Day 1 Documentation

Objective

Complete Day 1 by finalizing the lab setup on **VirtualBox with Windows 10** and **Splunk Enterprise**, verify Windows Security logging, and capture evidence screenshots. No theory memorization—focus on environment readiness and proof.

Environment Details

- **Host OS:** Windows
- **Virtualization:** VirtualBox
- **Guest OS:** Windows 10
- **SIEM:** Splunk Enterprise (local install on Windows 10)
- **Purpose:** SOC / Blue Team fundamentals, Windows log analysis

---

Key Definitions

Log

A **log** is a time-stamped record of events generated by systems, applications, or security devices. Logs are used for monitoring, troubleshooting, and incident investigation.

Event

An **event** is a specific action or occurrence (e.g., login attempt, file access) recorded inside a log.

SIEM

A **SIEM (Security Information and Event Management)** system collects, normalizes, correlates, and analyzes logs from multiple sources to detect threats.

Splunk

Splunk is a data platform widely used as a SIEM to ingest, search, analyze, and visualize machine-generated data (logs).

OVA

An **OVA (Open Virtual Appliance)** is a packaged virtual machine format used to import preconfigured systems into VMware or VirtualBox.

Tasks Completed

1. Installed Windows 10 VM on VirtualBox.
2. Installed **Splunk Enterprise** on Windows 10.
3. Accessed Splunk Web at http://localhost:8000.
4. Opened **Event Viewer → Windows Logs → Security**.
5. Filtered and inspected authentication events.

Commands / Actions Used

- VirtualBox: Devices → Insert Guest Additions CD Image
- Windows: Ran VBoxWindowsAdditions.exe → Reboot
- Splunk Web: Login via browser at http://localhost:8000
- Event Viewer: Filter Current Log → Security

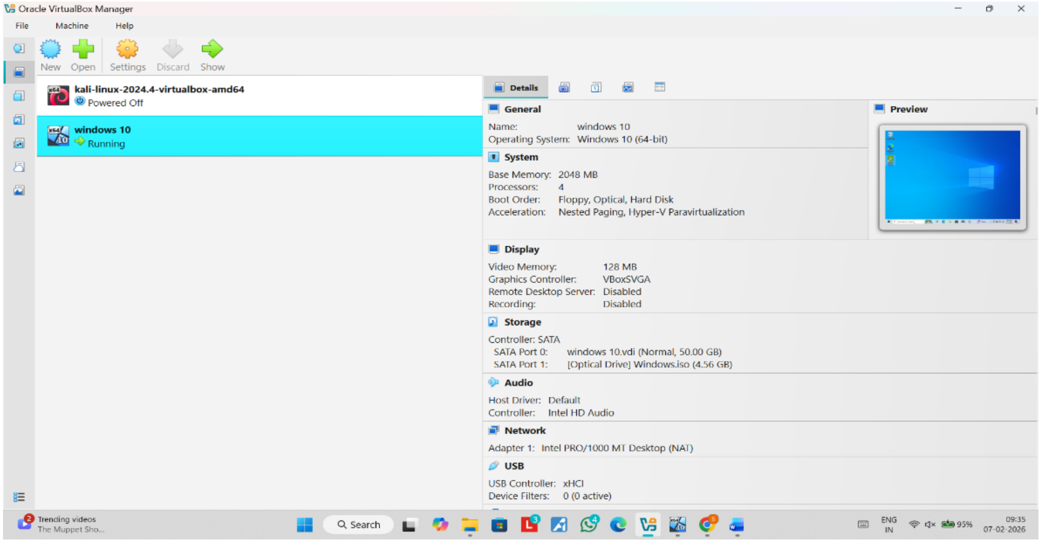
Observations

- System booted successfully.
- Initial access to terminal/UI confirmed.
- Log directory identified for further analysis.

Screenshots (Evidence)

1. VirtualBox Manager – VM Running

- Shows Windows 10 VM powered on.
- Filename: day1_vbox_vm_running.png



kali-linux-2024.4-virtualbox-amd64
Powered Off

windows 10
Running

General

```
Name:              windows 10
Operating System:  Windows 10 (64-bit)
```

System

```
Base Memory:   2048 MB
Processors:    4
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  Nested Paging, Hyper-V Paravirtualization
```

Display

```
Video Memory:           128 MB
Graphics Controller:    VBoxSVGA
Remote Desktop Server:  Disabled
Recording:              Disabled
```

Storage

```
Controller: SATA
 SATA Port 0:     windows 10.vdi (Normal, 50.00 GB)
 SATA Port 1:     [Optical Drive] Windows.iso (4.56 GB)
```

