# Windows Host Attack Detection

**Author:** Abhinav Kumar

## Environment

- Windows 11 Host
- Windows 10 Virtual Machine (Target)
- Kali Linux Virtual Machine (Attacker)

## 1. Project Overview

This project focuses on **host-based attack detection** using native Windows logging, without relying on third-party security tools. It demonstrates how Windows Security logs can be used to detect and analyze authentication-related activity, with a specific focus on failed and successful Remote Desktop Protocol (RDP) logon attempts. A controlled attack simulation was conducted from a Kali Linux virtual machine against a Windows 10 virtual machine, and the resulting security events were analyzed using Windows Event Viewer.

The objectives of this project are to demonstrate:

- Practical understanding of Windows security logging
- Identification of brute-force style login attempts
- Correlation of attacker actions with Windows security events

## 2. Lab Architecture

- **Host Operating System:** Windows 11
- **Target System:** Windows 10 Virtual Machine
- **Attacker System:** Kali Linux Virtual Machine
- **Network Configuration:** Host-only adapter to allow isolated VM-to-VM communication

## 3. Tools Used

- **Windows Event Viewer:** Security log analysis
- **FreeRDP (xfreerdp):** RDP authentication attempts from Kali Linux
- **Kali Linux:** Attack simulation platform
- **Windows Security Auditing:** Event generation and monitoring
- **VirtualBox:** Virtualized lab setup

# 4. Enabling and Observing Windows Security Logs

Windows Security auditing was enabled to capture authentication and process-related events. The following Event IDs were monitored throughout the project:

- **Event ID 4625:** Failed logon attempt
- **Event ID 4624:** Successful logon
- **Event ID 4688:** Process creation

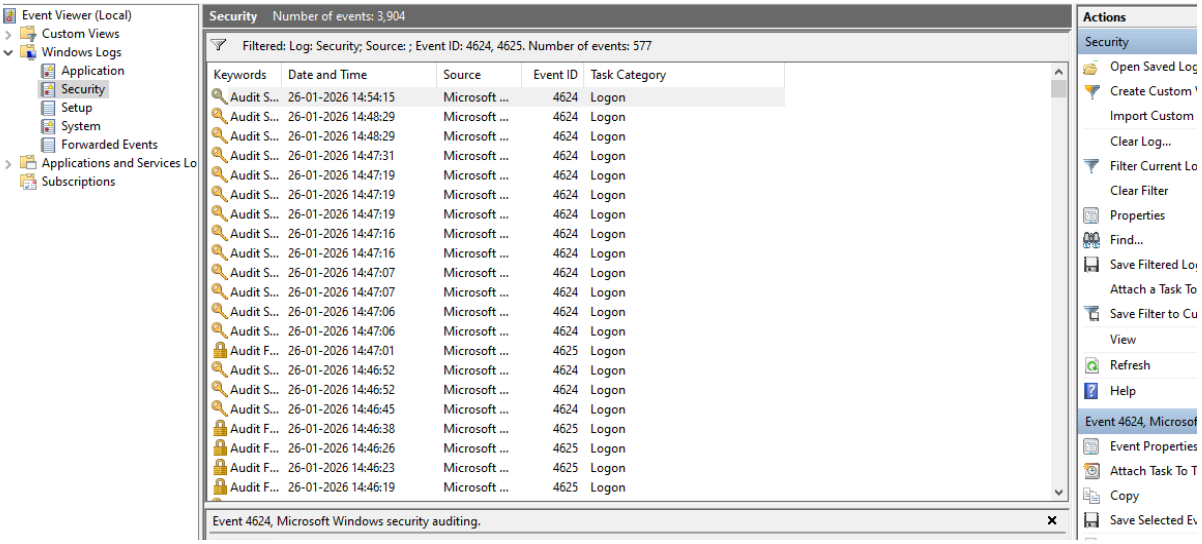
Windows Event Viewer was used to filter and analyze these events in real time.

# 5. Failed RDP Login Attempts (Attack Simulation)

From the Kali Linux virtual machine, multiple RDP login attempts were performed using incorrect credentials via the `xfreerdp` tool. These attempts were intentionally unsuccessful to simulate unauthorized access or brute-force behavior.

Each failed attempt generated corresponding **Event ID 4625 (Audit Failure)** entries in the Windows Security log, confirming that Windows accurately recorded failed authentication activity.

RDP was chosen because it is a common attack vector in real-world Windows environments and frequently targeted during initial access attempts.



