SIEM LOG MONITORING AND THREAT DETECTION

Installation of sysmon

1) Download Sysmon

1. Download the latest Sysmon release from Microsoft Sysinternals (choose Sysmon.exe for 32-bit or Sysmon64.exe for 64-bit). Microsoft Learn
2. Extract the ZIP to a folder, e.g. C:\Sysmon.

---

2) Choose a configuration file (don't use the default empty config)

- Sysmon works best with a tuned XML config that tells it what to log and what to ignore. Community-maintained configs such as SwiftOnSecurity's sysmon-config are a great starting point — they're well-commented and widely used. Download sysmonconfig-export.xml from that repo and put it next to the Sysmon binary. GitHub+1

Why use a config:

- Sysmon by default may log too little or too much. The config allows you to record useful events (process creation, network connects, filetime changes, driver loads, etc.) and filter noisy benign events (trusted system processes, installers, etc.).

---

3) Install Sysmon (exact commands)

Open an elevated CMD (Run as Administrator) and run the installer with the config:

cd C:\Sysmon

.\Sysmon64.exe -accepteula -i sysmonconfig-export.xml

- -accepteula accepts the license so the install doesn't prompt.
- -i <file> installs Sysmon and imports the XML config at install time. Microsoft Learn

If you need a silent install or to deploy at scale, you can call the same command from a remote-management tool (SCCM, PDQ, etc.) or use an MSI wrapper.

---

4) Verify installation & check the current config

- Check the service is installed and running: open Services → Sysmon should be present.
- Check Sysmon channel in Event Viewer: Applications and Services Logs → Microsoft → Windows → Sysmon → Operational — you should start to see events. Microsoft Learn

You can also confirm from the command-line:

.\Sysmon64.exe -c

(That prints current configuration/status — use the binary's help .\Sysmon64.exe -? if needed.)

---

5) Example minimal config snippet (small, safe to paste)

Below is a tiny example that logs Process Create and Network Connect events while excluding a couple of noisy system processes. Save it as my-sysmon.xml if you want to test a minimal setup:

```
<Sysmon schemaversion="4.50">
  <EventFiltering>
    <!-- Log process creation (Event ID 1) -->
    <ProcessCreate onmatch="include">
      <CommandLine condition="contains">powershell</CommandLine>
    </ProcessCreate>
    <!-- Log network connections (Event ID 3) -->
    <NetworkConnect onmatch="include" />

    <!-- Exclude common noisy processes -->
    <ProcessCreate onmatch="exclude">
      <Image condition="is">C:\Windows\System32\svchost.exe</Image>
    </ProcessCreate>
  </EventFiltering>
</Sysmon>
```

Note: real production configs are larger and more nuanced (many includes/excludes). Use the SwiftOnSecurity or sysmon-modular templates and then tune for your environment. GitHub+1

---

6) Update / change configuration without reinstalling

- To update the config while Sysmon is installed, run:

.\Sysmon64.exe -c new-config.xml

This pushes a new configuration to the running Sysmon service (no uninstall/reinstall needed). Microsoft Learn

- To uninstall Sysmon:

.\Sysmon64.exe -u

7) What Sysmon logs (useful Event IDs)

Common Sysmon event types you'll use for detections and Splunk correlation:

- Event ID 1 — Process Create (very important)
- Event ID 3 — Network Connection
- Event ID 5 — Process Terminate
- Event ID 11 — FileCreate (new)
- Event ID 12 — Registry object added/modified
- Event ID 7 — Image loaded (DLLs / drivers)
  (Use these in Splunk searches/alerts.) Microsoft Learn

---

8) Forwarding Sysmon to Splunk (quick)

Using Splunk Universal Forwarder on the Windows host, enable the Sysmon channel in inputs.conf:

[WinEventLog://Microsoft-Windows-Sysmon/Operational]

disabled = 0

index = sysmon

Restart the forwarder. Then in Splunk Search you can query:

index=sysmon sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"

(If you use Winlogbeat or Windows Event Forwarding, they'll also read the Microsoft-Windows-Sysmon/Operational channel.) Elastic+1

---

9) Tuning tips (reduce noise, increase signal)

- Start with a community config (SwiftOnSecurity or sysmon-modular) and tune: exclude installers, antivirus, and known benign services. GitHub+1
- Focus on logging:
  - Process command lines (CommandLine) — critical for PowerShell/script detection
  - Network connections for processes (Event 3) — spotlight unusual outbound connections
  - File creation time changes and image loads for persistence/malware activity
- Test changes on a single host first to evaluate event volume.

---

10) Common pitfalls & troubleshooting

- No events seen: confirm forwarder reads Microsoft-Windows-Sysmon/Operational. Sysmon must be installed as admin and the Event Log channel must be enabled. Microsoft Learn
- Too many events: your config is too permissive — add excludes for known-good processes/paths. GitHub
- Endpoint crashes / driver conflicts: older Sysmon versions or driver conflicts with AV can cause issues — check vendor knowledge bases for known interactions (some products require exclusions). If you see unresponsiveness, remove or tune the config (CISA and vendor KBs document steps). Support Portal+1

---

11) Helpful resources (read next / reference)

- Official Sysmon download and docs (Microsoft Sysinternals). Microsoft Learn
- SwiftOnSecurity sysmon-config (good starting config). GitHub
- sysmon-modular (alternative modular config). GitHub

Pull Sysmon logs to Splunk

Quick workflow summary

1. Ensure Sysmon is installed and logging to Microsoft-Windows-Sysmon/Operational.
2. Install Splunk Universal Forwarder on the Windows host (or use Winlogbeat).
3. Configure the UF to forward the Sysmon event channel to your Splunk indexer (outputs.conf).
4. Create an index on the Splunk indexer (e.g., sysmon).
5. Verify ingestion in Splunk and run searches / create alerts.

