# ACTIVE DIRCTORY

# Team Members

- Reham Rafie El-said Seria
- AbdelRahman Mohamed Mosad
- Hager Saad Abdelkhabeer
- Ahmed Samir Mohamed

## Mamdouh Al-Tahiry

linkedin.com/in/mamdouh-el-tahiry

# ABOUT PROJECT

This Active Directory project simulates a small network environment for incident response and security monitoring. It includes an Active Directory server and a Windows 10 client, both configured with Splunk Universal Forwarder and Sysmon for detailed log collection. Logs are centralized on a Splunk Server for analysis.

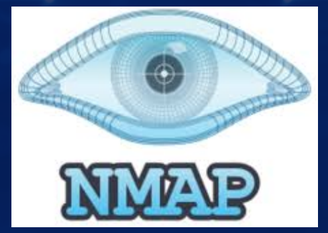
A Kali Linux machine serves as the attacker to simulate security threats. The setup focuses on detecting and responding to security incidents using Splunk, while monitoring system and network activity.

# Environment Setup

**Used Software:**






Environment Setup

**Ubuntu Server:**
The Ubuntu Server acts as the central logging hub, where Splunk is installed to aggregate logs from the connected systems.

**PC (Windows 10):**
The Windows 10 machine serves as the primary target for the brute force attack simulation.

**Windows Server:**
used to monitor login attempts and collect logs related to administrative access and system events.

**PC (Kali Linux):**
This machine is used to simulate brute force attacks on the Windows 10 target and the Ubuntu server.

Environment Setup

## Data Collection:

- Authentication Logs:
  - From both the Windows 10 target machine and the Windows Server logs
- System Security Events:
  - This includes logs related to unauthorized access attempts, login failures, and abnormal login behaviors.

## Data Flow:

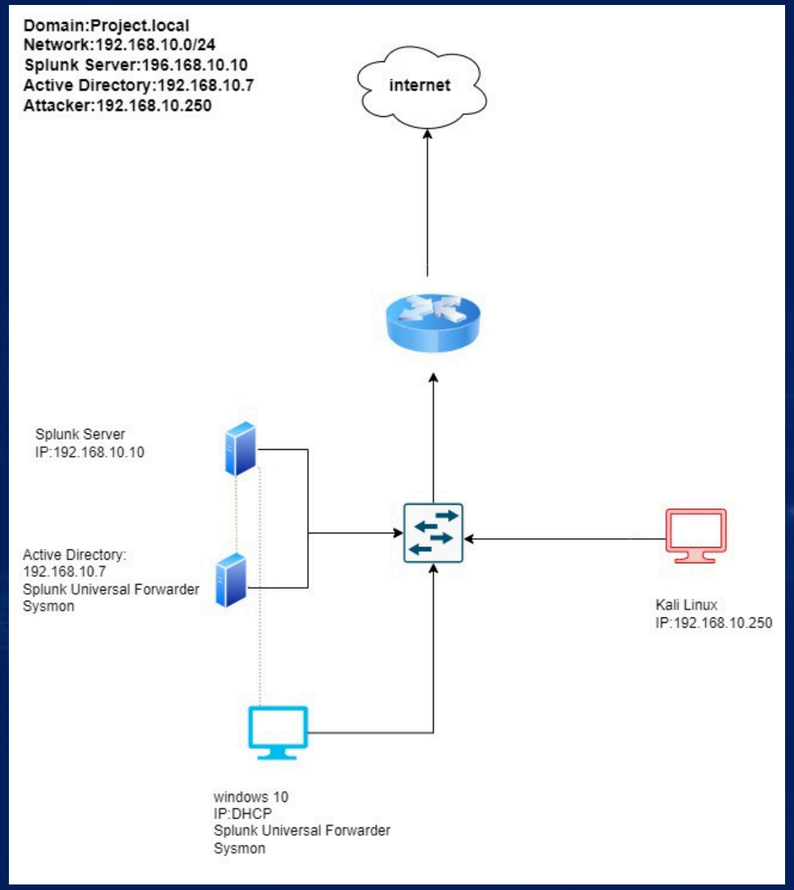
- Logs from the Windows 10 target and the Windows Server are continuously forwarded to the Ubuntu server where Splunk is installed. The data is processed in real-time
- This multi-system setup creates an effective environment for detecting and analyzing **brute force attack scenarios**, providing valuable insights into the attack methods and security responses.

# Installation Steps and Guide

## Network Configuration:

The network used for this project is 192.168.10.0/24, with the following machines and their IP addresses:

- Splunk Server (Ubuntu): 192.168.10.10
- Active Directory (Windows Server): 192.168.10.7
- Target PC (Windows 10): 192.168.10.20
- Attacker Machine (Kali Linux): 192.168.10.250



