

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.

```
(root@kali)~[/home/kali/Downloads]
# hydra -l Administrator -P /home/kali/Downloads/wordlist.txt 192.168.244.134 rdp
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-21 06:01:23
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of par
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:1/p:24), ~6 tries per task
[DATA] attacking rdp://192.168.244.134:3389/
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.244.134 login: Administrator password: 
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-21 06:01:34
```

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

The screenshot shows a Windows Remote Desktop session titled 'FreeRDP: 192.168.244.134'. The terminal window is running a Windows PowerShell session as Administrator. The user has executed several commands: 'export https_proxy=http://proxy.contoso.com:3128/xfreerdp3 /g:rdp.contoso.com ...', 'whoami' (output: PS C:\Users\Administrator> whoami windows-server/administrator), 'whoami /groups' (output: PS C:\Users\Administrator> ipconfig), 'ipconfig' (output: Windows IP Configuration, Ethernet adapter Ethernet0: Connection-specific DNS Suffix . : localdomain, Link-local IPv6 Address : fe80::edd0:37ca:7ee:dc8132, IPv4 Address. : 192.168.244.134, Subnet Mask : 255.255.255.0, Default Gateway : 192.168.244.2), 'systeminfo' (output: PS C:\Users\Administrator> systeminfo), and 'netstat -ano' (output: PS C:\Users\Administrator> netstat -ano). The terminal also shows a list of system information including OS Name, Version, Manufacturer, Configuration, Product ID, Original Install Date, System Boot Time, System Manufacturer, System Model, System Type, and OS-based PC.

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)

@timestamp	source.ip	user.name	event.code	winlog.event_data.LogonType
Feb 21, 2026 @ 12:01:34.058	192.168.244.128	Administrator	4625	3
Feb 21, 2026 @ 12:01:34.027	192.168.244.128	Administrator	4625	3
Feb 21, 2026 @ 12:01:33.782	192.168.244.128	Administrator	4625	3
Feb 21, 2026 @ 12:01:32.287	192.168.244.128	Administrator	4625	3
Feb 21, 2026 @ 12:01:32.041	192.168.244.128	Administrator	4625	3
Feb 21, 2026 @ 12:01:32.003	192.168.244.128	Administrator	4625	3
Feb 21, 2026 @ 12:01:31.753	192.168.244.128	Administrator	4625	3

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 login)
- LogonType: 3 (Network Logon)
- Grouped by source IP, username and count of records

elastic Find apps, content, and more. AI Assistant

Dashboards Edit visualization Explore in Discover Inspect Settings Cancel Save to library Save and return

Data view Security solution default agent.name: "Windows-Server" and event.code: 4625 and winlog.event_data.LogonType : "3" Today Refresh

Search field names 0

Selected fields 3

- Records
- source.ip
- user.name

Available fields 430

- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- data_stream.dataset
- data_stream.namespace

Source IP	Username	Count of records
192.168.244.128	Administrator	24

Suggestions

Table Security solution default

Rows Optional

Source IP

Username

+ Add or drag-and-drop a field

Split metrics by Optional

+ Add or drag-and-drop a field

Metrics

Count of records

+ Add or drag-and-drop a field

KQL:

agent.name: "Windows-Server" and event.code: 4625 and winlog.event_data.LogonType: 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.

elastic Find apps, content, and more. AI Assistant

Dashboards Edit visualization Explore in Discover Inspect Settings Cancel Save to library Save and return

Data view Security solution default agent.name: "Windows-Server" and event.code: 4624 and winlog.event_data.LogonType: 10 Today Refresh

Search field names 0

Selected fields 3

- Records
- source.ip
- user.name

Available fields 430

- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- data_stream.dataset
- data_stream.namespace

Source IP	Username	Count of records
192.168.244.128	Administrator	1

Suggestions

Table Security solution default

Rows Optional

Source IP

Username

+ Add or drag-and-drop a field

Split metrics by Optional

+ Add or drag-and-drop a field

Metrics

Count of records

+ Add or drag-and-drop a field

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

The dashboard displays two tables side-by-side. The left table, 'RDP Failed Authentications', has columns for Source IP, Username, and Count of records. It shows one entry for Source IP 192.168.244.128 and Username Administrator with a count of 24. The right table, 'RDP Successful Authentications', has the same columns and shows one entry for Source IP 192.168.244.128 and Username Administrator with a count of 1.

