**ISEC 3700 Information Security Practices**

Honey Pot Project

**Demonstrated Skills:**

* *Server configuration planning*
* *File auditing*
* *Network monitoring software installation and configuration*
* *Server change management logging*
* *Network analysis and evidence of intercepted intrusion attempts*
* *Network security recommendations*
* *Penetration testing using Kali Linux*

**ISEC3700 Honey Pot**

**Jeff Guitard, Joseph Guatto, Avelino Cardoso, Zack Stiles**

**November 25th, 2022**

[1. Team Information 3](#_Toc130997860)

[2. Planning Document 4](#_Toc130997861)

[3. Auditing Setup and Configurations 6](#_Toc130997862)

[4. Software Setup and Configurations 10](#_Toc130997863)

[5. Install and Change Management 23](#_Toc130997864)

[6. Blue Team 24](#_Toc130997865)

[Team Monitoring Schedule 24](#_Toc130997866)

[Intercepted Intrusion Attempts Table 25](#_Toc130997867)

[Intercepted Intrusion Attempts Table Supporting information 27](#_Toc130997868)

[Security Recommendations 32](#_Toc130997869)

[7. Red Team 33](#_Toc130997870)

[Intrusions Methods and Attempts 33](#_Toc130997871)

[Security Recommendations 41](#_Toc130997872)

# Team Information

**Authors**

|  |  |
| --- | --- |
| Name: Zachary Stiles  Member ID: W0451027  Department or Title: Researcher | Name: Jeff Guitard  Member ID W0465443  Department or Title: Alternate Team Lead |
| Name: Joseph Guatto  Member ID: W0255815  Department or Title: Team Lead | Name: Avelino Cardoso  Member ID: W0452640  Department or Title: Researcher |

# Planning Document

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activity List/Plan** | | | | | |
| **Project: ISEC – Honey Pot Final Project** | | | | | **Date: 28 November 2022** |
| **Activity ID No.** | **Activity Name** | **Description of Work** | | | **Responsibility** |
| A001 | Documentation required for install and configuration. | Naming Convention Document on Brightspace | | | POD 3 |
| A002 | Resources required for install. | .exe for software to install   * Event Sentry * Adobe Reader * Microsoft Network Monitor | | | POD 3 |
| A003 | Documentation of object names required for implementation. | **Specify object names in preparation for implementation** | | | POD 3 |
| OS | Windows Server 2019 Datacenter | |
| **System** Hardware Configuration: | Primary HD | 150GB |
| Additional HDs | N/A |
| RAM | 16GB |
| Processors/Cores | 1 / 4 |
| Network | IP Address (DHCP) | 172.16.136.71 |
| Subnet Mask | 255.255.255.0 |
| G/W Address | 172.16.136.250 |
| DNS Server Addresses (2) | 172.16.136.3  172.16.136.2 |
| Installation Mode | Existing Install/Additional Configuration | |
| Time Zone: | Atlantic Time (Canada) | |
| Server Type | Webserver | |
| **Server** “Administrator” Password: | )y5V9R( | |
| **Server** Host Name: | LONGHORNED | |
| Domain Name: | WORKSTATION | |
|  | | |
| *Name and description of each snapshot to be taken during install.*  *Create a schedule of regular rollback points of the server and take regular snapshots of your server in shutdown state.* |  | |
| A004 | Required configurations or settings applied | Change Admin Password   * Password does not expire   Create new user   * Name: Charlotte Bruce * Password: Passw0rd * Member of power users group * Password does not expire   Perform all windows updates  Create IIS Web site that includes a Group Company Name, graphic and email link to the Web Administrator  Create a password protected .zip file using the administrator password on the administrator’s desktop  Create a PDF on how to setup auditing without a DC in the C:\Scripts folder  Create Read Only Document that contains a link to software installed in Charlotte Bruce’s “Documents” directory  Install EventSentry Lite for system monitoring.  Install Microsoft Network Monitor for network monitoring.  *\*Set up auditing on all red items above.* | | | POD 3 |
| A005 | Additional Software required as part of planning, setup or configuration. | Event Sentry (System monitoring)  Adobe Reader  Microsoft Network Monitor (Network Monitoring) | | | POD 3 |

# Auditing Setup and Configurations

How to setup auditing without a DC

Open **File Explorer**, then find the file or folder for auditing.

Graphical user interface, text, application

Description automatically generated

Right click the file or folder, select **Properties,** and then click **Security**

Click **Advanced**, and then click **Auditing**

Graphical user interface, text, application, email

Description automatically generated

Click **Add** to set up auditing for a new user or group, then click **Select a principal**

Graphical user interface, text, application, email

Description automatically generated

In the **Name box**, select a user from the list and then click **OK** to open the **Auditing Entry** box.

Graphical user interface, text, application, email

Description automatically generated

In the **Auditing Entry**, click the **Type** dropdown menu and select **Success**, **Fail**, or **All** tochoose events to be audited. Select an option from the **Applies to** drop down boxand select an option. Select **Basic Permissions**, then check the **Only apply these auditing settings to objects and/or containers within this container** box if required. Click **OK** to close the **Auditing Entry** box. Then click **Apply**, then **OK** to finalize the setting.

*\*To view or change existing auditing for a user or group, click the name, and then click* ***View/Edit****.*

*\*To remove auditing for a user or group, click the name, and then click* ***Remove****.*

In the GPO under Computer configuration/Windows settings/Security settings/Advanced Audit Policies/

We have made several changes Any that are Configured.

Under Account management

Graphical user interface, text, application

Description automatically generated

Under Detailed Tracking

Graphical user interface, text, application

Description automatically generated

Under Object Access

Table

Description automatically generated with medium confidence

Under Global Object Access Auditing

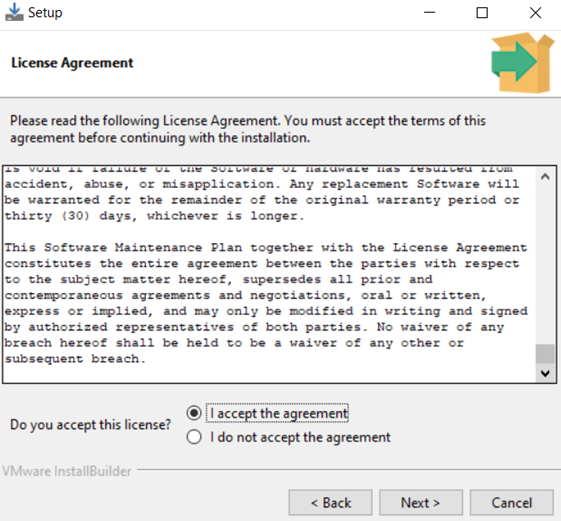
Graphical user interface, application, Word

