



ACTIVE DIRECTORY

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/](https://www.linkedin.com/in/mamdouh-el-tahiry/)



ABOUT PROJECT

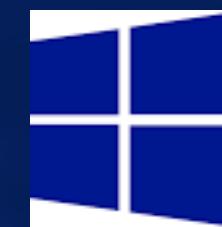
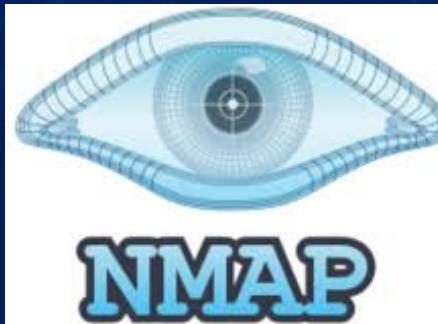
This Active Directory project simulates a small network environment for incident response and security monitoring. It includes an Active Directory server and a Windows 10 client, both configured with Splunk Universal Forwarder and Sysmon for detailed log collection. Logs are centralized on a Splunk Server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

Environment Setup

Used Software:



Windows Server

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.

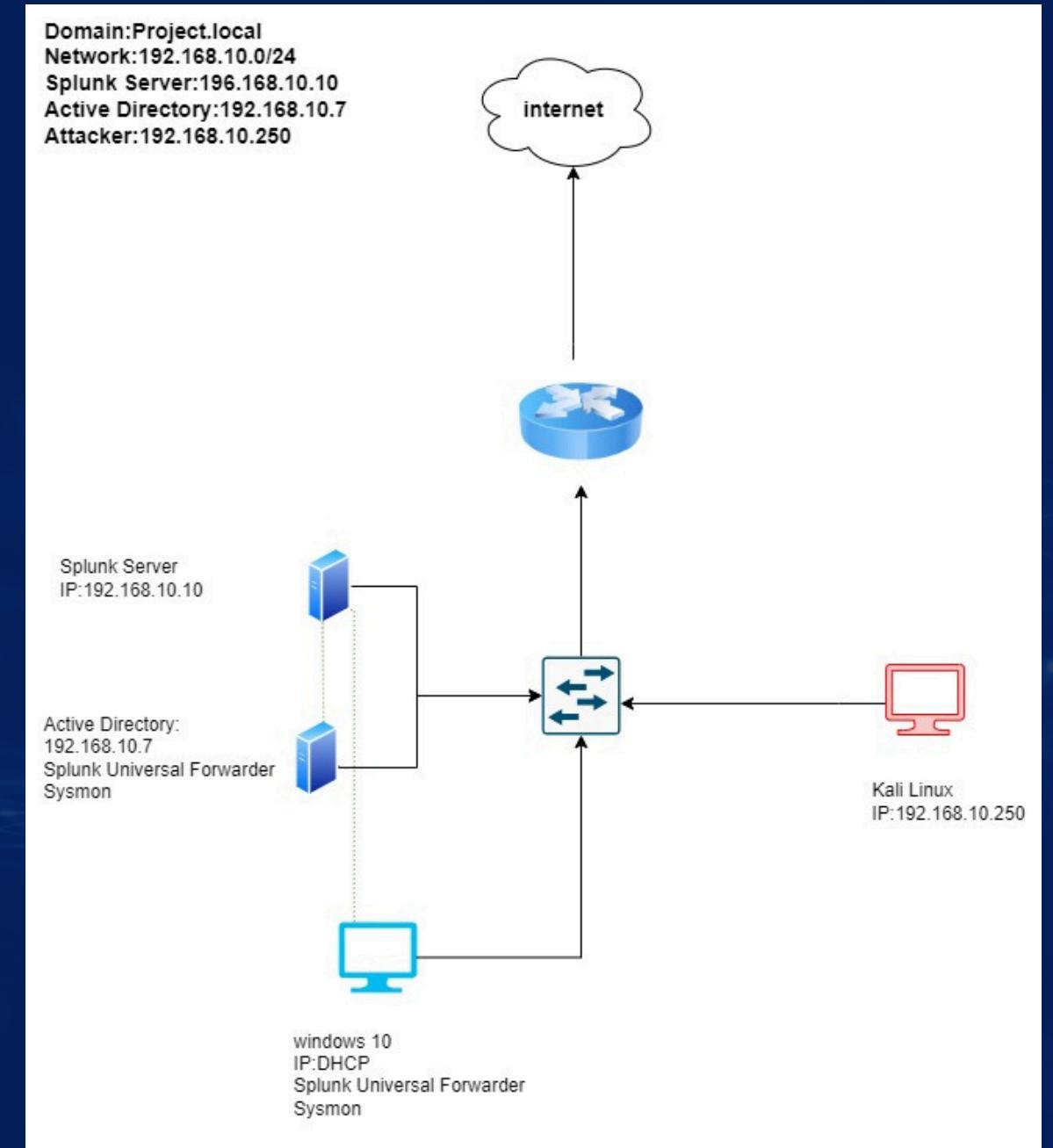
Installation Steps and Guide

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**



Installation Steps and Guide : Installation and Configuration of Ubuntu Server with Splunk

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:

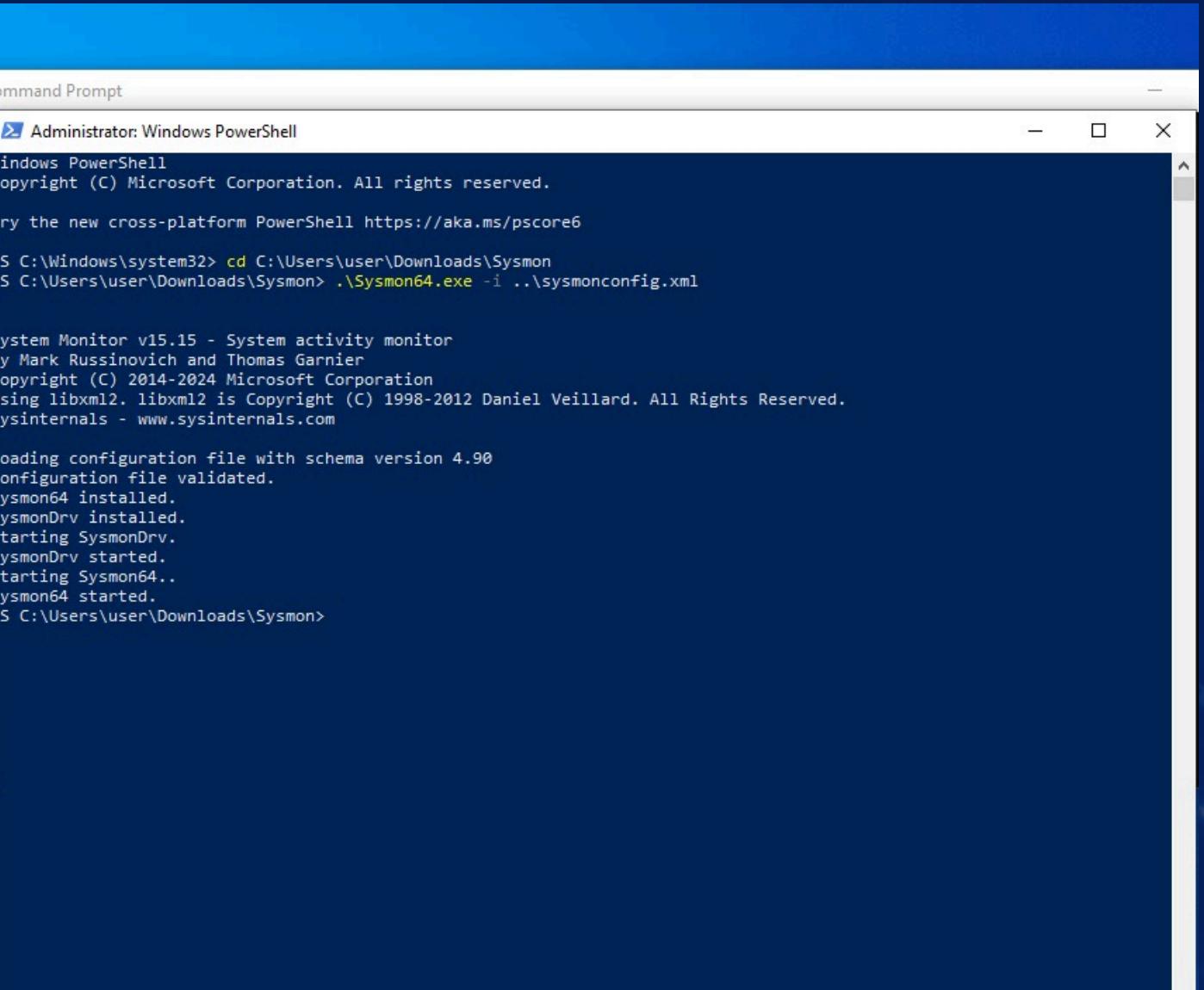
Splunk was started with the sudo /opt/splunk/bin/splunk start command, and the license agreement was accepted.

```
ir@splunk:~/share$ sudo dpkg -i splunk-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 97371 files and directories currently installed.)
Preparing to unpack splunk-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb ...
Unpacking splunk (9.2.0.1+d8ae995bf219) ...
Configuring splunk (9.2.0.1+d8ae995bf219) ...
ir@splunk:~/share$ cd /opt/splunk
ir@splunk:/opt/splunk$ ls -la
total 3392
drwxr-x 12 splunk splunk 4096 Feb 16 21:10 .
drwxr-x  3 root   root  4096 Feb 16 21:09 ..
drwxr-x  4 splunk splunk 4096 Feb 16 21:10 bin
drwxr-x  2 splunk splunk 4096 Feb 16 21:10 cmake
drwxr--  1 splunk splunk 57 Feb  6 23:21 copyright.txt
drwxr-x 17 splunk splunk 4096 Feb 16 21:10 etc
drwxr--  1 splunk splunk 426 Feb 16 21:10 ftr
drwxr-x  3 splunk splunk 4096 Feb 16 21:10 include
drwxr-x  8 splunk splunk 4096 Feb 16 21:10 lib
drwxr--  1 splunk splunk 85405 Feb  6 23:21 license-eula.txt
drwxr-x  3 splunk splunk 4096 Feb 16 21:10 log
drwxr-x  3 splunk splunk 4096 Feb 16 21:09 opt
drwxr-x  2 splunk splunk 4096 Feb 16 21:10 generated_files
drwxr--  1 splunk splunk 524 Feb  6 23:25 README-splunk.txt
drwxr-x  4 splunk splunk 4096 Feb 16 21:10 share
drwxr--  1 splunk splunk 3324622 Feb  6 23:48 splunk-9.2.0.1-d8ae995bf219-linux-2.6-x86_64
```

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.



