Description

This script file is for method to identify all TCP IP session IPs on the system from netstat session and by using a fast method call each IP via http request and if the response content of page is consist of pre-specified blacklist text such as “Ubuntu, centOS, apache, …”, block that IP from CSF firewall and then send the email about the status.

Solution

- ## Specify the black-list text

```
search_Texts=(
    apache
    apache2
    centos
    ubuntu
    )
```

- ## Identify the TCP sessioned IPs by netstat cmd.

We can get TCP sessioned IPs by the following command:

```
netstat -atun | awk '{print $5}' | cut -d: -f1 | sed -e '/^$/d' |sort | uniq -c | sort -n | awk '{print $2}'
```

From this cmd we can get sessioned IPs but there may be invalid IPs such as “address”, “and” or “0.0.0.0”, so filter this IP array using user-defined Validation fuction.

```
validate_ip $IP
```

- ## Get the content of response pages and check black-list text in them.

We can get the content of the IP’s response page by using the following command:

```
wget http://$valid_IP --timeout=3 --output-document=./html/$valid_IP.html --tries=1 --inet4-only
```

Here, timeout=3 is time to try to get response from IP and tries=1 is how many time try to reconnect when unable to connect.

This response data is save in /html folder by output-document=./html/$valid_IP.html.

For example, 192.168.1.1.html

Next, we can check easily if there is any pre-specified blacklist text by using the following command:

```
grep $search_Text ./html/$html_file
```

- ## If there is any black-list text, drop that IP.

Defined CSF_Drop_IP function.

In this function, first check if the IP is already denied. If then, ignore.

We can do this by investigating the /etc/csf/csf.deny file.

And then, deny the IP by using the following command:

```
Csf –d $IP
```

- ## Send email notification to administrator.

Email is sent by mutt command.

```
echo "$body" | mutt -s "$subject" -e "my_hdr From:$from" -- $to
```

We can install mutt by the following command:

```
Sudo apt-get install mutt
```

Also, To use this service please check the following URL:

https://linuxmeditation.com/how-to-setup-and-configure-ssmtp/