Description automatically generated

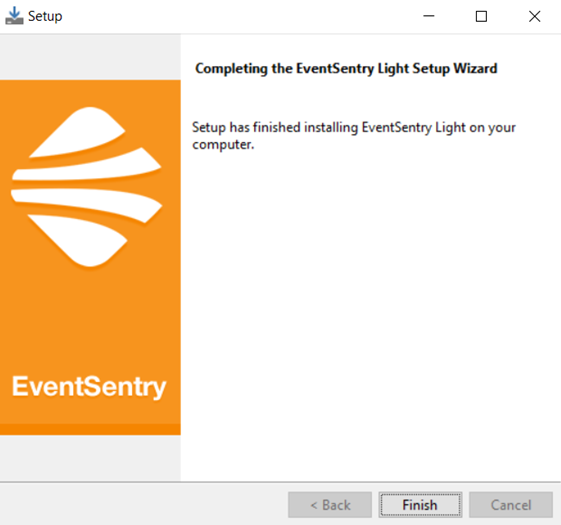
# Software Setup and Configurations

**EventSentry Setup Guide**

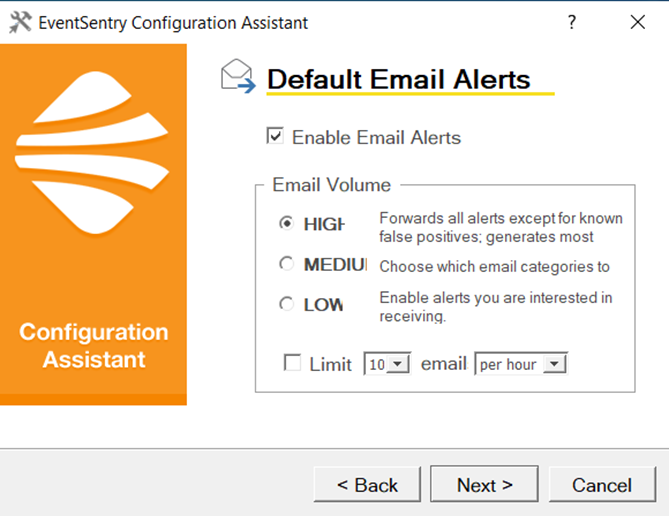
Download the EventSentry Light installer <https://www.eventsentry.com/downloads/select-edition>



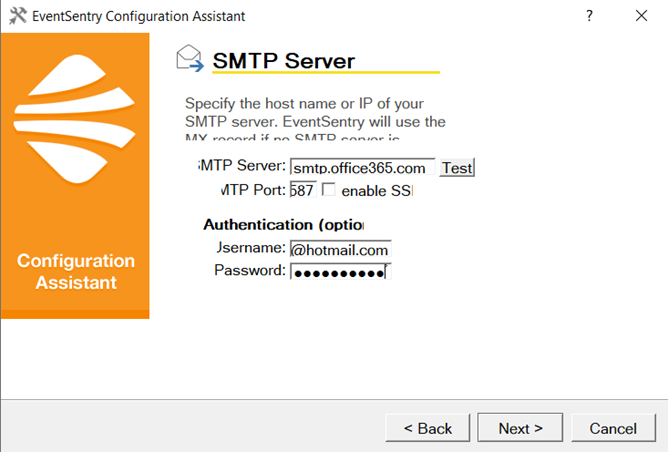
Read and accept the agreement and click Next



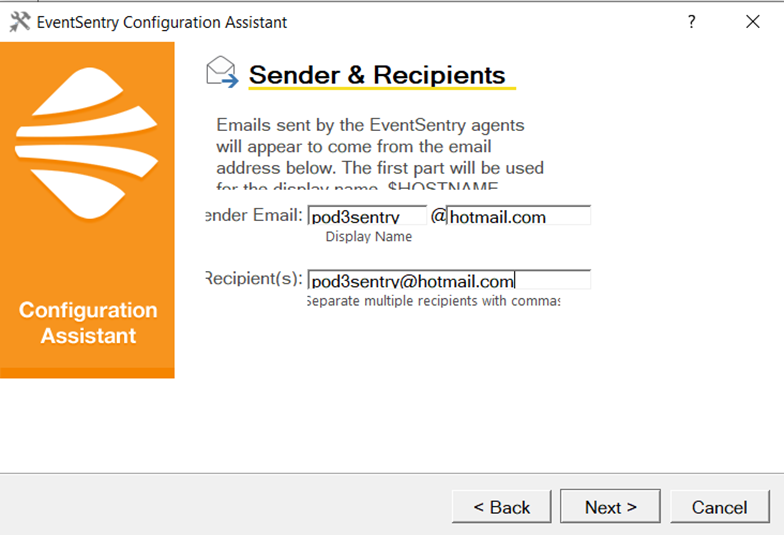
When setup is complete, click Finish



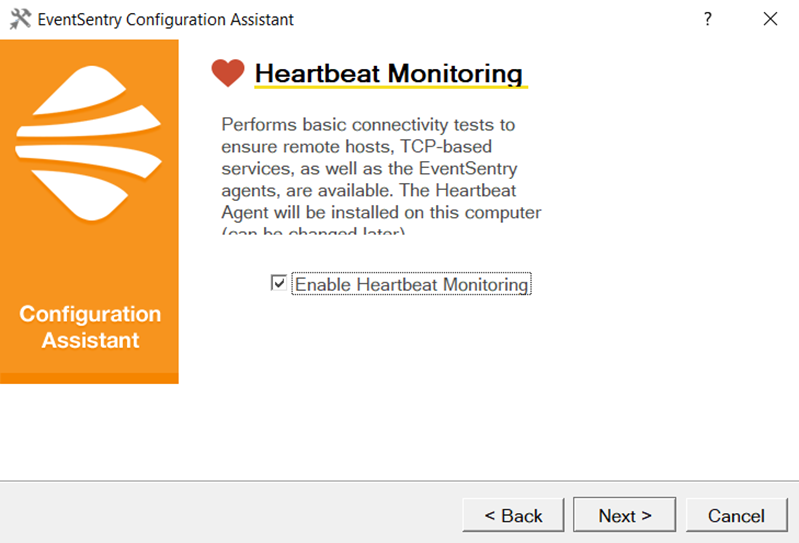
Set Email Alerts to HIGH with and uncheck Limit box.



