Cyber Club

CYBER SECURITY FOR WEB APPLICATION

BY- SUNAN CHANNARONG

Cyber Club

គោលបំណងនៃមេរៀន

- ស្វែងយល់អ្វីជា Cybersecurity?
- បទល្មើសបច្ចេកវិទ្យា និងច្បាប់នៅកម្ពុជា
- ត្រៀមខ្លួនដើម្បីក្លាយជា Cybersecurity
- យល់ពី Web applications
- យល់ពី Kali ជាអ្វី?

Cyber Club

មាតិការ

1. អ្វីទៅជាសន្តិសុខសាយប័រ ?
2. ការងារក្នុងវិស័យសាយប័រ ?
3. អ្នកវាយប្រហារ និងអ្នកជំនាញផ្នែកសន្តិសុខសាយប័រ
4. ច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យានៅកម្ពុជា
5. ការវាយប្រហារ គំនិត និងបច្ចេកទេស
6. យល់ពីមូលដ្ឋានរបស់ Web applications
7. តាពចង្អោះប្រហោងលើ Web applications
8. ស្វែងយល់ពី Kali និងTools របស់វា

Cyber Club

១. អ្វីជាសន្តិសុខសាយប័រ?

តើអ្វីជា Cybersecurity?

Cybersecurity គឺជាការរៀបចំប្រព័ន្ធណាមួយ ដើម្បីការពារ ទប់ទល់ ទប់ស្កាក់ ពីការវាយប្រហារពី Internet មកក្នុងប្រព័ន្ធណាមួយចូលទៅកាន់ស្ថាប័ន រឺអង្គភាពណាមួយ ដែលមកពីក្រុម អាណាមិត (Black Hacker)

តើអ្នកណាជាគោលដៅសម្រាប់ក្រុម Black Hacker

គោលដៅរបស់ក្រុម ហេគឃើ មួកខ្មៅមានដូចជា៖
ធនាគា, ស្ថាប័ន និងអង្គភាពរបស់រដ្ឋ, ស្ថាប័នឯកជន, ក្រុមហ៊ុនធំៗដែលមានតម្លៃ

ការងារក្នុងវិស័យប័រអាចជាមានអ្វីខ្លះ?

Network Security: គឺអ្នកធ្វើការការពារទៅលើប្រព័ន្ធ Network និងការពារទិន្នន័យពីការបំពានឬការគំរាមកំហែងផ្សេងៗមកកាន់ស្ថាប័នខ្លួន។ ដូចជា Firewalsl, Virus, Software, Access Control, Encryption, Protection from Cyber Attacks

Cyber Club

១. អ្វីជាសន្តិសុខសាយប័រ ? (ត)

Cyber Security Consultant: គឺជាអ្នកចាយតម្លៃទៅលើផ្នែកបច្ចេកទេសលើប្រព័ន្ធ Network ការគ្រប់គ្រងណាមួយដែលមានតាពងាយរងគ្រោះពីក្រុម អ្នកណាមិតចូលក្នុងស្ថាប័ន។

Skills and Qualifications មានដូចជាៈ

Technical Skill : តាពស្ទាត់ជំនាញក្នុងឧបករណ៍សាយប័រ និងបច្ចេកវិទ្យាសន្តិសុខតាមអ៊ីនធឺណិត ដូចជា firewall , intrusion detection system(IDS) និង សន្តិសុខព័តមាន និង security information and event management (SIEM)

Analytical Skill : សម្ថតាពវិភាគទៅលើទិន្នន័យស្មុគស្មាញ និង ហេតុការណ៏ដើម្បីកំណត់អត្តសញ្ញាណ និង ការជ្រៀតចូលដែលមានសក្តានុពល

Knowledge of security frameworks : យល់ពី security framework និង ស្តង់ដារ ដូចជា NIST , ISO 27001 និង PCI-DSS

Certification : certification ពាក់ព័ន្ធដូចជា CompTIA security+ , CISSP ,CEH CISM

Cyber Club

១. អ្វីជាសន្តិសុខសាយប័រ ? (ត)

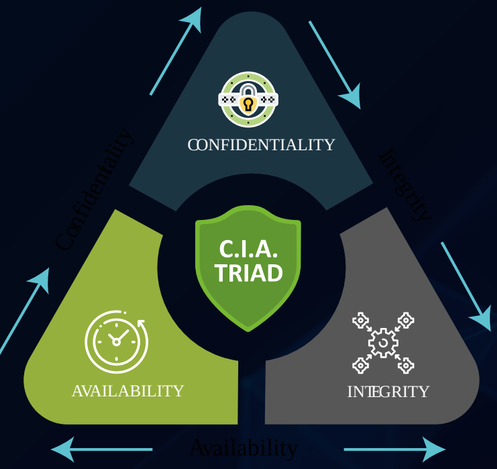
Cybersecurity Analyst: គឺជាអ្នកជំនាញវិភាគ លើប្រព័ន្ធសុវត្ថិភាពលើ Internet Systems ដែលមានភាពងាយរងគ្រោះហើយរកដំណោះស្រាយជូនដល់ស្ថាប័នដែលបានរាយតម្លៃ។

Technical Expertise : ចំណេះដឹងរាយប្រហារទាក់ទងTools និងបច្ចេកទេសមួយចំនួន ដូចជា Metasploit , Nmap , Burp suite និង wireshark ព្រមទាំងចំណេះដឹងបណ្តាញណេតវឺក ប្រព័ន្ធប្រតិបត្តិការ និង ភាសាកូដដែលចាំបាច់
Analytical Skill : សមត្ថភាពវិភាគលើប្រព័ន្ធស្មុគស្មាញ និង កំណត់អត្តសញ្ញាណដែលមានភាពខ្សោយ
Problem solving : ជំនាញដោះស្រាយបញ្ហា ដើម្បីមានវិធីសាស្ត្រ exploit vulnerabilities និង ចូលទៅកាន់តំបន់សុវត្ថិភាព

Cyber Club

១. អ្វីជាសន្តិសុខសាយប័រ ? (ត)

Penetration Tester: (Ethical Hacker ក្រុមហេគយើ មួក ស)
គឺជា អ្នកជំនាញក្នុងការធ្វើការសាក់ល្បងរកតាពងាយរងគ្រោះ ទៅលើ Web applications, Networks, system, window applications ហើយធ្វើការបង្ហាញពីចន្លោះប្រហោងដែលមាន និង ផ្តល់ព័ត៌មានទាក់ទងទៅ អ្នកបង្កើតប្រព័ន្ធដើម្បីធ្វើការកែតម្រូវឡើងវិញ។



Skills and Qualifications:

- Technical Expertise: Proficiency in various hacking tools and techniques, such as Metasploit, Nmap, Burp Suite, and Wireshark. Knowledge of network protocols, operating systems, and programming languages is also essential.
- Knowledge of security standard : ចំណេះដឹងសន្តិសុខសាយប័រជាមួយsecurity framework ស្តង់ដាដូចជា OWASP និង NIST
- Certifications : certification ពាក់ព័ន្ធដូចជា OSCP , CEH ,CPT
- Ethical and Legal awareness : ជំនាញទាក់ទងethical hacking អនុវត្តច្បាប់ និង តាព អនុញ្ញាតមុនធ្វើការ pentest

១. អ្វីជាសន្តិសុខសាយប័រ ? (ត)

- Knowledge of Security Standards: Familiarity with security frameworks and standards, such as OWASP (Open Web Application Security Project) and NIST (National Institute of Standards and Technology).
- Certifications: Relevant certifications, such as OSCP (Offensive Security Certified Professional), CEH (Certified Ethical Hacker), or CPT (Certified Penetration Tester), are often required or highly recommended.
- Ethical and Legal Awareness: Understanding of ethical hacking practices and legal implications, including obtaining proper authorization before conducting tests.

