Dmitry (email, subdomain, whois, quet TCP, lay thong tin tu Netcraft)

Whois (thu nhap thong tin may chu)

TheHarvester (email, subdomain, whois, quet TCP, lay thong tin tu Netcraft)

Sslscan (liệt kê các bộ mã hóa và chứng chỉ trên máy chủ)

DNSenum (thu nhap thong tin DNS: dia chi ip, name server, bruteforces subdomain)

Nmap ( quet cong port, xac dinh he dieu hanh, quet lo hong bao mat)

Netcat (port scan, truyen du lieu 2 may, lang nghe ket noi den)

Uniscan (quet lo hong bao mat SQL Injection, XSS, quet nhieu site cung luc, … )

Nikto (cau hinh phia may chu, may chu hoac phan mem sai sot, file, lo hong, do loi qua port hoac proxy)

Skipfish (danh gia bao mat)

Amap (check cac ung dung dang chay port)

GoBuster (bruteforces URL, DNS subdomain, 3 mode DIR (dò url), DNS, vHOST (dò host))

Sitadel (quet lo hong, quet tinh, quet dong, tao bao cao)

Darkjumper (quet lo hong, dinh danh user tren server, ho tro proxy, quet cong, lay thong tin header , check FTP co cho phep nguoi dung an danh)

WPScan Tool (quet lo hong WordPress, viet bang Ruby, thu nhap username, do mat khau, ..)

------------------------------------------------------------

SQLmap (quet lo hong SQL, do mat khau, .. )

SQLmapGUI

Tlssled (danh gia bao mat, dua tren ssls scan)

Xsser (khai thac loi xss)

Cac cong cu GUI

Brup Suite (proxy chan va chinh sua luu luong https, quet lo hong bao mat, do mat khau)

ZAP (quet lo hong bao mat, quet lo hong qua proxy)

BeEF (quet lo hong bao mat trinh duyet)

OpenVas (quet lo hong cac thiet bi mang, quet lo hong he dieu hanh)

Metasploit (tan cong xam nhap kiem thu, phat trien he thong phat hien xam nhap)

BlueKeep (lo hong WinXP)

**OWASP Top 10**, danh sách các lỗ hổng bảo mật phổ biến và nguy hiểm nhất trong ứng dụng web

Tấn công Path traversal là kỹ thuật cho phép hacker truy cập đến những file/thư mục bị giới hạn của máy chủ web

Lỗ hổng File Inclusion cho phép tin tặc truy cập trái phép vào những tập tin nhạy cảm trên máy chủ web hoặc thực thi các tệp tin độc hại bằng cách sử dụng chức năng “include”.

CSRF (Cross Site Request Forgery) là kỹ thuật tấn công vào người dùng bằng cách sử dụng quyền chứng thực của người dùng đối với một website.

 **ssh sv102102102@wandertour.ddns.net** (Truy cập từ xa vào máy OpenStack).

 **openstack –help** (Hiển thị danh sách các lệnh của OpenStack).

 **ping 192.168.x.x** (Kiểm tra kết nối mạng tới một địa chỉ IP cụ thể).

 **df -h** (Hiển thị dung lượng ổ đĩa đang sử dụng theo định dạng dễ đọc).

 **cat /etc/hosts** (Hiển thị nội dung của tệp /etc/hosts).

 **nova quota-show** (Hiển thị thông tin về giới hạn tài nguyên của OpenStack).

 **neutron quota-show** (Hiển thị thông tin về giới hạn tài nguyên của Neutron).

 **openstack token issue** (Hiển thị token từ dịch vụ Keystone).

 **nova service-list** (Hiển thị danh sách các dịch vụ Nova đang chạy).

 **neutron net-create intnetXYZ01** (Tạo mạng nội bộ mới có tên intnetXYZ01).

 **neutron subnet-create** (Tạo một subnet cho mạng).

 **openstack network list** (Liệt kê tất cả các mạng trong hệ thống).

 **neutron port-list --device\_owner network**

(Hiển thị các cổng DHCP trong Neutron).