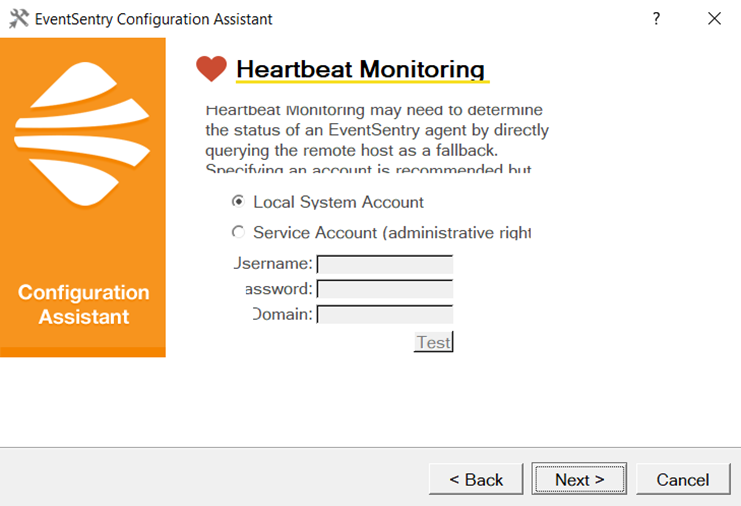
SMTP server: smtp.office365.com, Port: 587, Email: [pod3sentry@hotmail.com](mailto:pod3sentry@hotmail.com) Password: (enter password)



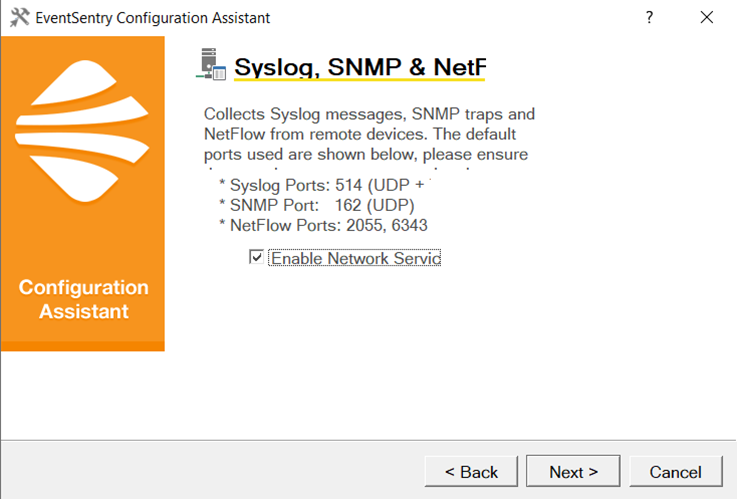
Sender email : [pod3sentry@hotmail.com](mailto:pod3sentry@hotmail.com) Recipients: [pod3sentry@hotmail.com](mailto:pod3sentry@hotmail.com)



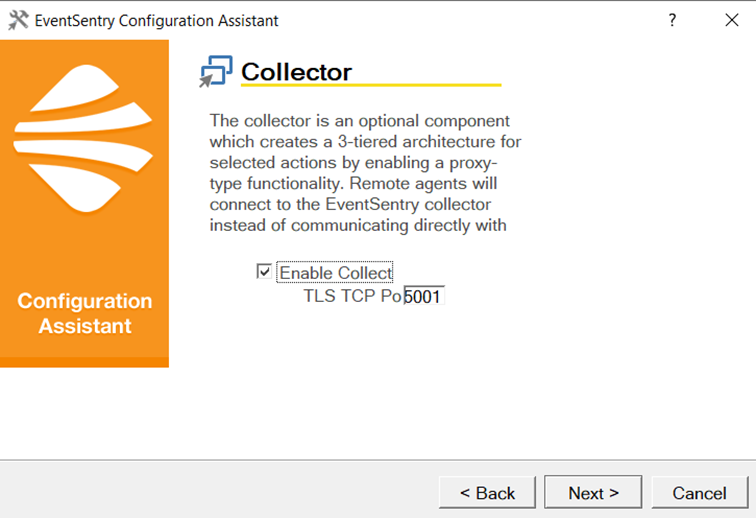
Enable heartbeat monitoring



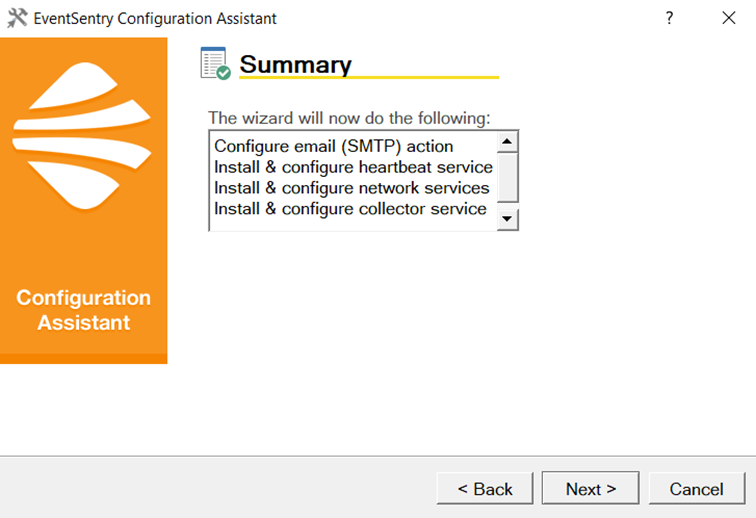
Select Local System Account



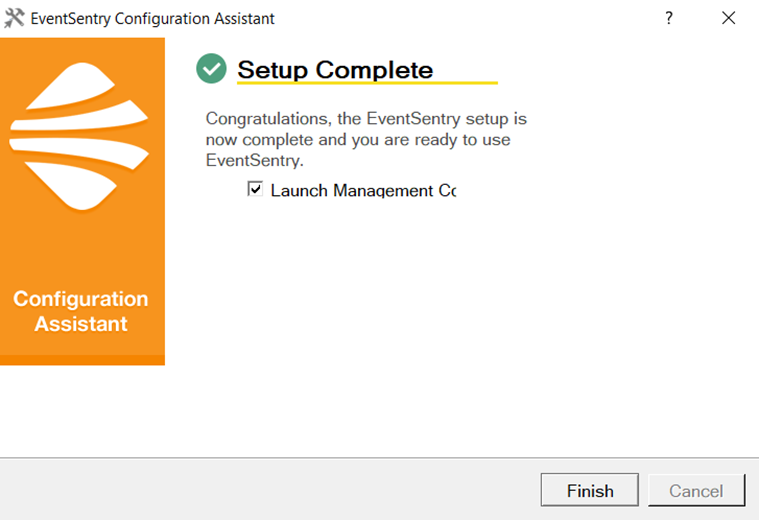
Accept default settings for Syslog, SNMP, and NETFlow



