Murad Yarmammadov

Overview

This walkthrough documents a small SOC-style investigation in my Elastic (ELK) home lab. Scenario: an attacker performs a **password brute force against RDP** on a Windows Server, gains access, and executes **post-login discovery commands**. I then detect and investigate the activity in Kibana using Windows Security logs and Sysmon.

Lab Setup

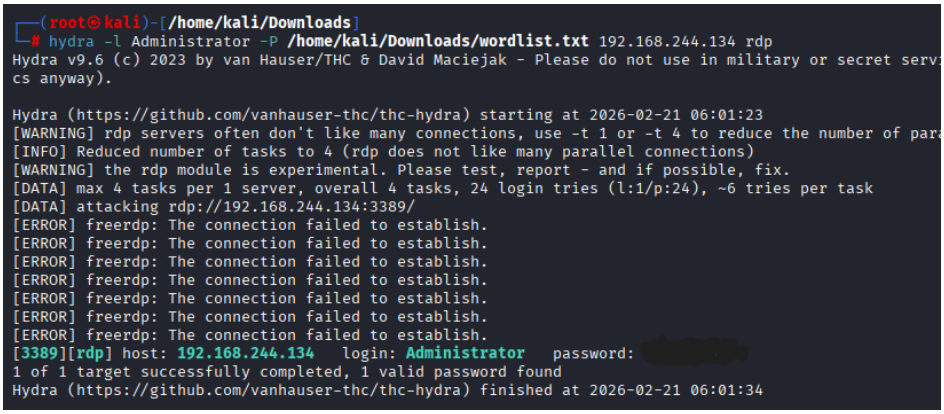
Hosts

- **Attacker (Kali Linux):** 192.168.244.128
- **Target (Windows Server 2022):** 192.168.244.134 (Elastic Agent + Sysmon installed)
- **ELK/Fleet Server:** (Elastic stack + Fleet for agent management)

Attack Walkthrough

1) Brute force attack

I executed an RDP brute force attempt from Kali using **Hydra** with a wordlist against the Windows Server.



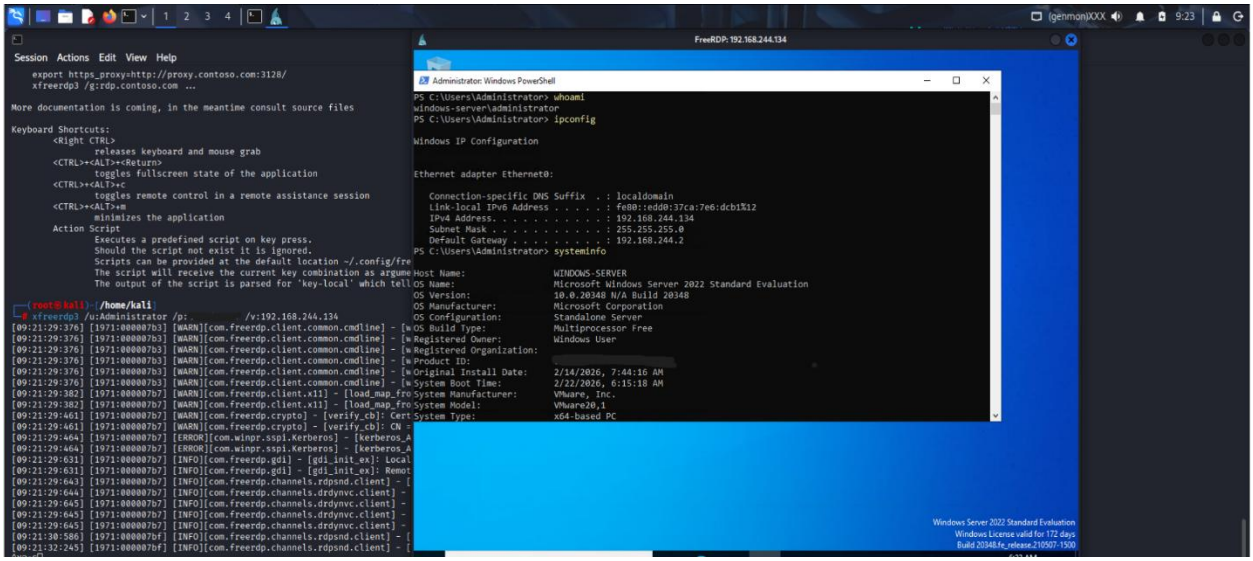
Result: Hydra identified valid credentials for the targeted account (password **redacted** in this report).

