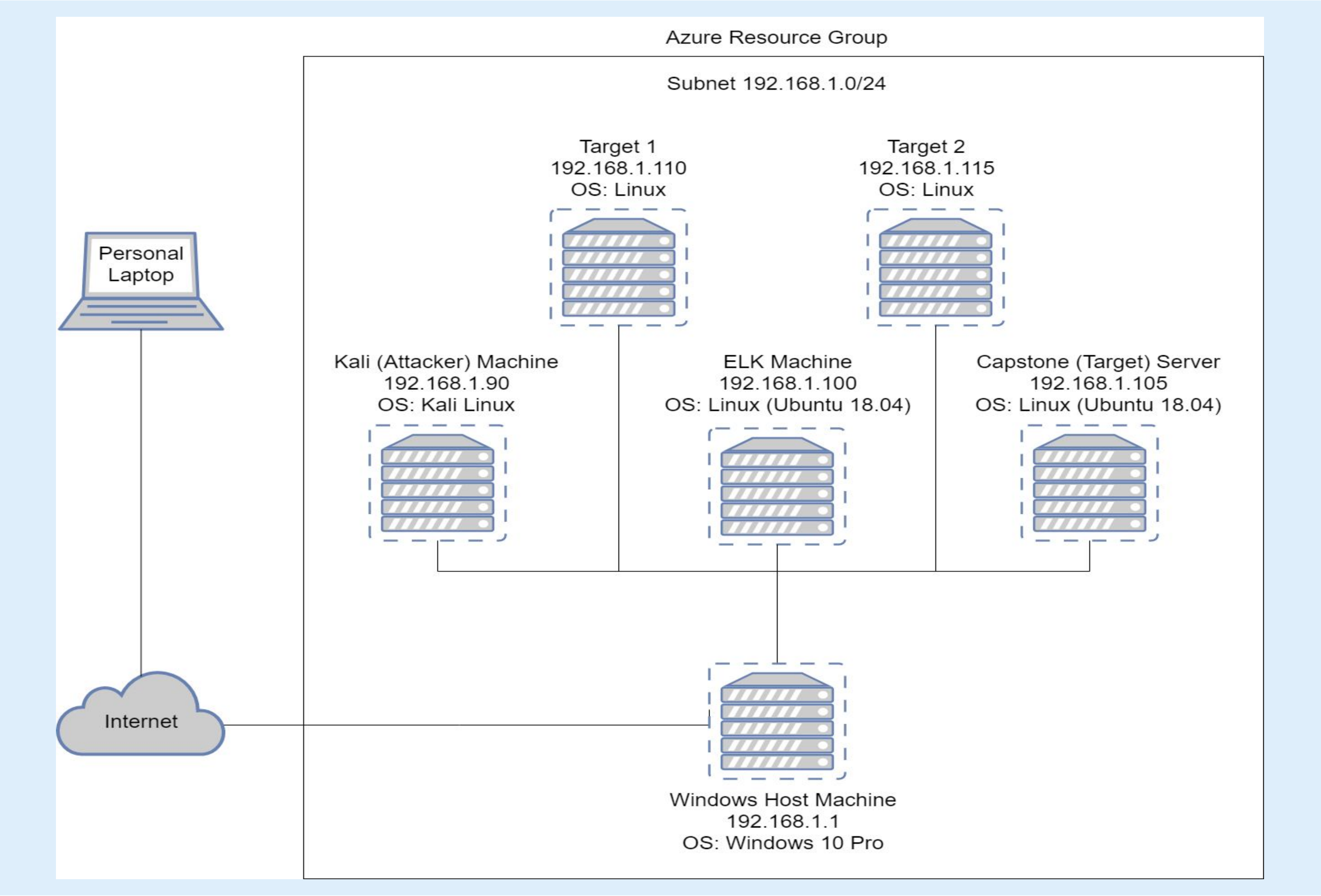
Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.240.0
Gateway:

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux (Ubuntu 18.04)
Hostname: ELK

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

Critical Vulnerabilities

Critical Vulnerabilities: Brute-Forceability

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
CWE-521: Weak Password Requirements	The product does not require users to have strong passwords.	An attacker can easily guess user passwords or crack passwords using tools such as john the ripper and gain user access.
CWE-306: Missing Authentication for Critical Function	The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.	Exposing critical functionality essentially provides an attacker with the privilege level of that functionality which allows them to read or modifying sensitive data, access to administrative or other privileged functionality, or possibly even execution of arbitrary code.
CWE-307: Improper Restriction of Excessive Authentication Attempts	Software has insufficient measures to prevent multiple failed authentication attempts in a short time frame.	An attacker can perform any amount of authentication attempts and eventually gain access to an account.

