SIEM CASE Analysis

You are a member of an organization security operation centre team. You were told to investigate a suspected cybersecurity breach. It was suspected that the attacker gained an initial foothold into the organization through the company website hosted on a Linux server. You have been provided the log files from the base Linux server and the web server Apache logs. Investigate the breach and provide the necessary information for remediation.

Setup Guide

1. Install the free 60-day trial splunk enterprise software

Download Link:

<https://www.splunk.com/en_us/download.html?utm_campaign=bing_apac_aus_en_search_brand&utm_source=bing&utm_medium=cpc&utm_content=free_trials_downloads_TR&utm_term=splunk%20enterprise&_bk=splunk%20enterprise&_bt=&_bm=p&_bn=o&_bg=1142393259223237&device=c&msclkid=e3feaf041fdf13686a02cfbefb01a049>

1. Upload the log files into your Splunk instance:

Resource:

https://www.youtube.com/watch?v=3GKhCZfQqDM

1. Query the dataset for the investigation.

Resource:

Splunk fundamentals 1 training: [Free Splunk Fundamentals 1 | Splunk](https://www.splunk.com/en_us/training/free-courses/splunk-fundamentals-1.html)

Walkthrough of a similar investigation : [(40) Splunk BOTS - Boss Of The SOC (v3) Walkthrough & Analysis - YouTube](https://www.youtube.com/watch?v=RXDbir6B5mE)

Important Linux Log Files: [12 Critical Linux Log Files You Must be Monitoring - (eurovps.com)](https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring/)

1. What popular scanning scripting engine tool was utilized by the attacker was utilized by the attacker against the webserve? (Hint: \*\*\*\*)

Answer: nmap

1. The attacker downloaded a pcap file from the webserver. What is the name of the pcap file that the attacker downloaded? (Hint: \*\*\*\*\*\*\*.cap)

Answer: analyze.cap

1. The attacker created a reverse shell by editing and getting a php file located on the WordPress site. What is the name of the php file the attacker used to gain access to the system? (Hint: \*\*\*.php)

Answer: 404.php

1. After discovering user credentials in the pcap file, the attacker used ssh to log into the system using this user. What was the user that was used to ssh into the system? (Hint: \*\*\*\*\*\*\*\*\*\*\*\*)

Answer: webdeveloper

1. What was the attackers IP address that he used to ssh into the system? (Hint: \*\*\*. \*\*\*.\*.\*\*\*)

Answer: 192.168.1.113

1. After connecting to the system as a valid account, The attacker echoed the content of the malicious php file into a system file. What is the system file the contents of the php file was echoed to? (Hint: /\*\*\*/.\*\*\*)

Answer: /tmp/.test

1. The attacker initially attempted to create a new user but it failed, what was the name of the user he tried to create? (Hint: \*\*\*\*\*\*\*\*\*\*)

Answer: Compromise

1. The attacker successfully created a new user after becoming root. What was the name of the account that was created? (Hint: \*\*\*\*\*\*\*\*)

Answer: attacker

1. What time was the successful user created (Hint: \*\*: \*\* \*\*) (hh:mm pm)

Answer: 10:15 pm

1. What was the UID of the successful username created?

Answer: 1003