.

**📅 Date:** 25th July 2025  
**✍️ Author:** Supriya Santosh Jaiswal Intern ID: 289  
**🎯 Purpose:** Assignment as an intern at Digisuraksha Parahari Foundation

**Tools POC Report – John the Ripper**

🛠 **Tool Name:** John the Ripper (john)

🔍 **History:**

John the Ripper, commonly called "john," is an open-source password cracking tool developed by Openwall. Initially released for Unix password files, it evolved to support a wide variety of hash types and operating systems.

📄 **Description:**

John the Ripper is a powerful password cracking tool used to detect weak passwords in a system. It supports dictionary attacks, brute force, and rainbow tables, and is popular among security professionals and ethical hackers.

❓ **What Is This Tool About?**

John identifies and cracks hashed passwords using different attack strategies. It helps test password strength and identify security gaps in authentication systems.

🔑 **Key Characteristics / Features:**

* Supports multiple hash types (MD5, SHA1, NTLM, etc.)
* Fast dictionary & brute-force attacks
* Custom rule-based cracking
* Supports password cracking via GPU (John Jumbo)
* Works on Windows, Linux, macOS
* Password auditing capabilities
* Can detect weak, reused, or default credentials
* Supports integration with other tools (Hashcat, Hydra)
* Highly customizable
* Open-source with active community

🧩 **Types / Modules Available:**

* Single crack mode
* Wordlist mode
* Incremental brute-force mode
* External mode (custom scripts)
* Jumbo version (adds support for more hash types)

🛠️ **How Will This Tool Help?**

* Cracks leaked or stolen password hashes
* Identifies weak or default passwords in systems
* Aids in penetration testing of authentication mechanisms
* Helps organizations enforce stronger password policies

📝 **15-Liner Summary:**

* Open-source
* Multi-platform
* Fast password cracker
* Supports over 100 hash types
* Wordlist & brute-force
* Configurable rules
* Rainbow table support
* Single mode for Unix
* External scripting
* Useful in auditing
* Part of pentesting suites
* Active community
* GPU acceleration (Jumbo)
* Recovers lost passwords
* Ethical hacking approved

⏱ **Time to Use / Best Case Scenarios:**

* During password audits
* In penetration testing assessments
* When analyzing password dump breaches
* When evaluating internal authentication policies

🕵️ **When to Use During Investigation:**

* After acquiring a password hash dump
* During credential exposure analysis
* When evaluating insider threat risks
* Post-compromise incident analysis

👤 **Best Person to Use & Required Skills:**

**User:** Ethical Hacker / Penetration Tester / Incident Responder  
**Skills:**

* Familiarity with Linux command-line
* Knowledge of password hashing
* Understanding of authentication protocols
* Basic scripting for rule modification

⚠️ **Flaws / Suggestions to Improve:**

* No GUI in default version
* May struggle with salted hashes without context
* Brute-force can be time consuming
* GPU acceleration requires Jumbo version and setup
* Steep learning curve for new users

✅ **Good About the Tool:**

* Lightweight & efficient
* Free and open-source
* Supports wide range of password types
* Strong for offline attacks
* Large support community

📌 **John the Ripper in Action**

**Figure 1: Command Output – Cracking NTLM Hash**

bash

CopyEdit

$ john --format=NT --wordlist=rockyou.txt ntlm\_hashes.txt

Shows how john uses a popular wordlist to crack NTLM hashes in real-time, displaying cracked passwords on the screen.

📊 **Figure 2: Sample Hash File for Cracking**

A text file containing sample hashes (e.g., from a dumped database), showing various password hashes that john will attempt to crack.

💡 **Sample Use Case:**

**Scenario:**  
An internal audit at a financial firm discovers leaked credentials in a database dump. Investigators extract the password hashes and use John the Ripper with a custom wordlist to recover plaintext passwords. The tool reveals weak passwords like 12345678 and password1 used by employees, prompting a mandatory password policy update.

📊 **Comparison – John vs. Hydra (optional context)**

| **Feature** | **John the Ripper** | **Hydra** |
| --- | --- | --- |
| Attack Type | Offline (hashes) | Online (protocols) |
| Interface | CLI | CLI |
| Speed | Very Fast | Fast |
| Target | Hashes | Login services (SSH, FTP) |
| GPU Support | Yes (Jumbo version) | No |
| Forensics Use | Yes | Limited |

🌐 **Real-World Applications:**

* Used by ethical hackers in red team exercises
* Internal IT teams for credential audits
* Universities for cybersecurity training labs
* Digital forensics teams in password recovery
* National CERTs for breach impact analysis

✅ **Conclusion:**

John the Ripper is a versatile and effective password-cracking tool used for auditing and testing authentication systems. Its wide hash support and customization make it a preferred choice in digital forensics and ethical hacking operations.