Critical Vulnerabilities: Sensitive Data Access

Vulnerability	Description	Impact
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.	An attacker can attain sensitive data and can use this to perform an exploit.
CWE-284: Improper Access Control	The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.	Attackers can gain access to resources within a system that allow them to gain sensitive information or execute exploits.
CWE-552: Files or Directories Accessible to External Parties	The product makes files or directories accessible to unauthorized actors, even though they should not be.	Unauthorised actors can read files or directories; modify files or directories.

Critical Vulnerabilities: Inadequate Data Encryption

Vulnerability	Description	Impact
CWE-261: Weak Encoding for Password	Obscuring a password with a trivial encoding does not protect the password.	An attacker can gain privileges to a system or assume an identity.
CWE-326: Inadequate Encryption Strength	The software stores or transmits sensitive data using an encryption scheme that is theoretically sound but is not strong enough for the level of protection required.	An attacker may be able to decrypt the data using brute force attacks.
CWE-328: Reversible One-Way Hash	The product uses a hashing algorithm that produces a hash value that can be used to determine the original input.	Attackers can easily crack the hash and gain access to sensitive information on the database.
CWE-916: Use of Password Hash with Insufficient Computational Effort	The software generates a hash for a password, but it uses a scheme that does not provide a sufficient level of computational effort that would make password cracking attacks hard.	If an attacker can gain access to the hashes, then it will be easier to conduct brute force attacks using tools such as John the Ripper.