2) RDP login + command execution

Using the discovered credentials, I logged into the target over RDP using xfreerdp, then executed common discovery commands in PowerShell.

Example commands executed (discovery):

- whoami
- whoami /groups
- ipconfig
- systeminfo
- netstat -ano
- net localgroup administrators

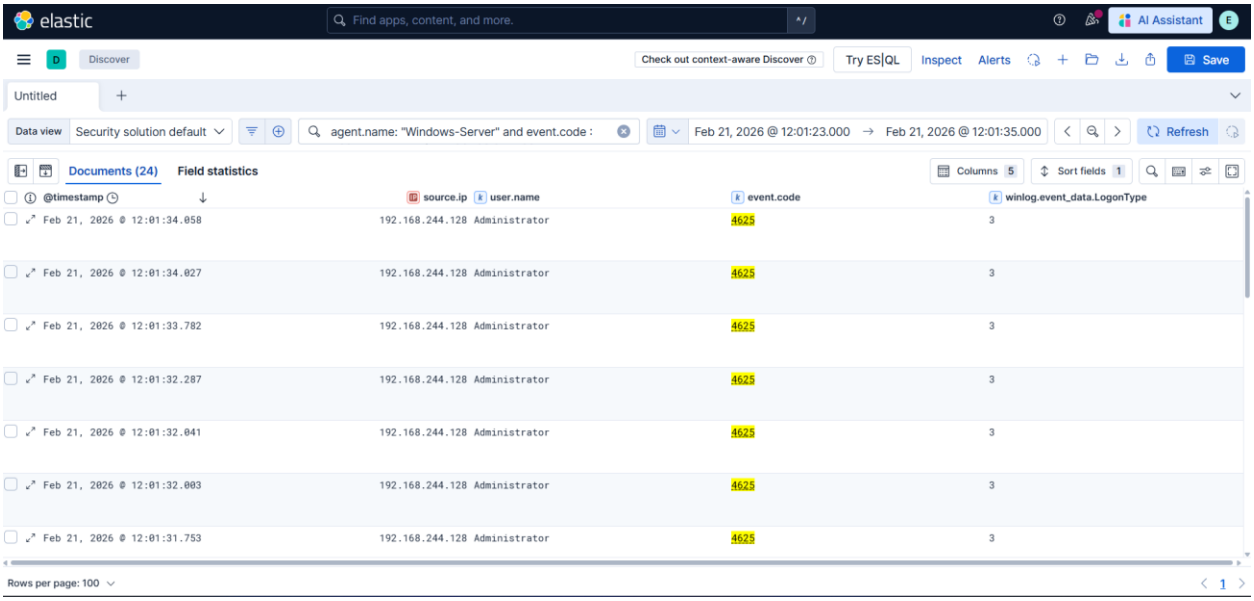


Detection & Investigation in Kibana

1) Identify brute force attempts in logs.

In Kibana (Discover), I filtered for failed authentications:

- **Event ID:** 4625 (Failed logon)
- Observed repeated failures from attacker IP 192.168.244.128 targeting Administrator
- LogonType in my failures shows **3** (common during NLA/authentication phase)



