Assignment

Subject: Computer Security

Instructor: Asad Raza

Note:

I have not worked on SIEM (Alien Vault) myself. I will try my best to help you and answer all of your questions regarding the assignments, but I may not be able to answer all of your questions. You will have to do a lot of research and get help from online forums in this regard.

*****SIEM and Alient Vault are used interchangeably in the assignment**

A SIEM offers:
1. Intrusion Detection & Anamoly Detection (Snort)
2. Vulnerability Scanning (OpenVas or Nessus)
3. Availability & Network Flow Monitoring (NTOP & Nagios), Asset inventory

Common Assignment for all groups

Each group is required to setup Alient Vault (open source version) and has to make sure that all of the above mentioned services are running and the events are being generated at Alent Vault .

One of the group is required to install OpenVas and the other two groups can install NESSUS for vulnerability scanning service . Other two services are same for all the three groups.

Each group is required to document the installation procedure separately.

Assignment for Group A

How AlienVault can be used to identify attacks in real time?
Present a demonstration in which you will have to carry out an attack via MetaSploit on another machine and based on the events that are coming to SIEM by Snort, define correlation and Generate Alarms at SIEM if the system has been exploited.

Assignment for Group B

Many devices (Cisco Devices, Firewalls, Exchange server) on network sends logs to alien vault, Your task is to configure Juniper Firewall generate the events on Alien Vault and as is it possible to identify based on the logs that a system is compromised?

- If you find any problems with Juniper configuration , I can arrange a student who can help you configure juniper firewall

Assignment for Group C

How AlienVault can be used as Vulnerability Management Solution. Check for the vulnerabilities in the systems and then define a cross correlation (usually a cross correlation is done when a vulnerability is identified and snort is also showing that an attack is in progress due to that vulnerability on the basis of it several events can be correlated to generate a single alarm)

- This assignment is different from the first one. In the first assignment group A has to work specifically on metasploit but you guys have to work on vulnerabilities on an un-patched system.