Exploits

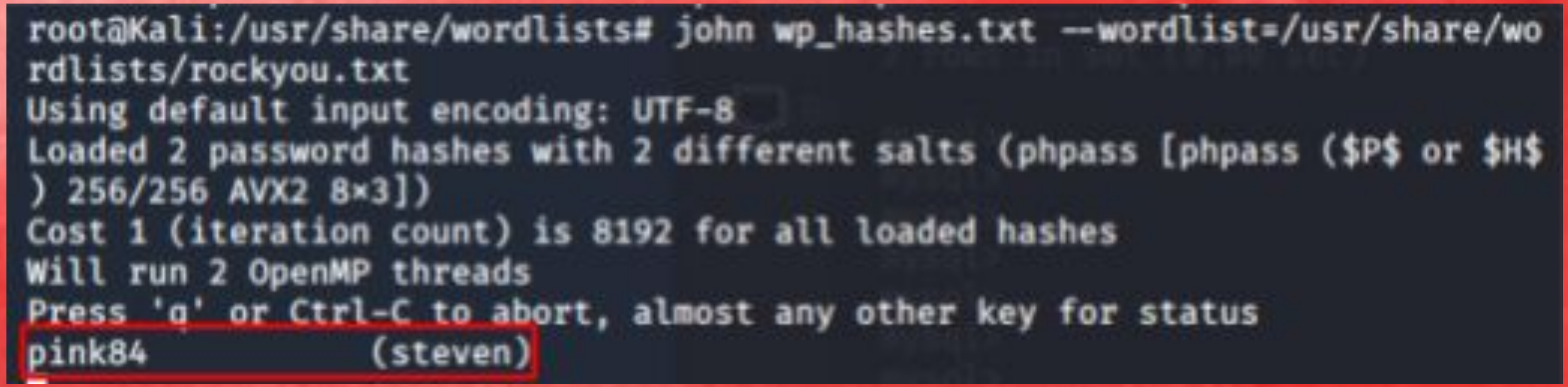
Exploitation: Brute-Forceability

1 Guessed user’s weak passwords

michael:michael

root:toor

2 Used John the Ripper with a dictionary to crack another user password

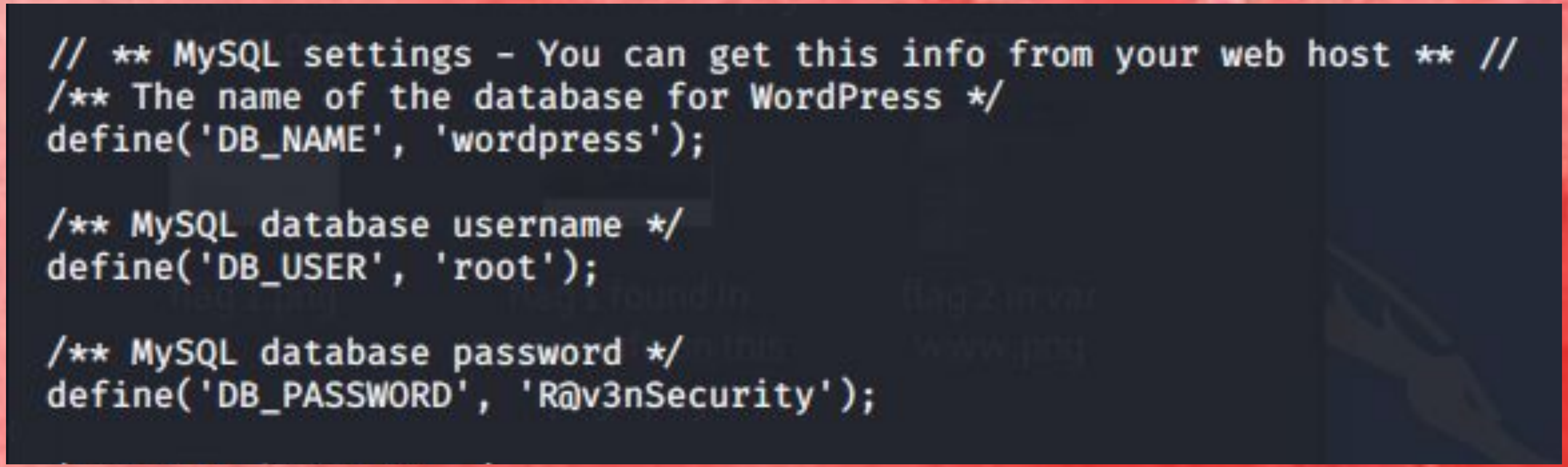


```
root@Kali:/usr/share/wordlists# john wp_hashes.txt --wordlist=/usr/share/wo
rdlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$
) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84           (steven)
```

