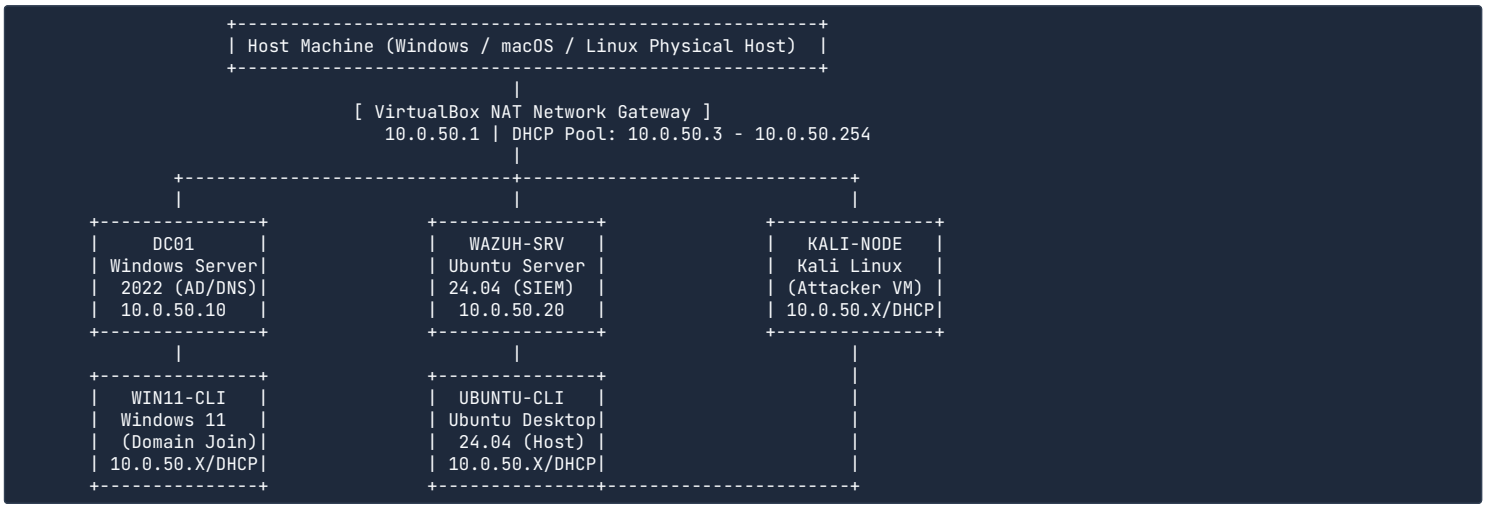
1. RANGE ARCHITECTURE & SUBNET TOPOLOGY OVERVIEW

This field manual provisions an enterprise-representative detection and adversary emulation range inside Oracle VM VirtualBox at zero financial cost. It isolates Active Directory identity services, centralized SIEM telemetry, Linux host auditing, an isolated mail transfer agent, and an offensive security node on a dedicated internal subnet.



2. BILL OF VIRTUAL MATERIALS & RESOURCE SIZING MATRIX

Host Identifier	Role / Workload	Operating System	vCPU / RAM / Disk	IP Assignment & Ports
DC01	Domain Controller, DNS, PKI, Mail	Windows Server 2022 Eval	2 vCPU / 4096 MB / 60 GB	`10.0.50.10` (Static) | 53, 88, 135, 389, 445, 25, 143
WAZUH-SRV	Indexer, Manager, SIEM Web Dashboard	Ubuntu Server 24.04 LTS	2 vCPU / 4096 MB / 50 GB	`10.0.50.20` (Static) | 443 (HTTPS), 1514 (Agents), 1515, 55000
WIN11-CLI	Domain Endpoint Victim Client	Windows 11 Enterprise Eval	2 vCPU / 4096 MB / 60 GB	Dynamic DHCP (`10.0.50.X`) | Sysmon v15, Wazuh Agent
UBUNTU-CLI	Linux Client / Analyst Workstation	Ubuntu Desktop 24.04 LTS	2 vCPU / 4096 MB / 40 GB	Dynamic DHCP (`10.0.50.X`) | Auditd Engine, Wazuh Agent
KALI-NODE	Threat Simulation & Adversary Emulation	Kali Linux Rolling (Appliance)	2 vCPU / 3072 MB / 40 GB	Dynamic DHCP (`10.0.50.X`) | Impacket, Swaks, Nmap, Hydra

3. VIRTUALBOX & NAT NETWORK SETUP

1. Download & install **VirtualBox** and the **Extension Pack** from `virtualbox.org`.
2. In VirtualBox Manager, click **Tools > Network** > select **NAT Networks** tab.
3. Click **Create** (+) and configure the properties:
   - **Network Name:** `LabNet-DHCP`
   - **IPv4 Prefix:** `10.0.50.0/24`
   - **Enable DHCP: Checked** (Auto leases)
   - **Enable IPv6: Unchecked**
4. Click **Apply**. All VMs will attach to this network.

