BERINGIN KUNING CORPORATION

FINAL PROJECT NETWORK TRAFFIC REPORT

DECEMBER 2023

Analyze by:

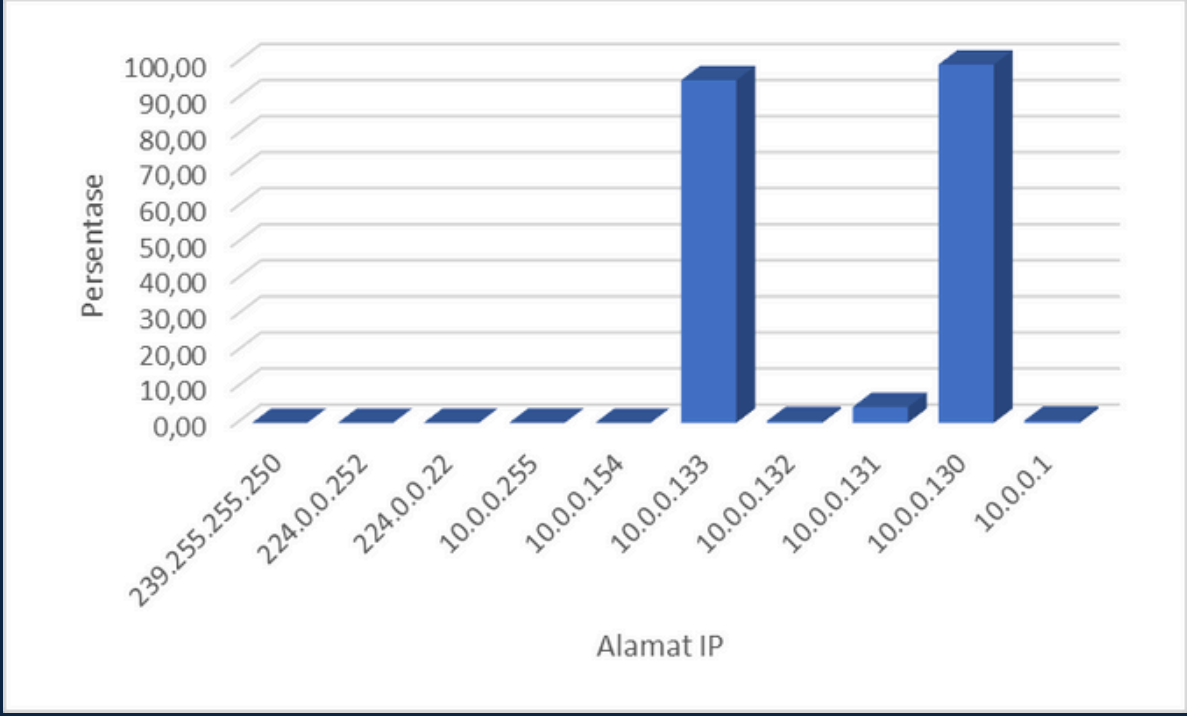
Nuriah Fadhilaturachman

DAFTAR ISI

1

Indikasi Lateral Movement

Distribusi Alamat IP



Alamat IP Multicast:

- **239.255.255.250: 0.03%**
- **224.0.0.252: 0.00%**
- **224.0.0.22: 0.02%**
- **Alamat IP multicast memiliki persentase yang rendah, menunjukkan bahwa lalu lintas multicast mungkin tidak signifikan dalam jaringan.**

Alamat IP Broadcast:

- **10.0.0.255: 0.08%**
- **10.0.0.254: 0.00%**
- **Alamat IP broadcast juga memiliki persentase rendah, yang menandakan bahwa lalu lintas broadcast mungkin tidak dominan.**

Alamat IP Tertentu:

- **10.0.0.133: 95.01%**
- **10.0.0.132: 0.50%**
- **10.0.0.131: 4.39%**
- **10.0.0.130: 99.37%**
- **10.0.0.1: 0.60%**
- **Alamat IP 10.0.0.133 dan 10.0.0.130 mendominasi lalu lintas dengan persentase yang tinggi**

