Penetration Test Report

Pulkit Sanadhya

November 18, 2019

Contents

Executive Summary

Background

The goal of this exercise is to identify a possible target for sslstrip.

Recommendation Summary

The kali attack box will be used for this purpose .

Technical Report

Exploitation

Here , initially we went to the innerouter(172.30.0.3) and forwarded the port 22 on it to the host 10.30.0.32 by configuring the NAT rules.

Now , we used the following command on the kali host to do ssh to 10.30.0.32:

```
ssh m.mason@172.30.0.3
```

And, we got access to the m.mason account on the machine 10.30.0.32 by providing the password that we got in mykeys.txt file.

Now , we typed the following command cat /etc/sudoers and we found that m.mason account was able to run the ps command only , so copied the file from /bin/bash to /bin/ps and got the access to root by executing the command sudo ps.

Now , we used the command scp /usr/sbin/tcpdump m.mason@172.30.0.3:/usr/sbin , and copied tcpdump from to the target machine and we were able to use tcpdump in devbox.

now after using the following command :

```
tcpdump -i ens33 dst port 80 or dst port 443 -X
```

We were able to see that herd.m3g4c0rp.com was constantly trying to connect to ns.m3g4c0rp.com on both port 80 and 443. So we can say it can be a potential candidate for sslstrip as it has a http landing page and goes to https for login.

Now, we copied the sslstrip directory from kali host to devbox by using the SCP command.

Now , here we enable ip forwarding by using the following command :

```
echo 1 ¿ /proc/sys/net/ipv4/ip$_{forward}$ :
```

Now , we directed the http traffic to sslstrip by using the following command:

```
iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT
–to-port 5555
```

Now using the following command to ssl strip :

```
python sslstrip.py -l 5555 -W output.log ;
```

and using the following command to arpspoof:

```
arpspoof -i ens33 -t 10.30.0.98 172.30.0.128
```

Now , we ran used tcpdump to capture the packets instead of ettercap by using the following command :

```
tcpdump -i ens33 -t 10.30.0.98 10.30.0.1
```

Now opening the file output.log we were able to find the KEY 17 :

KEY 17 : WaGco/h+g7lEQAk0Ey1Clg==

Now , in the http header we found the basic authorization credentials which uses base 64 encoding , so now after using the following command:

```
echo ’string’ — base64 –decode
```

We were able to decode the string and found the key16 as a result:

KEY16:v6lF0fAFjWbqkW0GrzdjuQ==

Here , the client was identified as 10.30.0.98 and the server was identified to be 172.30.0.128.

Here, the landing page at 172.30.0.128 was http so we got to know that sslstrip is possible in such case.

By using this we were able to capture credentials such as key 17 and key 16 .

This places www.m3g4c0rp.com in a situation where it is vulnerable to MITM attacks and the sensitive information can be captured to gain unauthorized access to its network.

Conclusion

We were able to successfully able to use sslstrip to capture the KEY 17 and KEY 16 .