4. OFFICIAL MEDIA SOURCING MATRIX

- **Windows Server 2022 (180-Day Eval ISO):** Microsoft Evaluation Center (`microsoft.com/evalcenter`)
- **Windows 11 Enterprise (90-Day Eval ISO):** Microsoft Evaluation Center (`microsoft.com/evalcenter`)
- **Ubuntu Server 24.04 LTS ISO:** Canonical (`ubuntu.com/download/server`)
- **Ubuntu Desktop 24.04 LTS ISO:** Canonical (`ubuntu.com/download/desktop`)
- **Kali Linux Appliance:** OffSec (`kali.org/get-kali/#kali-virtual-machines`)

5. PROVISIONING THE `DC01` VIRTUAL MACHINE

1. In VirtualBox, click **New** (`Ctrl + N`):
   - **Name:** `DC01` | **Type:** `Microsoft Windows` | **Version:** `Windows 2022 (64-bit)`
   - **ISO Image:** Browse and select the downloaded `Windows_Server_2022_Eval.ISO`.
   - **Skip Unattended Installation: Checked** (ensures manual control over partitioning and local accounts).
2. **Hardware Allocation:** Set **Base Memory** to `4096 MB` (4 GB) and **Processors** to `2 vCPUs`. Leave *Enable EFI* **unchecked**.
3. **Virtual Disk:** Select **Create a Virtual Hard Disk Now**, set size to `60.00 GB` (Dynamically Allocated VDI), and click **Finish**.
4. **Network Binding:** Open **Settings > Network > Adapter 1**:
   - **Attached to:** `NAT Network` | **Name:** `LabNet-DHCP`
   - **Advanced > Promiscuous Mode:** `Allow VMs` (or `Allow All`) | **Cable Connected:** `Checked`.

6. WINDOWS SERVER 2022 OS INSTALLATION & BASELINE SETUP

1. Power on `DC01`. Press any key when prompted to boot from the mounted ISO.
2. Confirm Language/Keyboard settings > click **Next > Install Now**.
3. Select **Windows Server 2022 Standard Evaluation (Desktop Experience)** > accept license terms > click **Next**.
4. Choose **Custom: Install Microsoft Server Operating System only (advanced)** > highlight **Drive 0 Unallocated Space (60.0 GB)** > click **Next**.
5. When installation completes, enter a secure lab administrator password (e.g., `P@ssw0rd2026!`) and click **Finish**.
6. Log in via **Input > Keyboard > Insert Ctrl-Alt-Del**.
7. Mount Guest Additions: Click **Devices > Insert Guest Additions CD Image...**, open File Explorer (`Win + E`), navigate to CD Drive (`D:`), and run `VBoxWindowsAdditions.exe`. Complete setup, unmount ISO (`Devices > Optical Drives > Remove disk`), and reboot.

7. STATIC NETWORK BINDING & HOSTNAME CONFIGURATION

Domain Controllers require a fixed IP address to prevent DNS routing failures. Open PowerShell as Administrator on `DC01` and run:

```
# 1. Identify network adapter alias
Get-NetAdapter

# 2. Assign static IP, subnet mask, and gateway
New-NetIPAddress -InterfaceAlias "Ethernet" `
  -IPAddress 10.0.50.10 `
  -PrefixLength 24 `
  -DefaultGateway 10.0.50.1

# 3. Point primary DNS to local loopback (self) and secondary to NAT gateway
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" `
  -ServerAddresses ("127.0.0.1", "10.0.50.1")

# 4. Rename computer and reboot
Rename-Computer -NewName "DC01" -Restart
```

8. ACTIVE DIRECTORY DOMAIN SERVICES (AD DS) & DNS PROMOTION

Step 1: Install Server Roles

1. In **Server Manager**, click **Manage > Add Roles and Features**.
2. Installation Type: **Role-based or feature-based installation**.
3. Server Selection: Select **DC01**.
4. Check: **Active Directory Domain Services** and **DNS Server** (accept required features).
5. Advance to Confirmation and click **Install**.

Step 2: Promote Server to Domain Controller

1. Click the yellow **Notification Flag** > select **Promote this server to a domain controller**.
2. Deployment: Select **Add a new forest** > Root domain: `lab.local`.
3. Domain Controller Options: Set DSRM password to `DSRMP@ssw0rd2026!`.
4. Additional Options: Verify NetBIOS name defaults to `LAB`.
5. Paths / Prerequisites: Accept defaults > click **Install** (reboots automatically).

9. POST-PROMOTION HEALTH VERIFICATION

Log in as `LAB\Administrator` and run the following PowerShell diagnostics to verify Global Catalog and DNS health:

```
# Verify Domain Controller role, Global Catalog status, and IP binding
Get-ADDomainController -Identity DC01 | `
  Select-Object Name, Domain, Forest, IPv4Address, IsGlobalCatalog

# Verify authoritative DNS diagnostic health
dcdiag /test:DNS /v
```

10. ACTIVE DIRECTORY CERTIFICATE SERVICES (AD CS / ENTERPRISE PKI)

1. In **Server Manager** on `DC01`, navigate to **Manage > Add Roles and Features**.
2. On Server Roles, check **Active Directory Certificate Services** > click **Next**.
3. On Role Services, check **Certification Authority** > click **Next > Install**.
4. Click the **Notification Flag** > select **Configure Active Directory Certificate Services**:
   - **Credentials:** `LAB\Administrator` | **Role Services:** Check **Certification Authority**.
   - **Setup Type:** Select **Enterprise CA** (integrates with AD DS) | **CA Type: Root CA**.
   - **Private Key: Create a new private key** | **Cryptographic Provider:** `RSA#Microsoft Software Key Storage Provider`.
   - **Key Length / Hash:** `2048` / `SHA256` | **Validity Period:** `5 Years` > click **Configure**.