Audio

```
Host Driver:  Default
Controller:   Intel HD Audio
```

Network

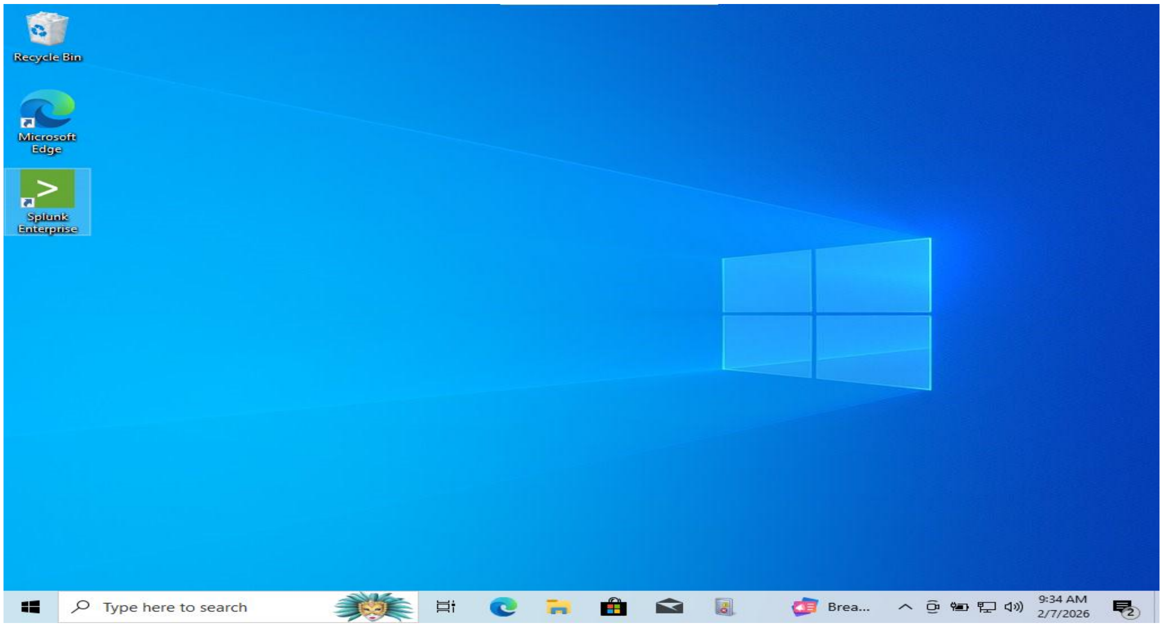
```
Adapter 1:  Intel PRO/1000 MT Desktop (NAT)
```

USB

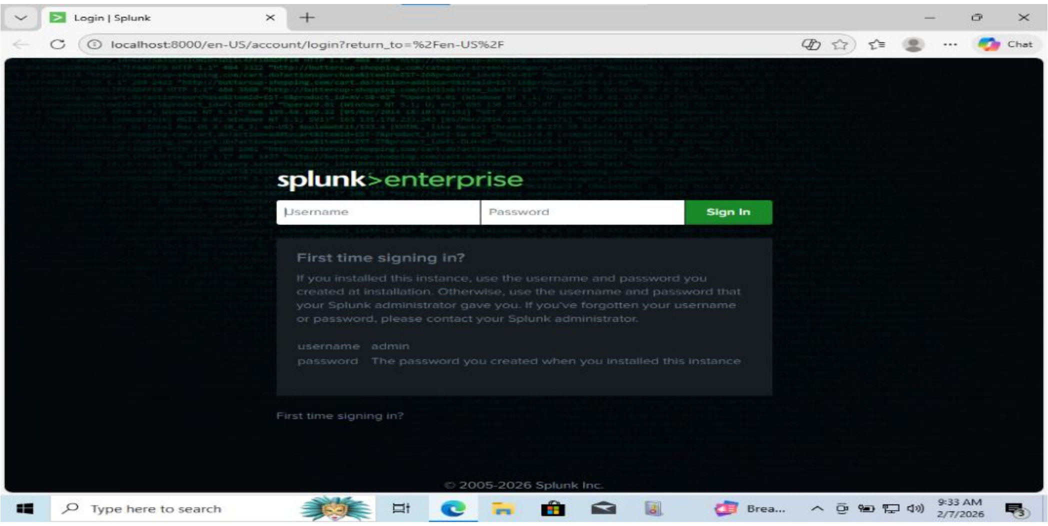
```
USB Controller:  xHCI
Device Filters:  0 (0 active)
```

2. Windows 10 Desktop

- Confirms successful login and usable desktop.
- Filename: day1_windows_desktop.png



3. **Splunk Web Dashboard**
    - Browser at http://localhost:8000 logged in.
    - Filename: day1_splunk_dashboard.png



First time signing in?