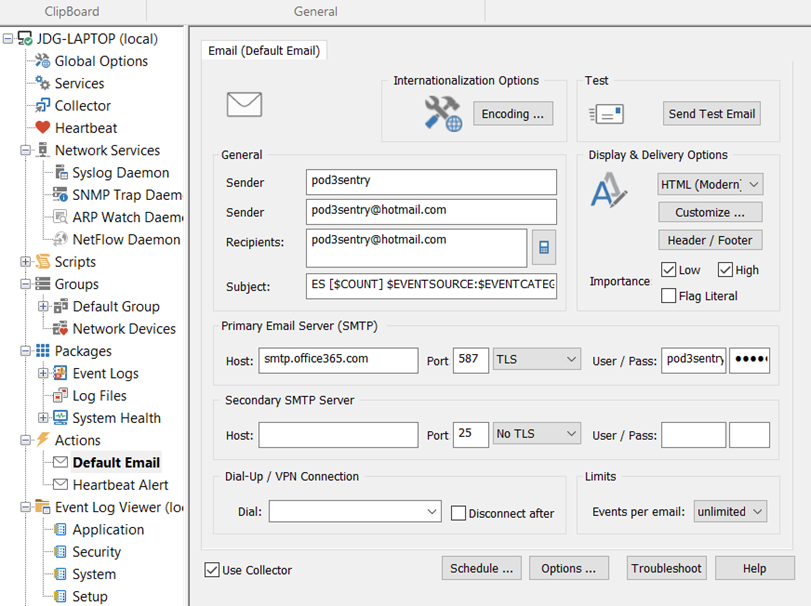
Enable Collect using default TLS TCP Port



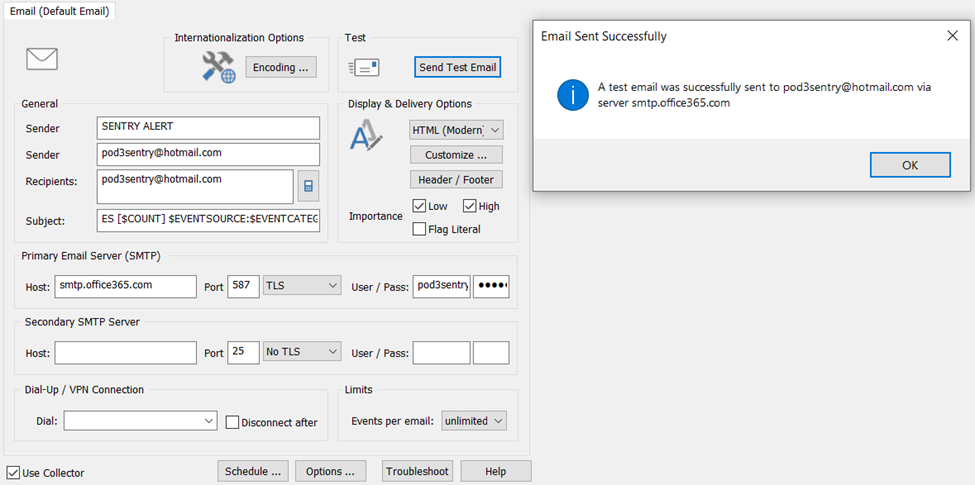
Click Next on Wizard summary screen



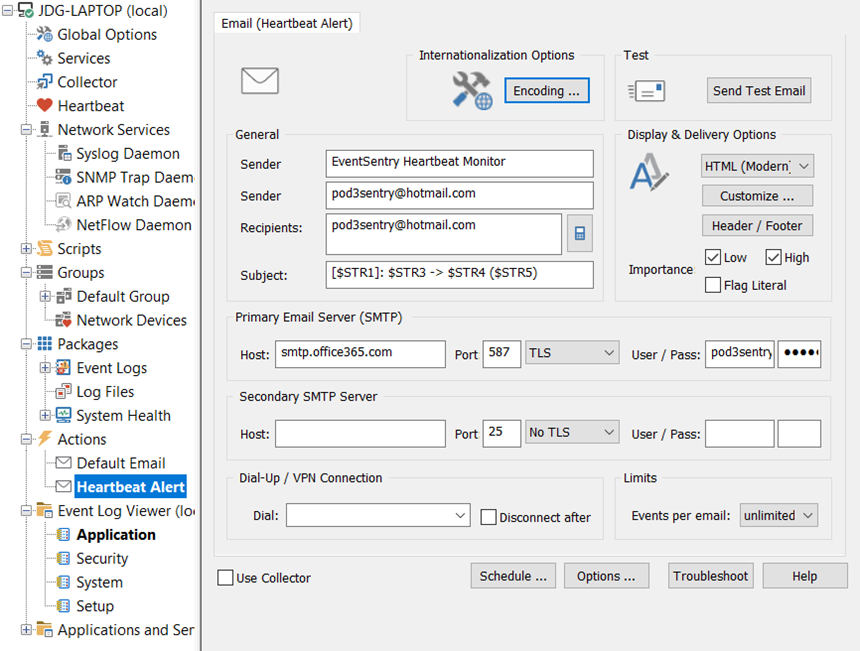
Click Finish to Launch Management Console



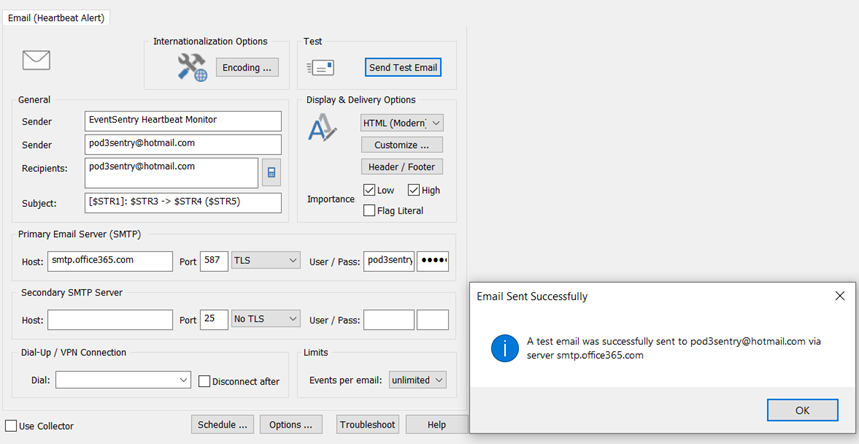
Click on Default Email on Left pane



Confirm email settings and click Send Test Email to confirm successful alert setup.