RDP Failed Authentications		
Source IP	Username	Count of records
192.168.244.128	Administrator	24

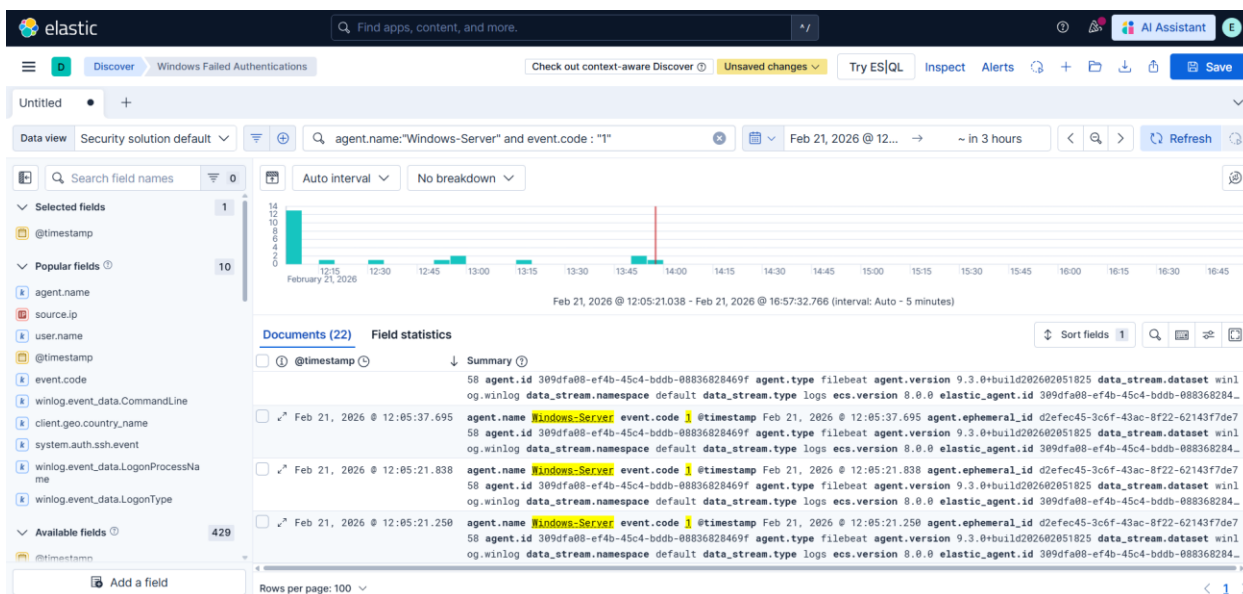
RDP Successful Authentications		
Source IP	Username	Count of records
192.168.244.128	Administrator	1

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



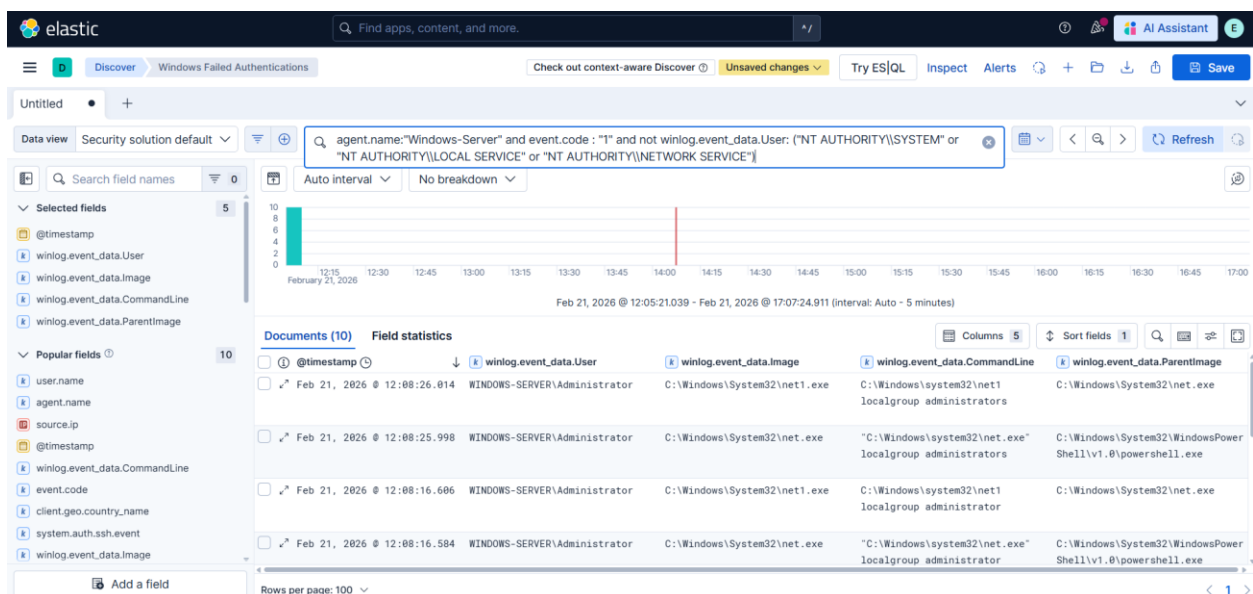
KQL:

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")

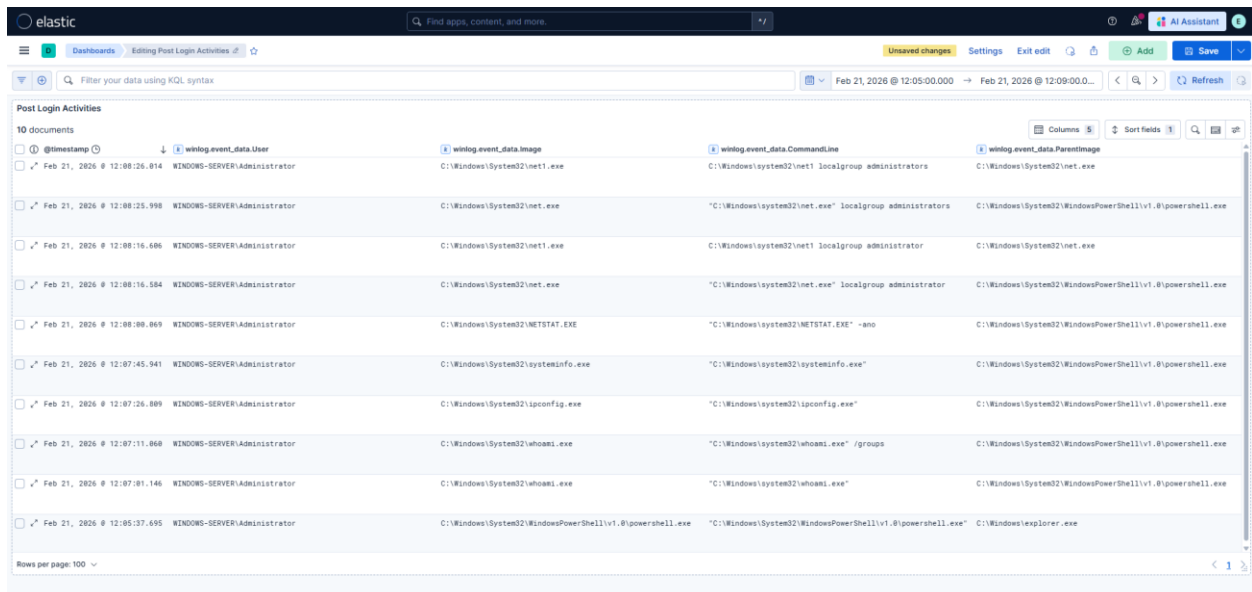
This reduced noise and allowed me to clearly identify the processes executed under the compromised user context

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)



The screenshot shows the Elastic Post Login Activities dashboard. The table displays 10 documents with the following columns: @timestamp, winlog_event_data.User, winlog_event_data.Image, winlog_event_data.CommandLine, and winlog_event_data.ParentImage. The data shows a sequence of events starting from a login at 12:05:00, followed by the execution of net.exe, net1.exe, powershell.exe, and various system discovery commands like whoami, ipconfig, systeminfo, netstat, and net localgroup administrators.

@timestamp	winlog_event_data.User	winlog_event_data.Image	winlog_event_data.CommandLine	winlog_event_data.ParentImage
Feb 21, 2026 @ 12:05:26.814	WINDOWS-SERVER\Administrator	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 localgroup administrators	C:\Windows\System32\net.exe
Feb 21, 2026 @ 12:08:25.998	WINDOWS-SERVER\Administrator	C:\Windows\System32\net.exe	"C:\Windows\system32\net.exe" localgroup administrators	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:08:16.686	WINDOWS-SERVER\Administrator	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 localgroup administrator	C:\Windows\System32\net.exe
Feb 21, 2026 @ 12:08:16.584	WINDOWS-SERVER\Administrator	C:\Windows\System32\net.exe	"C:\Windows\system32\net.exe" localgroup administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:08:09.869	WINDOWS-SERVER\Administrator	C:\Windows\System32\NETSTAT.EXE	"C:\Windows\system32\NETSTAT.EXE" -ano	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:07:45.941	WINDOWS-SERVER\Administrator	C:\Windows\System32\systeminfo.exe	"C:\Windows\system32\systeminfo.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:07:26.889	WINDOWS-SERVER\Administrator	C:\Windows\System32\ipconfig.exe	"C:\Windows\system32\ipconfig.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:07:11.868	WINDOWS-SERVER\Administrator	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe" /groups	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:07:01.146	WINDOWS-SERVER\Administrator	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:05:37.695	WINDOWS-SERVER\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\explorer.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