GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: RedLegg Blog

Title: "Why the Network Is Central to IoT Security"

Website: RedLegg Blog

Organization: RedLegg Cybersecurity Solutions

Date: 21 February 2019

URL: https://www.redlegg.com/blog/6-steps-of-vulnerability-scanning-best-practices

Accessed: 19 Oct 2019

Synopsis: Vulnerability scanning (vuln-scan) is the process of finding exploits, flaws, security holes, insecure access entry points to systems, and system misconfigurations. While vulnerability scanning is usually focused on systems connected to the internet, systems behind firewalls within secure internal networks should also be part of the engagement scope.

Scanning is an automated process using special-purpose tools to assess the security protection status of network assets. Each device in a network is an asset component with certain value to the business, measured by its importance to business services and the impact on the services availability. The scope of a vuln-scan can cover the entire network assets or be limited to a specific set of assets within the network.

In a world of attackers working faster than security professionals to exploit vulnerable systems, security protection to business assets is a clear and strict goal for enterprises today.

6 Steps of Vulnerability Scanning Best Practices

RedLegg Blog

View RedLegg's Pen Test Offerings

Vulnerability scanning (vuln-scan) is the process of finding exploits, flaws, security holes, insecure access entry points to systems, and system misconfigurations. While vulnerability scanning is usually focused on systems connected to the internet, systems behind firewalls within secure internal networks should also be part of the engagement scope.

Scanning is an automated process using special-purpose tools to assess the security protection status of network assets. Each device in a network is an asset component with certain value to the business, measured by its importance to business services and the impact on the services availability. The scope of a vuln-scan can cover the entire network assets or be limited to a specific set of assets within the network.

In a world of attackers working faster than security professionals to exploit vulnerable systems, security protection to business assets is a clear and strict goal for enterprises today.

Penetration testing is different than vulnerability scanning: vuln-scan finds the system security holes, while penetration testing intentionally exploits those holes to gain access to those systems.

Access the Free Guide to Selecting the Right Test Vendor for Your Business.

Vulnerability Scanning Best Practices

1. Scan every device that touches your ecosystem
2. Scan frequently
3. Assign owners to critical assets
4. Prioritize the patching process
5. Document all scans and their results
6. Establish a remediation process

1. Scan every device that touches your ecosystem

Failing to scan every device and access point leaves your network and systems open to weaknesses. Gaining knowledge about possible weaknesses in your network keeps you aware. Scanning all assets within the ecosystem helps bring to light the various vulnerabilities within the infrastructure and allows formulation of a remediation plan or acceptance of risk. Additionally, create an inventory list including all devices in the network regardless of their function, and decide which targets to include in the

vulnerability scanning list from your inventory.

2. Scan frequently

The time interval between a vuln-scan and the next scan is a risk factor, because this gap between scans leaves your systems open to new vulnerabilities. Scanning weekly, monthly, or quarterly is a decision you have to make, and to be aware of its impact on your business. Not every device in your network would need a weekly scan, and not every device should be on the list of every quarterly scan.

Your network architecture, device impact on the network, and other factors are the deterministic factors to decide the vulnerability scanning frequency for devices.

3. Assign owners to critical assets

Accountability for each asset determines the distribution list of asset owners: who is responsible about keeping that device patched, and who is the affected audience if that device is compromised.

Keep in mind that asset owners are not limited to technical teams; there should be a business owner specifically accountable for each system.

4. Prioritize the patching process

Patching internet-facing devices for all discovered vulnerabilities is more important that patching similar devices that have already been blocked by settings or firewalls.

Prioritizing does not mean neglecting; it is a time-management practice that is required due to resource limitations. It is essential to focus on assets that provide the highest risk levels to the organization.

5. Document all scans and their results

Every vulnerability scan should be scheduled using a management-approved timetable, with an audit process mandated to provide detailed reports covering each scan and its results.

By documenting the scan run according to its approved timetable, your organization can track vulnerability trends and issue recurrence, uncovering susceptible systems and establishing accountability.

Reports should be readable to technically savvy business teams to certain extent, but should also be accessible to non-technical management and high-level personnel, without requiring interpretation.

6. Establish a remediation process

With documented scans results in place and a priority assigned to each device, the remediation process should dictate specific levels of severity and the urgency to remediate each discovered vulnerability, including the required timeframe.

The remediation process should be documented as part of the 6-steps framework.

Use vulnerability scanning to your advantage.

Establish a framework that cover the 6 steps of the process, document it, and use it to execute the vulnerability scanning process. Do not ignore management buy-in or fully understanding the process, the value, and the cost on the business if you don't complete a scan.

View RedLegg's Pen Test Offerings

Want more? Read...

- how vulnerability scanning works
- how to read a vulnerability assessment report
- vulnerability scans and assessments contribute to the pen testing process