REPORT

Finding Sensitive HTTP traffic

About the Auth.pcap file

This file cannot be opened or accessed by any software like **Ms word** or other document-opening softwares so I had to use **Wireshark**. I was able to upload the file on wireshark which displays the *auth.pcap* contents. Auth.pcap has 7 columns(No , time , source , desination , protocol , length and info) and 12,957 rows.

Process

Since , the challenge is to find the sensible http traffic so I start to check for all http requests so I can find the sensitive one, it was quite difficult and time-consuming to find it among the thousands of requests , so I wasn't able to find the sensitive one at first, posing a great challenge and I was really bothered.

In my struggles , I realized I could check for the sensitive http request by using a wireshark display fliter : ***http.autobasic*** which I did , and that was my eureka! Moment

N.B : ***<u>http.autobasic</u>*** *is used to find http request that contain* ***basic authentication data****, which serves as a great lead to find the username and password we are looking for.*

Findings

As I entered the display filter , a http request packet was returned ,with the SourceIP address to be ***192.168.0.13*** and Destination IP to be 192.168.0.14. I proceed to inspect the packet , expanded the hypertext protocol and I found the **Authorization basic header base64 encoded credentials** (YmFzaE5pbmphOmZsYWd7aGVscC1tZS1vYml3YW59) , I figured out the details I seek lies in the encoded credentials which I decoded with the help of an online tool(named **Base64 decode**) , I was able to decode the encoded credentials to be ***'BashNinja :flag{help-me-obiwan}'*** .

Which means the username is **b**_**ashNinja**_ and Password is ***'flag{help-me-obiwan}'***

Eureka!

Results

Based on my Findings:

Source IP (Attacker's Machine): *192.168.0.13*
Destination IP (Attacked Service): *192.168.0.14*
Username: *bashNinja*
Password: *flag{help-me-obiwan}*

<u>Conclusion</u>

Using Unencrypted HTTP traffic can be dangerous, as credentials can be easily captured.