## Download Splunk:

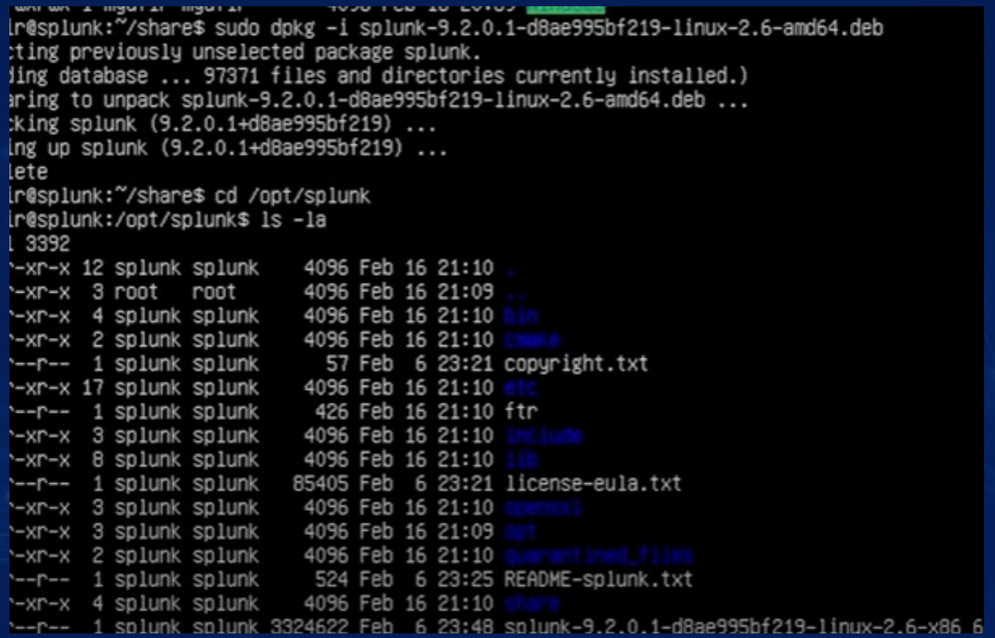
Splunk was downloaded using wget directly to the Ubuntu machine.

## Install Splunk:

The downloaded Splunk package was installed using the dpkg command.

## Start Splunk:

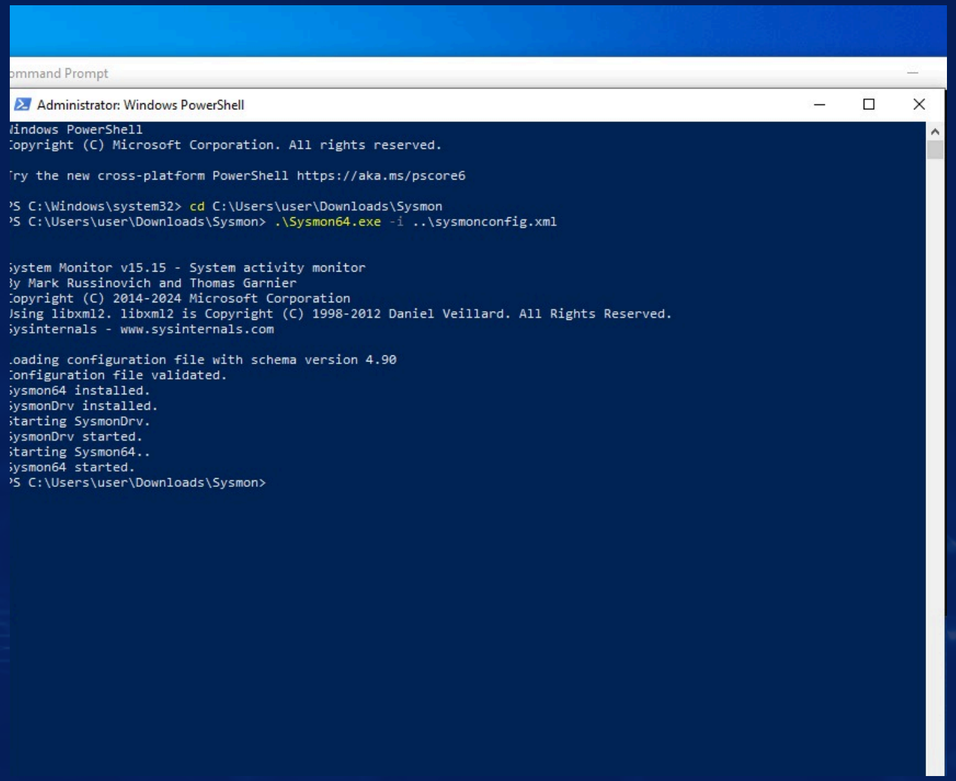
Splunk was started with the sudo /opt/splunk/bin/splunk start command, and the license agreement was accepted.

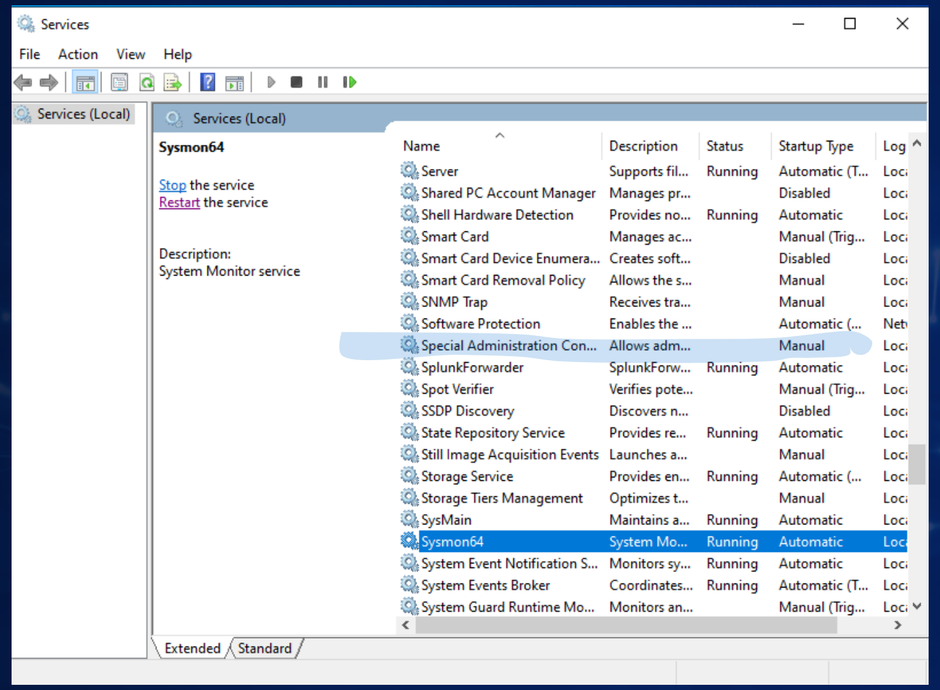


# Splunk Installation on Windows OS

## Sysmon and Splunk Integration Installation on Both Windows Server and target:

The integration of Sysmon and Splunk provides comprehensive monitoring and detection of security events within the network. This setup helps in identifying potential threats and assists in incident response.