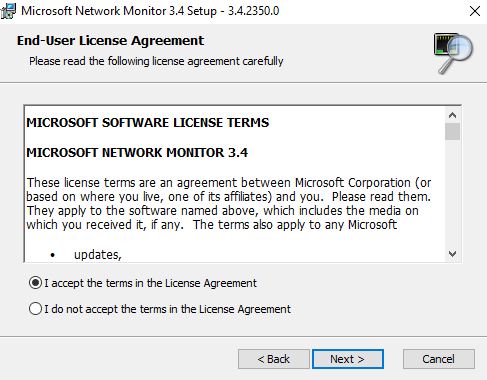
Click on Heartbeat Alert on Left pane



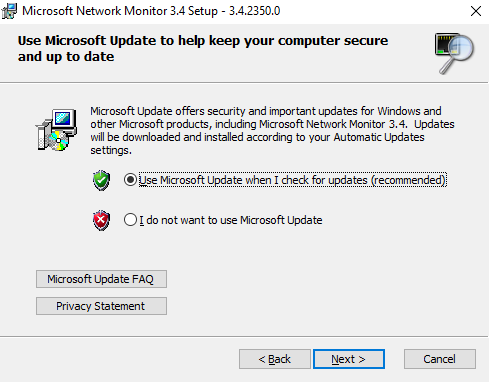
Confirm Heartbeat Monitor settings and click Send Test Email to confirm successful alert setup.

**Microsoft Network Monitor Setup Guide**

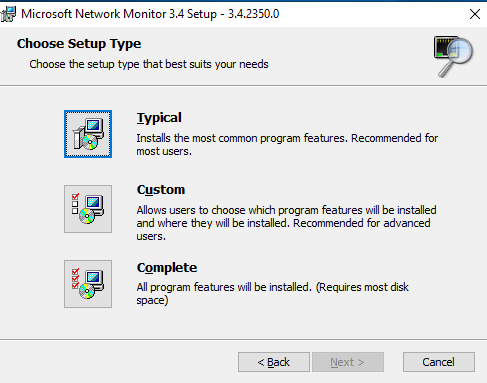
**Download Microsoft Network Monitor**

**https://www.microsoft.com/en-us/download/confirmation.aspx?id=4865**

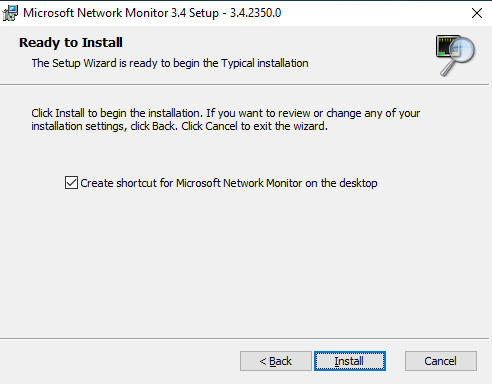
Read and accept the agreement and click Next



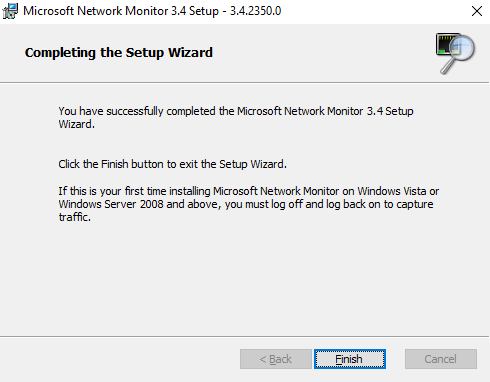
Select Use Microsoft Update when I check for updates (recommended) and click Next



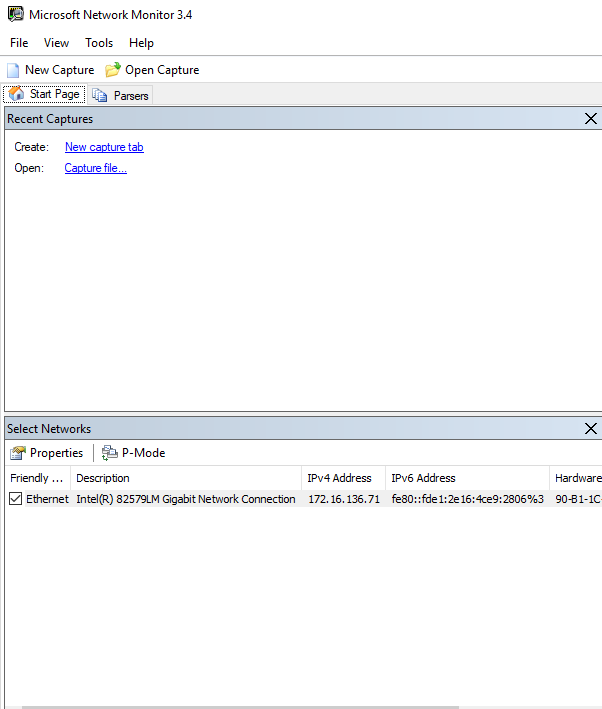
Select the Typical installation and click Next



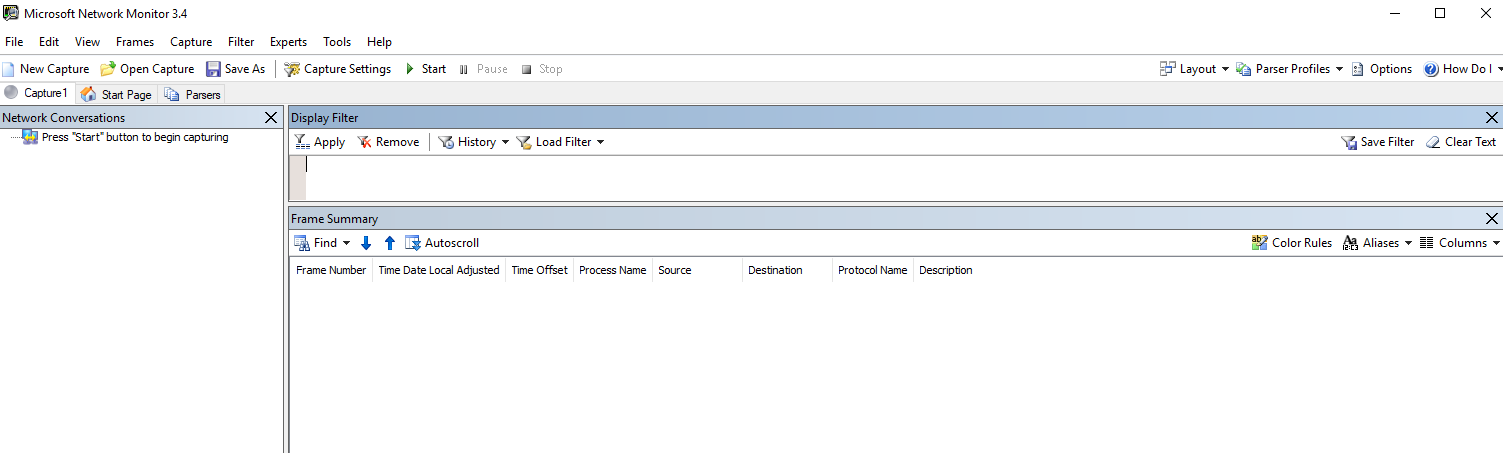
Accept the default setting and click Install