Indikasi Lateral Movement (Cont'd)

IPv4 Statistics

Addresses	Percent	Burst Rate	Burst Start
239.255.255.250	0,03%	0,0100	272,122
224.0.0.252	0,00%	0,0100	33,11
10.0.0.255	0,08%	0,0100	11,983
10.0.0.255	0,08%	0,0100	11,983
10.0.0.254	0,00%	0,0100	32,2
10.0.0.133	95,01%	4,1200	483,385
10.0.0.132	0,50%	0,0100	0
10.0.0.131	4,39%	2,9100	548,371
10.0.0.130	99,37%	4,1200	483,385
10.0.0.1	0,60%	0,0200	415,488

Analisis statistik alamat IP memberikan wawasan terkait distribusi lalu lintas pada alamat IP jaringan.

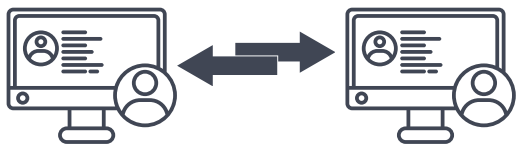
- **Alamat IP 10.0.0.130 memiliki persentase Burst Rate tertinggi dan mendominasi lalu lintas yang mencakup sekitar (99,37%), menunjukkan bahwa host dengan alamat IP ini memiliki lonjakan lalu lintas yang signifikan.**
- **Alamat IP 10.0.0.133 juga memiliki kontribusi yang besar terhadap lonjakan lalu lintas, sebesar (95,01%).**
- **Alamat IP lainnya, seperti 10.0.0.132 dan 10.0.0.131 memiliki persentase masing-masing 0.50% dan 4.39%**
- **Burst rate yang tinggi pada alamat IP 10.0.0.130 dan 10.0.0.133 dapat menunjukkan adanya aktivitas yang patut dicurigai. Burst rate yang tinggi dapat menunjukkan aktivitas yang cepat atau perubahan tiba-tiba dalam lalu lintas jaringan.**
- **Berdasarkan data statistik, tampaknya alamat IP yang mencurigakan adalah 10.0.0.130, karena memiliki aktivitas yang signifikan yang mencakup sekitar 99,37% dari semua aktivitas pada jaringan**

Indikasi Lateral Movement (Cont'd)

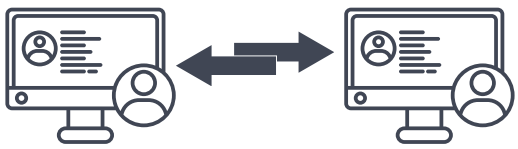
"tcp.port == 445"

Untuk analisis llayanan SMB (Server Message Block), yang mencakup berbagai protokol untuk berbagi file dan print, serta layanan untuk pengelolaan sesi dan otentikasi.

Dominasi Traffic



10.0.0.130 10.0.0.133



10.0.0.130 10.0.0.131

Analisis dari hasil filter tersebut menunjukan adanya permintaan untuk memulai koneksi. Dalam hal ini, mesin dengan IP Address 10.0.0.130 ingin memulai koneksi dengan mesin yang memiliki IP Address 10.0.0.133 pada port 445. Stelah itu, mesin dengan IP Address 10.0.0.130 juga memulai koneksi dengan mesin yang memiliki IP Address 10.0.0.131.

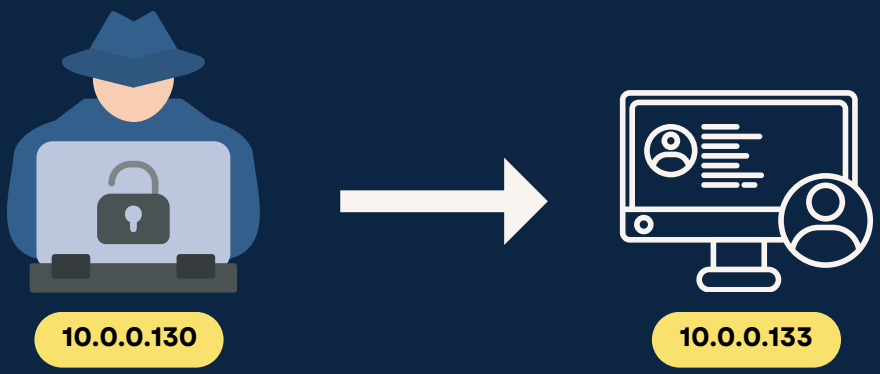
Berdasarkan analisis ada indikasi terjadinya lateral movement, tampaknya Attacker menggunakan alamat IP dari device 10.0.0.130

