ISEC2700

Assignment 3

Pod #5\_6

10/09/2024

Table of Contents

[Networking Information 3](#_Toc179911975)

[Task 2 – pfSense VM Creation | Authors – Kyle Jacob 3](#_Toc179911976)

[Task 3 – Questions | Authors – Kyle, Reily, Shash, Jacob 3](#_Toc179911977)

[Task #4 – VPN |Authors – Kyle, Jacob 6](#_Toc179911978)

[Documentation/Screenshots: 6](#_Toc179911979)

[Screenshot #1 – VPN Certificate #1 6](#_Toc179911980)

[Screenshot #2 – VPN Certificate #2 7](#_Toc179911981)

[Screenshot #3 – Server Mode Settings 7](#_Toc179911982)

[Screenshot #4 – CBruce Creation 8](#_Toc179911983)

[Screenshot #5 – Successful VPN Connection 9](#_Toc179911984)

[Screenshot #6 – CBruce VPN Authentication 9](#_Toc179911985)

[Gold Copy and Snapshot: 10](#_Toc179911986)

[Screenshot #7 – Snapshot 10](#_Toc179911987)

[Screenshot #8 – Gold Copy Properties 10](#_Toc179911988)

[Work Journals 11](#_Toc179911989)

[Team Rubric 12](#_Toc179911990)

[Bibliography 20](#_Toc179911991)

## Networking Information

WAN (em0) Config: DHCP 192.168.208.135/24

LAN (em1) Config: Static 192.168.208.100/24

## Task 2 – pfSense VM Creation | Authors – Kyle Jacob

## Task 3 – Questions | Authors – Kyle, Reily, Shash, Jacob

* **Q1. What does Snort VRT do and why are we enabling it?**

Snort Vulnerability Research Team is a network security team at Cisco’s Talos intelligence. By enabling it, snort will receive consistent updates to its ruleset, making it better at intrusion detection.

* **Q2. What is OpenAppID and what is the difference between OpenAppID and AppID Open Text rules, why did we enable both?**

Both OpenAppID and AppID are application detection engines used by snort. The key difference is openness and flexibility. Since OpenAppID is opensource, it is inherently more customizable and developer friendly. Wear as AppID is proprietary and therefor secure but rigid. Both were enabled because we will be working with Snort for OpenAppID and presumably OpenText software in the future.

* **Q3.  What does the IPS Policy do and why are we selecting it?**

IPS is Intrusion Prevention System, it is a set of rules that was created to detect and neutralize any threats to a network. It analyzes the network traffic, while identifying and mitigating the potential attacks before they can harm the system. It’s done by monitoring the patterns. Why are we selecting it? IPS helps protect a network by PROACTIVELY stopping threats, it ensures the compliance with a security protocol and by selecting a policy, we’re adding a layer of defense to prevent vulnerabilities

* **Q4. What does the IPS Policy Selection do and why did we set our selection to “Security”?**

The IPS Policy Selection allow you to choose an already existing policy or create custom settings that dictate how the IPS will work. These selections typically vary based on the type of security that is wanted. Why do we set the selection to security? We set it to security as it provides the most protection and security of all the pre-determined options

* **Q5.  What are the 7 logs are available in your Log Mgmt/Log Size and Retention Limits? What do they capture and how do you access the logs?**

1. Alert – 14 days (retention) / It captures snort alerts and event details
2. Snort\_xxxxx.u2 - 14 days (retention) / It captures snort alerts and event details in Unified2 binary log format
3. Appid-alerts – 30 days (retention) / It captures Application ID Alerts
4. App-stats – 14 days (retention) / It captures Application ID statistics
5. Event pcaps – 14 days (retention) / It captures snort alert related packet captures
6. Sid\_changes – 14 days (retention) / It captures SID changes made by SID mgmt conf files
7. Stats – 7 days (retention) / It captures snort performance statistics

It is accessed via Select Log Mgmt from the Snort menu

* **Q6. What is “Talos” and what is it used for and who uses it?**

Talos is the Talos Intelligence Group, a branch of Cisco who research threats to help keep Snort up to date. Network Administrators using Snort on their servers would actively be using Talos any time they are using their IPS rules.