11. ENTERPRISE DIRECTORY HIERARCHY & USER POPULATION SCRIPT

Execute in elevated PowerShell on `DC01` to provision the complete organizational structure, security groups, simulated enterprise accounts, and a Kerberoastable SQL service account with a registered Service Principal Name (SPN):

```
Import-Module ActiveDirectory

# 1. Provision Organizational Units (OUs)
$RootOU = "OU=PORT_ZERO_ENTERPRISE,DC=lab,DC=local"
New-ADOrganizationalUnit -Name "PORT_ZERO_ENTERPRISE" -Path "DC=lab,DC=local" -ProtectedFromAccidentalDeletion $false

@("Administrative_Accounts","Service_Accounts","Workstations","Servers","Departments") | ForEach-Object {
    New-ADOrganizationalUnit -Name $_ -Path $RootOU -ProtectedFromAccidentalDeletion $false
}
@("Executive","Finance","Human_Resources","Information_Technology") | ForEach-Object {
    New-ADOrganizationalUnit -Name $_ -Path "OU=Departments,$RootOU" -ProtectedFromAccidentalDeletion $false
}

# 2. Provision Security Groups
New-ADGroup -Name "Sec_IT_Admins" -GroupScope Global -GroupCategory Security -Path "OU=Administrative_Accounts,$RootOU"
New-ADGroup -Name "Sec_Finance_Users" -GroupScope Global -GroupCategory Security -Path "OU=Finance,OU=Departments,$RootOU"
New-ADGroup -Name "Sec_Standard_Employees" -GroupScope Global -GroupCategory Security -Path "OU=Departments,$RootOU"

# 3. Provision Enterprise Users
$Pass = ConvertTo-SecureString "CyberLab2026!" -AsPlainText -Force
$Users = @(
    @{F="John"; L="Doe"; U="jdoe"; D="Information_Technology"; T="Senior Systems Engineer"},
    @{F="Alice"; L="Smith"; U="asmith"; D="Finance"; T="Financial Controller"},
    @{F="Robert"; L="Taylor"; U="rtaylor"; D="Human_Resources"; T="HR Coordinator"},
    @{F="Evelyn"; L="Vance"; U="evance"; D="Executive"; T="Chief Operating Officer"}
)
foreach ($u in $Users) {
    New-ADUser -Name "$($u.F) $($u.L)" -GivenName $u.F -Surname $u.L `
               -SamAccountName $u.U -UserPrincipalName "$($u.U)@lab.local" `
               -Path "OU=$($u.D),OU=Departments,$RootOU" `
               -AccountPassword $Pass -Enabled $true -Title $u.T -PasswordNeverExpires $true
    Add-ADGroupMember -Identity "Sec_Standard_Employees" -Members $u.User
}
Add-ADGroupMember -Identity "Sec_IT_Admins" -Members "jdoe"

# 4. Provision Service Account with Service Principal Name (SPN) for Kerberoasting
New-ADUser -Name "svc_sql_prod" `
           -SamAccountName "svc_sql_prod" `
           -UserPrincipalName "svc_sql_prod@lab.local" `
           -Path "OU=Service_Accounts,$RootOU" `
           -AccountPassword (ConvertTo-SecureString "SQL_Svc_2026!" -AsPlainText -Force) `
           -Enabled $true -PasswordNeverExpires $true

Set-ADUser -Identity "svc_sql_prod" `
           -ServicePrincipalNames @{Add="MSSQLSvc/db01.lab.local:1433"}
```

12. GROUP POLICY OBJECT (GPO) DEFENSIVE AUDIT BASELINE

1. Open **Group Policy Management** (`gpmc.msc`). Right-click domain `lab.local` > select **Create a GPO in this domain, and Link it here...**; name it `GPO-Defensive-Audit-Baseline`.
2. Right-click `GPO-Defensive-Audit-Baseline` > **Edit**.
3. Navigate to: `Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies`:

Audit Category	Subcategory / Setting	Configured State	Analyst Telemetry Objective
Account Logon	Audit Kerberos Service Ticket Operations	Success & Failure	Captures TGS requests and Kerberoasting activity (Event ID 4769)
Account Logon	Audit Kerberos Authentication Service	Success & Failure	Captures TGT requests and AS-REP roasting activity (Event ID 4768)
Account Management	Audit User Account Management	Success & Failure	Tracks user account creations, edits, and password resets (Event ID 4720, 4738)
Detailed Tracking	Audit Process Creation	Success & Failure	Captures executable launches across systems (Event ID 4688)
Logon/Logoff	Audit Logon / Audit Special Logon	Success & Failure	Tracks session authentications and elevated admin logins (Event ID 4624, 4672)
Privilege Use	Audit Sensitive Privilege Use	Success & Failure	Detects token privilege manipulation and impersonation (Event ID 4673)

4. Navigate to: `Computer Configuration > Policies > Administrative Templates > System > Audit Process Creation`:
   - Double-click **Include command line in process creation events** > select **Enabled** > click **OK**.
5. Navigate to: `Computer Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell`:
   - Enable **Turn on PowerShell Script Block Logging** (logs full script code in Event ID 4104).
   - Enable **Turn on Module Logging** (Module names: `*`).
6. Open PowerShell as Administrator on `DC01` and force policy application:

```
gpupdate /force
auditpol /get /category:*
```

13. PROVISIONING THE `WIN11-CLI` VIRTUAL MACHINE

1. In VirtualBox, click **New** (`Ctrl + N`):
   - **Name:** `WIN11-CLI` | **Type:** `Microsoft Windows` | **Version:** `Windows 11 (64-bit)`
   - **ISO Image:** Select `Windows_11_Enterprise_Eval.ISO` | **Skip Unattended Installation: Checked**.
2. **Hardware Allocation:** Base Memory: `4096 MB` (4 GB), Processors: `2 vCPUs`.
   - **Enable EFI: Checked** | **TPM Type:** `v2.0` | **Secure Boot: Enabled**.
3. **Virtual Disk:** Create a `60.00 GB` Dynamically Allocated VDI.
4. **Network Binding:** Open **Settings > Network > Adapter 1** > Attached to: `NAT Network` > Name: `LabNet-DHCP` > Promiscuous: `Allow VMs`.

