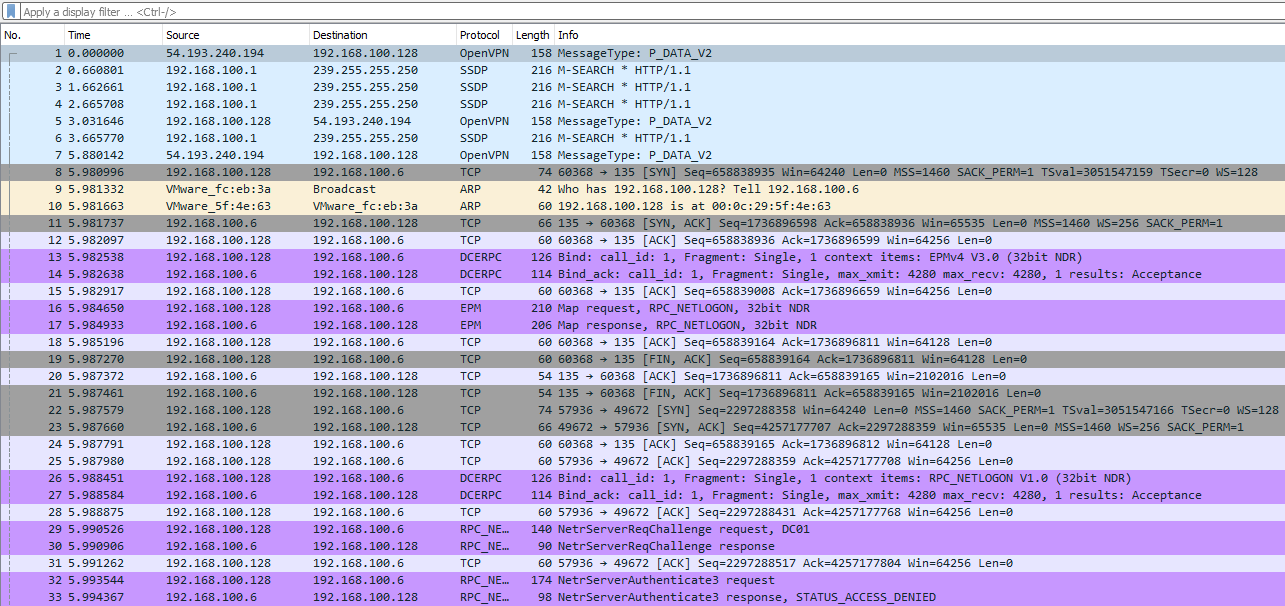
Zerologon PCAP Overview

We have gathered PCAP files from a recent Windows Active Directory Exploit called Zerologon or CVE-2020-1472. The scenario within the PCAP file contains a Windows Domain Controller with a private IP of 192.168.100.6 and an attacker with the private IP of 192.168.100.128. Let's walk through the steps of analyzing the PCAP and coming to a hypothesis of the events that happened.