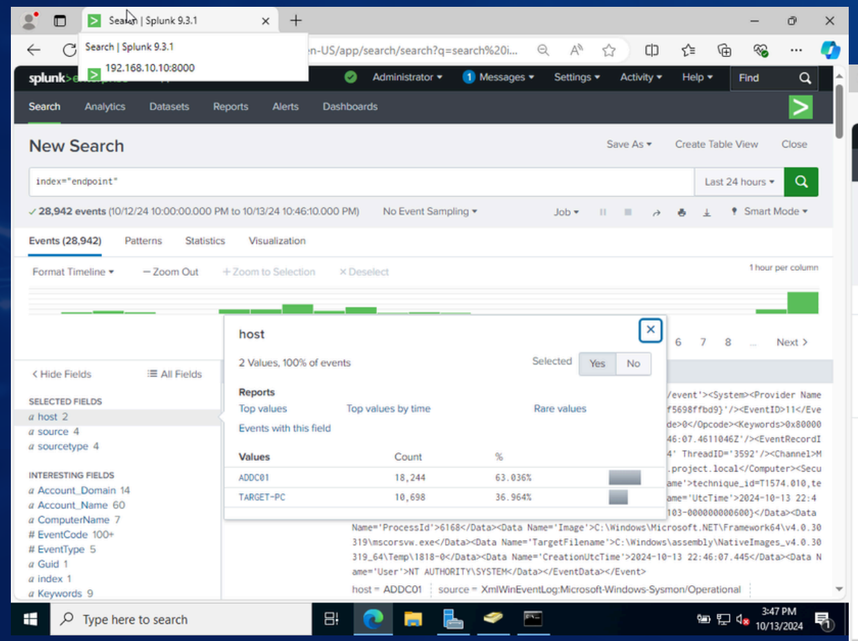


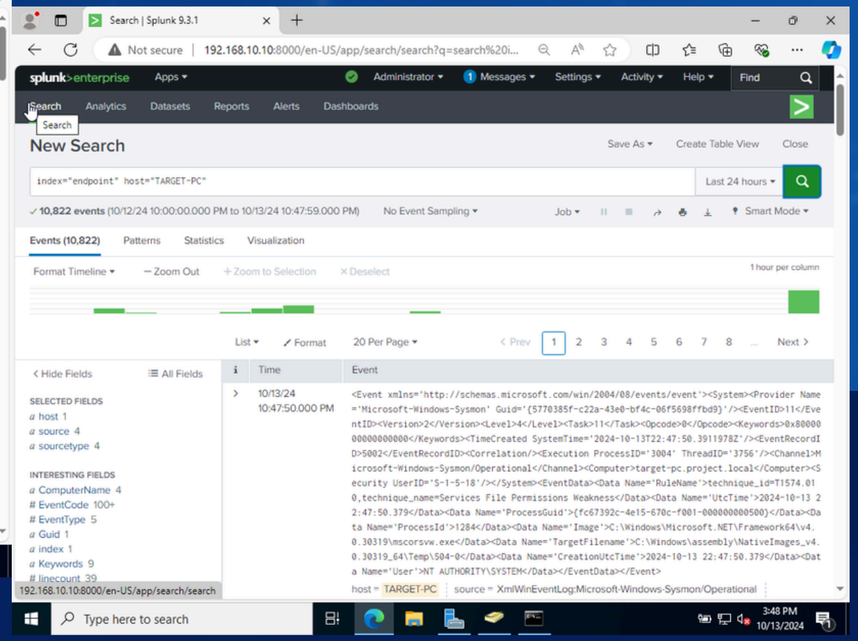


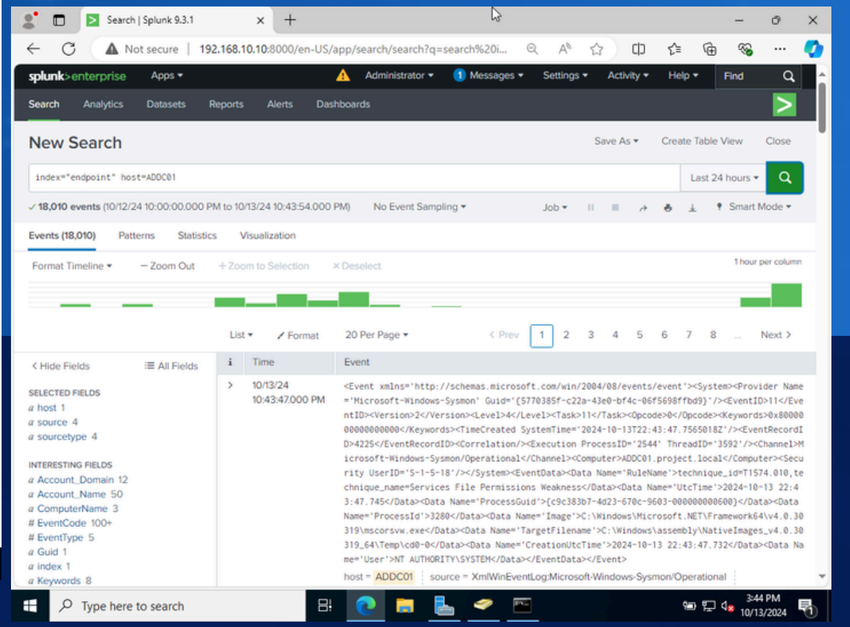

# INSTALL SPLUNK &SYSMON

# SPLUNK

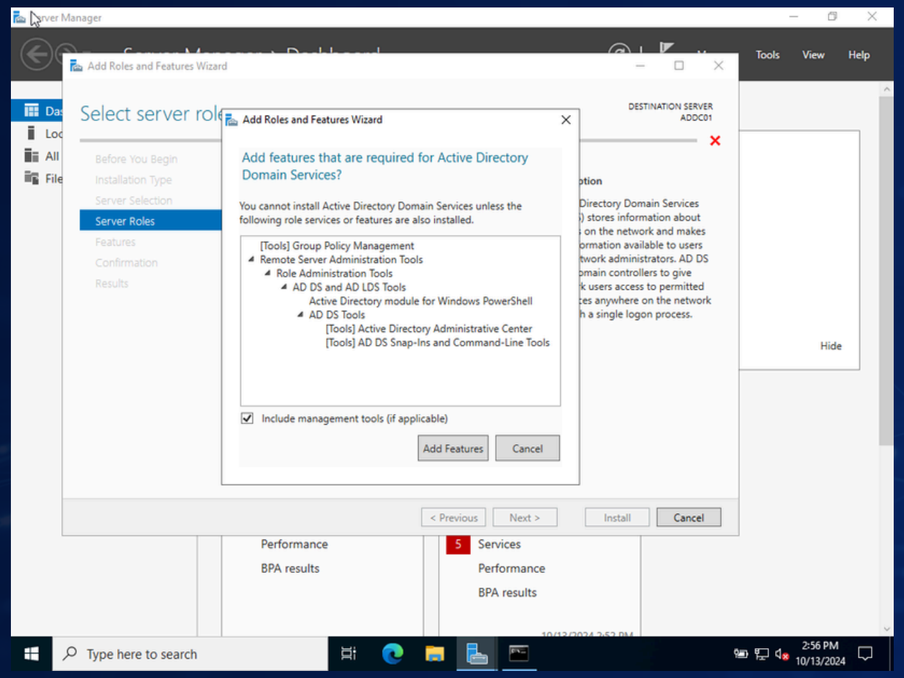
Access Splunk Web Interface:
The Splunk web interface was accessed from http://192.168.10.10:8000 using the admin credentials.