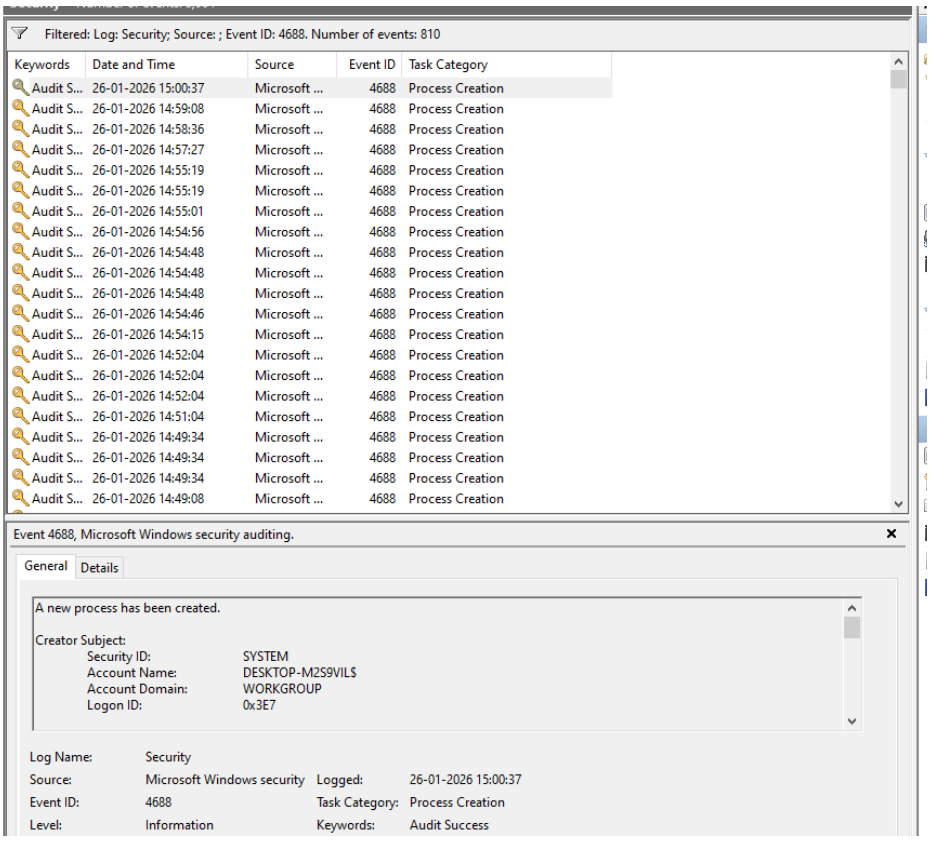

# 6. Successful RDP Login

After several failed attempts, valid credentials were used to successfully authenticate to the Windows 10 virtual machine via RDP.

This resulted in the generation of:

- **Event ID 4624:** Successful logon

The appearance of a successful logon event following multiple failed attempts illustrates a common attack pattern and highlights the importance of monitoring authentication trends rather than individual events.