 **neutron router-create routerXYZ01** (Tạo router mới có tên routerXYZ01).

 **neutron router-interface-add routerXYZ01 subnetXYZ01** (Thêm subnet vào router).

 **openstack security group list** (Liệt kê các nhóm bảo mật).

 **nova secgroup-add-rule default tcp 22 22 0.0.0.0/0** (Thêm quy tắc cho phép kết nối SSH).

 **openstack keypair create** (Tạo cặp khóa SSH mới).

 **nova flavor-list** (Liệt kê các loại cấu hình máy ảo có sẵn).

 **openstack image list** (Liệt kê các ảnh hệ điều hành có sẵn trong OpenStack).

 **openstack floating ip list** (Liệt kê các địa chỉ IP floating đã được cấp).

 **openstack server create** (Tạo máy ảo mới).

 **openstack network create --share --external** (Tạo mạng ngoài mới).

 **nova list** (Hiển thị danh sách các máy ảo trong hệ thống).

 **openstack server reboot vmCirrosXYZ01** (Khởi động lại máy ảo).

 **openstack server delete vmCirrosXYZ01** (Xóa máy ảo).

 **openstack network agent list** (Hiển thị danh sách các tác nhân mạng trong hệ thống).

 **nova hypervisor-list** (Hiển thị danh sách các hypervisor).

 **openstack compute service list** (Liệt kê tất cả các dịch vụ compute).

 **openstack flavor create** (Tạo loại cấu hình máy ảo mới).

|  |  |  |
| --- | --- | --- |
| **TT** | **Nội dung cảnh báo** | **Giải thích** |
|  | Absence of Anti-CSRF Tokens | Cảnh báo (alert) của ZAP để chỉ một ứng dụng web bị thiếu các token Anti-CSRF. |
|  | Anti-CSRF tokens (hay CSRF tokens) | Cơ chế bảo vệ chống lại các cuộc tấn công CSRF (Cross-Site Request Forgery).  CSRF là một loại tấn công mà kẻ tấn công lừa một người dùng đăng nhập vào một trang web và sau đó sử dụng quyền truy cập của người dùng đó để thực hiện các hành động không mong muốn trên trang web đó.  NSD có thể edit các Alert bằng cách click vào chúng. |
|  | Missing Anti-clickjacking Header | Cảnh báo này xuất hiện khi ứng dụng web thiếu tiêu đề Anti-clickjacking (X-Frame-Options header) hoặc không đặt chính xác.  Tiêu đề này được sử dụng để ngăn chặn tấn công clickjacking, trong đó kẻ tấn công đưa nội dung độc hại vào một trang web khác và lừa người dùng nhấp chuột vào nó. |
|  | Cookie Poisoning | Cảnh báo cho thấy cookie trong ứng dụng web có thể bị tấn công bằng cách thay đổi nội dung của chúng.  Cookie là một thành phần quan trọng để duy trì trạng thái và xác thực trong các ứng dụng web, và khi bị nhiễm độc, nó có thể dẫn đến các hành vi không mong muốn hoặc vi phạm bảo mật. |
|  | Timestamp Disclosure | Cảnh báo này xuất hiện khi ứng dụng web tiết lộ thông tin về thời gian, chẳng hạn như thời gian tạo, sửa đổi hoặc xóa dữ liệu.  Thông tin về thời gian có thể cung cấp cho kẻ tấn công các gợi ý về cấu trúc hệ thống và thậm chí giúp tấn công theo thời gian (timing attacks). |
|  | Cookie without SameSite Attribute | Cảnh báo này khi cookie trong ứng dụng web không đặt thuộc tính SameSite hoặc không đặt chính xác.  Thuộc tính SameSite được sử dụng để xác định việc chia sẻ cookie giữa các trang web. Nếu không đặt đúng, có thể có nguy cơ tấn công CSRF hoặc thông tin đăng nhập bị rò rỉ. |
|  | Cookie Without Secure Flag | Cảnh báo này xuất hiện khi cookie không đặt cờ bảo mật (Secure flag) khi được truyền đi. Cờ bảo mật chỉ ra rằng cookie chỉ được gửi qua kết nối an toàn HTTPS, giúp ngăn chặn tấn công lắng nghe (eavesdropping) và đánh cắp thông tin đăng nhập. |
|  | Information Disclosure | Cảnh báo này xuất hiện khi ZAP phát hiện thông tin nhạy cảm hoặc thông tin quan trọng được tiết lộ trong phản hồi của ứng dụng web. Ví dụ, nó có thể là hiển thị thông tin về phiên làm việc, lỗi hệ thống, thông tin cấu trúc, hoặc thông tin đăng nhập không được bảo vệ. |
|  | Directory Listing | Cảnh báo này xuất hiện khi ZAP tìm thấy thư mục trên máy chủ web được cấu hình để hiển thị danh sách các tệp tin bên trong. Điều này có thể tiết lộ thông tin quan trọng về cấu trúc và nội dung hệ thống. |
|  | Open Redirect | Cảnh báo này xuất hiện khi ứng dụng web cho phép chuyển hướng không an toàn từ một URL đến một URL khác nằm ngoài tầm kiểm soát của ứng dụng. Kẻ tấn công có thể lợi dụng điều này để lừa người dùng truy cập vào các trang web độc hại hoặc nguy hiểm. |
|  | Server Misconfiguration | Cảnh báo này xuất hiện khi ZAP phát hiện các lỗ hổng bảo mật liên quan đến cấu hình không chính xác của máy chủ web. Điều này có thể bao gồm việc bật các tính năng không cần thiết, thiết lập quyền truy cập không đúng, hay cấu hình SSL/TLS không an toàn. |
|  | Unvalidated Redirects and Forwards | Cảnh báo này xuất hiện khi ứng dụng web cho phép chuyển hướng hoặc chuyển tiếp yêu cầu người dùng mà không thực hiện kiểm tra đúng đắn. Điều này có thể dẫn đến khả năng tấn công chuyển hướng không an toàn hoặc chuyển tiếp không mong muốn. |