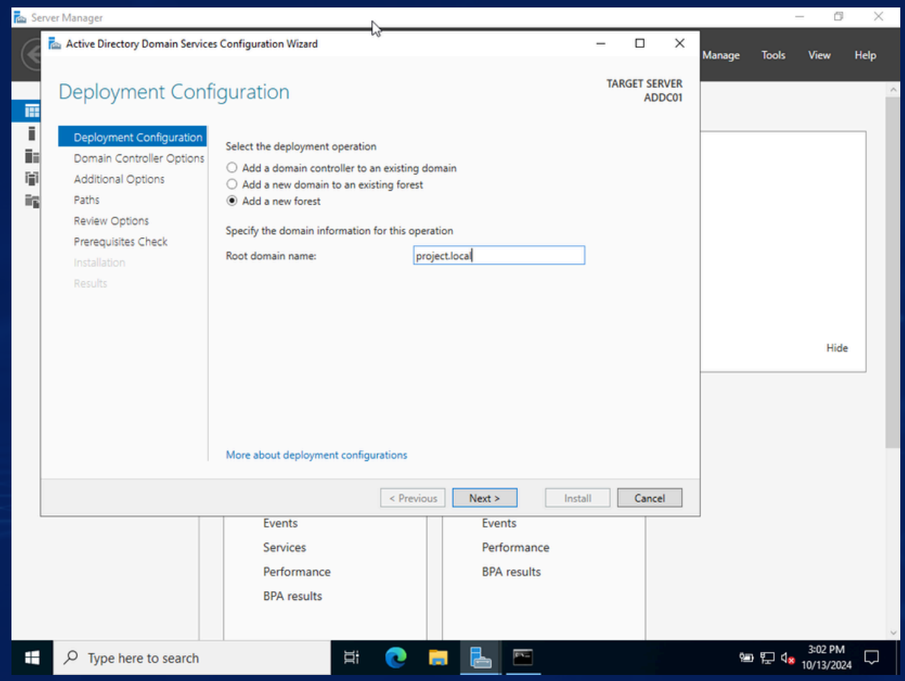


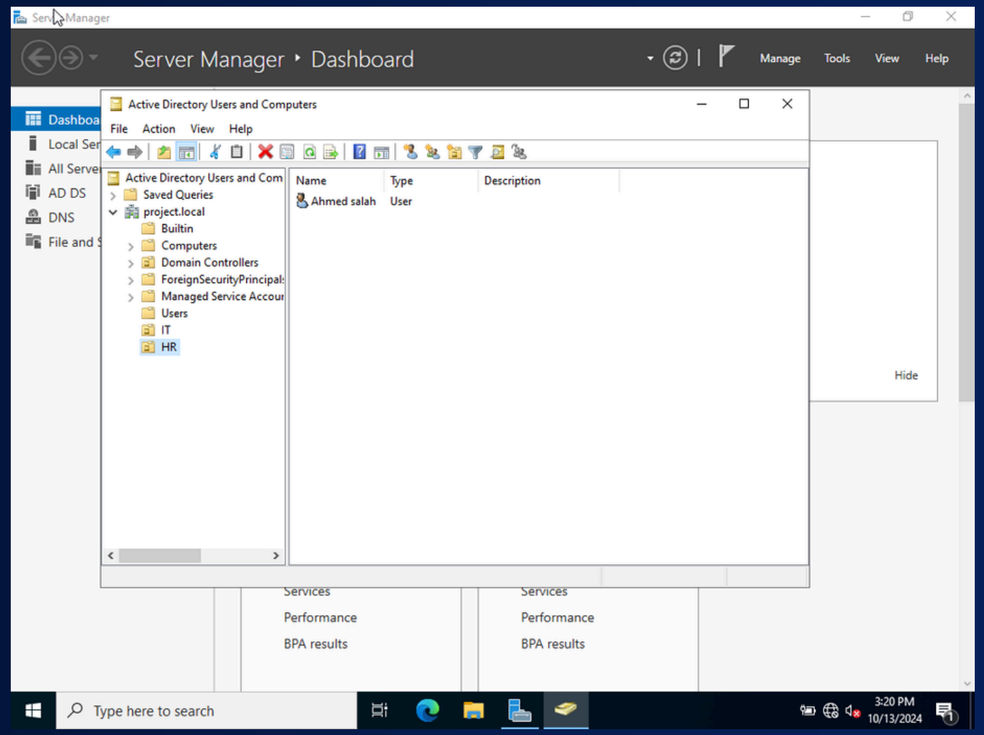



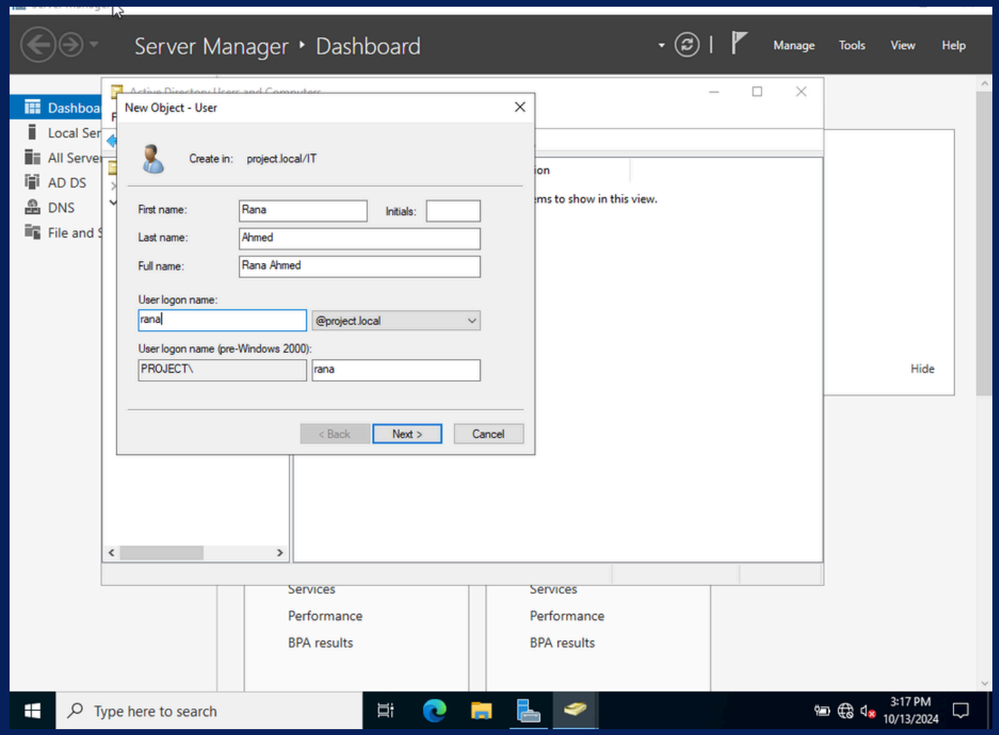



# DOMAIN CONTROLLER

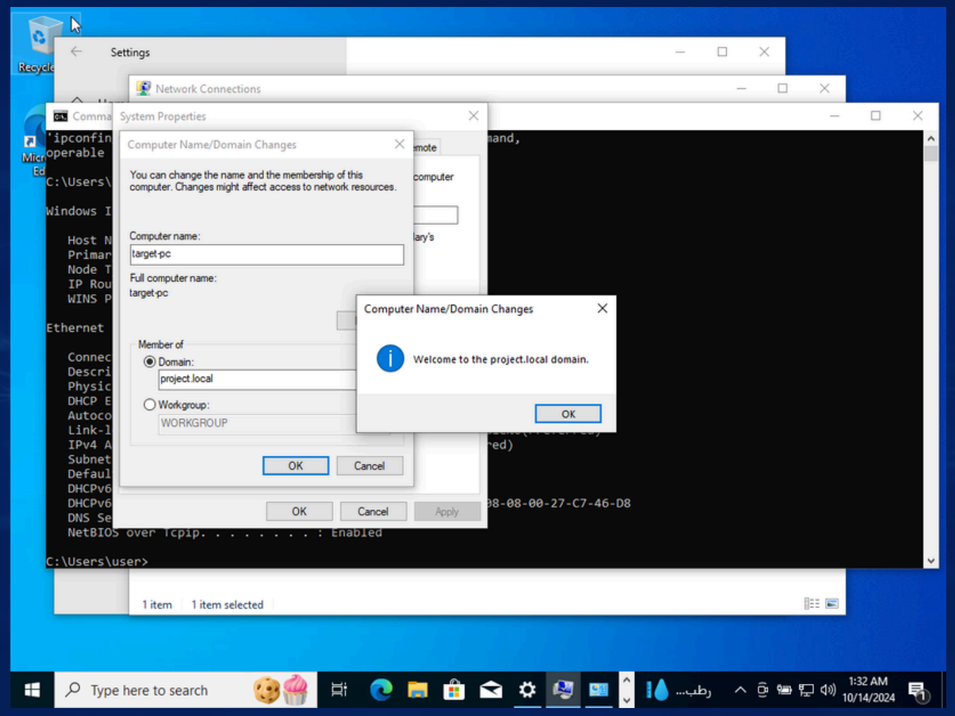

Server Manager
Add Roles and Features Wizard
Select server role
DESTINATION SERVER
ADDC01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Performance
BPA results
Services
Performance
BPA results
Type here to search
2:56 PM
10/13/2024

