CIRT Playbook Battle Card: **GSPBC-1030 - Reconnaissance - Active Scanning**

(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. Verify that firewall, SIEM, IDS, and IPS appliances and software are up-to-date
6. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
7. Restrict access to RDP, SSH, and similar protocols
8. Remove default banners from remote connection protocols
9. Remove default headers from web application responses

(I) Identification

1. Monitor for:
    a. Excessive requests on public facing assets, especially if coming from a single source
    b. Abnormal requests for public facing applications and protocols
2. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual behavior
3. Analyze web application metadata for suspicious user-agent strings and other artifacts
4. Investigate and clear ALL alerts

(C) Containment

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

(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

(R) Recovery

1. Address any collateral damage by assessing exposed technologies
2. Resolve any related security incidents

(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

References:

1. MITRE ATT&CK Technique T1595: https://attack.mitre.org/techniques/T1595/
2. Active Scanning Sub-technique T1595.001: https://attack.mitre.org/techniques/T1595/001
3. Active Scanning Sub-technique T1595.002: https://attack.mitre.org/techniques/T1595/002

Resources:

- ➔ IT Disaster Recovery Planning: https://www.ready.gov/it-disaster-recovery-plan
- ➔ Report Cybercrime: https://www.ic3.gov/Home/FAQ

GUARDSIGHT