#JonSecOps

End-to-End Brute-Force Attack Simulation and Monitoring in an AD Environment

FIGURE 1: LOGICAL DIAGRAM

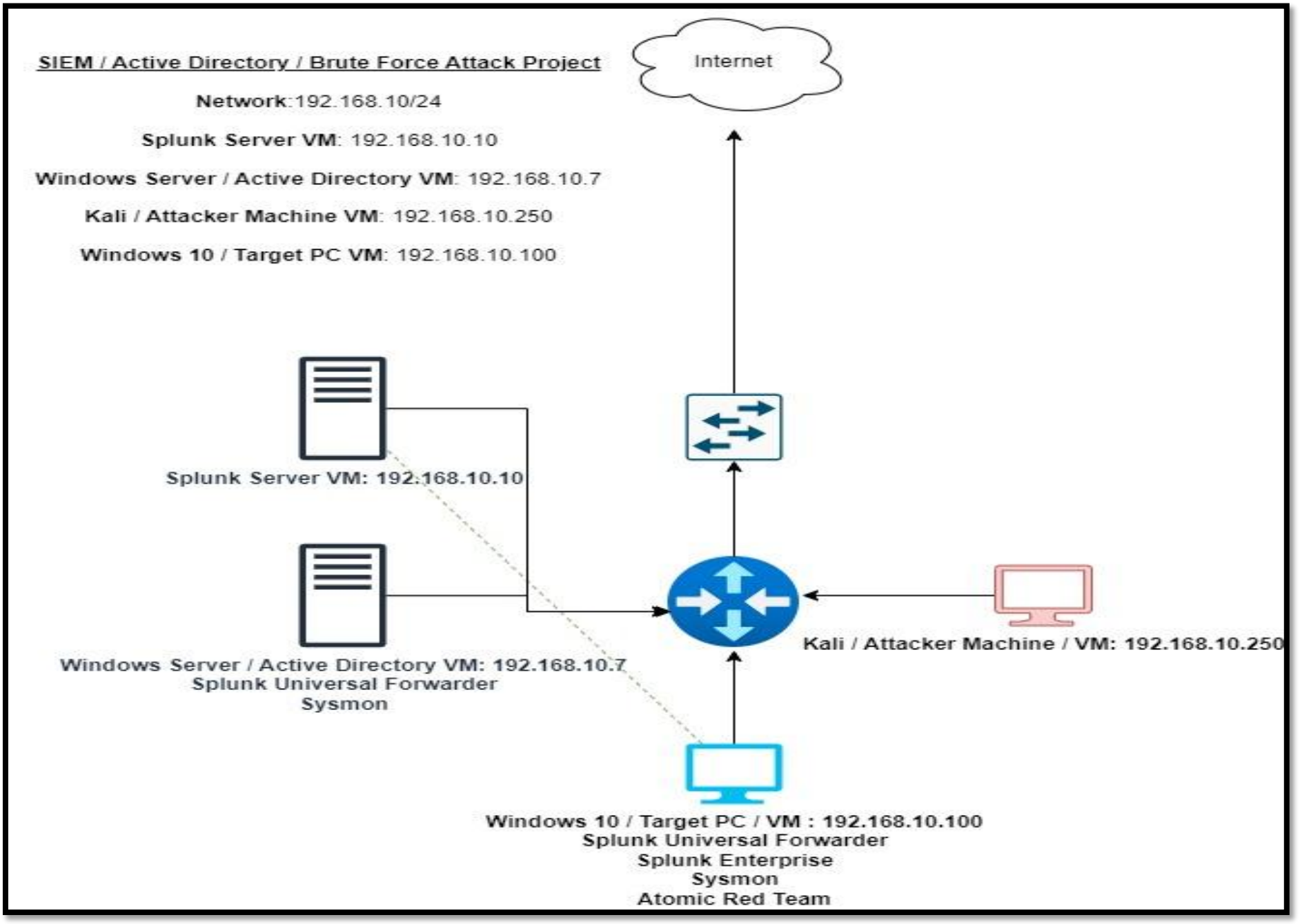


FIGURE 2: SYSTEM CONFIGURATIONS

Splunk Server: 192.168.10.10

- Installed Splunk on an Ubuntu server.
- Upgraded the server using sudo apt-get upgrade.
- Configured the Splunk server's IP address as a static IP to match the logical design.
- Added a user after installing Splunk on the Ubuntu server.

Windows Server / Active Directory: 192.168.10.7
Splunk Universal Forwarder
Sysmon

- Configured the computer name to ACTDIRSERVER.
- Assigned a static IP address to align with the logical design.
- Installed the Splunk Universal Forwarder and configured the inputs.conf file by copying it from the etc/system/default directory to the local folder. This defined the data to forward to the Splunk server.
- Installed Sysmon.
- Configured receiving settings and set the port to 9997 to ensure the Splunk server can receive data.
- Configured Server Manager to add roles and features, including the Active Directory Domain Services role.
- Promoted the server to a domain controller and created a new forest.
- Created users in Active Directory for a brute-force attack simulation using a Kali/attacker machine.

Windows 10 / Target PC : 192.168.10.100
Splunk Universal Forwarder
Splunk Enterprise
Sysmon
Atomic Red Team

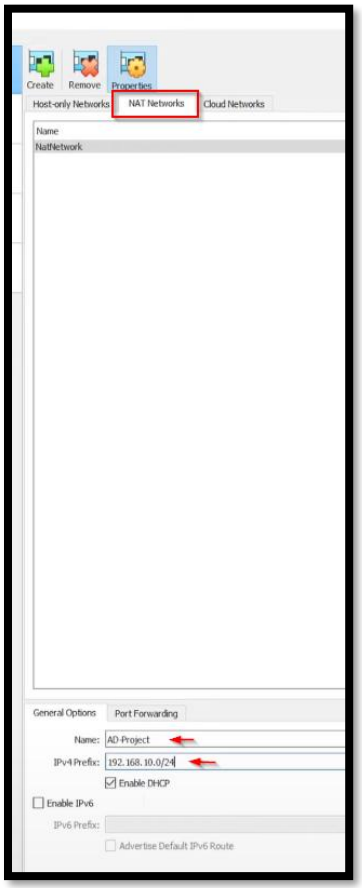
- Renamed the computer to TARGET-PC.
- Configured a static IP address to align with the logical design.
- Installed the Splunk Universal Forwarder, created a copy of the inputs.conf file from the etc/system/default directory, and pasted it into the local folder to define the data to forward to the Splunk server.
- Installed Sysmon.
- Created an index called endpoint in Splunk Enterprise to collect telemetry from the configured input file in Splunk Universal Forwarder.
- Configured Splunk Enterprise receiving settings to use port 9997, ensuring the Splunk server can receive data.
- Connected the Windows target machine to the ACTDIRSERVER domain controller (LAB.local) and authenticated using the Jenny Smith account.
- Configured the Active Directory server with two users.
- Installed Atomic Red Team to simulate attacks and generate telemetry visible in Splunk.
- Enabled Remote Desktop access for Active Directory users jsmith and tsmith.