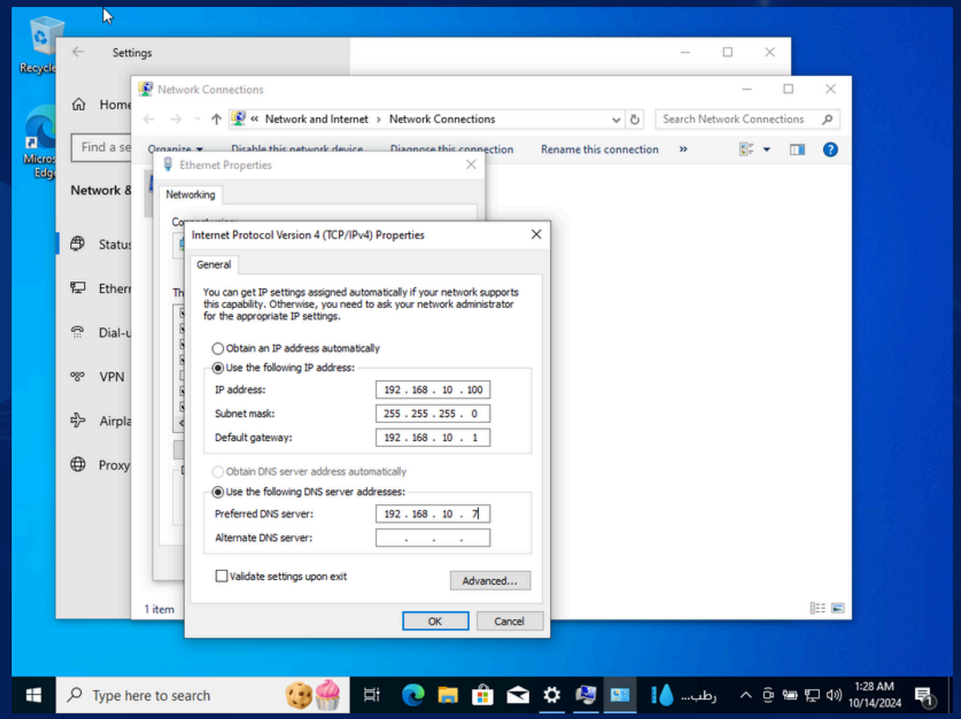

Server Manager
Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
ADDC01
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
project.local
More about deployment configurations
< Previous
Next >
Install
Cancel
Manage
Tools
View
Help
Hide
Events
Services
Performance
BPA results
Events
Performance
BPA results
Type here to search
3:02 PM
10/13/2024


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
project.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
IT
HR
Name
Type
Description
Ahmed salah
User
Hide
Services
Performance
BPA results
Type here to search
3:20 PM
10/13/2024

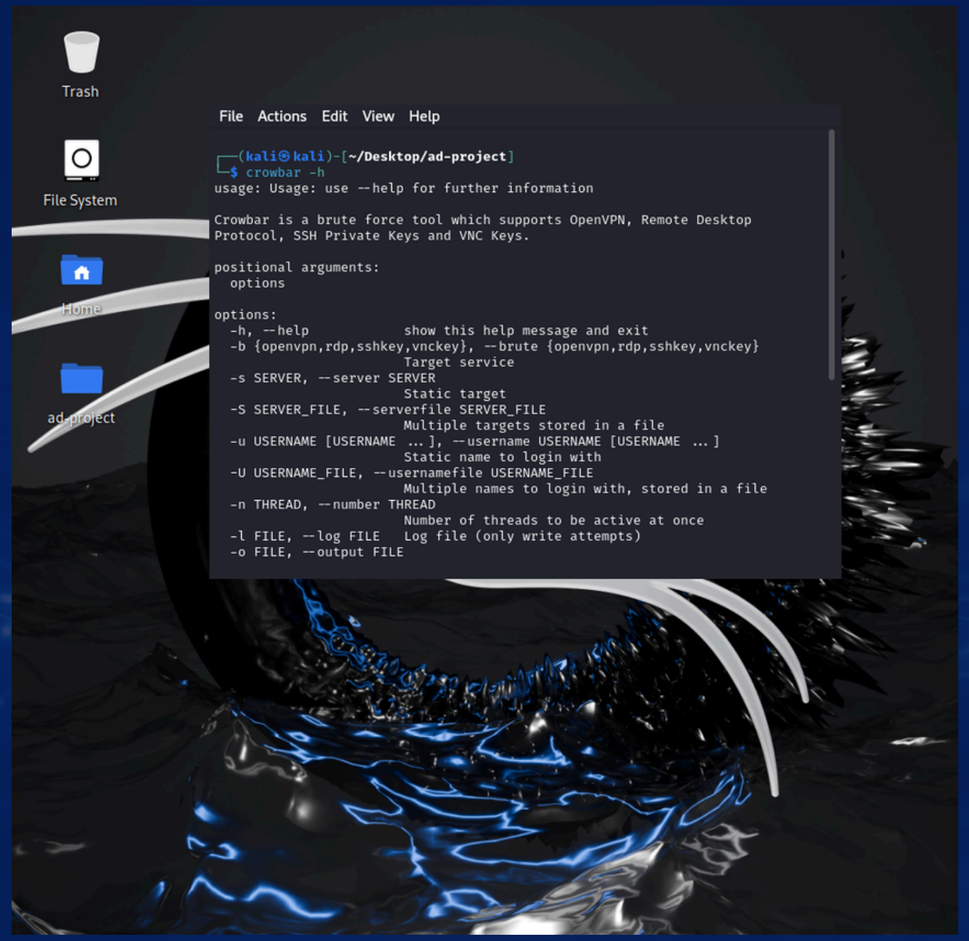

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
New Object - User
Create in: project.local/IT
First name:
Rana
Initials:
Last name:
Ahmed
Full name:
Rana Ahmed
User logon name:
rana
@project.local
User logon name (pre-Windows 2000):
PROJECT\
rana
< Back
Next >
Cancel
Hide
Services
Performance
BPA results
Type here to search
3:17 PM
10/13/2024