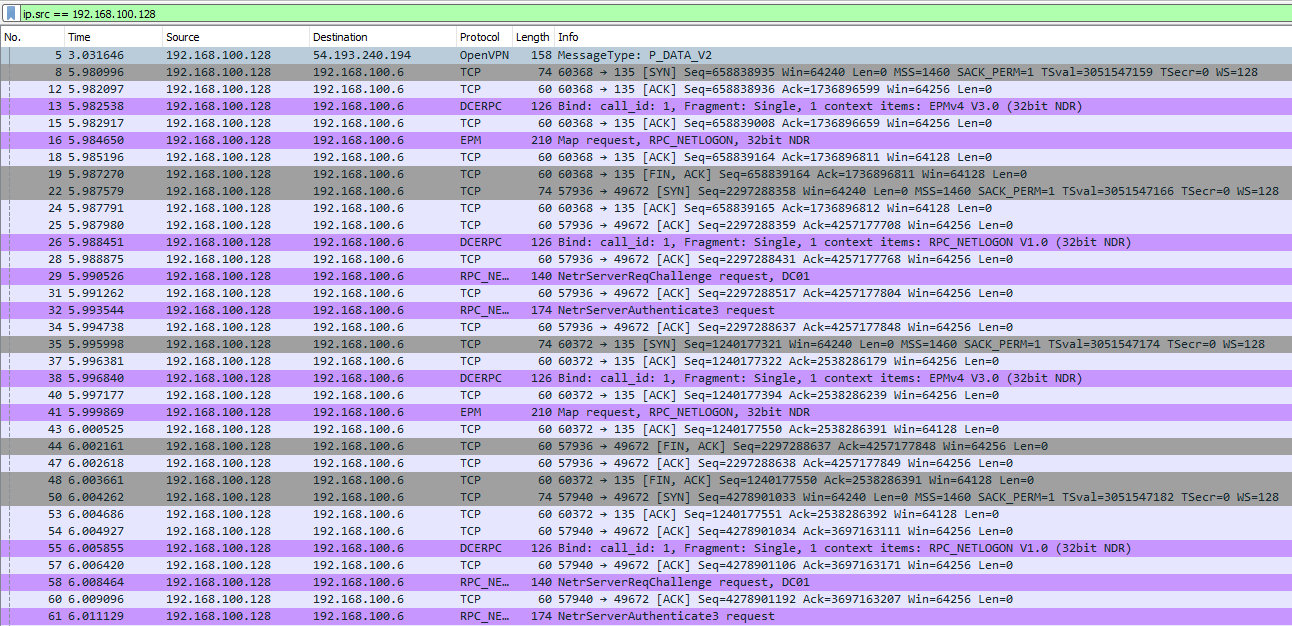


Identifying the Attacker

Immediately upon opening the PCAP file we see some things that may be out of the ordinary. First, we see some normal traffic from OpenVPN, ARP, etc. We then start to identify what would be known as unknown protocols in this case DCERPC and EPM.

Looking at the packets we see that 192.168.100.128 is sending all of the requests, so we can assume that the device is the attacker. We can continue looking at packets coming from this IP to narrow down our hunt.

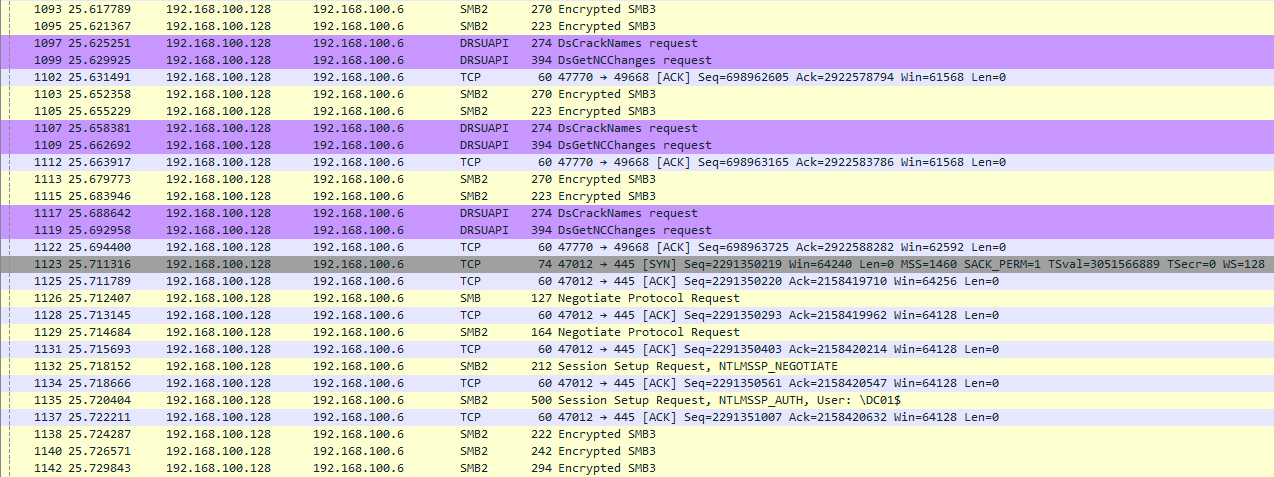
Zerologon POC Connection Analysis



We can set a filter for the src of the IP that we believe to be suspicious. When analyzing PCAPS we need to be aware of IOCs or Indicators of Compromise particular exploits may have with them. This is known as Threat Intelligence, which is out of the scope of this room; I recommend that after completing this room if you're interested more then do your own research on the topic. In this case, if we had background knowledge of the Zerologon exploit, we would know that the exploit uses multiple RPC connections, and DCERPC requests to change the machine account password, which could be verified with the PCAP.

Secretsdump SMB Analysis

Looking further at the PCAP we can see SMB2/3 traffic and DRSUAPI traffic, again with prior knowledge of the attack we know that it **uses secretsdump to dump hashes. Secretsdump abuses SMB2/3 and DRSUAPI** to do this, so we can assume that this traffic is secretsdump.



Each exploit and attack will come with its unique artifacts, in this case, it is clear what happened and the order of events that occurred. Once we have identified the attacker we would need to move on to other steps to identify and isolate as well as report the incident if we were on a Threat Hunting or DFIR team.