Detecting Exfiltration (HTTP)

`Data exfiltration` inside the POST body is a technique that attackers employ to extract sensitive information from a compromised system by disguising it as legitimate web traffic. It involves transmitting the stolen data from the compromised system to an external server controlled by the attacker using HTTP POST requests. Since POST requests are commonly used for legitimate purposes, such as form submissions and file uploads, this method of data exfiltration can be difficult to detect.

To exfiltrate the data, the attackers send it as the body of an HTTP POST request to their command and control (C2) server. They often use seemingly innocuous URLs and headers to further disguise the malicious traffic. The C2 server receives the POST request, extracts the data from the body, and decodes or decrypts it for further analysis and exploitation.

To detect data exfiltration via POST body, we can employ network monitoring and analysis tools to aggregate all data sent to specific IP addresses and ports. By analyzing the aggregated data, we can identify patterns and anomalies that may indicate data exfiltration attempts.

In this section, we will monitor the volume of outgoing traffic from our network to specific IP addresses and ports. If we observe unusually large or frequent data transfers to a specific destination, it may indicate data exfiltration.

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 Exfiltration (HTTP)

```
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/cobaltstrike_exfiltration_http`
- **Related Splunk Index:** `cobaltstrike_exfiltration_http`
- **Related Splunk Sourcetype:** `bro:http:json`

Detecting HTTP Exfiltration With Splunk & Zeek Logs

Now let's explore how we can identify HTTP exfiltration, using Splunk and Zeek logs.

Detecting Exfiltration (HTTP)

```
index="cobaltstrike_exfiltration_http" sourcetype="bro:http:json" method=POST
| stats sum(request_body_len) as TotalBytes by src, dest, dest_port
| eval TotalBytes = TotalBytes/1024/1024
```

New Search Save As Create Table View Close

```
index="cobaltstrike_exfiltration_http" sourcetype="bro:http:json" method=POST
| stats sum(request_body_len) as TotalBytes by src, dest, dest_port
| eval TotalBytes = TotalBytes/1024/1024
```

All time

✓ 528 events (before 8/20/23 3:24:09.000 AM) No Event Sampling Job Fast Mode

Events Patterns Statistics (1) Visualization

20 Per Page Format Preview

src	dest	dest_port	TotalBytes
10.0.10.100	192.168.151.181	80	256.0760498046875

Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

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.

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 140ms

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 "cobaltstrike_exfiltration_https" index and the "bro:conn:json" sourcetype. Create a Splunk search to identify exfiltration through HTTPS. Enter the identified destination IP as your answer.

192.168.151.181

Submit

Previous Next

Mark Complete & Next