3 Gained user access and a root shell

Exploitation: Sensitive Data Access

1. Searched through directories > found a wordpress file with MYSQL database credentials



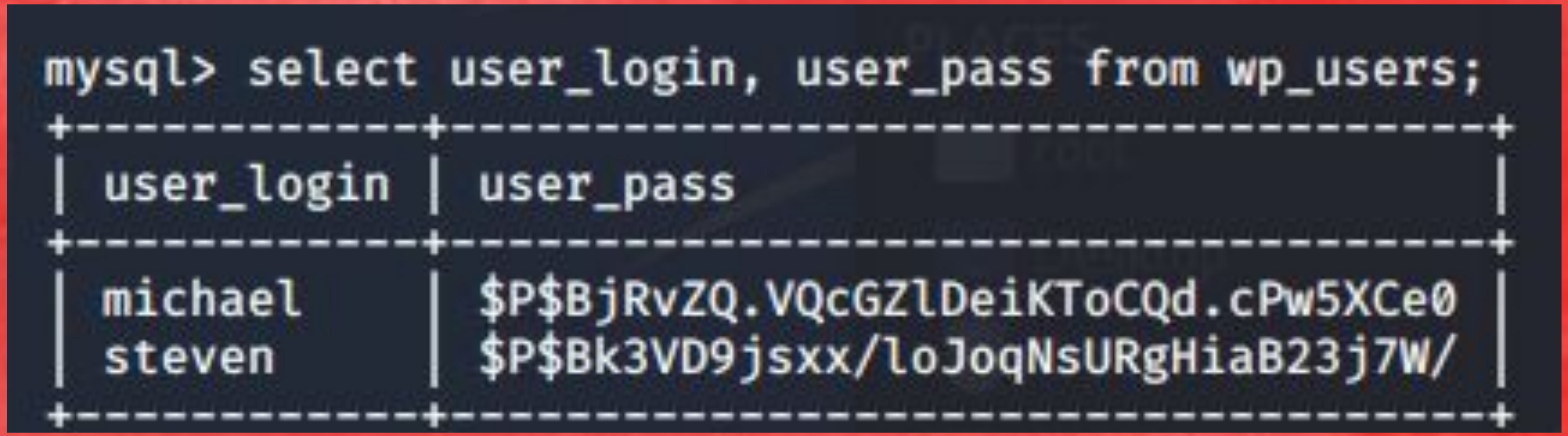
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');
```

2. Used the credentials to gain access to MYSQL database and search through it

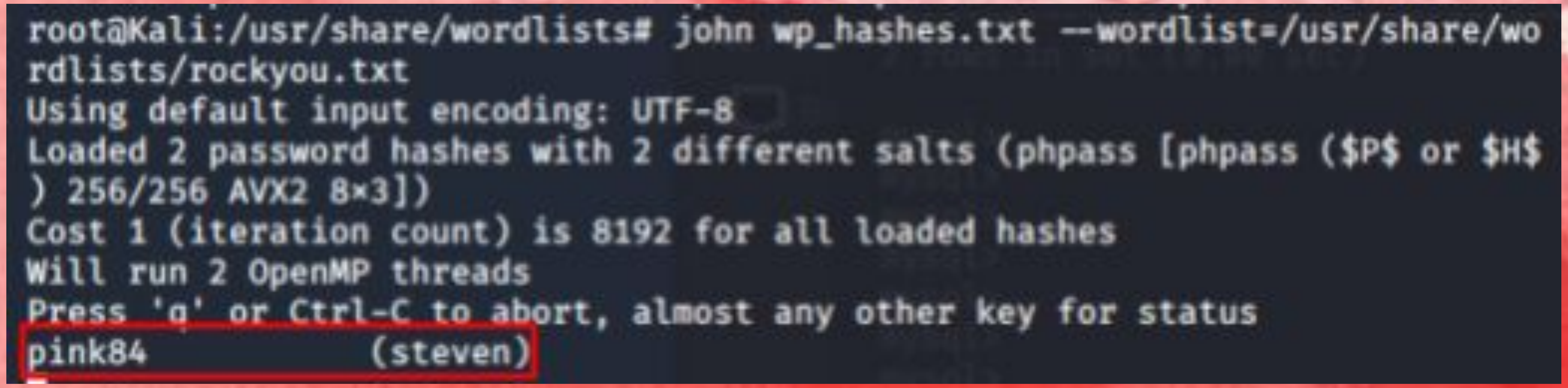
3. Gained user password hashes



