Project: Intrusion Detection System

Analyzing Alert Data and Network Traffic

Success Criteria	Specifications
Analyze alerts from an Intrusion Detection System (IDS)	`ticket.docx` contains a summary of the malicious traffic identified via Snort alerts.
Determine whether alerts are incidents (true positives) or false positives.	`ticket.docx` contains a summary of network traffic, under False Positives, that triggered Snort alerts but that appear to be false positives. Format: `2020-05-31 13:05:41 198.51.100.7:52192 -> 203.0.113.19:25`
Monitor network traffic and capture packets in order to investigate suspicious activity.	`dns.pcap` contains a single DNS request.
Analyze network traffic in order to investigate suspicious activity.	The *Additional indicators* section of `ticket.docx` contains summaries for traffic you believe may be related to the malicious connection you identified. In addition to the summary, include a short description. Use the following format: `2020-05-31 13:14:43 192.168.0.7:55321 ->203.0.113.12:81 (HTTP request on non-standard port)`
Create rules in an Intrusion Detection System (IDS) based on specified network traffic.	`local.rules` contains one valid Snort rule that will catch malicious traffic similar to the traffic you identified after the initial indicator of compromise. If your rule is too specific, it may not alert on malicious traffic that is altered in minor ways. If your rule is too broad, it may generate too many false positives. Tip: Don't forget to test your rule! It should have more than 1 result, but not more than 7.

Log Monitoring

Success Criteria	Specifications
Use a SIEM to collect and analyze network and host-based data.	search.png is a Screenshot of a Splunk search and search results that displays one result, the network connection that matches the initial malicious event that appeared in Sguil.
Monitor systems for suspicious activity using a Splunk dashboard.	dashboard.png is a screenshot of the Splunk dashboard showing events from the start of May 31 to the end of the day May 31. dashboard.png should contain the following columns in this order: _time, hostname, username, sudo_command. The events should be ordered by _time in ascending order (earliest time value first).
Monitor systems for suspicious activity using Splunk report.	report.pdf displays a summary of the top usernames in failed authentication attempts. It should contain the headers auth_user, user, count, and percent and cover the time period from the start of May 31 to the end of the day May 31.

Reporting

Success Criteria	Specifications
Follow incident handling procedures	ticket.docx includes evidence that the steps from the appropriate incident response playbook were followed. Some of the steps, such as resetting a user's password, you won't be able to follow. Simply note in the ticket that you reset the user's password or contacted the appropriate group to reset the user's password. Include an approximate time (seconds are not necessary!).
Document incident evidence and construct a timeline, and detail mitigation next steps	ticket.docx includes summaries of network connections (*Initial detection* and _Additional indicators) including timestamps. Mitigation/recovery next steps are included in the *Recovery* and *Post-incident recommendations* section of ticket.docx.