White Paper

MAC Address Monitoring and Reporting – A log management approach

Abstract

The Dynamic Host Configuration Protocol (DHCP) is a widely used IP address allocation scheme used worldwide. DHCP can use the computer's Media Access Control (MAC) address to determine what IP address to issue that computer. Thus it is very important for the Network Administrators to know what MAC addresses exist and need to be alerted if any foreign MAC address intrudes their environment. In this whitepaper an approach to solving this problem using Splunk will be demonstrated to achieve this objective.

Table of Contents

Author's Disclaimer and Copyright:

This publication contains proprietary and confidential information of expit and is not to be copied in whole or part.

Information furnished is believed to be accurate and reliable. However, expit assumes no responsibility for the consequences of use of such information or for any infringement of patents or other rights of third parties which may result from its use. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied.

Trademarks used in this text: expit logo, expit are registered trademarks of expit.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. expit, disclaims any proprietary interest in trademarks and trade names other than its own.

Introduction

Splunk is an IT search, monitoring and reporting tool for IT system administrators. It crawls logs, metrics, and other data from applications, servers and network devices and indexes them in a searchable repository from which it can generate graphs, reports, and alerts. It is intended to assist system administrators in the identification of patterns and the diagnosis of problems. Log files can be correlated across systems and software components which can help administrators uncover the cause analysis of system failures. The paper assumes the reader has prior experience with using and administrating Splunk.

Situation

A Network Administrator is using DHCP to assign IP addresses across his environment. The IP address decides the privileges a user gains in the environment. Since MAC address can be used to determine which IP address a user gets only in static allocation mode, it becomes critical in certain cases to keep track of MAC addresses in the environment if dynamic allocation is elected. To track authorized and unauthorized MAC address activity within the environment, an administrator will typically require either expensive Network Access Control (NAC) solutions, or monitor MAC addresses manually, in this white paper, we offer an alternative to both approaches based on Log Management and reporting.

Solution

Splunk as an IT search and reporting engine could be customized to solve the Foreign MAC address and MAC address Spoofing simultaneously. The approach presented here is based on white list tagging for MAC addresses captured via SNMP traps.

Configuration the Network Devices

A Cisco switch is used to demonstrate this concept; but it could be replicated to any network device capable of sending Simple Network Management (SNMP) traps.

We have to enable MAC address notifications in the switch we would like to monitor. MAC address notification enables you to track users on a network by storing the MAC address activity on the switch. Whenever the switch adds or removes a MAC address, an SNMP notification can be generated and sent to the Splunk server.

Example:

```
Switch(config)# snmp-server host SPLUNK_SERVER traps private
Switch(config)# snmp-server enable traps mac-notification
Switch(config)# mac address-table notification
Switch(config)# mac address-table notification interval 60
```

```
Switch(config)# mac address-table notification history-size 100
Switch(config)# interface fastethernet0/4
Switch(config-if)# snmp trap mac-notification added|removed[i]
```

This will send the SNMP traps to the Splunk Sever whenever a MAC address is added or removed from the Switch.

Configuring Splunk to receive SNMP traps

Splunk Indexer inherently cannot receive SNMP traps thus depending on the base OS we will have to do the following

- *Nix OS
  Configure snmptrapd to write to a file on disk
  ```
  # touch /var/run/snmp-traps
  # snmptrapd -Lf /var/run/snmp-traps
  ```

  Configure the Splunk server to add the file as an input[ii]

- Windows
  Enable "snmptrap.exe" on the Server and use any SNMP Management server to write the Traps to a file.

  Configure the Splunk server to add the file as an input

Configuration Splunk for Reporting Anomalies.