អ្នកវាយប្រហារ និងអ្នកជំនាញសន្តិសុខសាយប័រ

ប្រភេទនៃអ្នកវាយប្រហារ (Attackers)

Amateurs

ក្រុមហេគក័រដែលចង់សាក់សម្តតាពខ្លួនក្នុងការវាយទៅលើអ្វីមួយគេហៅថា Script Kiddies ។

Hacker

គឺក្រុមឧក្រិដ្ឋជនដែលវាយប្រហារទៅលើប្រព័ន្ធកុំព្យូទ័រ រឺបណ្តាញណេតវឺតដើម្បីជ្រៀតចូលក្នុងគោលដៅផ្សេងៗគ្នា។

Organized Hacker

គឺជាក្រុមឧក្រិដ្ឋជនដែលវាយប្រហារទៅលើរដ្ឋាភិបាល ស្ថាប័នរដ្ឋ ដើម្បីលួចឯកសារសម្ងាត់រដ្ឋ។

Hacktivism

Hacktivist គឺជាក្រុមដែលប្រឆាំងការពារ នយោបាយសាធារណៈ ដែលបង្ហោះ អត្ថបទ ទម្លាយទិន្នន័យសំខាន់ៗ និងធ្វើសកម្មភាព វាយប្រហារតាម DDos Attack។

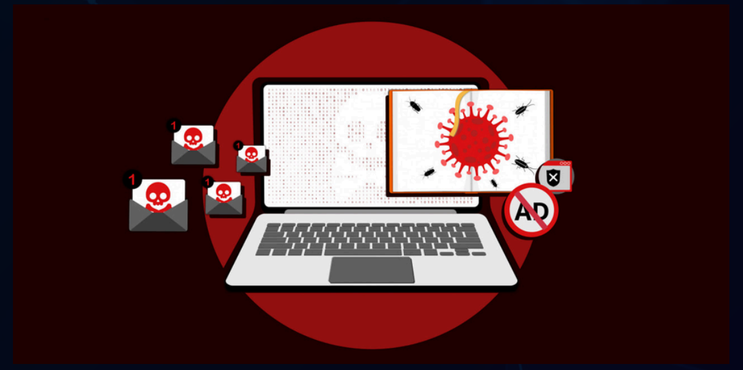
អ្នកវាយប្រហារ និងអ្នកជំនាញសន្តិសុខសាយប័រ

មេរោគកុំព្យូទ័រជាអ្វី?

យើងអាចនិយាយបានមេរោគ គឺជា Script រឺកម្មវិធីមួយដែលត្រូវបានបង្កើតដោយឧក្រិដ្ឋជនបច្ចេកវិទ្យាបានប្រើប្រាស់មេរោគនេះដើម្បីលួចព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នក ផ្ញើសារឥតបានការ (spam) និងប្រព្រឹត្តការលួចបន្លំ ឬបោកប្រាស់ផ្សេងៗដោយអ្នកមិនបានដឹងខ្លួន។ មេរោគមានច្រើនប៉ែប ច្រើនយ៉ាងទៅតាម ឧក្រិដ្ឋជនប្រើប្រាស់មានដូចជា៖

Spyware is a type of malicious software designed to secretly monitor and collect information about a user’s activities without their consent.

Bot A bot (short for "robot") is a type of software that performs automated tasks over the internet. In a malicious context, bots can be used to perform various types of cyber attacks or malicious activities.



ប្រភេទនៃការវាយប្រហារ និងអ្នកជំនាញសន្តិសុខសាយប័រ (ត)

DoS and DDoS

DoS (Denial of Service): A DoS attack aims to make a service or network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests.

DDoS (Distributed Denial of Service): A DDoS attack is a more sophisticated form of DoS attack. Instead of a single source, it involves multiple compromised systems (often part of a botnet) working together to flood the target with excessive traffic.

BY- SUNAN CHANNARONG

អ្នកវាយប្រហារ និងអ្នកជំនាញសន្តិសុខសាយប័រ (ក)

យើងតែងលឺថា ក្រុមហេគកឺរ គឺចែកចេញជា 3?

Black Hacker:

Gray Hacker:

White Hacker:

?

អ្នកវាយប្រហារ និងអ្នកជំនាញសន្តិសុខសាយប័រ (ត)

Black Hacker (ក្រុមហេគកឺរមួក ខ្មៅ)

These hackers operate with malicious intent and are often involved in illegal activities, including data theft, system sabotage, and creating or distributing malware.

Gray Hacker (ក្រុមហេគកឺរមួក ប្រផេះ)

Gray hats operate in a morally ambiguous area, sometimes breaking laws to find vulnerabilities but not necessarily with malicious intent. They might disclose their findings to the public or the affected organization.

White Hacker (ក្រុមហេគកឺរមួក ស)

These are ethical hackers who perform security testing and vulnerability assessments to help organizations strengthen their security posture. They often work with organizations legally to identify and fix security weaknesses.

Cyber Club

អ្នកវាយប្រហារ និងអ្នកជំនាញសន្តិសុខសាយប័រ (ត)

Nation-State Actors: These are hackers affiliated with or sponsored by governments. They often engage in cyber-espionage, cyber-warfare, or state-sponsored attacks. Examples include

Cybercrime Groups: These groups are motivated primarily by financial gain and engage in activities like ransomware attacks, identity theft, and fraud.

REvil (Sodinokibi): Known for ransomware attacks.
DarkSide: Another ransomware group responsible for high-profile attacks.

Hacktivist Groups: These hackers are motivated by political or social causes. They use hacking to promote their agenda or to protest against perceived injustices.

បទល្មើសបច្ចេកវិទ្យា និងច្បាប់នៅកម្ពុជា

ការកកើតមានបទល្មើសបច្ចេកវិទ្យាតាមរយៈអ្វី ?

នៅកម្ពុជាយើងមាន ក្រមព្រហ្មទណ្ឌ និងនីតិវិធីព្រហ្មទណ្ឌ សម្រាប់ធ្វើការកំណត់ ទោស ជនជាប់ចោទ តែមា
មាត្រា ចំនួន ៦៧២ ចំពោះក្រមព្រហ្មទណ្ឌ ឯនីតិវិធីព្រហ្មទណ្ឌ មានមាត្រាចំនួន ៦១២។