14. OS INSTALLATION & OUT-OF-BOX EXPERIENCE (OOBE) WORKAROUND

1. Start `WIN11-CLI`. Press any key when prompted to boot from ISO.
2. Select Language preferences > click **Install Now** > select **Windows 11 Enterprise Evaluation**.
3. Select **Custom: Install Windows only (advanced)** > highlight Drive 0 > click **Next**.
4. When prompted in OOBE with *How would you like to set up this device?*:
   - Select **Set up for work or school** > click **Next**.
   - On the *Sign in with Microsoft* screen, click **Sign-in options** > select **Domain join instead**.
   - Set local admin username: `LocalAdmin` | Password: `P@ssw0rd2026!` (complete the 3 security questions).
5. Mount Guest Additions (`Devices > Insert Guest Additions CD Image...`), run `VBoxWindowsAdditions.exe`, and reboot.

15. DNS CONFIGURATION & DOMAIN JOIN (`LAB.LOCAL`)

Windows endpoints must query `DC01` for Active Directory SRV discovery. Open PowerShell as Administrator on `WIN11-CLI`:

```powershell
# 1. Identify active interface and redirect DNS to DC01
$Adapter = Get-NetAdapter | Where-Object {$_.Status -eq "Up"}
Set-DnsClientServerAddress -InterfaceIndex $Adapter.InterfaceIndex `
  -ServerAddresses ("10.0.50.10", "10.0.50.1")

# 2. Test domain controller reachability
Resolve-DnsName -Name "lab.local"
Test-NetConnection -ComputerName "DC01.lab.local" -Port 389

# 3. Join the domain and move computer account into the Workstations OU
$Creds = Get-Credential -UserName "LAB\Administrator" `
  -Message "Enter Domain Admin Credentials"
Add-Computer -DomainName "lab.local" -Credential $Creds `
  -OUPath "OU=Workstations,OU=PORT_ZERO_ENTERPRISE,DC=lab,DC=local" `
  -NewName "WIN11-CLI" -Restart
```

Post-Reboot Authentication: Send `Ctrl+Alt+Del` > select **Other user** > log in as `LAB\jdoe` (Password: `CyberLab2026!`).

16. SYSMON V15 TELEMETRY ENGINE DEPLOYMENT

Deploy Microsoft Sysinternals Sysmon with the SwiftOnSecurity configuration on `WIN11-CLI` (and `DC01`):

```powershell
# Run in elevated PowerShell on WIN11-CLI:
New-Item -Path "C:\Tools\Sysmon" -ItemType Directory -Force
Set-Location "C:\Tools\Sysmon"

# Fetch Sysmon binary and SwiftOnSecurity detection XML
Invoke-WebRequest -Uri "https://download.sysinternals.com/files/Sysmon.zip" `
  -OutFile "Sysmon.zip"
Expand-Archive -Path "Sysmon.zip" -DestinationPath "." -Force

Invoke-WebRequest `
  -Uri "https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-config/master/sysmonconfig-export.xml" `
  -OutFile "sysmonconfig.xml"

# Install Sysmon service and verify driver state
.\Sysmon64.exe -accepteula -i sysmonconfig.xml
Get-Service -Name "Sysmon64"
```

17. PROVISIONING THE `WAZUH-SRV` VIRTUAL MACHINE

1. In VirtualBox, click **New** (`Ctrl + N`):
   - **Name:** `WAZUH-SRV` | **Type:** `Linux` | **Version:** `Ubuntu (64-bit)`
   - **ISO Image:** Select `ubuntu-24.04-live-server-amd64.iso` | **Skip Unattended Installation: Checked**.
2. **Hardware Allocation:** Set **Base Memory** to `4096 MB` (6144 MB recommended) and **Processors** to `2 vCPUs`. Leave EFI unchecked.
3. **Virtual Disk:** Create a `50.00 GB` Dynamically Allocated VDI.
4. **Network Binding:** Open **Settings > Network > Adapter 1** > Attached to: `NAT Network` > Name: `LabNet-DHCP` > Promiscuous: `Allow VMs`.
5. Start VM, install Ubuntu Server (create user: `analyst` / password: `P@ssw0rd2026!`), enable OpenSSH Server, and complete install.

18. NETPLAN STATIC IP CONFIGURATION

Log in to `WAZUH-SRV` as `analyst` and configure a fixed IP address via Netplan:

```
# Edit Netplan configuration file (ensure 2-space indentation, no tabs)
sudo nano /etc/netplan/50-cloud-init.yaml
```

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
        - 10.0.50.20/24
      routes:
        - to: default
          via: 10.0.50.1
      nameservers:
        addresses:
          - 10.0.50.10
          - 10.0.50.1
```

```
# Apply and verify static binding
sudo netplan apply
ip addr show enp0s3
ping -c 2 10.0.50.10
```

19. WAZUH SINGLE-NODE ALL-IN-ONE SIEM ENGINE INSTALLATION

```
# 1. Update repositories and install deployment utilities
sudo apt update && sudo apt install -y curl apt-transport-https lsb-release gnupg

# 2. Download and execute the official unattended all-in-one assistant
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
sudo bash ./wazuh-install.sh -a

# 3. Extract and display the generated administrative credentials
sudo tar -xvf wazuh-install-files.tar
cat wazuh-passwords.txt

# 4. Verify system services
sudo systemctl status wazuh-indexer wazuh-manager wazuh-dashboard --no-pager
```

Wazuh SIEM Web Console: `https://10.0.50.20` | **Username:** `admin` | **Password:** *(Extracted from wazuh-passwords.txt)*

20. WAZUH AGENT ENROLLMENT & WINDOWS TELEMETRY CHANNELS

Run on `WIN11-CLI` and `DC01` in PowerShell as Administrator:

