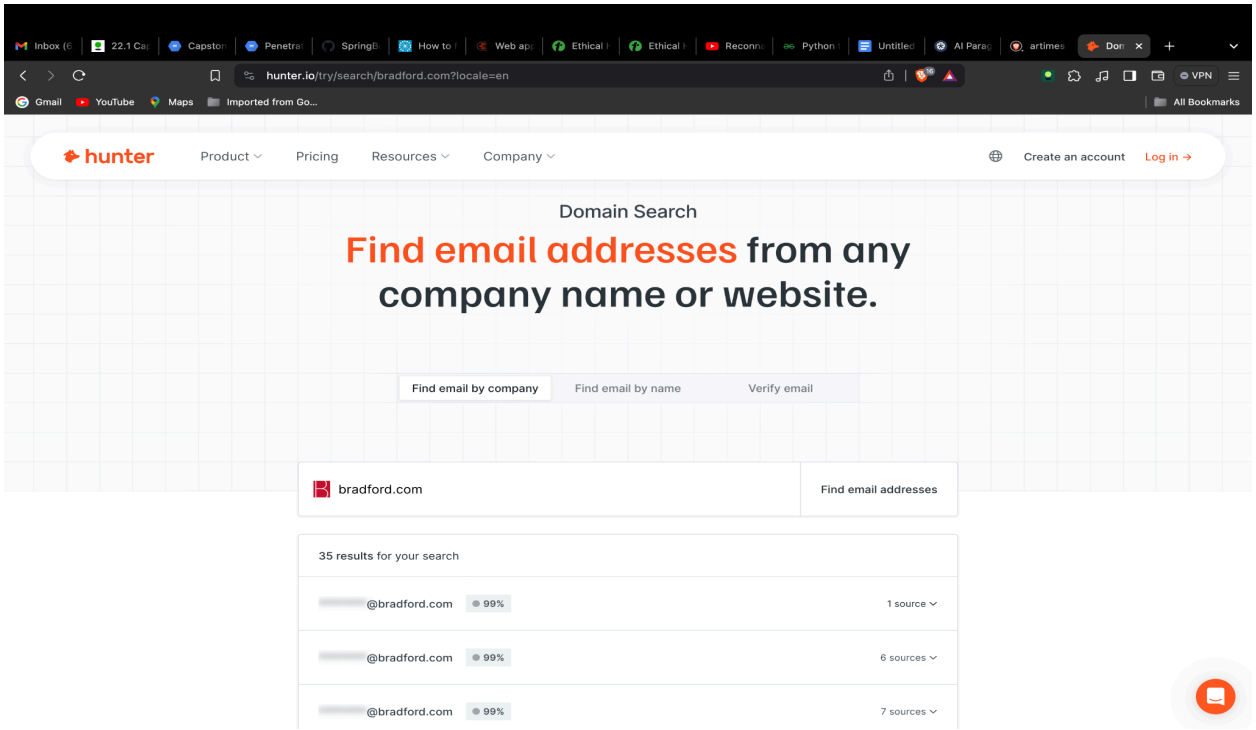
Reconnaissance is the act of gathering information or intelligence about an enemy or a situation. It involves observing and gathering details to better understand the surroundings or plan for future actions. During reconnaissance, individuals or groups may use various tools like maps, cameras, or even drones to collect data from a distance. This information is crucial for making informed decisions and developing strategies in military operations or other critical situations.

In everyday life, reconnaissance can also be applied for different purposes, such as market research or exploration. It helps individuals or businesses to assess opportunities, risks, and potential outcomes before making important decisions. By conducting reconnaissance, one can gain valuable insights that play a significant role in achieving success and avoiding possible pitfalls. So, whether in military operations or everyday scenarios, reconnaissance is a vital process for enhancing situational awareness and planning effectively

Here I am going to perform reconnaissance using 15 tools on different domains which are publicly available:

Tool 1:Hunter.io

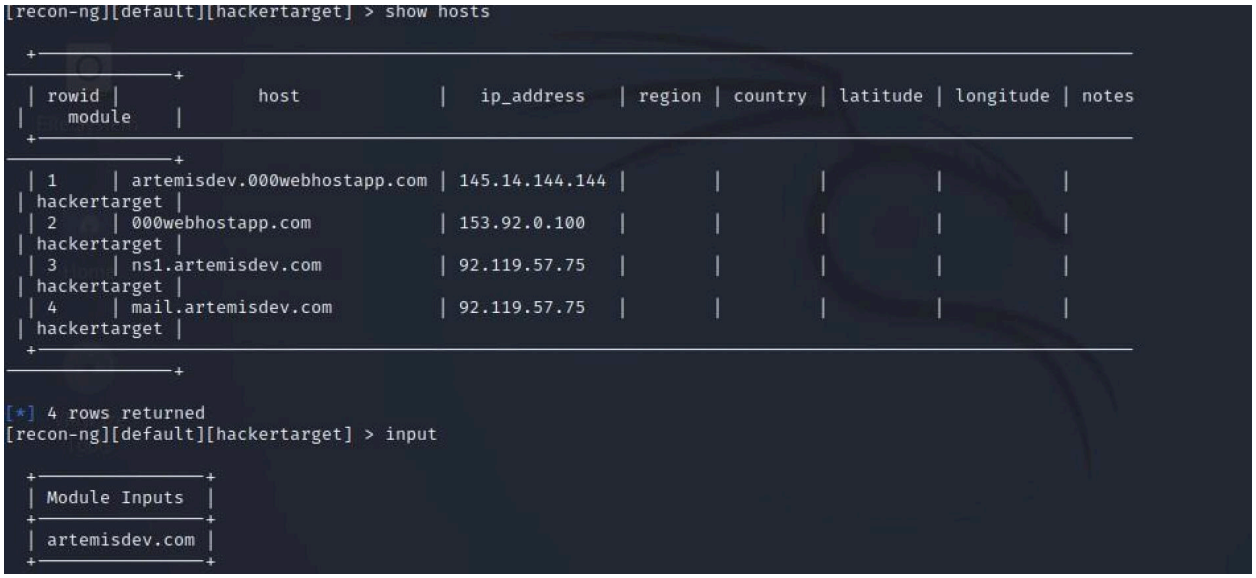
Hunter.io is a helpful tool used for finding email addresses. It searches for email addresses connected to a specific website or domain. Users can input the website name and Hunter.io will provide a list of email addresses associated with that website. It is a useful resource for contacting professionals or potential clients. Many businesses use Hunter.io to gather contact information efficiently.



The example above is used with bradford.com as a domain.

TOOL2:Recon-ng

Recon-ng is a tool used for gathering information with a user-friendly console. The hackertarget module is specifically utilized by the Artemis company to find subdomains. In this case, the source is artemisdev.com, which is displayed by using a command. When the command show hosts is executed, recon-ng identifies four hosts: Artemisdev.000webhostapp.com, 000.webhostapp.com, Ns1.artemisdev.com, and Mail.artemisdev.com. Each of these hosts serves a different purpose for the Artemis company.