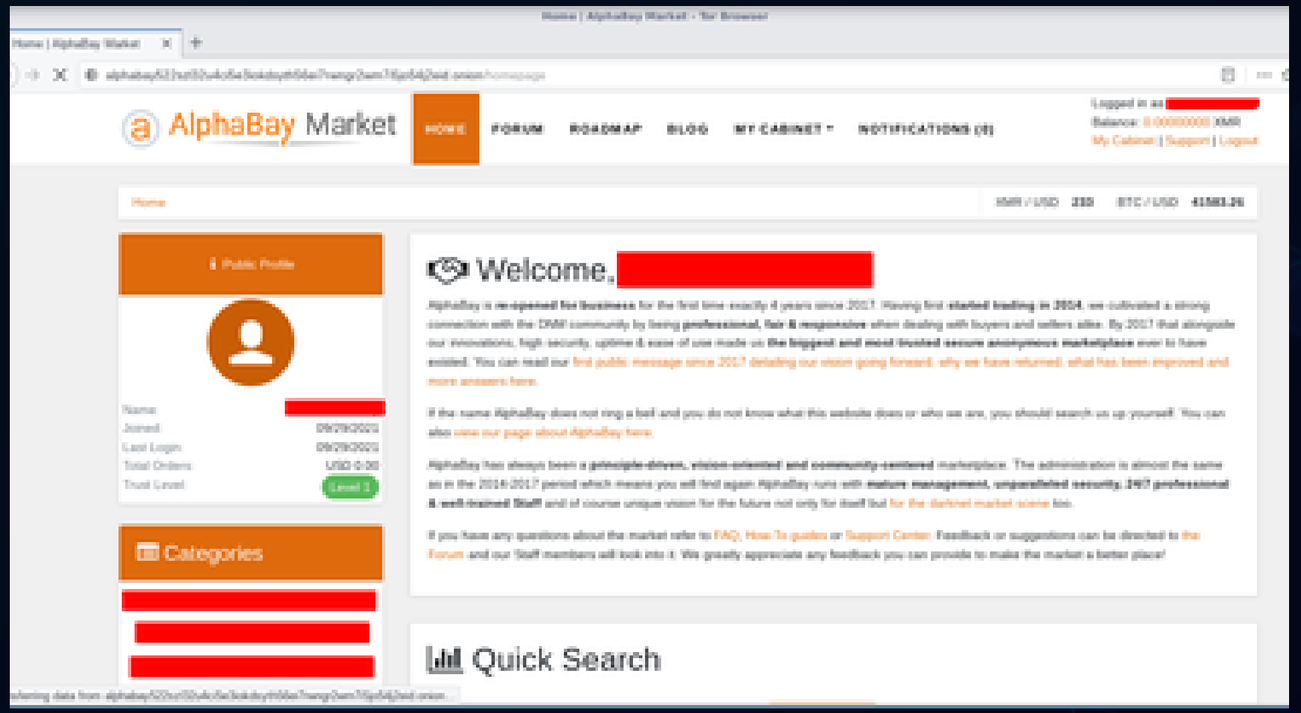
សម្រាប់បទល្មើស ក្នុងវិស័យព័ត៌មានវិទ្យា ស្ថិតក្នុងជំពូកទី ២ ហើយមានមាត្រា ចំនួន ៦ ដែលស្ថិត
នៅក្នុងក្រម។

តើអំពើណាមួយដែរចាត់ទុកជា បទល្មើស ក្នុងវិស័យព័ត៌មានវិទ្យា ?

បទពិសោធន៍ករណីសិក្សា

AlphaBay was a darknet market operating at different times between September 2014 and February 2023

After it was shut down in July 2017 following law enforcement action in the United States, Canada, and Thailand as part of Operation Bayonet

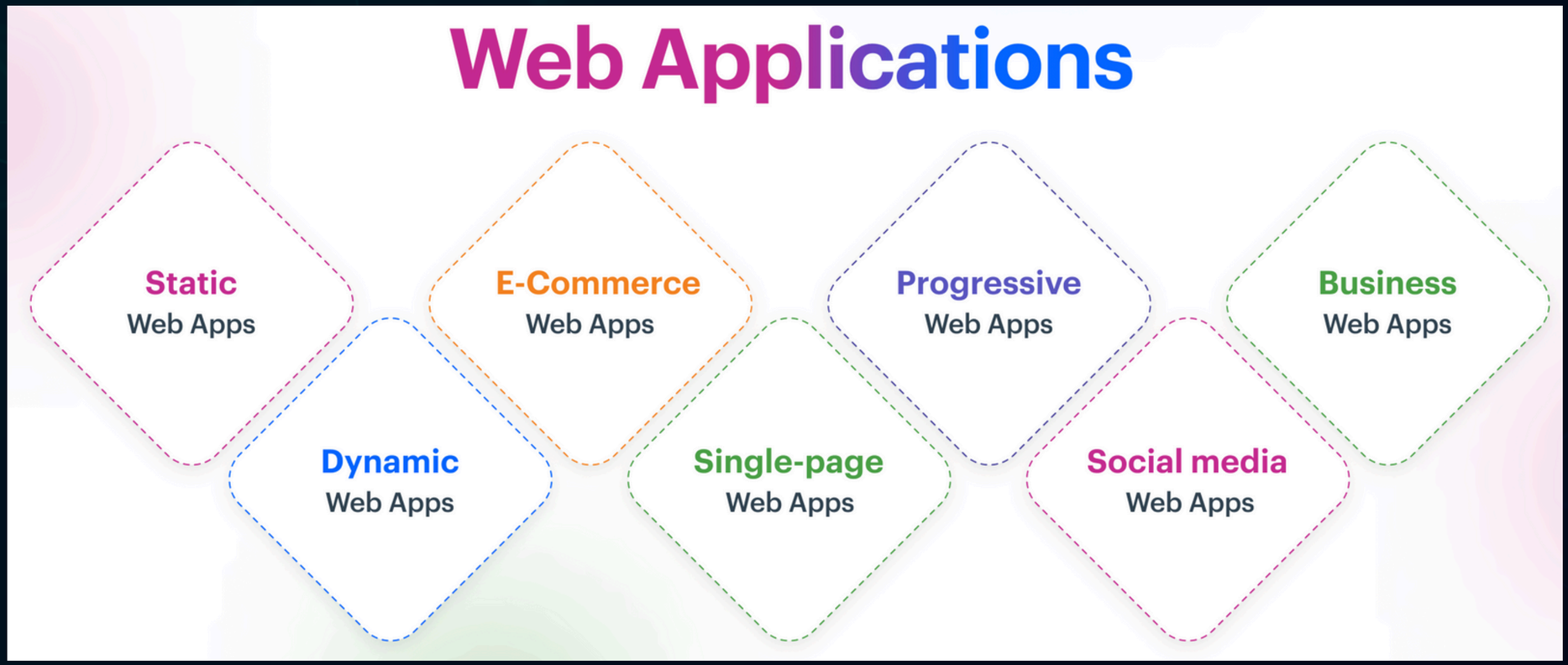


គេហទំព័រ Alpha bay បានបង្កើតឡើង ៩០ថ្ងៃ មានសមាជិកចន្លួន ១៤,០០០នាក់។

គេហទំព័រ Alpha bay ក្នុង ខែ កក្កដា ឆ្នាំ ២០១៧ មានអតិជនចំនួន ៤០០,០០០នាក់ ហើយអ្នកប្រើសកម្មមានចំនួន ៣០០,០០នាក់។

WEB APPLICATIONS

តើអ្វីជា Web application?



WEB APPLICATIONS

They typically use technologies like HTML, CSS, and JavaScript for the frontend, and may use server-side technologies like Node.js, Ruby on Rails, or PHP, along with databases like MySQL or MongoDB for the backend.