```
Invoke-WebRequest `
  -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.0-1.msi `
  -OutFile ${env:TEMP}\wazuh-agent.msi

msiexec.exe /i ${env:TEMP}\wazuh-agent.msi /q `
  WAZUH_MANAGER='10.0.50.20' `
  WAZUH_REGISTRATION_SERVER='10.0.50.20' `
  WAZUH_AGENT_NAME=$env:COMPUTERNAME
```

Append inside `<ossec_config>` in `C:\Program Files (x86)\ossec-agent\ossec.conf` on both Windows nodes:

```
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
<localfile>
  <location>Microsoft-Windows-PowerShell/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
<localfile>
```

```
  <location>Security</location>
  <log_format>eventchannel</log_format>
</localfile>
```

```
Restart-Service -Name "Wazuh"
```

21. DEPLOYING UBUNTU DESKTOP (`UBUNTU-CLI`)

1. In VirtualBox, click **New** (`Ctrl + N`):
   - **Name:** `UBUNTU-CLI` | **Type:** `Linux` | **Version:** `Ubuntu (64-bit)`
   - **ISO Image:** Select `ubuntu-24.04-desktop-amd64.iso` | **Skip Unattended Installation: Checked**.
2. **Hardware Allocation:** Base Memory: `4096 MB` (4 GB), Processors: `2 vCPUs`. Dynamic Disk: `40.00 GB`.
3. **Network Binding:** Adapter 1 on `LabNet-DHCP` (Promiscuous: `Allow VMs`).
4. Install Ubuntu Desktop (Interactive > Default selection > Erase disk > User: `analyst` / Password: `P@ssw0rd2026!`).
5. Install Guest Additions and configure DNS client to query `DC01`:

```
sudo apt update && sudo apt install -y virtualbox-guest-utils virtualbox-guest-x11
sudo nmcli connection modify "Wired connection 1" ipv4.dns "10.0.50.10 10.0.50.1"
sudo nmcli connection up "Wired connection 1"
ping -c 2 lab.local
```

22. LINUX AUDIT DAEMON (`AUDITD`) & TELEMETRY ENGINEERING

Deploy the Linux Audit framework to track critical authentication files, sudo executions, and privileged commands:

```
# 1. Install auditd and plugins
sudo apt install -y auditd audispd-plugins
sudo systemctl enable --now auditd

# 2. Append high-signal detection rules to /etc/audit/rules.d/audit.rules
sudo tee -a /etc/audit/rules.d/audit.rules << 'EOF'
# Track identity file tampering
-w /etc/passwd -p wa -k identity_modification
-w /etc/shadow -p wa -k identity_modification
-w /etc/sudoers -p wa -k identity_modification

# Track elevated command execution
-a always,exit -F arch=b64 -S execve -F euid=0 -k elevated_execution
EOF

# 3. Reload audit rules
sudo augenrules --load
sudo auditctl -l
```

23. WAZUH AGENT ENROLLMENT ON LINUX WORKSTATION

```
# 1. Add Wazuh repository key and source
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | \
  sudo gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import
sudo chmod 644 /usr/share/keyrings/wazuh.gpg

echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | \
  sudo tee -a /etc/apt/sources.list.d/wazuh.list
sudo apt update

# 2. Install agent pointing to WAZUH-SRV
sudo WAZUH_MANAGER='10.0.50.20' WAZUH_AGENT_NAME='UBUNTU-CLI' apt install -y wazuh-agent
sudo systemctl enable --now wazuh-agent
```

24. KALI LINUX ATTACK APPLIANCE IMPORT (`KALI-NODE`)

1. Download the pre-built **Kali Linux VirtualBox (.7z)** image from `kali.org`.
2. Extract and import via VirtualBox **Machine > Add...** (`Ctrl + A`) and select the `.vbox` file.
3. Open **Settings > Network > Adapter 1**:
   - Attached to: `NAT Network` | Name: `LabNet-DHCP` | Promiscuous: `Allow VMs` (or `Allow All`).
4. Power on `KALI-NODE`, log in (`kali` / `kali`), update password via `passwd`, and verify network connectivity:

```
ip addr show eth0
ping -c 2 10.0.50.10
ping -c 2 10.0.50.20
```

25. CENTRALIZED SIEM AGENT VERIFICATION MATRIX

On `WAZUH-SRV`, run the manager control utility to verify all three lab nodes are actively communicating:

```
sudo /var/ossec/bin/agent_control -l
```

Expected Active Nodes: `ID: 001, Name: DC01` | `ID: 002, Name: WIN11-CLI` | `ID: 003, Name: UBUNTU-CLI`.

26. DNS MAIL RECORD MAPPING ON `DC01`

Active Directory DNS must map the Mail Transfer Agent (MTA) host and domain MX records. Run in elevated PowerShell on `DC01`:

```
# 1. Create Host (A) record for the mail server
Add-DnsServerResourceRecordA -Name "mail" -ZoneName "lab.local" -IPv4Address 10.0.50.10

# 2. Create Mail Exchanger (MX) record with Priority 10
Add-DnsServerResourceRecordMX -Name "." -ZoneName "lab.local" -MailExchange "mail.lab.local" -Preference 10

# 3. Verify DNS resolution
Resolve-DnsName -Name "lab.local" -Type MX
```

27. DEPLOYING & CONFIGURING HMAILSERVER ON `DC01`

1. Download and launch `hMailServer-5.x.x.exe` on `DC01`.
2. Database Selection: Select **Use built-in database engine (SQL Server Compact)** > set master password: `hMailAdmin2026!`.
3. Open **hMailServer Administrator** > click **Connect**:
   - Navigate to **Domains > Add domain...** > Domain: `lab.local` > click **Save**.
   - Under **Domains > lab.local > Accounts > Add...**:
     - Account 1: `jdoe` | Password: `CyberLab2026!` | Max size: `100 MB`.
     - Account 2: `analyst` | Password: `CyberLab2026!` | Max size: `100 MB`.
   - Navigate to **Settings > Advanced > IP Ranges > Internet**:
     - Verify range covers `0.0.0.0` - `255.255.255.255`.
     - Under **Allow connections**, ensure **SMTP (25)** and **IMAP (143)** are checked.
     - Under **Require SMTP authentication**, ensure *Local to local e-mail addresses* is checked.
4. Open firewall ports via elevated PowerShell on `DC01`:

```
New-NetFirewallRule -DisplayName "hMailServer SMTP (25)" `
  -Direction Inbound -LocalPort 25 -Protocol TCP -Action Allow

New-NetFirewallRule -DisplayName "hMailServer IMAP (143)" `
  -Direction Inbound -LocalPort 143 -Protocol TCP -Action Allow
```

28. CONFIGURING MOZILLA THUNDERBIRD ON `WIN11-CLI`

1. On `WIN11-CLI`, install Mozilla Thunderbird. On setup, enter: Name: `John Doe` | Email: `jdoe@lab.local` | Password: `CyberLab2026!`.
2. Click **Configure manually...** and apply parameters:
   - **Incoming (IMAP):** Server: `mail.lab.local` | Port: `143` | Security: `None` | Auth: `Normal password`.
   - **Outgoing (SMTP):** Server: `mail.lab.local` | Port: `25` | Security: `None` | Auth: `Normal password`.
3. Click **Done** and accept the self-signed certificate warning.

29. SIMULATING PHISHING ATTACKS VIA SWAKS (`KALI-NODE`)

```
# Execute from Kali terminal to inject a spoofed executive spear-phishing message
swaks --to jdoe@lab.local \
      --from "executive-notice@external-spoof.com" \
      --header "From: Evelyn Vance <evelyn.vance@lab.local>" \
      --header "Reply-To: evance.attacker@gmail.com" \
      --header "Subject: URGENT: Q4 Bonus Verification & Wire Routing" \
      --server 10.0.50.10 --port 25 \
      --body "John,\n\nPlease review attached wire details and verify immediately.\n\nBest,\nEvelyn Vance\nCOO"
```

30. RFC 5322 EMAIL HEADER FORENSIC TRIAGE GUIDE

On `WIN11-CLI`, open Thunderbird, open the incoming email, and press `Ctrl + U` to inspect raw headers:

Header Field	Forensic Significance	SOC Analyst Indicator / Discrepancy
`Received:`	Hop-by-hop transport trace generated by MTAs in reverse chronological order.	Bottom-most `Received:` line reveals true origin IP (`10.0.50.X`/Kali node).
`Return-Path:`	Envelope sender address specified during initial SMTP handshake.	Discrepancy between `Return-Path` and user-facing `From:` header indicates spoofing.
`Reply-To:`	Address where user responses are automatically routed.	Redirects sensitive replies to an external attacker inbox (`evance.attacker@gmail.com`).
`Message-ID:`	Unique message identifier assigned by transmitting MTA.	Identifies non-standard mail generation scripts (e.g., Swaks or Python SMTP tools).

31. HANDS-ON SOC ANALYST INVESTIGATION SCENARIOS

SCENARIO 1: ACTIVE DIRECTORY KERBEROASTING — **MITRE ATT&CK: T1558.003 | Target: DC01.lab.local**

Adversary Emulation (from Kali terminal):

```
impacket-GetUserSPNs lab.local/jdoe:CyberLab2026! -dc-ip 10.0.50.10 -request -outputfile kerberoast_hashes.txt
```

SIEM Triage (Wazuh Dashboard): Query `data.win.system.eventID: "4769"`. Verify Service Name: `svc_sql_prod`, Ticket Encryption: `0x17` (legacy RC4-HMAC), and correlate the requesting IP address to `KALI-NODE`.

SCENARIO 2: MALICIOUS PROCESS LINEAGE VIA ENCODED POWERSHELL — **MITRE ATT&CK: T1059.001 | Target: WIN11-CLI**

Adversary Emulation (on WIN11-CLI Command Prompt):

```
powershell.exe -NoP -NonI -W Hidden -EncodedCommand
VwByAGkAdABlAC0ASABvAHMAdAAgACIAUAByAG8AYwBlAHMAcwAgAEkAbgBqAGUAYwB0AGkAbwBuACAAUwBpAG0AdQBsAGEAdABpAG8AbgAiAA==
```

SIEM Triage (Wazuh Dashboard): Filter for `agent.name: "WIN11-CLI"`. Locate Sysmon **Event ID 1** (Process Creation) and PowerShell **Event ID 4104** (Script Block). Inspect parent lineage (`ParentImage`) and decode Base64 payload in CyberChef.

SCENARIO 3: HOST INTEGRITY & LINUX PRIVILEGE TAMPERING — **MITRE ATT&CK: T1548.003 | Target: UBUNTU-CLI**

Adversary Emulation (on UBUNTU-CLI Terminal):

