**NORTH METRO TAFE**

**ADV DIP CYBER SECURITY**

**Honeypot Project**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_PLAYBOOK\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |
| --- | --- | --- |
| **Prepared by** | **Date** | **Signature** |
| **Jake Silvestro** | **05/11/2020** | **J.Silvestro** |
| **Approved by** | **Date** | **Signature** |
| **Stephen Oakley** | **30/11/2020** | **S.Oakley** |

**Document Control**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Configuration** | | | | |
| **Version** | **Date** | **Author** | **Summary of Changes** | **Status** |
| 1.0 | 05/11/2020 | Jake Silvestro | Initial Draft | Draft |
| 1.1 | 30/11/2020 | Ben Armstrong | Added instructions for managing honeypots | Completed |
| 1.2 | 30/11/2020 | Matt Dockrell | Added instructions for creating Splunk Dashboards | Completed |
| 1.3 | 30/11/2020 | Declan Miranda | Added instructions for malware analysis on cuckoo sandbox | Completed |
| 1.4 |  |  |  |  |
| 1.5 |  |  |  |  |

Contents

[Background 4](#_Toc57657504)

[Scope 4](#_Toc57657505)

[Managing Honeypots 4](#_Toc57657506)

[Creating and Monitoring Splunk Dashboards 5](#_Toc57657507)

[Cuckoo Sandbox Malware Analysis 5](#_Toc57657508)

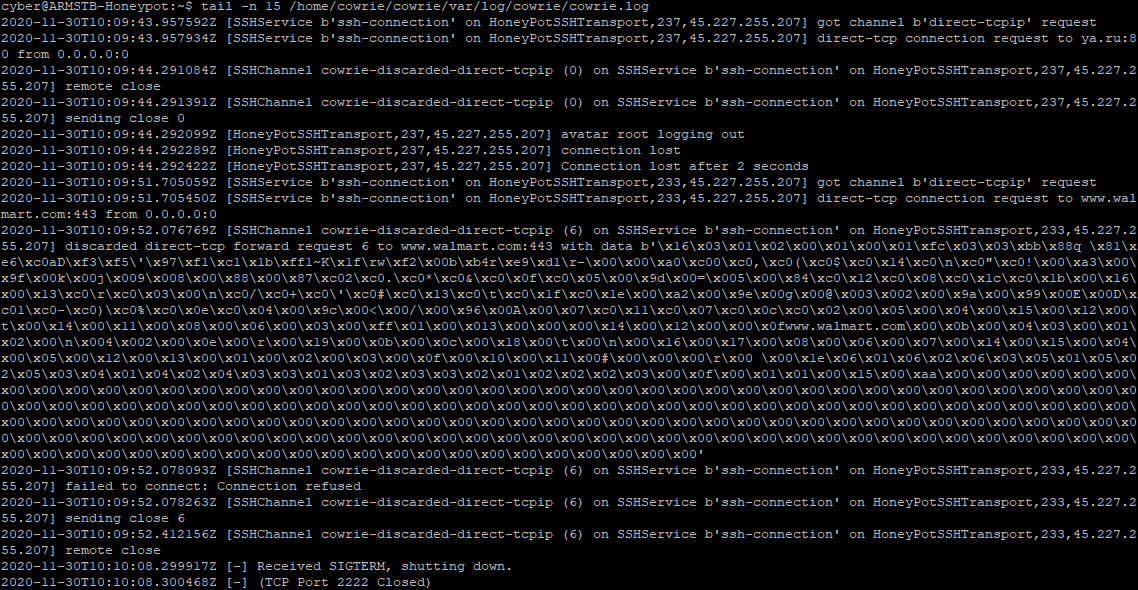
### Background

The Honeypot project is a class project in which a Honeypot is set up to acquire insight into how attackers initially try to get a foothold in the system. This includes top usernames and passwords entered, what commands are run and what domains are being reached from the honeypot. This information will be ingested into Splunk and monitored in a Splunk Dashboard. A Cuckoo Sandbox will be run for malware analysis to get information on malware that has been installed on the honeypot from attackers.

### Scope

Setting up the Honeypot in VMWare Workstation 16.  
Managing Honeypots.  
Tying the system together.  
Ingest data into Splunk.  
Create Splunk Dashboards for monitoring.  
Utilizing Cuckoo Sandbox for malware analysis.

