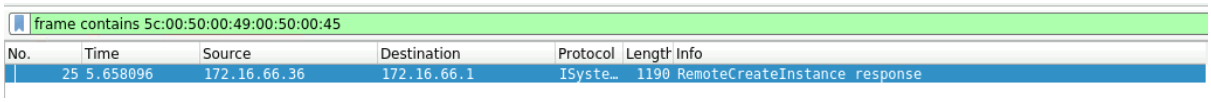
The ClearEventLogW function is invoked with opnum 0, we can filter for this and find the answer:



The attacker used "named pipes" for communication, suggesting they may have utilised Remote Procedure Calls (RPC) for lateral movements across the network. RPC allows one

program to request services from another remotely, which could grant the attacker unauthorised access or control. What is the name of the service that communicated using this named pipe?

To find what service communicated using this named pipe, we can search for the following hex sequence:



This is the hex representation of \PIPE.

Here we can see that the service is atsvc

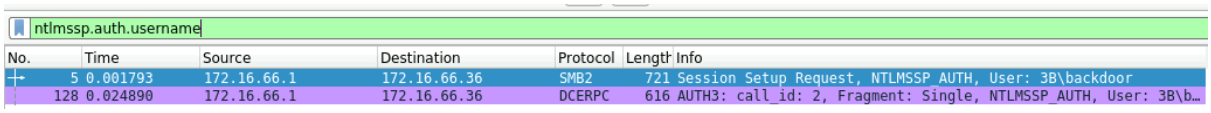
Measuring the duration of suspicious communication can reveal how long the attacker maintained unauthorised access, providing insights into the scope and persistence of the attack. What was the duration of communication between the identified addresses 172.16.66.1 and 172.16.66.36?

Navigate to Statistics > Conversations > IPv4 to find the duration of these communicating hosts:

11.7247.

The attacker used a non-standard username to set up requests, indicating an attempt to maintain covert access. Identifying this username is essential for understanding how persistence was established. Which username was used to set up these potentially suspicious requests?

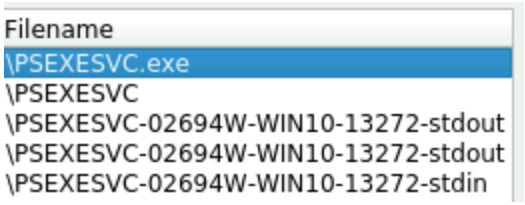
We can use the following display filter to search for NTLM authentication messages:



As you can see, the username is backdoor.

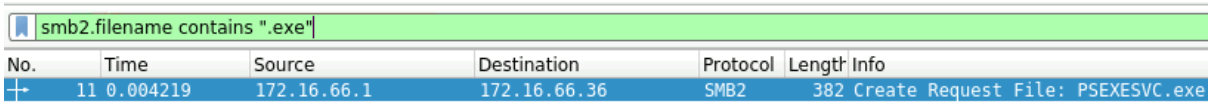
The attacker leveraged a specific executable file to execute processes remotely on the compromised system. Recognising this file name can assist in pinpointing the tools used in the attack. What is the name of the executable file utilised to execute processes remotely?

Navigate to File > Export Objects > SMB:



The binary used to execute processes remotely is PSEXESVC.exe. This appears to be PsExec, which is a non-malicious program part of the sysinternals suite of tools. It is often used by threat actors or malware to remotely execute programs.

As stated in the hint, you can also filter for .exe in the smb2 filename field:



This was an enjoyable lab and was also my first experience working with SMB traffic. Furthermore, it was my first experience using CyberDefenders, and I am pleasantly surprised with the content. If you have any feedback or need help with this lab, feel free to reach out.