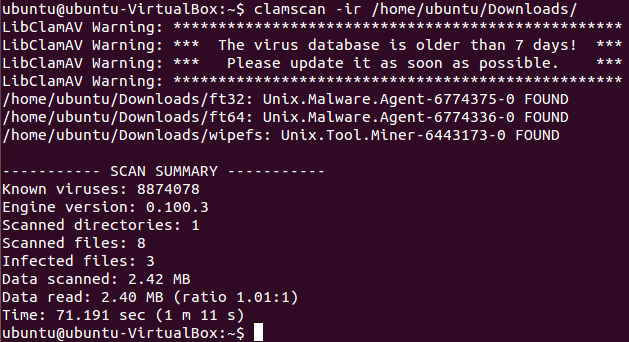
**Executive Summary: North Udan sponsored Security Attack**

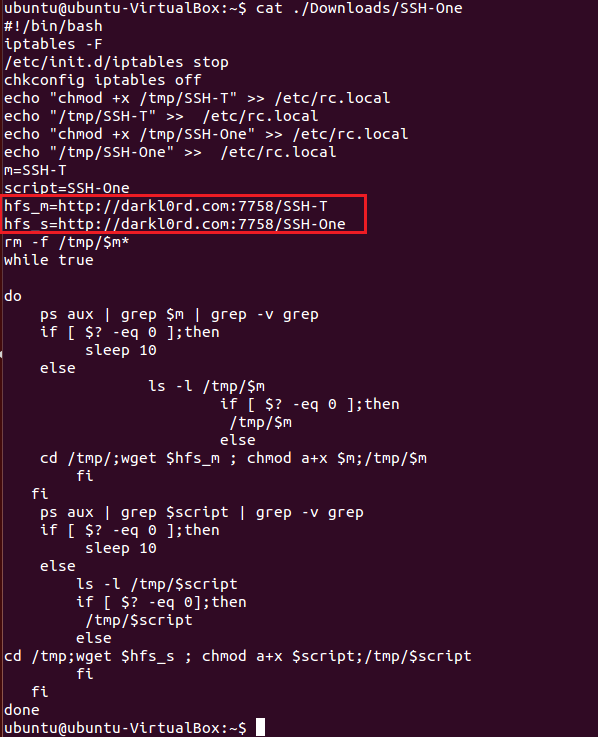
1. **Detection**

Using ClamAV scan tool, three files were reported as infected.



**Figure1 – ClamAV Scan report**

Inspection of executable files in the same directory of the infected files revealed few potential files being retrieved from internet.



**Figure2 – Suspicious script fetch from internet**

1. **Mitigation**
   1. **Investigation**

This investigation resulted in log analysis for any suspicious or malicious activity using OSSEC HIDS.

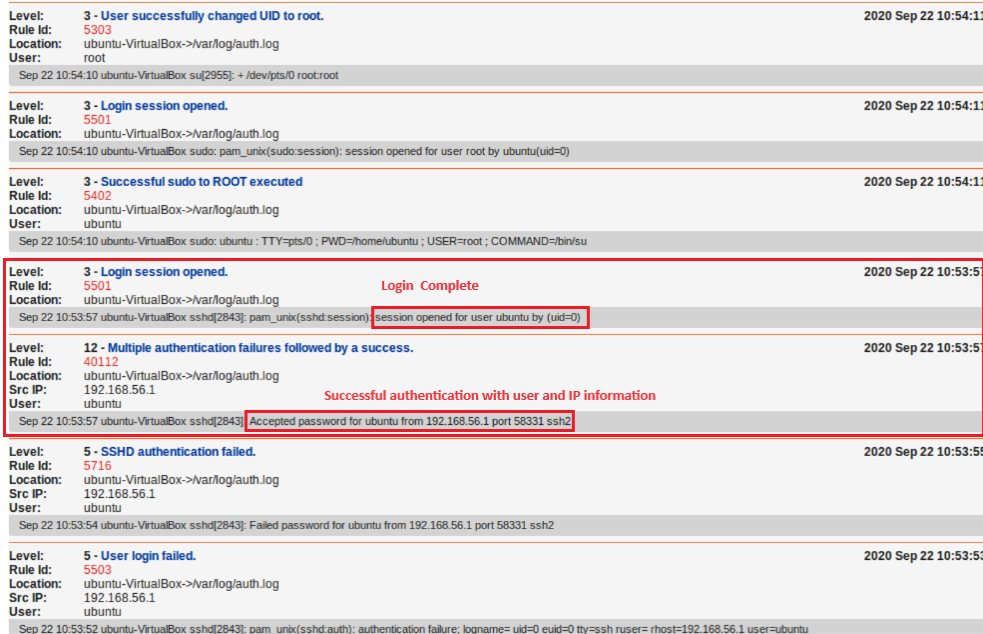
1. It was found that multiple failed login attempts within few seconds that were followed by a successful login, pointing to a brute force attack potentially using an automated process.

