**Cybersecurity 401**

**Module 6 - Threat Modeling and Analysis**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Read 26 - Remote Code Execution**

## 

**| Rodrigo Brasil 12/2023 |**

## **Reading**

[**Cyber Threat Analyst: Key Job Skills and Expected Salary**](https://www.toolbox.com/security/vulnerability-management/articles/cyber-threat-analyst-key-jobs-and-salary/)

[**Tracking, Detecting, and Thwarting PowerShell-based Malware and Attacks**](https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/tracking-detecting-and-thwarting-powershell-based-malware-and-attacks)

1. **You just got a new job as a Cyber Threat Analyst, how would you explain your role to a family member?**
   1. My job is to analyze the network of the company to prevent and mitigate cyber attacks.
2. **Explain what makes PowerShell such an effective attack vector.**
   1. Attackers can use fileless malware to get around these safeguards by injecting payloads into running applications or by utilizing scripting.

PowerShell is an ideal channel for delivering these attacks because of its wide deployment and access to all parts of a host via the .NET framework.

1. **What are two things you can do to mitigate attacks that leverage PowerShell?**
   1. Tracking powershell activities with logs, countering obfuscation and behavior monitoring.