Kali / Attacker Machine: 192.168.10.250

- Configured a static IP address to match the logical design.
- Installed the Crowbar tool.
- Created a directory named Lab-project.
- Located the rockyou wordlist pre-installed in Kali Linux under the usr/share/wordlists directory.
- Unzipped the rockyou.txt file and copied it to the Lab-project directory.
- Extracted the first 20 lines from the rockyou.txt file and saved them in a new file named passwords.txt.
- Edited the passwords.txt file to include the Active Directory users' passwords, used for the brute-force password attack.
- Conducted a successful brute-force password attack against the Active Directory users.
- Captured the telemetry in Splunk, including EventCode 4625, indicating failed login attempts for the accounts.

Kali Linux, Windows 10, Windows Server 2022 and Splunk Server software was installed. Once the virtual machines for these systems were created, the NAT Network settings within VirtualBox was changed so that all created virtual machines will be on the same network called AD-Project. The IPv4 address was changed to 192.168.10.0/24 which coincides with the IP address within the logical diagram.

FIGURE 3: NAT NETWORK SETTINGS CONFIGURATION

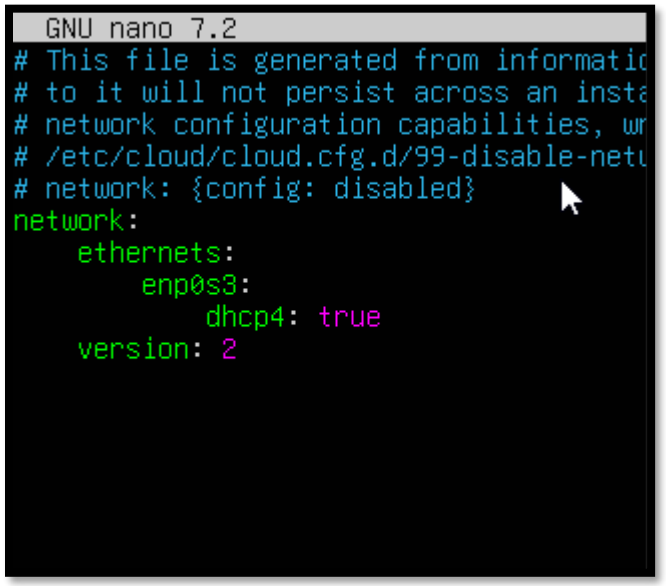


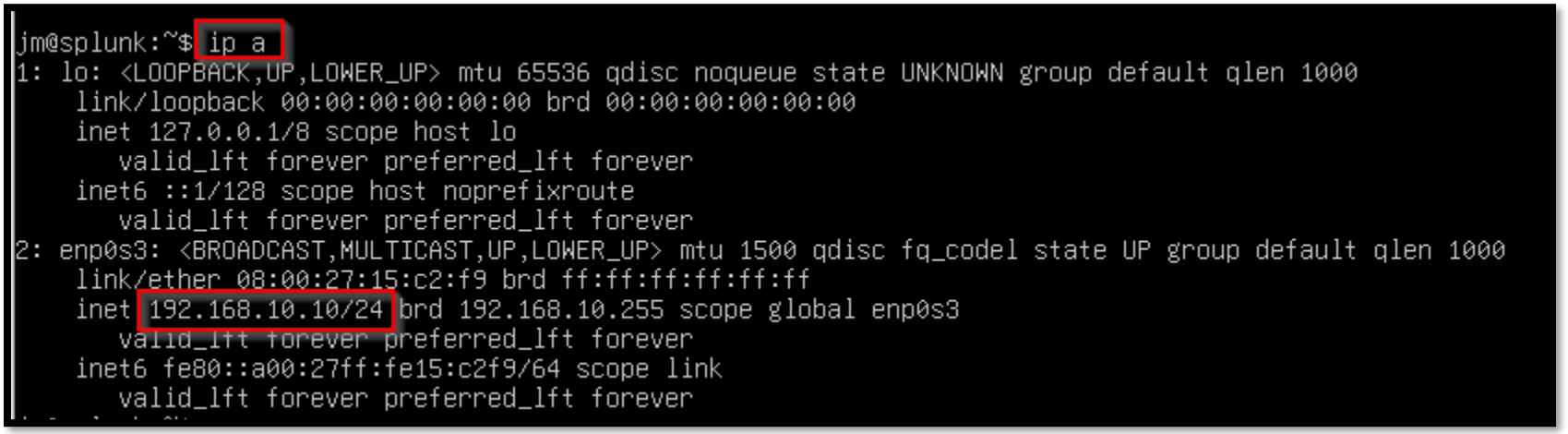
The splunk servers IP address was changed to match the IP address within the logical diagram which is 192.168.10.10. The '**sudo nano /etc/netplan/50-cloud-init.yaml**' command was used to change this.

```
jm@splunk:~$ sudo nano /etc/netplan/50-cloud-init.yaml
```

Once entered, the following network configurations were made within the yaml file. Displayed is the original configurations next to the changed configurations. Once completed the '**sudo netplan apply**' command was used to allow the configuration changes. The ' **ip a** ' command was used to display the newley created IP address of 192.168.10.10.

