Ransomware

A system within the network has been compromised with ransomware. However, the attacker was not very smart. They left behind a few remnants of their work. These files, as well as the encrypted files, have been left for you to analyze and can be retrieved from the http://challenge.us (http://10.5.5.5) webpage from any in-game system. Try to recover the data and find the token within.

SQL Injection

You have been provided with the IIS web logs from the web server during the period of attack. These files can be retrieved from the http://challenge.us (http://10.5.5.5) webpage from any in-game system. Use these logs to ascertain the IP address of the target web server. Use the provided .asp page to find out more about the page itself. Then, IP your system accordingly and inspect the page, if necessary (Win10-SQL-Injection will work as is with eth1). Use the logs and .asp page file to discover the specific SQL injection method/tool used, replicate this act, and ultimately dump the table containing the token to confirm whether the attackers could have also retrieved this data via SQL injection.

*Note: If using sqlmap, the necessary operation can take time, be sure to start this early so that you may work on other tasks while it runs

Unauthorized Samba Service Access

You have been provided with a log file produced by the Samba service hosted on the 'kali-samba' system. This file can be retrieved from the http://challenge.us (http://10.5.5.5) webpage from any in-game system. Analyze the log file to determine the method that the attackers used to retrieve credentials and gain access to the server. You must then replicate this attack to discover what file(s) they gained access to. The token/flag for this task can be found within the file.

Local data exfiltration

It is believed that a malicious insider stole data via a direct copy to an attached thumb drive. You have been provided with the compromised system's HDD image and a timeline of events on the CD/DVD drive of the Win10-Forensics system. Discover which files they viewed and find the token within the specific file in question based on the submission field request. The incident occurred on or around 1 AM EDT on September 13th, 2021. However, the compromised system in question was set to PST. Ensure that you correlate time zones accordingly within any tools.

*Note: Timeline Explorer is available on the Windows 10 systems, you may find it runs faster if the timeline file is first copied to the system versus running it from the ISO.