Virtual Lab Setup for AD Services with Planned Wazuh SIEM Integration

Table of Contents

Introduction

This document outlines the setup of a virtual cybersecurity lab environment using VMware Workstation, with a focus on Active Directory services and a planned Wazuh SIEM deployment. Due to hardware limitations on the host system, it was not feasible to run a third virtual machine (Ubuntu Server) required for the Wazuh Manager. Consequently, while the actual SIEM integration could not be executed, the steps and configurations necessary for a successful Wazuh deployment are included for documentation purposes and future implementation once resources become available.

Lab Environment Overview

- Host: VMware Workstation on host OS (specify version).
- VMs: Windows Server 2019 (Domain Controller), Windows 10 Pro (clients).
- Note: Ubuntu Server VM for Wazuh was planned but not deployed due to insufficient system resources.
- Virtual Network: Host-Only network VMnet1 with subnet 192.168.100.0/24.

Virtual Machine Setup

1. Windows Server 2019

- VM settings: 2 vCPU, 4 GB RAM, 60 GB disk.
- Network Adapter: Host-Only VMnet1.
- ISO checksum: .
- Post-install: Installed VMware Tools.

2. Windows 10 Pro

- VM settings: 2 vCPU, 4 GB RAM, 60 GB disk.
- Network Adapter: Host-Only VMnet1.
- Post-install: VMware Tools installed.

3. Ubuntu Server for Wazuh (Planned)

- Planned VM settings: 2 vCPU, 4 GB RAM, 40 GB disk.
- Planned Network Adapter: Host-Only VMnet1.
- Planned Static IP: 192.168.100.30/24.
- Status: Not deployed due to resource limitations.

Networking and Connectivity

- IP assignments:
  - Server (SRV-DC01): 192.168.1.19
  - Clients(CLT-01): 192.168.1.10,
  - Wazuh Manager (Planned): 192.168.1.30
- DNS: DC (192.168.1.19) as DNS server for all VMs.
- ICMP test: Successful between deployed VMs.

Active Directory Deployment

- Renamed server to SRV-DC01 before promotion.
- Installed AD DS role and created domain: lab.local.
- DNS installed on Domain Controller.
- Time synchronization:
  - DC syncs via internet NTP.
  - Clients sync to DC.

Firewall Rules Between VMs

- Opened the following TCP ports:
  - 389, 22, 443, 3389 (inbound/outbound) on Windows Firewall (Server and Clients).
- Used PowerShell snippets to configure and document firewall rules.

OU and GPO Structure

Organizational Units (OUs)

- OU1: Finance
- OU2: HR

Group Policy Objects (GPOs)

- GPO_Wallpaper_OU1: Deploy wallpaper1.jpg.
- GPO_Wallpaper_OU2: Deploy wallpaper2.jpg.
- GPO_Deploy_Putty: Assign putty.msi.
- GPO_Disable_CP_TM_FW_OU1: Disable Control Panel, Task Manager, Firewall UI.
- GPO_Disable_PS_CMD_REG_OU2: Disable PowerShell, CMD, Registry Editor.

- GPO_Disable_USB: Deny removable storage access.
- GPO_Network_Config: Set IPv4 preferences (for static IP scenarios).
- Security Filtering: Default.
- Testing: Verified with gpresult, tested user policies and system restrictions

Wazuh SIEM Deployment (Planned Steps)

1. Ubuntu Preparation (Hypothetical)

- Perform system update:
  ```
  apt update && apt upgrade
  ```
- Configure static IP and confirm.
- Configure UFW Firewall to allow:
  - Ports 1514, 1515 (from Windows subnet)
  - Port 5601 (Wazuh Dashboard)

2. All-in-One Installation (Hypothetical)

- Download installer script:
  ```
  curl -sO https://packages.wazuh.com/4.x/wazuh-install.sh
  ```
- Execute script:
  ```
  sudo bash wazuh-install.sh --all-in-one
  ```
- Store Kibana admin credentials securely.
- Verify services (Wazuh Manager, Filebeat, Elasticsearch, Kibana).

3. Agent Installation on Windows (Planned)

- MSI available at: \\SRV-DC01\SoftwareDeploy$\wazuh-agent.msi
- Silent installation:
  ```
  msiexec /i wazuh-agent.msi /qn
  ```
- Agent registration:
  ```
  .\agent-auth.exe -m 192.168.100.30
  ```
- Verify agent:
  ```
  manage_agents -l
  ```
- Configure ossec.conf for eventchannel logs.
- Ensure outbound firewall rules allow Wazuh ports.

4. Log Collection Tests (Planned)

- Simulate failed logins and create test events.

- Verify event visibility in Wazuh Dashboard.
- Capture screenshots of alerts and dashboards.

Troubleshooting

- VMs Not Communicating
  Cause: Wrong network type or firewall rules.
  Fix: Set both VMs to Host-Only or Internal network; enable ICMP in firewall.

- Domain Join Failure
  Cause: Incorrect DNS or unreachable DC.
  Fix: Set client DNS to server IP; test connectivity with `ping` and `nslookup`.

- GPO Not Applying
  Cause: GPO not linked or user not in correct OU.
  Fix: Use `gpupdate /force` and `gpresult /h report.html` to verify.

- Wallpaper or Software Not Deploying
  Cause: Incorrect UNC path or permissions.
  Fix: Ensure shared folder is accessible (e.g., `\\SRV-DC01\Wallpapers$`), and assign Read rights.

- GPO Restrictions (e.g., USB, CMD) Not Working
  Cause: Wrong scope or conflicting policies.
  Fix: Confirm correct OU targeting; restart client; ensure settings under User/Computer Configuration.

- Shared Folder Not Accessible from Offline VM
  Cause: VMware Tools not installed or sharing not enabled.
  Fix: Install VMware Tools, enable Shared Folders, map using `\\vmware-host\Shared Folders\LabDownloads`.

- Wazuh Agent Not Sending Logs (if deployed)
  Cause: Agent misconfigured or port blocked.
  Fix: Verify manager IP in agent config, open ports 1514/udp and 1515/tcp, and restart the agent.

- Agent connection issues (anticipated):
  Check firewall ports and verify manager IP.

- Time drift:
  Use Windows Time Service and DC/NTP alignment.

- Elasticsearch memory/resource errors (if deployed):
  Increase VM RAM allocation.
- GPO issues:
  Diagnose using gpresult, gpupdate, and OU membership checks.

Snapshots and Backup

- Took VM snapshots at milestones:
  Before AD promotion
- Backed up GPOs using GPMC export feature.

References

- VMware Networking: Host-Only and LAN segments.
- Group Policy: Desktop Wallpaper, Software Deployment.
- Wazuh: All-in-One Installation Guide.
- Microsoft: Group Policy Settings Documentation.