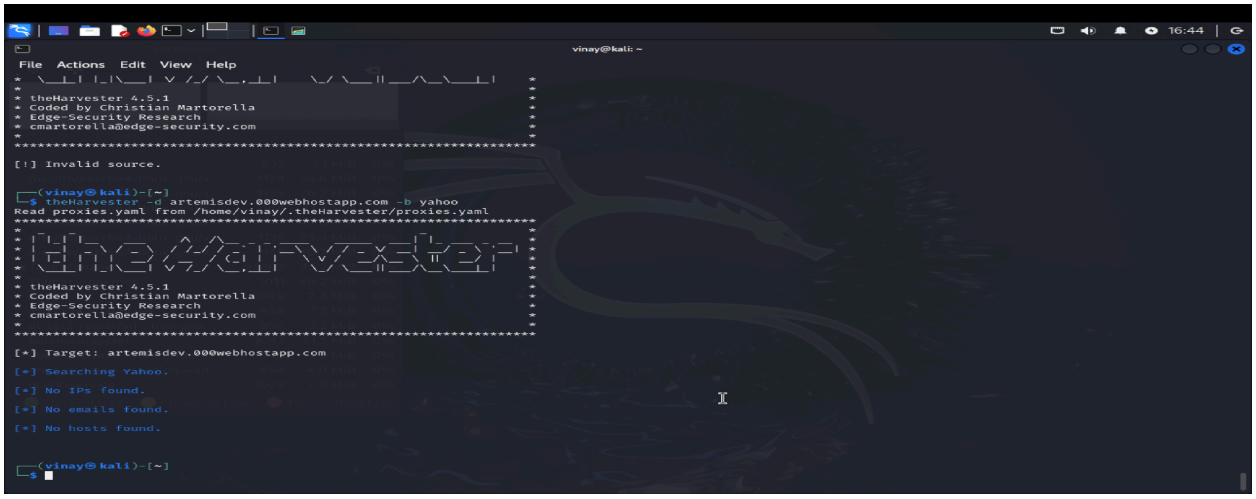


Tool3:theHarvester

theHarvester is a powerful tool used by cybersecurity professionals to gather information about an organization's online presence. It can help identify possible security vulnerabilities and weaknesses that could be exploited by cyber attackers. By utilizing theHarvester, security experts can obtain crucial data such as email addresses, domain names, and subdomains associated with the target organization.

This tool is instrumental in conducting reconnaissance activities to assess the digital footprint of a company, helping security teams proactively strengthen their defenses. Its capability to search across various sources on the internet makes it a valuable asset in threat intelligence gathering. Overall, theHarvester plays a vital role in enhancing cybersecurity measures by providing valuable insights into potential risks and aiding in the protection of sensitive information.

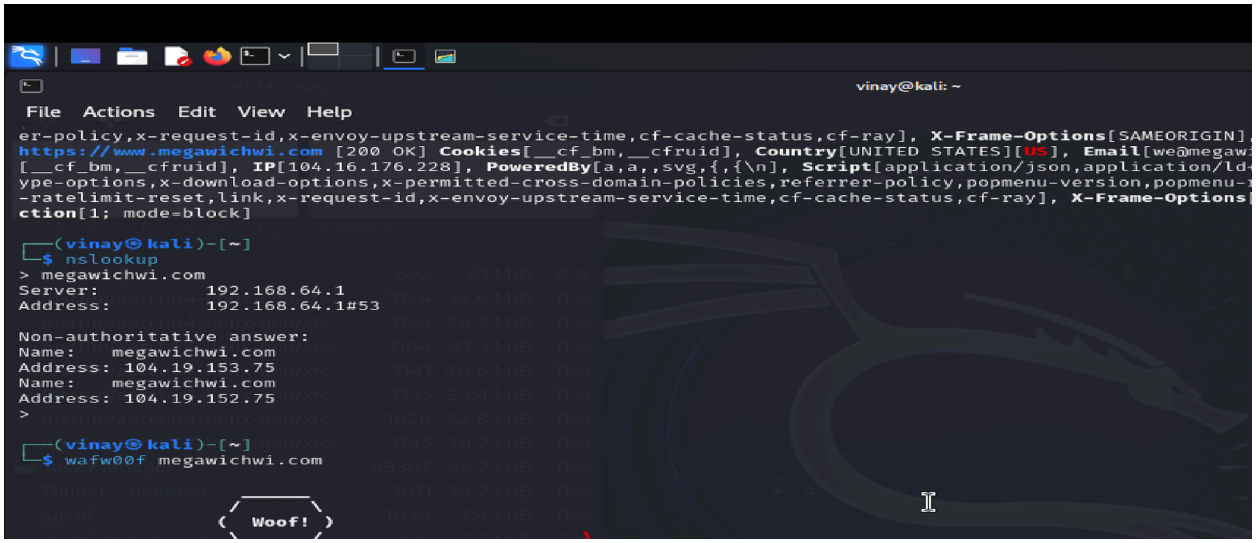
The below screenshot shows that i have performed theHarvester on the given company.



Tool4:nslookup

Nslookup is a useful tool that helps you find information about a specific domain or IP address. When you use nslookup, it sends a request to a DNS server to ask for details like the IP address associated with a domain name. This can be helpful in troubleshooting network issues or verifying the connectivity of a website. By entering the command in the command prompt or terminal, you can quickly access this information and gain insights into the online world.

Using nslookup is straightforward and can provide valuable information in just a few simple steps. By typing "nslookup" followed by the domain name or IP address, you can retrieve details such as the server name and its IP address. This can be particularly useful for system administrators or anyone wanting to quickly check the network settings of a website or server. With nslookup, you can easily gather the necessary information to understand the online presence of a specific domain or address.