2 Host Target

Memulai sesi dengan 10.0.0.133

Attacker

HR-PC



10.0.0.130

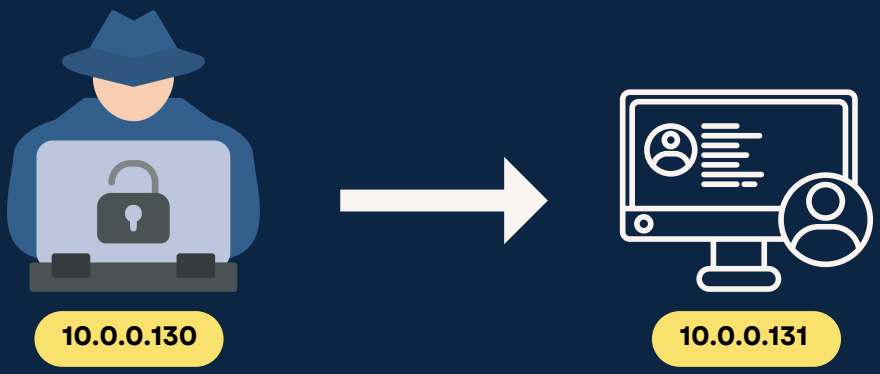
10.0.0.133

Mengakhiri sesi dengan 10.0.0.133

Memulai sesi dengan 10.0.0.131

Attacker

HR-PC



10.0.0.130

10.0.0.131

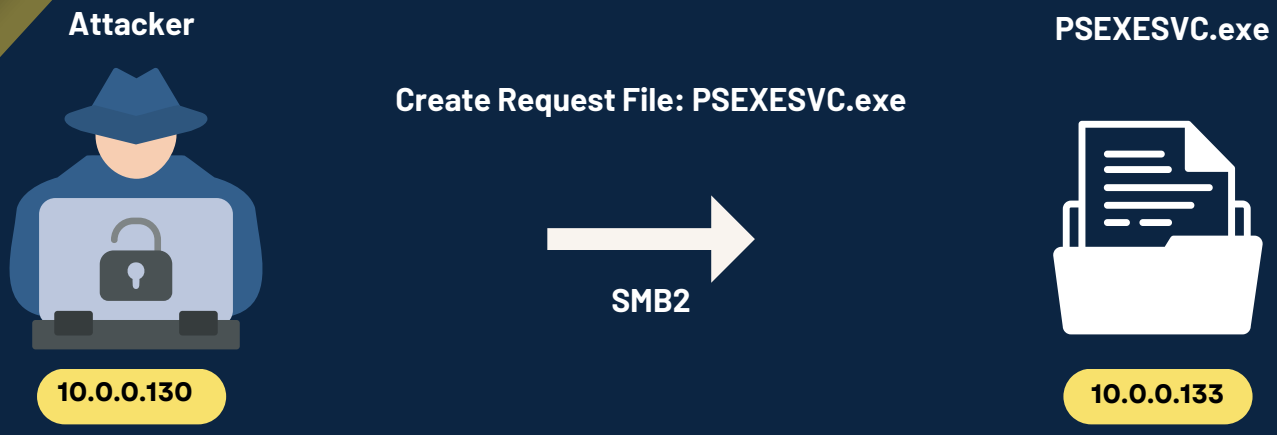
Dari data yang telah dianalisis, dapat dilihat jika Attacker ingin berpindah dari host dengan IP 10.0.0.130 ke host dengan IP 10.0.0.133. Setelahnya, Attacker juga terlihat berinteraksi dengan host yang memiliki alamat IP 10.0.0.131. Kedua IP ini (diidentifikasi sebagai HR-PC). Dengan asumsi HR-PC adalah mesin target yang diincar oleh pelaku, itu adalah mesin yang mungkin menjadi sasaran lateral movement atau serangan.