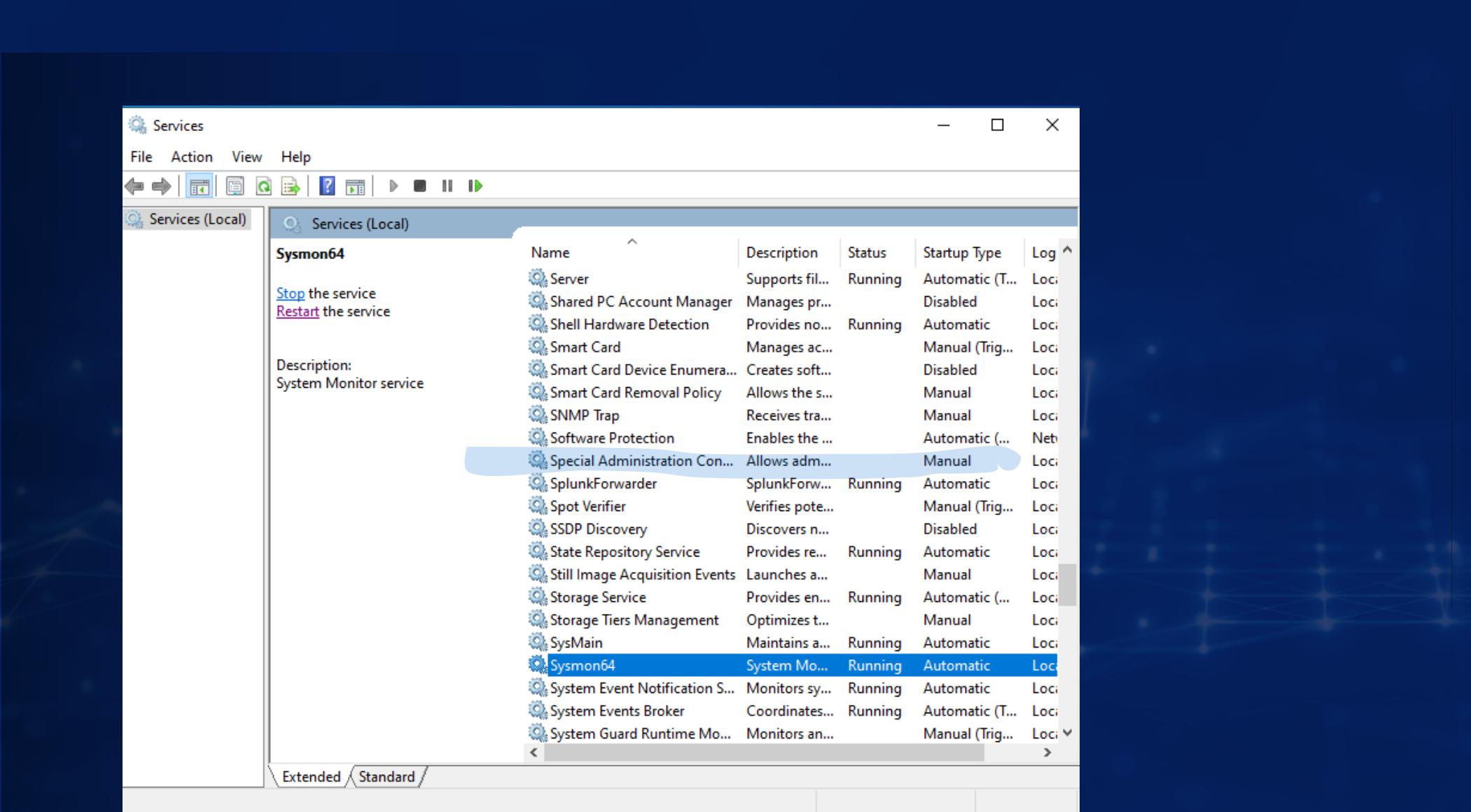
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

>S C:\Windows\system32> cd C:\Users\user\Downloads\Sysmon
>S C:\Users\user\Downloads\Sysmon> .\Sysmon64.exe -i ..\sysmonconfig.xml