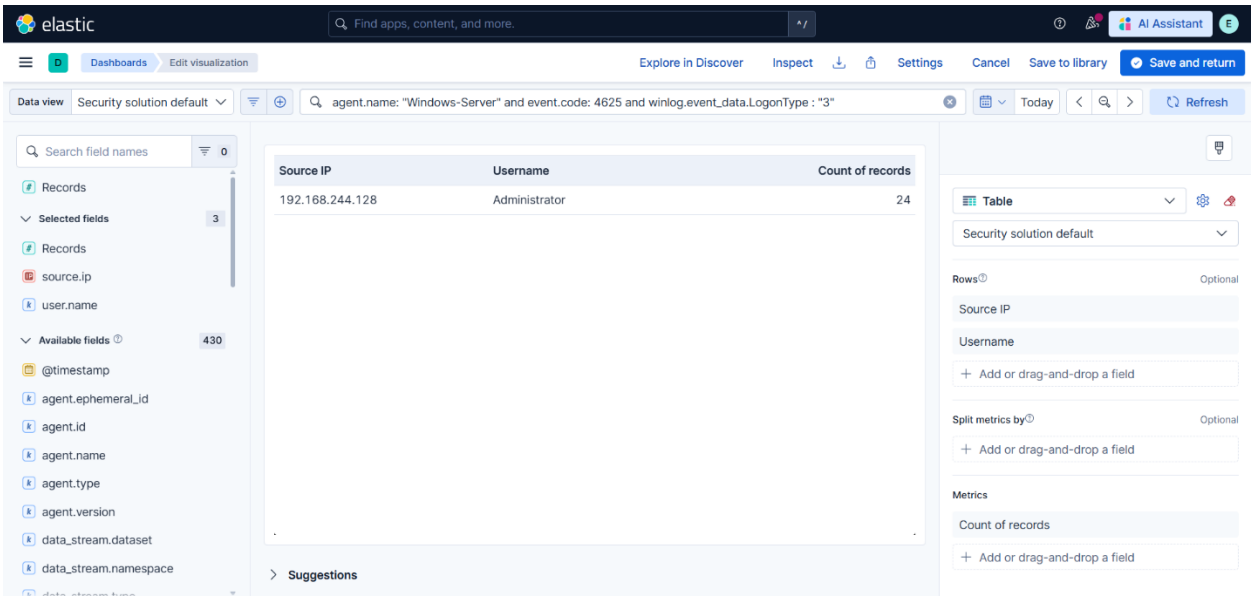
KQL:

agent.name: "Windows-Server" and event.code : 4625 and source.ip : "192.168.244.128"

2) Create visualization: RDP Failed and Successful Authentications

I created a Kibana table visualization to summarize failed RDP authentications grouped by:

- Event ID: 4625 (Failed logon)
- LogonType: 3 (Network Logon)
- Grouped by source IP, username and count of records

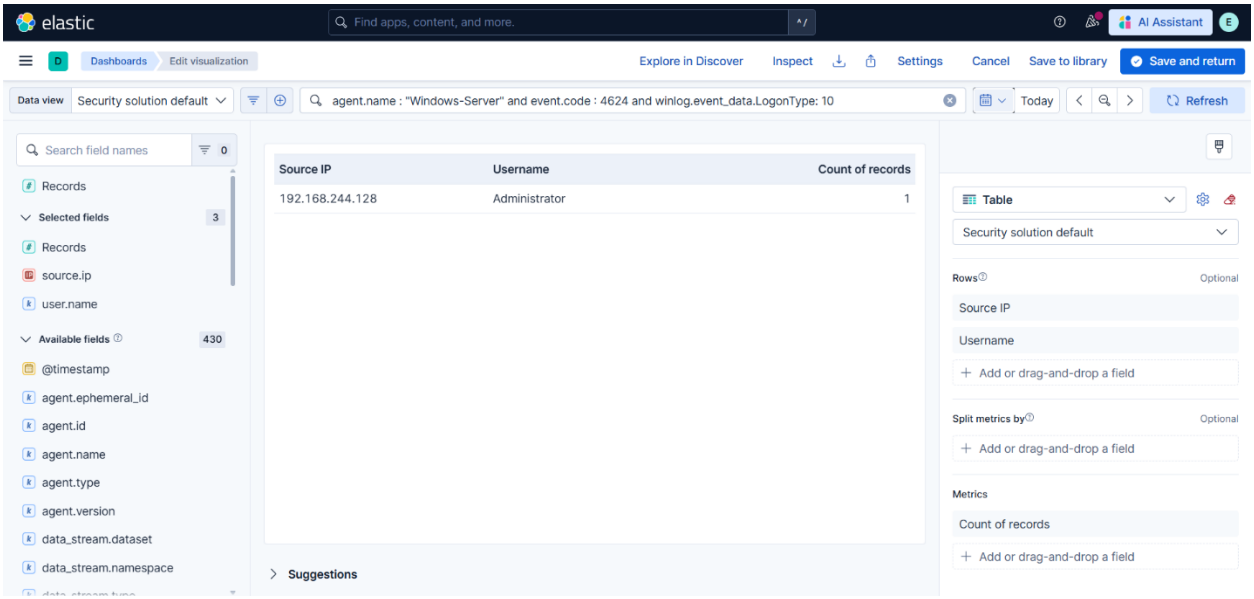


KQL:

agent.name: "Windows-Server" and event.code: 4625 and winlog.event_dataLogonType: 3

