CyberDefenders: PsExec Hunt

The following writeup is for PsExec Hunt on CyberDefenders, it involves investigating a pcap file using wireshark.

Scenario: Our Intrusion Detection System (IDS) has raised an alert, indicating suspicious lateral movement activity involving the use of PsExec. To effectively respond to this incident, your role as a SOC Analyst is to analyse the captured network traffic stored in a PCAP file.

To effectively trace the attacker's activities within our network, can you determine the IP address of the machine from which the attacker initially gained accessed to our network?

I started off by navigating to Statistics > Conversations and then clicked the IPv4 tab, here we can see an IP (10.0.0.130) that has sent a lot of packets:

Ethernet · 10 | IPv4 · 10 | IPv6 | TCP · 81 | UDP · 6

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A
10.0.0.1	10.0.0.255	27	2 kB	27	2 kB	0
10.0.0.1	239.255.255.250	14	10 kB	14	10 kB	0
10.0.0.130	10.0.0.131	1,755	2 MB	1,136	1 MB	619
10.0.0.130	10.0.0.133	38,284	7 MB	19,237	4 MB	19,047
10.0.0.130	10.0.0.255	1	243 bytes	1	243 bytes	0
10.0.0.131	10.0.0.255	4	972 bytes	4	972 bytes	0
10.0.0.131	224.0.0.22	7	422 bytes	7	422 bytes	0
10.0.0.131	224.0.0.252	1	72 bytes	1	72 bytes	0
10.0.0.132	10.0.0.1	200	15 kB	200	15 kB	0
10.0.0.254	10.0.0.131	1	342 bytes	1	342 bytes	0

This amount of traffic is unusual compared to the other hosts and therefore is the answer. Alternatively, if you focus on the Info column in Wireshark, we can see 10.0.0.130 requesting PsExec:

```
10.0.0.130      10.0.0.133      445      SMB2    Create Request File: PSEXESVC.exe
10.0.0.133      10.0.0.130      49696    SMB2    Create Response File: PSEXESVC.exe
10.0.0.130      10.0.0.133      445      SMB2    Write Request Len:65536 Off:0 File: PSEXESVC.exe
```

To fully comprehend the extent of the breach, can you determine the machine's hostname to which the attacker first pivoted?

If we investigate the SMB traffic of 10.0.0.130, we come across frame number 192 which if you follow its TCP steam, you can see the machine's hostname.

```
......NTLMSSP.........8........|...wk.........`.`.H...
.aJ....S.A.L.E.S.-.P.C.....S.A.L.E.S.-.P.C.....S.A.L.E.S.-.P.C.....S.a.l.e.s.-.P.C.....S.a.l.e.s.-.P.C........p.
```

After identifying the initial entry point, it's crucial to understand how far the attacker has moved laterally within our network. Knowing the username of the account the attacker used for authentication will give us insights into the extent of the breach. What is the username utilised by the attacker for authentication?

If we use the following filter and look through the results, we can see that the attacker has authenticated to the “ssales” user:

10.0.0.130	10.0.0.133	445	SMB2	Session Setup Request, NTLMSSP_AUTH, User: \ssales

The ntlmssp filter is pretty unnecessary for this task, you can just filter for smb2 traffic and look for session setup requests to find the same answer.

After figuring out how the attacker moved within our network, we need to know what they did on the target machine. What’s the name of the service executable the attacker set up on the target?

Soon after the Session Setup Request, we can see a Write Request for file PSEXESVC.exe, therefore the answer is PSEXESVC:

10.0.0.130	10.0.0.133	445	SMB2	Create Request File: PSEXESVC.exe
10.0.0.133	10.0.0.130	49696	SMB2	Create Response File: PSEXESVC.exe
10.0.0.130	10.0.0.133	445	SMB2	Write Request Len:65536 Off:0 File: PSEXESVC.exe
10.0.0.130	10.0.0.133	445	SMB2	Write Request Len:65536 Off:65536 File: PSEXESVC.exe
10.0.0.133	10.0.0.130	49696	SMB2	Write Response
10.0.0.133	10.0.0.130	49696	SMB2	Write Response
10.0.0.130	10.0.0.133	445	SMB2	Write Request Len:65536 Off:131072 File: PSEXESVC.exe

Alternatively, you can go to File > Objects > SMB:

