檢測 Shellshock 攻擊

Wazuh 能夠通過分析來自受監控端點的 Web 伺服器日誌來檢測 Shellshock 攻擊。在這個使用案例中，您在 Ubuntu 端點上設置了一個 Apache Web 伺服器並模擬了一個 Shellshock 攻擊。

基礎架構

端點

描述

Ubuntu 22.04

受害端點運行 Apache 2.4.54 Web 伺服器。

RHEL 9.0

攻擊端點向受害者的 Web 伺服器發送惡意 HTTP 請求。

配置

Ubuntu 端點

執行以下步驟來安裝 Apache Web 伺服器並使用 Wazuh 代理監控其日誌。

更新本地套件並安裝 Apache Web 伺服器：

```
sudo apt update
sudo apt install apache2
```

如果啟用了防火牆，請修改它以允許對 Web 端口的外部訪問。如果防火牆已禁用，則跳過此步驟：

```
sudo ufw app list
sudo ufw allow 'Apache'
sudo ufw status
```

檢查 Apache Web 伺服器是否正在運行：

```
sudo systemctl status apache2
```

將以下行添加到 Wazuh 代理的/var/ossec/etc/ossec.conf 配置文件。這會設置 Wazuh 代理來監控 Apache 伺服器的訪問日誌：

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/apache2/access.log</location>
</localfile>
```

重新啟動 Wazuh 代理以應用配置更改：

```
sudo systemctl restart wazuh-agent
```

攻擊模擬

將<WEBSERVER_IP>替換為 Ubuntu IP 地址，然後從攻擊端點執行以下命令：

```
sudo curl -H "User-Agent: () { :; }; /bin/cat /etc/passwd" <WEBSERVER-IP>
```

視覺化警報

您可以在 Wazuh 儀表板中視覺化警報資料。要這樣做，進入 Security events 模組，並在搜尋欄中添加過濾器以查詢警報。

```
rule.description:Shellshock attack detected
```

如果您有 Suricata 監控端點流量，您也可以查詢 rule.description:CVE-2014-6271以查詢相關的 Suricata 警報。