Detecting Cobalt Strike's PSExec

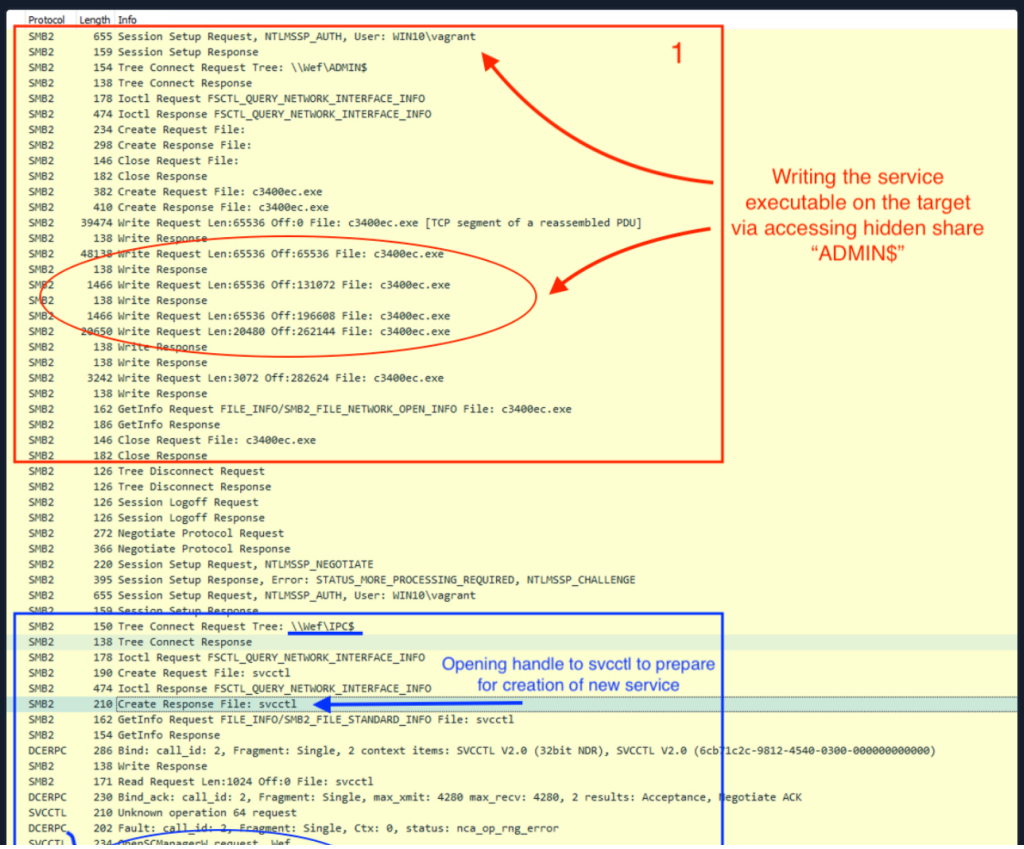
Cobalt Strike's `psexec` command is an implementation of the popular PsExec tool, which is a part of Microsoft's Sysinternals Suite. It's a lightweight telnet-replacement that lets you execute processes on other systems. Cobalt Strike's version is utilized to execute payloads on remote systems, as part of the post-exploitation process.

When the `psexec` command is invoked within Cobalt Strike, the following steps occur:

- `Service Creation`: The tool first creates a new service on the target system. This service is responsible for executing the desired payload. The service is typically created with a random name to avoid easy detection.
- `File Transfer`: Cobalt Strike then transfers the payload to the target system, often to the `ADMIN$` share. This is typically done using the SMB protocol.
- `Service Execution`: The newly created service is then started, which in turn executes the payload. This payload can be a shellcode, an executable, or any other file type that can be executed.
- `Service Removal`: After the payload has been executed, the service is stopped and deleted from the target system to minimize traces of the intrusion.
- `Communication`: If the payload is a beacon or another type of backdoor, it will typically establish communication back to the Cobalt Strike team server, allowing for further commands to be sent and executed on the compromised system.

Cobalt Strike's `psexec` works over port 445 (SMB), and it requires local administrator privileges on the target system. Therefore, it's often used after initial access has been achieved and privileges have been escalated.

How Cobalt Strike PSExec Traffic Looks Like



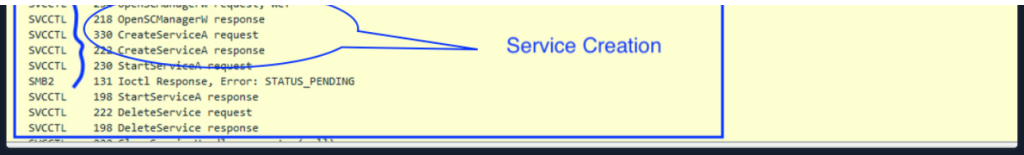


Image Source: https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/

Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, access the Splunk interface at https://[Target IP]:8000 and launch the Search & Reporting Splunk application. The vast majority of searches covered from this point up to end of this section can be replicated inside the target, offering a more comprehensive grasp of the topics presented.

Additionally, we can access the spawned target via RDP as outlined below. All files, logs, and PCAP files related to the covered attacks can be found in the /home/htb-student and /home/htb-student/module_files directories.

Detecting Cobalt Strike's PSExec

```
MisaelMacias@htb[/htb]$ xfreerdp /u:htb-student /p:'HTB_@cademy_stdnt!' /v:[Target IP] /dynamic-res
```

Related Evidence

- **Related Directory**: /home/htb-student/module_files/cobalt_strike_psexec
- **Related Splunk Index**: cobalt_strike_psexec
- **Related Splunk Sourcetype**: bro:smb_files:json

Detecting Cobalt Strike's PSExec With Splunk & Zeek Logs

Now let's explore how we can identify Cobalt Strike's PSExec, using Splunk and Zeek logs.

Detecting Cobalt Strike's PSExec

```
index="cobalt_strike_psexec"
sourcetype="bro:smb_files:json"
action="SMB::FILE_OPEN"
name IN ("*.exe", "*.dll", "*.bat")
path IN ("*\\c$", "*\\ADMIN$")
size>0
```

i	Time	Event
>	8/22/21 7:00:41.000 AM	{ [-] action: SMB::FILE_OPEN id.orig_h: 192.168.38.104 id.orig_p: 49394 id.resp_h: 192.168.38.102 id.resp_p: 445 name: be5312f.exe path: \\DC\ADMIN$ size: 285696 times.accessed: 2021-08-22T07:00:20.467586Z times.changed: 2021-08-22T07:00:20.475082Z times.created: 2021-08-22T07:00:20.467586Z times.modified: 2021-08-22T07:00:20.475082Z ts: 2021-08-22T07:00:41.577519Z uid: CfuL6Kn6isF0IrfXl }

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK — 136ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File

Target(s): Click here to spawn the target system!

+ 1 Use the "change_service_config" index and the "bro:dce_rpc:json" sourcetype to create a Splunk search that will detect SharpNoPSExec (https://gist.github.com/defensivedepth/ae3f882efa47e20990bc562a8b052984). Enter the IP included in the "id.orig_h" field as your answer.

192.168.38.104

Submit