CRUZ, JOHN MICHAEL A.
IV-DINS
ELECTIVE 5

1. **IDENTIFY EACH PROBLEM THAT WAS ENCOUNTERED DURING SCANNING ACTIVITY**

| PROBLEM | DESCRIPTION |
|---|---|
| github.com | During the scanning activity, several vulnerabilities were identified for github.com. One of the primary concerns was Attack Surface Discovery, where public-facing servers were detected, making them potential targets for attackers to scan for open ports, vulnerable services, or outdated software. This increases the risk of unauthorized access and exploitation. Another issue found was the threat of DDoS Targeting. The IP addresses discovered could be used in Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks, which could overwhelm the servers, leading to downtime and service disruption. Additionally, there was a risk of Misconfigured Services. If critical services like SSH, FTP, or RDP are unintentionally exposed, they could serve as entry points for attackers, allowing unauthorized access and potential system compromise. |
| **pnwx.com** | The scanning results for pnwx.com highlighted several potential security issues. One major concern was the presence of Exposed Admin Panels or Login Pages, which could be targeted by attackers using brute-force methods to gain unauthorized access. If admin interfaces like /admin, /login, or /wp-admin are left unprotected, they become prime targets for intrusion attempts. Another issue was Sensitive Information Leakage, where URLs may reveal critical data such as debug endpoints, API keys, or internal documentation, potentially aiding attackers in crafting more sophisticated attacks. The scan also identified the existence of Old or Forgotten Web Pages. These legacy pages, if running outdated software, can harbor unpatched vulnerabilities that malicious actors could exploit to gain access to the system. |
| **lingscars.com** | The scanning activity for lingscars.com did not produce specific issues or vulnerabilities. While no explicit threats were identified, it is still advisable to conduct regular security assessments and routine vulnerability scans to ensure the domain remains protected against emerging cyber threats. Continuous monitoring and preventive security measures can help safeguard the system from potential future risks. |
| **Beverlyhills graphicdesign .com** | For beverlyhillsgraphicdesign.com, the scanning process generated an output, but no particular security concerns or vulnerabilities were explicitly highlighted. Despite the absence of immediate threats, |

| | |
|---|---|
| | adopting proactive security practices such as implementing HTTPS, conducting regular vulnerability assessments, and maintaining up-to-date software can help in minimizing the risk of potential exploitation. Regular audits and monitoring can also ensure that any hidden or future vulnerabilities are detected early. |

## 2. GIVE SOLUTIONS TO THE PROBLEMS THAT WAS IDENTIFIED DURING THE SCANNING/SURVEY ACTIVITY FOR EACH DOMAIN/DNS/WEBSITE

**1. github.com**

- **Attack Surface Discovery**
    - Solution: Deploy firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) to monitor and control incoming and outgoing network traffic based on predefined security rules. Firewalls act as a barrier between trusted and untrusted networks, while IDS/IPS detect and prevent potential threats. According to Palo Alto Networks, firewalls filter traffic based on security rules, IDS monitors and alerts on potential security breaches, and IPS actively blocks threats.
- **DDoS Targeting**
    - Solution: Utilize DDoS mitigation services to protect against Distributed Denial of Service attacks. These services analyze network traffic in real-time to detect and mitigate DDoS attacks, ensuring the availability of services. Cloudflare emphasizes the importance of implementing scalable and resilient multilayered DDoS protection solutions as a vital part of a defense strategy.
- **Misconfigured Services**
    - Solution: Regularly audit and configure network services to ensure only necessary services are active and properly secured. Implementing strict access controls and routinely updating service configurations can prevent unauthorized access. Juniper Networks highlights that IDS/IPS monitor all traffic on the network to identify any known malicious behavior, which can help in detecting misconfigured services.

**2. pnwx.com**

- **Exposed Admin Panels or Login Pages**
    - Solution: Restrict access to administrative interfaces by implementing IP whitelisting, VPNs, or multi-factor authentication (MFA). Ensuring that only authorized personnel can access these critical areas reduces the risk of unauthorized access.

- **Sensitive Information Leakage**
    - Solution: Conduct regular code reviews and employ automated scanning tools to identify and remove exposed sensitive data, such as API keys or internal documentation. Ensuring that debug modes are disabled in production environments further minimizes the risk of information leakage.
- **Old or Forgotten Web Pages**
    - Solution: Perform routine audits to identify and update or remove outdated web pages. Maintaining an updated inventory of web assets helps in managing and securing the website effectively.

**3. lingscars.com**

- **Preventive Measures:**
    - Solution: Even in the absence of specific issues, it's prudent to implement general security practices such as regular software updates, security assessments, and the deployment of Web Application Firewalls (WAF) to protect against common web threats.

**4. beverlyhillsgraphicdesign.com**

- **Preventive Measures:**
    - Solution: Adopt security measures including enforcing HTTPS, conducting vulnerability assessments, and ensuring regular backups. These steps help in safeguarding the website against potential threats and data loss.

**5. cameronsworld.net**

- **Multiple Hosting Networks (Infrastructure Weaknesses)**
    - Solution: Standardize security policies across all hosting providers to ensure consistent protection. Regular security audits and selecting providers that adhere to robust security standards are essential. The Canadian Centre for Cyber Security recommends implementing scalable and resilient multilayered DDoS protection solutions as part of a defense strategy.
- **Weaker Security Policies in Some ASNs**
    - Solution: Evaluate and choose hosting providers based on their security practices. Consolidating services under providers with strong security measures can reduce vulnerabilities associated with weaker policies.

3. **Justify your answer provide supporting documents, research and application to your solutions.**

- Canadian Centre for Cyber Security. (n.d.). *Defending against distributed denial of service (DDoS) attacks (ITSM.80.110).* Retrieved from **https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110?utm_source=chatgpt.com**
- Cloudflare. (n.d.). *DDoS protection & mitigation solutions*. Retrieved from https://www.cloudflare.com/ddos/
- Cloudflare. (n.d.). *Magic Transit | DDoS protection for networks*. Retrieved from https://www.cloudflare.com/network-services/products/magic-transit/
- GigaNetworks. (n.d.). *Palo Alto Networks IDS/IPS solution*. Retrieved from https://giganetworks.com/products/ids-ips-solutions/palo-alto-networks/
- Juniper Networks. (n.d.). *What is IDS/IPS?* Retrieved from https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html?utm_source=chatgpt.com
- Palo Alto Networks. (n.d.). *IPS vs. IDS vs. firewall: What are the differences?*. Retrieved from https://www.paloaltonetworks.com/cyberpedia/firewall-vs-ids-vs-ips