# ADD TARGET TO DOMAIN



# KALI LINUX



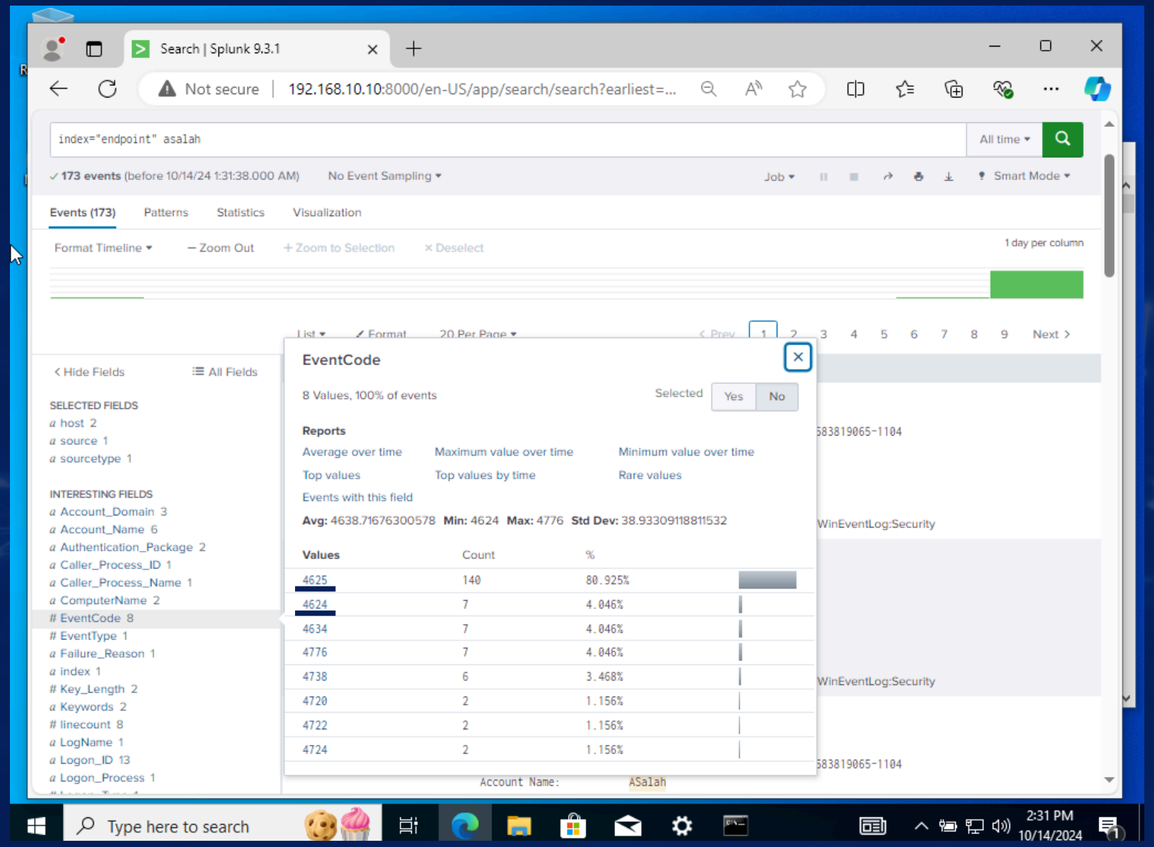

**Crowbar** is a brute-forcing tool used to crack SSH, VNC, RDP, and OpenVPN credentials by using SSH keys or password lists. It automates login attempts to test for weak or default passwords in network services, making it a popular tool for penetration testing and security assessments.

**RockYou is a famous password dictionary file included in Kali Linux, containing millions of common passwords. It's widely used in brute-force attacks to test password strength during penetration testing and security audits, helping identify weak or easily guessable passwords.**

# OPEN RDP IN TARGET


- crowbar: Tool for brute force attacks.
- -b rdp: Targets Remote Desktop Protocol (RDP).
- -u asalah: Username for the attack.
- -C password.txt: File containing passwords to test
- -s 192.168.10.100/32: Target IP address.

