Active Directory Purple Team Project

Status Completed

Timing Dec 15, 2025 to Jan 12, 2026

Owners Ron Leong

Overview

This project demonstrates a complete Active Directory attack lifecycle paired with real time detection, response, and hardening in a realistic on-premises AD environment.

Objectives

- Simulate Enterprise Vulnerabilities
- Implement centrailzed monitoring
- Validate Defensive Mechanisms

Setup & Tools

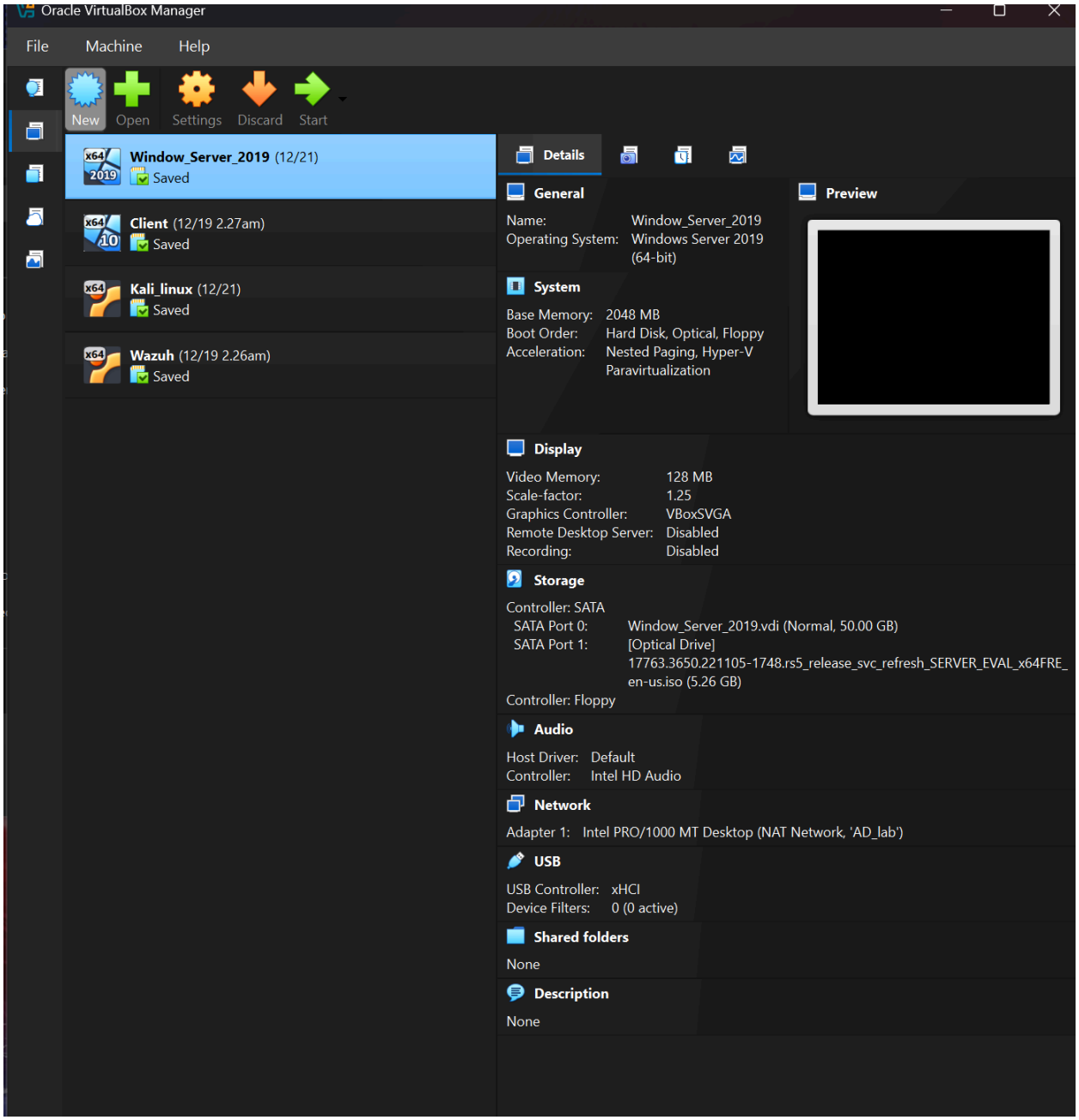
Domain Controller - Windows Server 2019
Attack machine- Kali Linux
Client machine- Windows 10 Pro
SIEM- Wazuh

Tools

Category	Tools
Reconnaissance	Nmap, Responder
Credential Access	John the Ripper
AD Exploitation	Impacket Suite
Privilege Escalation	GodPotato
Monitoring	Sysmon, Wazuh, Windows Event Logs
Infrastructure	Oracle VirtualBox, Windows Server 2019, Window 10 pro