Click Finish



To start a new monitoring Capture, select the Network adapter and Create: New capture tab



Click Start to begin capture and Stop to end the capture session

# Install and Change Management



# 6. Blue Team

## Team Monitoring Schedule

**November 28th – December 4th**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Member** |  |  | **Nov. 30** | **Dec.1** | **Dec.2** | **Dec.3** | **Dec.4** |
| Jeff |  |  |  | Server Logs |  | Monitor Email |  |
| Joseph |  |  |  | Monitor Email |  |  | Monitor Email |
| Avelino |  |  | Server Logs |  | Monitor Email |  |  |
| Zack |  |  | Monitor Email |  | Server Logs |  |  |
|  |  |  |  |  |  |  |  |

**December 5th – December 11th**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Member** | **Dec.5** | **Dec.6** | **Dec.7** | **Dec.8** | **Dec.9** |  |  |
| Jeff | Server Logs |  |  | Server Logs | Server Logs |  |  |
| Joseph | Monitor Email |  |  | Monitor Email | Monitor Email |  |  |
| Avelino |  | Server Logs | Monitor Email |  |  |  |  |
| Zack |  | Monitor Email | Server Logs |  |  |  |  |

* Members are to perform monitoring during the “class hours” each day. Mon, Thurs 8:30am-3:30pm & Tues, Wed, Fri 8:30am-12:30pm.
* Major incidents are reported to the rest of the team when observed.
* Weekend email monitoring is performed on a voluntary basis.

## Intercepted Intrusion Attempts Table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Item # | Date | Time | Intruder IP | Intruder Port | Protocol | Details |
| 1 | 11/30/2022 | 10:59am | 172.16.136.228 | 443 | TCP/HTTPS | Used **nslookup** to determine this intercepted intrusion came from inwsd316 18.ad.net172.ca, Ben Whalen |
| 2 | 12/1/2022 | 10:24am | 172.16.136.228 | 443 | TCP/HTTPS | Ben continues his attempts to get onto our server |
| 3 | 12/1/2022 | 10:31am | 172.16.136.228 | 25022 | TCP | Logon attempt failed User Kali |
| 4 | 12/1/2022 | 11:00am | 172.16.136.228 | 3389 | TCP/RDP | Logon attempt failed User CBruce |
| 5 | 12/2/2022 | 2:52pm | 172.16.128.127 | 443 | TCP/HTTPS | Used nslookup but could not find hostname of computer |
| 6 | 12/3/2022 | 11:29pm | 172.16.128.121 | 443 | TCP/HTTPS | Used nslookup but could not find hostname of computer |
| 7 | 12/5/2022 | 9:57am | 172.16.136.235 | 3389 | TCP/RDP | Logon attempt failed User MDutka  Used **nslookup** to determine this intercepted intrusion came from inwsd31625.adnet172.ca, Louis Guitton’s computer. |
| 8 | 12/8/2022 | 10:08am | 172.16.136.224 | 62985 | ARP | Used **nslookup** to determine this intercepted intrusion came from inwsd31614.ad.net172.ca, Sukhman Singh’s computer. |
| 9 | 12/8/2022 | 10:54am | 172.16.136.216 | 80 | TCP/HTTP | Used **nslookup** to determine this intercepted intrusion came from inwsd31606.ad.net172.ca, Michael Rotimi’s computer. |
| 10 | 12/8/2022 | 12:34pm | 172.16.136.235 | 3389 | TCP/RDP | Used **nslookup** to determine this intercepted intrusion came from inwsd31625.ad.net172.ca, Louis Guitton’s computer. |
| 11 | 12/8/2022 | 1:24pm | 172.16.136.235 | 3389 | TCP/RDP | Used **nslookup** to determine this intercepted intrusion came from inwsd31625.ad.net172.ca, Louis Guitton’s computer. |
| 12 | 12/8/2022 | 4:51pm | 172.16.136.233 | 443 | TCP/HTTPS | Used **nslookup** to determine this intercepted intrusion came from inwsd31623.ad.net172.ca, Elizabeth Oluwakoya’ computer. |
| 13 | 12/9/2022 | 8:53am | 172.16.136.234 | 3389 | TCP/RDP | Used **nslookup** to determine this intercepted intrusion came from inwsd31624.ad.net172.ca, Skyler Carr’s computer. |
| 14 | 12/9/2022 | 9:20am | 172.16.136.234 | 3389 | TCP/RDP | Skyler Carr continuing aggressively without success. |
| 15 | 12/9/2022 | 9:27am | 172.16.136.235 | 3389 | TCP/RDP | Skyler Carr’s teammate Louis Guitton joined in on the efforts. |
| 16 | 12/9/2022 | 10:07am | 172.16.136.234 | 3389 | TCP/RDP | Skyler Carr continues his assault. |
| 17 | 12/9/2022 | 10:24am | 172.16.136.213 | 445 | TCP/SMB | Used **nslookup** to determine this intercepted intrusion came from inwsd31603.ad.net172.ca, Dylan Oakley’s computer. |
| 18 | 12/9/2022 | 11:20am | 172.16.137.198 | 443 | TCP/HTTPS | Used **nslookup** to determine this intercepted intrusion came from inwsd31605.ad.net172.ca, Jeff Smith’s computer. |
| 19 | 12/9/2022 | 12:02pm | 172.16.136.235 | 3389 | TCP/RDP | Used **nslookup** to determine this intercepted intrusion came from inwsd31625.ad.net172.ca, Louis Guitton’s computer. |
| 20 | 12/9/2022 | 12:10pm | 172.16.136.214 | 3389 | TCP/RDP | Used **nslookup** to determine this intercepted intrusion came from inwsd31604.ad.net172.ca, Alex Garcia’s computer. |