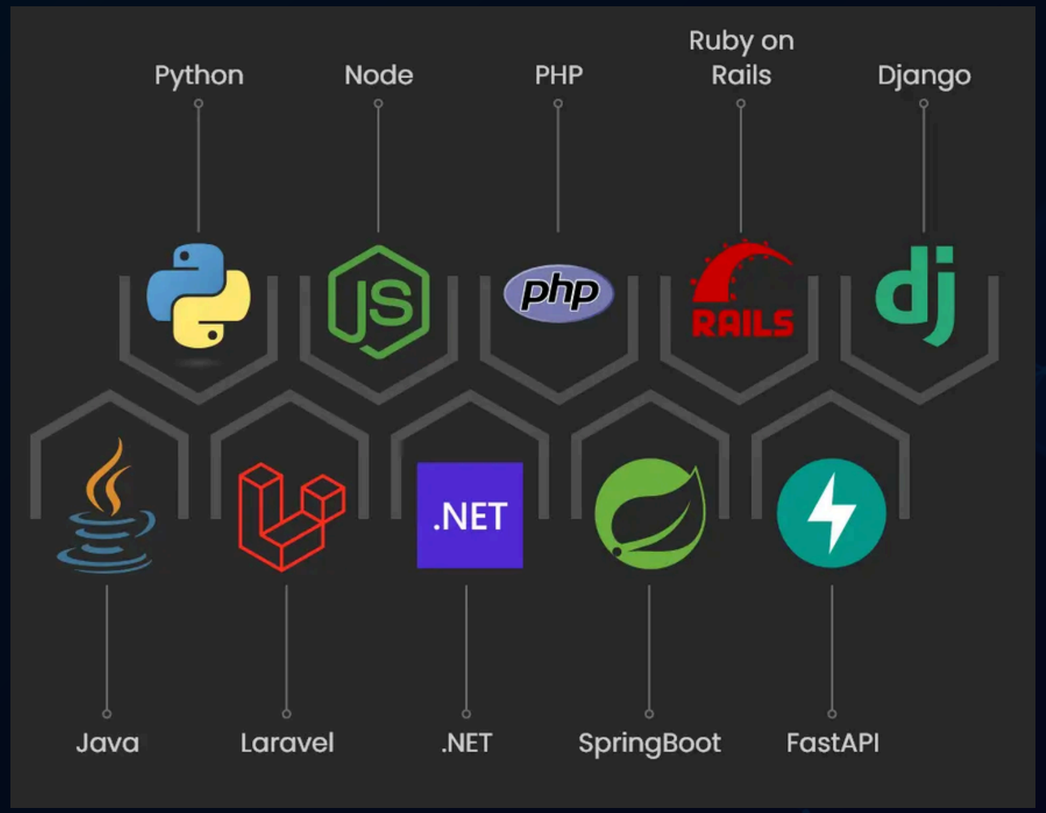
Frontend Development

- HTML (HyperText Markup Language): Defines the structure and content of web pages. It's used to create elements like headings, paragraphs, links, images, and forms.
- CSS (Cascading Style Sheets): Handles the styling and layout of web pages. It controls the visual presentation, including colors, fonts, spacing, and positioning.
- JavaScript: Adds interactivity and dynamic behavior to web pages. It's used for client-side scripting to handle events, create animations, and interact with APIs.

WEB APPLICATIONS

Backend Development

- Node.js: A JavaScript runtime built on Chrome's V8 engine that allows server-side scripting with JavaScript. It’s often used with frameworks like Express.js.
- Python: Used with frameworks like Django and Flask to create web applications. Python is known for its readability and simplicity.
- Ruby: Known for its elegant syntax, Ruby is often used with the Ruby on Rails framework for building web applications.
- PHP: A server-side scripting language commonly used for web development. It’s often paired with databases like MySQL.
- Java: Used with frameworks like Spring Boot for building robust and scalable web applications. Java is known for its performance and portability.
- C#: A language developed by Microsoft, used with the ASP.NET framework for building web applications on the .NET platform.

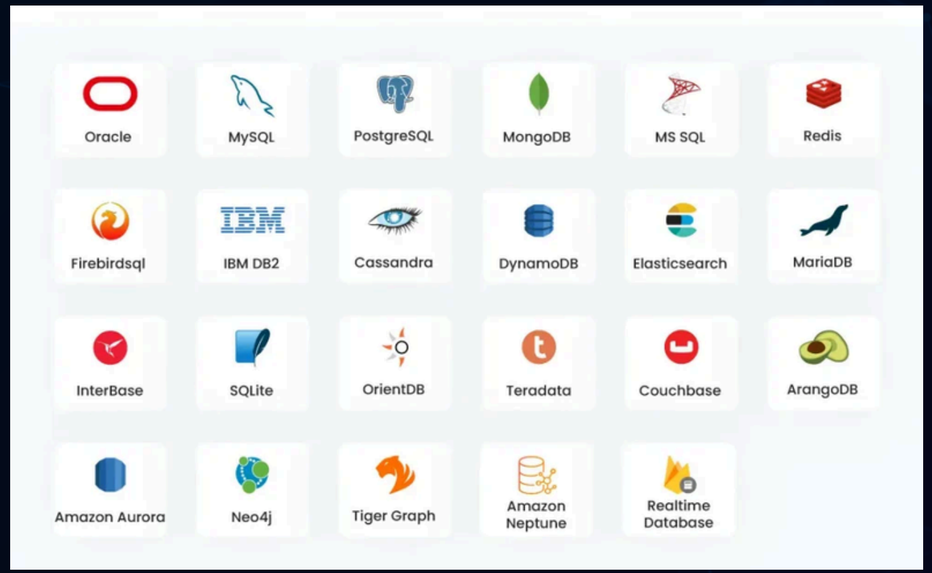


WEB APPLICATIONS

Database Technologies

- SQL (Structured Query Language): Used for managing and querying relational databases like MySQL, PostgreSQL, and Microsoft SQL Server.

- NoSQL Databases: Non-relational databases like MongoDB, Cassandra, and Redis are used for handling unstructured or semi-structured data.

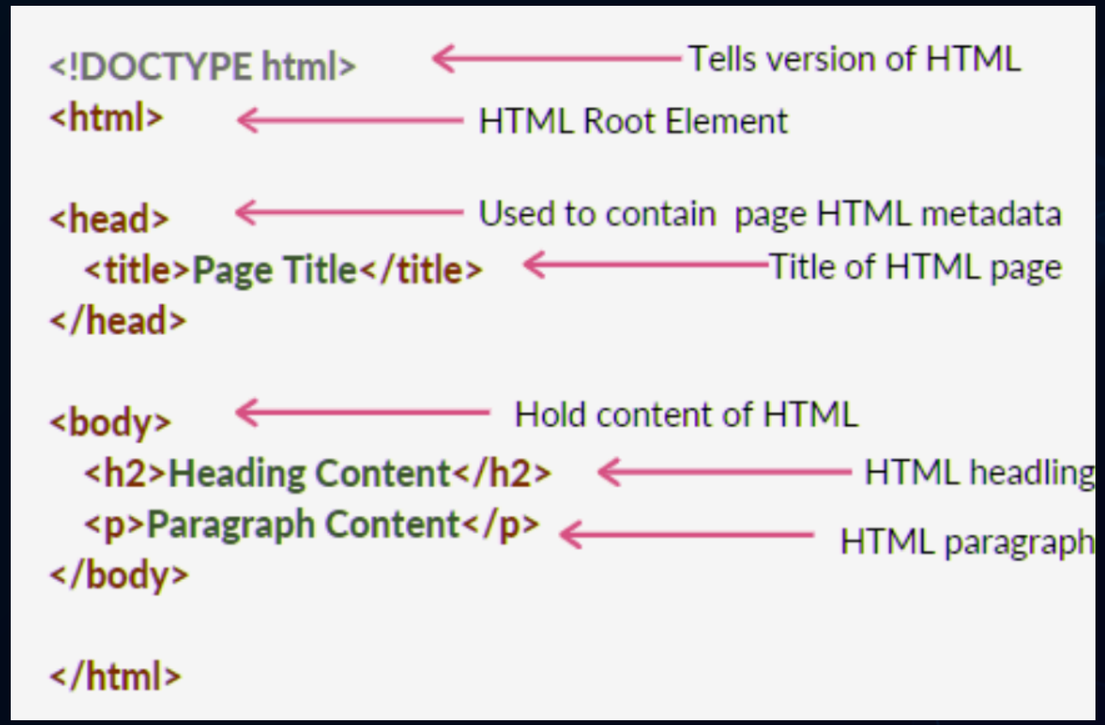


តើអ្វីទៅជា HTML, CSS, JAVASCRIP, JQUERY

HTML: **ភាសាពេញរបស់វាគឺ** (HyperText Markup Language)

