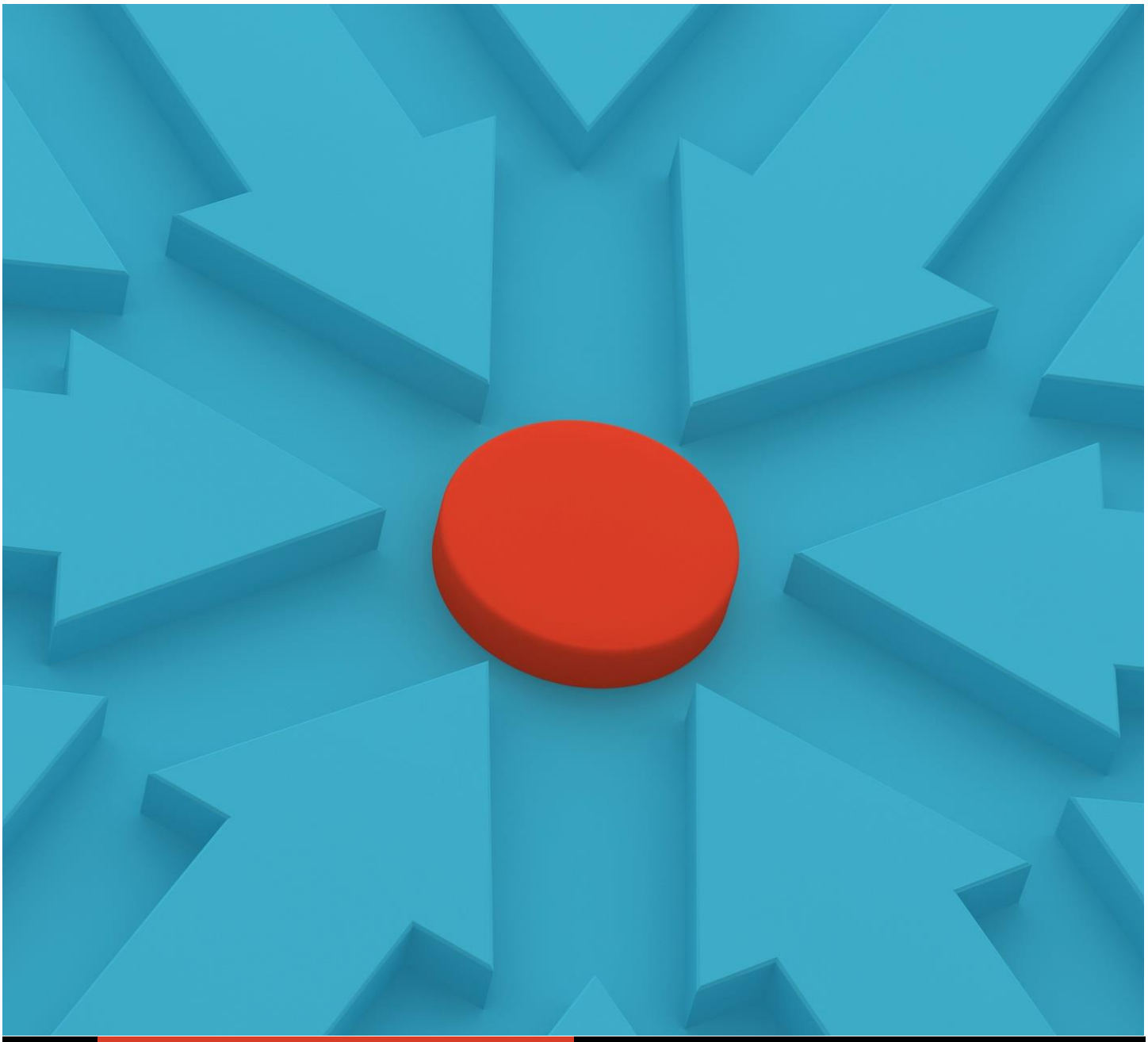
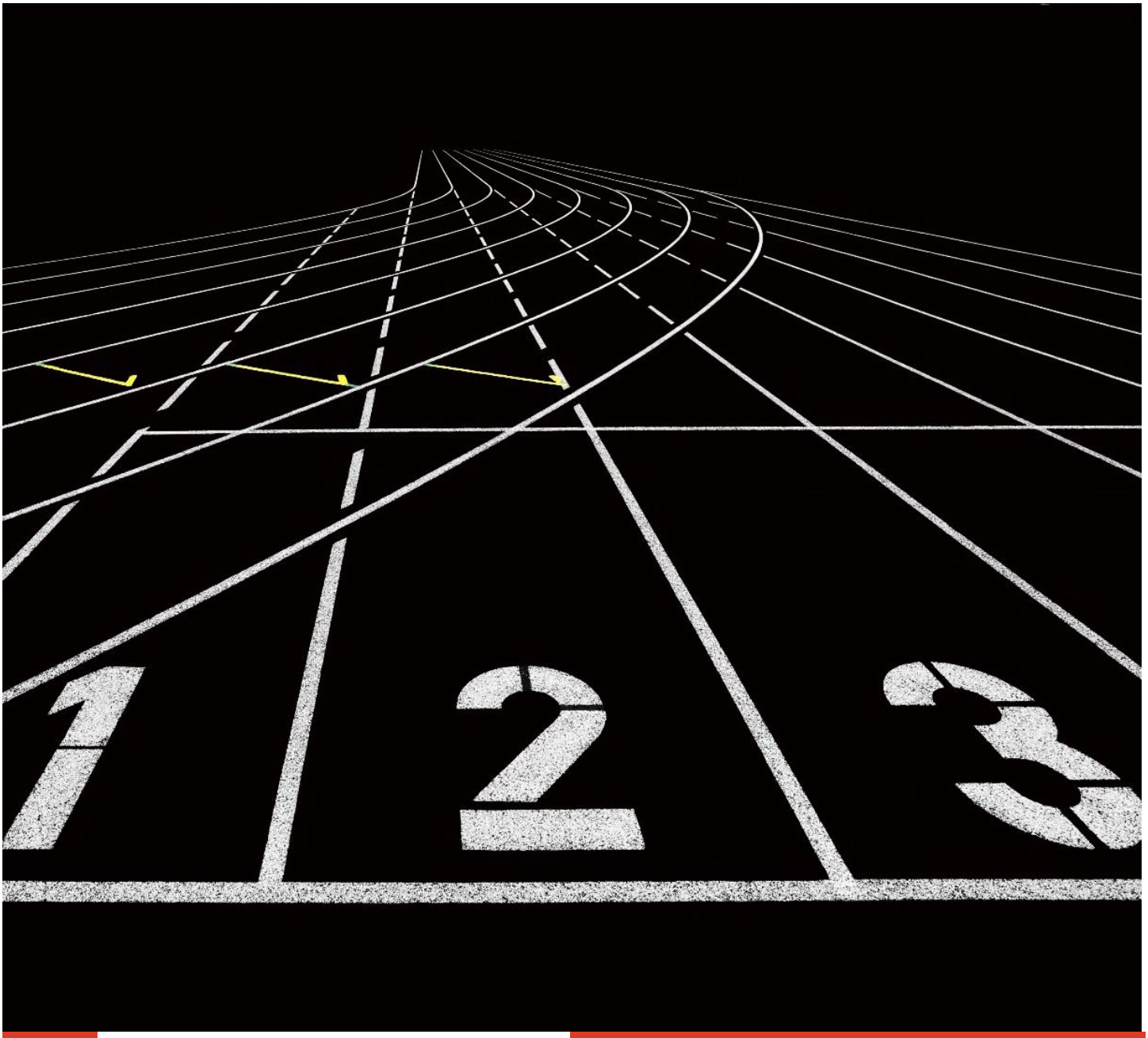