A. On the Splunk Indexer (receiver)

1. **Enable receiving on port 9997**
    - Splunk Web: Settings → Forwarding and receiving → Configure receiving → New → Port 9997 → Save
    - Or on indexer server CLI:
    - $SPLUNK_HOME/bin/splunk enable listen 9997 -auth admin:changeme
2. **Create an index for Windows logs (if you want a dedicated index)**
    - Splunk Web: Settings → Indexes → New Index
        - Index name: sysmon
    - Or edit/create $SPLUNK_HOME/etc/system/local/indexes.conf:
    - [sysmon]

- homePath = $SPLUNK_DB/sysmon/db
- thawedPath = $SPLUNK_DB/sysmon/thaweddb
- coldPath = $SPLUNK_DB/sysmon/colddb
- Restart Splunk if you changed conf files:
- $SPLUNK_HOME/bin/splunk restart

B. On the Windows host with Sysmon — Install Splunk Universal Forwarder

1. **Download & install UF**
   - Use the Splunk Universal Forwarder MSI for Windows and run installer as Administrator.
   - During install you can skip specifying indexer; we'll set outputs.conf manually.
2. **Stop UF while editing config**
3. net stop splunkforwarder

C. Configure UF to read the Sysmon event channel

Place these files under the UF app local directory, e.g.:
C:\Program Files\SplunkUniversalForwarder\etc\apps\local_sysmon_app\local\

Create the app folder if needed:

mkdir "C:\Program Files\SplunkUniversalForwarder\etc\apps\local_sysmon_app\local"

1) inputs.conf

inputs.conf — tells UF to monitor the Sysmon event channel and optionally Security (4625) etc.

[WinEventLog://Microsoft-Windows-Sysmon/Operational]

disabled = 0

index = sysmon

sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

[WinEventLog://Security]

disabled = 0

index = sysmon

sourcetype = WinEventLog:Security

Notes:

- sourcetype for Sysmon channel is usually XmlWinEventLog:Microsoft-Windows-Sysmon/Operational. That preserves XML fields.
- Add other channels (Application, System) as needed.

2) outputs.conf

Point the UF to your indexer (replace INDEXER_IP with the indexer hostname/IP):
C:\Program Files\SplunkUniversalForwarder\etc\system\local\outputs.conf

[tcpout]

defaultGroup = indexerGroup

[tcpout:indexerGroup]

server = INDEXER_IP:9997

[tcpout-server://INDEXER_IP:9997]

3) props.conf (optional — set sourcetype and additional parsing)

If you want to ensure parsing the Sysmon XML correctly or rename sourcetype, add:
C:\Program Files\SplunkUniversalForwarder\etc\apps\local_sysmon_app\local\props.conf

[XmlWinEventLog:Microsoft-Windows-Sysmon/Operational]

NO_BINARY_CHECK = true

SHOULD_LINEMERGE = false

DATETIME_CONFIG = CURRENT

D. Restart the Universal Forwarder

net start splunkforwarder

or

& 'C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe' restart

---

E. Verify logs are arriving in Splunk

Basic validation searches (on indexer Splunk Web → Search & Reporting)

1. Recent Sysmon events:

index=sysmon sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" | head 20

2. Count by event id:

index=sysmon sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"

| stats count by EventCode

| sort -count

3. Find PowerShell commandlines from process create (Event ID 1):

index=sysmon sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1

| where like(CommandLine, "%powershell%") OR like(CommandLine, "%IEX%") OR like(CommandLine, "%DownloadString%")

| table _time, ComputerName, User, Image, CommandLine

| sort -_time

If you see events, ingestion is working.

F. Useful Splunk field extraction tips

- Sysmon XML events include nested tags. Splunk typically extracts EventCode, ComputerName, User, Image, CommandLine, DestinationIp, DestinationPort etc. If fields are missing, use spath to extract:

index=sysmon sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"

| spath input=EventXml output=ProcessCommand path=Event.EventData.Data{?Name=="CommandLine"}

| table _time ComputerName EventCode ProcessCommand

G. Common issues & troubleshooting

1. **No events arriving**
    - Verify Sysmon is producing events in Event Viewer: Applications and Services Logs → Microsoft → Windows → Sysmon → Operational.
    - Check UF is running: sc query splunkforwarder
    - UF logs: C:\Program Files\SplunkUniversalForwarder\var\log\splunk\splunkd.log
    - Check firewall between UF and indexer (port 9997 open).
2. **UF cannot reach indexer**
    - Test connectivity from Windows host:
    - Test-NetConnection -ComputerName INDEXER_IP -Port 9997
    - If connection fails, open port on indexer firewall or use correct network routing.

3. **Events are present but fields missing**
    - Use spath to inspect XML structure.
    - Ensure sourcetype is set correctly and props.conf is not overriding XML parsing.
4. **Large event volume (too noisy)**
    - Tune Sysmon config to add exclusions for benign processes or specific paths.
    - Use transforms/props to drop or index only needed fields.
5. **Time drift**
    - Make sure both host and indexer use NTP / correct time zone.