FIGURE 4: SPLUNK SERVER NETWORK ADDRESS CONFIGURATIONS



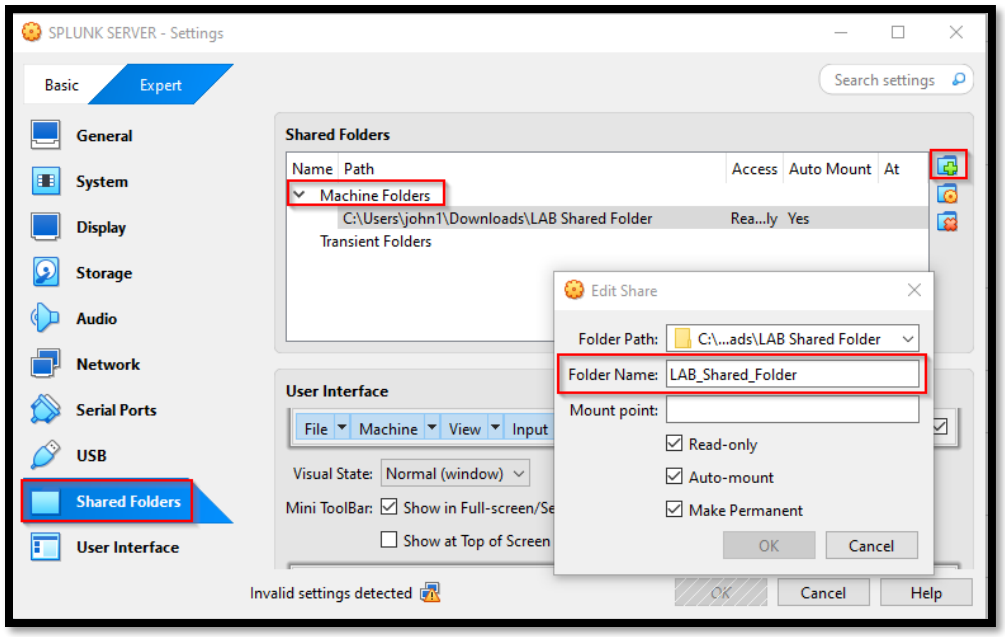


Splunk Enterprise for Linux was then downloaded on the host machine. Within the Splunk Server the guest add-ons for Virtual Box needed to be installed so the '**sudo apt-get install virtualbox-guest-additions-iso**' command was entered.

```
jm@splunk:~$ sudo apt-get install virtualbox-guest-additions-iso
```

To share folders from the host machine to the Splunk Server machine, the Splunk Server Vms shared folder settings was configured and a folder named LAB_Shared_Folder was created. The downloaded Splunk Enterprise file was then copied to the LAB_Shared_Folder folder on the host system.

FIGURE 5: ALLOWING HOST COMPUTER TO SHARE FILES WITH SPLUNK SERVER VM



To add a user to the vboxsf group in the Splunk Server the '**sudo apt-get install virtualbox-guest-utils**' command was entered followed by the '**sudo adduser jm vboxsf**' command.

```
jm@splunk:~$ sudo apt-get install virtualbox-guest-utils
```

```
jm@splunk:~$ sudo adduser jm vboxsf
```

To make a directory called *share,* the '**mkdir share**' command was entered followed by the 'ls -la' command to display the created diretory.

```
jm@splunk:~$ mkdir share
```

```
jm@splunk:~$ ls -la
total 40
drwxr-x--- 5 jm   jm   4096 Feb 10 16:30 .
drwxr-xr-x 3 root root 4096 Dec 12 01:24 ..
-rw------- 1 jm   jm   1394 Dec 16 16:16 .bash_history
-rw-r--r-- 1 jm   jm    220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 jm   jm   3771 Mar 31  2024 .bashrc
drwx------ 2 jm   jm   4096 Dec 12 01:25 .cache
-rw------- 1 jm   jm     20 Feb 10 16:30 .lesshst
-rw-r--r-- 1 jm   jm    807 Mar 31  2024 .profile
drwxrwxr-x 2 jm   jm   4096 Dec 12 02:04 share
drwx------ 2 jm   jm   4096 Dec 12 01:25 .ssh
-rw-r--r-- 1 jm   jm      0 Dec 12 01:25 .sudo_as_admin_successful
```

To mount the created LAB_Shared_Folder on our host machine to our created directory named share within the Splunk Server, the '**sudo mount -t vboxsf -o uid=1000, gid=1000 LAB_Shared_Folder share/**' was entered. To install the Splunk Enterprise file from the host sytem to the Splunk server the '**cd share**' command was used followed by the '**sudo dpkg -i splunk-9.2.0.1-d8ae995bf219-linux-2.6-amd.64.deb**' command.

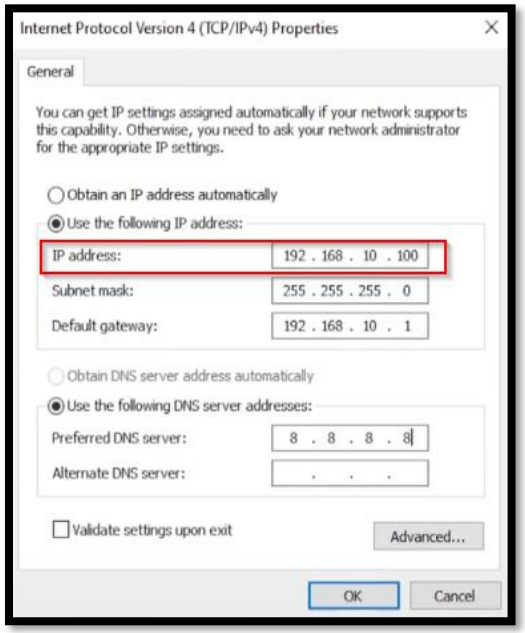
(add imagE)

After installation the '**sudo -u splunk bash**' command was entered to change to the user splunk. The '**cd bin**' command was entered to get into splunks binary files and the **'./splunk start'** command was entered to run the installer.

