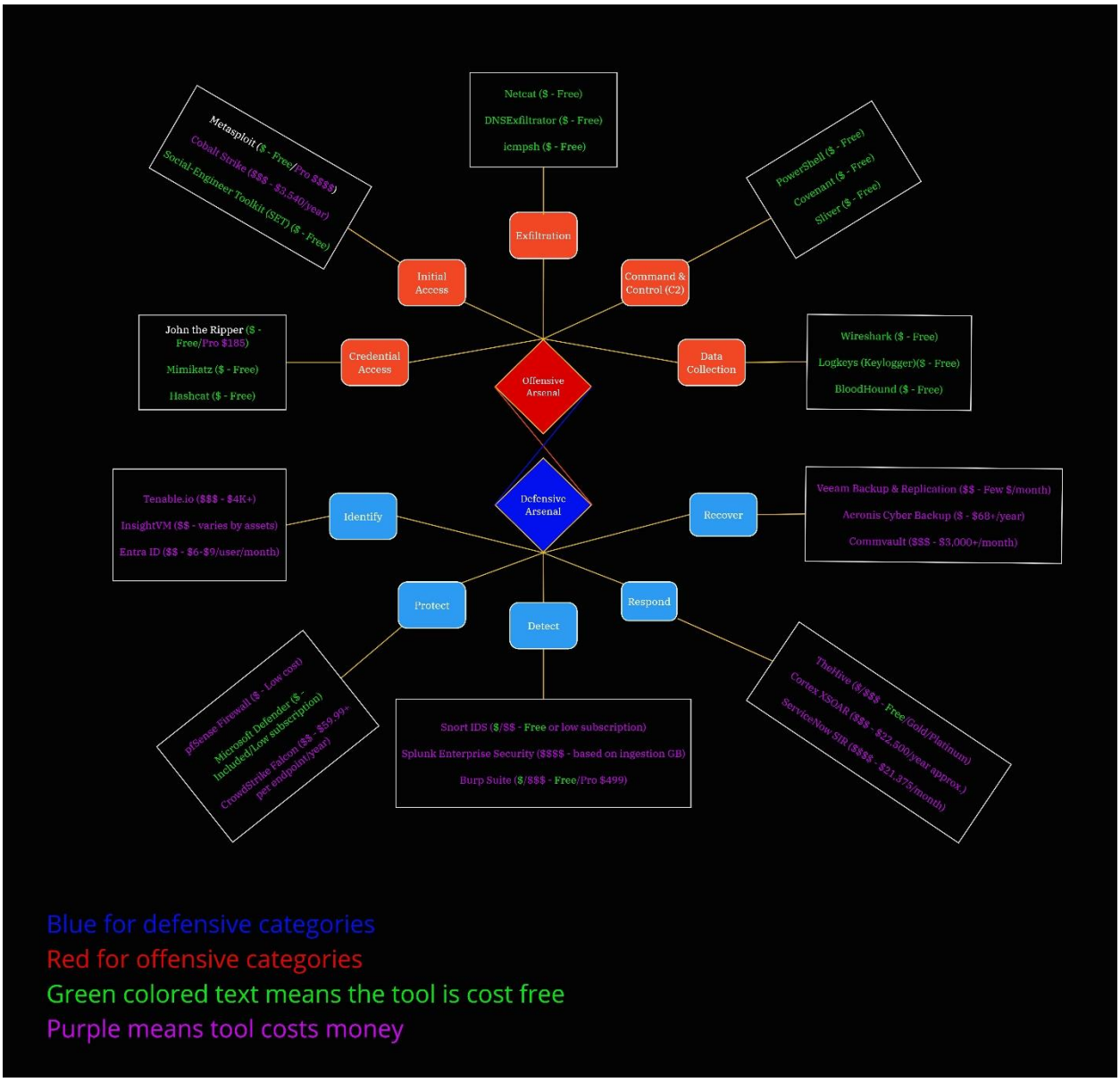
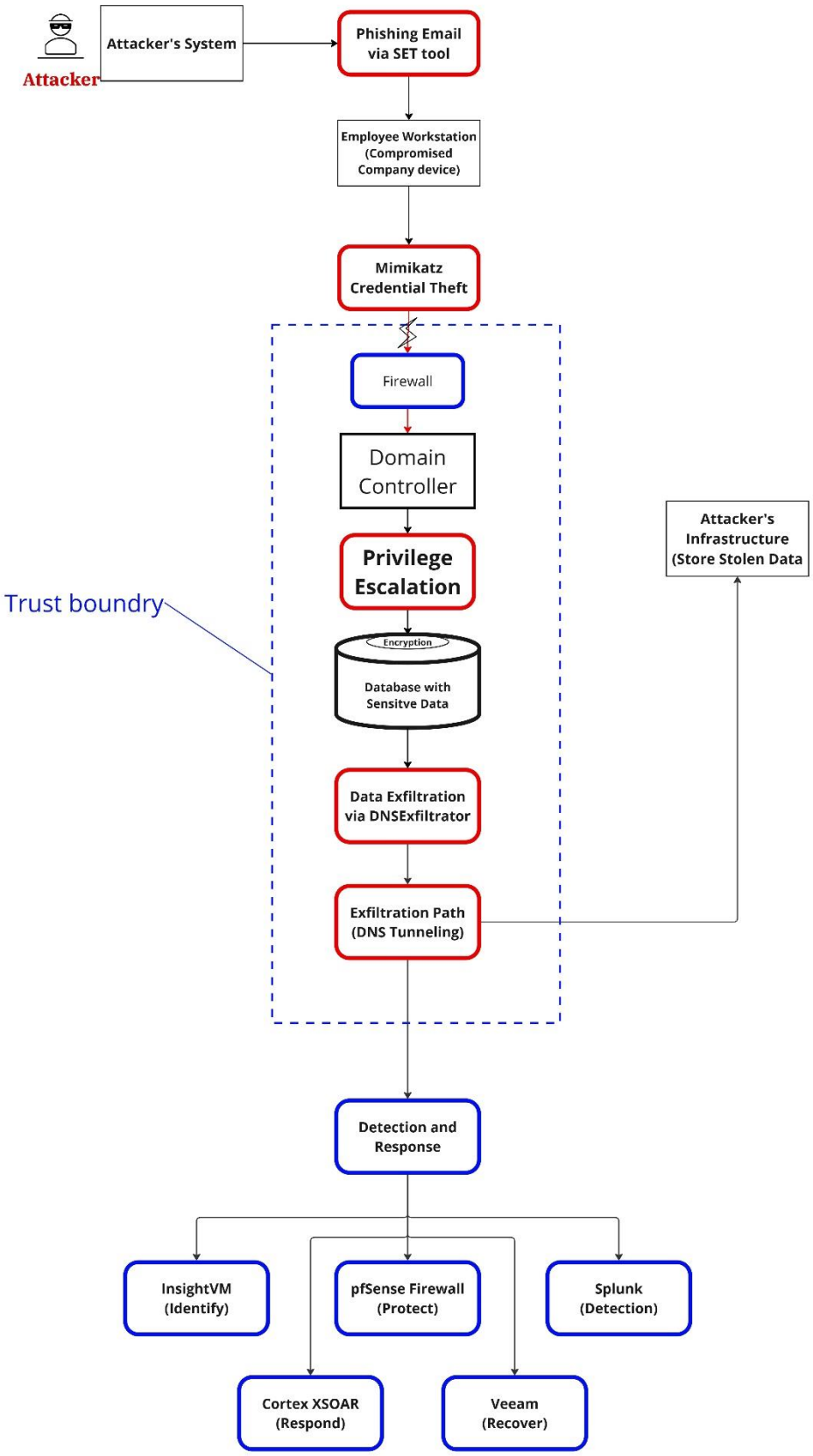
Hidar Elhassan
Lindah Kotut
INFO 415
12/05/2024