Purpose: HTML provides the structure and content of web pages. It uses a system of tags and attributes to define elements such as headings, paragraphs, links, images, and forms.

```
<html>
 <head>
  <title>My Web Page</title>
 </head>
 <body>
  <h1>Welcome to My Web Page</h1>
  <p>This is a paragraph</p>
  <a href="https://www.example.com">Visit
Example</a>
 </body>
</html>
```



ឆ្នើរៀន HTML, CSS, JAVASCRIP, JQUERY

CSS (Cascading Style Sheets)

```
body {
  font-family: Arial, sans-serif;
  background-color: #f4f4f4;
}
h1 {
  color: #333;
  text-align: center;
}
p {
  margin: 20px;
}
```

```
<!DOCTYPE html>
<html>
<head>
    <title>CSS</title>
    <style>
    body{
    text-align: center;
    }
    h1::first-letter {
    font-family: Lucida Calligraphy;
    font-size: 3cm;
    color: red;
    text-shadow: 5px 8px 9px cyan;
    }
    h1{
    color: red;
    }
    </style>
</head>

<body>
    <h1>Welcome to Simplilearn</h1>
    <h2> This is an example of ::first-letter pseudo-element</h2>
</body>
</html>
```

```
<!DOCTYPE html>
<html>
<head>
    <title>CSS</title>
    <style>
    .box{
        background-color: pink;
        width: 300px;
        height: 200px;
        margin: auto;
        font-size: 40px;
        text-align: center;
    }

    .box:hover{
        background-color: cyan;
    }

    h1, h2{
        color: black;
        text-align: center;
    }
    </style>
</head>

<body>
    <h1>Simplilearn</h1>
    <h2>:hover Pseudo-class</h2>
    <div class="box">
        My color changes if you hover over me!
    </div>
</body>
</html>
```

ការរៀនទាំង HTML, CSS, JAVASCRIP

JavaScript

JavaScript is a programming language that adds interactivity and dynamic behavior to web pages. It can manipulate HTML and CSS, handle events, and perform tasks like form validation and animations.

```html
<!DOCTYPE html>
<html>
  <head>
    <title>My Website</title>
    <script>
      function changeBackground() {
        document.body.style.backgroundColor = "blue";
      }
    </script>
  </head>
  <body onload="changeBackground()">
    <h1>Welcome to my website!</h1>
  </body>
</html>
```

ភាពចន្លោះប្រហោងលើ WEB APPLICATIONS

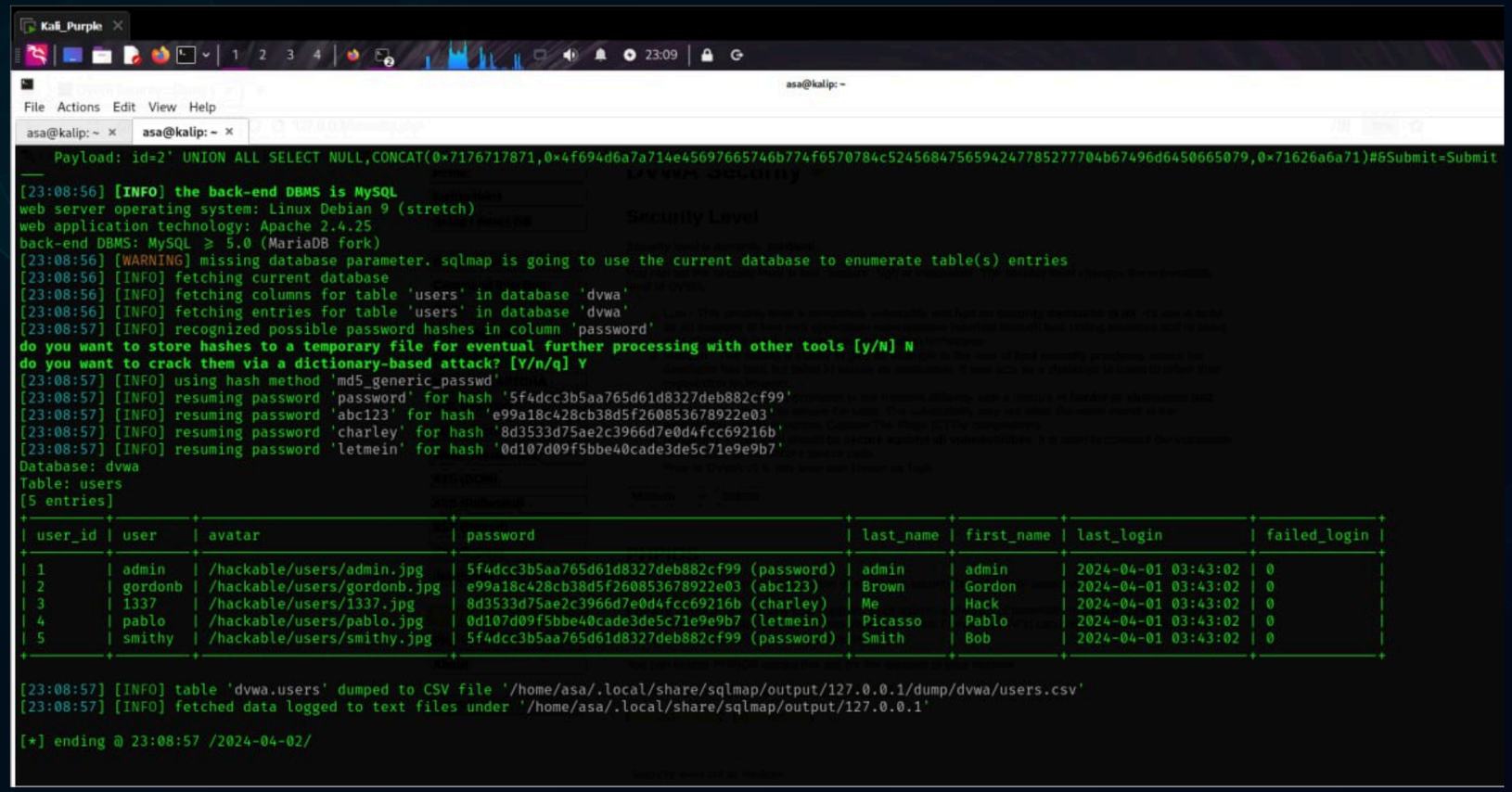
ក្រុមឧក្រិដ្ឋជនធ្វើការយ៉ាងដើម្បីជ្រៀតចូលក្នុង ប្រព័ន្ធរបស់យើង?

