CIRT Playbook Battle Card: **GSPBC-1054 - Discovery - Password Policy Discovery**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Conduct employee security awareness training
7. Restrict users to the least privileges required
8. Set and enforce secure password policies for all accounts [1]
9. Refer to NIST guidelines when creating password policies [2]
10. Ensure all accounts with elevated permissions have passwords that are unique, complex, and required to be changed periodically

(I) Identification

1. Monitor for:
   a. Access to detailed information about the organization’s local password policy [3]
   b. Access to cloud-based password policies such as AWS [3]
   c. Multiple failed authentication attempts across one or various accounts
   d. Attempts by a user account to gain access to unusual or unauthorized systems or networks
   e. Sign-in failures from out-of-the-ordinary locations or repeated MFA failures
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities
7. Reset accounts that have been breached immediately

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

References:

1. MITRE ATT&CK Mitigation M1027: https://attack.mitre.org/mitigations/M1027/
2. NIST Digital Identity Guidelines: https://pages.nist.gov/800-63-3/sp800-63-3.html
3. MITRE ATT&CK Technique T1201: https://attack.mitre.org/techniques/T1201/

Resources:

- ➔ GuardSight GSVSOC Incident Response Plan: https://github.com/guardsight/gsvsoc_cybersecurity-incident-response-plan
- ➔ IT Disaster Recovery Planning: https://www.ready.gov/it-disaster-recovery-plan
- ➔ Report Cybercrime: https://www.ic3.gov/Home/FAQ

GUARDSIGHT