* **Q7. When we view our PfSense Dashboard we can see several different pieces of information under System Information that help us management our security server. Other then CPU Usage, identify 5 other pieces of information and explain why it is helpful/important to have this data.**
  + - **Version** is important to see front and center to know whenever an update is available and to verify that you are running the latest software.
    - **Current date/time** helps verify that Chrony is running and configured to stop any desync issues
    - **DNS Server** is helpful to have displayed in case of any connectivity issues with host machines.
    - **Name** displays the servers NetBIOS/FQDN in full, helpful for double-checking domain connections.
    - **Memory usage** is helpful in a similar way to CPU, to make sure the server is not under a heavy load or to help diagnose speed or connection issues.
* **Q8. While watching your Traffic Graph your should see at least 2 or more IPs. Record the 2 IPs from your graph and identify the device they reference. Include a screenshot of your Graph captures and IP capture.**

A screenshot of a graph

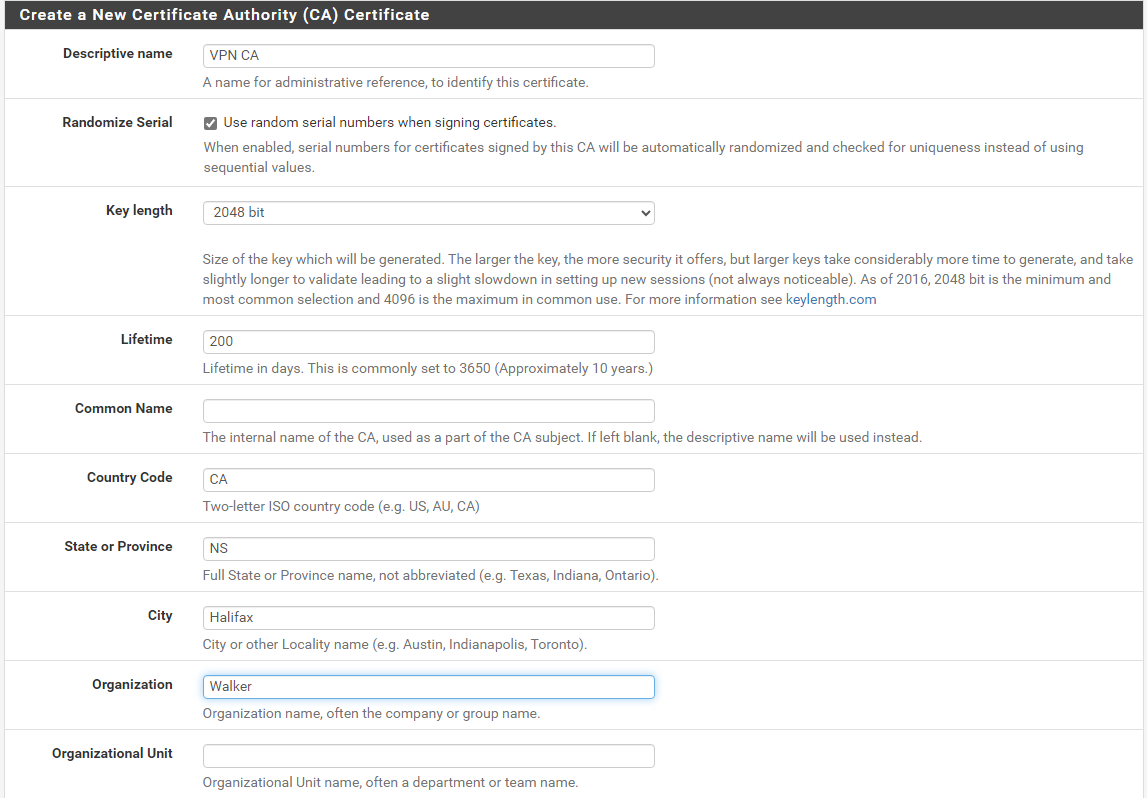
Description automatically generated

*WAN is NIC1 and LAN is NIC2*

## Task #4 – VPN |Authors – Kyle, Jacob

## Documentation/Screenshots:

### Screenshot #1 – VPN Certificate #1



*VPN Certificate 1*

### Screenshot #2 – VPN Certificate #2

A screenshot of a computer

Description automatically generated

*VPN Certificate 2*

### Screenshot #3 – Server Mode Settings

A screenshot of a computer

Description automatically generated

*Server Mode Settings*

### Screenshot #4 – CBruce Creation

A screenshot of a computer

Description automatically generated

*CBruce User Creation*

### Screenshot #5 – Successful VPN Connection

A screenshot of a computer error

Description automatically generated

*VPN Connectivity*

### Screenshot #6 – CBruce VPN Authentication

A screenshot of a computer

Description automatically generated

*CBruce Vpn Authentication*

## Gold Copy and Snapshot:

### Screenshot #7 – Snapshot

A screenshot of a computer

Description automatically generated

*pfSense Server Snapshots*

### Screenshot #8 – Gold Copy Properties

A screenshot of a computer

Description automatically generated

*pfSense Gold Copy Properties*

# Work Journals

|  |
| --- |
| Work Journals: ISEC2700 Assignment 3 |
|  |
| **Name** = Jacob |
| **Role** = Researcher |
| **Work Details:** |
| Wed Oct 9th | |
| 2 hours Creating pfSense VM, Tasks 1-3 | | |

