<NMAP>

1. Host Discovery (Ping Scan)

* Discovers live hosts on the network, knowing which devices are active in the environment which can be targeted for exploitation

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

1. Port Scanning

* Identify which services are running. HTTP on port 80 may be associated with vulnerable services. This port can be used as entry points to exploit known vulnerabilities.

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

1. Service Version Detection

* Identify the exact version of a service running on an open port. Knowing the version will allow the attackers to cross-reference it with known vulnerabilities (Older, unpatched versions of services can be vulnerable)

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

1. Operating System Detection

* Identifying the OS running on a device can provide link or hint to specific known vulnerabilities and potential weaknesses that each OS has its own set of vulnerabilities.

텍스트, 스크린샷, 폰트, 소프트웨어이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

1. Aggressive Scan

* OS detection, version detection, script scanning, and traceroute
* In-depth information about the target

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

1. Nmap Scripting Engine(NSE) Scanning

* Using scripts to scan automated, detailed known vulnerabilities
* nmap --script-help=all (list all available scripts)

Canning for multiple common vulnerabilities

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Service discovery (finding open ports/services)

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Authentication issues

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Heartbleed vulnerability

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

SMB-related vulnerabilities

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

1. TCP Connect Scan

* Can detect firewalls or intrusion detection system by completing full TCP handshake.

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

1. DNS interrogation

* Scanning DNS servers or performing brute force DNS queries can uncover subdomains or misconfigurations that attackers can exploit

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Name and Group Enumeration

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

script could not gather any user information. This is because the target system either isn't exposing SMB on this port, or a security device (firewall, IDS/IPS) is preventing the probe from reaching the service.

텍스트, 스크린샷, 폰트, 디자인이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

<Nikto>

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Find hidden directories, files, and paths (it does by testing common file and file directory names)

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Scans for vulnerabilities in CGI scripts (common gateway interface) used in web servers. CGI scripts are often used to process user input and generate dynamic content. Misconfigured or poorly coded CGI scripts may lead to remote code execution, directory traversal, or data leaks.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

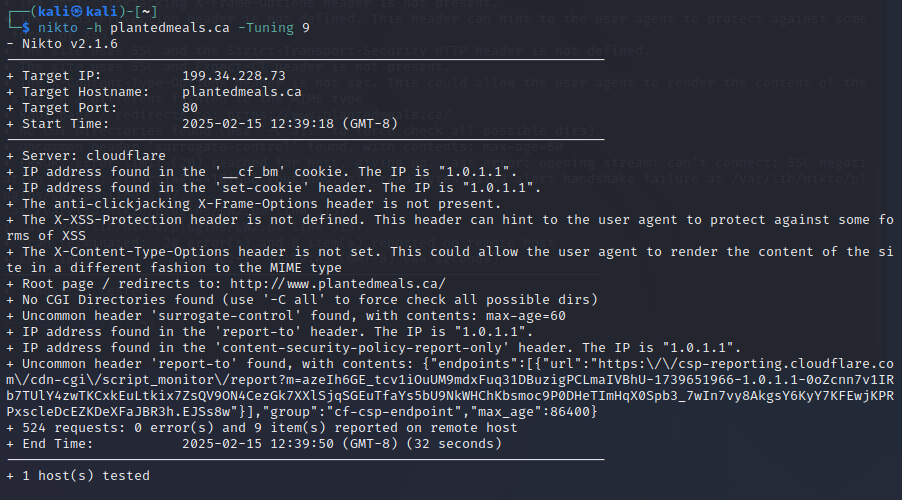
AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Scan the SSL/TLS configuration to check for insecure protocols or weak ciphers.

텍스트, 스크린샷, 소프트웨어, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Also checks security headers such as X-Content-Type-Options, X-Frame-Options, Strict-Transport-Security, and Content-Security-Policy.



Scan for known vulnerabilities in the web server. (since it is only checking port 80, I guess that is why we do not get any results)

텍스트, 스크린샷, 폰트, 소프트웨어이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Checks for default files, default configurations, and server banners that may have been left exposed. Default settings could provide attackers with access to administrative interfaces or system details.

Command : nikto -h <ipaddress> -Display V

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Scans for common web vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection flaws.

텍스트, 스크린샷, 폰트, 소프트웨어이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Enable directory traversal testing (allow access files outside of the web root directory)

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

<p0f>

Passive OS fingerprinting. It works by analyzing network traffic (such as SYN packets) already passing through the network. This makes it ideal for passive OS discovery without alerting the target.

sudo apt install p0f

sudo p0f -i eth0

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

It can be saved as pcap file and analyzed with wireshark

<enum4linux>

텍스트, 스크린샷, 폰트, 소프트웨어이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Not proper to use

<Whatweb>

Perform detailed fingerprinting of the technologies used by a web application, including the underlying **web server**, **operating system**, **database**, and other technologies.

텍스트, 스크린샷, 폰트, 소프트웨어이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Better to use command “whatweb -v plantedmeals.ca” since this gives more detailed information.

<Hydra>

Attempt to log into various services like SSH, FTP, HTTP, and more, using a list of common usernames and passwords

텍스트, 스크린샷, 폰트, 정보이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

try to brute-force login attempts on web applications and CMS platforms

텍스트, 스크린샷, 폰트, 정보이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.