3 Username yang digunakan Attacker

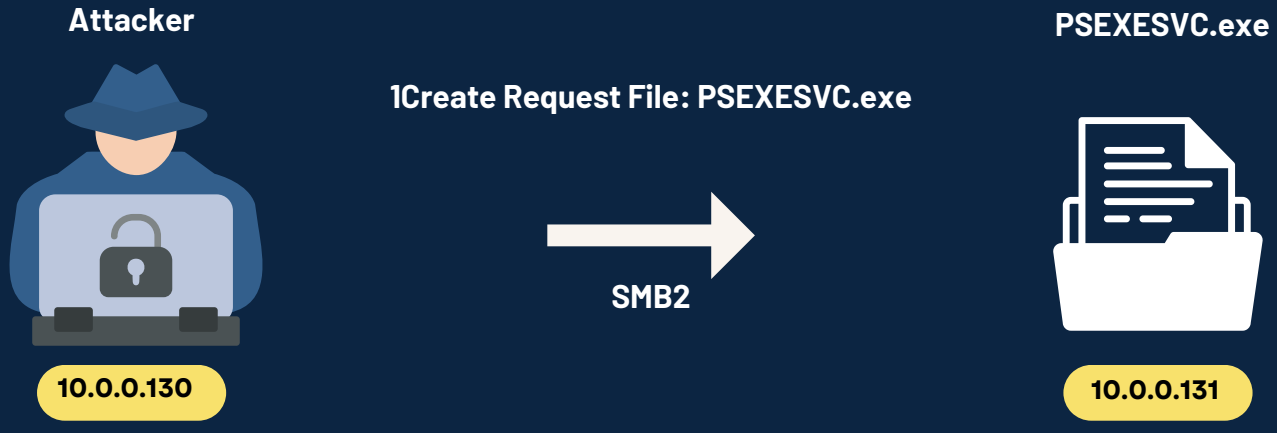
Username yang digunakan oleh attacker dalam melakukan lateral movement adalah "\ssales". Hal ini terlihat pada sesi SMB (Server Message Block) dengan kode perintah "Negotiate Protocol" yang mencantumkan informasi username dalam permintaan protokol SMB yang dikirimkan dari host 10.0.0.130 ke host 10.0.0.133.

Selama lateral movement, pelaku menggunakan akun dengan username "\IEUser" (domain tidak terlihat, mungkin domain lokal).

4 Executable service yang digunakan Attacker



terlihat ada sebuah aktivitas dengan menciptakan sebuah file bernama "PSEXESVC.exe" yang dilakukan oleh pelaku pada host target. Hal ini terlihat pada paket jaringan pada Frame, di mana terdapat respon pembuatan file dengan nama tersebut sebagai bagian dari sesi SMB2 antara host 10.0.0.133 dan 10.0.0.130. Adanya executable service dengan nama "PSEXESVC.exe" ini perlu diinvestigasi lebih lanjut sebagai potensi backdoor yang dibuat oleh pelaku di dalam target mesin.