```
mysql> select user_login, user_pass from wp_users;
+------------+------------------------------------+
| user_login | user_pass                          |
+------------+------------------------------------+
| michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 |
| steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ |
+------------+------------------------------------+
```

Exploitation: Inadequate Data Encryption

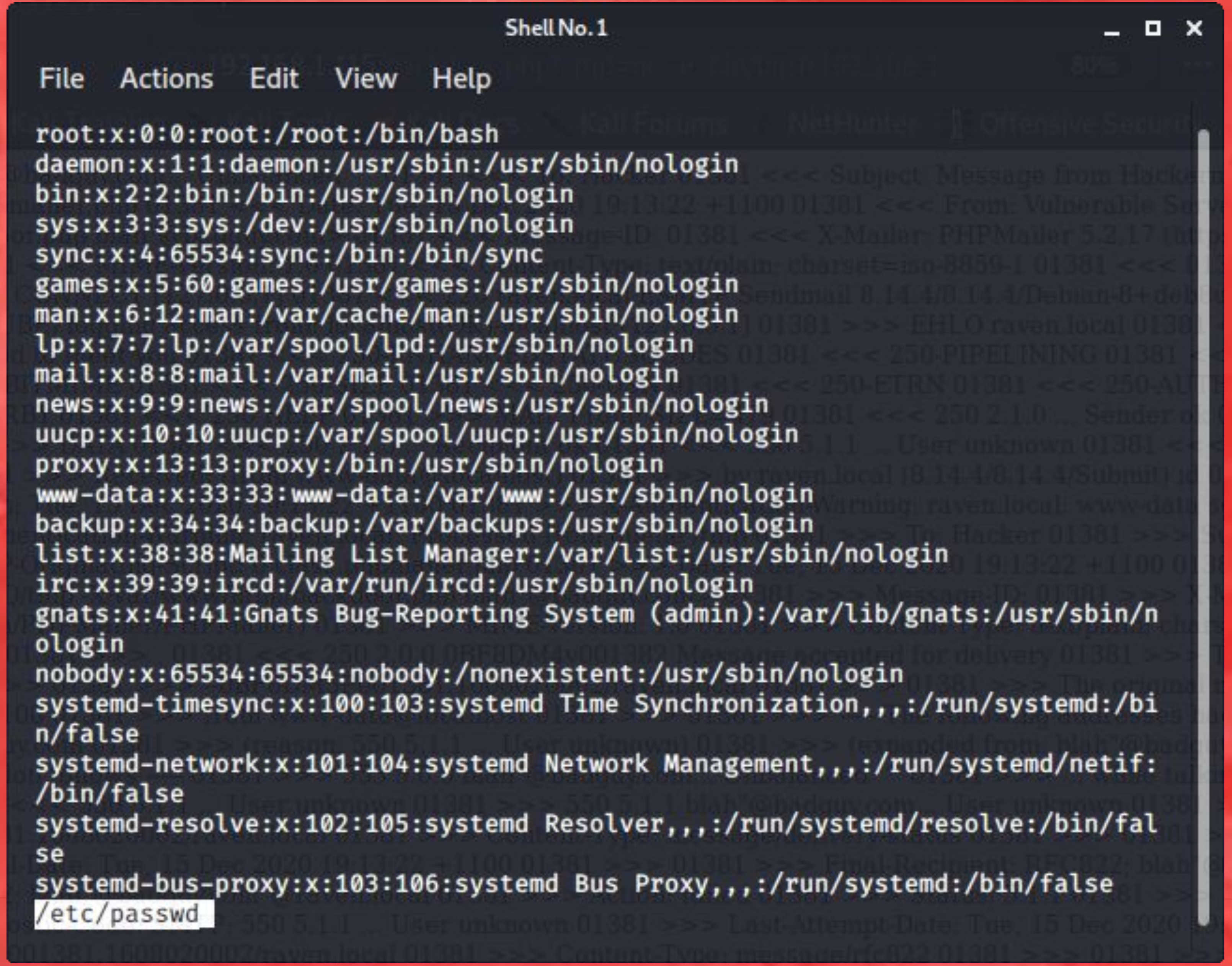
1 Used John the Ripper to crack the password hash found in MYSQL



```
root@Kali:/usr/share/wordlists# john wp_hashes.txt --wordlist=/usr/share/wo
rdlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$
) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84           (steven)
```

2 Gained user access to Stevens account and checked priveleges

3 Gained access to sensitive /etc/passwd file



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/n
ologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bi
n/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:
/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/fal
se
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
/etc/passwd
```

Hardening

Hardening Against Brute-Forceability

Patches to include:

1. Adjust password parameters

   Password lockout

2. Alarm activates when no. of 401 HTTP status codes issued in 10 second intervals reaches 5.

Why they work:

1. Inhibits brute force attacks due to password lockout

2. Alarm allows company to act quickly to mitigate attack and prevent same attack happening again

Hardening Against Sensitive Data Access

Patches to include:

1. Secure installation of MYSQL with cmd: sudo-mysql-secure-installation
2. Alarm activates when any non-specified IP address requests access to a specified directory.

Why they work:

1. Secure installation of MYSQL hardens MYSQL database in a cost effective and efficient way
2. Alarm allows company to act quickly to mitigate attack and prevent same attack happening again

Hardening Against Inadequate Data Encryption

Patches to include:

1. Better encryption of sensitive documents e.g. RSA key encryption, Advanced Encryption Standard

2. Alarm activates when no. of 401 HTTP status codes issued in 10 second intervals reaches 5.

Why they work:

1. Ensures no readable data for unauthorized users and at the very least is a deterrent to potential attackers

2. Alarm allows company to act quickly to mitigate attack and prevent same attack happening again

THE END