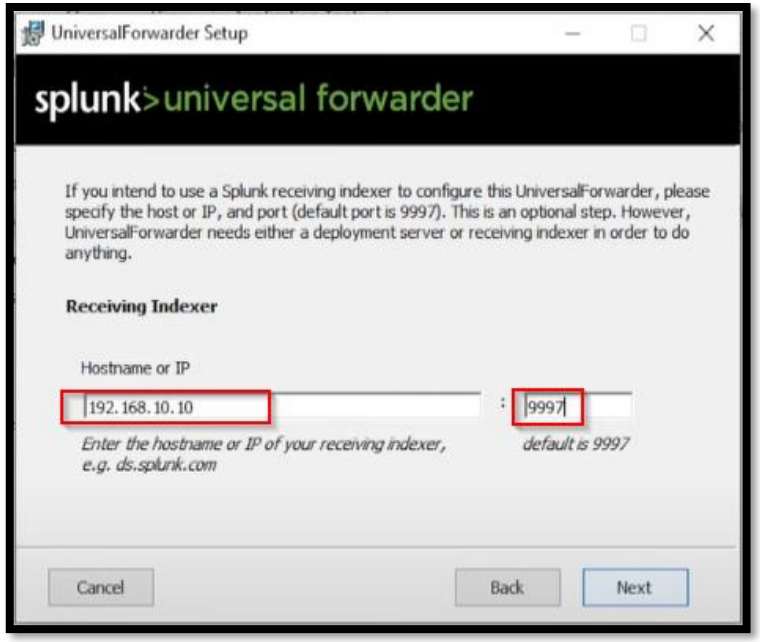
```
jm@splunk:/opt/splunk$ sudo -u splunk bash
splunk@splunk:~$ cd bin
splunk@splunk:~/bin$ ./splunk start
```

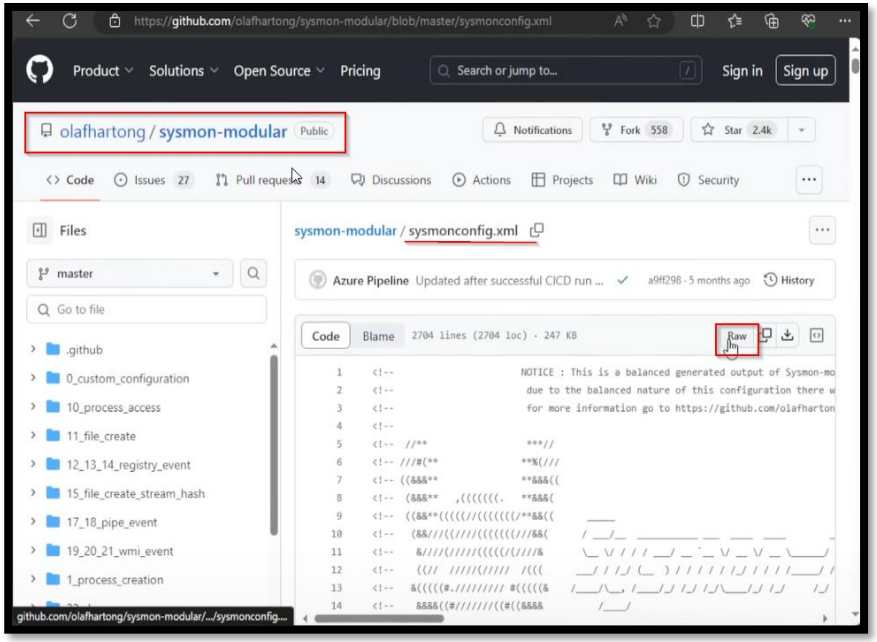
After the administrator and username creation for splunk, the '**exit**' command was entered to switch back to the user jm. The '**cd bin**' command was used to get into the binary files, and the '**sudo ./splunk enable boot-start -user splunk**' to allow splunk to run with the user splunk after the vm reboots.

The Windows 10 machine name was changed to Target PC and its IP address was changed to 192.168.10.100 within the network settings.

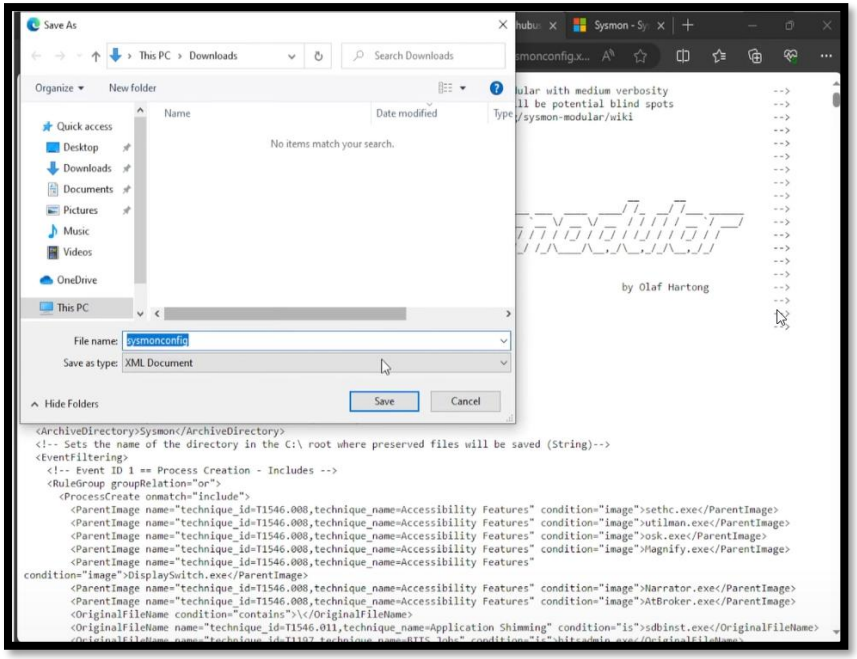


On the Windows 10 Target PC machine, Spunk Universal Forwarder was installed/configured and Sysmon with installed with olaf configuration (sysmonconfig.xml) from github.