Here are some of the samples of SNMP MAC address notification as seen in Splunk.

```
Operation: Added    Vlan: 146    MAC Addr: 0000.6c11.1111 Dot1dBasePort: 3
History Index 2, Entry Timestamp 921715, Despatch Timestamp 92171

Operation: Deleted Vlan: 146    MAC Addr: 000b.5f76.7280 Dot1dBasePort: 3
History Index 3, Entry Timestamp 942366, Despatch Timestamp 942366

Operation: Added    Vlan: 146    MAC Addr: 0000.6c11.0001 Dot1dBasePort: 3
History Index 4, Entry Timestamp 944973, Despatch Timestamp 944973

Operation: Deleted Vlan: 146    MAC Addr: 0000.6c11.0001 Dot1dBasePort: 3
History Index 5, Entry Timestamp 945174, Despatch Timestamp 945174
```

In the above example we have to extract 2 fields *Operation* and *MAC_Address*

Key value pairs for the fields

KEY	Value
Operation	Added
	Deleted
MAC_Address	
	0000.6211.0001
	0000.6c11.1111
	000b.5f76.7280
	000b.5f76.7280

With help of Splunk Interactive Field Extractor we will create 2 fields to create Key value pairs. i.e Operation and MAC_Address.

These are the Fields which will be used for tagging, searching (filtering) and reporting.

Tagging:

Tag is the feature of Splunk which enables the user to add Domain knowledge. In this example, tagging will assist us in identifying trusted MAC addresses from other, to achive this, all trusted MAC addresses must be tagged Trusted in Splunk. To perform this task, two options are available. The first option is to edit the Tags.conf if the list of trusted MAC addresses is available to the administrator. The second option is to tag through the GUI.
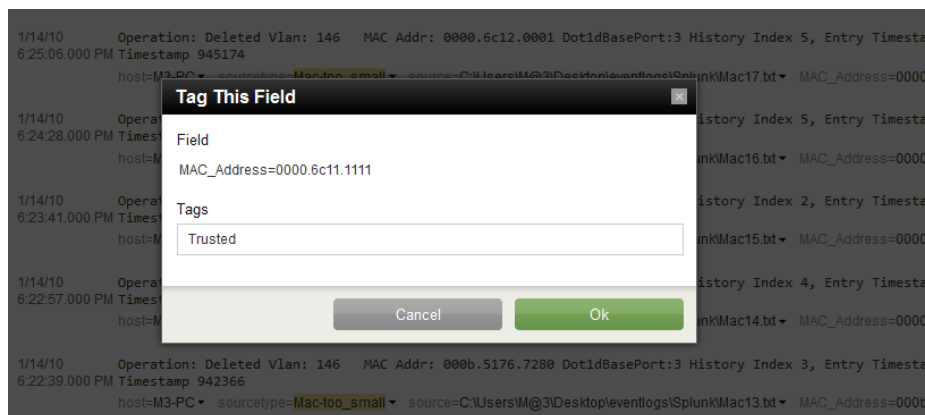
Assume traps are saved under the name sourcetype:CiscoTraps

we have to search the traps as per requirement.

Trap requirement 1: If we need to see the activity of the Trusted MAC:

Input the following into the search field: "sourcetype=CiscoTraps tag:: Trusted | stats count by MAC_address"

Following are the actual results taken from Splunk.

MAC_Address	count
0000.6211.0001	2
0000.6c11.1111	3
0000.6c11.1211	1
0000.6c12.0001	2
000b.5f76.7280	2

Trap requirement 2: If we need to see the activity of a Foreign MAC

Input the following into the search field: "sourcetype=CiscoTraps NOT tag:: Trusted | stats count by MAC_address"

This will give you the list of Foreign MAC address to take action on

MAC_Address	count
0000.6c11.0001	1
0000.6c11.0201	1
0000.6c11.11x1	1
0000.6c11.1p11	1
0000.6c31.0001	1
000b.5176.7280	1

Report:

Any search can be saved and scheduled for continual monitoring and can trigger alerts via email or RSS. You can even kick-off a script to take remedial actions or generate a ticket at a service desk. Alerts can be triggered based on a variety of threshold, trend-based conditions and even more complex searches.

Conclusion

Splunk an IT data search engine tool was customized to receive MAC address change notifications through SNMP traps. The Splunk based solution was customized by adding the domain specific knowledge to create alerts for foreign MAC_Address intrusions in the environment.

About the Author

Mohmed Dalwai is a Senior IT Consultant working with Expit Kuwait ,he currently is responsible for the Compliance Management program at expit. His responsibilities include advising and designing log management solutions, IT Auditing, and IT Business intelligence.

References

[i] www.cisco.com
[ii] www.splunk.com