Phase 0: Lab Setup

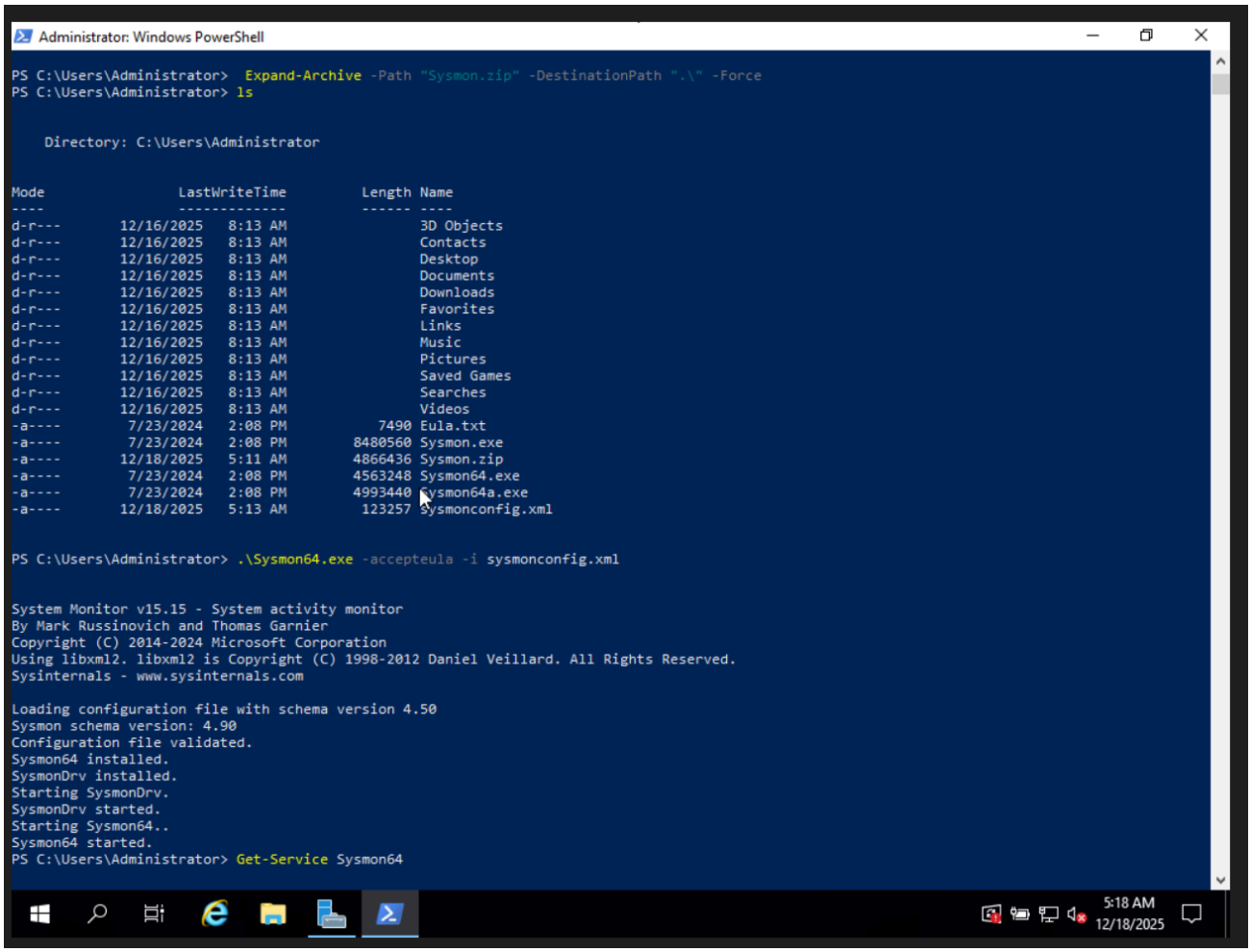
Objective: Build a working pipeline to make sure all attack is observable before exploitation



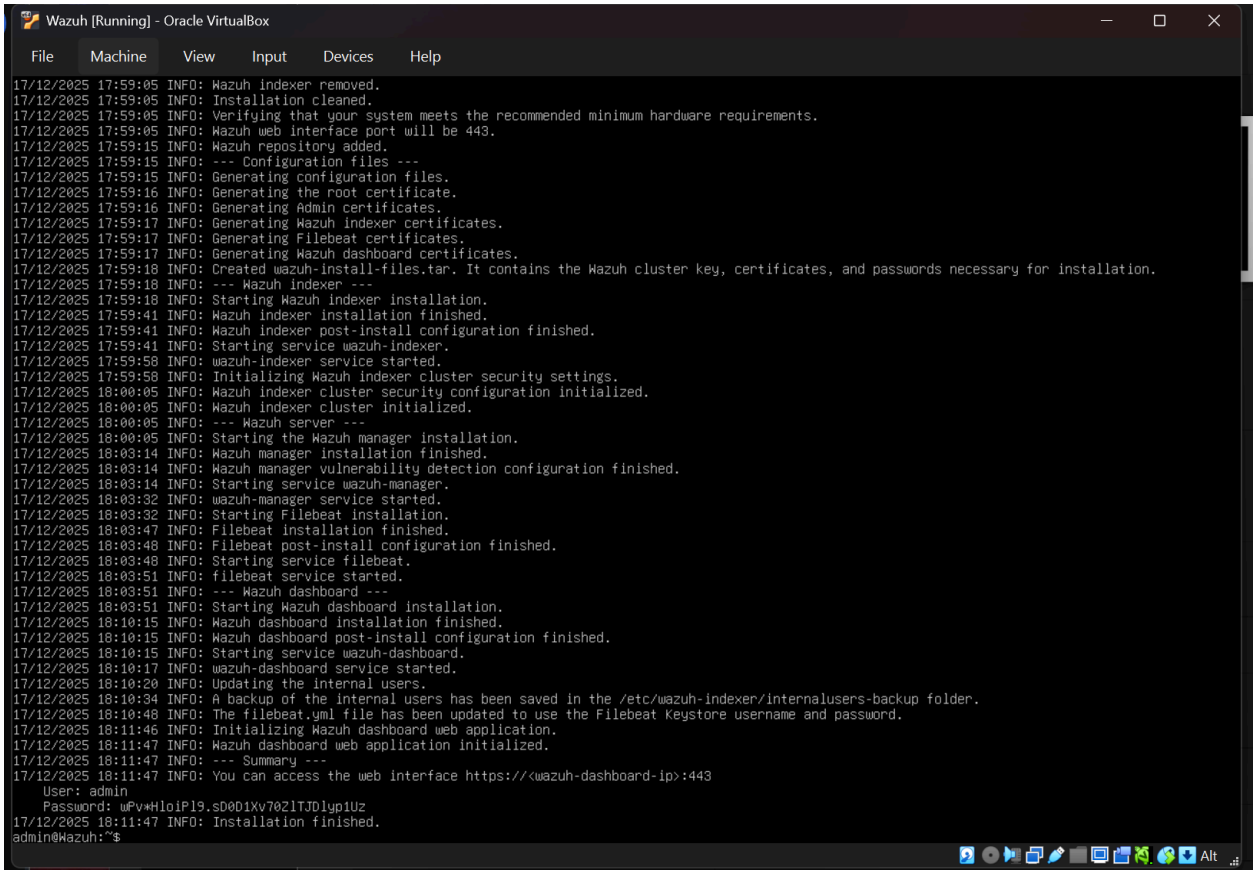
Setup Window Server, a Client Machine with admin and user ‘Bob’, Kali linux machine and a Wazuh Manager

