CIRT Playbook Battle Card: GSPBC-1004 - Lateral Movement - Pass the Hash

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations
4. Ensure that servers and workstations are logging to a central location
5. Network segmentation and firewalls can help reduce impact
6. Disable NTLM authentication where possible
    a. SMB
    b. HTTP
    c. SMTP

(I) Identification

1. Monitor for:
    a. Unusual user activity
    b. Unexpected logins using NTLM
2. Investigate and clear ALL alerts associated with the impacted assets

(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. Lock accounts suspected of having a compromised hash
6. Systems believed to have malware on them should be removed from the network

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Perform Endpoint/AV scans on the systems of affected users
4. Review logs to identify other potential cases of passing the hash

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Change the passwords of any potentially compromised accounts
4. Determine the chain of events that led to the pass the hash incident
5. 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

Notes:

1. Report cybercrime: https://www.ic3.gov/default.aspx