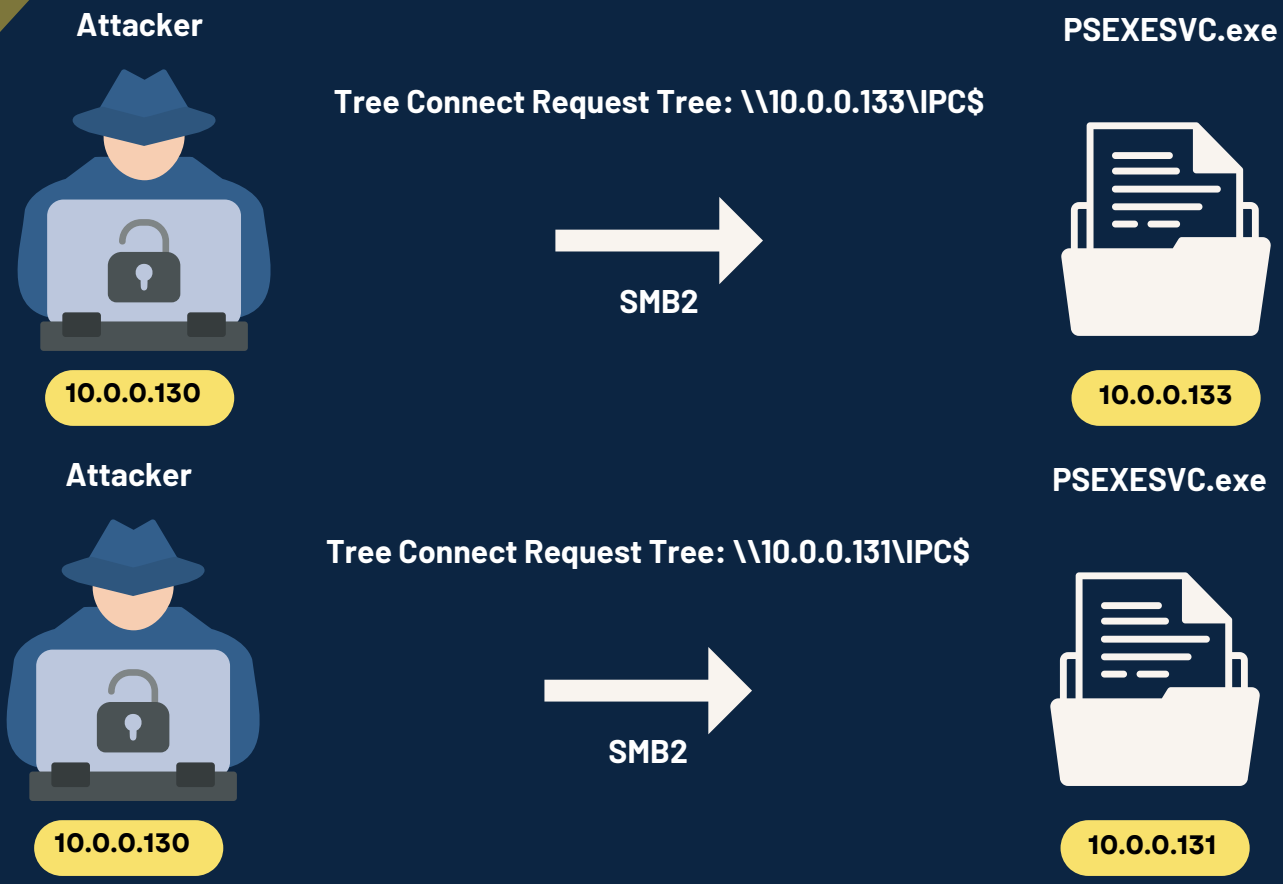
Attacker juga membuat file "PSEXESVC.exe" yang sama pada saat melakukan sesi dengan host 10.0.0.131.

5 Network Share yang digunakan Attacker

Attacker mengirim permintaan Tree Connect dalam protokol SMB2 (Server Message Block Protocol version 2) untuk membuat file "PSEXESVC.exe" pada network share dengan path "\10.0.0.133\ADMIN$" dan "\10.0.0.131\ADMIN$". Jadi, network share yang digunakan oleh pelaku untuk memasang service backdoor tersebut adalah "\10.0.0.133\ADMIN$" dan "\10.0.0.131\ADMIN$" yang kemudian digunakan pada organisasi

Network share ADMIN$ umumnya digunakan untuk akses administratif pada mesin Windows dalam lingkup jaringan. Pelaku mungkin menggunakan akses ini untuk mengeksploitasi mesin target dan melakukan tindakan yang tidak sah.

