

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 services 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 parallel connections
[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.
[3389][rdp] host: 192.168.244.134 login: Administrator password: [REDACTED]
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 terminal session on a Linux host (Ubuntu 22.04) connected via FreeRDP to a Windows Server 2022 Standard Evaluation machine. The terminal window displays command-line history for whoami, ipconfig, systeminfo, netstat, and net localgroup. A separate PowerShell window titled 'Administrator: Windows PowerShell' shows the output of whoami, ipconfig, and systeminfo. The PowerShell window also displays the Windows Server configuration, including the OS name (Windows Server 2022 Standard Evaluation), OS version (10.0.20348 N/A Build 20348), manufacturer (Microsoft Corporation), configuration (standard), processor (Multiprocessor Free), and other details like the IP address (192.168.244.134), subnet mask (255.255.255.0), and default gateway (192.168.244.2). The bottom right of the screen shows the Windows Server license information: Windows Server Standard Evaluation, Windows License valid for 72 days, Build 20348.4e, release.210907-1500.

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 @ 12:01:32.083	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 logon)
- LogonType: 3 (Network Logon)
- Grouped by source IP, username and count of records

The screenshot shows the Kibana Data View interface. The search bar at the top contains the query: `agent.name: "Windows-Server" and event.code: 4625 and winlog.event_data.LogonType: "3"`. The main area displays a table with three columns: Source IP, Username, and Count of records. One row is shown: 192.168.244.128, Administrator, 24. On the left, the sidebar shows selected fields: Records, source.ip, user.name, and available fields like @timestamp, agent.id, etc. On the right, the visualization configuration panel is visible, showing settings for Rows (Source IP, Username) and Metrics (Count of records).

Source IP	Username	Count of records
192.168.244.128	Administrator	24

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.

This screenshot shows a second Kibana Data View visualization for successful logons. The search bar contains the same query: `agent.name: "Windows-Server" and event.code: 4624 and winlog.event_data.LogonType: 10`. The table results are identical to the first one, showing a single row for source IP 192.168.244.128 and username Administrator with a count of 1. The sidebar and visualization configuration panel are also similar to the first one.

Source IP	Username	Count of records
192.168.244.128	Administrator	1

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

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

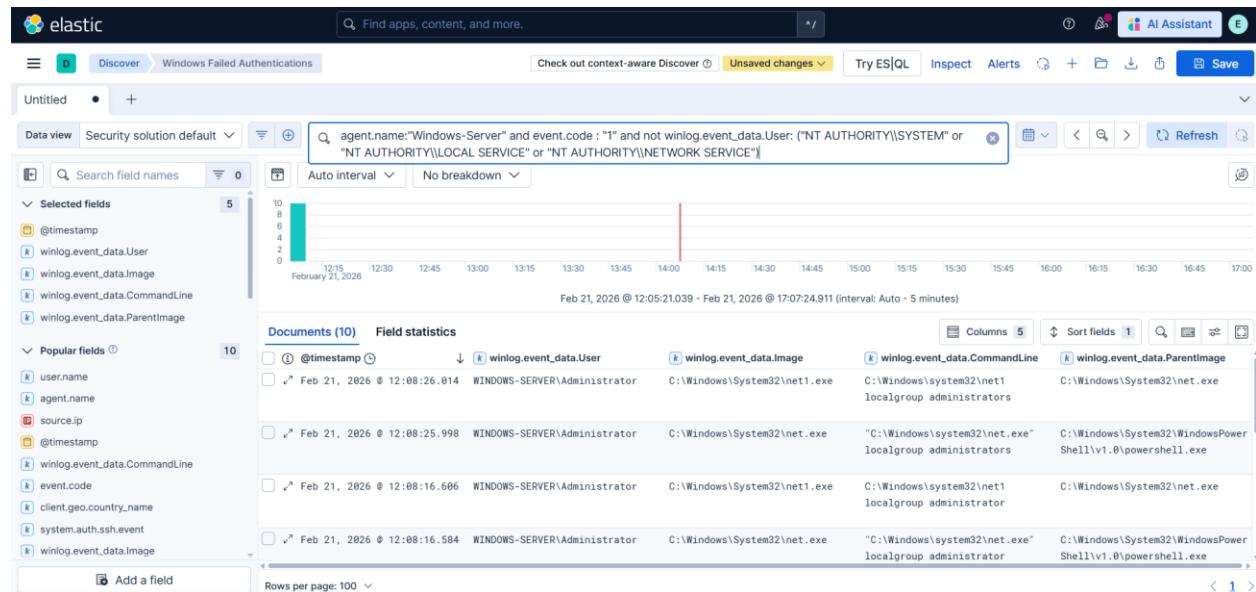
KQL:

```
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)

timestamp	user	process	command line	parent
Feb 21, 2026 @ 12:05:37.695	WINDOWS-SERVER\Administrator	C:\Windows\System32\cmd.exe	"C:\Windows\System32\cmd.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:05:41.146	WINDOWS-SERVER\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:05:41.146	WINDOWS-SERVER\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:05:41.146	WINDOWS-SERVER\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:05:41.146	WINDOWS-SERVER\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:05:41.146	WINDOWS-SERVER\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:05:41.146	WINDOWS-SERVER\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:05:41.146	WINDOWS-SERVER\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:05:41.146	WINDOWS-SERVER\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Feb 21, 2026 @ 12:05:41.146	WINDOWS-SERVER\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.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