H. Example end-to-end checklist (copy/paste)

- Sysmon installed and Microsoft-Windows-Sysmon/Operational shows events.
- Splunk index sysmon created on indexer.
- Splunk indexer listening on port 9997.
- Universal Forwarder installed on Windows host.
- inputs.conf contains WinEventLog://Microsoft-Windows-Sysmon/Operational and index=sysmon.
- outputs.conf points to INDEXER_IP:9997.
- UF restarted and splunkd.log shows connection to indexer.
- Splunk search shows recent Sysmon events.

Installation of VM Ware

Overview

You will:

1. Download **Kali Linux ISO** or ready-made VMware image
2. Create a **new virtual machine** in VMware Workstation Pro
3. Install Kali Linux
4. Configure **VMware Tools & networking**

Step 1: Download Kali Linux

two options

Option 1: Ready-made VMware Image (Easiest)

Highly recommended for beginners — no manual installation needed.

1. Go to the official site:
   https://www.kali.org/get-kali/#kali-virtual-machines
2. Under **"Kali Virtual Machines"**, choose:
   - **VMware (64-bit)** → download .7z file
3. Extract it using **7-Zip** or **WinRAR** → You'll get .vmx and .vmdk files.

That's it! You can skip directly to **Step 4** to import it.

Option 2: Install from ISO (Manual Installation)

If you prefer to learn installation:

1. Go to:
   https://www.kali.org/get-kali/#kali-installer-images
2. Download:
   - **Kali Linux 64-bit Installer ISO**
3. Save it to your system (e.g., Downloads\kali-linux-2025.2-installer-amd64.iso)

Step 2: Open VMware Workstation Pro

1. Launch **VMware Workstation Pro**
2. Click **Create a New Virtual Machine**
3. Choose **Typical (recommended) → Next**

Step 3: Load the ISO File

1. Choose **Installer disc image file (ISO)**
2. Browse → select your Kali Linux ISO
3. Click **Next**

Step 4: Configure VM Settings

1. **Guest OS** → choose:
    - Operating System: **Linux**
    - Version: **Debian 12.x 64-bit** (Kali is based on Debian)
2. **Name your VM:**
   Example: Kali-Linux-SOC-Lab
3. **Location:**
   Choose a folder where you want the VM stored (e.g., D:\VMs\Kali)

Step 5: Allocate Resources

- **Processors:** 2 (minimum), 4 if available
- **Memory (RAM):** 4 GB minimum, 8 GB recommended
- **Hard Disk:** 50 GB minimum
- **Network:** NAT (to access the internet through host)

Then click **Finish**.

Step 6: Start Kali Linux Installation

Once VM boots up with ISO loaded:

1. On the boot menu → choose **Graphical Install**
2. Follow the prompts:
    - **Language:** English
    - **Location:** India (or your region)
    - **Keyboard:** American English
    - **Hostname:** kali
    - **Username:** create your user (example: student)

- **Password:** choose a strong one
- **Partition Disks:** Use entire disk → All files in one partition
- **Finish and install GRUB bootloader** → Yes

Wait until the installation finishes (~10–15 mins).
When done → system reboots into Kali.

Step 7: Install VMware Tools (to enable full-screen, drag-drop)

1. In VMware top menu:
   - Click **VM → Install VMware Tools**
2. In Kali:
3. sudo apt update
4. sudo apt install open-vm-tools-desktop -y
5. reboot
6. After reboot → You'll have:
   - Auto screen resize
   - Shared clipboard (copy-paste)
   - Better mouse control

Step 8: Configure Networking

1. Go to VMware top bar → **VM → Settings → Network Adapter**
   - Choose **NAT** (recommended)
   - If doing multi-VM labs, create a **Host-only network** for isolation
2. In Kali, verify internet:
3. ping -c 4 google.com

If it replies → network is good

Step 9: Update Kali and Install Useful Tools

After boot:

sudo apt update && sudo apt full-upgrade -y

Install common tools:

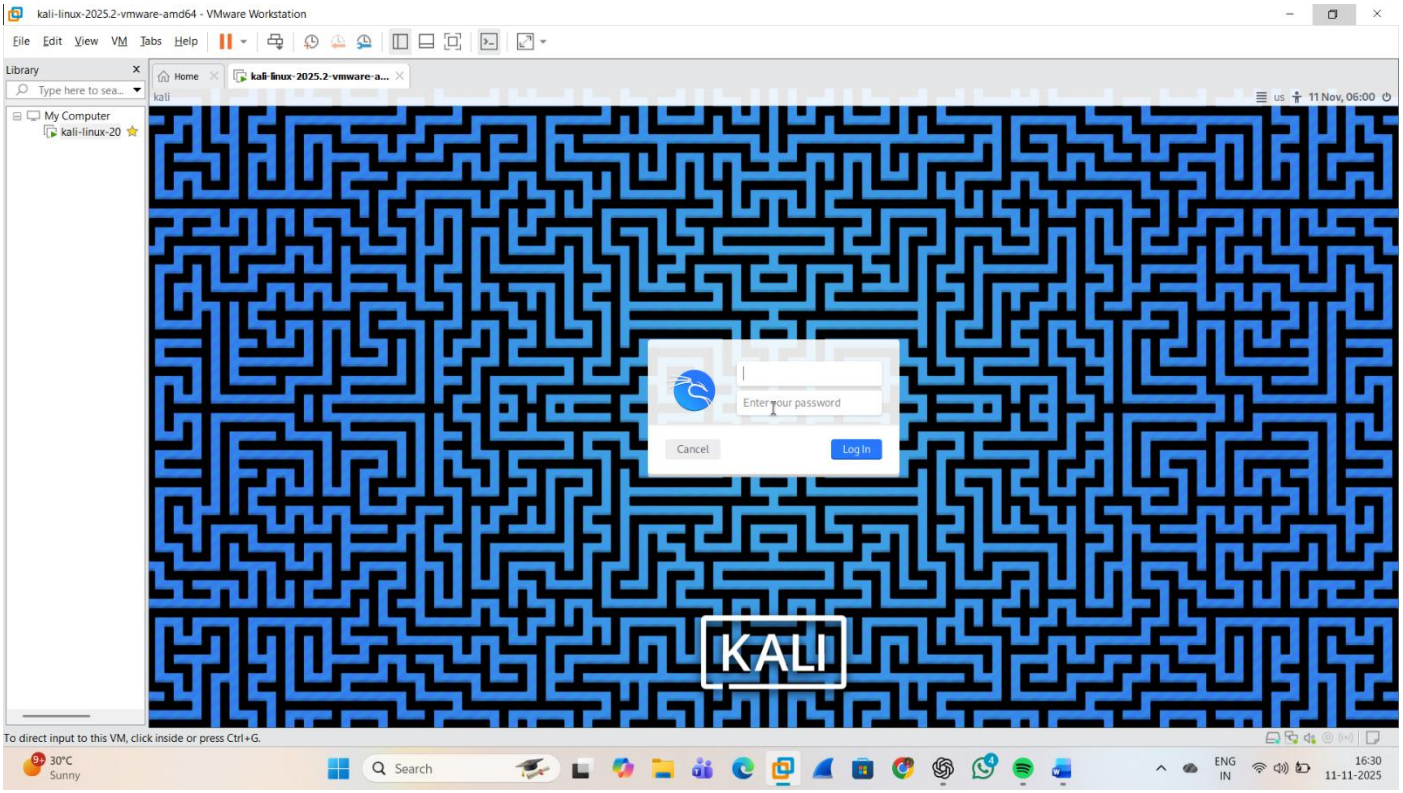
sudo apt install net-tools htop curl wget git -y

You can also install **Splunk Forwarder, Wireshark, nmap, etc.** later.

Step 10: (Optional) Take Snapshot

Before experimenting with attacks or malware simulations:

- Go to **VM → Snapshot → Take Snapshot**
    - Name: “Clean Install”
- This helps you restore to a clean state later.



Brute- Force Attack

A **brute-force attack** is a trial-and-error method attackers use to gain access to accounts, systems, or encrypted data by systematically trying many possible credentials, keys, or values until the correct one is found. It relies on computing power and persistence rather than exploiting a software flaw.

Common forms

- **Online password brute-force:** repeatedly attempt username/password combinations against a login interface (SSH, RDP, web login, API).
- **Offline brute-force:** attacker has a hashed password file and tries many passwords locally (faster because no network or lockouts).
- **Credential stuffing:** using large sets of leaked username/password pairs against other services (relies on reused passwords).
- **Password spraying:** try a small set of common passwords across many accounts to avoid lockouts and detection.

How attackers use it (examples)

- Trying admin/admin, admin/password1, admin@123 on an SSH service.
- Submitting thousands of password guesses to a web login page.
- Running a GPU-accelerated cracker like Hashcat against stolen password hashes.

Indicators of compromise (what to look for in logs)

- Multiple failed login attempts from a single IP within a short time window.
- Many failed attempts across many accounts from a single IP (spraying/credential stuffing).
- Rapid succession of authentication failures followed by a successful login.
- Account lockouts or password reset spikes.
- Suspicious source IPs (odd countries, proxies, TOR exit nodes) or unusual user agents.
- Authentication attempts at odd hours for the account.

Quick Splunk detection examples

(assume Sysmon/Windows Security logs forwarded into index=sysmon)

1) Many failed logins from one IP (Windows Security Event ID 4625):

index=sysmon sourcetype="WinEventLog:Security" EventCode=4625

| stats count by src_ip, Account_Name

| where count > 10

| sort -count

2) Failed attempts across many accounts from same IP (possible credential stuffing / spraying):

index=sysmon sourcetype="WinEventLog:Security" EventCode=4625

| stats dc(Account_Name) as distinct_accounts, count by src_ip

| where distinct_accounts > 5 AND count > 20

| sort -distinct_accounts desc

3) Multiple failures then success (same account):

index=sysmon sourcetype="WinEventLog:Security" (EventCode=4625 OR EventCode=4624)

| transaction Account_Name maxspan=15m startswith=(EventCode=4625) endswith=(EventCode=4624)

| search eventcount>5

| table Account_Name, src_ip, eventcount, duration, _time

(Adjust thresholds to your environment — e.g., 10 attempts may be noisy in high-auth environments.)

Preventive controls & mitigations

- Enforce **strong, unique passwords** and use **password managers**.
- Implement **multi-factor authentication (MFA)** — single best mitigation for online brute-force and credential stuffing.
- Enable account **lockout or progressive delays** after failed attempts (balance risk of denial-of-service).
- Use **rate limiting / CAPTCHA** on web login endpoints.
- Block / throttle suspicious IPs or IP ranges (automation + threat intel).
- Monitor and block known credential-stuffing lists and leaked credentials.
- Require password complexity and rotation policies where appropriate.
- Harden services: disable root/administrator remote logins, use key-based auth for SSH.