EXECUTIVE SUMMARY

2022

PAVLO TEYFEL

pavloteyfel@gmail.com



ATTACK FROM NORTH UDAN

The National Peace Agency of North Udan managed to compromise a Linux server which serves as a jump host to connect the Tridanium processing plant to the internet. They attempted to brute force the password of an employee account which triggered a security alarm. The security team immediately called onboard to respond to the security alarm and contain the ongoing cyberattack. The investigation began from the compromised jump box to detect and mitigate the threats. Since it's a mission-critical server, it is important to harden the server to proactively defeat future attacks from North Udan.

THREAT DETECTION

Malware Scanning

During malware scanning with the ClamAV, the following infected files were identified on the server:

- /home/ubuntu/Downloads/ft32: Unix.Malware.Agent-6774375-0 FOUND
- /home/ubuntu/Downloads/ft64: Unix.Malware.Agent-6774336-0 FOUND
- /home/ubuntu/Downloads/wipefs: Unix.Tool.Miner-6443173-0 FOUND

After the automatic scanning I additionally found a malicious file that contained:

- /home/ubuntu/Downloads/SSH-One

This is a bash file, that erases all the firewall rules, stops the firewall and turns if off entirely. It has embedded callout to the darkl0rd.com, a Command & Control server of the National Peace Agency. It also modified the /etc/rc.local file to start some other malicious files after system restart:

- /tmp/SSH-T
- /tmp/SSH-One

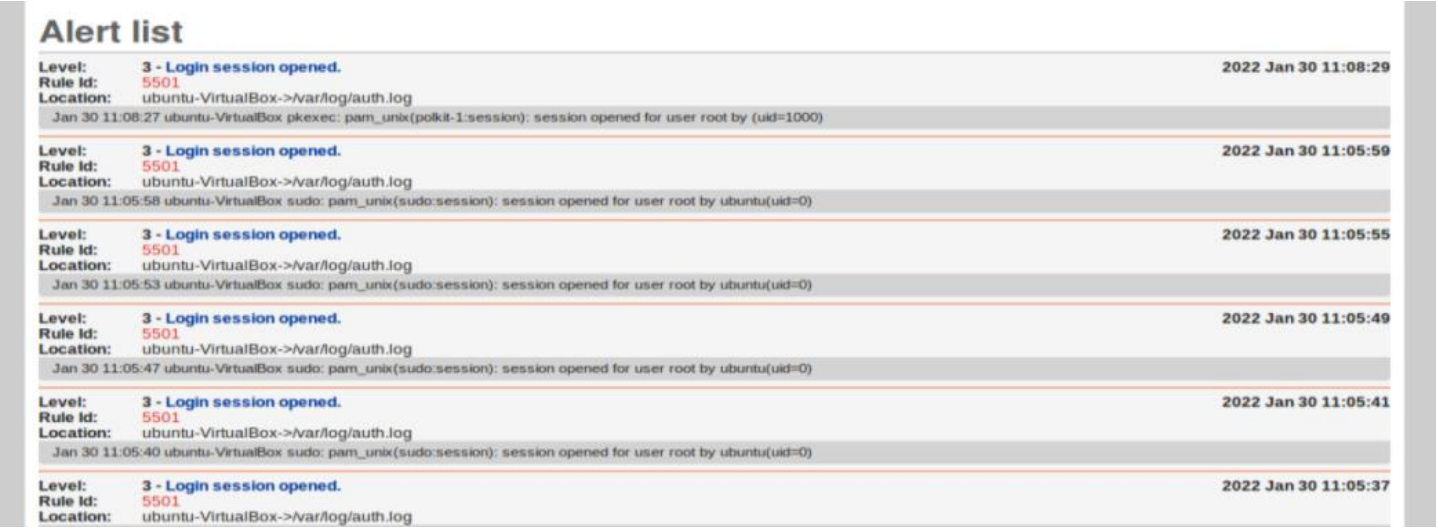
Improved Defense

After analyzing the manually found malware file, I prepared an additional rule to the malware detection software to have defense control against future threats.

THREAT MITIGATION

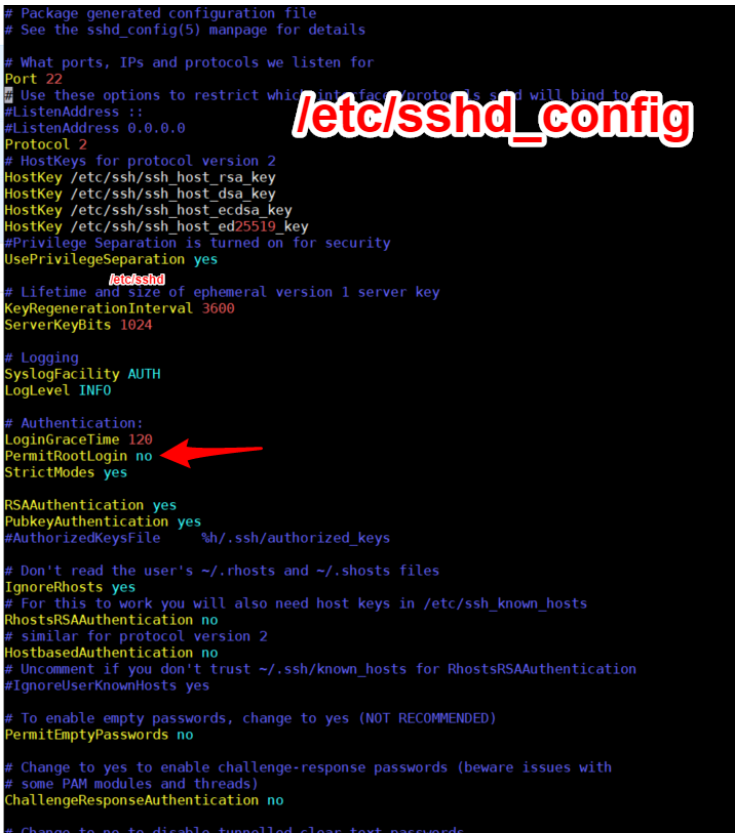
The Attacker's IP

After ensuring that the Host Based Intruder Detection System (HIDS) is up and running, I identified the attacker's IP address: 192.168.56.1 by means of the OSSEC.



