Blue Team Observation Checklist

Blue Team observation checklist

Observed by: Md Salam, Andrew Negapatan, Nickolai Balida

Date of observation: 03/11/2025 to 06/11/2025

Table 1 – Blue team observation checklist

Time	Attack detected	Victim IP	Source IP	Description	Response
03/11/2025 23:13:10	Vulnerability Scanning	10.30.0.235, 10.30.0.236, 10.30.0.237, 10.30.0.250	192.168.1.27	Vulnerability Scanning to identify any know vulnerabilities on target hosts	Setting up IDS or WAF to monitor and block suspicious scanning.
04/11/2025 14:25:41	Port scanning	10.30.0.250	192.168.1.27	Port scanning to discover open ports on the target	Setting up IDS or WAF to monitor and block suspicious scanning.
04/11/2025 22:56:51	Directory Busting	10.30.0.250	192.168.1.27	Web content scanning to discover hidden web content	Setting up IDS or WAF to monitor and block directory requests.
11/11/2025 22:49:05	Spidering	10.30.0.250	192.168.1.27	Web spidering to map web application's structure and find hidden items	Setting up IDS or WAF to monitor and block suspicious activities.

05/11/2025 16:40:34	Brute Force Attack	10.30.0.250	192.168.1.27	To gain unauthorized access to the target system by trying a large number of possible passwords in the dictionary	Setting up IDS or WAF to monitor for excessive failed login attempts and block suspicious IP addresses.
06/11/2025 00:04:31	Post-exploitation enumeration	10.30.0.250	192.168.1.27	To identify potential vulnerabilities or misconfigurations that could lead to privilege escalation or compromise	Treat the presence of linpeas.sh as a potential security incident. Initiate an incident response process.
06/11/2025 13:38:34	Privilege Escalation	10.30.0.250	192.168.1.27	To gain full access to the system	Blue team failed to monitor the activity