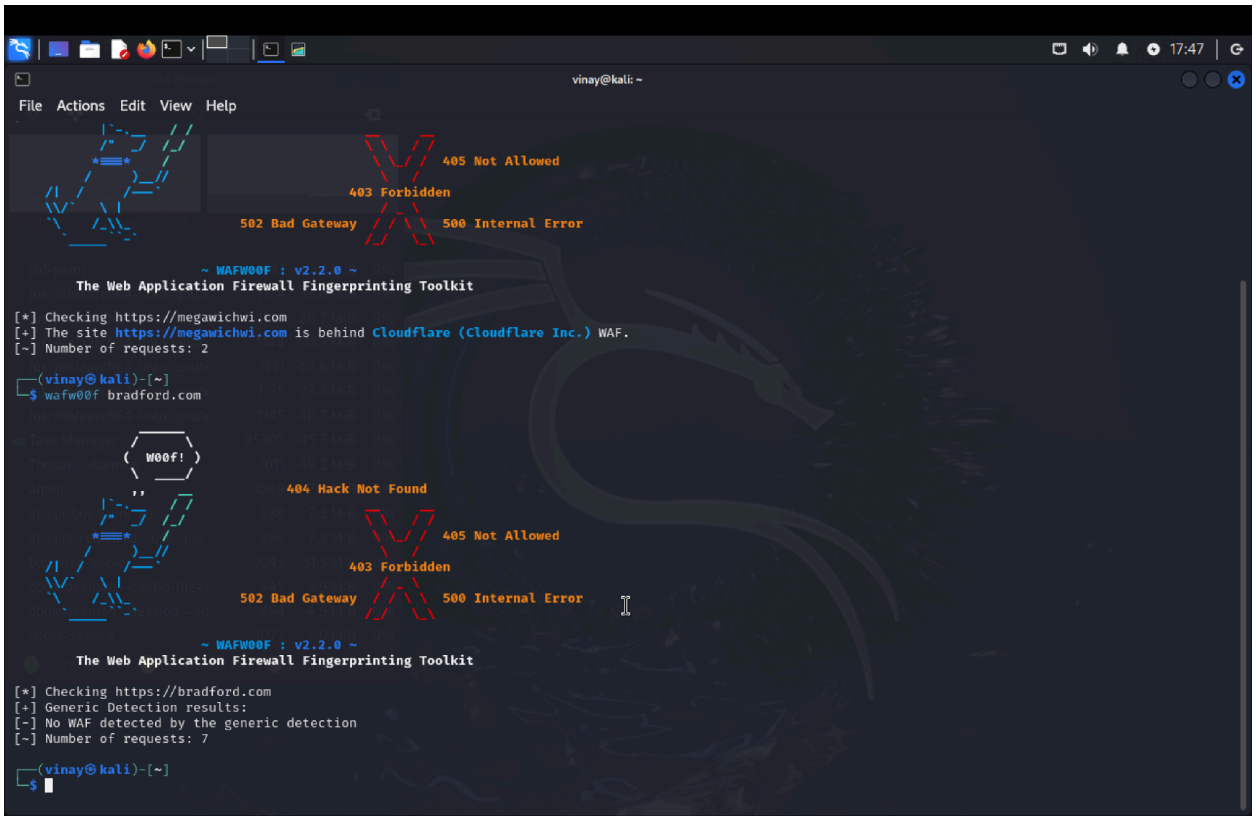


megawichwi.com as a domain name.

Tool:5 wafw00f

The Wafw00f tool is a helpful program that can identify and analyze web application firewalls (WAFs). It is designed to assist website owners and developers in understanding the security measures in place to protect their websites from cyber threats. By using the Wafw00f tool, users can determine if a WAF is actively safeguarding their web applications and explore its potential vulnerabilities. This tool aids in enhancing the overall security posture of websites by providing valuable insights that can be used to strengthen defenses against malicious attacks.

Moreover, the Wafw00f tool is user-friendly and easy to use, making it accessible to individuals with different levels of technical expertise. It scans websites efficiently and generates reports that highlight the presence of WAFs and their configurations. Users can leverage this information to make informed decisions about enhancing their website security and addressing any potential weaknesses in their WAF setup. Overall, the Wafw00f tool serves as a valuable resource for website security professionals and developers seeking to bolster the protection of their web applications against cyber threats.

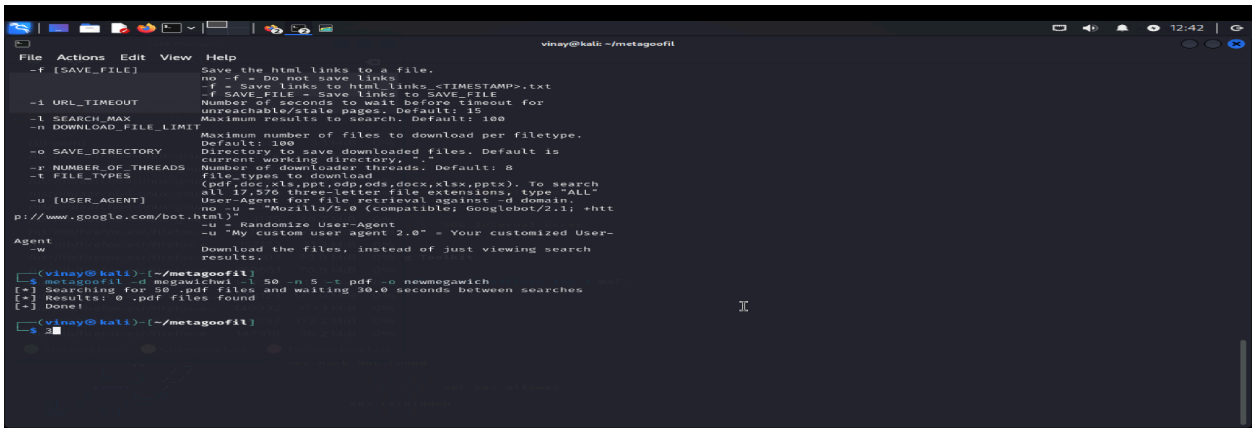


The above screenshot shows that I have performed wafw00f for two domains such as megawichwi.com and bradford.com and the results for the first domain it is behind cloudflare firewall.

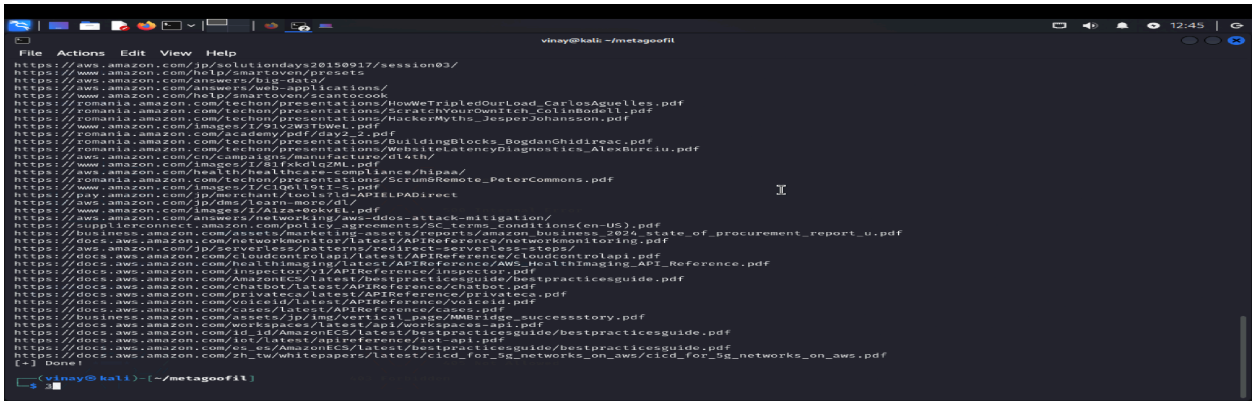
Tool:6 Metagoofil

Metagoofil is a tool used by cybersecurity professionals to gather information about a specific target by searching through metadata. It helps users extract and analyze valuable data such as usernames, file types, and locations from various online sources. By using Metagoofil, individuals can piece together information to gain a deeper understanding of a target's online footprint and potential vulnerabilities. This tool is commonly employed in digital investigations to aid in reconnaissance and intelligence gathering.

Security analysts utilize Metagoofil to conduct thorough research that can uncover critical details about a target's digital presence. By combing through metadata, users can identify potential security risks and vulnerabilities that may exist within a target's online files and documents. The information extracted with Metagoofil can assist in identifying weaknesses in a target's cybersecurity defenses and help organizations bolster their overall security posture. In summary, Metagoofil plays a crucial role in enhancing the cybersecurity analysis process and fortifying defenses against potential cyber threats.