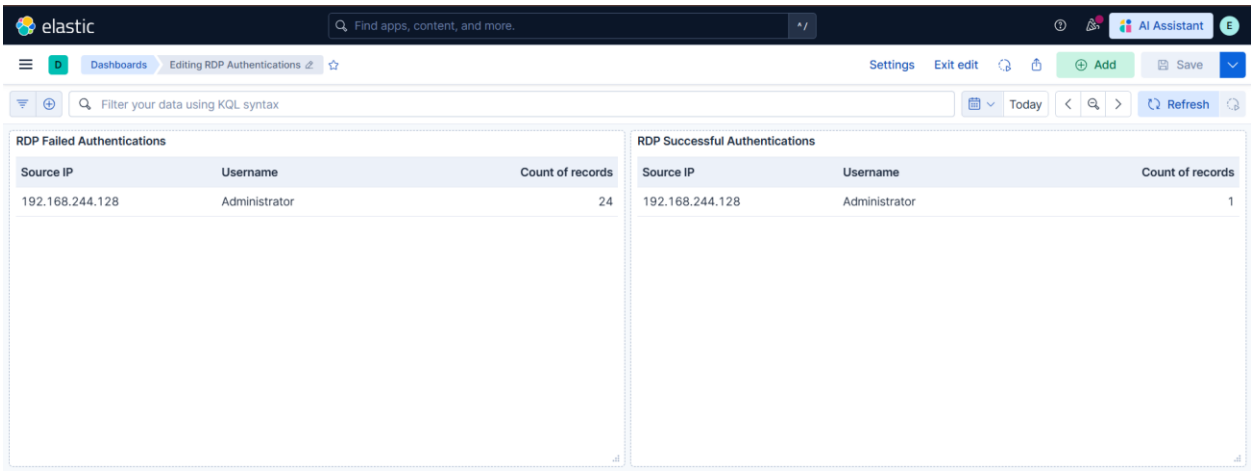
I created a second Kibana table visualization for successful logons:

- Event ID: 4624 (Successful logon)
- LogonType: 10 (RemoteInteractive → RDP)
- Grouped by source IP, username and count of records.



I combined both visualizations in a dashboard to show the complete authentication story:

- many failures from 192.168.244.128
- followed by a successful RDP authentication from the same IP

