CAPSTONE PROJECT

z

ACCESS ENFORCEMENT MANAGEMENT

Esther Ogunlana

SCENARIO

Suspicious Actor Attempts to Access PHL's Web Server

Suspicious Actor Gains Entry, Uses a Bot (sitechecker pro) to Scan the Server and Finally Gains Entry

Suspicious Actor Uses Powershell to Initiate Remote Commands and Delete our Database

Wireshark Analysis

- Unauthorized credential Use
- Lateral Movement
- Suspicious Data Exfiltration
- Indicators of Privilege Escalation

Access Enforcement Management

- AC-3: Access Enforcement
- AC-7: Unsuccessful Login Attempts
- AC-19: Access Control for Remote Systems

Esther Ogunlana

RECOMMENDATIONS

Monitoring

- Use SIEM tools for real-time detection of anomalies
- Set up alerts for unusual usage of admin tools

Strengthen Access Controls

- Implement least privilege principles
- Enforce MFA

Network Segmentation

* Limit Lateral Movement by isolating Critical Systems

THANK YOU FOR YOUR ATTENTION

Get In Touch

☎ +1 250-884-2103 ✉ esther.ogunlana@yahoo.com 🌐 www.linkedIn.com/esther-ogunlana

Esther Ogunlana

References

- National Institute of Standards and Technology . (2020, September). NIST SPECIAL PUBLICATION 800-53 Revision 5.

- Compass. Threat Scenario (Cyber Security Immersive). (n.d.). https://web.compass.lighthouselabs.ca/p/cyber/days/w11d3/activities/3242