Backdoor Details

From OSSEC it can be seen, that the ubuntu user after multiple unsuccessful login attempts has successfully logged in, changed UID to root and created a new user named "darklord". Among the running processes I saw the "remotesec" process running on the 56565 port that was started by the root user.



Mitigation Measures

I turned on the firewall and created a rule to block all incoming requests from the "192.168.56.1" IP address. The SSH was configured to not allow root login through it.

Additional Measures

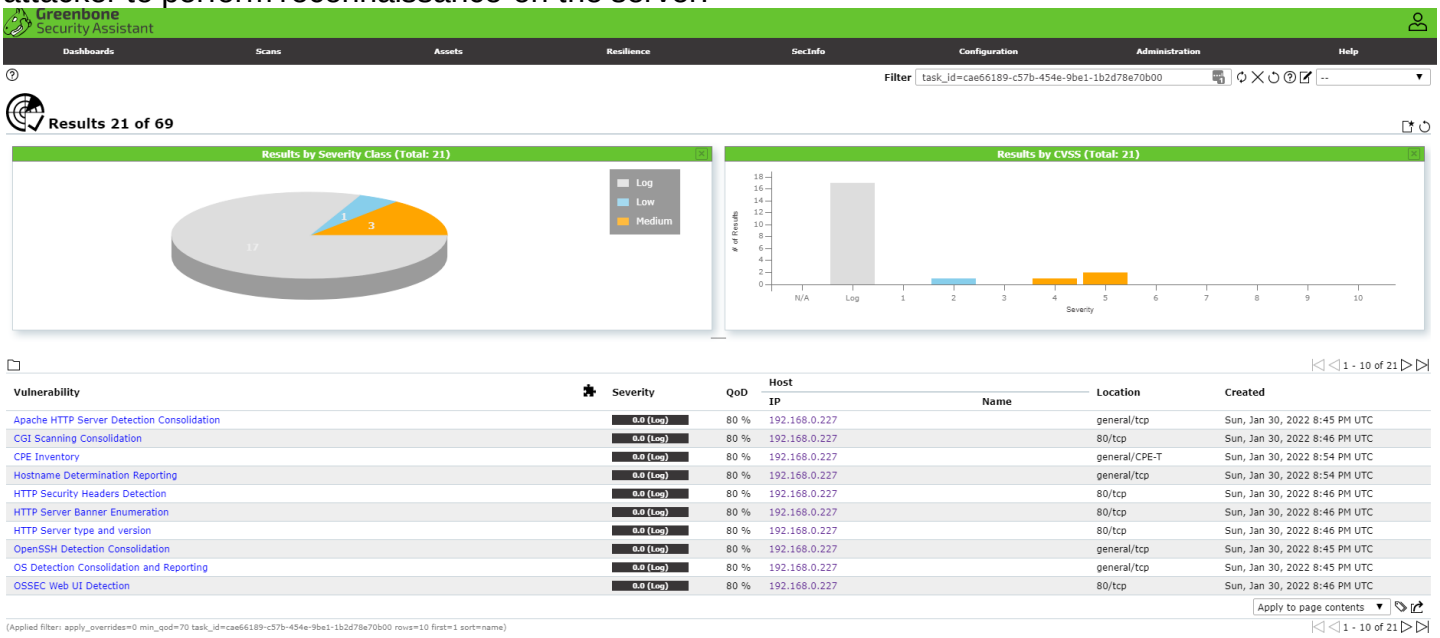
- Limit the login tries to max 3 attempts though the SSH. This can prevent brute force attacks.
- Configure SSH keys for login instead of passwords can make it even more difficult for attackers to brute force login credentials. Disable password-based access and instead generate public keys on the client machines and add them to the server.

- Define a list of permitted users. By doing this, you ensure that any other user is not able to log into the server even if it belongs to the same access group as other users in the list.
- Change the default port of the SSH service. This can help deflect automated bots and scanners who are looking for open port 22 randomly on the internet to brute force login credentials.
- Use multi-factor authentication (MFA) can be another way of further securing the client-server authentication.

HARDENING

Apache Server

I scanned the server with OpenVAS vulnerability scanner to identify potential weaknesses. As a result, the installed Apache HTTP server was misconfigured and can serve as an attack point in future incidents. I removed the version banner from being publicly visible. This would make it difficult to attacker to perform reconnaissance on the server.



Privileges

A new user and group were created “apache-user” and “apache-group”, to ensure that the Apache server runs as low privileged user.

Besides that, the root password was changed to further ensure that the attackers won't be able to use **sudo** to elevate their privilege to root.