### Managing Honeypots

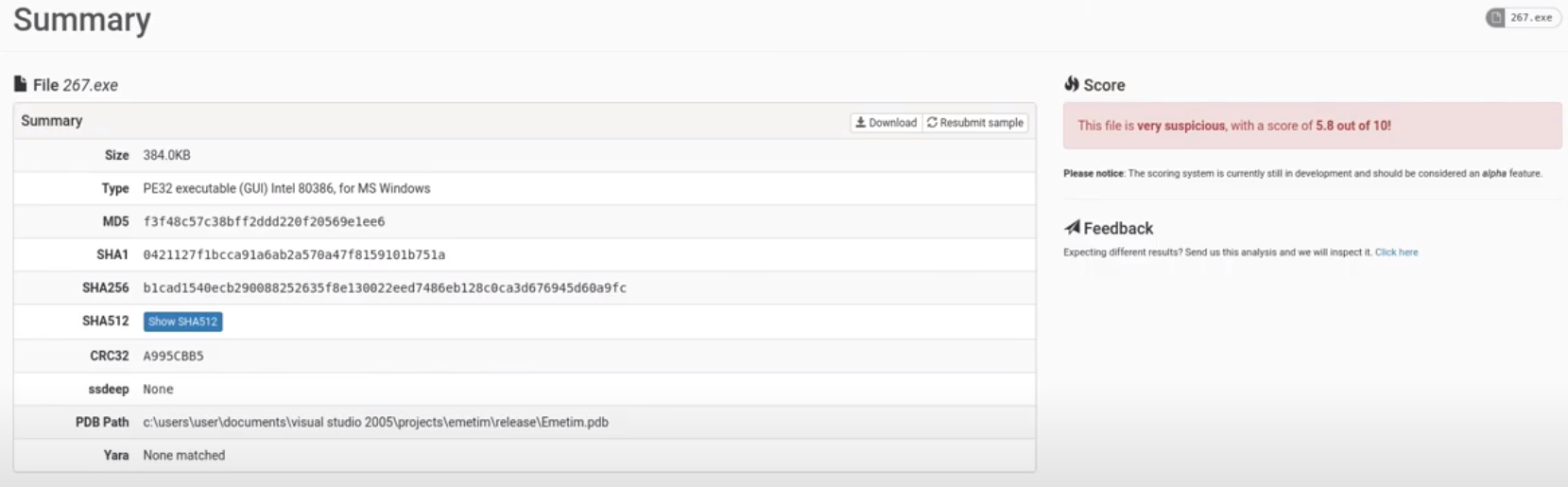
1. Ensure the honeypot is running by checking in VMWare Workstation and making sure the honeypot machine is turned on.
2. SSH to the honeypot using PuTTy at 49.255.84.54 and using the private SSH key and the credentials cyber:Pa55w.rd on port 2020 login.
3. Run the following command ‘sudo systemctl status cowrie’ and ensure that the status is **RUNNING**.  
   
4. Run the following command
   1. tail -n 15 /home/cowrie/cowrie/var/log/cowrie/cowrie.log  
      This will output the last 15 lines of the log file to analyse.  
      

### Creating and Monitoring Splunk Dashboards

1. Login to oracle at <https://oracle:8000/> using TDM credentials
2. In the Splunk home page, click on ‘Search and Reporting’ then ‘Dashboards’
3. Click on the ‘Ryan/Matt’ Dashboard, this is the project dashboard.
4. Click ‘Edit’ in the top right.
5. Click on ‘Add Panel’ in the top left.
6. Choose what panel is needed eg, bar charts, pie charts, events etc.
7. Set time picker to time desired.
8. Enter a title relevant to the specific dashboard.
9. Enter search string that is going to display the output in the dashboard.
10. Click ‘Add to Dashboard’

For monitoring of Dashboards, follow up to step 3.

### Cuckoo Sandbox Malware Analysis

1. Login to cuckoo through Mozilla Firefox at 100.100.128.140:8080 and login using cuckoo:cuckoo
2. In the top right corner, click on submit to submit a file.
3. Once the automated malware analysis has finished, cuckoo will show a summary  
   
4. Be mindful of the score that cuckoo has given the file.
5. Check the malware hashes in [www.virustotal.com](http://www.virustotal.com)
6. Sift through the summary to find all different artifacts from the file (Domains, IPs, Hashes, Behaviour, Service Names etc)