System Monitor v15.15 - System activity monitor
by Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
>S C:\Users\user\Downloads\Sysmon>
```



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.

The image displays three side-by-side screenshots of the Splunk 9.3.1 web interface, each showing a search results page for endpoint data. The interface includes a top navigation bar with links for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. Below this is a search bar and a 'New Search' section. The main area shows event counts, sampling options, and a timeline visualization. On the left, a sidebar provides details about selected fields like 'host' and 'source'. The bottom of each screenshot shows a Windows taskbar with the Splunk icon.

Screenshot 1 (Left): Shows 28,942 events from 10/12/24 to 10/13/24. The 'host' field is selected, showing values for ADDC01 and TARGET-PC. The event XML snippet shows a Microsoft-Sysmon event with a Process ID of 6168 and a Creation UtcTime of 2024-10-13 22:46:07.

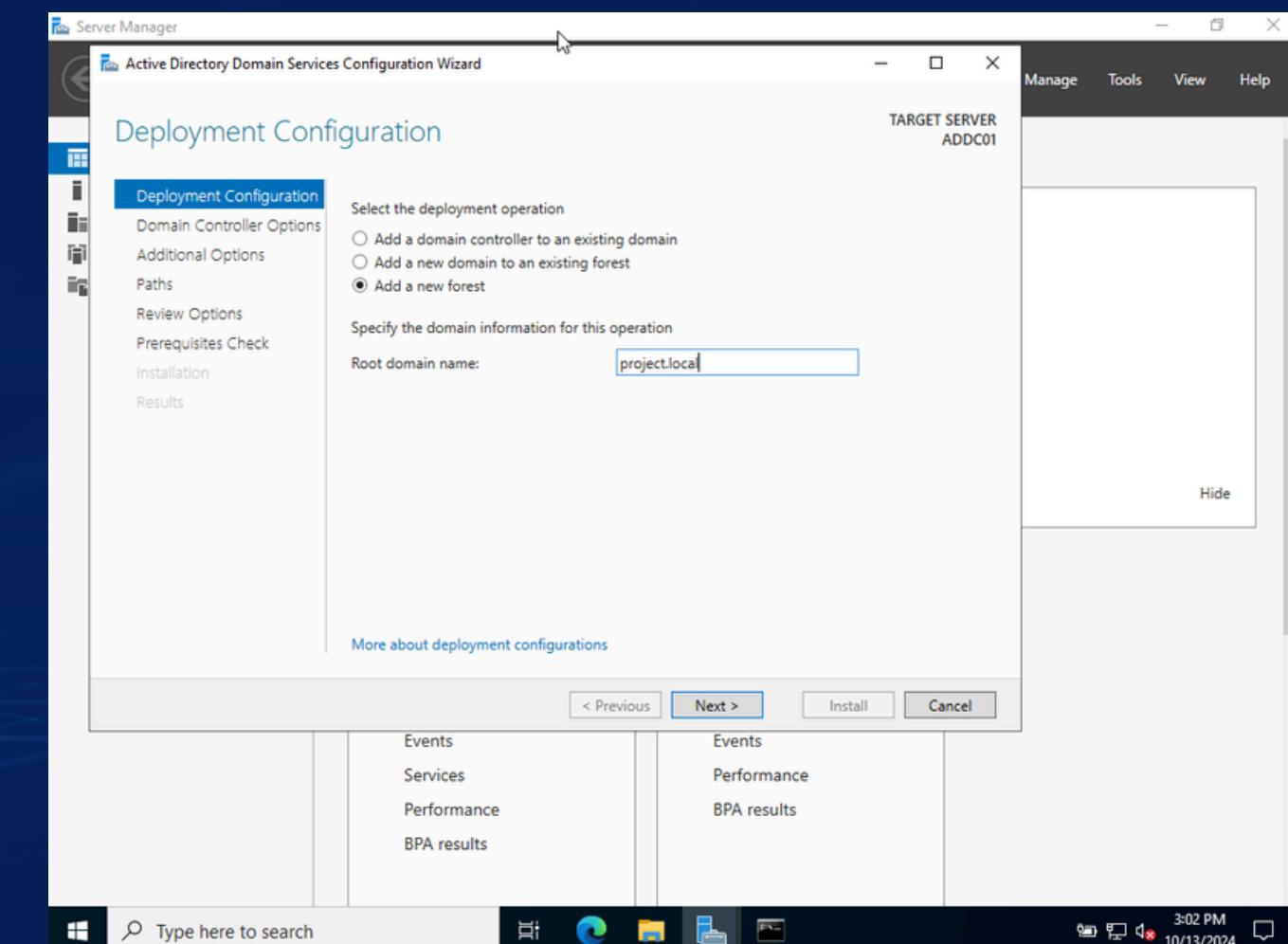
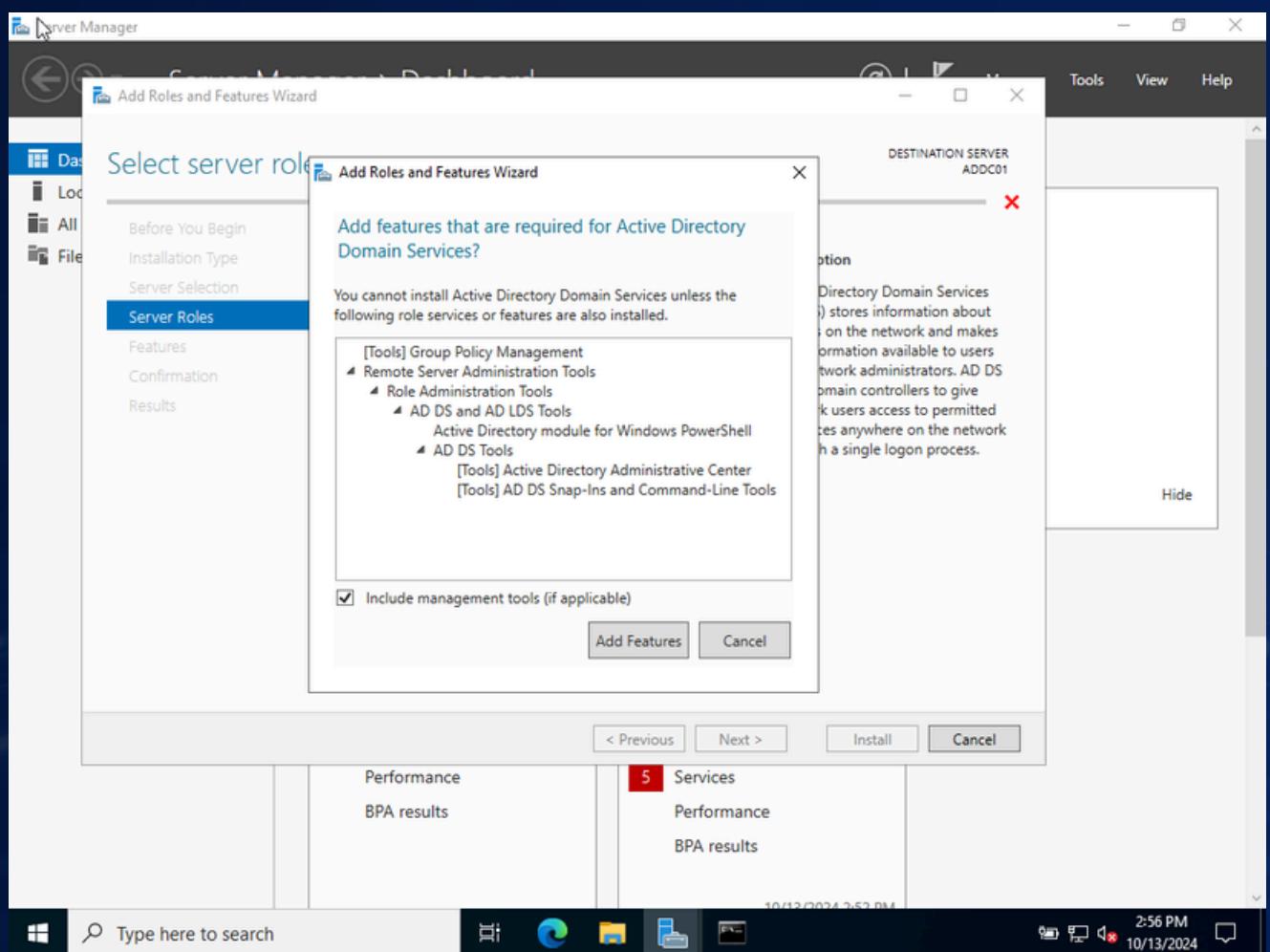
Screenshot 2 (Middle): Shows 10,822 events from 10/12/24 to 10/13/24. The 'host' field is selected, showing values for ADDC01 and TARGET-PC. The event XML snippet shows a Microsoft-Sysmon event with a Process ID of 3004 and a Thread ID of 3592.

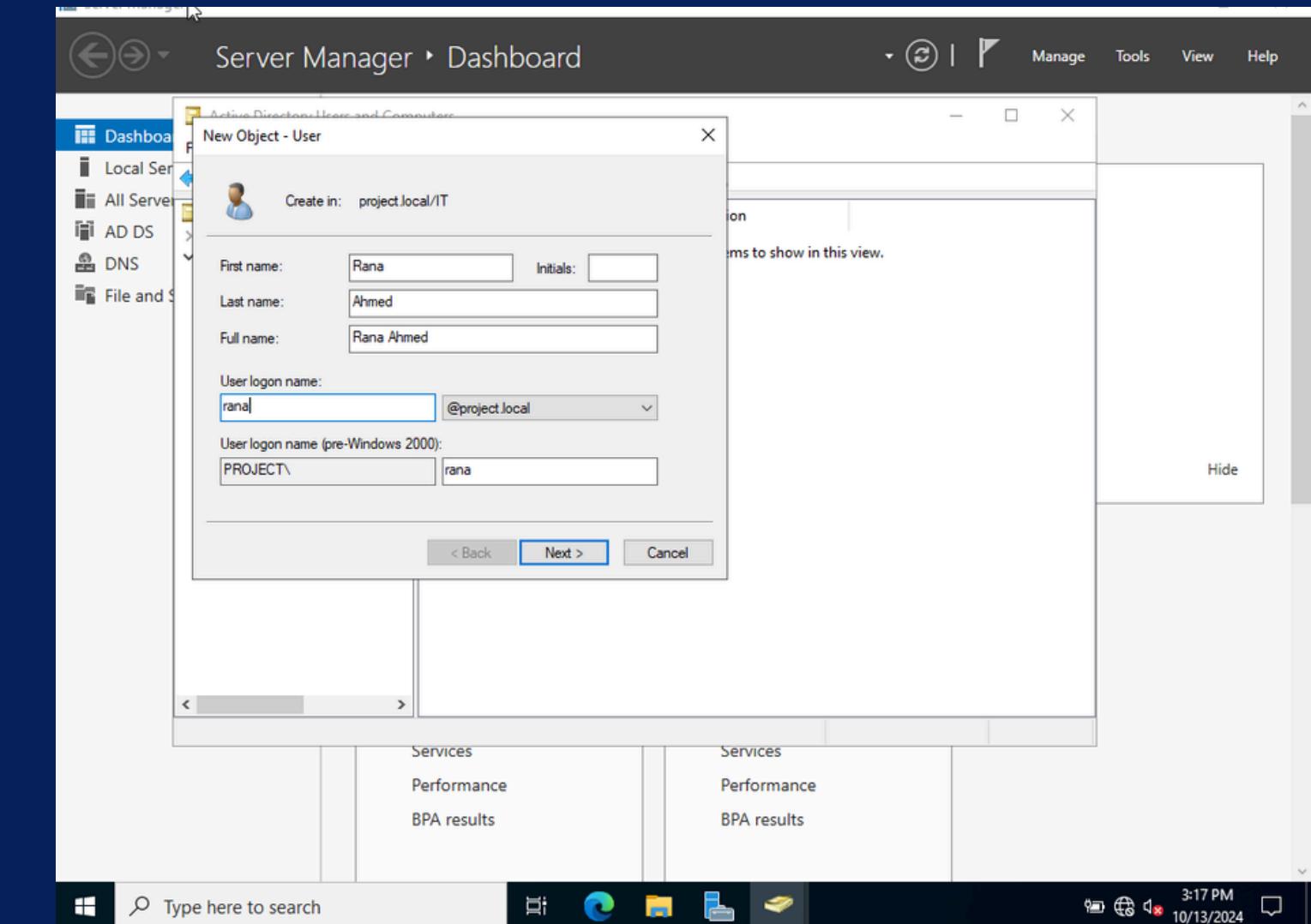
