Author: Jack Fitzgerald

Official Incident Report

Date: Jun, 13, 2021, 04:23 PM

Event ID: 94

Rule Name: SOC147 - SSH Scan Activity

Table of Contents

Alert Details

Severity: Medium

Type: Malware

Source Address: 172.16.20.5

Source Hostname: PentestMachine

File Name: nmap

File Hash: 3361bf0051cc657ba90b46be53fe5b36

File Size: 2.82 MB

Device Action: Allowed

Based on the information provided in the alert, it appears that **nmap**, a network discovery and security auditing software, has been run on host **172.16.20.5**. The alert is triggered by rule SOC147 - SSH Scan Activity.

Typically, the Pentest team sends notification emails to SOC teams before the Pentest activity. Upon reviewing the alert, it is observed that **nmap** has a file hash of **3361bf0051cc657ba90b46be53fe5b36**.

The device action is marked **allowed**, indicating that the file was successfully executed on the host machine.

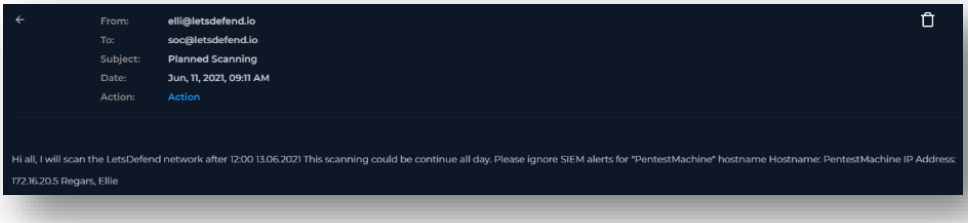
Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

As, nmap is a common program run by Pentester's, we should first check if there have been any emails sent notifying of future nmap usage, regarding the activity seen in the alert.



An email was found to be sent from **elli@letsdefend.io** to **soc@letsdefend.io** at Jun, 11, 2021, 09:11 AM, two days prior to the alert.

Analysis

To ensure our analysis is correct, the next step is to analyse the results of the **VirusTotal** file hash analysis.

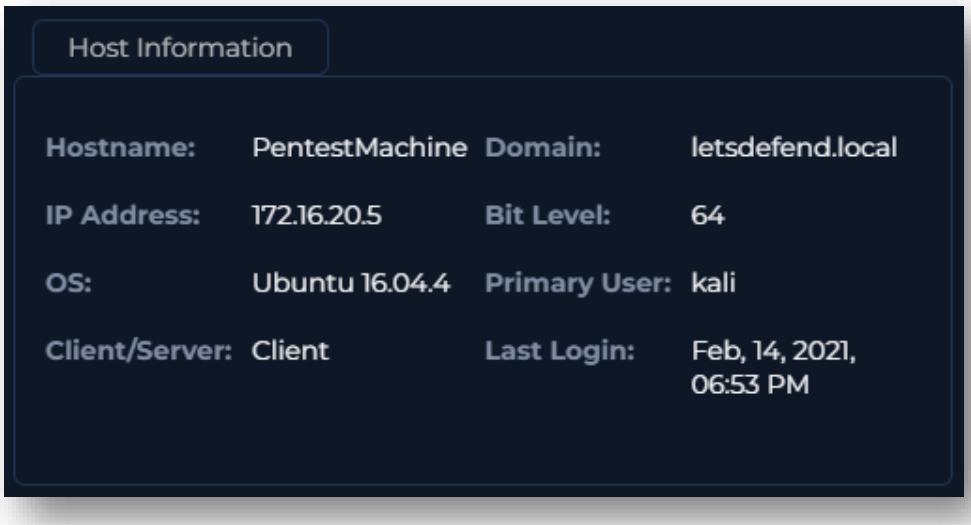
https://www.virustotal.com/gui/file/17e6235f28332367d640dd8d91359f826b1eaae888b2060e9868f1ba58ac4f67

No security vendors flagged this file as malicious

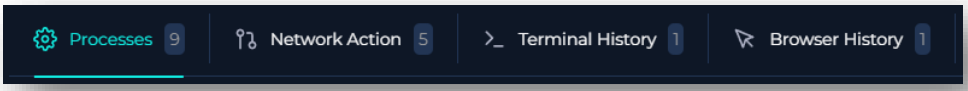
It was found that this hash is legitimate, and **not** a different program impersonating nmap.

The next step is to investigate Endpoint Security, which can provide valuable insights into the commands executed by the user and help us understand the scope and intent of the suspicious activity.

We determined some host information from here, such as Hostname, IP Address, OS, Client/Server, Domain, Bit Level, Primary User, and Last Login.



We can also investigate Processes, Network Action, Terminal History, and Browser History.



The internal system that triggered this alert is an Ubuntu 16.04.4 OS running Kali Linux, called **PentestMachine**. This machine's purpose is to run Pentests on the **letsdefend.local** domain, hence could the reason for nmap being run.

Command Line: nmap -sV -sP 172.16.20.0/24 [13.06.2021 - 16:23]

The user has run the above nmap command at the time of the alert.

- -sV: Service Version Detection – probes open ports, determines what services are running, and what version that service is running
- -sP: Ping Scan – pings host on the network, not scanning ports to determine which hosts are up
- 172.16.20.0/24 - determines the subnet to scan

This user activity is indicative of a simple Pentest, **probing for active hosts** and **enumerating the versions of services running** on those hosts.

We should also investigate the logs to determine the full scope of the activity. After analyzing the logs, it seems that the **PentestMachin**e scanned devices 172.16.20.{1, 2, 3, 4, 6} via nmap.

Containment

Based on the information gathered during the investigation, it is highly unlikely that the system has been compromised. There is no need to isolate the system from the network.

Summary

The incident involves a non-compromised system named **PentestMachine** with an IP address of **172.16.20.5**. The alert was triggered by the detection of SSH activity via the **nmap** program, based on the rule SOC147 - SSH Scan Activity.

Upon further analysis, it was discovered that **nmap** was used legitimately, as part of a planned Pentest. This is evidenced by an email sent from **elli** to the letsdefend **soc** team, notifying of Pentesting activity two days prior to the alert.

The analysis of **PentestMachine's** Endpoint Security and Log Management revealed no suspicious activity regarding this alert, only planned host and service enumeration.

Based on the findings of the incident, no immediate action needs to be taken to isolate the compromised system, and the event was identified as a **False Positive**.

Lessons Learned

- Email notice is not sufficient. Authorized activity must be documented and visible across SOC tools and processes
- Without integration between Pentest activities and SIEM logic, false positives are inevitable
- Detection logic needs refinement to reduce noise and allow for authorized testing patterns

Remediation Actions

- Implement a formal Pentest notification process that uses tickets, not emails
- Whitelist the Pentester's IP ranges for the duration of the engagement
- Improve detection logic for SSH Scan Activity

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Reconnaissance	T1595.002 - Active Scanning: Vulnerability Scanning
Reconnaissance	T1592 - Gather Victim Host Information

Artifacts

Value	Comment	Type
elli@letsdefend.io	Notification email to SOC team	E-mail Sender
letsdefend.io	Internal	E-mail Domain
172.16.20.5	PentestMachine	IP Address
3361bf0051cc657ba90b46be53fe5b36	nmap	MD5 Hash

LetsDefend Playbook

LetsDefend Event ID: 94