The above figure shows that zero files has been downloaded for megawichwi.com domain

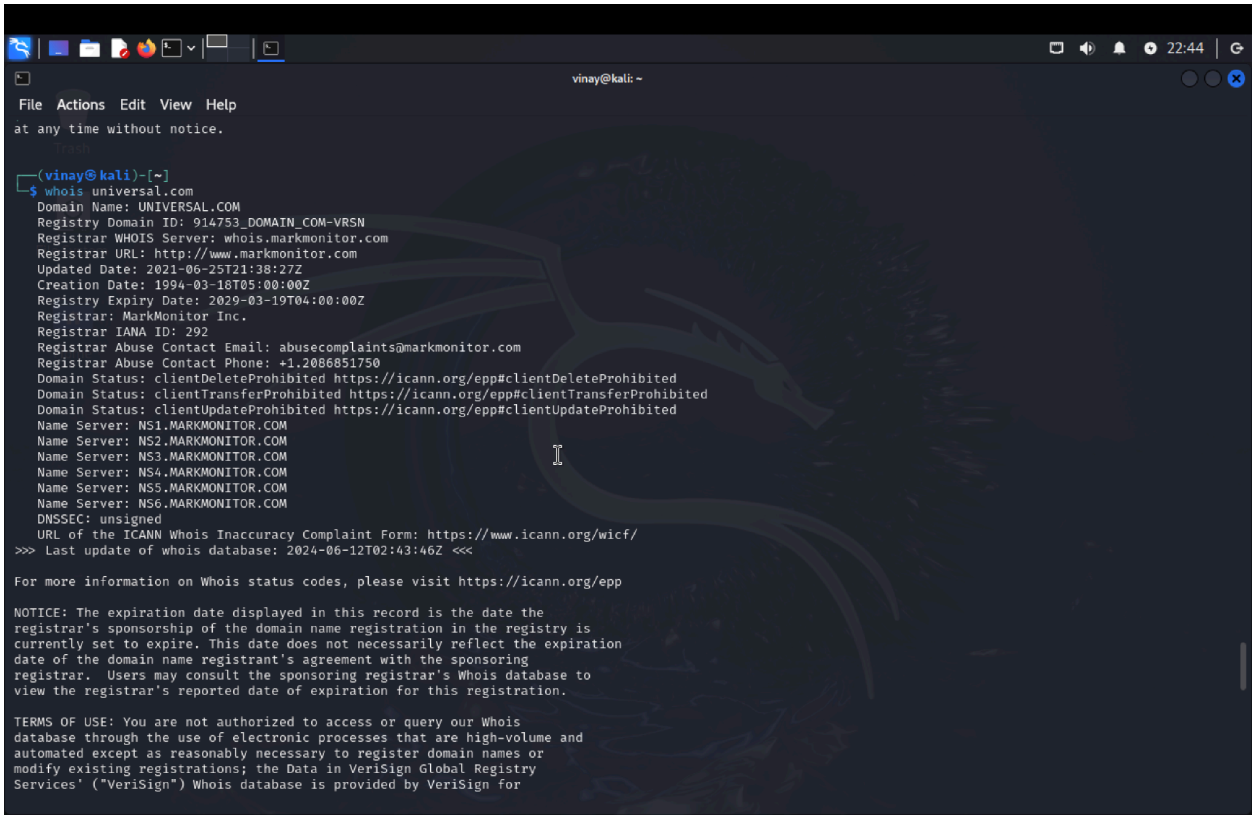


The above screenshot shows that 50 pdf's have been downloaded from the domain amazon.com after performing the metagoofil tool.

Tool :7 Whois

When you want to know who owns a website, you can find the information in a record called a "whois" record. The whois record contains details such as the website owner's name, contact information, and when the website was created. You can access the whois record of a website by using online tools that provide this information. Remember that not all websites may have a public whois record, as some owners choose to keep their information private. Checking the whois record can be helpful for understanding more about a website and its owner.

It is important to note that the information in a whois record can give you insights into the credibility and legitimacy of a website. By analyzing the details in the whois record, you can determine if a website is trustworthy or if it may be fraudulent. Understanding who owns a website can also help you in case you need to contact the owner for any reason, such as reporting an issue or seeking further information. Keeping in mind that the information in a whois record can vary depending on the website owner's preferences, it is still a valuable tool for anyone looking to learn more about a website's ownership.



Tool:8 Dig

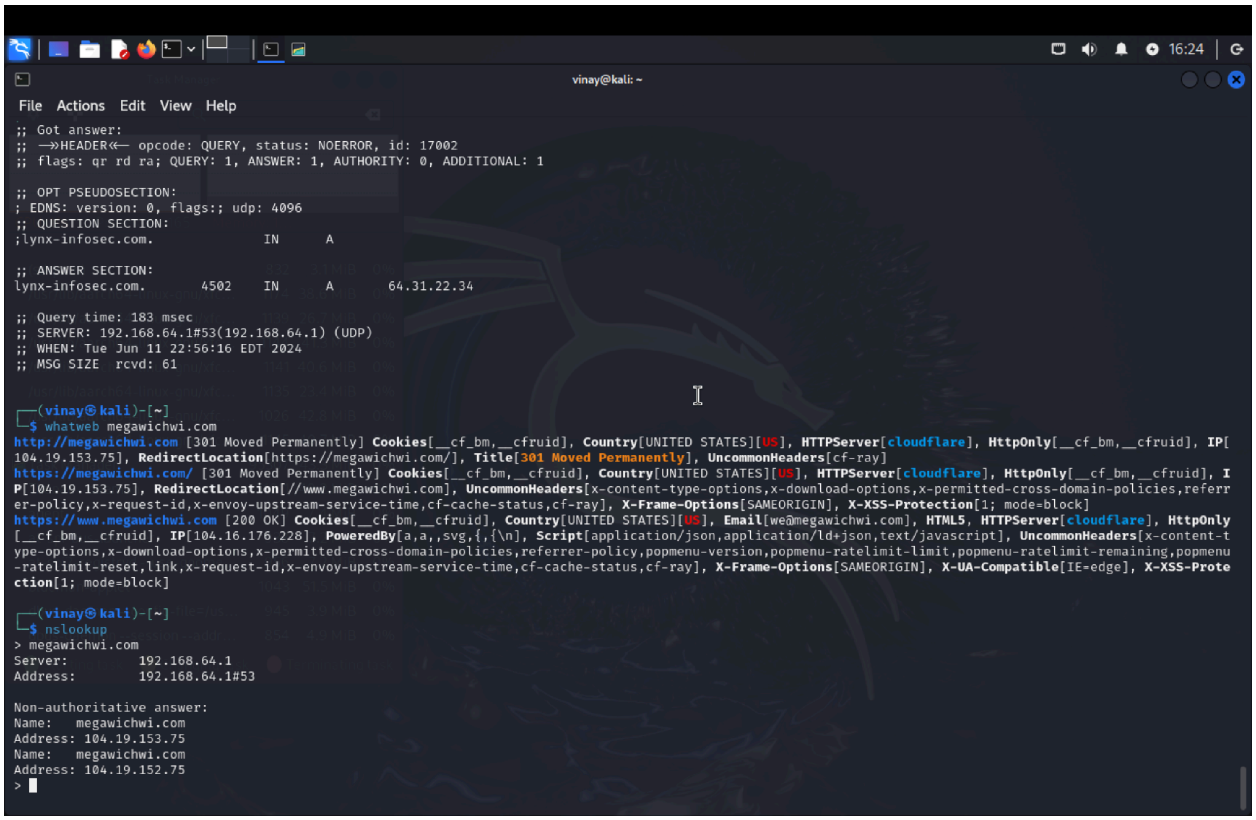
The "dig" command in Linux is a powerful tool used to query DNS (Domain Name System) servers. It helps in finding information about domain names, IP addresses, and name servers. By using the dig command, you can easily retrieve details like the IP address of a website, the name server responsible for a domain, and the time-to-live (TTL) value of a DNS record. This command is very useful for troubleshooting network issues, checking DNS configurations, and verifying the status of domain names. Overall, the dig command is an essential tool for anyone working with DNS and network administration.

