|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 執行日期：2021年03月02日 | | | | | | | |
| 偵蒐目標 | 目標名稱 | | | 恆盛能源股份有限公司 | | | |
| 網址 | | | http://61.130.70.150:3002 | | IP | 61.130.70.150 |
| 服務埠 | 3002 |
| 系統版本 | 東部戰區 |
| 弱點類型 | | | 密碼破解 | | | |
| 來源依據 | | | 北斗七星 | | | |
| 偵蒐類別 | | | 天線寶寶 | | | |
| 偵蒐地點 | 執行地點 | | | 我家 | | 偵蒐使用IP位址 | 45.87.213.86  (日本) |
| 偵蒐時間 | | | 2021年03月02日 | |
| 偵蒐記錄概況說明 | 1. 目標關聯：   利用CII關鍵基礎設施目標「衢州機場」，進而偵獲國網浙江省電力有限公司衢州供電公司，為衢州市區提供電力供應服務，以至於蒐獲恆盛能源股份有限公司將所生產的電力出售給國家電網等情資，利用該合作關係進行滲透。    (圖1)   1. 目標簡介說明：   恆盛能源股份有限公司主要負責為蒸汽生產和供應、電力的生產和銷售，以煤炭和生物質材料作為燃料，通過熱電聯產方式生產蒸汽和電力，承擔供熱範圍內工業用戶的蒸汽供應，並將所生產的電力出售給國家電網。   1. 目標滲透： 2. 登入系統輸入帳號、密碼     (圖2)   1. 進入恆盛能源股份有限公司智慧電廠首頁。     (圖3)   1. 可查看相關設備訊息並進行修改。     (圖4)   1. 查看巡邏路線，可修改並切換狀態。     (圖5)   1. 點位警報提供點位設備告警管理，若該設備異常將會告警，可透過修改忽略告警條件參數，達到忽略異常告警作用。     (圖6) | | | | | | |
| 網頁用途 | | 恆盛能源股份有限公司進行管理設備、巡檢和檢修等相關工作 | | | | | |
| 瀏覽人數 | | 網頁無提供統計 | | | | | |
| 獲取權限 | | 系統管理員 | | | | | |
| 預期成效 | | 查看公司設備名稱、巡檢路線點和人員等相關資訊。 | | | | | |
| 後續作為 | | 1.恆盛能源股份有限公司將所生產的電力出售給國家電網，可利用此關係而影響到電力供應，造成國家產業界損失及人民生活。  2.透過此系統告警功能，修改其參數，設備若出現異常，使監控告警設備忽略異常狀態，致使供電系統相關設備造成受損，影響衢州機場該區供電狀態。 | | | | | |
| 考核事由 | | |  | | 評分 | |  |
| 偵蒐人員 | | | admin | | 簽證 | |  |