Assignment 4: Tool kit III




The tools in my offensive and defensive arsenals were chosen based on their ability to address specific phases of a cyberattack, as outlined by frameworks like MITRE ATT&CK and the NIST Cybersecurity Framework. For my offensive toolkit, I focused on tools that align with critical stages of an attack,

including credential access (e.g., John the Ripper, Mimikatz, Hashcat), initial access (e.g., Metasploit, Cobalt Strike, SET), and exfiltration (e.g., DNSExfiltrator, Netcat). I evaluated each tool based on its cost, usability, and legality, ensuring they are versatile for ethical testing and research purposes. For my defensive toolkit, I selected tools to address the NIST functions Identify, Protect, Detect, Respond, and Recover. My choices (e.g., Tenable.io, CrowdStrike Falcon, Snort IDS, Veeam Backup) were guided by their ability to provide layered security and comprehensive incident response capabilities. I prioritized tools that are easy to integrate, cost-effective, and scalable to ensure my defensive strategy is as robust as possible.


Attacker
Attacker's System
Phishing Email via SET tool
Employee Workstation (Compromised Company device)
Mimikatz Credential Theft
Firewall
Domain Controller
Privilege Escalation
Encryption
Database with Sensitve Data
Data Exfiltration via DNSExfiltrator
Exfiltration Path (DNS Tunneling)
Attacker's Infrastructure (Store Stolen Data
Trust boundry
Detection and Response
InsightVM (Identify)
pfSense Firewall (Protect)
Splunk (Detection)
Cortex XSOAR (Respond)
Veeam (Recover)

In this scenario, a white hat hacker simulates an attack to test an organization's defenses. The attack begins with a phishing email sent via the Social-Engineer Toolkit (SET) to compromise an employee workstation. Using Mimikatz, credentials are extracted from the compromised device. The attacker then breaches the firewall within the trust boundary to escalate privileges on the domain controller. After gaining access, the hacker targets a sensitive database containing encrypted information. Using DNSExfiltrator, data is stealthily exfiltrated via DNS tunneling to an external attacker-controlled infrastructure. On the defensive side, tools like InsightVM identify vulnerabilities, the pfSense firewall protects the network, and Splunk detects suspicious activity. The response is automated with Cortex XSOAR, while Veeam ensures data recovery in case of loss.