The dig command can also be used to perform advanced DNS queries, such as retrieving specific types of DNS records like MX (Mail Exchange), SOA (Start of Authority), and NS (Name Server) records. It provides detailed information about the DNS responses received from the queried server, including the response code, flags, and additional records. Additionally, the dig command allows you to specify the DNS server to query, set the query type, and control the display format of the output. With its flexibility and versatility, the dig command is a valuable resource for analyzing and troubleshooting DNS-related issues in Linux systems.

Tool:9 whatweb

WhatWeb is a powerful tool that helps in identifying and gathering information about websites. It is designed to search for details such as server type, software versions, and technologies used on a website. By analyzing this data, WhatWeb enables users to understand the structure and components of a website effectively. This feature allows for better assessment and security

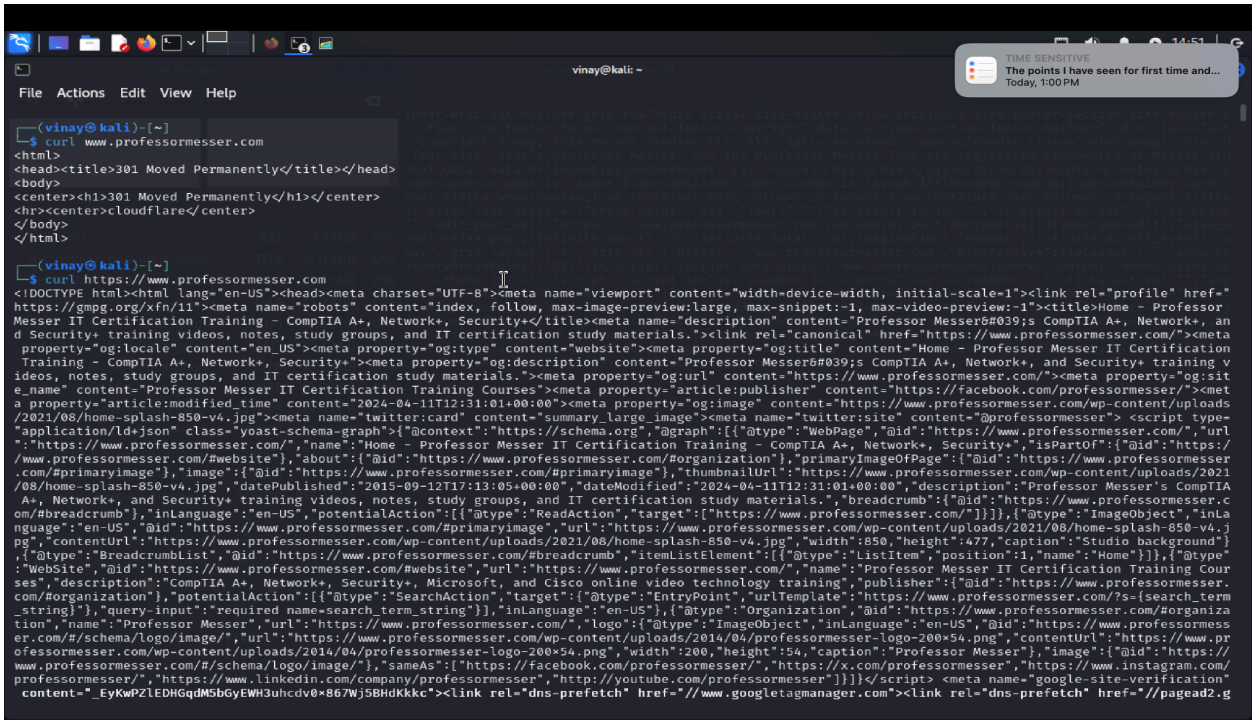
evaluation of websites. Overall, WhatWeb is an essential tool for professionals involved in website development and cybersecurity.



Tool:10 Curl

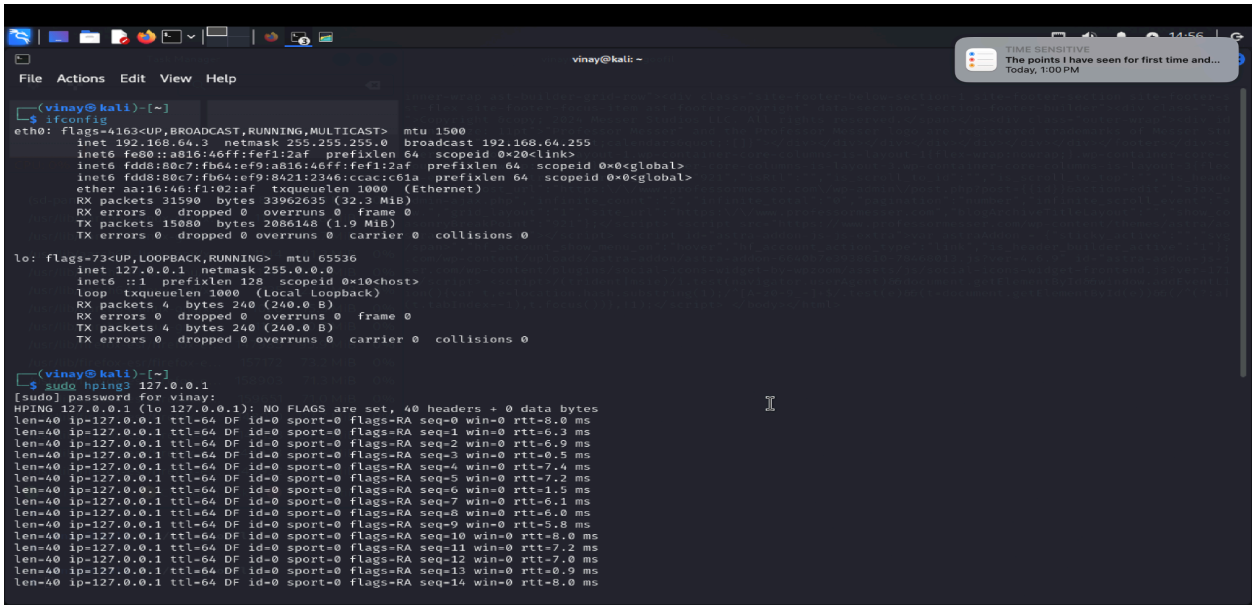
The curl tool is a powerful feature that allows you to transfer data between servers and the internet. It is commonly used in the command line interface to retrieve or send information over various network protocols such as HTTP, FTP, and others. With the curl tool, you can easily download files, connect to websites, and perform tasks that involve exchanging data with external servers. It is an essential tool for developers and system administrators who need to automate tasks or troubleshoot network-related issues efficiently.

Furthermore, the curl tool offers flexibility and customization options, enabling users to specify various parameters and options based on their requirements. By providing a simple and direct way to interact with different servers and protocols, the curl tool simplifies complex networking tasks and enhances productivity. Its straightforward syntax and versatile capabilities make it a valuable asset for anyone working with data transfers and remote servers. Mastering the curl tool can empower individuals to streamline their workflow and efficiently manage network communication processes.