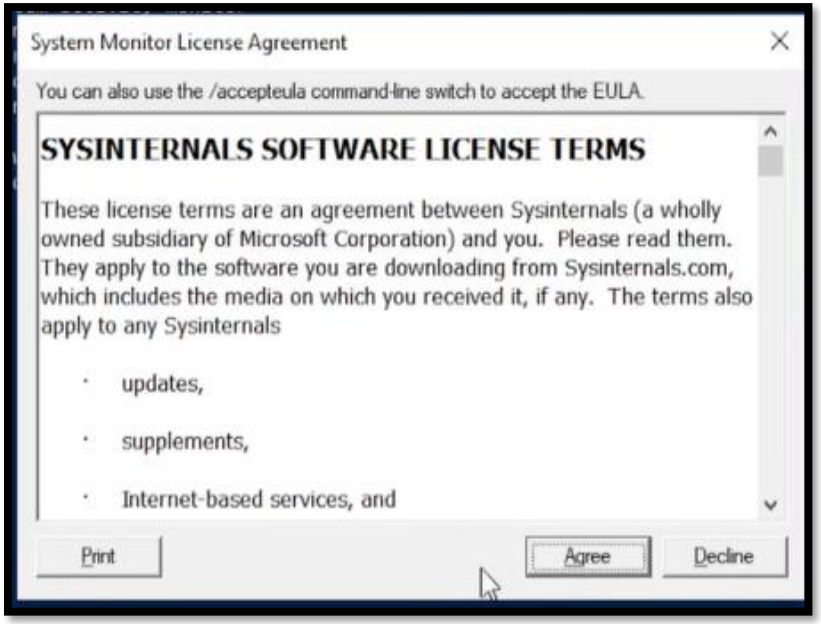


The sysmon configuration file was then saved to the Target PC.

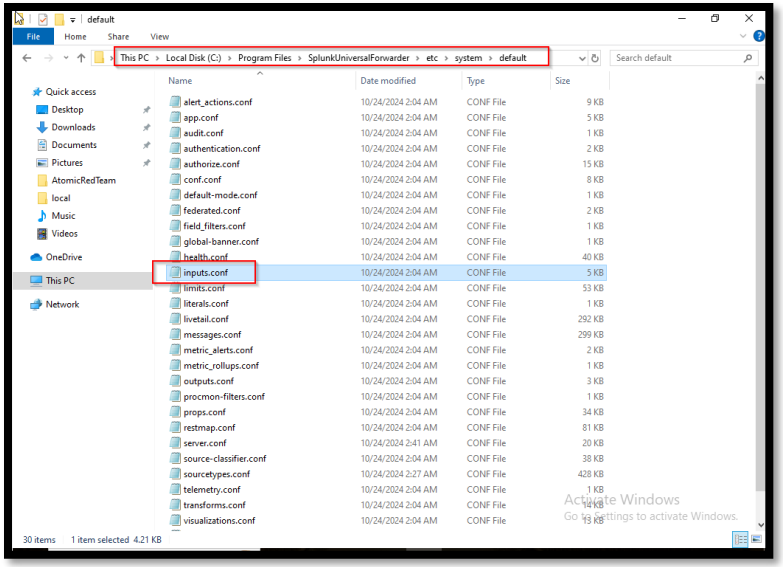


Sysmon was installed using the following command

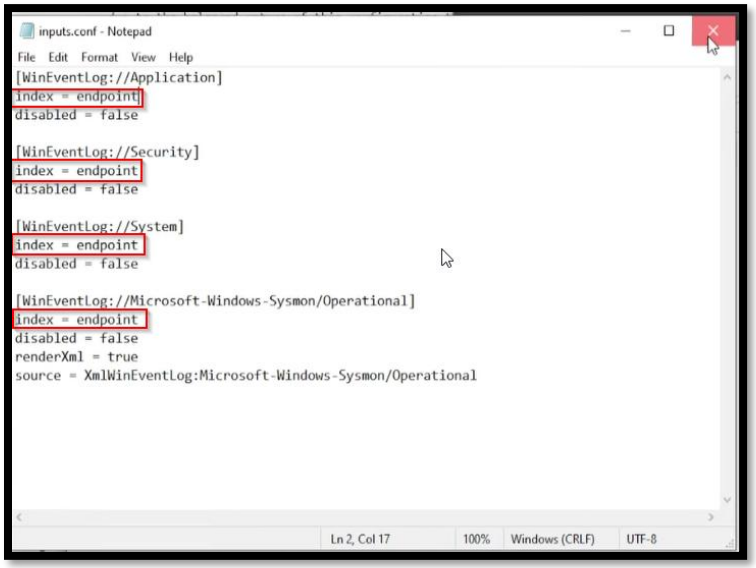
```
PS C:\Users\TARGET PC\Downloads\Sysmon> .\Sysmon64.exe -i ..\sysmonconfig.xml
```



To instruct our installed splunk forwader on what we want to send over to our splunk server the inputs.conf in the SplunkUniversalForwarder default folder needs to be copied and configured in the SplunkUniversalForwarders local folder.



The copied inputs.conf is first opened and configured in notepad as an administrator and saved in the local folder.