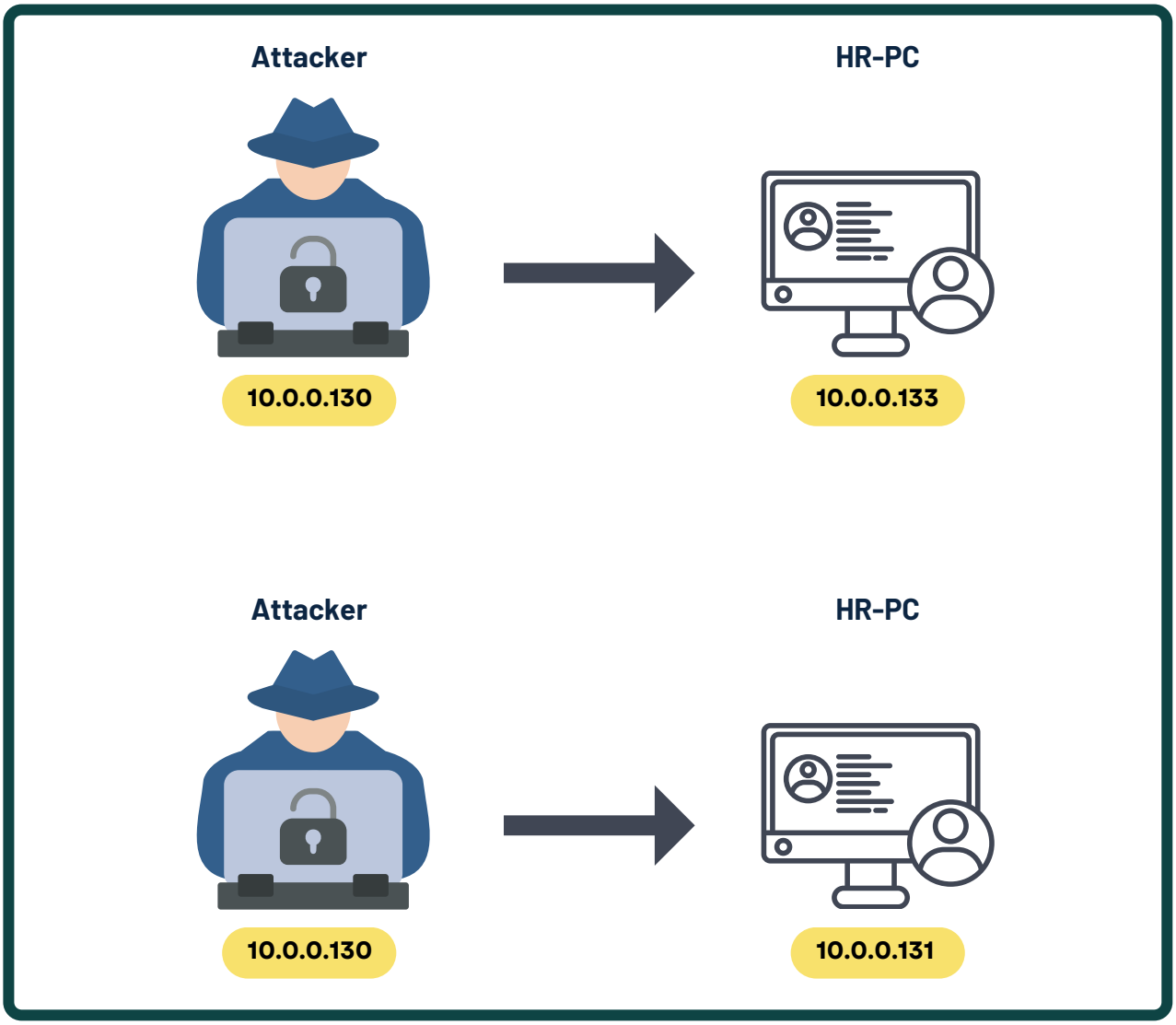
6 Host mesin yang Attacker coba lakukan Pivoting



Pelaku menggunakan path "\10.0.0.133\IPC$" dan "\10.0.0.131\IPC$" untuk komunikasi antar dua mesin di jaringan.