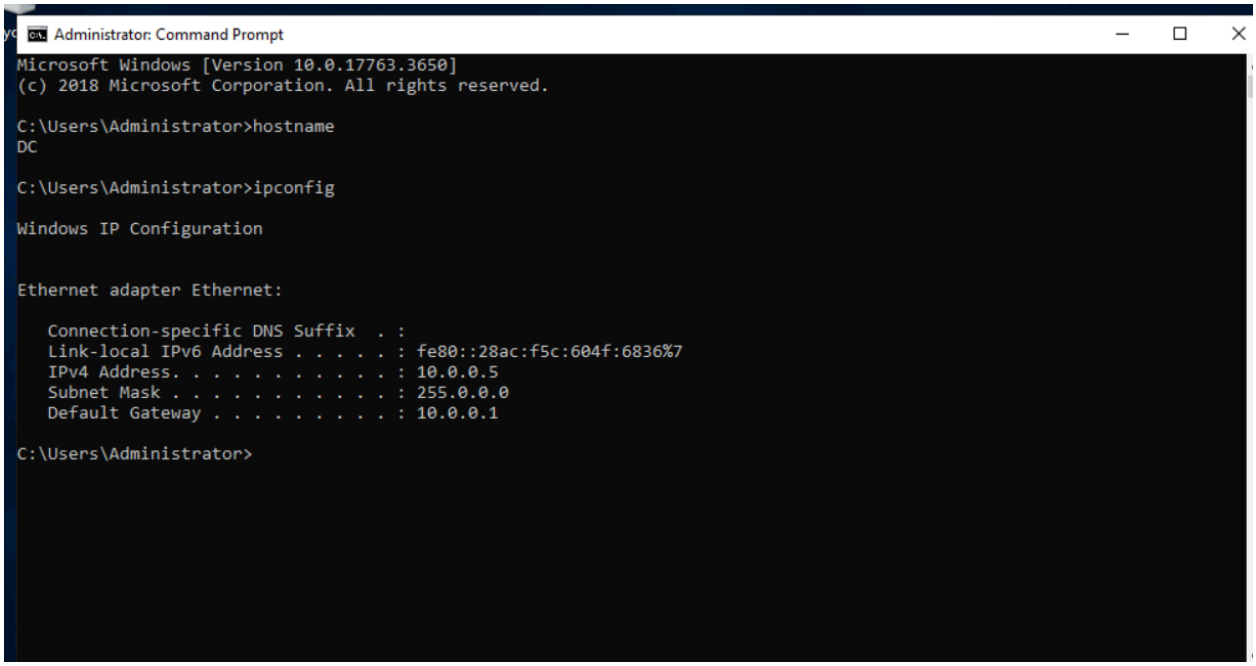
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -S MSSQLSvc/my-sql-server.domain.local:1433 sqlsvc
Checking domain DC=project,DC=lab