## Intercepted Intrusion Attempts Table Supporting information

Graphical user interface, application

Description automatically generated with medium confidence Text

Description automatically generated

Intercepted Intrusion item 1 Screenshot Intercepted Intrusion item 2 Screenshot

Text

Description automatically generated Text

Description automatically generated

Intercepted Intrusion item 3 Screenshot Intercepted Intrusion item 4 Screenshot

Text

Description automatically generated with low confidence Text

Description automatically generated

Intercepted Intrusion item 5 Screenshot Intercepted Intrusion item 6 Screenshot

Text

Description automatically generated

Intercepted Intrusion item 7 Screenshot





Intercepted Intrusion item 8 Screenshot





Intercepted Intrusion item 9 Screenshot

Graphical user interface, text, application, Word

Description automatically generated

Dec 8 12:34pm

Intercepted Intrusion item 10 Screenshot





Intercepted Intrusion item 11 Screenshot

Text

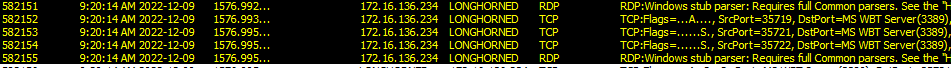
Description automatically generated with low confidence

Intercepted Intrusion item 12 Screenshot





Screenshots for Intercepted table item 13





Screenshots for Intercepted table item 14





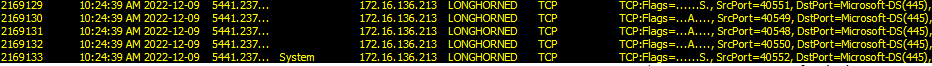
Screenshots for Intercepted table item 15

Shape, rectangle

Description automatically generated



Screenshots for Intercepted table item 16





Screenshots for Intercepted table item 17

Text

Description automatically generated with low confidence

Screenshots for Intercepted table item 18





Screenshots for Intercepted table item 19





Screenshots for Intercepted table item 20

## Security Recommendations

**Permissions –** Audit existing users on host machine and remove if not in use. Only grant elevated access when required. Utilize AD account security to manage users.

**Server Access -** Only allow physical access to the server to authorized employees or organization members. Limit critical file directories and applications to administrators only. Limit membership to admin users and groups for authorized users. Disable any open ports/network protocols not in use.

**Patch Vulnerabilities –** Ensure all system updates are applied and applications are up to date.

**Remote Access –** RDP should only be accessible using a VPN, direct access through the internet makes it more vulnerable to unauthorized attempts to gain access. Ensure that PowerShell and SSH are only accessible using a VPN to minimize potential security issues.

**Attack Surface –** Remove software that is not needed on your server. Disable any unneeded services.

**Monitor Servers –** Ensure logs are being checked frequently for login attempts, user activity and elevated privilege user activity. Perform server scans regularly to search for abnormalities that may indicate viruses, malware, and hack attempts.

# Red Team

## Intrusions Methods and Attempts

**Intrusion Method #1**

To gather additional information on each group, we went to their public website then looked at the page source. Through this page source, we were able to gain the Server Name of each group by looking at the webadmin email.

For example, the page source of 172.16.132.72 was:

|  |
| --- |
| **<html>** |
|  | **<body style="background-color:lightgreen";>** |
|  | **<center>** |
|  | **<h1>Welcome to VRS Webpage </hl>** |
|  | **<p><img srC="**[**thumbnail\_Logo.png**](http://172.16.136.72/thumbnail_Logo.png)**"> </p>** |
|  | **<h4>Intro to Security Analysis and Implementation-ISEC3700 </h4>** |
|  | **<br><p>web Master:<a href="**[**mailto:WebAdmin@Honey.ca?Subject-Hello820again**](mailto:WebAdmin@Honey.ca?Subject-Hello820again)**" target=" top"> WebAdmin@Honey.ca </a></p>** |
|  | **</center>** |
|  | **</body>** |
|  | **</html>** |

Using this method, we determined that 172.16.132.72 was HONEY and the group was Victor, Robert and Sukhman.

For each server we gathered the following information:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Date | Time | Honeypot Hostname | IP of honeypot | IP of Red Team node | Port used | Protocol Used | Details of intrusion | Notes |
| 12/2/2022 | 12:06pm | HONEY | 172.16.136.72 | 172.16.136.223 | 80 | TCP  (HTTP) | Looked at source code of web page. Using team logo image and webadmin email, determined group members | Team Members:  Victor, Robert, Sukhman |
| 12/2/2022 | 12:07pm | LEAF CUTTER | 172.16.136.73 | 172.16.136.223 | 80 | TCP  (HTTP) | Looked at source code of web page. Using team logo image and webadmin email, determined group members | Team Members:  Alex, Jeff, Jeff, Dylan |
| 12/2/2022 | 12:08pm | FLOWER | 172.16.136.74 | 172.16.136.223 | 80 | TCP  (HTTP) | Looked at source code of web page. Using team logo image and webadmin email, determined group members | Team Members:  Skylar, Louis, Elizabeth |
| 12/2/2022 | 12:09pm | BUMBLE | 172.16.136.75 | 172.16.136.223 | 80 | TCP  (HTTP) | Looked at source code of web page. Using team logo image and webadmin email, determined group members | Team Members:  Josh, Shon, Ben |
| 12/2/2022 | 12:10pm | MASON | 172.16.136.76 | 172.16.136.223 | 80 | TCP  (HTTP) | Looked at source code of web page. Using team logo image and webadmin email, determined group members | Team Members:  Mike, Waiyin, Meagan, Franklin |
| 12/2/2022 | 12:11pm | QUEEN BEE | 172.16.136.78 | 172.16.136.2234000 | 80 | TCP  (HTTP) | No web page set up as instructed for assignment | N/A |

**Intrusion Method #2**

Using Nmap, we scanned each IP address requesting the open ports, the services running on those ports and the version the of the services.

