檢測暴力攻擊

暴力攻擊是威脅行動者常用的攻擊手段，用於獲得未經授權的端點和服務訪問權限。Linux 端點上的 SSH 服務和 Windows 端點上的 RDP 服務通常容易受到暴力攻擊。Wazuh 通過相關多個身份驗證失敗事件來識別暴力攻擊。

"使用主動回應（Active Response）封鎖攻擊"一節描述了如何配置主動回應來封鎖攻擊者的 IP 地址。在這個使用案例中，我們展示了 Wazuh 如何檢測 RHEL 和 Windows 端點上的暴力攻擊。

基礎架構

端點

描述

Ubuntu 22.04

執行暴力攻擊的攻擊者端點。需要在此端點上安裝 SSH 客戶端。

RHEL 9.0

SSH 暴力攻擊的受害者端點。需要在此端點上安裝並啟用 SSH 服務。

Windows 11

RDP 暴力攻擊的受害者端點。需要在此端點上啟用 RDP。

配置

執行以下步驟來配置 Ubuntu 端點，這允許在受監控的 RHEL 和 Windows 端點上執行身份驗證失敗的嘗試。

在攻擊者端點上，安裝 Hydra 並使用它來執行暴力攻擊：

```
sudo apt update
sudo apt install -y hydra
```

攻擊模擬

創建一個包含10個隨機密碼的文本檔。

從攻擊者端點運行 Hydra 來對 RHEL 端點執行暴力攻擊。為此，請將<RHEL_IP>替換為 RHEL 端點的 IP 地址，並運行以下命令：

```
sudo hydra -l badguy -P <PASSWD_LIST.txt> <RHEL_IP> ssh
```

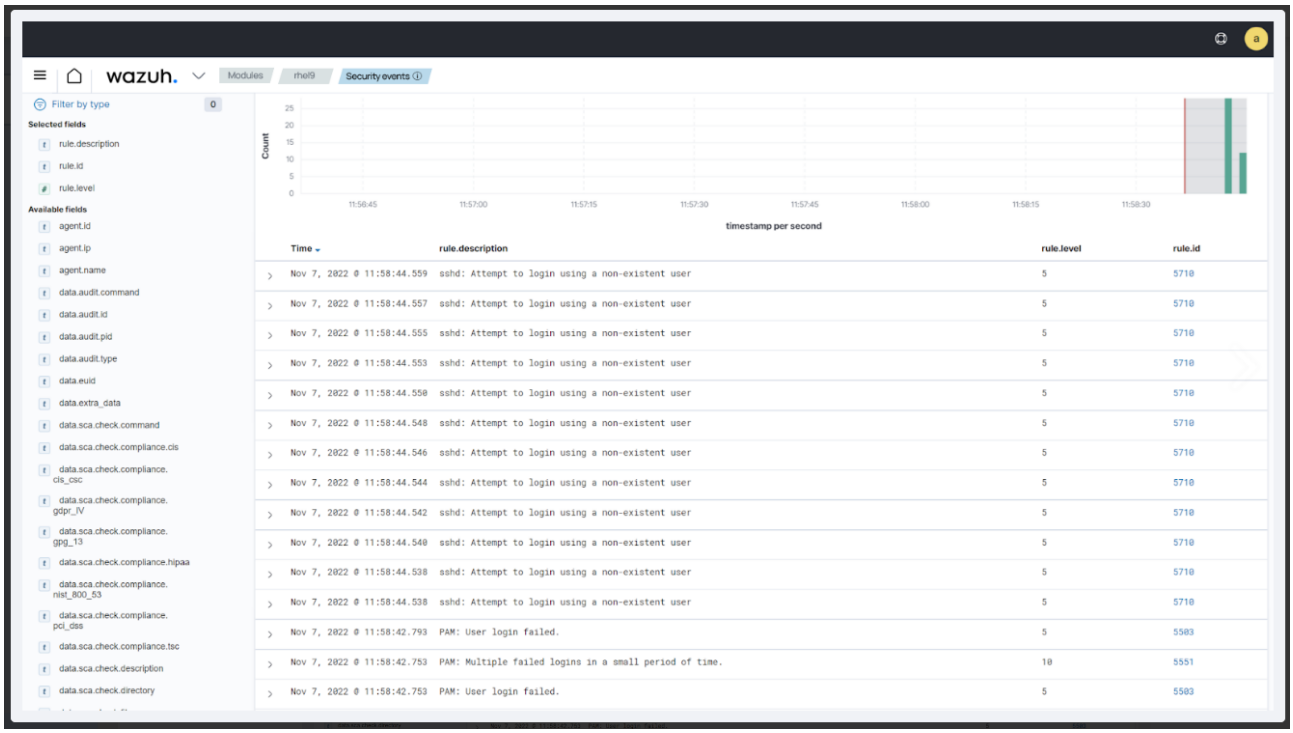
從攻擊者端點運行 Hydra 來對 Windows 端點執行暴力攻擊。為此，請將<WINDOWS_IP>替換為 Windows 端點的 IP 地址，並運行以下命令：

```
sudo hydra -l badguy -P <PASSWD_LIST.txt> rdp://<WINDOWS_IP>
```

可視化警報資料

您可以在 Wazuh 儀表板中視覺化警報資料。要做到這一點，請前往安全事件模組，並在搜尋欄中添加過濾器來查詢警報。

Linux - rule.id:(5551 OR 5712)。其他相關的規則有5710、5711、5716、5720、5503、5504。



Windows - `rule.id:(60122 OR 60204)`