Notes for Jul_05_2022

This is a note or a diary for the things I research in a day, this note intended for me not to forget the knowlegde I has gain (or things I has read).

Linux Events or Linux Logs

It is stored at /var/log/ so basically you forward all the things to your SIEM and you have the log, but the correlated event and stuff is not there yet. You must applied your knowledge to write these thing by using your SIEM rule or other detection rule that available

So there will be alot of learing right here so I found a link that quite useful link: https://pberba.github.io/security/2021/11/22/linux-threat-hunting-for-persistence-sysmon-auditd-webshell/

SecurityHub - AWS Foundational Best Practices

Link: https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-fsbp.html

I don't know much about AWS but I'm trying to understand the Security game of it, so it has this guide name Foundational Best Practices and stuff.

We will dive in to the first section that you will do go give someone a permission to your AWS environment that is IAM

IAM Practices

- IAM Policies should not allow full "*" admin privilege
- IAM users should not have IAM policies attached
- IAM users's access key should be rotated every 90days or less
- IAM root user access key should no exist
- MFA should be enalbed for all IAM users that has console password
- Password polices for IAM user should have strong config (follow the best practice of AWS)

AWS Environment using multiple Account AWS White Paper | Security OU

Using the **Security Tooling Account** servers as the admininistator account for security services that are managed in an admin/member structure throught out the AWS account,

---

How Linux Process Created and What kind of Log does it generated

The Linux by default doesn't log when the Process is created or not, Well you could say that but fork() and exec() is indicated of process creation

How can you actually detect that link https://unix.stackexchange.com/questions/163681/print-pids-and-names-of-processes-as-they-are-created