Registering ServicePrincipalNames for CN=sqlsvc,CN=Users,DC=project,DC=lab
        MSSQLSvc/my-sql-server.domain.local:1433
Updated object
```

Manually register Service Principal Name for sqlsvc account for Kerberos service ticket to be intercepted and exploited later in the lifecycle



Installed sysmon on Domain Controller to capture advanced endpoint events


Wazuh [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
17/12/2025 17:59:05 INFO: Wazuh indexer removed.
17/12/2025 17:59:05 INFO: Installation cleaned.
17/12/2025 17:59:05 INFO: Verifying that your system meets the recommended minimum hardware requirements.
17/12/2025 17:59:05 INFO: Wazuh web interface port will be 443.
17/12/2025 17:59:15 INFO: Wazuh repository added.
17/12/2025 17:59:15 INFO: --- Configuration files ---
17/12/2025 17:59:15 INFO: Generating configuration files.
17/12/2025 17:59:16 INFO: Generating the root certificate.
17/12/2025 17:59:16 INFO: Generating Admin certificates.
17/12/2025 17:59:17 INFO: Generating Wazuh indexer certificates.
17/12/2025 17:59:17 INFO: Generating Filebeat certificates.
17/12/2025 17:59:17 INFO: Generating Wazuh dashboard certificates.
17/12/2025 17:59:18 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
17/12/2025 17:59:18 INFO: --- Wazuh indexer ---
17/12/2025 17:59:18 INFO: Starting Wazuh indexer installation.
17/12/2025 17:59:41 INFO: Wazuh indexer installation finished.
17/12/2025 17:59:41 INFO: Wazuh indexer post-install configuration finished.
17/12/2025 17:59:41 INFO: Starting service wazuh-indexer.
17/12/2025 17:59:58 INFO: wazuh-indexer service started.
17/12/2025 17:59:58 INFO: Initializing Wazuh indexer cluster security settings.
17/12/2025 18:00:05 INFO: Wazuh indexer cluster security configuration initialized.
17/12/2025 18:00:05 INFO: Wazuh indexer cluster initialized.
17/12/2025 18:00:05 INFO: --- Wazuh server ---
17/12/2025 18:00:05 INFO: Starting the Wazuh manager installation.
17/12/2025 18:03:14 INFO: Wazuh manager installation finished.
17/12/2025 18:03:14 INFO: Wazuh manager vulnerability detection configuration finished.
17/12/2025 18:03:14 INFO: Starting service wazuh-manager.
17/12/2025 18:03:32 INFO: wazuh-manager service started.
17/12/2025 18:03:32 INFO: Starting Filebeat installation.
17/12/2025 18:03:47 INFO: Filebeat installation finished.
17/12/2025 18:03:48 INFO: Filebeat post-install configuration finished.
17/12/2025 18:03:48 INFO: Starting service filebeat.
17/12/2025 18:03:51 INFO: filebeat service started.
17/12/2025 18:03:51 INFO: --- Wazuh dashboard ---
17/12/2025 18:03:51 INFO: Starting Wazuh dashboard installation.
17/12/2025 18:10:15 INFO: Wazuh dashboard installation finished.
17/12/2025 18:10:15 INFO: Wazuh dashboard post-install configuration finished.
17/12/2025 18:10:15 INFO: Starting service wazuh-dashboard.
17/12/2025 18:10:17 INFO: wazuh-dashboard service started.
17/12/2025 18:10:20 INFO: Updating the internal users.
17/12/2025 18:10:34 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
17/12/2025 18:10:48 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
17/12/2025 18:11:46 INFO: Initializing Wazuh dashboard web application.
17/12/2025 18:11:47 INFO: Wazuh dashboard web application initialized.
17/12/2025 18:11:47 INFO: --- Summary ---
17/12/2025 18:11:47 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: wPv*HloiPl9.sD0D1Xv70ZlTJDlyp1Uz
17/12/2025 18:11:47 INFO: Installation finished.
admin@Wazuh:~$
Alt

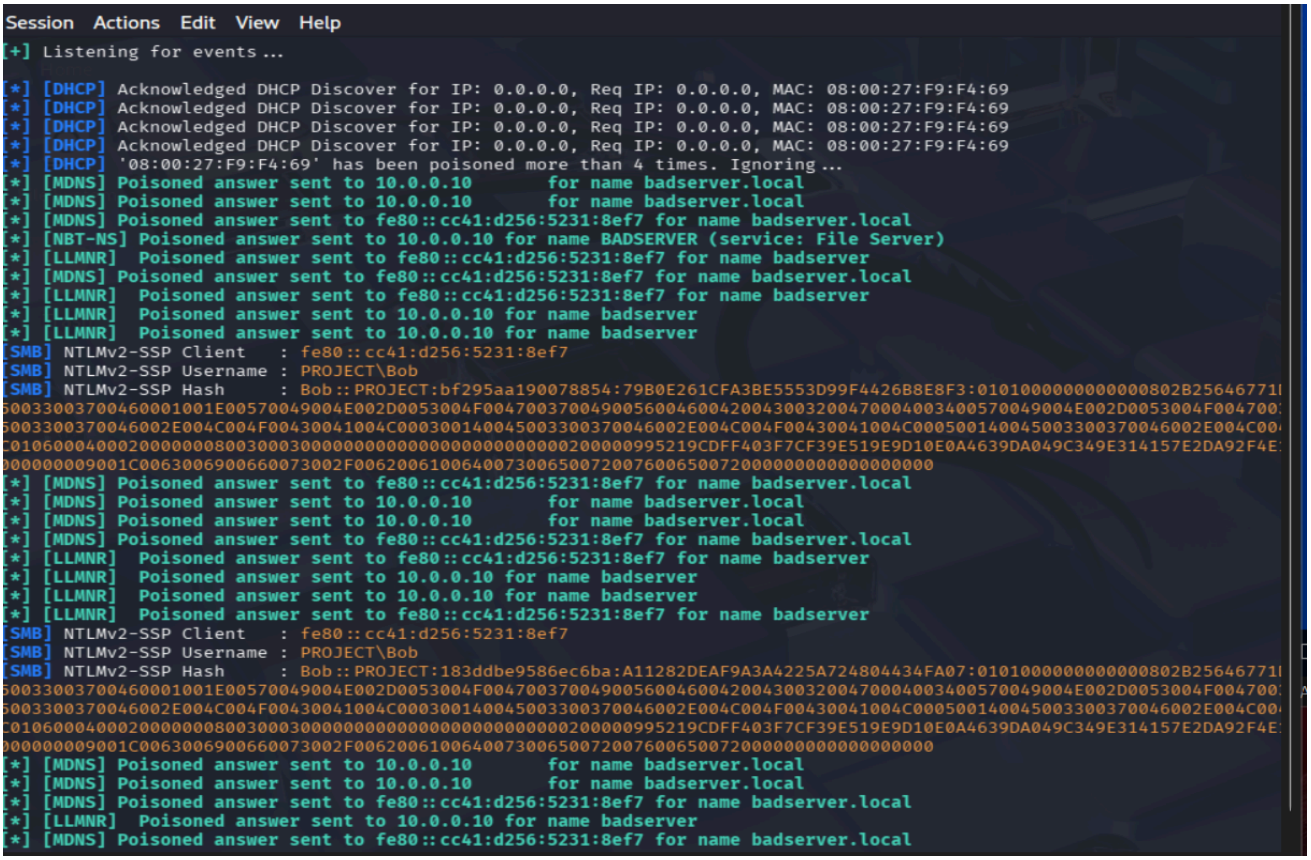


Verified connectivity and make sure Wazuh agent is up and running forwarding important information to the manager

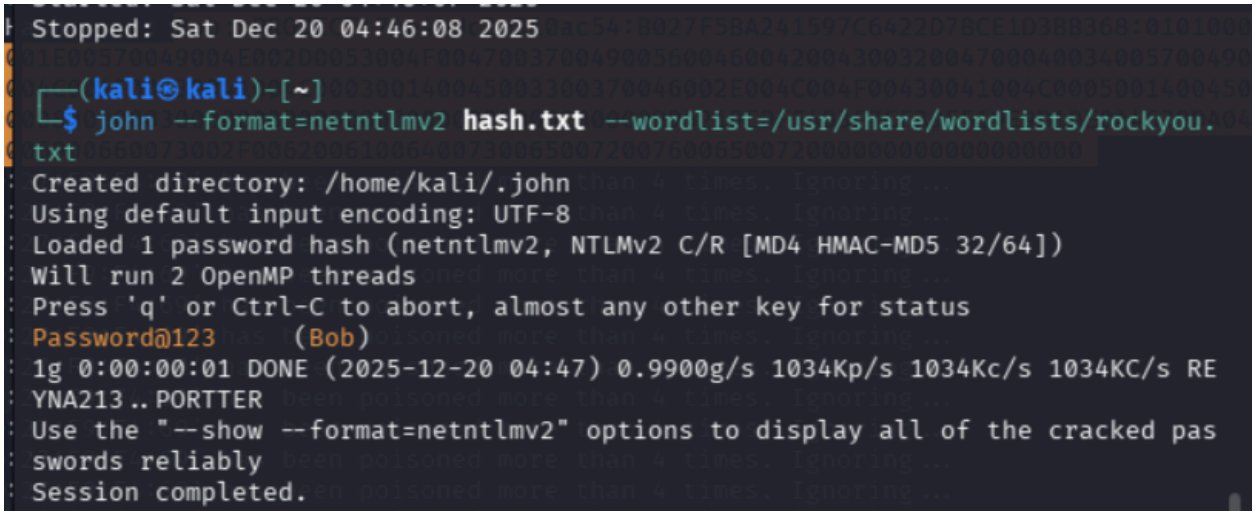
Phase 1: Initial Reconnaissance & Access

Objective: Gain authenticated domain access by exploiting broadcasts protocol

LLMNR Poisoning: LLMNR poisoning initiated using Responder to capture authentication attempts from domain users



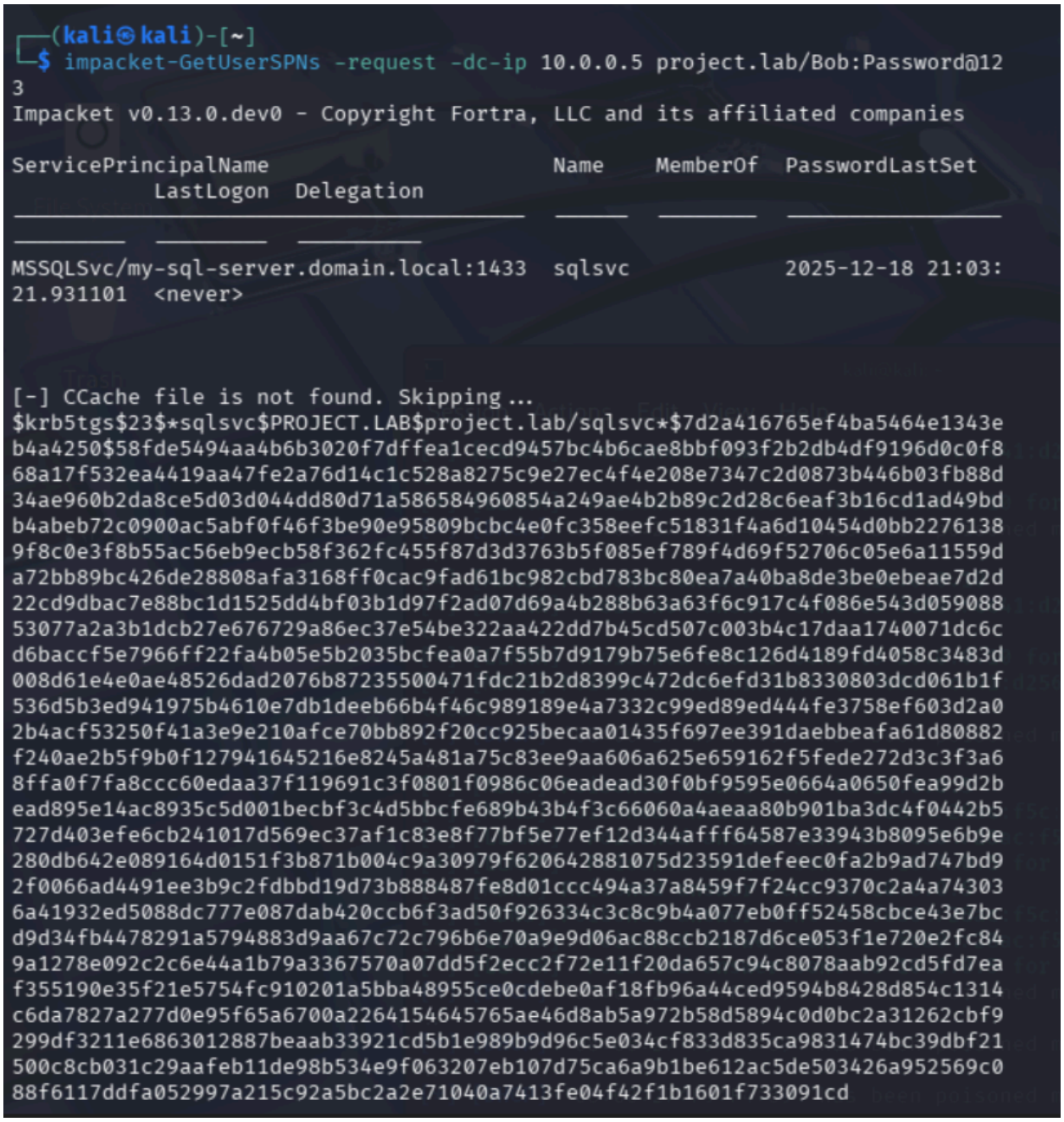
Successfully did the LLMNR poisoning to intercept authentication traffic from the domain environment



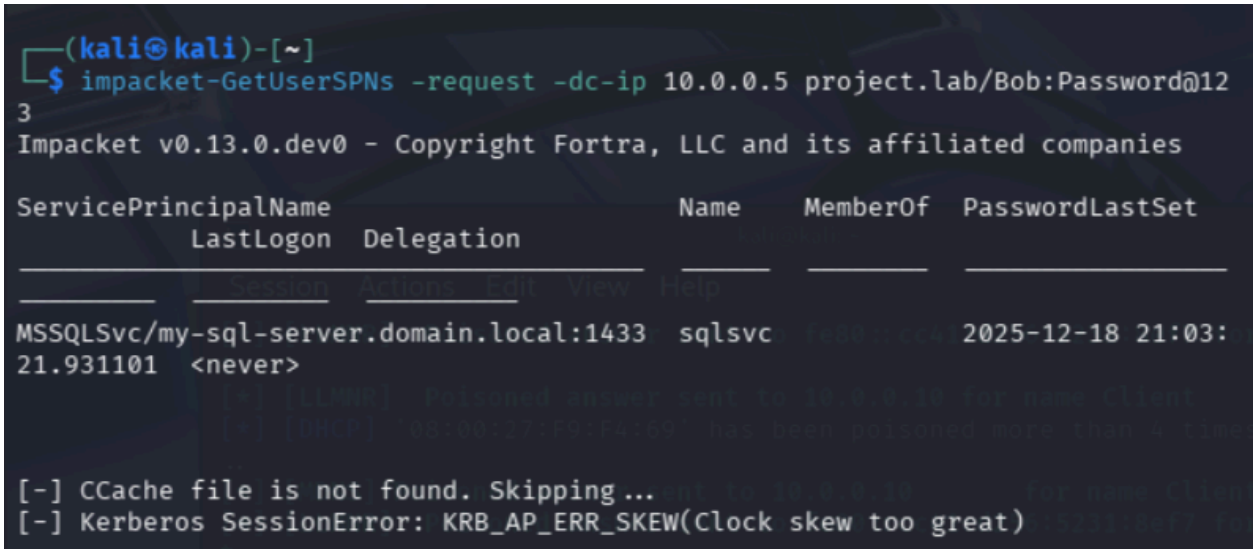
Credential Recovery: Cracking the NTLMv2 hash to get plaintext credentials of user ‘Bob’ using John the ripper

Phase 2 : Active Directory Exploitation

Objective: Escalate privileges by abusing Kerberos protocol misconfigurations

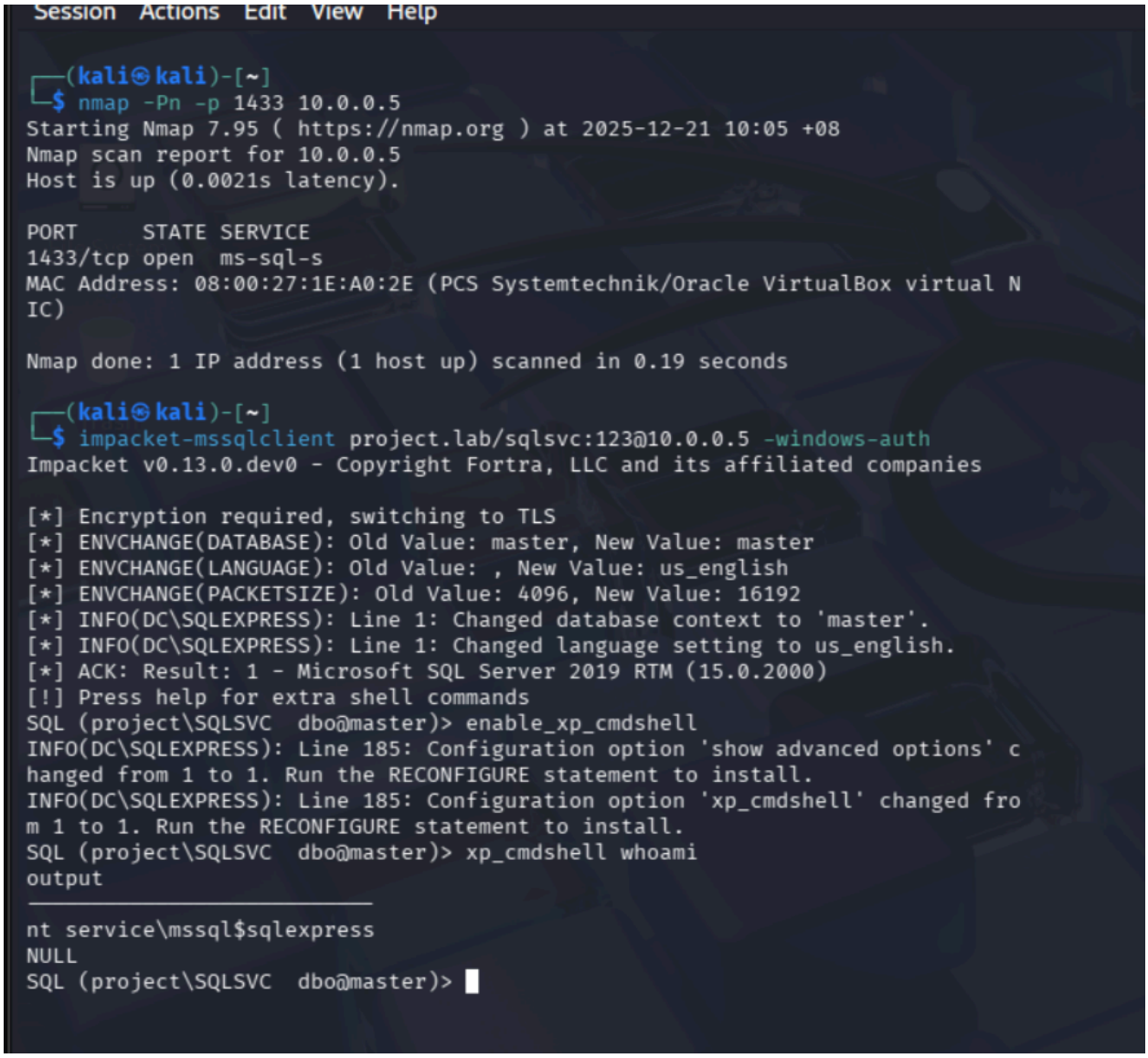


Kerberoasting: Performed SPN enumeration and extraction of ***sqlsvc*** account ticket for offline cracking

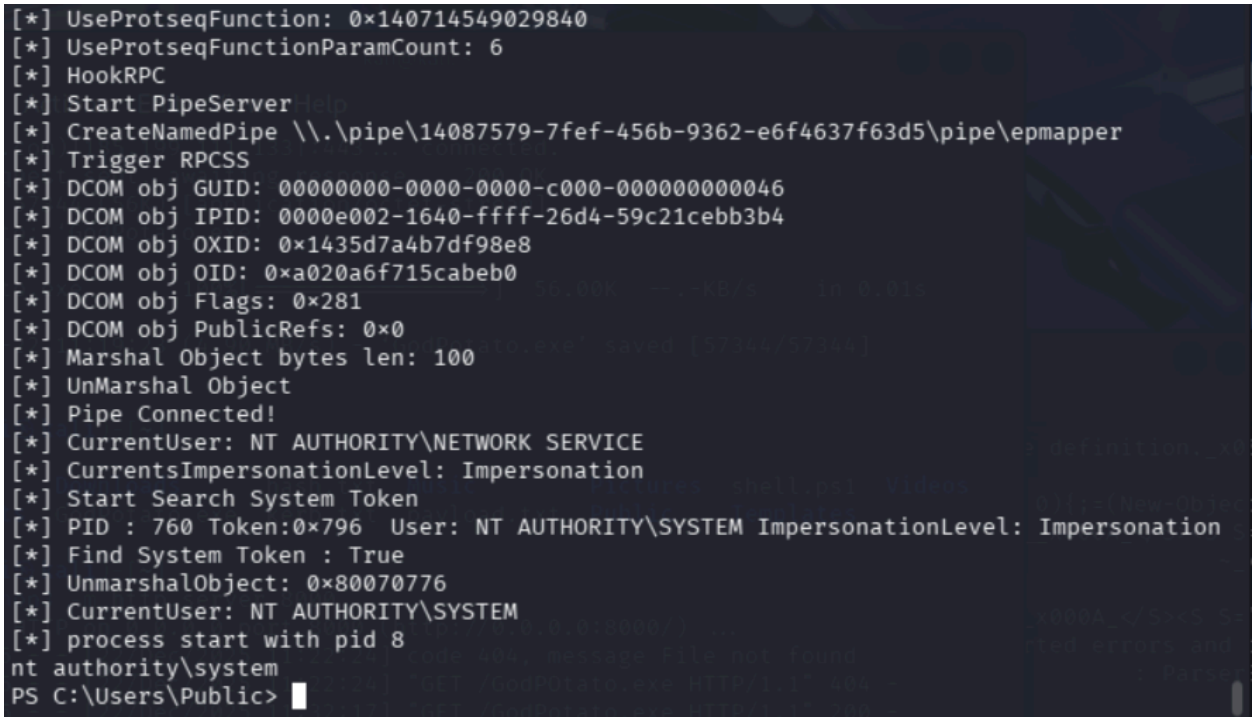


Troubleshooting - When performing Kerberoasting attack encountered a clock skew error between Kali machine and the Domain Controller. Resolve the issue by synchrozining both machines.

Phase 3 : Lateral Movement & Privilege Escalation



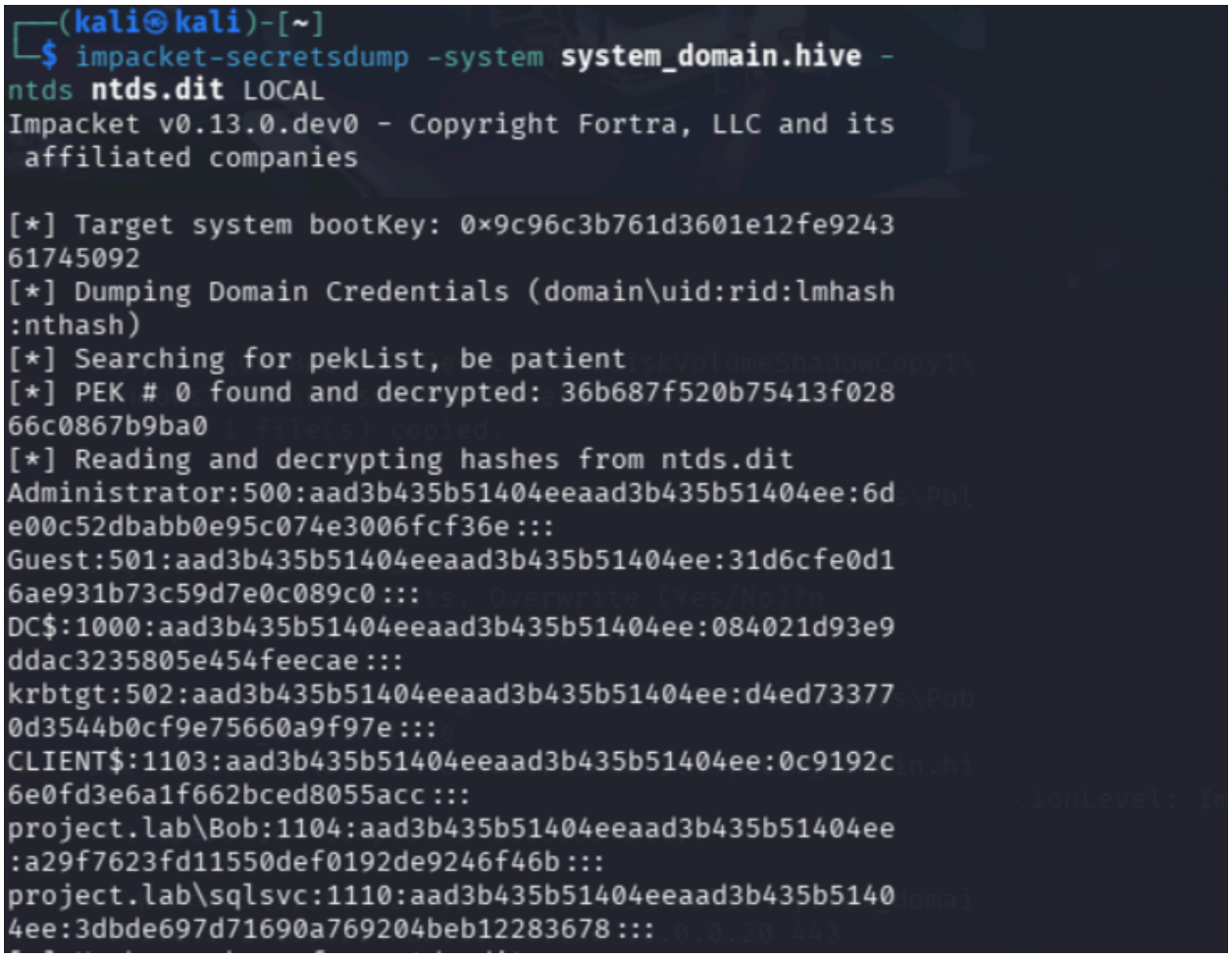
MSSQL exploitation: Identify an exposed database on port 1433 and used ***xp_cmdshell*** to spawn a remote system shell



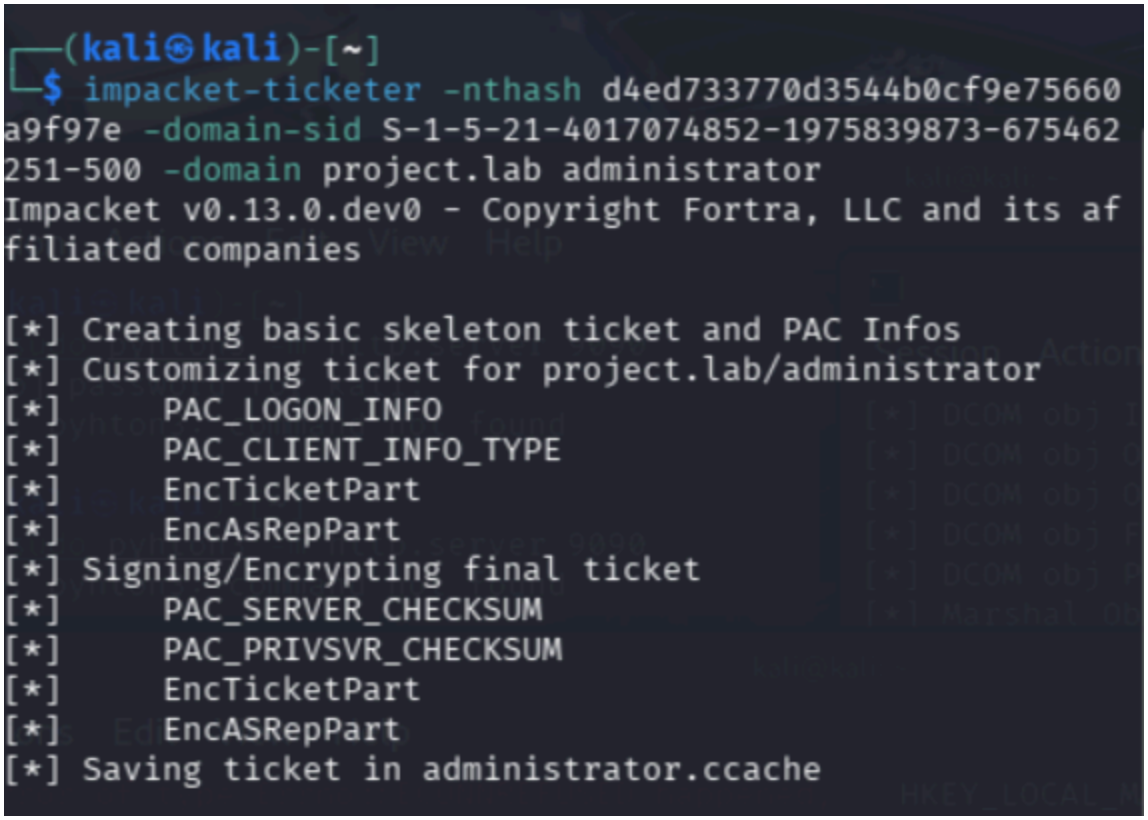
GodPotato Exploit: Escalate access to ***NT AUTHORITY\SYSTEM*** by abusing ***SetImpersonatePrivilege*** on the service account

Phase 4: Domain Dominance & Persistence

Objective: Achieve unrestricted and persistent access to the whole AD domain



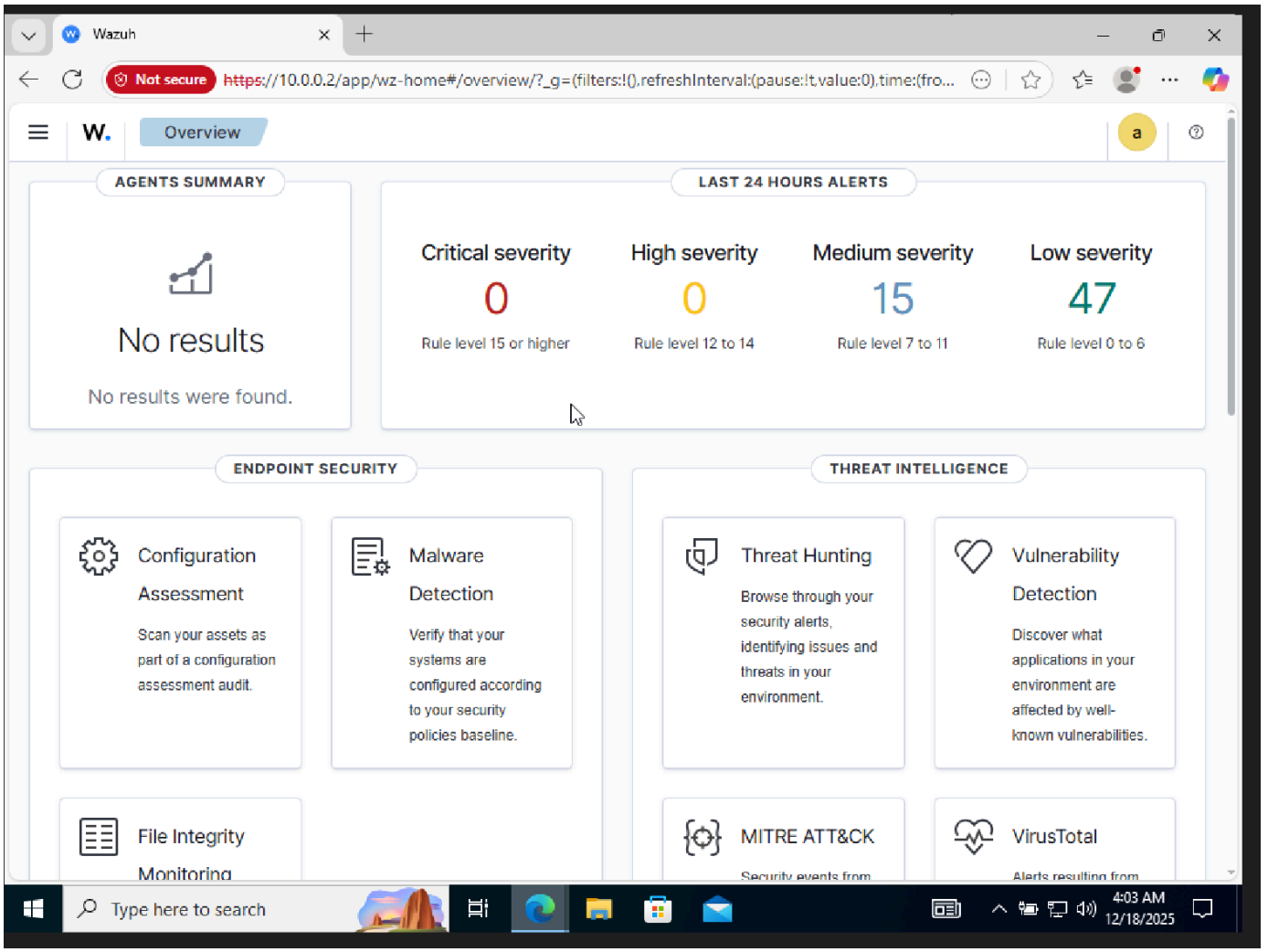
DCSync attack: Used secretdump to extract the KRBTGT hash from the compromised database



Golden Ticket Forgery: Successfully create a Kerberos Golden Ticket with domain wide persistence

Phase 5: Detection & Automated Response

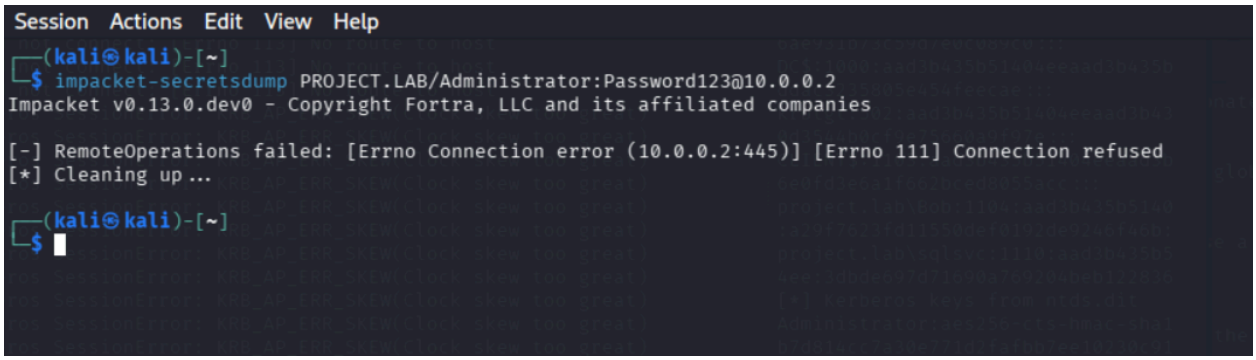
Objective: Demonstrate real time threat detection and incident response automation



A Wazuh Dashboard to centralized all alert and monitoring