Python or C/C++

ផ្នត់គំនិតរបស់ក្រុមឧក្រិដ្ឋជន

ការពង្រាងប្រយោងលើ WEB APPLICATIONS

ការប្រើប្រាស់ Tools មួយចំនួនក្នុងការស្វែងរក Data ទៅលើ Web បានបង្កើតនៅឆ្នាំទី ៣?



KALI LINUX

អ្វីជា Kali linux ?

Kali Linux is a specialized Linux distribution designed for penetration testing, cybersecurity, and digital forensics. Developed and maintained by Offensive Security, Kali Linux is widely used by security professionals and researchers to test and assess the security of systems and networks.

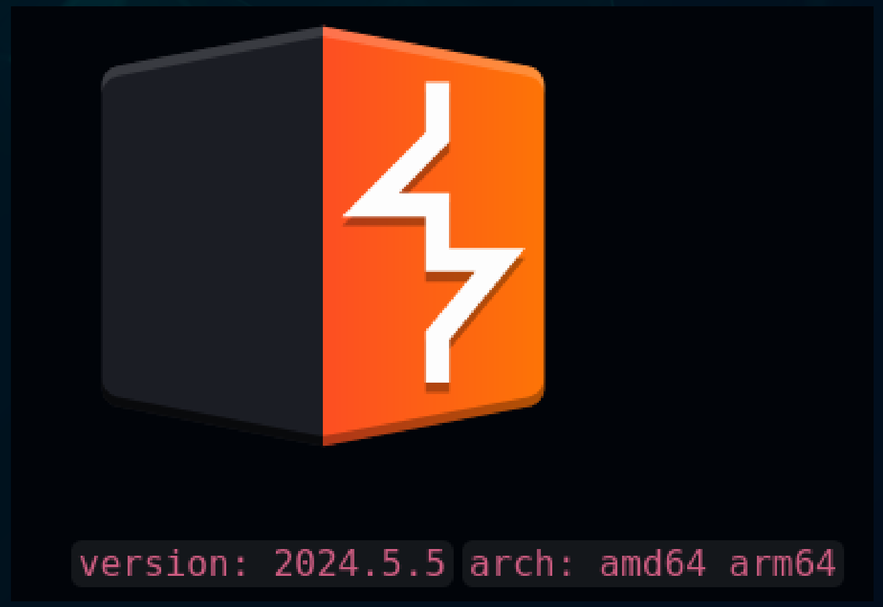
KALI LINUX

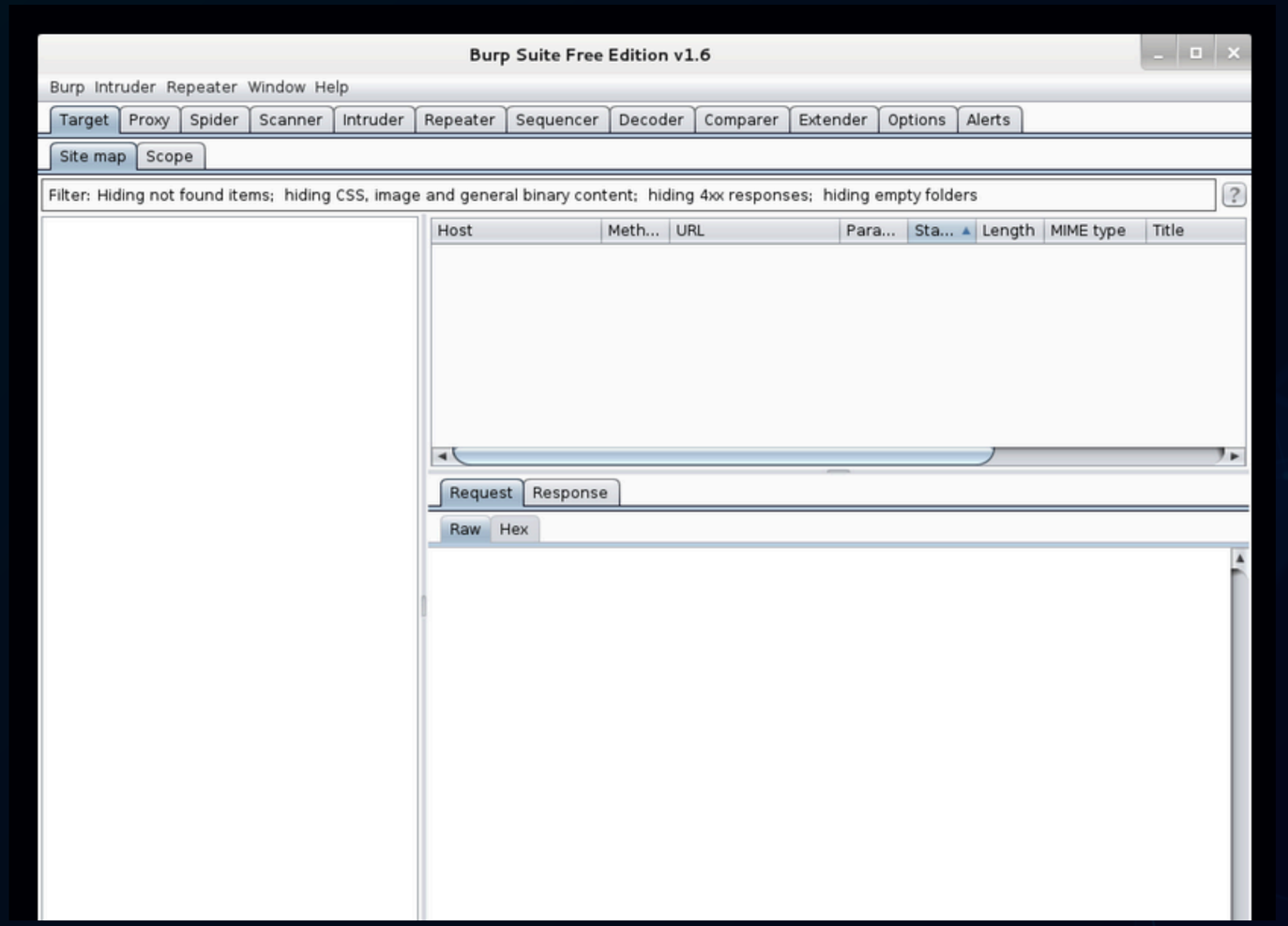
ស្វែងយល់ពី Tools ក្នុង Kali Linux

1. Burp Suite - Farmwork
2. SQLmap - Automated SQL injection and database takeover tool
3. Nikto - Web content scanner
4. Dirsearch - HTTP Bruteforcing
5. Nmap - Port scanning
6. Dir - Web content scanner
7. John - Password cracking tool
8. Hydra - Brute-force login attacks
9. Wifiphisher - Automated Wi-Fi phishing tool

KALI LINUX

Burp Suite - Farmwork





KALI LINUX

Burp Suite - Farmwork

```
$ burpsuite
```

```
root@kali:~# burpsuite --help
Usage:
--help
--version
--disable-extensions
--diagnostics
--use-defaults
--collaborator-server
--collaborator-config
--data-dir
--project-file
--developer-extension-class-name
--config-file
--user-config-file
--auto-repair
--unpause-spider-and-scanner
--disable-auto-update
```

burpsuite

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Installed size: `262.02 MB`
How to install: `sudo apt install burpsuite`

គឺជាopensource toolមួយដែលប្រើសម្រាប់ តេស្តរកvulnerability របស់ web applications វាវិភាគការវាយប្រហារផ្នែកfontដោយស្វែងរក និង exploit vulnerabilities

KALI LINUX

SQLmap

Sqlmap

version: 1.8.7 arch: all

sqlmap

sqlmap goal is to detect and take advantage of SQL injection vulnerabilities in web applications. Once it detects one or more SQL injections on the target host, the user can choose among a variety of options to perform an extensive back-end database management system fingerprint, retrieve DBMS session user and database, enumerate users, password hashes, privileges, databases, dump entire or user's specific DBMS tables/columns, run his own SQL statement, read specific files on the file system and more.