Response steps when detected

1. **Contain:** block offending IPs, throttle authentication endpoints.
2. **Protect accounts:** force password reset or lock impacted accounts, enable MFA if not present.

3. **Investigate:** check for successful logins, lateral movement, or data access.
4. **Remediate:** remove attacker persistence, reset credentials, patch misconfigurations.
5. **Harden & monitor:** add detection rules (like examples above) and tune alerts to reduce false positives.

Create a names file and password file

In kali linux, we have to create a names list file and passwords list file by using **cat** command.

Cat >> file_name

List of passwords saved as, passwords.txt

List of names saved as, names.txt

To do Brute-force attack

─(root㉿kali)-[/home/kali]

└─# hydra -L names.txt -P passwords.txt 192.168.1.3 ssh

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-11 08:24:09

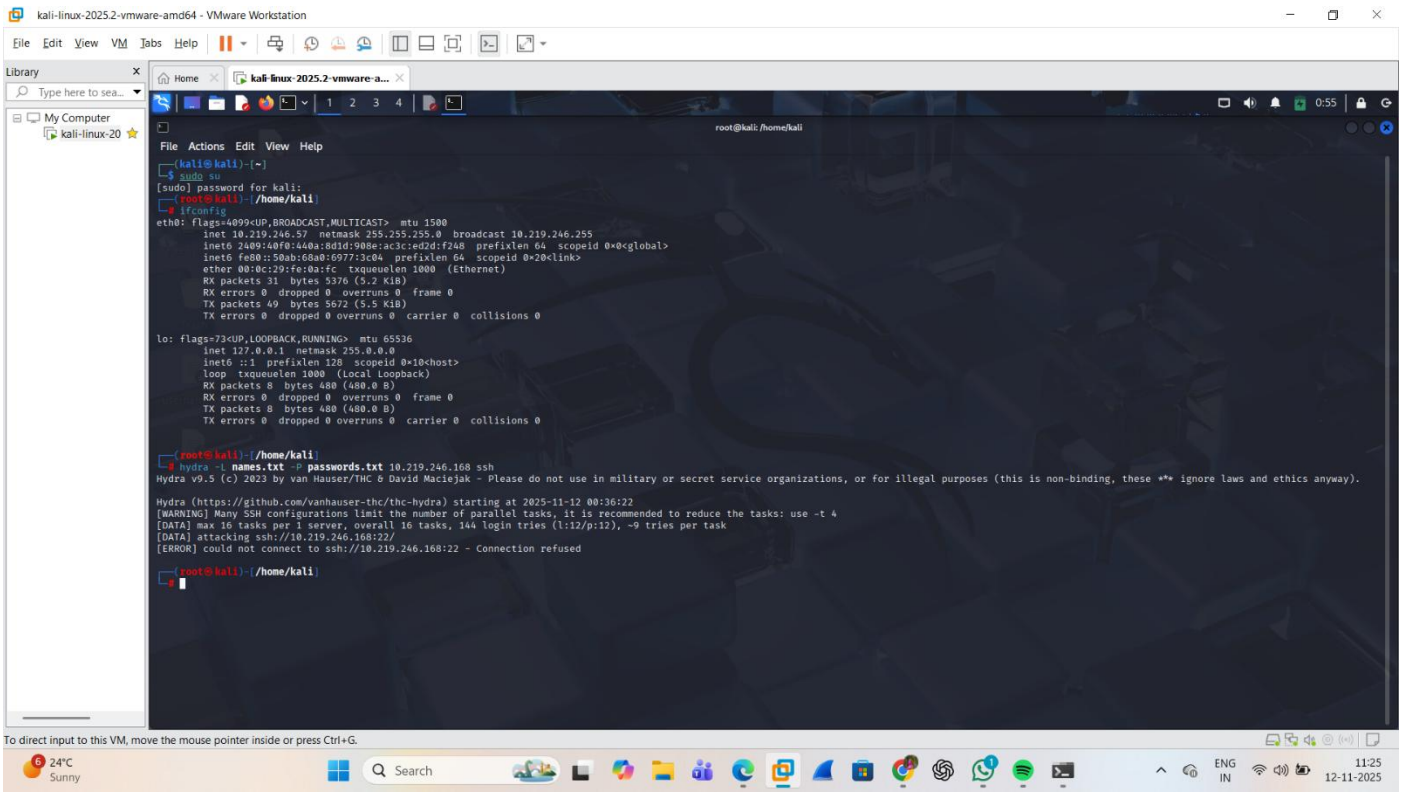
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4

[DATA] max 16 tasks per 1 server, overall 16 tasks, 144 login tries (l:12/p:12), ~9 tries per task

[DATA] attacking ssh://192.168.1.3:22/

[ERROR] could not connect to ssh://192.168.1.3:22 - Timeout connecting to 192.168.1.3

