Incident handling with Splunk

## **Incident Handling with Splunk – Notes**

### **Scenario**

* SOC Analyst investigation of a **website defacement** attack on imreallynotbatman.com (Wayne Enterprise).
* Activity mapped to **Cyber Kill Chain** phases.

### **1. Reconnaissance Phase**

**Findings:**

* Attacker IP: **40.80.148.42**
* Used **Acunetix** web scanner to probe the web server.

### **2. Exploitation Phase**

**Findings:**

* **Brute-force attack** detected.
* Originating IP: **23.22.63.114**
* Access gained via IP: **40.80.148.42**
* **142 attempts** in total; 1 successful.

### **3. Installation Phase**

**Findings:**

* Malicious executable **3791.exe** uploaded from attacker’s IP.
* **MD5 hash** recorded from Sysmon logs for the executable.

### **4. Action on Objective**

**Findings:**

* Website defaced after compromise.
* Identified **specific file** used to carry out the defacement.

### **5. Weaponization Phase**

**Information Available:**

* Domain: **prankglassinebracket.jumpingcrab.com**
* IP: **23.22.63.114**

**Findings:**

* Multiple **masquerading domains** tied to attacker’s IP.
* Email linked to attacker: **Lillian.rose@po1s0n1vy.com**

### **6. Delivery Phase**

**Findings:**

* Secondary malware: **MirandaTateScreensaver.scr.exe**
* MD5: **c99131e0169171935c5ac32615ed6261**
* Associated with attacker’s infrastructure for fallback compromise attempts.

✅ **Key Takeaways**

* Splunk can be used across **all Cyber Kill Chain phases** for detection and investigation.
* Threat intel platforms are valuable for **enriching IOCs** like IPs, hashes, and domains.
* Mapping attack activity to phases gives clear insight into **attack progression** and assists in remediation.

 