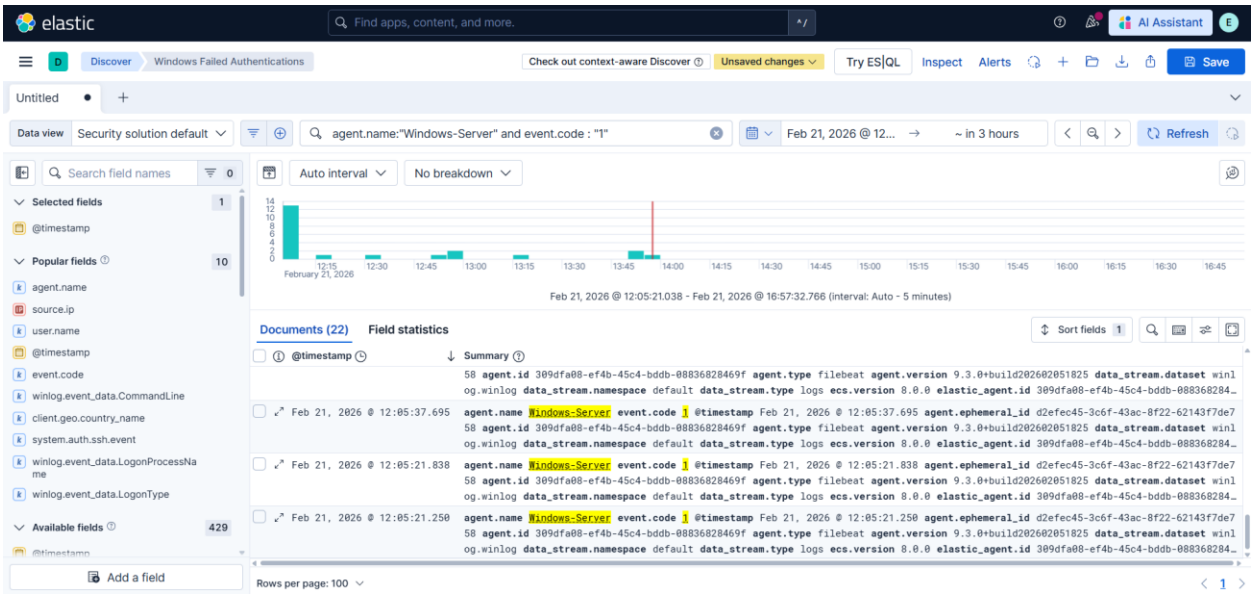


Post-Login Analysis

1) Pivot to Sysmon Process Create events (Event ID 1: Process creation)

After confirming the successful login, I pivoted to Sysmon process creation logs:

- **Sysmon Event ID:** 1 (Process Create)
- Goal: identify commands/processes executed after the compromise



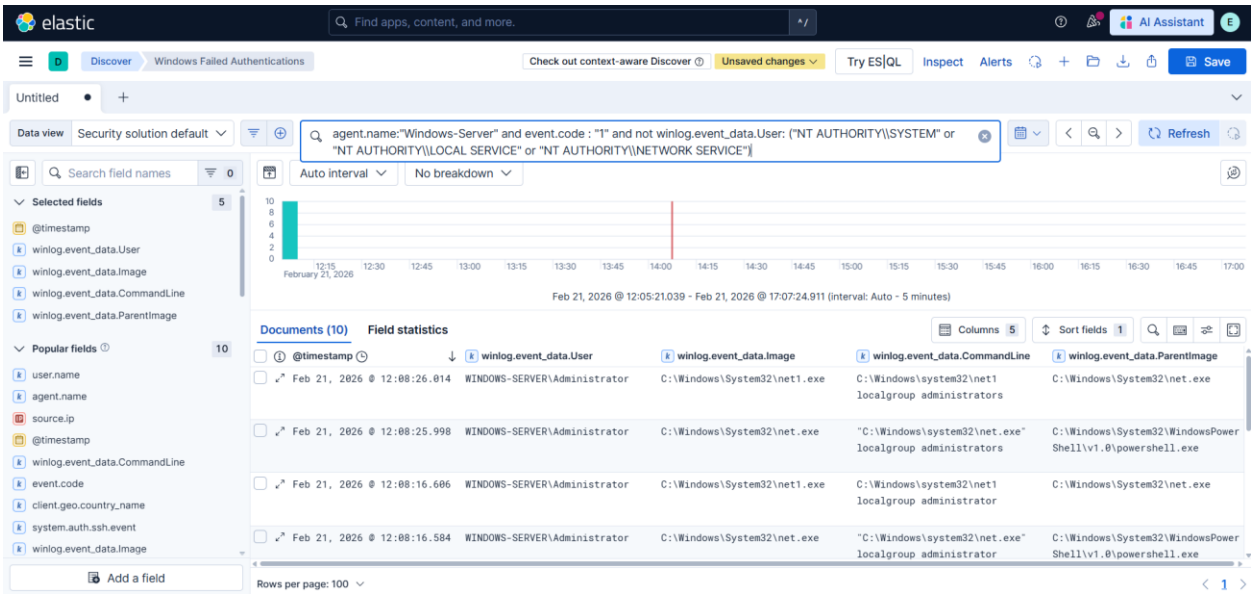
KQL:

agent.name: “Windows-Server” and event.code: “1”

During this time window, there were **22 Sysmon process creation events**. However, some of these processes were generated by built-in service accounts (normal background activity), such as:

- NT AUTHORITY\\SYSTEM
- NT AUTHORITY\\LOCAL SERVICE
- NT AUTHORITY\\NETWORK SERVICE

To focus specifically on **interactive attacker activity**, I filtered out those service accounts and kept only user-driven execution.