# SEARCH IN SPLUNK



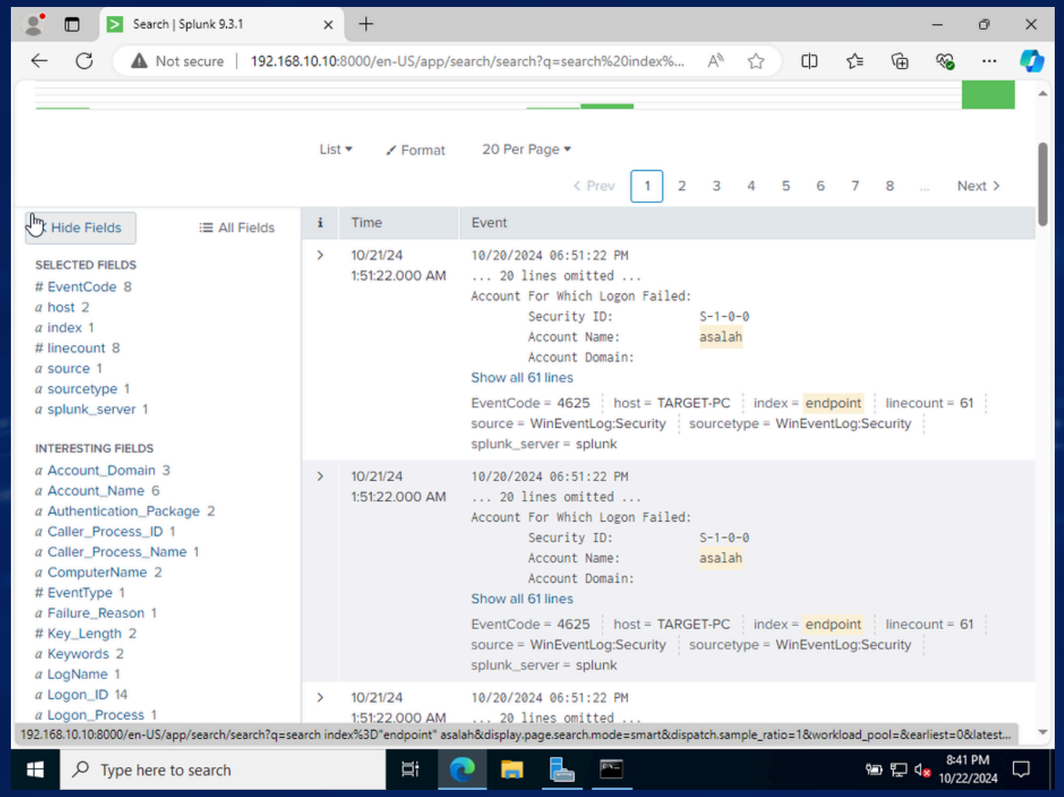

**Windows Security Log Event ID 4625**

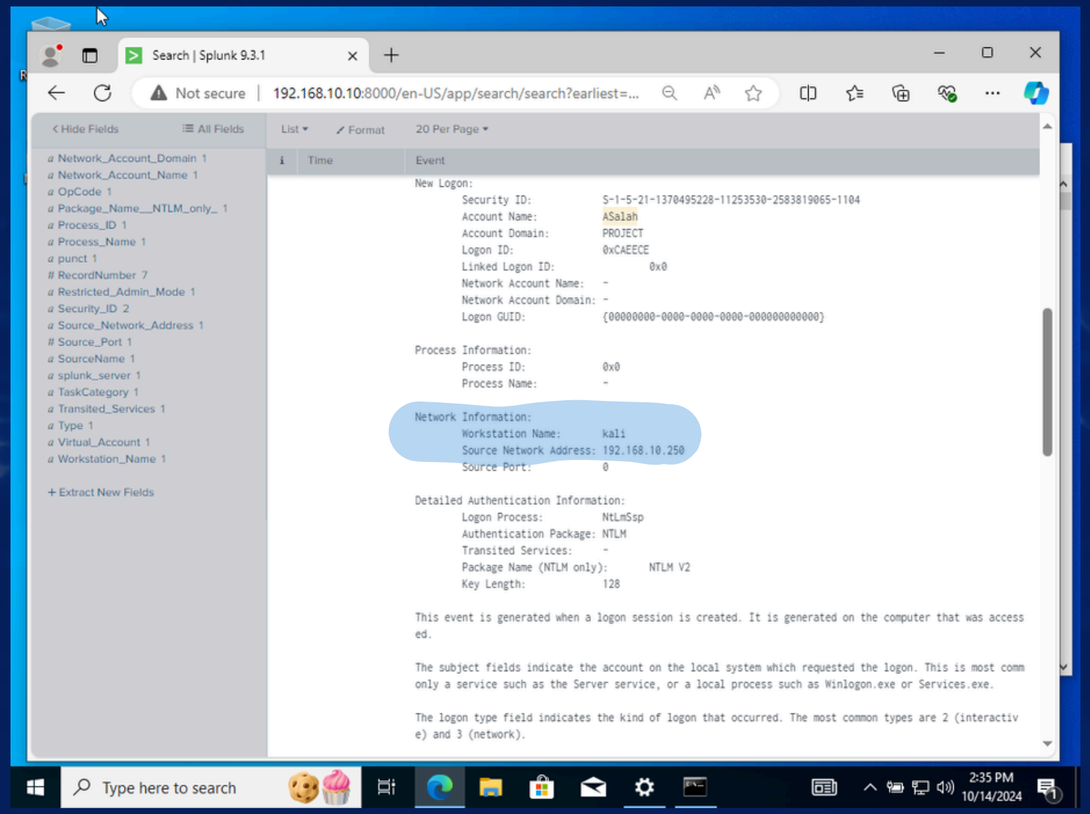
4625: An account failed to log on

**Windows Security Log Event ID 4624**

4624: An account was successfully logged on

# Logs in Splink



# Incident Response and Development plan

# Incident Response and Development plan

## Responding to Brute Force Attempts:

The initial steps when detecting a Brute Force attempt include reviewing the logs to gather details about the attack, tracing the attack's source using appropriate tools, and isolating the affected systems to ensure no further damage or data leakage occurs.

## Mitigation Actions:

Afterward, the aim is to minimize the chances of successful attacks by implementing advanced security policies, such as locking accounts after failed login attempts, enforcing strong password requirements with two-factor authentication, strengthening network defenses, and conducting regular reviews of security protocols
.

## Post-Incident Review and Documentation:

Enhancing organizational security involves conducting in-depth attack analysis to identify vulnerabilities and anticipate future threats, maintaining comprehensive documentation of all incidents to improve response strategies, and providing continuous training for employees to increase awareness of security risks and foster a culture of responsibility towards security.

# THANK YOU FOR YOUR ATTENTION