Text

Description automatically generated

172.16.132.72 HONEY Victor, Robert, Sukhman

A screenshot of a computer

Description automatically generated

172.16.136.73 LEAFCUTTER Alex, Jeff, Jeff, Dylan

A screenshot of a computer

Description automatically generated with medium confidence

172.16.136.74 FLOWER Skylar, \*Elizabeth, Lou

A screenshot of a computer

Description automatically generated with medium confidence

172.16.136.75 BUMBLE Josh, Shon, Ben

Text

Description automatically generated

172.16.136.76 MASON Mike, Waiyin, Meagan, Franklin (this group closed ports)

Text

Description automatically generated

172.16.136.78 QUEEN BEE Elizabeth (Using social engineering we determined this was Elizabeth, since she was no longer a part of the group with Louis and Skyler)

For each server we gathered the following information:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Date | Time | Honeypot Hostname | IP of honeypot | IP of Red Team node | Port used | Protocol Used | Details of intrusion | Notes |
| 12/8/2022 | 8:51am | HONEY | 172.16.132.72 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | Port scan | TCP | Scanned each IP address requesting the open ports, the services running on those ports and the version the of the services | Screenshot is included in document of the scan results of each honeypot |
| 12/8/2022 | 8:54am | LEAF CUTTER | 172.16.136.73 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | Port scan | TCP | Scanned each IP address requesting the open ports, the services running on those ports and the version the of the services | Screenshot is included in document of the scan results of each honeypot |
| 12/8/2022 | 9:00am | FLOWER | 172.16.136.74 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | Port scan | TCP | Scanned each IP address requesting the open ports, the services running on those ports and the version the of the services | Screenshot is included in document of the scan results of each honeypot |
| 12/8/2022 | 8:25am | BUMBLE | 172.16.136.75 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | Port scan | TCP | Scanned each IP address requesting the open ports, the services running on those ports and the version the of the services | Screenshot is included in document of the scan results of each honeypot |
| 12/8/2022 | 9:03am | MASON | 172.16.136.76 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | Port scan | TCP | Scanned each IP address requesting the open ports, the services running on those ports and the version of the services. Found closed ports. | Screenshot is included in document of the scan results of each honeypot |
| 12/8/2022 | 9:05am | QUEEN BEE | 172.16.136.78 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | Port scan | TCP | Scanned each IP address requesting the open ports, the services running on those ports and the version the of the services | Screenshot is included in document of the scan results of each honeypot |

**Intrusion Method #3**

Here we used Metasploit to attempt to access each server using a http file server remote command execution exploit

**A picture containing graphical user interface

Description automatically generated**

**Text

Description automatically generated** Text

Description automatically generated

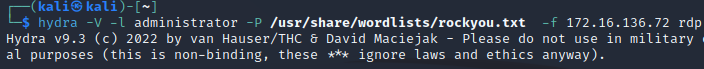
In this example, we configured the exploit to attack 172.16.136.72 (HONEY: Victor, Robert and Sukhman)

We attempted this exploit on each server:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Date | Time | Honeypot hostname | Ip of honeypot | Ip of red team node | Port used | Protocol used | Details of intrusion | notes |
| 12/2/2022 | 9:59am | HONEY | 172.16.136.72 | 172.16.136.222 | 80 | TCP  (HTTP) | Used Metasploit to attempt to access the server using http file server remote command execution exploit | The Exploit was completed but no session was created and was not successful |
| 12/2/2022 | 10:00am | LEAFCUTTER | 172.16.136.73 | 172.16.136.222 | 80 | TCP  (HTTP) | Used Metasploit to attempt to access the server using http file server remote command execution exploit | The Exploit was completed but no session was created and was not successful |
| 12/2/2022 | 10:02am | FLOWER | 172.16.136.74 | 172.16.136.222 | 80 | TCP  (HTTP) | Used Metasploit to attempt to access the server using http file server remote command execution exploit | The Exploit was completed but no session was created and was not successful |
| 12/2/2022 | 10:05am | BUMBLE | 172.16.136.75 | 172.16.136.222 | 80 | TCP  (HTTP) | Used Metasploit to attempt to access the server using http file server remote command execution exploit | The Exploit was completed but no session was created and was not successful |
| 12/2/2022 | 10:08am | MASON | 172.16.136.76 | 172.16.136.222 | 80 | TCP  (HTTP) | Used Metasploit to attempt to access the server using http file server remote command execution exploit | The Exploit was completed but no session was created and was not successful |
| 12/2/2022 | 10:10am | QUEEN BEE | 172.16.136.78 | 172.16.136.222 | 80 | TCP  (HTTP) | Used Metasploit to attempt to access the server using http file server remote command execution exploit | The Exploit was completed but no session was created and was not successful |

**Intrusion Method #4**

We used the Hydra application on Kali Linux to password attack each server using RDP and the rockyou.txt wordlist. \**We attacked all the honeypot servers simultaneously.*



In this example we were attacking the HONEY team (Victor, Robert, Sukhman)

We attempted this wordlist based password cracking attempt on each server:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Date | Time | Honeypot hostname | Ip of honeypot | Ip of red team node | Port used | Protocol used | Details of intrusion | notes |
| 12/5/2022 | 10:30am | HONEY | 172.16.136.72 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | 3389 | TCP  (RDP) | Used Hydra to attempt to guess the Administrator password. Rockyou.txt wordlist contains 14344402 possibilities. | Hydra was unsuccessful in matching the password with a wordlist entry. |
| 12/5/2022 | 10:30am | LEAFCUTTER | 172.16.136.73 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | 3389 | TCP  (RDP) | Used Hydra to attempt to guess the Administrator password. Rockyou.txt wordlist contains 14344402 possibilities. | Hydra was unsuccessful in matching the password with a wordlist entry. |
| 12/5/2022 | 10:30am | FLOWER | 172.16.136.74 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | 3389 | TCP  (RDP) | Used Hydra to attempt to guess the Administrator password. Rockyou.txt wordlist contains 14344402 possibilities. | Hydra was unsuccessful in matching the password with a wordlist entry. |
| 12/5/2022 | 10:30am | BUMBLE | 172.16.136.75 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | 3389 | TCP  (RDP) | Used Hydra to attempt to guess the Administrator password. Rockyou.txt wordlist contains 14344402 possibilities. | Hydra was unsuccessful in matching the password with a wordlist entry. |
| 12/2/2022 | 10:30am | MASON | 172.16.136.76 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | 3389 | TCP  (RDP) | Used Hydra to attempt to guess the Administrator password. Rockyou.txt wordlist contains 14344402 possibilities. | Hydra was unsuccessful in matching the password with a wordlist entry. |
| 12/2/2022 | 10:30am | QUEEN BEE | 172.16.136.78 | 192.168.208.141  (Kali VM)  172.16.136.223  (Workstation) | 3389 | TCP  (RDP) | Used Hydra to attempt to guess the Administrator password. Rockyou.txt wordlist contains 14344402 possibilities. | Hydra was unsuccessful in matching the password with a wordlist entry. |

## Security Recommendations

**Passwords** - Use complex passwords using numbers, symbols, uppercase and lowercase letters.

**Ports** - Close unnecessary ports to minimize potential for unauthorized access attempts.

**Public web pages** - When creating HTML documents, avoid putting sensitive information in the webpage code

**Firewall** - Configure a firewall to block IP addresses when a port scan is detected.

**User Access -** Configure login settings to deny access after a specified number of failed login attempts.

**Updates** - Ensure updates are applied as they are released to address potential vulnerabilities