Tool :11 hping

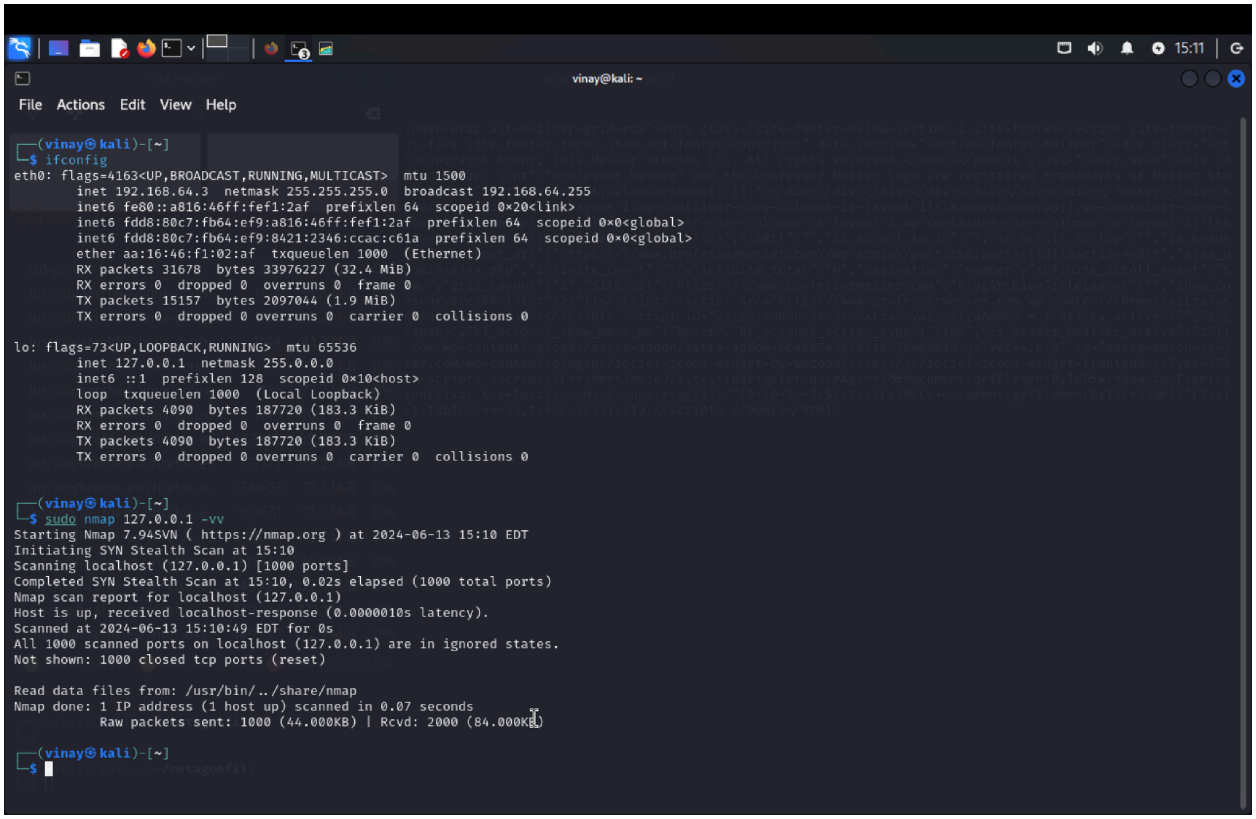
Hping is a useful tool that helps test and troubleshoot computer networks. It allows you to send various types of data packets to a specific destination to check the network's response. By analyzing the responses, you can identify potential issues and improve the network's performance. Using hping can help you understand how information travels across a network and diagnose any connectivity problems that may arise.



Tool:12 Nmap

Nmap is a powerful tool used for network scanning and mapping. It helps to discover devices connected to a network and their respective open ports. By sending specially crafted packets to target devices, Nmap can gather information about their operating system, services, and potential vulnerabilities. Security professionals often use Nmap to assess the security posture of a network and identify potential risks that need to be addressed.

One of the key features of Nmap is its ability to provide detailed reports on network devices and their configurations. Its flexible scanning options allow users to customize the scan to meet specific requirements. Nmap can be used to monitor network activity, identify unauthorized devices, and detect potential security breaches. Overall, Nmap is a essential tool for network administrators and cybersecurity professionals to keep their networks secure and well-maintained.



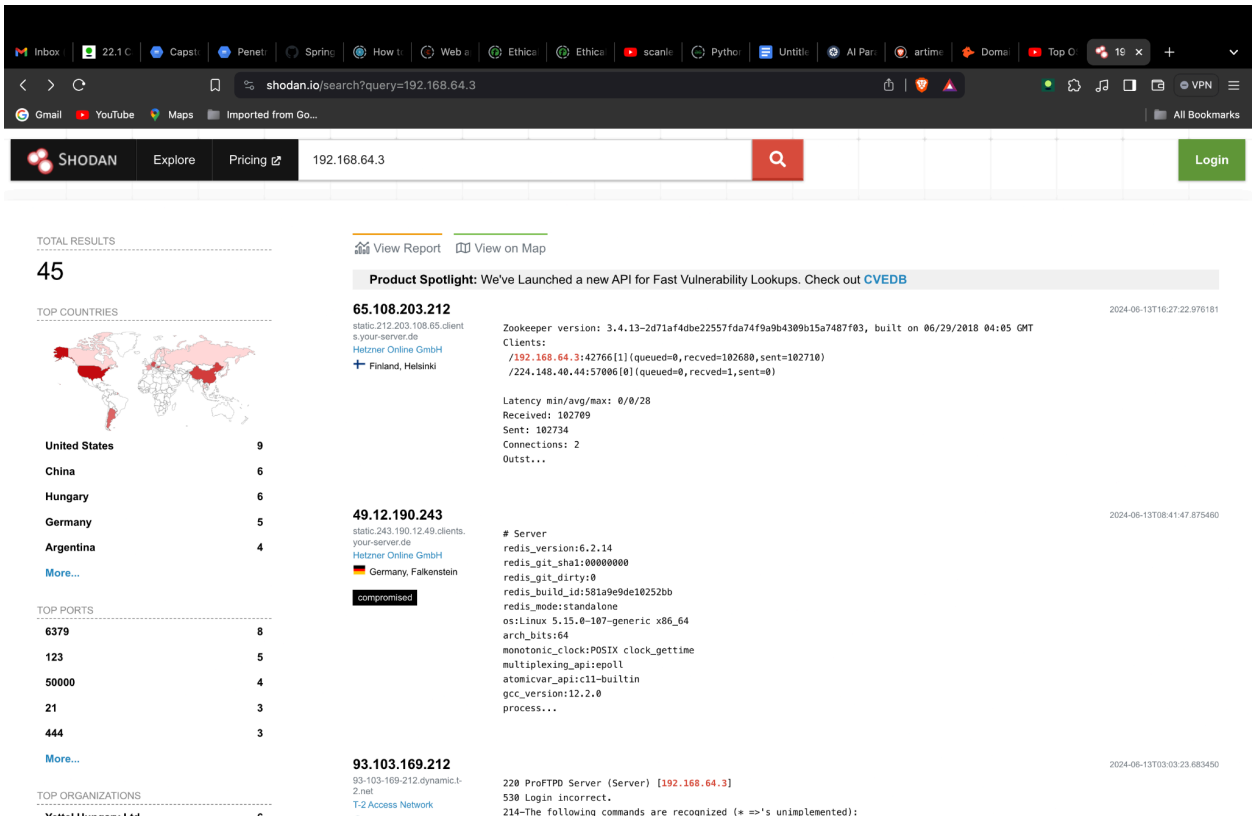
Tool:13

Artemis company uses Zcaler secure remote access to connect to the company's intranet. To locate the Access Points (AP) in the Artemis company, you can use a tool like aircrack-ng. First, you need to switch the wireless network card into monitor mode. This mode lets your card observe all the traffic nearby. Next, by running the airodump-ng command, you can capture the BSSID (MAC address) of the AP or client. This helps us determine how many APs Artemis has.

