**Internship Logbook**

|  |
| --- |
| Date: 12th September 2022 (Week 7) |
| Objective of the activities:   * How to do Linux hardening * Understanding Solaris OS and Scalable Process Architecture (SPARC), Solaris logical domain (LDom) and control domain (CDom) * Understanding cluster in IT * Understanding Red Hat cluster failover, Veritas cluster, Active/Active and Active/Passive failover, quorum disk * Research IT security tools, i.e., DS-Agent, TripWire, Splunk, and OCS Agent * Audit routers hostname and switches hostname and IP address using Nagios |
| Contents:   1. Understanding in technical knowledge  * The guideline for hardening a Linux server has been made by Center for Internet Security (CIS) which is commonly known as CIS benchmark. * Solaris OS is an UNIX-based operating system, initially made by Sun Microsystems then bought by Oracle. Solaris supports both Intel x86 and SPARC for the hardware requirement. Solaris is a stable OS which provides great security that is suitable for enterprise infrastructure, especially for banking industry. Some of these security features are secure sandboxes to do testing, security compliance assessment, Solaris cluster compliance checks, etc. Besides security, Solaris also ensures backward compatibility when releasing new version. This is critical in large infrastructure since compatibility is one of patching main problem. Lastly, Solaris OS with SPARC able to provide good performance in multi-threaded processes which is suitable for industry that requires to serve huge amount of users. In Solaris world, there are two terms known as LDom and CDom. CDom is often referred as the physical server whereas LDom refers to virtual server running under hypervisor which is hardware-based (type 1). * Cluster in IT refers to a group of nodes (computer) which ensures high availability with fault tolerance. This is possible since a cluster is seen as a single entity and failure of a node would not bring down the entire cluster. * In general, there are two types of failover, i.e., Active/Passive and Active/Active. In Active/Passive, one node is running the service while the other node sits idle acting as backup node. Active/Active, on the other hand, has two nodes running services and in case one node is failing the other node will help run services from the failing node. In Red Hat cluster, there are various failover characteristics, i.e., unrestricted (specify a subset of nodes as the preferred backup), restricted (requires at least one of the specified node to be available in order to run the cluster service), unordered (backup nodes are chosen randomly), ordered (backup nodes are chosen based on priority), failback (in the event that a failure node recovers, it will handle back the service again). * Veritas is a cluster provider which monitor the nodes overall health (file systems, network interfaces, etc.) and use it to detect when a node is failing. One of the essential components in a cluster is a quorum disk. A quorum disk is responsible to specify which nodes are to keep running in case when there is communication issue between nodes. For instance, there are 5 nodes labelled 1 to 5 where nodes number 1-3 are unable to communicate with nodes number 4-5, in case of majority wins, then the quorum disk would state that node 1-3 still run and allow them to access storage while node 4-5 are not allowed to access the storage. This is done to prevent split brain, where data is not synced to all node members. * DS-Agent is a software from TrendMicro which provides real-time and on-demand anti-malware, web reputation service, firewall, IPS, real-time and on-demand integrity monitoring, log inspection, application control and scanner. TripWire is another security tool which provides integrity monitoring, security configuration management, threat detection, compliancy control, and DevOps security. Splunk can be used as an SIEM (Security Information and Event Management) which act as central repository for logs and analyse them to do real-time monitoring and alert system. Lastly, OCS Agent is an inventory/asset tracking software by collecting hardware, software, and network information of a server.  1. Understanding in non-technical knowledge  * Not applicable  1. Understanding in skills  * Utilize regular expression in Nagios to search devices’ hostname or IP address effectively  1. Development of experience  * Exposed to various IT security tools used in enterprise environment and IT clustering which ensure infrastructure high availability  1. Development of experience for future career  * Exposed to Nagios in auditing network inventory  1. Demonstrate the personal skills in organisation  * Punctuality in attending scheduled meeting  1. Demonstrate the personal skills in people  * Effective communication on discussing research findings |

Company Supervisor’s signature & stamp: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: