CyRadar Website Vulnerability Assessment

Giới thiệu

- CyRadar Website Vulnerability Assessment (CyRadar WVA) thực hiện rà quét, phát hiện và vẽ ra bức tranh toàn cảnh về tình trạng an ninh, số lượng điểm yếu, lỗ hổng của website. Điều này cho phép quản trị viên nắm được thực trạng chi tiết an ninh của website, từ đó dễ dàng khoanh vùng và thực hiện các biện pháp xử lý, khắc phục để đảm bảo an toàn cho website.
- CyRadar WVA cho phép PHÁT HIỆN và HỖ TRỢ KHẮC PHỤC các nguy cơ an ninh cho hệ thống website trước khi cuộc tấn công diễn ra

Năng lực hệ thống

Tiêu chí	Năng lực
Số lượng mã nhận diện lỗ hổng /điểm yếu an ninh	> 20.000
Số lượng script để phát hiện lỗ hổng đặc thù hoặc thực hiện kiểm thử xâm nhập tự động.	> 1.000
Số lượng mã nhận diện cập nhật hàng tháng	> 100

Cách hoạt động

CyRadar WVA sẽ tự động rà quét, phát hiện các điểm yếu an ninh CỦA WEBSITE. Mọi hành động đánh giá an ninh WVA đều được thực thi tự động và định kỳ. Bất kỳ dấu hiệu bất thường nào đều được cảnh báo tức thì tới quản trị viên.

Tính năng kỹ thuật

1. Thu thập thông tin (Information Gathering)

- Phát hiện các thông tin liên quan tới máy chủ Web, hệ điều hành máy chủ, phiên bản phần mềm.
- Phát hiện ngôn ngữ lập trình: PHP, Java, .Net, JS.
- Phát hiện thông tin về cổng và dịch vụ.
- Phát hiện các thông tin liên quan tới nền tảng phát triển Website: Joomla, CakePHP, Wordpress, Sharepoint, Drupal.
- Rà quét thông tin cấu trúc website, liệt kê toàn bộ các đường dẫn có thể thu thập được đối với website đó.

2. Rà quét (Discover)

- Rà quét các lỗ hổng nguy hiểm nhất của Website: SQL injection, Blind SQL injection, Command injection, PHP Code injection, Directory Traversal, XSS.
- Phát hiện lộ lọt các thông tin nhạy cảm (tài khoản mặc định, mật khẩu yếu).
- Phát hiện các lỗi có nguy cơ lộ lọt thông tin: Directory Listing, Script Source Code Disclosure, Application Error Message, .htaccess File Readable.
- Kiểm tra cấu hình an ninh của một Webserver.
- Kiểm tra các nguy cơ liên quan tới upload dữ liệu và nguy cơ bị Hacker upload mã độc để chiếm quyền điều khiển hệ thống.
- Rà quét, phát hiện Website bị đưa vào blacklist.
- Rà quét nguy cơ với các Website cần đăng nhập.
- Rà quét đa luồng tốc độ cao có thể thu thập dữ liệu. Cơ sở dữ liệu với hơn 40000 plugin phát hiện và kiểm thử lỗ hổng an ninh
- Cập nhật plugin hàng tuần
- Thông tin chi tiết các lỗ hổng theo các chuẩn về lỗ hổng an ninh CVE, CPE và OVAL.

3. Kiểm thử xâm nhập (Penetration testing)

Kiểm tra thâm nhập với các lỗ hổng mức độ nghiêm trọng, có mã khai thác

4. Cảnh báo/Thông báo (Alert/Notify)

- Phát hiện, cảnh báo tức thời các lỗ hổng/nguy cơ có khả năng khai thác thông qua Email/OTT.
- Tự động gửi thông báo hiện trạng an ninh của toàn hệ thống hàng tuần qua email

5. Khắc phục (Remediation)

- Có đề xuất khắc phục đối với từng lỗ hổng: Mô tả, Sự ảnh hưởng, Giải pháp, Thông tin dường dẫn, tham số
- Có khả năng ghi nhớ lỗ hổng cảnh báo nhầm (false positive)

7. Báo cáo (Report)

- Hỗ trợ xuất báo cáo định dạng word (docx), excel (xlsx)...,tạo báo cáo sau mỗi lần thực hiện rà quét Hỗ trợ các loại báo cáo tổng quan, báo cáo chi tiết cho từng dường dẫn thiết bị, lỗ hổng, báo cáo hỗ trợ sửa lỗi
- Báo cáo theo các chuẩn an ninh quốc tế
- Hỗ trợ xuất báo cáo đa ngôn ngữ: Tiếng Anh, Tiếng Việt

CyRadar Network Vulnerability Assessment

Giới thiệu

- CyRadar Network Vulnerability Assessment (CyRadar NVA) thực hiện rà quét, phát hiện và vẽ ra bức tranh toàn cảnh về tình trạng an ninh, số lượng điểm yếu, lỗ hổng của máy chủ, thiết bị mạng. Điều này cho phép quản trị viên nắm được thực trạng chi tiết an ninh, từ đó dễ dàng khoanh vùng và thực hiện các biện pháp xử lý, khắc phục để đảm bảo an toàn cho máy chủ, thiết bị mạng.

- CyRadar NVA cho phép PHÁT HIỆN và HỖ TRỢ KHẮC PHỤC các nguy cơ an ninh cho hệ thống mạng trước khi cuộc tấn công diễn ra.

Năng lực hệ thống

Tiêu chí	Năng lực
Số lượng mã nhận diện lỗ hổng/điểm yếu an ninh	> 120.000
Số lượng script để phát hiện lỗ hổng đặc thù hoặc thực hiện kiểm thử xâm nhập tự động.	> 1.000
Số lượng mã nhận diện cập nhật hàng tháng	> 500
Số lượng kiểu thiết bị được hỗ trợ (Máy tính, máy in...)	> 1.000

Cách hoạt động

CyRadar NVA đứng bên trong firewall và tham gia vào hệ thống như một thiết bị bình thường, được cấu hình để kết nối logic được đến toàn bộ thiết bị trong hệ thống mạng.

CyRadar NVA sẽ tự động rà quét, phát hiện các điểm yếu an ninh. Mọi hành động đánh giá an ninh của NVA đều thực thi tự động và định kỳ. Bất kỳ dấu hiệu bất thường nào đều được cảnh báo tức thì tới quản trị viên.

Tính năng kỹ thuật

1. Thu thập thông tin (Information Gathering)

- Phát hiện các thiết bị trong hệ thống mạng bao gồm: Firewall, Router, máy chủ, máy tính, máy in, camera, các thiết bị wifi, các thiết bị IoT...
- Phát hiện các thông tin cơ bản: thông tin cổng, dịch vụ, phiên bản tương ứng, thông tin hệ điều hành.
- Phát hiện thiết bị trong mạng: địa chỉ IP, Hệ điều hành, Địa chỉ MAC, Hostname

2. Rà quét (Discover)

- Rà quét, phát hiện các lỗ hổng/điểm yếu hệ điều hành
- Rà quét, phát hiện các lỗ hổng/điểm yếu phần mềm
- Rà quét, phát hiện các lỗ hổng/điểm yếu dịch vụ và giao thức mạng như: SSH, SMB.
- Thông tin chi tiết các lỗ hổng theo các chuẩn về lỗ hổng
- an ninh CVE, CPE và OVAL
- Cơ sở dữ liệu với hơn 110000 plugin phát hiện và kiểm
- thử lỗ hổng an ninh
- Cập nhật plugin hàng tuần

3. Kiểm thử xâm nhập (Penetration testing)

Kiểm tra thâm nhập với các lỗ hổng mức độ nghiêm trọng, có mã khai thác

4. Cảnh báo/Thông báo (Alert/Notify)

- Phát hiện, cảnh báo một số các bất thường xảy ra với hệ thống mạng như việc có sự biến động tăng/giảm về số lượng cổng/dịch vụ trên thiết bị; biến động về số lượng thiết bị tham gia vào hệ thống mạng.
- Phát hiện, cảnh báo tức thời các lỗ hổng/nguy cơ có khả năng khai thác thông qua Email/OTT.
  Tự động phát hiện và gửi cảnh báo tức thì qua Email,
- OTT: Thiết bị mới hoặc có sự bất thường trong mạng, Cảnh báo phát hiện lỗ hổng có khả năng xâm nhập
- Tự động gửi thông báo hiện trạng an ninh của toàn hệ thống hàng tuần qua email

5. Khắc phục (Remediation)

- Có đề xuất khắc phục đối với từng lỗ hổng: Mô tả, Sự ảnh hưởng, Giải pháp, Thông tin Cổng/Dịch vụ, địa chỉ IP
- Theo dõi số lượng lỗ hổng đã khắc phục và chưa khắc phục qua giao diện quản trị
- Ghi dấu, theo dõi, giám sát quá trình: Ghi nhật ký khắc phục, Có thể tự ghi chú vào từng lỗ hổng
- Có khả năng ghi nhớ lỗ hổng cảnh báo nhầm (false positive)

6. Giám sát (Monitor)

- Phát hiện, cảnh báo thông tin lỗ hổng/điểm yếu
- Phát hiện, cảnh báo một số các bất thường xảy ra với hệ thống mạng như việc có sự biến động tăng/giảm về số lượng cổng/dịch vụ trên thiết bị; biến động về số lượng thiết bị, Ghi dấu lịch sử trạng thái bất thường trong mạng
- Giám sát liên tục 24/7, phát hiện và cảnh báo sớm các tấn công có chủ đích APT.
- Ghi dấu lịch sử trạng thái an ninh hệ thống, lịch sử rà quét mục tiêu tham gia vào hệ thống mạng.

7. Báo cáo (Report)

- Hỗ trợ xuất báo cáo định dạng word (docx), excel (xlsx)...,tạo báo cáo sau mỗi lần thực hiện rà quét.
- Hỗ trợ các loại báo cáo tổng quan, báo cáo chi tiết cho từng thiết bị, lỗ hổng, báo cáo hỗ trợ sửa lỗi
- Báo cáo theo các chuẩn an ninh khác nhau
- Hỗ trợ xuất báo cáo đa ngôn ngữ: Tiếng Anh, Tiếng Việt

8. Quản lý (Management)

- Quản lý nguy cơ an ninh theo từng phòng ban, tổ chức và vẽ ra sơ đồ hệ thống
- Cấu hình mạng và các thông số cho thiết bị thông quan giao diện quản trị
- Tổng hợp và thống kê nguy cơ an ninh của hệ thống từng gặp phải theo thời gian
- Lập lịch quét an ninh định kỳ: Hàng ngày, Hàng tuần, Hàng tháng
- Hỗ trợ xem và theo dõi: lịch sử cập nhật lỗ hổng và phần mềm, Cơ sở dữ liệu lỗ hổng của thiết bị, Thông tin về phần cứng, Thông tin bản quyền
- Hỗ trợ cấu hình và cài đặt: Thông số mạng, Cài đặt máy chủ email, Sao lưu dữ liệu dự phòng
- Hỗ trợ tích hợp hệ thống quản trị nguy cơ tập trung diện rộng, có khả năng thích nghi với mọi hệ thống mạng khác nhau.