┌──(root㉿kali)-[/home/kali

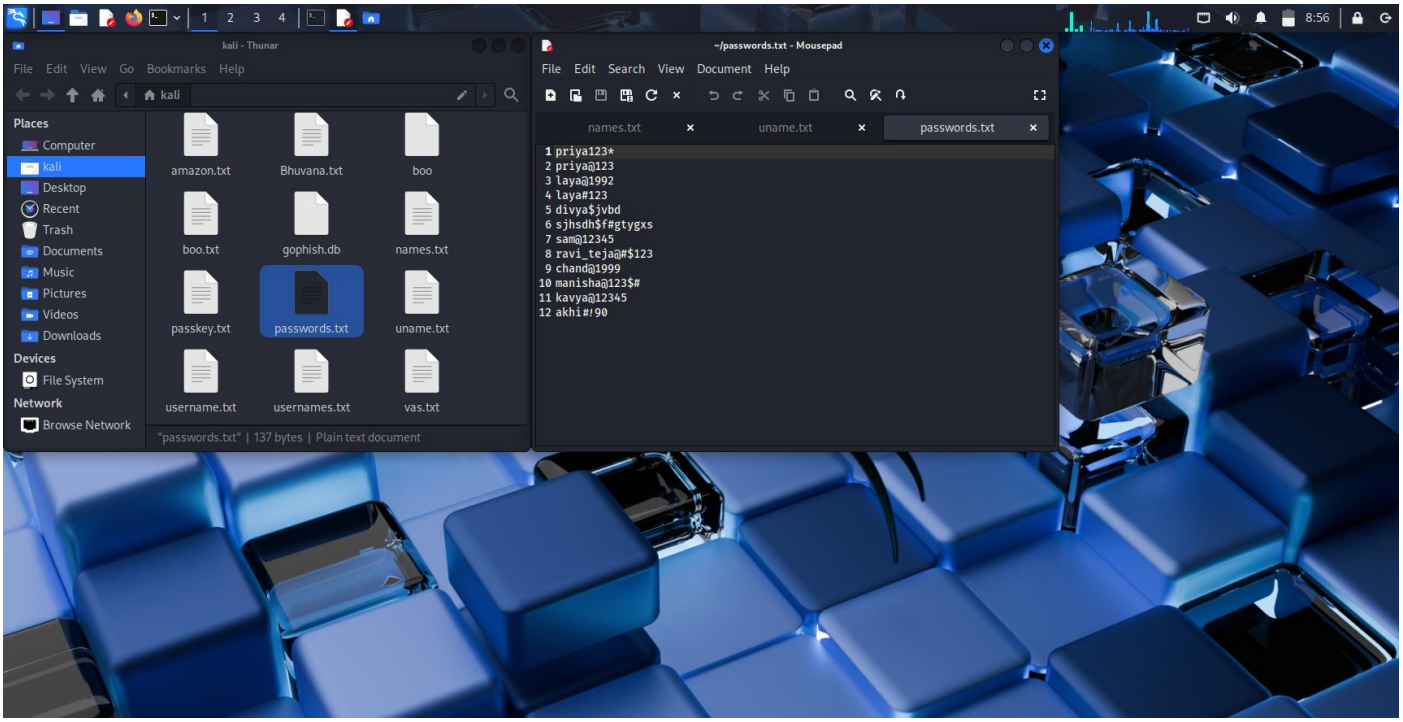


No True positive sign in attempted, connection refused.

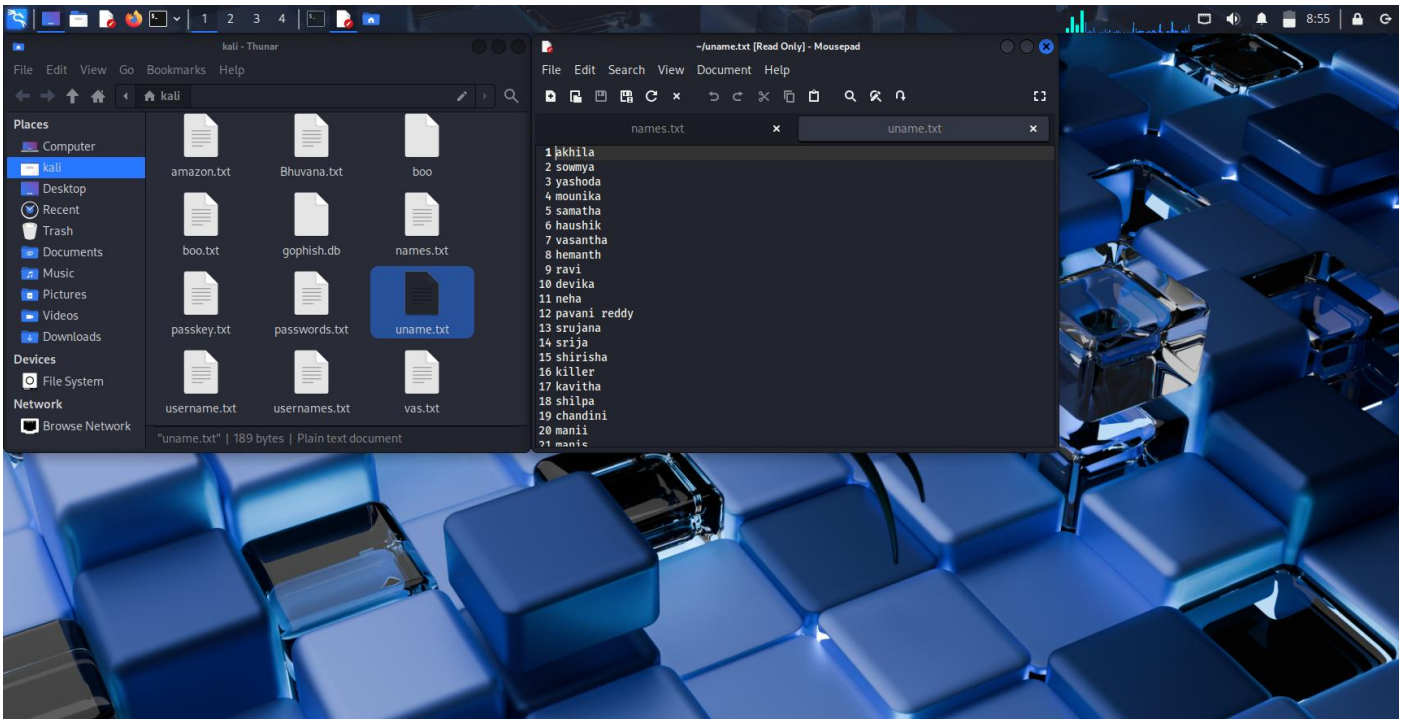
Here, we go

Let’s do the Brute- Force attack

Here, create a file having Usernames file and Passwords file.