|  |
| --- |
| Work Journals: ISEC2700 Assignment 3 |
|  |
| **Name** = Kyle |
| **Role** = Author |
| **Work Details:** |
| Wed Oct 9th | |
| 2 hours Creating pfSense VM, Tasks 1-3 | | |

|  |
| --- |
| Work Journals: ISEC2700 Assignment 3 |
|  |
| **Name** = Jacob |
| **Role** = Researcher |
| **Work Details:** |
| Tues Oct 15th | |
| 2 hours Setting Up VPN, Task 4 | | |

|  |
| --- |
| Work Journals: ISEC2700 Assignment 3 |
|  |
| **Name** = Kyle |
| **Role** = Author/TL |
| **Work Details:** |
| Tues Oct 15th | |
| 2 hours Setting Up VPN, Task 4 | | |

|  |
| --- |
| Work Journals: ISEC2700 Assignment 3 |
|  |
| **Name** = Reily |
| **Role** = Researcher |
| **Work Details:** |
| Tues Oct 15th | |
| 1 hour completing Task 3 Questions | | |

|  |
| --- |
| Work Journals: ISEC2700 Assignment 3 |
|  |
| **Name** = Jacob |
| **Role** = Researcher/Author |
| **Work Details:** |
| Tues Oct 15th | |
| 0.5 hours formatting final document | | |

# Team Rubric

**Kyle:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Category*** | ***% of Mark*** | **4** | **3** | **2** | **1** | **0** |
| **Attendance** | **30%** | Student attends all team meetings as well as classes (100%). As well as submitting a work journal of homework/work whenever done. | Student attends most team meetings and most classes (75%). As well as submitting work journal 75% of the time whenever homework/work was completed. | Student sometimes attends team meetings and classes (50%). As well as submitting work journal 50% of the time whenever  homework/work was completed. | Student rarely attends team meetings and classes (25%). As well as submitting work journal 25% of the time whenever homework/work was completed. | Student does not attend team meetings or classes. As well as not submitting work journal. |
| **Communication** | **20%** | Student can always be contacted and replies in a timely manner. Can communicate with others in a respectful manner all the time. Team consensus averaged 4 for communication | Student can most of the time be contacted and replies in a timely manner most of the time. Can communicate with others in a respectful manner most of the time. Team consensus averaged 3 for communication | Student sometimes be contacted and replies in a timely manner sometimes. Can sometime communicates with others in a respectful manner. Team consensus averaged 2 for communication | Student rarely replies in a timely manner and is hard to contact most of the time. Cannot communicate with others in a respectful manner most of the time. Team consensus averaged 1 for communication | Student cannot be contacted and expected to reply in a timely manner. Student cannot communicate in a respectful manner. Team consensus averaged 0 for communication |
| **Quality of Submitted Work** | **20%** | Student submits quality work that meets expectations every time asked.  When compared to assignment rubric, team consensus determines quality is excellent (100%-80%). Comment on Dropbox from each member will score out of 10 | Student submits quality work that meets expectations most of the time. When compared to assignment rubric, team consensus determines quality is acceptable (80%-70%) Comment on Dropbox from each member will score out of 10. | Student submits mediocre work, that sometimes meets expectations. When compared to assignment rubric, team consensus determines quality is mediocre (70% -50%). Comment on Dropbox from each member will score out of 10. | Student submits mediocre work most of the time, and the work rarely meets expectations. When compared to assignment rubric, team consensus determines quality is poor (>50%). Comment on Dropbox from each member will score out of 10. | Student does not submit quality work or any work at all, anything submitted rarely or never meets expectations. When compared to assignment rubric, team consensus determines quality is very poor and is not worth submitting. Comment on Dropbox will score out of 10. |
| **Deadlines** | **30%** | Student completes work before all deadlines. | Student completes all work by the **24-hour** team deadline. | Student completes all work by 12 hours post **24-hour** team deadline (12 hours remaining on Brightspace due date) | Student completes all work by 18-hour post **24-hour** team deadline (6 hours remaining on Brightspace due date) | Student does not complete work before Brightspace due date. Work is not accepted after 1 hour until Brightspace due date. |

