Biomedical Honeypot Device

Introduction

Task: Our team worked with INOVA to create a biomedical honeypot to collect data for information security analysis.

Goal: To attract threat actors so we can understand their tactics, techniques and procedures used when attacking the device.

What is a Honeypot?

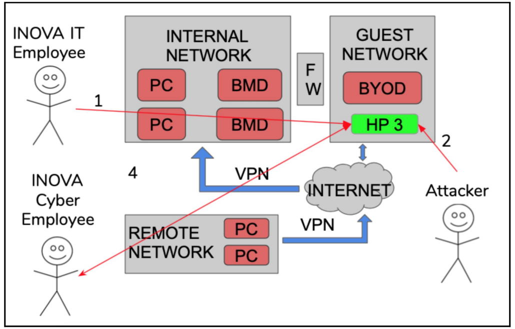
Honeypots are designed to resemble valid systems or devices, and appear to be a legitimate part of the network they are in; they are used to collect information about their attackers.

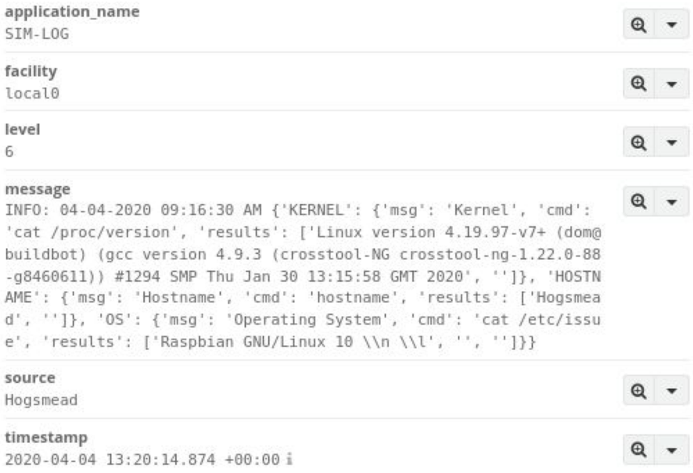
Our Implementation:

We created a two machine system. One was a logging server and one was a simulator. We rerouted all logs and commands from the simulator to the logging server.

The Code:

We used python to create a simulation script. We also got a basic Linux Enumeration script in python to run on our system to simulate an attacker.





```
application_name
SIM-LOG

facility
local0

level
6

message
INFO: 04-04-2020 09:16:30 AM {'KERNEL': {'msg': 'Kernel', 'cmd':
'cat /proc/version', 'results': ['Linux version 4.19.97-v7+ (dom@
buildbot) (gcc version 4.9.3 (crosstool-NG crosstool-ng-1.22.0-88
-g8460611)) #1294 SMP Thu Jan 30 13:15:58 GMT 2020', '']}, 'HOSTN
AME': {'msg': 'Hostname', 'cmd': 'hostname', 'results': ['Hogsmea
d', '']}, 'OS': {'msg': 'Operating System', 'cmd': 'cat /etc/issu
e', 'results': ['Raspbian GNU/Linux 10 \\n \\l', '', '']}}

source
Hogsmead

timestamp
2020-04-04 13:20:14.874 +00:00
```

Methods and Results

Our system was tested with an "attacker" script that is a open-source enumeration script. It aims to connect with our system and query for more information. When this script is run, it triggers our logging server and alerts are sent to a designated party.

By running our script and comparing its actions with recordings on our logging server, we verified the accuracy of the model.

Conclusions and Future Work

An attacker, when trying to compromise a seemingly vulnerable device, will try a wide variety of tactics including: testing default passwords, accessing open ports, scanning for vulnerable sensitive data, and much more.

By constantly monitoring and securing a device, when an attacker performs these actions, increasing the security and response time of the device will become increasingly easier and more efficient, as well as predicting and preparing for future attacks.

How can an organization use this product?

Our model is flexible enough to be applied to a wide variety of products and situations. By taking our model and adding device specific information, an organization will have an easy, ready-to-go reusable honeypot and logging server that will help them understand what threats they are facing and increase their overall security posture.

Acknowledgements

We would like to thank our advisor Thomas Winson, our professor Peggy Brouse, and our INOVA Subject Matter Expert Matthew Wilkes.

References

https://github.com/sleventyeleven/linuxprivchecker/blob/master/linuxprivchecker.py