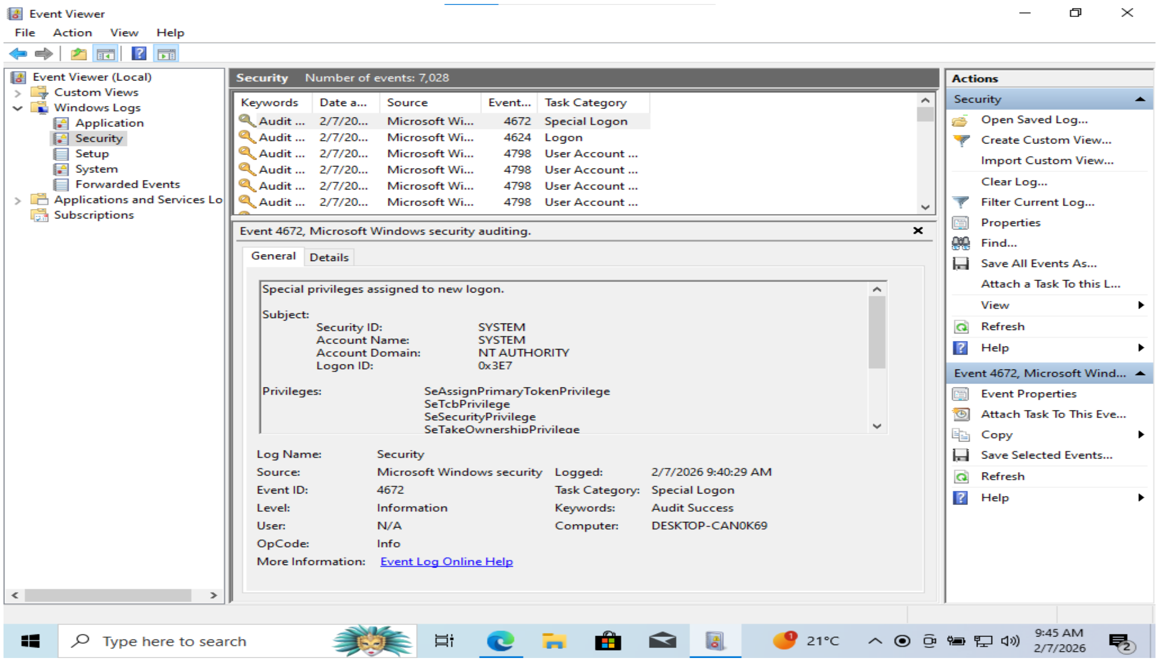
If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password The password you created when you installed this instance

First time signing in?

© 2005-2026 Splunk Inc.

4. **Event Viewer – Security Log**
    - Path visible: Windows Logs → Security.
    - Filename: day1_eventviewer_security.png



Security Number of events: 7,028

Keywords	Date a...	Source	Event...	Task Category
Audit ...	2/7/20...	Microsoft Wi...	4672	Special Logon
Audit ...	2/7/20...	Microsoft Wi...	4624	Logon
Audit ...	2/7/20...	Microsoft Wi...	4798	User Account ...
Audit ...	2/7/20...	Microsoft Wi...	4798	User Account ...
Audit ...	2/7/20...	Microsoft Wi...	4798	User Account ...
Audit ...	2/7/20...	Microsoft Wi...	4798	User Account ...

Event 4672, Microsoft Windows security auditing.

General Details

```
Special privileges assigned to new logon.

Subject:
        Security ID:            SYSTEM
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3E7

Privileges:             SeAssignPrimaryTokenPrivilege
                        SeTcbPrivilege
                        SeSecurityPrivilege
                        SeTakeOwnershipPrivilege
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/7/2026 9:40:29 AM
Event ID:	4672	Task Category:	Special Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-CAN0K69
OpCode:	Info		
More Information:	Event Log Online Help		

Learning Outcome (Be Specific)

- Verified a working **Windows + Splunk** SOC lab.
- Confirmed access to **Windows Security logs**.
- Established a habit of **evidence-first documentation**.

Next Day Plan

- Deep-dive one Windows authentication event.
- Translate coded fields to meaning.
- Ingest Windows logs into Splunk and validate searches.