```
sudo bash -c 'echo "backdoor_user ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers' && sudo cat /etc/shadow
```

SIEM Triage (Wazuh Dashboard): Filter for `rule.groups: "auditd"`. Confirm rule key `identity_modification` and system call `execve` (euid: 0) modifying target `/etc/sudoers`.

32. MASTER BLUE TEAM DETECTION & EVENT ID REFERENCE MATRIX

Telemetry Source	Event ID / Key	Event Description	Threat Detection & Analyst Value
Windows Security	`Event ID 4624`	Successful Account Logon	Session tracking; verify Logon Type 3 (Network) & 10 (Remote Desktop).
Windows Security	`Event ID 4625`	Failed Logon Attempt	Brute-force and password spraying detection; correlates attacking IP.
Windows Security	`Event ID 4720`	User Account Created	Unauthorized persistence; detects rogue local/domain user creations.
Windows Security	`Event ID 4768`	Kerberos Authentication (TGT)	AS-REP roasting detection; identify pre-authentication disabled accounts.
Windows Security	`Event ID 4769`	Kerberos Ticket Request (TGS)	Kerberoasting detection; look for legacy encryption type `0x17` (RC4).
Microsoft Sysmon	`Event ID 1`	Process Creation	Full command-line arguments, parent process PID, hashes, and process tree.
Microsoft Sysmon	`Event ID 3`	Network Connection	C2 beacons, outbound reverse shells, and unauthorized internal port scans.
Microsoft Sysmon	`Event ID 7`	Image Loaded (DLL)	Detects DLL search order hijacking, side-loading, and reflective injection.
Microsoft Sysmon	`Event ID 10`	Process Access (LSASS)	Credential dumping detection (e.g., Mimikatz, ProcDump access masks).
PowerShell Operational	`Event ID 4104`	Script Block Execution	Captures complete de-obfuscated script code and dynamic payloads.
Linux Auditd	`identity_modification`	File Integrity Tampering	Monitors attribute changes and writes to `/etc/passwd` and `/etc/sudoers`.

33. VIRTUALBOX SNAPSHOT STRATEGY ("GOLDEN BASELINES")

To avoid rebuilding your virtual environment when testing destructive malware, credential attacks, or persistence mechanisms, implement a structured VirtualBox snapshot schedule across all lab nodes:

Snapshot Identifier	Execution Timing	Recovery Objective
`SNAP-01-CleanOS`	Immediately after OS install and Guest Additions.	Clean fallback if domain joins or network packages corrupt.
`SNAP-02-BaselineReady`	Post Active Directory promotion, Sysmon deployment, Wazuh Agent enrollment, and GPO linking.	**Master Golden Image:** Revert to this state after executing attack scenarios to clear artifacts.
`SNAP-03-PostScenario`	Immediately following an attack run (before cleanup).	Preserves forensic disk states for offline triage and report writing.

34. 16 GB HOST RAM & STAGGERED BOOT OPTIMIZATION

Running 5 virtual machines concurrently on a standard 16 GB host machine requires active resource orchestration. Follow these operational rules to prevent host memory exhaustion:

Staggered Boot Sequence

1. **Step 1:** Start `DC01` and `WAZUH-SRV` first. Allow 3–4 minutes for Active Directory and Elasticsearch indices to stabilize.
2. **Step 2:** Start your target endpoint (`WIN11-CLI` or `UBUNTU-CLI`).
3. **Step 3:** Start `KALI-NODE` only when actively staging an attack.

VirtualBox Headless Mode Execution

Run background servers (`DC01` and `WAZUH-SRV`) without a graphical window to save 500 MB+ of host RAM per machine:

*Hold `Shift` and click **Start** in VirtualBox* (or select **Headless Start**). Manage servers via web dashboard, SSH, or RDP.

35. TOP 3 LAB TRIP-UPS & TROUBLESHOOTING CARD

Symptom / Error	Root Cause	Engineering Fix / CLI Command
Kerberos Authentication & Ticket Failures	VM clock drift exceeds the 5-minute Kerberos maximum skew tolerance.	Resync the Windows endpoint clock with the Domain Controller: `w32tm /resync /force`
Windows Endpoint Loses Domain Resolution	DHCP lease renewal overwrote the custom DNS address back to default gateway.	Re-apply static DNS pointing to `DC01`: `Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses ("10.0.50.10", "10.0.50.1")`
Wazuh Agent Reports "Never Connected"	Ubuntu UFW firewall blocking registration or agent traffic ports.	On `WAZUH-SRV`, permit agent ports: `sudo ufw allow 1514/tcp && sudo ufw allow 1515/tcp` Test from endpoint: `Test-NetConnection 10.0.50.20 -Port 1514`

36. 60-SECOND PRE-FLIGHT RANGE VERIFICATION ("GREEN BOARD" TEST)

Before executing attack scenarios, run this rapid verification routine across your virtual hosts to confirm all telemetry and identity pipelines are actively operational:

1. Active Directory & DNS Check (`DC01`)

```
Resolve-DnsName -Name "lab.local"
Resolve-DnsName -Name "mail.lab.local"
Get-Service -Name "NTDS", "DNS", "hMailServer"
```

2. Centralized SIEM Ingestion (`WAZUH-SRV`)

```
sudo /var/ossec/bin/agent_control -l
# Confirm all 3 agents (DC01, WIN11-CLI, UBUNTU-CLI) display status "Active"
```

3. Endpoint Telemetry Sensors (`WIN11-CLI`)

```
Get-Service -Name "Sysmon64", "Wazuh"
Test-NetConnection -ComputerName 10.0.50.20 -Port 1514
```

4. Adversary Route Verification (`KALI-NODE`)