Let me know if you'd like this exported as a **Word (.docx)** file or zipped.

Ask ChatGPT

**You said:**

intern id is 289

**ChatGPT said:**

Thanks! Here's the updated POC with the **Intern ID: 289** and your name.

**📅 Date:** 25th July 2025  
**✍️ Author:** Supriya Santosh Jaiswal Intern ID: 289  
**🎯 Purpose:** Assignment as an intern at Digisuraksha Parahari Foundation

**Tools POC Report – John the Ripper**

🛠 **Tool Name:** John the Ripper (john)

🔍 **History:**

John the Ripper was developed by Openwall and originally targeted Unix password files. Over time, it evolved into a powerful password cracking tool that supports a wide range of hash algorithms and platforms.

📄 **Description:**

John the Ripper is an open-source password cracking software used in security testing and digital forensics. It helps identify weak passwords by attempting to crack password hashes using various attack techniques.

❓ **What Is This Tool About?**

It’s a password audit tool used to detect and crack password hashes using dictionary attacks, brute-force, and rule-based approaches. Ideal for penetration testing and cybersecurity audits.

🔑 **Key Characteristics / Features:**

* Supports wide range of hashes (MD5, SHA, bcrypt, NTLM, etc.)
* Fast and efficient cracking
* Rule-based attack support
* Brute-force and dictionary attack modes
* GPU acceleration (Jumbo version)
* Cross-platform (Linux, Windows, macOS)
* Highly scriptable
* Open-source
* Community maintained
* Supports hash dumps and password files

🧩 **Types / Modules Available:**

* Single crack mode
* Wordlist mode
* Incremental mode
* External mode
* Jumbo patch (extended version)

🛠️ **How Will This Tool Help?**

* Cracks weak and reused passwords
* Assesses system password strength
* Aids in password recovery
* Helps penetration testers find vulnerable credentials

📝 **15-Liner Summary:**

* Open-source password cracker
* Multi-hash support
* CLI-based tool
* Highly customizable
* Works offline
* Fast dictionary attacks
* Brute-force capable
* Wordlist integration
* Rainbow table support
* GPU support (optional)
* Good for audits
* Great in red teaming
* Scriptable interface
* Active community
* Forensic-friendly

⏱ **Time to Use / Best Case Scenarios:**

* During password audits
* Post-breach credential testing
* Red team password testing
* Recovery from hash dumps

🕵️ **When to Use During Investigation:**

* After a credential leak
* When analyzing password databases
* During internal system audits
* In post-incident response

👤 **Best Person to Use & Required Skills:**

**User:** Penetration Tester / Security Auditor  
**Skills Required:**

* Linux command-line usage
* Understanding of hashing algorithms
* Knowledge of authentication systems
* Familiarity with attack vectors

⚠️ **Flaws / Suggestions to Improve:**

* No GUI interface
* Brute-force is time-consuming
* Configuration can be complex
* Needs pre-formatted hash input
* GPU version setup is technical

✅ **Good About the Tool:**

* Lightweight and powerful
* Customizable for advanced users
* Reliable cracking engine
* Ideal for password audits
* Free and open-source

📌 **John the Ripper in Action**

**Figure 1: Cracking MD5 Hash using a Wordlist**

bash

CopyEdit

john --wordlist=rockyou.txt --format=raw-md5 hashes.txt

Shows real-time password cracking results.

📊 **Figure 2: Example of a Hash File**

CopyEdit

5f4dcc3b5aa765d61d8327deb882cf99

Demonstrates a raw hash input (MD5 in this case) passed to John.

💡 **Sample Use Case:**

**Scenario:**  
A cybersecurity audit reveals a database dump with hashed employee credentials. Using John, the security team cracks weak passwords like qwerty and welcome123, helping enforce stricter password policies.

🌐 **Real-World Applications:**

* Used in CTFs and ethical hacking challenges
* Password recovery in investigations
* Used by SOC teams for internal testing
* Academic and corporate cybersecurity training
* Digital forensics operations

✅ **Conclusion:**

John the Ripper is a trusted and robust password cracking tool for digital security professionals. Its flexible attack options and strong community support make it a must-have utility for testing and strengthening authentication defenses.

Top of Form

Bottom of Form