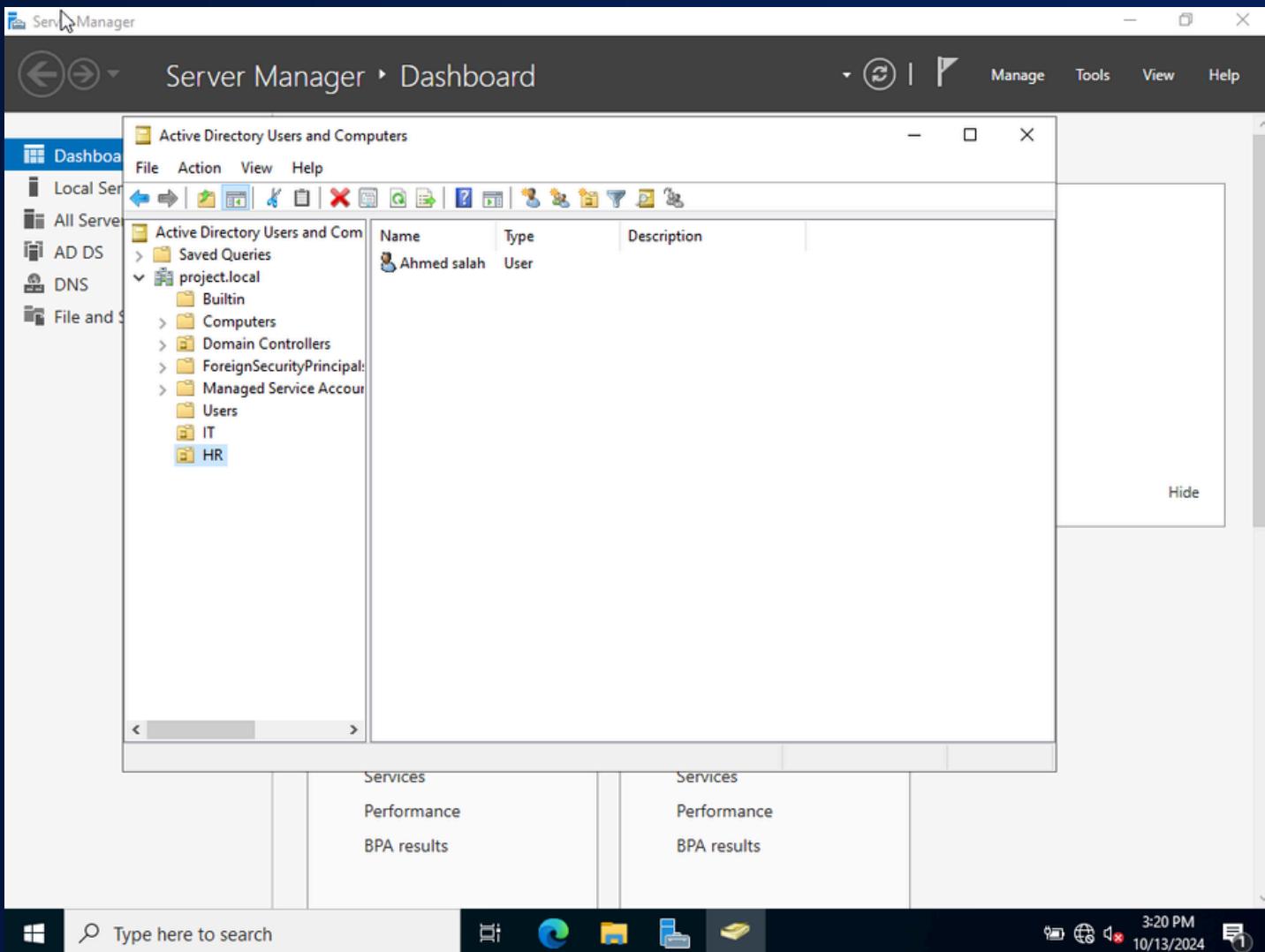
Screenshot 3 (Right): Shows 18,010 events from 10/12/24 to 10/13/24. The 'host' field is selected, showing values for ADDC01 and TARGET-PC. The event XML snippet shows a Microsoft-Sysmon event with a Process ID of 2544 and a Thread ID of 3592.



DOMAIN CONTROLLER

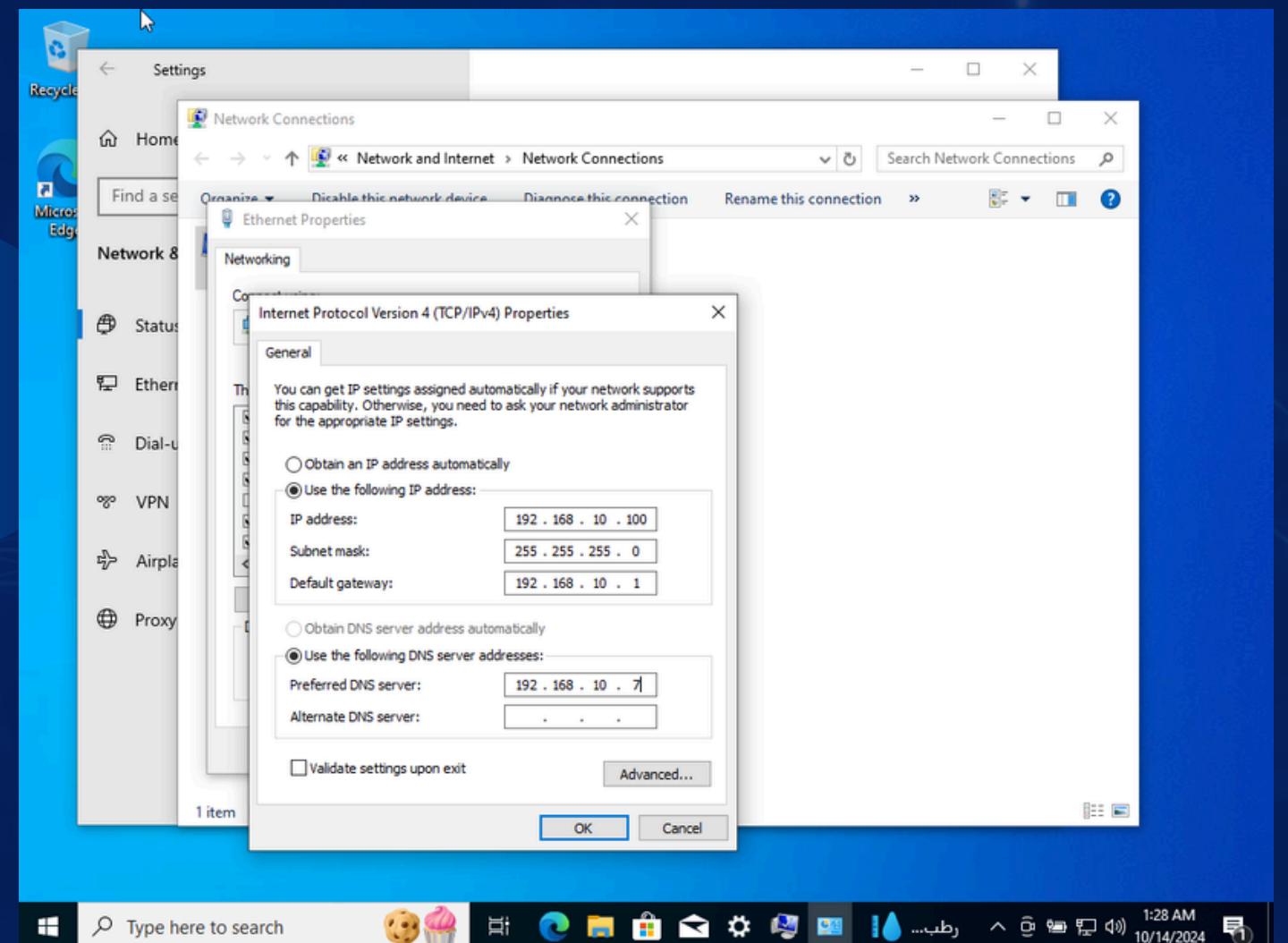
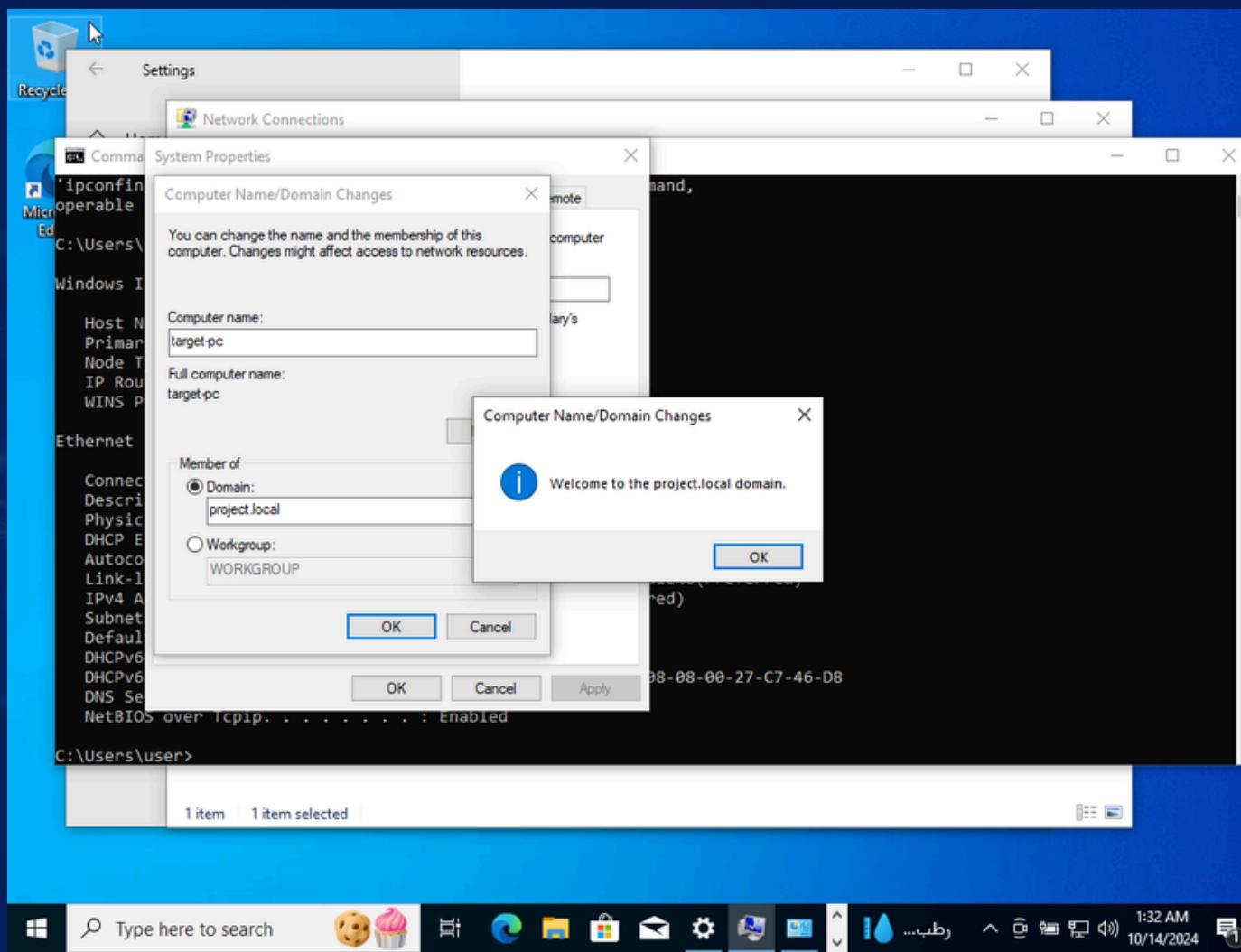








ADD TARGET TO DOMAIN





KALI LINUX