Installed size: `10.63 MB`
How to install: `sudo apt install sqlmap`

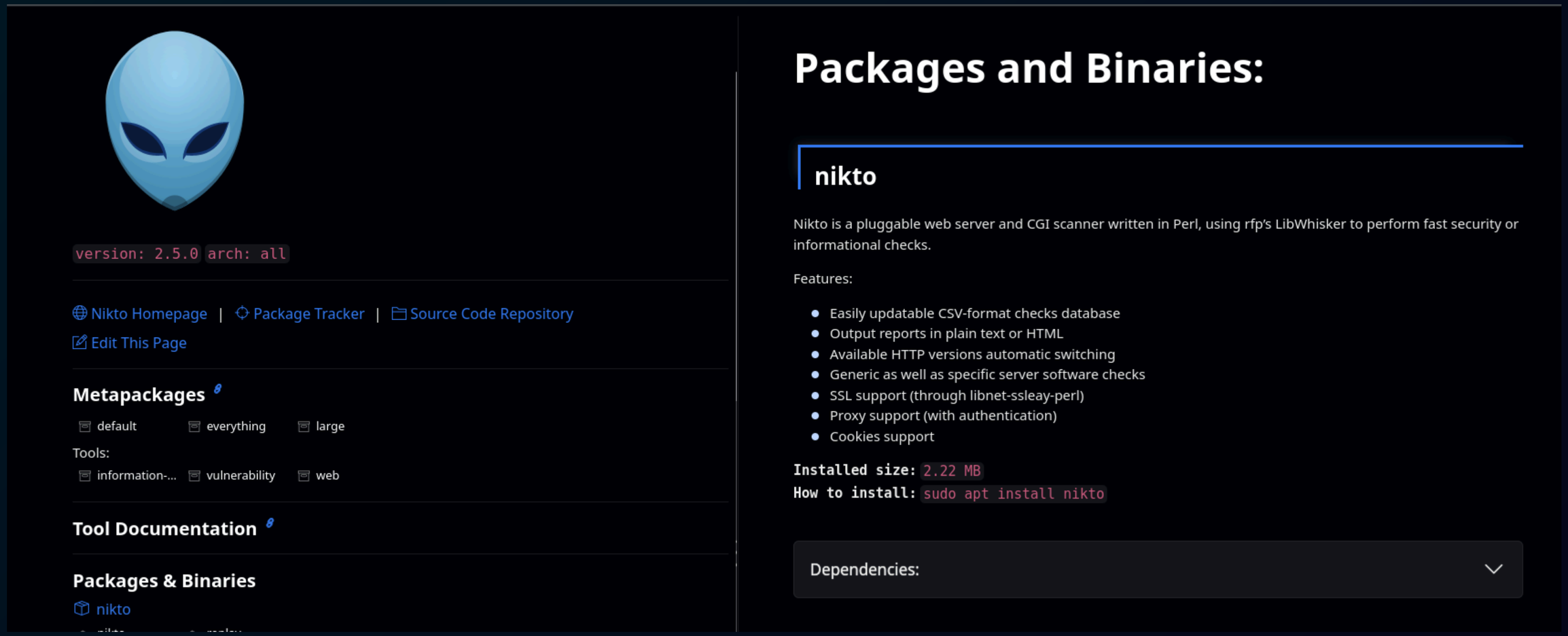
$ sqlmapapi

Automatic SQL injection tool, api server

```
root@kali:~# sqlmapapi -h
Usage: sqlmapapi [options]

Options:
  -h, --help            show this help message and exit
  -s, --server          Run as a REST-JSON API server
  -c, --client          Run as a REST-JSON API client
  -H HOST, --host=HOST  Host of the REST-JSON API server (default "127.0.0.1")
  -p PORT, --port=PORT  Port of the REST-JSON API server (default 8775)
  --adapter=ADAPTER     Server (bottle) adapter to use (default "wsgiref")
  --database=DATABASE   Set IPC database filepath (optional)
  --username=USERNAME   Basic authentication username (optional)
  --password=PASSWORD   Basic authentication password (optional)
```