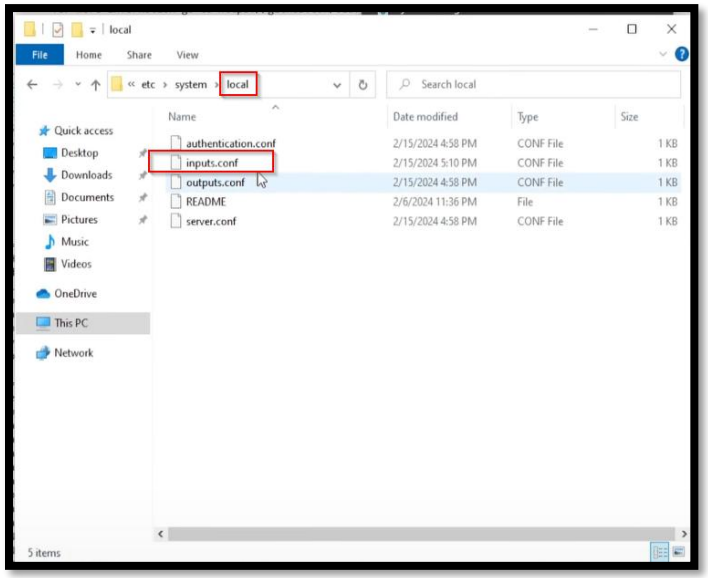
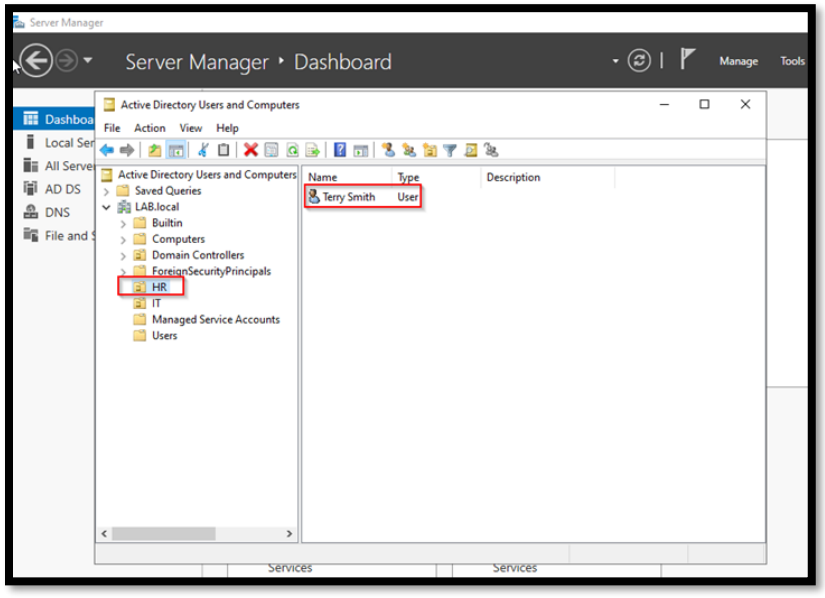


