**Unit 1.2 - Cybersecurity Threat Landscape (Part I - Vocabulary)**

Fill in the below tables using the reports provided and independent research. Try to be as detailed as possible and stick to language that could be easily understood by a lay person.

**Group Member Names:**

Source: *Symantec Internet Security Threat Report (Volume 23)*

|  |  |  |
| --- | --- | --- |
| **Term** | **Definition** | **Context / Significance** |
| Coinminer Attack | Coinminer attacks are ones in which hackers use the processing power of a victim’s machine to shoulder the cost of cryptocurrency mining. These attacks are a revenue generator for hackers and rarely detected. | “The coin mining gold rush resulted in a 8,500 percent increase in detections of coinminers on endpoint computers in 2017.” |
| Ransomware |  |  |
| Zero Day |  |  |
| Malware |  |  |
| “Living Off the Land” |  |  |
| Spear Phishing |  |  |
| Infection Vector |  |  |
| Trojan |  |  |
| Attack Chain |  |  |
| Intrusion Prevention System |  |  |
| Botnet |  |  |
| Targeted Attack |  |  |
| Off-The-Shelf Attack Tools |  |  |
| Watering Hole Attacks |  |  |
| Lateral Movement Techniques |  |  |
| DDoS Attacks |  |  |
| Exploit |  |  |
| DNS |  |  |
| BGP Hijacking |  |  |
| Man in the Middle Attack |  |  |
| Collateral Infection |  |  |
| Script Downloader |  |  |
| Command and Control (C2C) |  |  |
| Payload |  |  |
| Honeypot |  |  |
| IoT |  |  |
| Spyware |  |  |
| Subnet |  |  |

Source: *Verizon* *2018 Data Breach Investigations Report (11th Edition)*

|  |  |  |
| --- | --- | --- |
| **Term** | **Definition** | **Context / Significance** |
| Incident |  |  |
| Breach |  |  |
| Password Dumper |  |  |
| Privilege Abuse |  |  |
| Ram Scraper |  |  |
| Skimmer |  |  |
| Pretexting |  |  |
| Brute Force (Hacking) |  |  |
| Adware |  |  |
| Riskware |  |  |
| Chargeware |  |  |
| PCI |  |  |
| Telnet |  |  |
| SSH |  |  |
| Certificate Forgery |  |  |
| URI Redirection |  |  |
| Buffer Overflow |  |  |

Source: *Akamai State of the Internet / Security Q4 2017 Report*

|  |  |  |
| --- | --- | --- |
| **Term** | **Definition** | **Context / Significance** |
| SQLi |  |  |
| Local File Inclusion |  |  |
| Cross Site Scripting |  |  |
| APIs |  |  |
| SYN Flood |  |  |
| DNS Flood |  |  |
| UDP Flood |  |  |
| Reflection Attacks |  |  |
| Remote Code Injection |  |  |