```
ping -c 2 10.0.50.10
ping -c 2 10.0.50.20
nc -zv 10.0.50.10 25 88 389
```

37. ESSENTIAL PORTABLE ANALYST TOOLKIT (`C:\TOOLS`)

Pre-stage these zero-install, lightweight forensic utilities on `WIN11-CLI` to streamline incident analysis and malware triage without requiring active internet connectivity during simulations:

Utility	Recommended Version / Path	Analyst Forensic Purpose
CyberChef (Offline Build)	Standalone `cyberchef.html`	Offline decoding of Base64, XOR, URL-encoded scripts, and timestamp conversions.
Sysinternals Process Explorer	`C:\Tools\Sysinternals\procexp64.exe`	Advanced process hierarchy mapping, DLL inspection, and verification of running image signatures.
Sysinternals Autoruns	`C:\Tools\Sysinternals\Autoruns64.exe`	Comprehensive inspection of persistence hooks: Registry Run keys, Scheduled Tasks, and Services.
Sysinternals TCPView	`C:\Tools\Sysinternals\Tcpview64.exe`	Real-time visualization of endpoint network sockets and active process-to-IP bindings.
KAPE / EZ-Tools (Eric Zimmerman)	`C:\Tools\EZTools\`	Targeted forensic artifact triage: Prefetch (`PECmd`), Shimcache, and $MFT parser (`MFTECmd`).

38. STANDARD SOC INCIDENT TRIAGE NOTE TEMPLATE

Use this structured 5-field Markdown template to document your lab investigations, creating professional artifacts suitable for technical portfolio submissions and GitHub repositories:

```
# SOC INCIDENT TRIAGE REPORT | CASE ID: INC-2026-XXXX
**Incident Classification:** [e.g., Credential Access / Kerberoasting]
**MITRE ATT&CK Technique:** [e.g., T1558.003 - Steal or Forge Kerberos Tickets]
**Severity Level:** [ ] Low  [ ] Medium  [X] High  [ ] Critical
**Affected Asset(s):** DC01.lab.local (10.0.50.10) | Target Account: svc_sql_prod

---
### 1. Executive Detection Summary
Brief synopsis describing initial alert detection, correlated SIEM rules, and potential operational impact.

### 2. Chronological Timeline of Adversary Activity
* **YYYY-MM-DD HH:MM:SS UTC** - Initial authentication / Kerberos TGT requested for source user `jdoe`.
* **YYYY-MM-DD HH:MM:SS UTC** - Sysmon Event ID 1 captures anomalous execution of CLI utility.
* **YYYY-MM-DD HH:MM:SS UTC** - Security Event ID 4769 logged with legacy encryption `0x17` targeting `svc_sql_prod`.

### 3. Forensic Artifacts & Indicators of Compromise (IOCs)
* **Source IP / Hostname:** `10.0.50.X` (`KALI-NODE`)
* **Observed Hashes (SHA256):** `[Executable / Script Block Hash]`
* **Command Line Strings:** `powershell.exe -NoP -NonI -W Hidden -EncodedCommand ...`

### 4. Root Cause Analysis
Identification of exploited misconfigurations (e.g., weak service account passwords, legacy RC4 support, un-audited SPNs).

### 5. Containment, Remediation & Detection Engineering Recommendations
* **Short-Term Actions:** Revoke compromised Kerberos tickets, disable target account, and isolate endpoint.
* **Long-Term Hardening:** Enforce AES256 encryption on SPNs, implement 25+ character managed service accounts (gMSAs).
```

39. SECURITY ANALYST CAREER ACCELERATOR & RESUME BULLETS

Verifiable Resume Bullet Points for SOC / Blue Team Applications:

- *"Architected an isolated, 5-node detection and response lab inside VirtualBox, provisioning Windows Server 2022 AD DS, PKI, and centralized Wazuh SIEM telemetry."*
- *"Engineered high-signal endpoint detection pipelines deploying Sysmon v15 and Linux Auditd, enforcing domain-wide GPOs to log Kerberos TGS requests (Event ID 4769) and CLI executions."*
- *"Emulated real-world adversary techniques (Kerberoasting, encoded PowerShell, and spear-phishing), correlating telemetry in Wazuh and performing RFC 5322 MIME header forensics."*

40. OFFICIAL SOFTWARE DOWNLOADS & MASTER ENDPOINT MATRIX

Lab Component / Tool	Official Resource & Download Endpoint
Oracle VM VirtualBox & Extension Pack	`https://www.virtualbox.org/wiki/Downloads`
Microsoft Evaluation Center (Server 2022 & Win 11)	`https://www.microsoft.com/evalcenter`
Microsoft Sysinternals Sysmon & Suite	`https://download.sysinternals.com/files/Sysmon.zip`
SwiftOnSecurity Sysmon High-Signal Config	`https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-config/master/sysmonconfig-export.xml`
Ubuntu Linux (Server & Desktop 24.04 LTS)	`https://ubuntu.com/download`
Kali Linux Pre-Built VirtualBox Appliance	`https://www.kali.org/get-kali/#kali-virtual-machines`
Wazuh Open Source SIEM Platform	`https://documentation.wazuh.com`
hMailServer Email Server Solution	`https://www.hmailserver.com/download`
Mozilla Thunderbird Email Client	`https://www.thunderbird.net`
CyberChef (Offline Web App)	`https://github.com/gchq/CyberChef/releases`
Impacket Threat Emulation Framework	`https://github.com/fortra/impacket`
PORT::ZERO Educational Media (YouTube)	`https://www.youtube.com/@PORTZERO-Rick-Kelly`

41. ATTRIBUTION & COMMUNITY LICENSE NOTICE

Open Educational Resource (OER) Declaration:

This publication, *The Zero-Dollar Virtual Cybersecurity Home Lab Master Field Manual*, was created by **PORT::ZERO Cyber Solutions** in partnership with **The Ginger Hacker Initiative Conference (GHI-CON)**.

This document is provided freely to the cybersecurity community to support aspiring analysts, career changers, students, and veterans in developing practical, verifiable blue-team and detection engineering capabilities. You are free to share, adapt, and distribute this material for personal, educational, and institutional non-commercial training with appropriate attribution.

© 2026 PORT::ZERO Cyber Solutions LLC. All rights reserved. Registered trademarks belong to their respective holders.

PORT::ZERO
CYBER SOLUTIONS
Protect Against Cyber Threats ®