FIGURE 3: ADDED USERS IN ACTIVE DIRECTORY SERVER



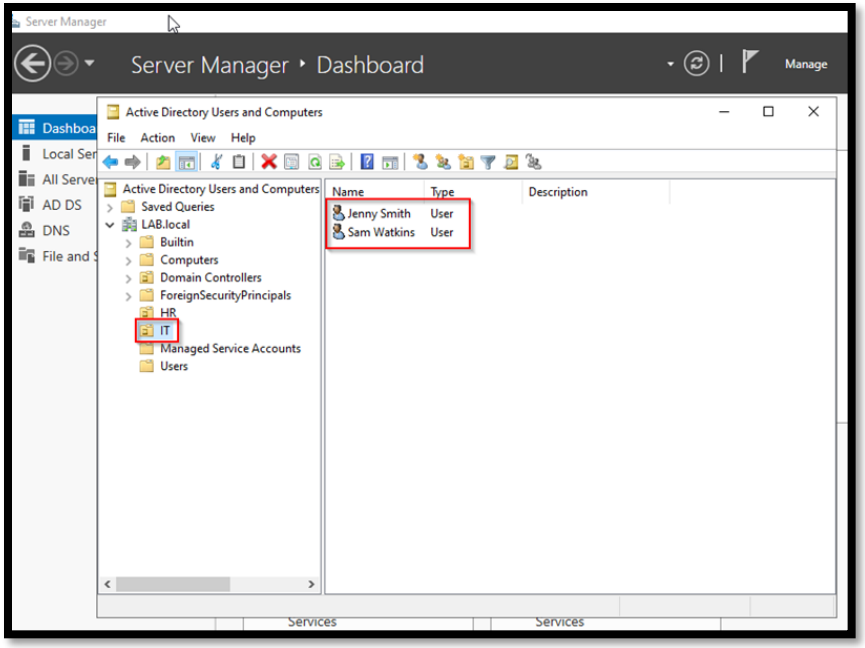


FIGURE 4: KALI / ATTACKER MACHINE COMMANDS

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wordlists

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt.gz

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo gunzip rockyou.txt.gz

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sq

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cp rockyou.txt ~/Desktop/lab-project
```

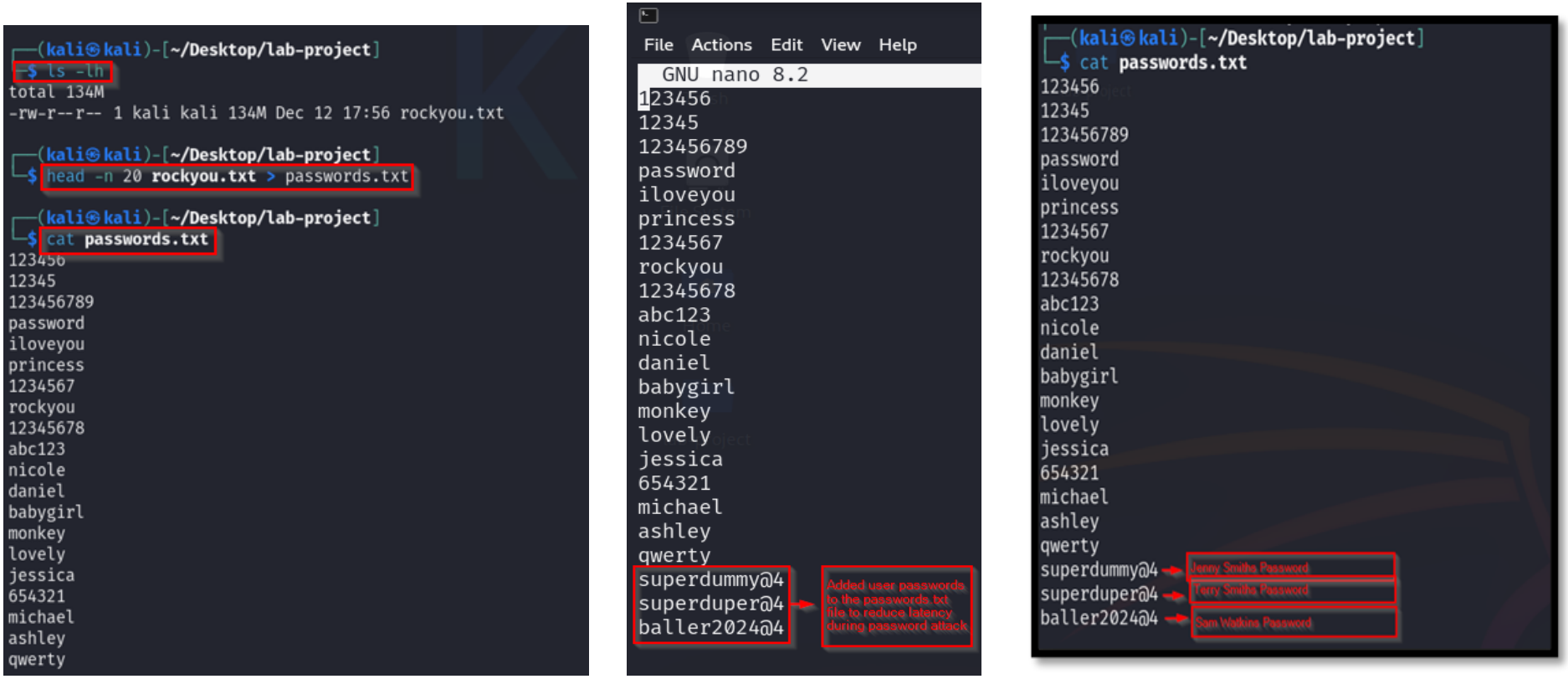


FIGURE 5: SUCCESSFUL BRUTE FORCE ATTACK

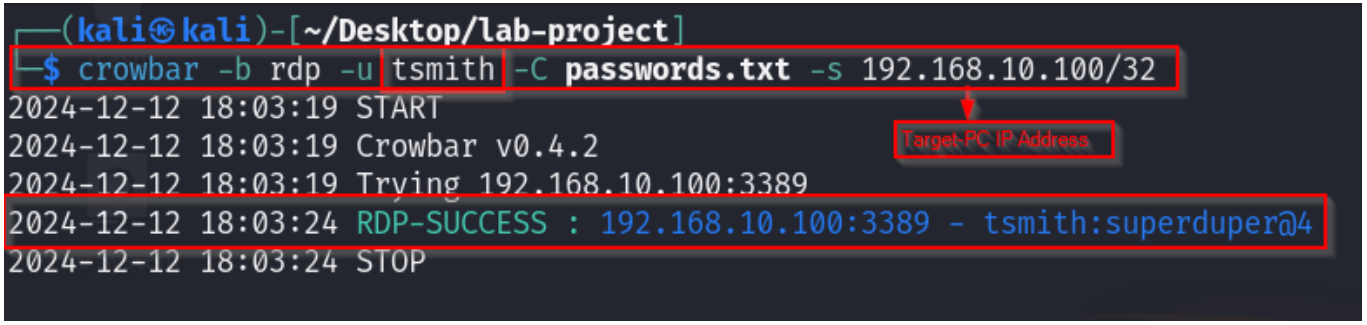
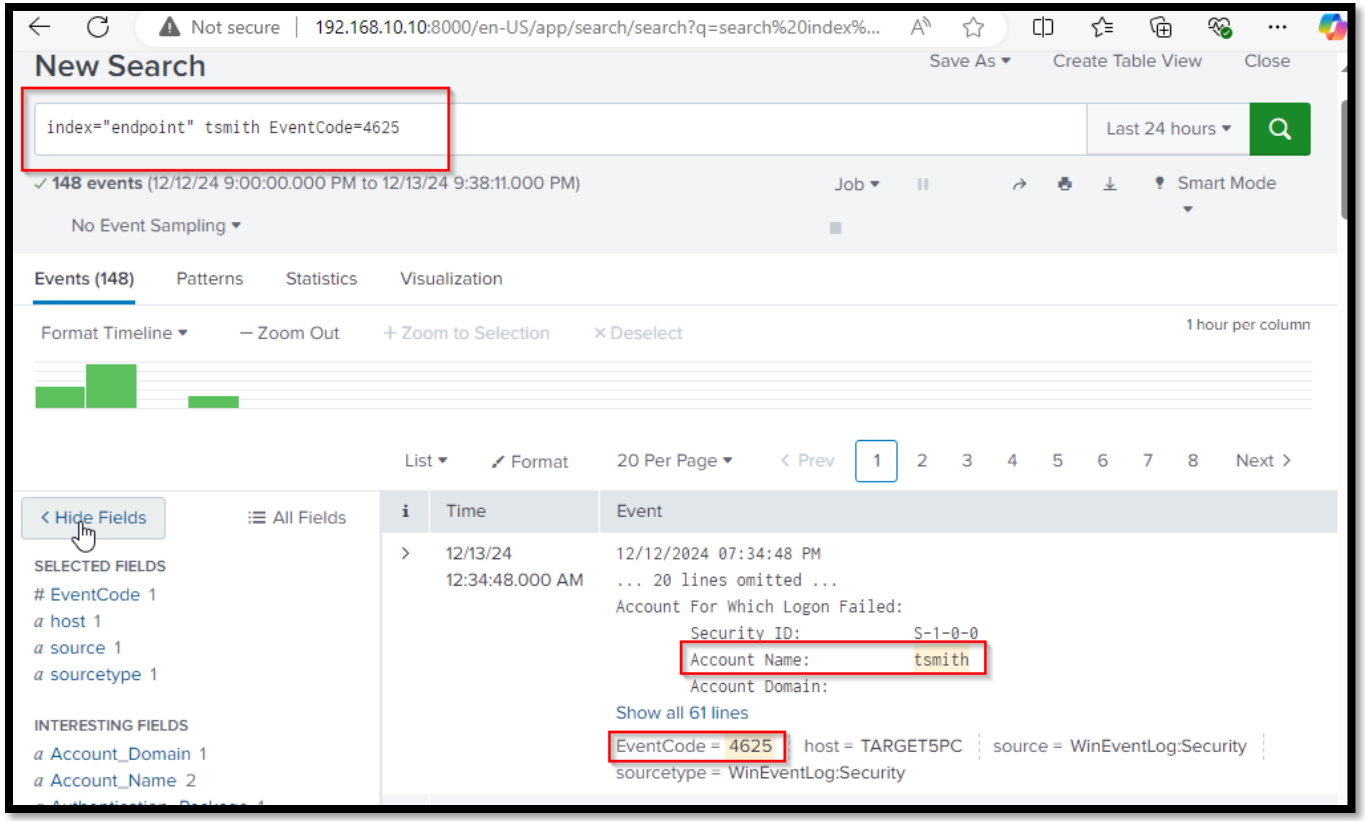
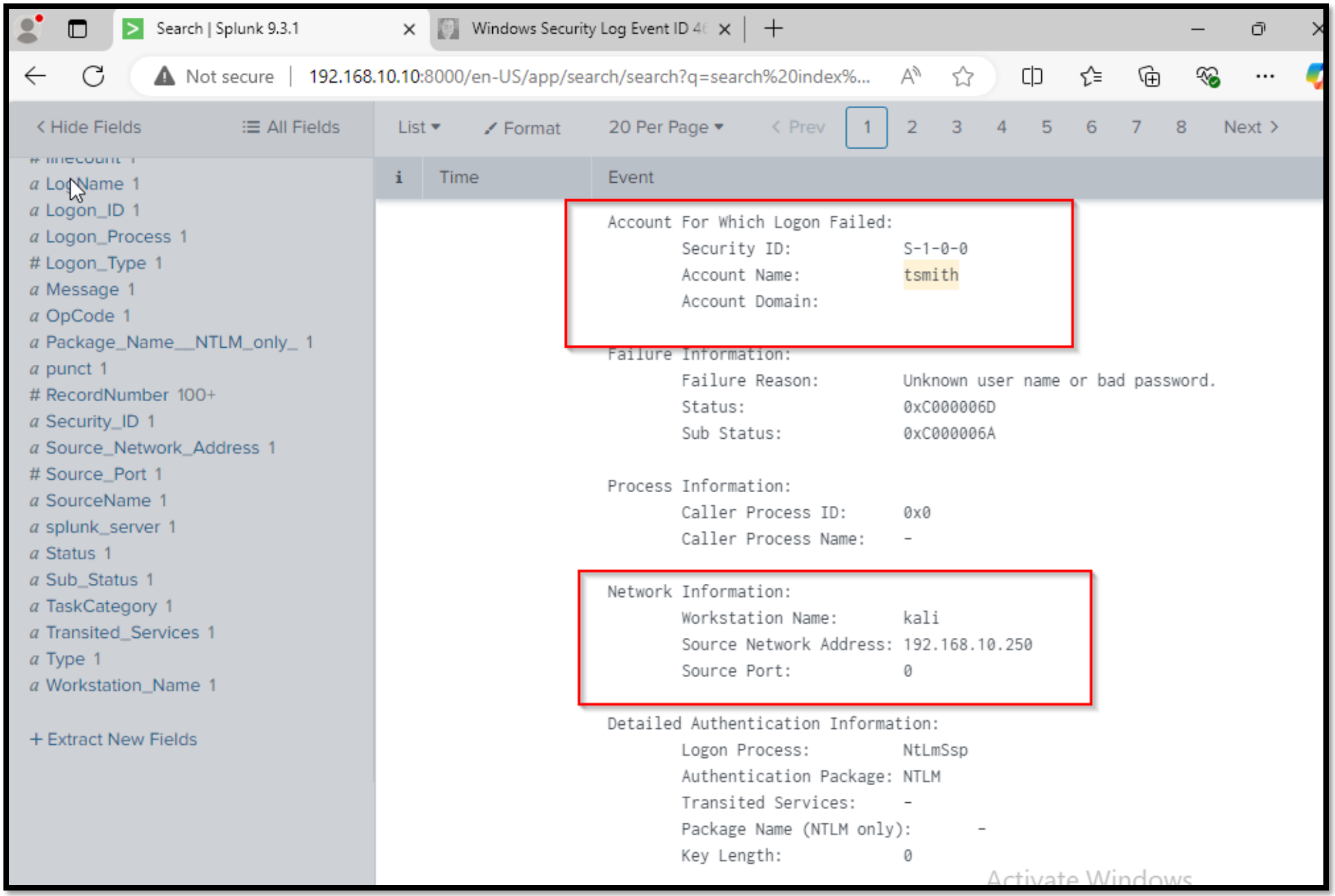


FIGURE 6: SPLUNK TELEMETRY OF BRUTE FORCE ATTACK ON TARGET MACHINE


Not secure | 192.168.10.10:8000/en-US/app/search/search?q=search%20index%...
New Search
Save As
Create Table View
Close
index="endpoint" tsmith EventCode=4625
Last 24 hours
148 events (12/12/24 9:00:00.000 PM to 12/13/24 9:38:11.000 PM)
Job
Smart Mode
No Event Sampling
Events (148)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
EventCode 1
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Account_Domain 1
a Account_Name 2
Time
Event
12/13/24
12:34:48.000 AM
12/12/2024 07:34:48 PM
... 20 lines omitted ...
Account For Which Logon Failed:
Security ID: S-1-0-0