MARK: 18/20 – 90%

**Jacob:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Category*** | ***% of Mark*** | **4** | **3** | **2** | **1** | **0** |
| **Attendance** | **30%** | Student attends all team meetings as well as classes (100%). As well as submitting a work journal of homework/work whenever done. | Student attends most team meetings and most classes (75%). As well as submitting work journal 75% of the time whenever homework/work was completed. | Student sometimes attends team meetings and classes (50%). As well as submitting work journal 50% of the time whenever  homework/work was completed. | Student rarely attends team meetings and classes (25%). As well as submitting work journal 25% of the time whenever homework/work was completed. | Student does not attend team meetings or classes. As well as not submitting work journal. |
| **Communication** | **20%** | Student can always be contacted and replies in a timely manner. Can communicate with others in a respectful manner all the time. Team consensus averaged 4 for communication | Student can most of the time be contacted and replies in a timely manner most of the time. Can communicate with others in a respectful manner most of the time. Team consensus averaged 3 for communication | Student sometimes be contacted and replies in a timely manner sometimes. Can sometime communicates with others in a respectful manner. Team consensus averaged 2 for communication | Student rarely replies in a timely manner and is hard to contact most of the time. Cannot communicate with others in a respectful manner most of the time. Team consensus averaged 1 for communication | Student cannot be contacted and expected to reply in a timely manner. Student cannot communicate in a respectful manner. Team consensus averaged 0 for communication |
| **Quality of Submitted Work** | **20%** | Student submits quality work that meets expectations every time asked.  When compared to assignment rubric, team consensus determines quality is excellent (100%-80%). Comment on Dropbox from each member will score out of 10 | Student submits quality work that meets expectations most of the time. When compared to assignment rubric, team consensus determines quality is acceptable (80%-70%) Comment on Dropbox from each member will score out of 10. | Student submits mediocre work, that sometimes meets expectations. When compared to assignment rubric, team consensus determines quality is mediocre (70% -50%). Comment on Dropbox from each member will score out of 10. | Student submits mediocre work most of the time, and the work rarely meets expectations. When compared to assignment rubric, team consensus determines quality is poor (>50%). Comment on Dropbox from each member will score out of 10. | Student does not submit quality work or any work at all, anything submitted rarely or never meets expectations. When compared to assignment rubric, team consensus determines quality is very poor and is not worth submitting. Comment on Dropbox will score out of 10. |
| **Deadlines** | **30%** | Student completes work before all deadlines. | Student completes all work by the **24-hour** team deadline. | Student completes all work by 12 hours post **24-hour** team deadline (12 hours remaining on Brightspace due date) | Student completes all work by 18-hour post **24-hour** team deadline (6 hours remaining on Brightspace due date) | Student does not complete work before Brightspace due date. Work is not accepted after 1 hour until Brightspace due date. |

MARK: 19/20 – 95%

**Reily:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Category*** | ***% of Mark*** | **4** | **3** | **2** | **1** | **0** |
| **Attendance** | **30%** | Student attends all team meetings as well as classes (100%). As well as submitting a work journal of homework/work whenever done. | Student attends most team meetings and most classes (75%). As well as submitting work journal 75% of the time whenever homework/work was completed. | Student sometimes attends team meetings and classes (50%). As well as submitting work journal 50% of the time whenever  homework/work was completed. | Student rarely attends team meetings and classes (25%). As well as submitting work journal 25% of the time whenever homework/work was completed. | Student does not attend team meetings or classes. As well as not submitting work journal. |
| **Communication** | **20%** | Student can always be contacted and replies in a timely manner. Can communicate with others in a respectful manner all the time. Team consensus averaged 4 for communication | Student can most of the time be contacted and replies in a timely manner most of the time. Can communicate with others in a respectful manner most of the time. Team consensus averaged 3 for communication | Student sometimes be contacted and replies in a timely manner sometimes. Can sometime communicates with others in a respectful manner. Team consensus averaged 2 for communication | Student rarely replies in a timely manner and is hard to contact most of the time. Cannot communicate with others in a respectful manner most of the time. Team consensus averaged 1 for communication | Student cannot be contacted and expected to reply in a timely manner. Student cannot communicate in a respectful manner. Team consensus averaged 0 for communication |
| **Quality of Submitted Work** | **20%** | Student submits quality work that meets expectations every time asked.  When compared to assignment rubric, team consensus determines quality is excellent (100%-80%). Comment on Dropbox from each member will score out of 10 | Student submits quality work that meets expectations most of the time. When compared to assignment rubric, team consensus determines quality is acceptable (80%-70%) Comment on Dropbox from each member will score out of 10. | Student submits mediocre work, that sometimes meets expectations. When compared to assignment rubric, team consensus determines quality is mediocre (70% -50%). Comment on Dropbox from each member will score out of 10. | Student submits mediocre work most of the time, and the work rarely meets expectations. When compared to assignment rubric, team consensus determines quality is poor (>50%). Comment on Dropbox from each member will score out of 10. | Student does not submit quality work or any work at all, anything submitted rarely or never meets expectations. When compared to assignment rubric, team consensus determines quality is very poor and is not worth submitting. Comment on Dropbox will score out of 10. |
| **Deadlines** | **30%** | Student completes work before all deadlines. | Student completes all work by the **24-hour** team deadline. | Student completes all work by 12 hours post **24-hour** team deadline (12 hours remaining on Brightspace due date) | Student completes all work by 18-hour post **24-hour** team deadline (6 hours remaining on Brightspace due date) | Student does not complete work before Brightspace due date. Work is not accepted after 1 hour until Brightspace due date. |