A screenshot of a computer

Description automatically generated

**Figure3- Failed logins**

1. The remote host IP and user that was used was identified from logs:



**Figure4 - Successful Login**

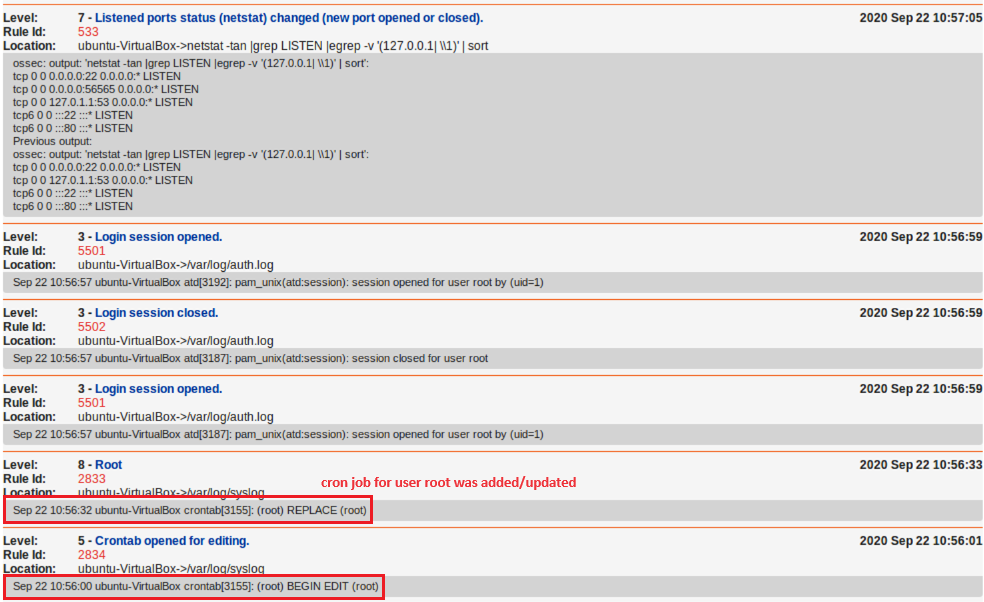
1. User elevated its rights and added a new user named ‘darklord’:

A screenshot of a computer

Description automatically generated

**Figure 5 – New User added**

1. A cron job was added for root user



**Figure6 – Updated cron job for ‘root’**

1. The script that was added to crontab was investigated. The script is ‘/etc/darklord.sh’

The script generates a copy of Linux ‘netcat’ file under the new name ‘/tmp/remotesec’. This script can read/write data across network and opens a port not used by common applications from higher port ranges. Port opened is 56565. The malicious user also checks to confirm the port is open.



**Figure6 – Updated cron job for ‘root’**

* 1. **Mitigation and recommendations**

To mitigate this attack two actions were taken:

* + 1. Block any requests from the remote host the attack was initiated from.
    2. Disabled remote SSH to ‘root’ user.

While these steps can help block access from remote host, additional steps can be taken to improve the security layers.

* Encourage use of password-less entry using public/private key pairs
* Reduce the number of failed retries for login by setting *MaxAuthTries* value in /etc/ssh/sshd\_config file.
* Use of non-standard port for SSH adds additional layer to securing the system.
* Password rotation is a good practice for added security layers.
* Carefully designing sudoer capabilities for the users can prevent unwanted elevation of rights for added security.
* Outgoing ports for malicious or suspicious scripts should be blocked

1. **Hardening**

System was scanned for vulnerabilities and few items were identified. The following actions were taken to add additional hardening.

* + 1. The server is running a web service. It is recommended to disabled/remove the version banner. This was done by updating apache2 configuration.
    2. A new user was added so the web service runs with the new lower privilege account.

Further actions are recommended for additional hardening:

* Patch system to remove weak encryption and MAC algorithms
* Disable HTTP debugging and tracing through apache2 configuration update