SMB Open Share Enumeration

Prepared by: Hiren Vikhram S

Red Team - Information Security Team

Thursday, July 14, 2022

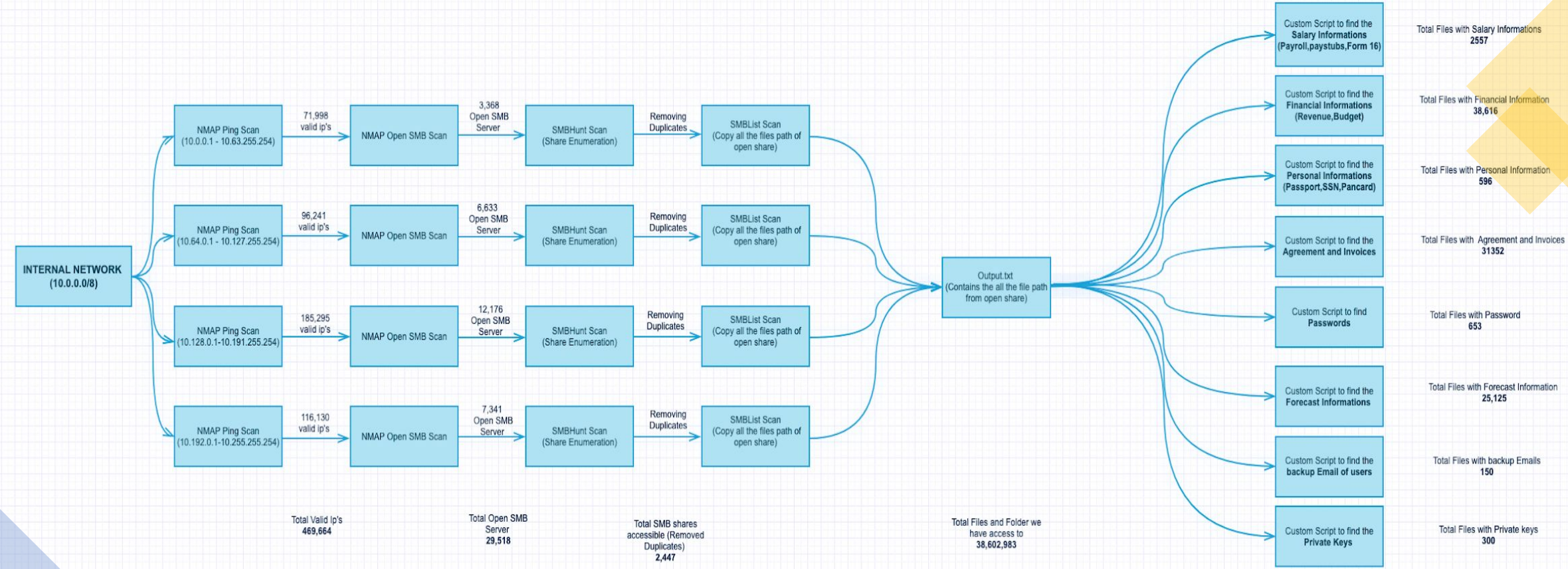
Summary:

- SMB (Server Message Block) is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain.
- Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.
- Businesses of all sizes have file shares with awful file permissions which are not monitored.
- The users are granted access rights that enable them to read or edit files containing sensitive data that they shouldn’t see.
- We created an automated script, which finds the all the SMB Server inside our network and enumerates for sensitive information which are exposed to all the users within network.

Automation Pipeline:

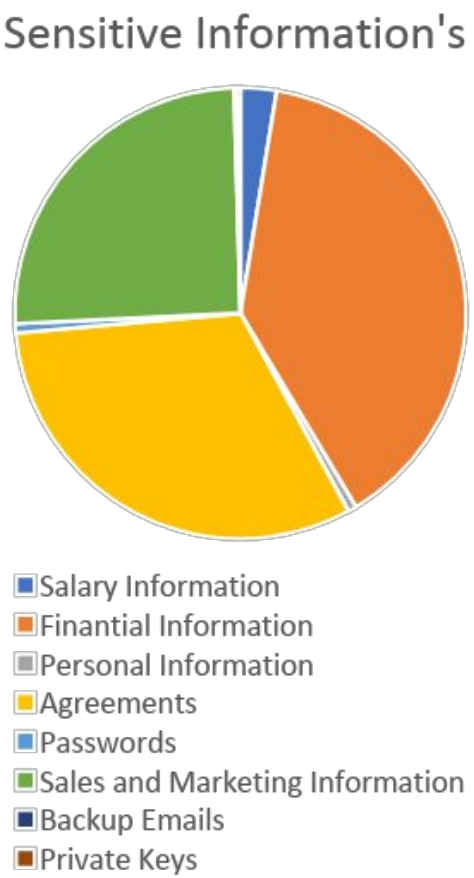
- Step1: We scanned the entire internal network(10.0.0.0/8) to find the pingable Ip’s. As a result of it we got 469,664 pingable Ip's.
- Step2: We found the Open SMB ports by port scanning the pingable Ip's. As a result of it we got 29,518 servers with SMB service open.
- Step 3: We scanned the 29,518 servers to find the share with read or write privilege. As a result of it we got 31,408 folders with read or write access.
- Step 4: We remove the duplicates and crawled these 2,447 shares and lists out all the files with read and write privilege. If we can read them, so can the ransomware and we copied the data to the output file.
- Step 5: We used a custom script to filter the sensitive information from output file.
- This whole operation is detection less.

Automation Pipeline Architecture:



Sensitive Information's:

- Salary Information (2,557 files)
- Financial Information (38,616 files)
- Personal Information (SSN, Passport, Pan card) (596 files)
- Agreement and Invoices (31,352 files)
- Passwords (653 files)
- Sales and Marketing Forecast (25,125 files)
- Backup Emails (150 files)
- Private Keys (300 files)



Critical Information's:

- Bank account numbers and the account balance for acquired companies.
- Latest revenue details from different countries and much more.

Further Enhancements: