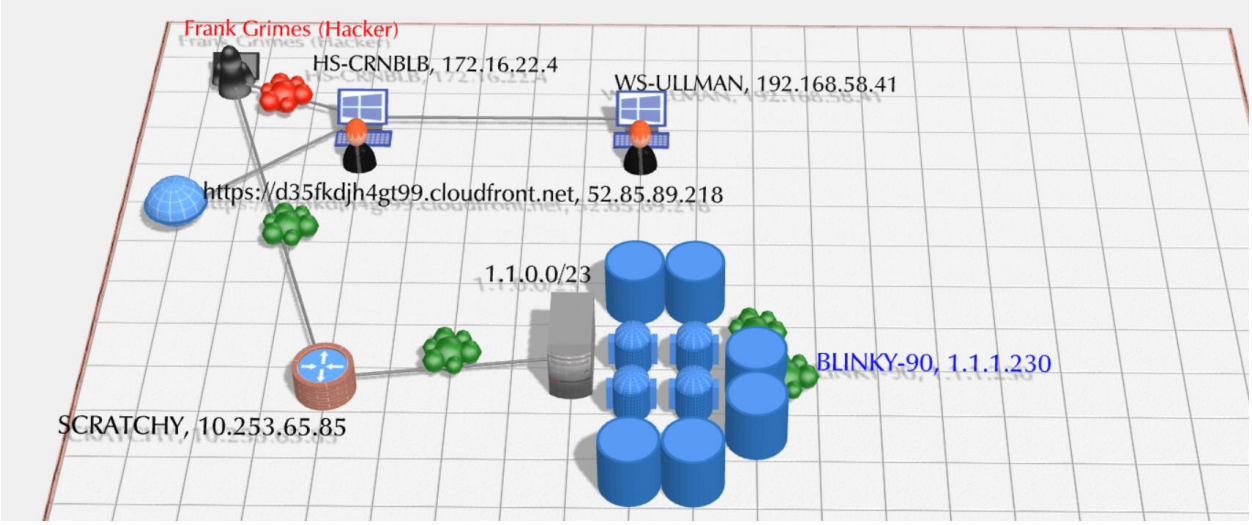
SCADA CONSULTING EXERCISE

1. **Diagram.** Please create a diagram that depicts the following scenario where Springfield Power Plant's network has been breached by an attacker. Visio, PowerPoint, LucidChart (free), GraphViz (free) or other software may be used to create the diagram.

Scenario

- An attacker sends a spear phishing message with the subject "Free Donuts in Cafeteria at Noon: Details in Attachment" containing a malicious Microsoft Word attachment to Homer Simpson who opens the attachment and enables Macros when prompted to view the sweet, sweet donut details. (mmmmmmmm….donuts)
- Once opened, a macro is executed which runs a PowerShell command that establishes a command and control (C2) channel to a domain (https://d35fkdjh4gt99.cloudfront.net, 52.85.89.218) which ultimately resolves to a machine controlled by the attacker (Frank Grimes) in Amazon's EC2 cloud.
- Frank Grimes escalates his privileges on Homer Simpson's computer (HS-CRBNBLB, 172.16.22.4) to gain administrative access and extracts password hashes using Mimikatz.
- Frank Grimes then uses the shared local administrator password obtained from Homer Simpsons computer to move laterally on the network to Wayland Smithers' computer (WS-ULLMAN, 192.168.58.41).
- Wayland Smithers' computer contains an unprotected SSH private key file for an SSH jump box that grants access to the SCADA systems network within the power plant.
- Using those passwords, Frank Grimes authenticates using PuTTY to the jump box (SCRATCHY, 10.253.65.85) and then uses Nmap to scan for open ports on the SCADA network (1.1.0.0/23) for open port TCP/666 which controls the reactor.
- Frank identifies open port TCP/666 and connects to the reactor (BLINKY-90, 1.1.1.230) over Telnet without a password required.
- Frank then places malware on the system designed to alter the core temperature of the reactor in the next 30 days.

2. **Defensive Controls Mapping.** Note for each step which defensive toolset or process would be used to help mitigate and detect what Frank Grimes has been able to successfully do as an attacker. We expect detailed explanations in paragraph form. If it is not already obvious, the exercise is Simpsons-themed, so please have fun with it!



1. An attacker sends a spear phishing message with the subject “Free Donuts in Cafeteria at Noon: Details in Attachment” containing a malicious Microsoft Word attachment to Homer Simpson who opens the attachment and enables Macros when prompted to view the sweet, sweet donut details. (mmmmmmmm….donuts)
2. Once opened, a macro is executed which runs a PowerShell command that establishes a command and control (C2) channel to a domain (https://d35fkdjh4gt99.cloudfront.net, 52.85.89.218) which ultimately resolves to a machine controlled by the attacker (Frank Grimes) in Amazon’s EC2 cloud.
3. Frank Grimes escalates his privileges on Homer Simpson’s computer (HS-CRBNBLB, 172.16.22.4) to gain administrative access and extracts password hashes using Mimikatz.
4. Frank Grimes then uses the shared local administrator password obtained from Homer Simpsons computer to move laterally on the network to Wayland Smithers’ computer (WS-ULLMAN, 192.168.58.41).
5. Wayland Smithers’ computer contains an unprotected SSH private key file for an SSH jump box that grants access to the SCADA systems network within the power plant.
6. Using those passwords, Frank Grimes authenticates using PuTTY to the jump box (SCRATCHY, 10.253.65.85) and then uses Nmap to scan for open ports on the SCADA network (1.1.0.0/23) for open port TCP/666 which controls the reactor.
7. Frank identifies open port TCP/666 and connects to the reactor (BLINKY-90, 1.1.1.230) over Telnet without a password required.
8. Frank then places malware on the system designed to alter the core temperature of the reactor in the next 30 days.

---

1. The initial exploitation and attack vector which is through an endpoint on the network—HS-CRBNBLB, is partially a social engineering technique as it is exploiting the user’s trust over the email message’s authenticity and also the legitimacy of its attachments. By giving Homer Simpson, the designated owner of endpoint HS-CRBNBLB (172.16.22.4), proper information security awareness training, the attack may have been totally

prevented as he would recognize the email was using a spoofed email address, coming from an untrusted sender address or domain, and exercise special awareness due to the fact the email is not only suspicious but has a suspicious attachment that could be malicious.

   a. Homer could then after recognizing the email is suspicious:
      i. Raise a security incident with the organization so the SOC can investigate
      ii. Delete the email or flag as spam, quarantining the payload and segmenting it on his endpoint pending SOC investigation, rendering it totally useless.
      iii. Contribute to organization and regional CTI as the malicious email and its payload can be forensically identified and deconstructed to identify the attacker, Frank Grimes, and their TTPs, thus furthering the organizations cybersecurity intelligence as well as within the broader community to prevent against future attacks from the attacker and, if applicable, their group.
   b. Secured mail gateway
      i. A sophisticated secure mail gateway may have prevented the email from entering into the user's inbox or, at a minimum, flagged the email as spam alerting user that the message and its attachments are possibly malicious. It could have also deleted, quarantined, or removed the malicious attachments before any user attempts to retrieve them in the event Homer had no infosec awareness training.
   c. Protected View GPO
      i. Mandatory protected view with disablement requiring second-level approval may have prevented execution of the malicious macros on the Word document while also preventing the subsequent C2 connection.
      ii. Additionally, endpoint detection such as McAfee correlated to a SIEM/SOAR suite such as Splunk or QRadar may have alerted the SOC to the macros attempt and thus an attempt at a breach.

2. Endpoint detection
   a. Behavioral endpoint detection may have discovered the malicious execution of the MS Word document macros and flagged an alert on the SOC's SIEM/SOAR
   b. At the very least, endpoint detection would be expected to discover the establishment of a connection to the C2 channel https://d35fkdjh4gt99.cloudfront.net, 52.85.89.218
   c. After discovery by SOC, they would presume this to be a valid IoC and would immediately isolate, quarantine, and segment HS-CRBNBLB (172.16.22.4) from the network to further proceed with incident response-- discovering and removing the malware, and purging the compromised system. This would have alerted SOC to compromise and any other unusual activities on the entire network would be flagged likely preventing any further pivoting or ingress.
3. (also 4.) Endpoint detection would best be suited for privilege escalation prevention on the network boundary

   a. Additionally, disabling password caching to prevent Mimikatz's harvesting might be an effective control on the workstation in addition to forcing Kerberos authentication on administrator users within the LAN. The attack appears to not be on the level of a TGT-compromise, so Frank Grimes would be not be able to further escalate after endpoint compromise with the macros and deploying Mimikatz. Finally, correlated EDR/UEBA may be best suited for detecting higher-level Active Directory, KGT-TGT attacks.
   b. Mimikatz may be flagged by good endpoint software as well, preventing any additional pivoting or escalation once it is discovered resident although in this situation, the caveat is that the C2 channel was likely the vector for deployment so it never hit the victim's local storage disk. Therefore, detection would be limited to mainly the C2 connection and also unusual Windows events and behaviors on the infected machine that would point towards privilege escalation or lateral movement. This would require EDR flagging the C2 connection, good correlation from UEBA, and also a vigilant SOC viewing the activity.
5. By far, encrypting and password-protecting SSH keys is the first line of defense for preventing unauthorized access and use.
   a. Secondly, air gapping the SSH keys on retained, removable media that is tagged by RFID to prevent removal from the worksite could prevent this attack as it would require the media to be inserted in order to be accessible during Frank's pivot. In fact, the USB device could only be inserted during the initial authentication phase into the jump box as needed for Wayland Smithers to administer the SCADA network and jump box and removed otherwise, providing an extremely narrow window of time for compromise by an attacker even with direct persistence and full access on the user's workstation.
6. Whitelisting the jump box's acceptable IP address list could possibly prevent Frank from remote SSH access into the jump box, however since they have obtained other devices during the initial exploitation and lateral movement, they most likely have host information to spoof and would likely spoof Wayland's IP and host information as they had ownership over the SSH keys into the jump box. Therefore, enabling MFA on the jump box authentication architecture would be the next best step in preventing unauthorized access. Due to the criticality of the infrastructure, 3FA may be the best next step with hardcoded TOTP token devices in addition to 3rd-level 2FA (facial recognition).
   a. Additionally, the jump box should be physically segmented when not in use. This would create a full airgap into SCADA and make intrusion much more difficult.
   b. An IPS/IDS setup in front of the SCADA (1.1.0.0/23) LAN entry node would be critically important here as not only would it provide good defense against many different attacks; it would detect and drop the port scan attempts through the jump box and flag the activity on the SIEM/SOAR. The SOC would then be immediately alerted to an IoC near the critical infrastructure's network, would presume deep intrusion or persistence from an attacker, and would then take an equivalent level of aggressiveness in their incident response.

7. Blocking open ports is a standard hardening procedure all network specialists must undertake to prevent access.
    a. Disabling telnet is also an extremely important task as it should always be blocked as part of an organization's baseline and preliminary hardening procedures when launching infrastructure.
    b. Behavioral analytics inside SCADA is extremely important to be made as the last line of defense to prevent compromise as SCADA activities are highly predictable and machine-like, and traditional AV and signature-based detection methods cannot detect their likely zero-day exploits and protect their legacy systems, embedded systems, and other exclusive components. This should absolutely be SIEM/SOAR correlated and on the front dashboard of all managing SOCs to prevent any compromises and to ensure availability in the event of a malfunction.
8. The anomalous core reactor changes by the malware would also be detected by these previously proposed UEBA, behavioral-based tools even in the absence of positive identification of the malware or compromise. This, *per se*, would be sufficient to trigger a possible IoC alerting the SOC into DFIR mode after isolating SCADA. High-end UEBA defense on the SCADA network would ideally suggest malware presence and immediately trigger a SOC DFIR.