MARK: 17/20 – 85%

**Shash:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Category*** | ***% of Mark*** | **4** | **3** | **2** | **1** | **0** |
| **Attendance** | **30%** | Student attends all team meetings as well as classes (100%). As well as submitting a work journal of homework/work whenever done. | Student attends most team meetings and most classes (75%). As well as submitting work journal 75% of the time whenever homework/work was completed. | Student sometimes attends team meetings and classes (50%). As well as submitting work journal 50% of the time whenever  homework/work was completed. | Student rarely attends team meetings and classes (25%). As well as submitting work journal 25% of the time whenever homework/work was completed. | Student does not attend team meetings or classes. As well as not submitting work journal. |
| **Communication** | **20%** | Student can always be contacted and replies in a timely manner. Can communicate with others in a respectful manner all the time. Team consensus averaged 4 for communication | Student can most of the time be contacted and replies in a timely manner most of the time. Can communicate with others in a respectful manner most of the time. Team consensus averaged 3 for communication | Student sometimes be contacted and replies in a timely manner sometimes. Can sometime communicates with others in a respectful manner. Team consensus averaged 2 for communication | Student rarely replies in a timely manner and is hard to contact most of the time. Cannot communicate with others in a respectful manner most of the time. Team consensus averaged 1 for communication | Student cannot be contacted and expected to reply in a timely manner. Student cannot communicate in a respectful manner. Team consensus averaged 0 for communication |
| **Quality of Submitted Work** | **20%** | Student submits quality work that meets expectations every time asked.  When compared to assignment rubric, team consensus determines quality is excellent (100%-80%). Comment on Dropbox from each member will score out of 10 | Student submits quality work that meets expectations most of the time. When compared to assignment rubric, team consensus determines quality is acceptable (80%-70%) Comment on Dropbox from each member will score out of 10. | Student submits mediocre work, that sometimes meets expectations. When compared to assignment rubric, team consensus determines quality is mediocre (70% -50%). Comment on Dropbox from each member will score out of 10. | Student submits mediocre work most of the time, and the work rarely meets expectations. When compared to assignment rubric, team consensus determines quality is poor (>50%). Comment on Dropbox from each member will score out of 10. | Student does not submit quality work or any work at all, anything submitted rarely or never meets expectations. When compared to assignment rubric, team consensus determines quality is very poor and is not worth submitting. Comment on Dropbox will score out of 10. |
| **Deadlines** | **30%** | Student completes work before all deadlines. | Student completes all work by the **24-hour** team deadline. | Student completes all work by 12 hours post **24-hour** team deadline (12 hours remaining on Brightspace due date) | Student completes all work by 18-hour post **24-hour** team deadline (6 hours remaining on Brightspace due date) | Student does not complete work before Brightspace due date. Work is not accepted after 1 hour until Brightspace due date. |

MARK: 13/20 – 65%

# Bibliography

IBM. (n.d.). *Intrusion prevention system*. IBM. Retrieved October 15, 2024, from <https://www.ibm.com/topics/intrusion-prevention-system>

Check Point Software Technologies Ltd. (n.d.). *What is IPS?* Check Point. Retrieved October 15, 2024, from <https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/>

Snort. (n.d.). *Snort: The open source network intrusion detection and prevention system*. Retrieved October 15, 2024, from <https://www.snort.org/>