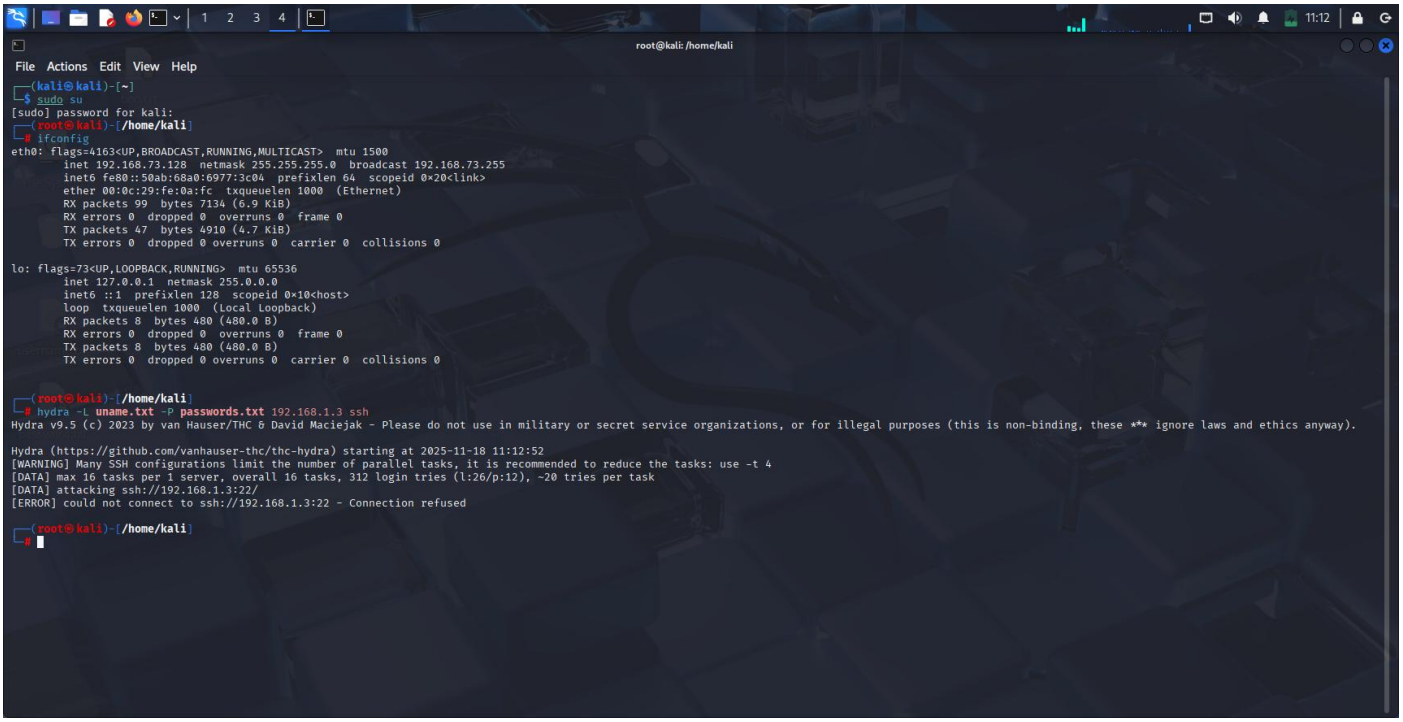


This is the list of Usernames.



This is the list of Passwords file.

Let’s do, the Brute- Force attack.



This is the Brute- force attack of password cracking command in kali Linux

Alerts from Splunk

Step 1: Confirm logs are coming into Splunk

Run this query:

index=* | head 20

If you don't see any logs → your *Universal Forwarder is not sending logs*.

Step 2: Find Authentication Failure Logs

For Windows brute-force attack, logs come from:

- EventID 4625 → Failed login
- EventID 4624 → Successful login

Check failures first:

index=* sourcetype=WinEventLog:Security EventCode=4625

If your brute-force from Kali was SSH, use:

index=* sourcetype=linux_secure "Failed password"

Step 3: Search for Brute-Force Pattern (Multiple Failures)

Windows Brute Force Detection SPL:

index=* sourcetype=WinEventLog:Security EventCode=4625

| stats count BY Account_Name, Workstation_Name, IpAddress

| where count > 5

| sort -count

This shows accounts with more than 5 failed logins → brute-force indicator.

Linux SSH Brute-Force Detection SPL:

index=* sourcetype=linux_secure "Failed password"

| stats count BY user, src

| where count > 5

| sort -count

Replace "Failed password" with "authentication failure" if needed.