```
(kali㉿kali)-[~/Desktop/ad-project]
$ crowbar -h
usage: Usage: use --help for further information

Crowbar is a brute force tool which supports OpenVPN, Remote Desktop Protocol, SSH Private Keys and VNC Keys.

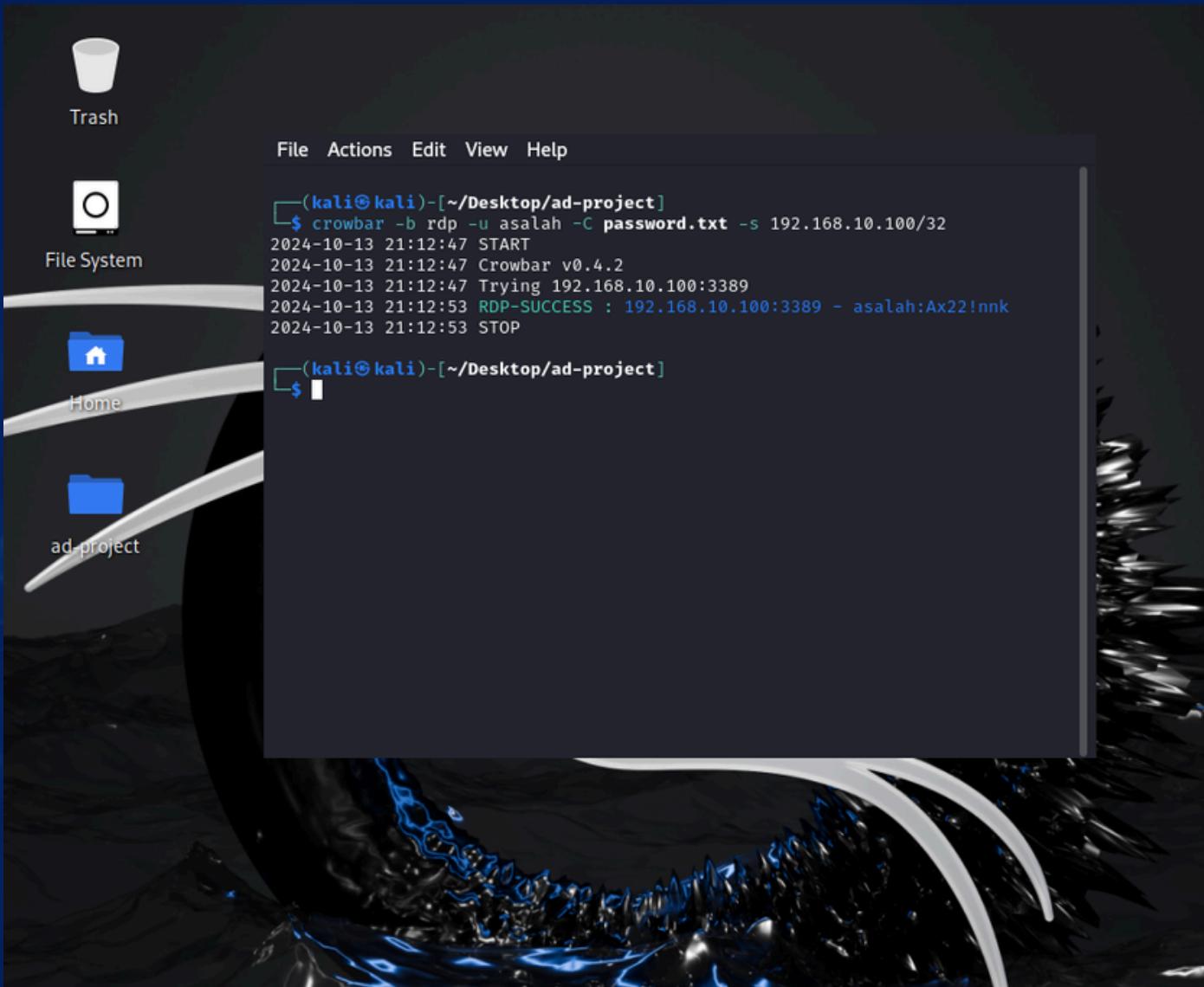
positional arguments:
  options

options:
  -h, --help            show this help message and exit
  -b {openvpn,rdp,sshkey,vnckey}, --brute {openvpn,rdp,sshkey,vnckey}
                        Target service
  -s SERVER, --server SERVER
                        Static target
  -S SERVER_FILE, --serverfile SERVER_FILE
                        Multiple targets stored in a file
  -u USERNAME [USERNAME ...], --username USERNAME [USERNAME ...]
                        Static name to login with
  -U USERNAME_FILE, --usernamefile USERNAME_FILE
                        Multiple names to login with, stored in a file
  -n THREAD, --number THREAD
                        Number of threads to be active at once
  -l FILE, --log FILE  Log file (only write attempts)
  -o FILE, --output FILE
```

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

Search | Splunk 9.3.1

Not secure | 192.168.10.10:8000/en-US/app/search/search?earliest=...

index="endpoint" asalah

173 events (before 10/14/24 1:31:38.000 AM) No Event Sampling

Events (173) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection × Deselect

1 day per column

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 Next >

EventCode

8 Values, 100% of events Selected Yes No

Reports

Average over time Maximum value over time Minimum value over time

Top values Top values by time Rare values

Events with this field

AVG: 4638.71676300578 Min: 4624 Max: 4776 Std Dev: 38.93309118811532

Values	Count	%
4625	140	80.925%
4624	7	4.046%
4634	7	4.046%
4776	7	4.046%
4738	6	3.468%
4720	2	1.156%
4722	2	1.156%
4724	2	1.156%

Account Name: ASalah

WinEventLog:Security

583819065-1104

WinEventLog:Security

583819065-1104

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

Screenshot of a Splunk search results page showing log entries for account logon failures. The interface includes a sidebar with selected fields and interesting fields, and a main table view.

Selected Fields:

- # EventCode 8
- # host 2
- # index 1
- # linecount 8
- # source 1
- # sourcetype 1
- a splunk_server 1

Interesting Fields:

- a Account_Domain 3
- a Account_Name 6
- a Authentication_Package 2
- a Caller_Process_ID 1
- a Caller_Process_Name 1
- a ComputerName 2
- # EventType 1
- a Failure_Reason 1
- # Key_Length 2
- a Keywords 2
- a LogName 1
- a Logon_ID 14
- a Logon_Process 1

Log Entries:

Time	Event
10/21/24 10:20/2024 06:51:22 PM 1:51:22.000 AM	... 20 lines omitted ... Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: asalah Account Domain: Show all 61 lines EventCode = 4625 host = TARGET-PC index = endpoint linecount = 61 source = WinEventLog:Security sourcetype = WinEventLog:Security splunk_server = splunk
10/21/24 10:20/2024 06:51:22 PM 1:51:22.000 AM	... 20 lines omitted ... Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: asalah Account Domain: Show all 61 lines EventCode = 4625 host = TARGET-PC index = endpoint linecount = 61 source = WinEventLog:Security sourcetype = WinEventLog:Security splunk_server = splunk
10/21/24 10:20/2024 06:51:22 PM 1:51:22.000 AM	... 20 lines omitted ...

Screenshot of a Splunk search results page showing a single log entry for a new logon event. The event details include security information, process information, network information, and authentication details. A callout bubble highlights the Network Information section.

Event Details:

New Logon:
 Security ID: S-1-5-21-1370495228-11253530-2583819065-1104
 Account Name: ASalah
 Account Domain: PROJECT
 Logon ID: 0xCAEECE
 Linked Logon ID: 0x0
 Network Account Name: -
 Network Account Domain: -
 Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
 Process ID: 0x0
 Process Name: -

Network Information:
 Workstation Name: kali
 Source Network Address: 192.168.10.250
 Source Port: 0

Detailed Authentication Information:
 Logon Process: NtLmSsp
 Authentication Package: NTLM
 Transited Services: -
 Package Name (NTLM only): NTLM V2
 Key Length: 128

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

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**