Public-Facing Network Scanning

All code needs to be tested for flaws, and given the types of attacks that work on a given type of code change as threat actors develop new techniques, deployed code needs to be tested regularly for known vulnerabilities.

For public-facing assets, various types of scanning can find known vulnerabilities and provide reports that prioritize them based on standardized severities. These scanning tools are automated and can run regularly to always keep you informed of your progress and any new issues due to changes you make or the evolving threat environment.

Common types of scanning or network testing include:

- Vulnerability Scanning: Reviews public-facing websites for vulnerabilities.
- Web application scanning: Reviews public-facing applications for vulnerabilities.
- Remote penetration testing: A more advanced method of using known tactics to simulate attacks and find more difficult to exploit vulnerabilities.

Goals

1. Deploy scanning tools on your public-facing assets (Level 1 maturity)
2. Deploy web application scanning tools (Level 1 maturity)
3. Use penetration testing to harden networks (Level 2 maturity)

Actions

For Public-Facing Network Scanning, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

1. Use free tools and services to conduct scans of your publicly-facing assets. This should include your website and any online portals you are responsible for that are used for elections purposes. CISA offers all of its cybersecurity assessment services at no cost to election offices.
   - Sign up for free vulnerability scanning by contacting CISA at vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services.”
   - If you have web applications, sign up for free web application scanning at vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services.”
2. Remediate any vulnerabilities or known issues found during the scans.

Note that scanning online systems you do not own may run afoul of the Computer Fraud and Abuse Act of 1986 (CFAA).

Level 2 and Level 3 Maturity

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Implement remote penetration testing.
   - Sign up for free remote penetration testing by contacting CISA at vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services.”
2. Sign up for the EI-ISAC’s Vulnerability Disclosure Program to allow the wide-ranging talent of security researchers to improve the security of your systems.

Cost-Effective Tools

- CISA Cyber Hygiene Services: CISA offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. Types of scans and assessments include vulnerability scanning, web application scanning, phishing campaign assessments, and remote penetration testing.
- ShieldsUP!: ShieldsUP is an online port scanning service that can alert the users of any ports that have been opened through their firewalls or through their NAT routers, which can be used by malicious users to take advantage of security vulnerabilities.

Mapping to CIS Controls and Safeguards

- 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
- 7.7: Remediate Detected Vulnerabilities

Mapping to CIS Handbook Best Practices

- 2, 19

Previous
Managing Wireless Networks

Next
Website Security