Tool:14 Shodan

Shodan is a search engine that helps people find devices connected to the internet. It is used by professionals to discover various devices like cameras, routers, and servers online. Shodan provides information on these devices, such as location, IP address, and even security vulnerabilities. It is important for individuals and businesses to be aware of what information about their devices is accessible through this search engine.

To use Shodan effectively, users must enter specific search queries to find the information they are looking for. By knowing how to navigate the platform, users can gain valuable insights into the security of their own devices or others. It is crucial for users to understand the potential risks associated with the information available on Shodan and take necessary precautions to protect their online privacy and security.

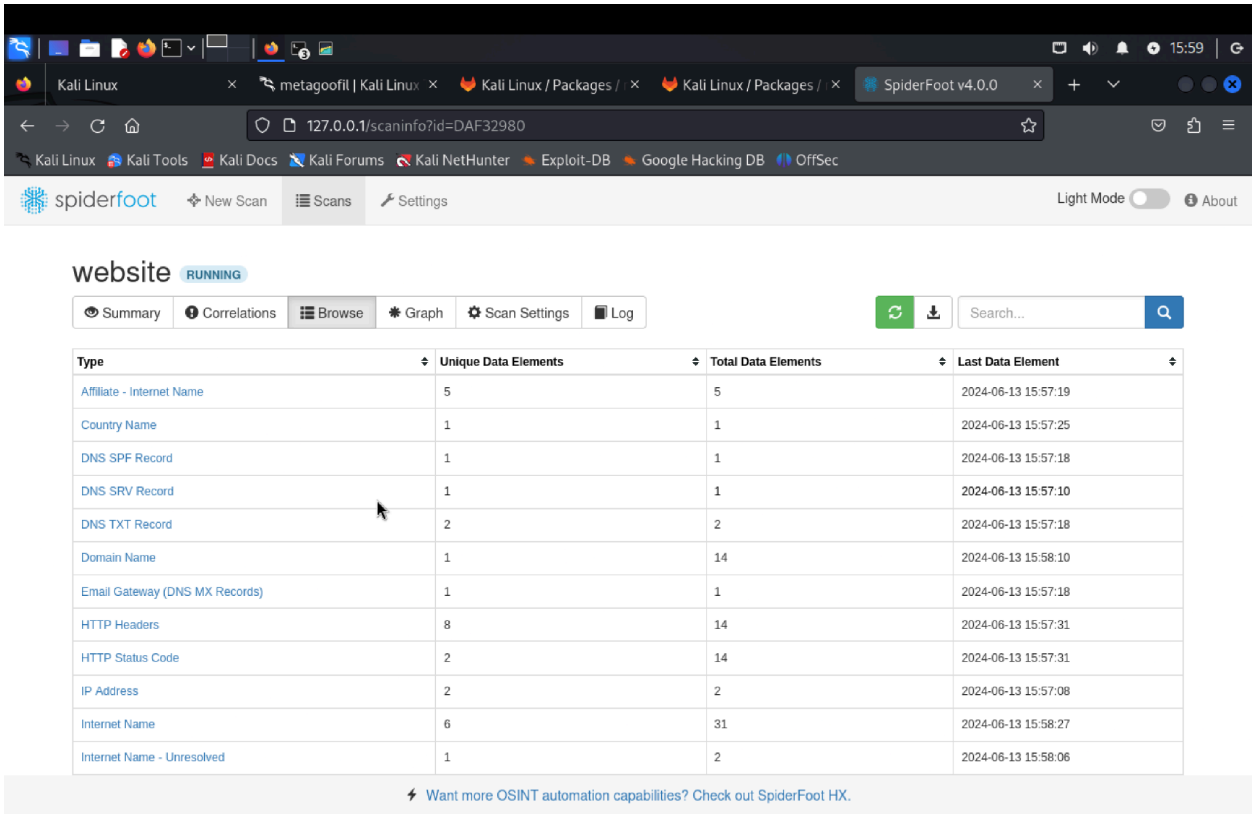


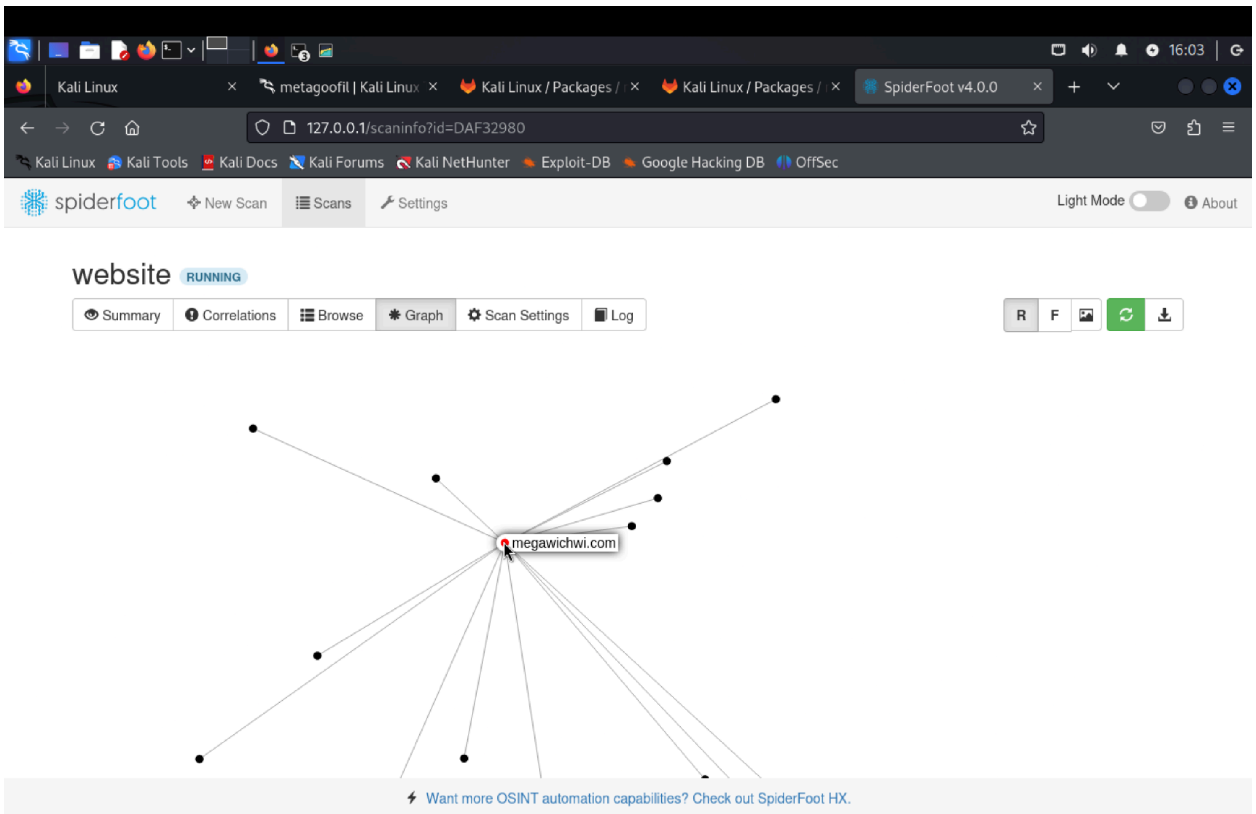
Tool:15 spiderfoot

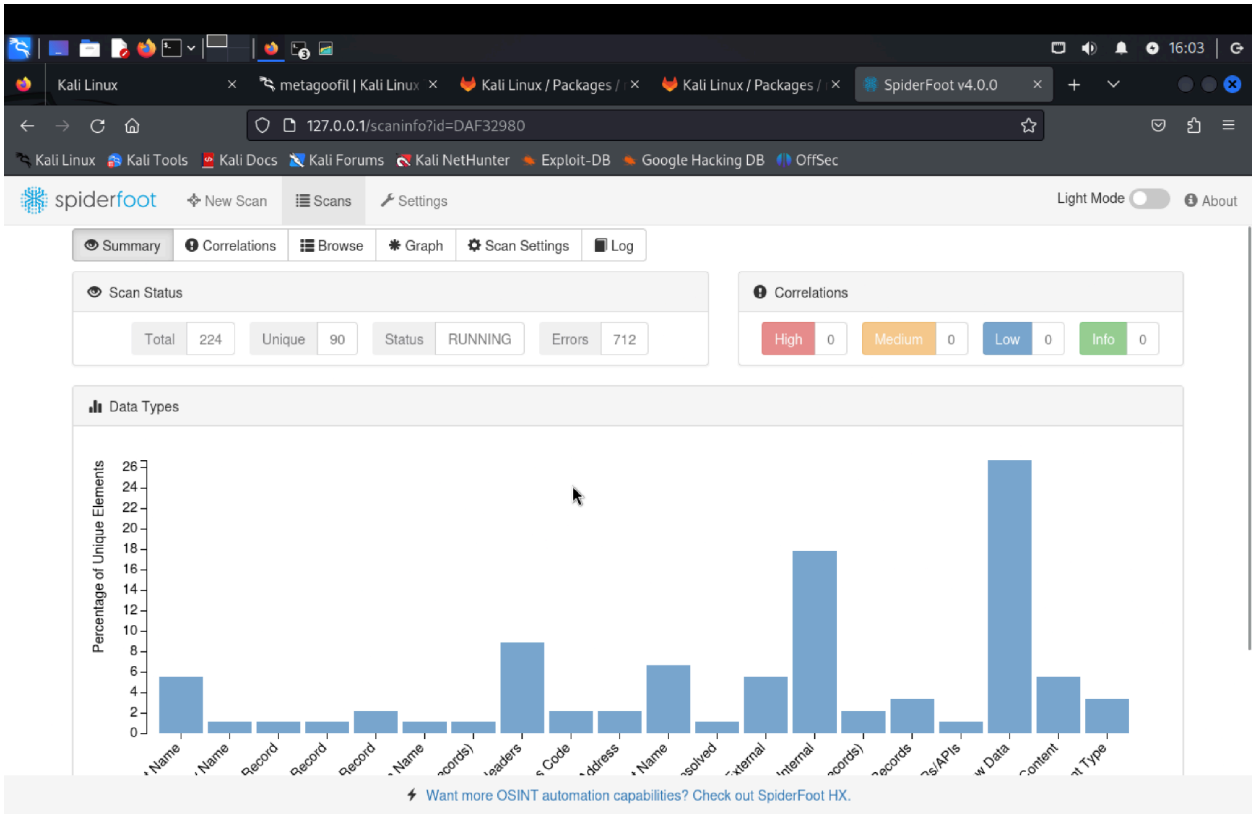
Spiderfoot is a powerful tool used to gather information from various sources on the internet. It can help cybersecurity professionals and investigators collect data about websites, IP addresses, and domains. By utilizing Spiderfoot, users can quickly discover valuable insights to assess potential security risks and vulnerabilities. This tool aids in analyzing online footprints, identifying potential threats, and monitoring digital activities for better protection against cyber threats.

Moreover, Spiderfoot simplifies the process of data collection and analysis by scanning the web for relevant information automatically. Its user-friendly interface allows individuals to navigate

through the data effortlessly and generate detailed reports for further examination. With Spiderfoot, users can enhance their cybersecurity practices by staying informed about potential risks, taking proactive measures to address security concerns, and safeguarding their online assets effectively. By leveraging the capabilities of Spiderfoot, professionals can strengthen their digital defenses and mitigate potential security breaches.


