CYBERDET
DETECTION ENGINEERING TEAM
3. GÖREV

Görev Veriliş Tarihi: 27.09.2024

Görev Teslim Tarihi: 06.10.2024

Görev Açıklaması

Bu görevde takım üyeleri bireysel olarak aşağıdaki görevleri 6 Ekim 2024 saat 23.59'a kadar tamamlayıp formdan göndermelidir.

1. Wazuh üzerinde, SMB protokolü üzerinden brute force saldırılarının tespiti. Wazuh üzerinde, FTP üzerinden yetkisiz dosya transferlerinin tespiti. Wazuh üzerinde, Port tarama (Nmap) kullanımının tespiti. Wazuh üzerinde, RDP üzerinden yetkisiz erişim girişimlerinin tespiti.
2. Linux terminalinde çalıştırılan komutların loglanıp Wazuhta gösterilmesi. Windows Powershellde çalışan komutların loglanıp Wazuhta gösterilmesi.
3. Windows bilgisayardan meterpreter ile shell alındıktan sonra RDP ile bilgisayara erişilmesi.

Her bir görev için izlenen adımların detaylı bir şekilde açıklanarak bir rapor halinde sunulması gerekmektedir.Linux için bash historyden yola çıkabilirsiniz. Powershelli sysmon üzerinden veya farklı yöntemler kullanarak yapabilirsiniz.

Teslim

Görev teslim linki: https://forms.gle/jJFNmsyPJPn37vb9A