Step 4: Check if Splunk Enterprise Security Alerts Are Available

If you installed ES (Enterprise Security):

Search for brute force in correlation searches:

| tstats summariesonly=t count from datamodel=Authentication where nodename=Authentication.Failed_Authentication by Authentication.src, Authentication.user

But if you're using *normal Splunk* → ignore this.

Ready-to-use SPL for General Brute Force:

index=* (EventCode=4625 OR "Failed password")

| stats count BY user, src

| where count > 10

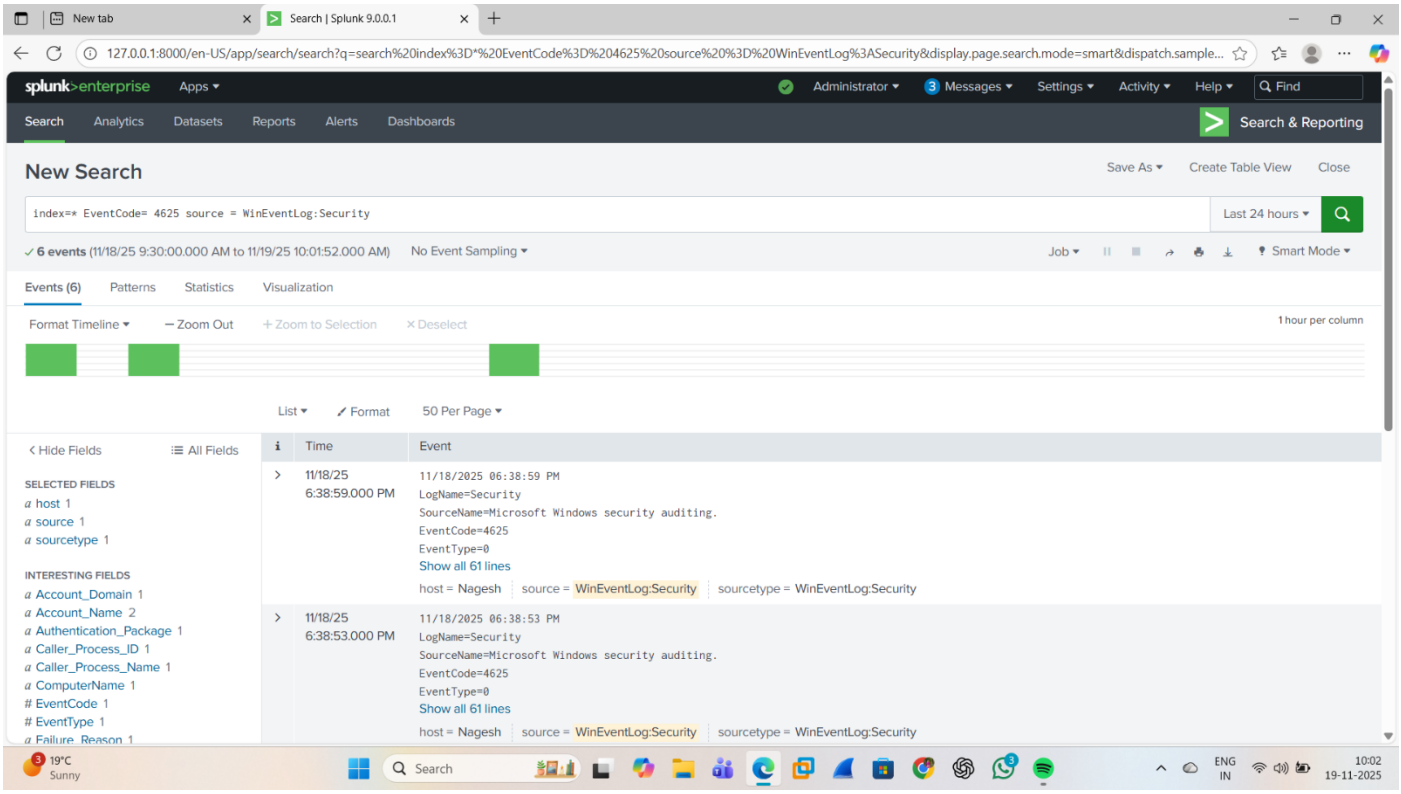
Important: Ensure UF is monitoring Security logs

Your inputs.conf must contain:

[WinEventLog://Security]

disabled = 0

Otherwise authentication logs will never reach Splunk.


New tab
Search | Splunk 9.0.0.1
127.0.0.1:8000/en-US/app/search/search?q=search%20index%3D*%20EventCode%3D%204625%20source%20%3D%20WinEventLog%3ASecurity&display.page.search.mode=smart&dispatch.sample...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=* EventCode= 4625 source = WinEventLog:Security
Last 24 hours
6 events (11/18/25 9:30:00.000 AM to 11/19/25 10:01:52.000 AM)
No Event Sampling
Job
Smart Mode
Events (6)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Account_Domain 1
a Account_Name 2
a Authentication_Package 1
a Caller_Process_ID 1
a Caller_Process_Name 1
a ComputerName 1
EventCode 1
EventType 1
a Failure_Reason 1
Time
Event
11/18/25 6:38:59.000 PM
11/18/2025 06:38:59 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4625
EventType=0
Show all 61 lines
host = Nagesh
source = WinEventLog:Security
sourcetype = WinEventLog:Security
11/18/25 6:38:53.000 PM
11/18/2025 06:38:53 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4625
EventType=0
Show all 61 lines
host = Nagesh
source = WinEventLog:Security
sourcetype = WinEventLog:Security
19°C
Sunny
Search
ENG
IN
10:02
19-11-2025

THE END