KQL:

agent.name:"Windows-Server"
and event.code:"1"
and not winlog.event_data.User:(
"NT AUTHORITY\\SYSTEM" or
"NT AUTHORITY\\LOCAL SERVICE" or
"NT AUTHORITY\\NETWORK SERVICE")

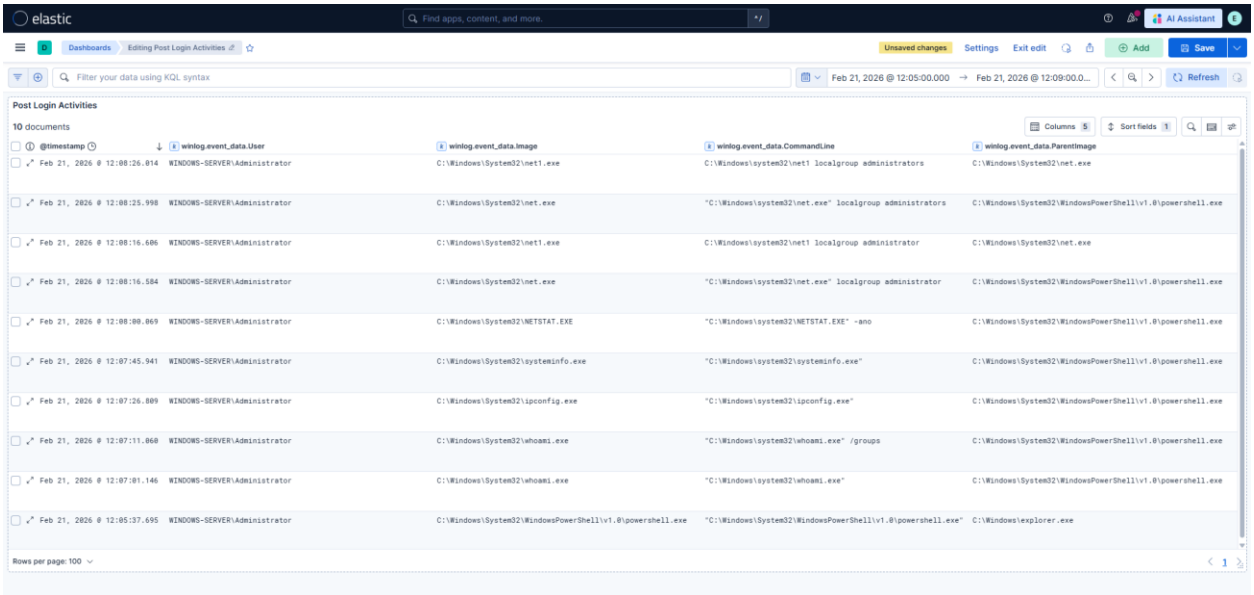
This reduced noise and allowed me to clearly identify the processes executed under the compromised user context

2) Post-Login Activity Dashboard

I built a post-login activity view showing processes executed by the compromised account with command lines and parents.

Key findings from Sysmon (executed under WINDOWS-SERVER\Administrator):

- PowerShell spawned at 12:05:37 (parent: explorer.exe) → indicates an interactive session
- Discovery commands executed shortly after via PowerShell:
    - whoami, whoami /groups
    - ipconfig
    - systeminfo
    - netstat -ano
    - net localgroup administrators (via net.exe/net1.exe)



Timeline Summary (with timestamps)

- Brute force activity detected (Failed logons – Event ID 4625, LogonType 3)
    - Start: Feb 21, 2026 @ 12:01:23.640
    - End: Feb 21, 2026 @ 12:01:34.058
    - Source IP: 192.168.244.128 → Target account: Administrator
- Successful compromise (Successful RDP logon – Event ID 4624, LogonType 10)
    - Feb 21, 2026 @ 12:01:34.312
    - Source IP: 192.168.244.128 → User: Administrator
- Post-login activity (Sysmon – Event ID 1: Process Create)
    - Shortly after the successful login, an interactive PowerShell session was spawned and multiple discovery commands were executed under WINDOWS-SERVER\Administrator, including:
        - whoami / whoami /groups
        - ipconfig
        - systeminfo
        - netstat -ano
        - net localgroup administrators

MITRE ATT&CK Mapping

- **T1110 – Brute Force** (4625 burst patterns)
- **T1021.001 – Remote Services: RDP** (4624 LogonType 10)
- **T1059.001 – PowerShell** (powershell.exe process creation + child commands)
- **Discovery** (examples):
    - systeminfo → System Information Discovery
    - ipconfig, netstat → Network Discovery
    - whoami /groups, net localgroup administrators → Permission Groups Discovery