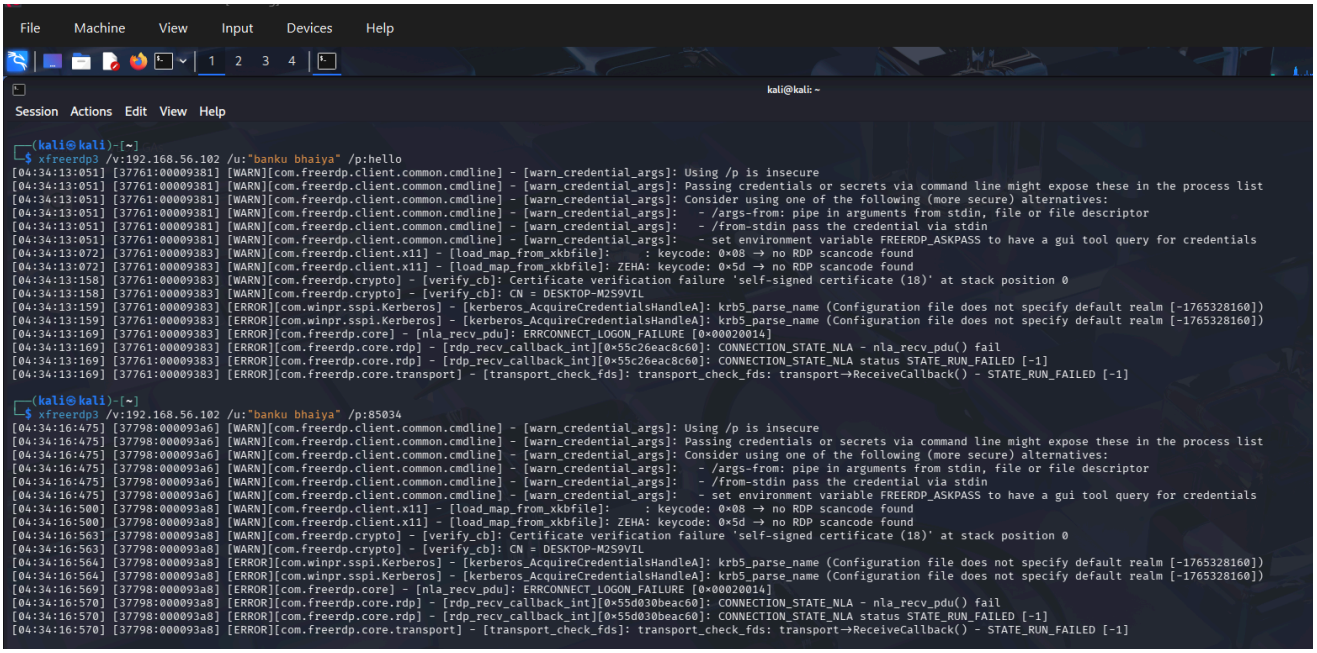



# 7. Process Creation Monitoring

Following successful authentication, Windows recorded **Event ID 4688**, indicating the creation of new processes under the authenticated user session.

Monitoring process creation events is critical for:

- Detecting post-compromise behavior
- Identifying suspicious or unauthorized processes launched after login

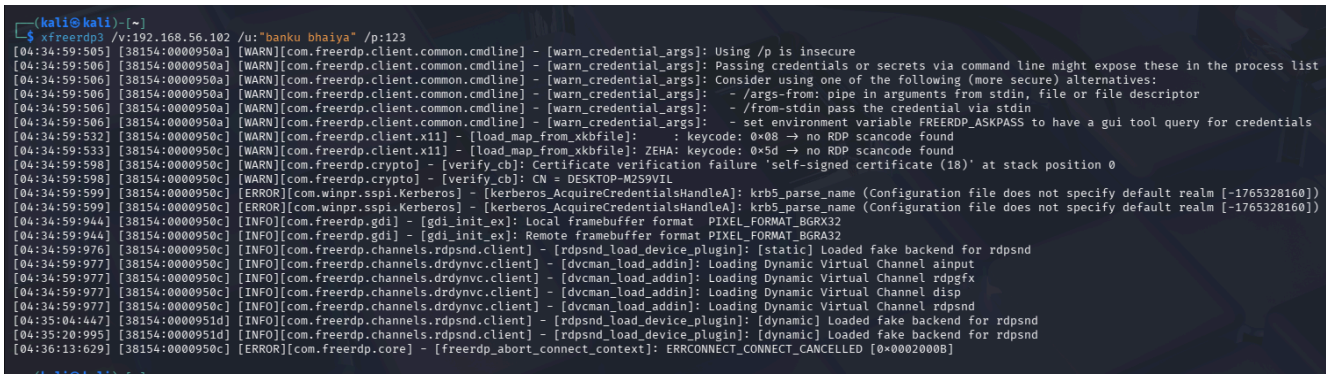



# 8. Attacker Perspective (Kali Linux)

On the attacker system, `xfreerdp` command output provided feedback on:

- Connection failures
- Authentication errors
- Successful login attempts

These outputs directly correlate with the Windows Security events, demonstrating visibility from both attacker and defender perspectives.




# 9. Analysis and Event Correlation

By correlating timestamps between Kali Linux command execution and Windows Security logs, the following relationships were identified:

- Failed RDP attempts correspond to **Event ID 4625**
- Successful RDP authentication corresponds to **Event ID 4624**

- Activity within the authenticated session corresponds to **Event ID 4688**

This correlation process reflects real-world blue team and Security Operations Center (SOC) analysis techniques.

# 10. Key Learnings

- Windows Security logs provide detailed insight into authentication activity.
- Failed login attempts can be reliably identified using Event ID 4625.
- Successful compromises leave clear forensic evidence through Event IDs 4624 and 4688.
- Proper log analysis enables accurate reconstruction of an attack timeline and supports early detection of suspicious behavior.

# 11. Conclusion

This project presents a realistic and beginner-friendly demonstration of Windows log analysis and RDP attack detection. By simulating authentication attacks and analyzing Security logs, the project highlights practical defensive skills applicable to SOC analyst, blue team, and cybersecurity monitoring roles.

Potential future enhancements include:

- Automated log parsing
- Alert generation for brute-force detection
- Forwarding Windows logs to a SIEM platform