Packet	Hostname	Content Type	Size	Filename
192	\\10.0.0.133\ADMIN$	FILE (197008/242064) W [81.00%]	242 kB	\PSEXESVC.exe
38593	\\10.0.0.131\ADMIN$	FILE (242064/242064) W [100.00%]	242 kB	\PSEXESVC.exe
39173	\\10.0.0.131\ADMIN$	FILE (242064/242064) W [100.00%]	242 kB	\PSEXESVC.exe
39756	\\10.0.0.131\ADMIN$	FILE (242064/242064) W [100.00%]	242 kB	\PSEXESVC.exe
521	\\10.0.0.133\TREEID_UNKNOWN	FILE (4/4) R [100.00%]	4 bytes	\PSEXESVC-HR-PC-7980-stdout
523	\\10.0.0.133\IPC$	FILE (176/176) R [100.00%]	176 bytes	\PSEXESVC-HR-PC-7980-stdout
566	\\10.0.0.133\IPC$	FILE (16/16) W [100.00%]	16 bytes	\PSEXESVC-HR-PC-7980-stdin
38219	\\10.0.0.133\TREEID_UNKNOWN	FILE (4/4) R [100.00%]	4 bytes	\PSEXESVC-HR-PC-7980-stderr
38221	\\10.0.0.133\IPC$	FILE (128/128) R [100.00%]	128 bytes	\PSEXESVC-HR-PC-7980-stderr
391	\\10.0.0.133\IPC$	FILE (65535/65535) R&W [100.00%]	65 kB	\PSEXESVC
38794	\\10.0.0.131\IPC$	FILE (65535/65535) R&W [100.00%]	65 kB	\PSEXESVC
39377	\\10.0.0.131\IPC$	FILE (65535/65535) R&W [100.00%]	65 kB	\PSEXESVC
39961	\\10.0.0.131\IPC$	FILE (65535/65535) R&W [100.00%]	65 kB	\PSEXESVC
39934	\\10.0.0.131\ADMIN$	FILE (16/16) W [100.00%]	16 bytes	\PSEXEC-HR-PC-CF174DD5.key
39350	\\10.0.0.131\ADMIN$	FILE (16/16) W [100.00%]	16 bytes	\PSEXEC-HR-PC-AF58F077.key
38767	\\10.0.0.131\ADMIN$	FILE (16/16) W [100.00%]	16 bytes	\PSEXEC-HR-PC-8FF87B23.key
366	\\10.0.0.133\ADMIN$	FILE (16/16) W [100.00%]	16 bytes	\PSEXEC-HR-PC-1C6C5D14.key

We need to know how the attacker installed the service on the compromised machine to understand the attacker’s lateral movement tactics. This can help identify other affected systems. Which network share was used by PsExec to install the service on the target machine?

We know that the ADMIN$ share was used:

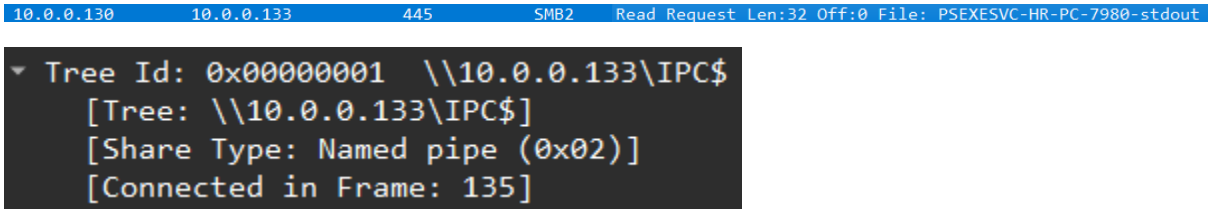
```
Tree Connect Request Tree: \\10.0.0.133\ADMIN$
Tree Connect Response
```

Right after those requests is the create request file packets. Also, in the SMB objects list we can see the hostname is \\10.0.0.133\ADMIN$.

We must identify the network share used to communicate between the two machines. Which network share did PsExec use for communication?

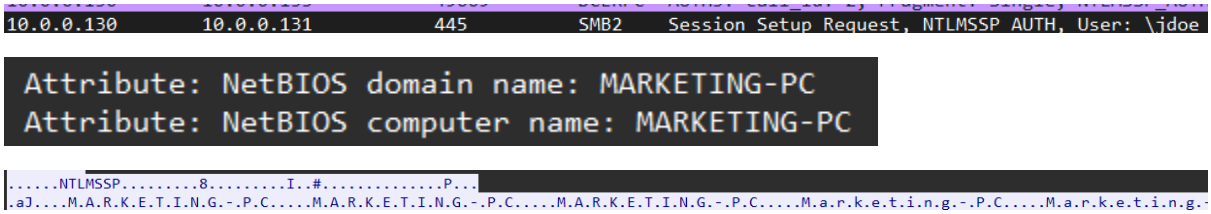
IPC$

Using the hint, it says that PsExec often utilised specific shares for command execution between machines, and to see if any file names include stdout, stdin, or stderr:



Now that we have a clearer picture of the attacker's activities on the compromised machine, it's important to identify any further lateral movement. What is the machines hostname to which the attacker attempted to pivot within our network?

If we search for packets that contain the NetBIOS domain name filed within the NTLMv2 Response, we can find the hostname of the machine to which the attacker attempted to pivot:



This room was pretty challenging for me, as I'm really only good at analysing HTTP traffic. However, it proved to be a wonderful learning experience as I learnt a lot regarding analysing SMB traffic.