```
<command>
  <name>win_route-null</name>
  <executable>route-null.cmd</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

<active-response>
  <command>win_route-null</command>
  <location>local</location>
  <level>12</level>
  <timeout>180</timeout>
</active-response>
```

SOC Engineering: Created a custom rule for system to identify Credential Dumping activity



SOAR implementation: The custom rule worked by instantly cut off the connection of the attacker's IP upon detection

Lesson Learned

This project reinforced that Identity and Access Management is the cornerstone of modern security where most attacks succeeded through identity misconfigurations rather than software bugs. Working across both offensive and defensive roles was insightful. Thinking like an attacker revealed which techniques are most effective, while the defensive perspective taught me how to detect and disrupt those patterns early. The technical challenges I encountered, from clock skew errors during Kerberoasting to connectivity issues, highlighted an important reality where security work often requires fixing infrastructure problems before you can even begin testing. This troubleshooting experience proved just as valuable as the attack and defense techniques themselves.

Technical Mapping

Phase	MITRE ATT&CK Technique	Primary Detection Source	Critical Event IDs
Phase 1	LLMNR Poisoning	Wazuh / Network Traffic	Event ID 4624: Unusual Logon Type 3
Phase 2	Kerberoasting	Windows Security Logs	Event ID 4769: Kerberos Service Ticket Request
Phase 3	Windows Command Shell	Sysmon / Wazuh	Event ID 4688: Suspicious process creation (`sqlservr.exe` → `cmd.exe`)
Phase 3	Access Token Manipulation	Windows Security Logs	Event ID 4672: Special Privileges Assigned

Phase 4	DCSync	Directory Service Access	Event ID 4662: Replication access
Phase 4	Golden Ticket	Kerberos Auth Logs	Event ID 4624: Logons with anomalous Ticket Granting Ticket lifetimes