15:59
Kali Linux
metagoofil | Kali Linux
Kali Linux / Packages
Kali Linux / Packages
SpiderFoot v4.0.0
127.0.0.1/scaninfo?id=DAF32980
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
spiderfoot
New Scan
Scans
Settings
Light Mode
About
website
RUNNING
Summary
Correlations
Browse
Graph
Scan Settings
Log
Search...
Type
Unique Data Elements
Total Data Elements
Last Data Element
Affiliate - Internet Name 5 5 2024-06-13 15:57:19
Country Name 1 1 2024-06-13 15:57:25
DNS SPF Record 1 1 2024-06-13 15:57:18
DNS SRV Record 1 1 2024-06-13 15:57:10
DNS TXT Record 2 2 2024-06-13 15:57:18
Domain Name 1 14 2024-06-13 15:58:10
Email Gateway (DNS MX Records) 1 1 2024-06-13 15:57:18
HTTP Headers 8 14 2024-06-13 15:57:31
HTTP Status Code 2 14 2024-06-13 15:57:31
IP Address 2 2 2024-06-13 15:57:08
Internet Name 6 31 2024-06-13 15:58:27
Internet Name - Unresolved 1 2 2024-06-13 15:58:06
Want more OSINT automation capabilities? Check out SpiderFoot HX.


16:03
Kali Linux
metagoofil | Kali Linux
Kali Linux / Packages
Kali Linux / Packages
SpiderFoot v4.0.0
127.0.0.1/scaninfo?id=DAF32980
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
spiderfoot
New Scan
Scans
Settings
Light Mode
About
website
RUNNING
Summary
Correlations
Browse
Graph
Scan Settings
Log
R
F
megawichwi.com
Want more OSINT automation capabilities? Check out SpiderFoot HX.


16:03
Kali Linux
metagoofil | Kali Linux
Kali Linux / Packages
Kali Linux / Packages
SpiderFoot v4.0.0
127.0.0.1/scaninfo?id=DAF32980
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
spiderfoot
New Scan
Scans
Settings
Light Mode
About
Summary
Correlations
Browse
Graph
Scan Settings
Log
Scan Status
Total 224
Unique 90
Status RUNNING
Errors 712
Correlations
High 0
Medium 0
Low 0
Info 0
Data Types
Percentage of Unique Elements
26
24
22
20
18
16
14
12
10
8
6
4
2
0
Want more OSINT automation capabilities? Check out SpiderFoot HX.