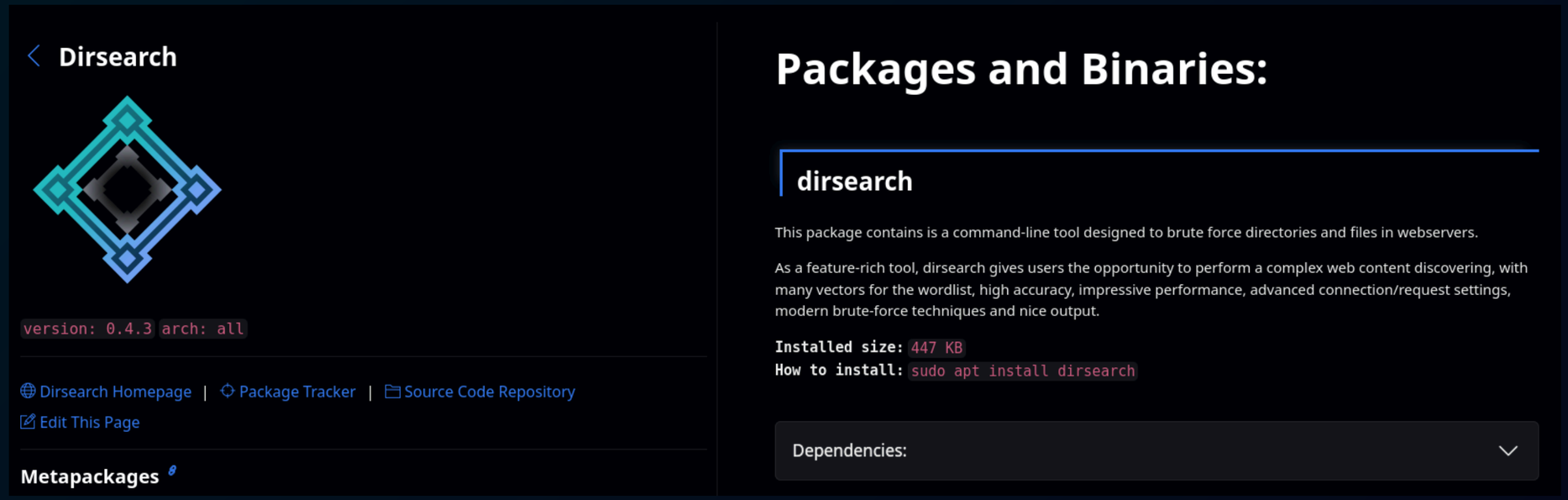
Nikto - Web content scanner



niktoជាopensource ដែលscan vulnerability ពី webserver មានដូចជាfile និង program

KALI LINUX

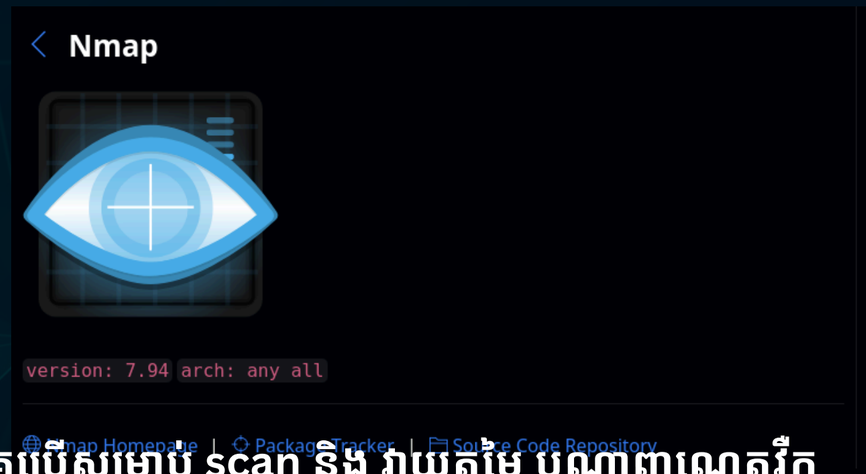
Dirsearch - HTTP Bruteforcing



Cyber Club

KALI LINUX

Nmap - Port scanning



Tool Documentation:

nmap Usage Example

Scan in verbose mode (`-v`), enable OS detection, version detection, script scanning, and traceroute (`-A`), with version detection (`-sV`) against the target IP (`192.168.1.1`):

```
root@kali:~# nmap -v -A -sV 192.168.1.1

Starting Nmap 6.45 ( http://nmap.org ) at 2014-05-13 18:40 MDT
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 18:40
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 18:40, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:40
Completed Parallel DNS resolution of 1 host. at 18:40, 0.00s elapsed
Initiating SYN Stealth Scan at 18:40
Scanning router.localdomain (192.168.1.1) [1000 ports]
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 3001/tcp on 192.168.1.1
```

nmap គឺជាopensource ដែលគេប្រើសម្រាប់ scan និង វាយតម្លៃ បណ្តាញណេតវឺក

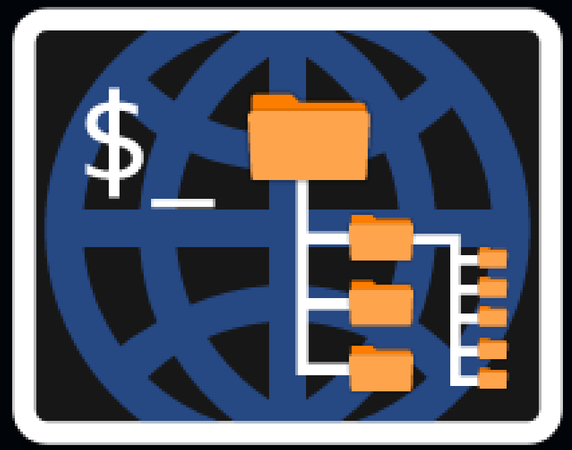
nmap-common

Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques, version detection (determine service protocols and application versions listening behind ports), and TCP/IP fingerprinting (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more. Most Unix and Windows platforms are supported in both GUI and commandline modes. Several popular handheld devices are also supported, including the Sharp Zaurus and the iPAQ.

This package contains the nmap files shared by all architectures.

Installed size: `21.03 MB`
How to install: `sudo apt install nmap-common`

Dirb - Web content scanner



`version: 2.22` `arch: any`

dirb

DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the responses.

DIRB comes with a set of preconfigured attack wordlists for easy usage but you can use your custom wordlists. Also DIRB sometimes can be used as a classic CGI scanner, but remember that it is a content scanner not a vulnerability scanner.

DIRB's main purpose is to help in professional web application auditing. Specially in security related testing. It covers some holes not covered by classic web vulnerability scanners. DIRB looks for specific web objects that other generic CGI scanners can't look for. It doesn't search vulnerabilities nor does it look for web contents that can be vulnerable.

Installed size: `1.43 MB`
How to install: `sudo apt install dirb`

John - Password cracking tool


```
kali@kali:~$ echo -n test2 | md5sum
ad0234829205b9033196ba818f7a872b  -
kali@kali:~$ echo -n test2 | md5sum | awk '{print $1}'
ad0234829205b9033196ba818f7a872b
kali@kali:~$ echo -n test2 | md5sum | awk '{print $1}' > hash
kali@kali:~$
kali@kali:~$ for x in $(seq 0 9); do echo test$x >> wordlists; done
kali@kali:~$ grep test2 wordlists
test2
kali@kali:~$ wc -l wordlists
10 wordlists
kali@kali:~$
kali@kali:~$ john --list=formats | grep -i 'md5'
descrypt, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,
aix-ssha512, andOTP, ansible, argon2, as400-des, as400-ssha1, asa-md5,
dahua, dashlane, diskcryptor, Django, django-scrypt, dmd5, dmg, dominosec,
mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12, multibit, mysqlna,
mysql-sha1, mysql, net-ah, nethalflm, netlm, netlmv2, net-md5, netntlmv2,
netntlm, netntlm-naive, net-sha1, nk, notes, md5ns, nsec3, NT, o10glogon,
PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1, PBKDF2-HMAC-SHA256,
PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY, pwsafe, qnx, RACF,
Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,
Stribog-256, Stribog-512, STRIP, SunMD5, SybaseASE, Sybase-PROP, tacacs-plus,
tcp-md5, telegram, tezos, Tiger, tc_aes_xts, tc_ripemd160, tc_ripemd160boot,
ZipMonster, plaintext, has-160, HMAC-MD5, HMAC-SHA1, HMAC-SHA224,
kali@kali:~$
kali@kali:~$ john  --format=raw-md5 --wordlist=wordlists hash
Created directory: /home/g0tmi1k/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 10 candidates left, minimum 12 needed for performance.
test2            (?)
1g 0:00:00:00 DONE (2021-11-04 10:30) 100.0g/s 1000p/s 1000c/s 1000C/s test0..tes
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords
Session completed
kali@kali:~$
```

KALI LINUX

Hydra - Brute-force login attacks

Hydra

`version: 9.5` `arch: any`

Hydra Homepage | Package Tracker | Source Code Repository

Edit This Page

hydra-gtk

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add.

This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

It supports: Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, HTTP(S)-FORM-POST, HTTP(S)-GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB(NT), SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

This package provides the GTK+ based GUI for hydra.

Installed size: `104 KB`
How to install: `sudo apt install hydra-gtk`

KALI LINUX

Wifiphisher - Automated Wi-Fi phishing tool

Wifiphisher

`version: 1.4` `arch: all`

Wifiphisher Homepage | Package Tracker | Source Code Repository

Edit This Page

Packages and Binaries:

wifiphisher

This package contains a security tool that mounts automated phishing attacks against Wi-Fi networks in order to obtain secret passphrases or other credentials. It is a social engineering attack that unlike other methods it does not include any brute forcing. It is an easy way for obtaining credentials from captive portals and third party login pages or WPA/WPA2 secret passphrases.

Installed size: `7.91 MB`
How to install: `sudo apt install wifiphisher`

THANK YOU FOR YOUR ATTENTION