Permintaan ini mencoba untuk terhubung ke "IPC$," yang merupakan bagian dari NetBIOS Session Service dan dapat digunakan untuk berbagai operasi di atas SMB. Path "\10.0.0.133\IPC$" merujuk pada IPC$ (Inter-Process Communication) share pada host dengan alamat IP 10.0.0.133. pelaku menggunakan “\\10.0.0.131\IPC$” DAN “\\10.0.0.131\IPC$” untuk melakukan Tree Connect Request dan mendapatkan akses ke share tersebut. Setelah terhubung, pelaku kemudian melakukan Create Request dengan tujuan membuat atau memanfaatkan sebuah named pipe (saluran komunikasi) yang disebut "PSEXESVC". Jadi, dalam konteks ini, pelaku menggunakan IPC$ (Inter-Process Communication) share untuk membuat saluran komunikasi antara dua mesin di jaringan menggunakan PsExec. IPC$ adalah sebuah default share yang menyediakan layanan komunikasi antarproses. Share IPC$ ini umumnya digunakan untuk berbagai keperluan, termasuk manajemen jarak jauh dan transfer file antar mesin dalam jaringan.

Pivoting



Pelaku terlihat mencoba melakukan pivoting atau berpindah ke host dengan alamat IP 10.0.0.133 dan 10.0.0.131. Dari aktivitas yang tercatat, terlihat adanya upaya koneksi dari host awal yang diduga milik pelaku ke host dengan alamat tersebut. Itulah mesin yang menjadi target berikutnya dalam usaha berpindah-pindah atau lateral movement oleh pelaku

Glosarium

IPv4 (Internet Protocol Version 4):
- Sebuah protokol komunikasi yang digunakan dalam jaringan komputer untuk mengidentifikasi dan lokalisasi perangkat di internet melalui alamat IP.

Alamat IP (IP Address):
- Sebuah rangkaian numerik yang diberikan kepada setiap perangkat yang terhubung ke internet. Alamat IP memungkinkan perangkat untuk saling berkomunikasi di dalam jaringan.

Alamat IP Multicast:
- Alamat IP yang digunakan untuk mengirim data ke beberapa perangkat secara bersamaan dalam jaringan.

Alamat IP Broadcast:
- Alamat IP yang digunakan untuk mengirim data ke semua perangkat dalam suatu jaringan.

Burst Rate:
- Kecepatan maksimum di mana data dapat ditransfer dalam jangka waktu tertentu.

Burst Start:
- Waktu mulai dari periode burst di mana transfer data berlangsung pada tingkat burst.

Lateral Movement:
- Pemindahan dari satu perangkat ke perangkat lain dalam jaringan komputer, biasanya dalam konteks keamanan untuk menyusup lebih dalam ke dalam jaringan.

Glosarium (Cont'd)

tcp.port==445:
- **Filter atau kondisi untuk memeriksa paket jaringan yang menggunakan port TCP 445.**

Port 445:
- **Penjelasan: Nomor port yang digunakan oleh protokol SMB (Server Message Block) untuk komunikasi file sharing dalam jaringan.**

SMB (Server Message Block):
- **Protokol komunikasi yang digunakan untuk berbagi file, printer, dan sumber daya lainnya dalam jaringan komputer.**

SMB2:
- **Versi kedua dari protokol Server Message Block, digunakan untuk meningkatkan keamanan dan kinerja.**

Tree Connect:
- **Proses di mana komputer atau perangkat dihubungkan ke suatu pohon (tree) dalam jaringan untuk mengakses sumber daya bersama.**

Backdoor:
- **Sebuah metode atau pintu belakang yang diciptakan oleh pengembang perangkat lunak atau penyerang untuk mengakses sistem atau aplikasi secara tidak sah.**

Pivoting:
- **Suatu teknik di dalam keamanan informasi di mana penyerang menggunakan satu titik akses atau kompromi untuk mencapai akses lebih lanjut ke dalam jaringan.**