Incident Report: Windows SOC Investigation Lab

1. Incident Summary

A suspicious PowerShell execution was detected on the Windows host. This was accompanied by multiple failed login attempts and indications of outbound network connections.

2. Investigation Steps

- Reviewed Windows Security logs for failed login attempts.
- Analyzed Sysmon logs for process creation events involving PowerShell.
- Examined network capture for suspicious outbound traffic.

3. Findings

- Multiple failed login attempts from an external IP address.
- PowerShell executed with encoded command lines, suggesting obfuscation.
- Outbound connections to non-standard ports and unknown IP addresses.

4. Conclusion

These indicators suggest a potential compromise via a PowerShell-based attack attempting to bypass detection and establish command and control channels.

5. Recommendations

- Block the suspicious external IP addresses at the firewall.
- Enable and review detailed PowerShell logging.
- Update endpoint protection and conduct user awareness training.
- Perform a full compromise assessment of affected hosts.

Signed

Anas Nawaf