Account Name: tsmith
Account Domain:
Show all 61 lines
EventCode = 4625
host = TARGET5PC
source = WinEventLog:Security
sourcetype = WinEventLog:Security


Search | Splunk 9.3.1
Windows Security Log Event ID 4
Not secure
192.168.10.10:8000/en-US/app/search/search?q=search%20index%...
Hide Fields
All Fields
List
Format
20 Per Page
Prev
1 2 3 4 5 6 7 8
Next
Time
Event
a LogName 1
a Logon_ID 1
a Logon_Process 1
Logon_Type 1
a Message 1
a OpCode 1
a Package_Name__NTLM_only_ 1
a punct 1
RecordNumber 100+
a Security_ID 1
a Source_Network_Address 1
Source_Port 1
a SourceName 1
a splunk_server 1
a Status 1
a Sub_Status 1
a TaskCategory 1
a Transited_Services 1
a Type 1
a Workstation_Name 1
+ Extract New Fields
Account For Which Logon Failed:
Security ID: S-1-0-0
Account Name: tsmith
Account Domain:
Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A
Process Information:
Caller Process ID: 0x0
Caller Process Name: -
Network Information:
Workstation Name: kali
Source Network Address: 192.168.10.250
Source Port: 0
Detailed Authentication Information:
Logon Process: NtLmSsp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): -
Key Length: 0
Activate Windows

Encyclopedia

- Event IDs
- All Event IDs
- Audit Policy

Go To Event ID: Go

Security Log Quick Reference Chart

⇦ Windows Security Log Event ID 4625 ⇨

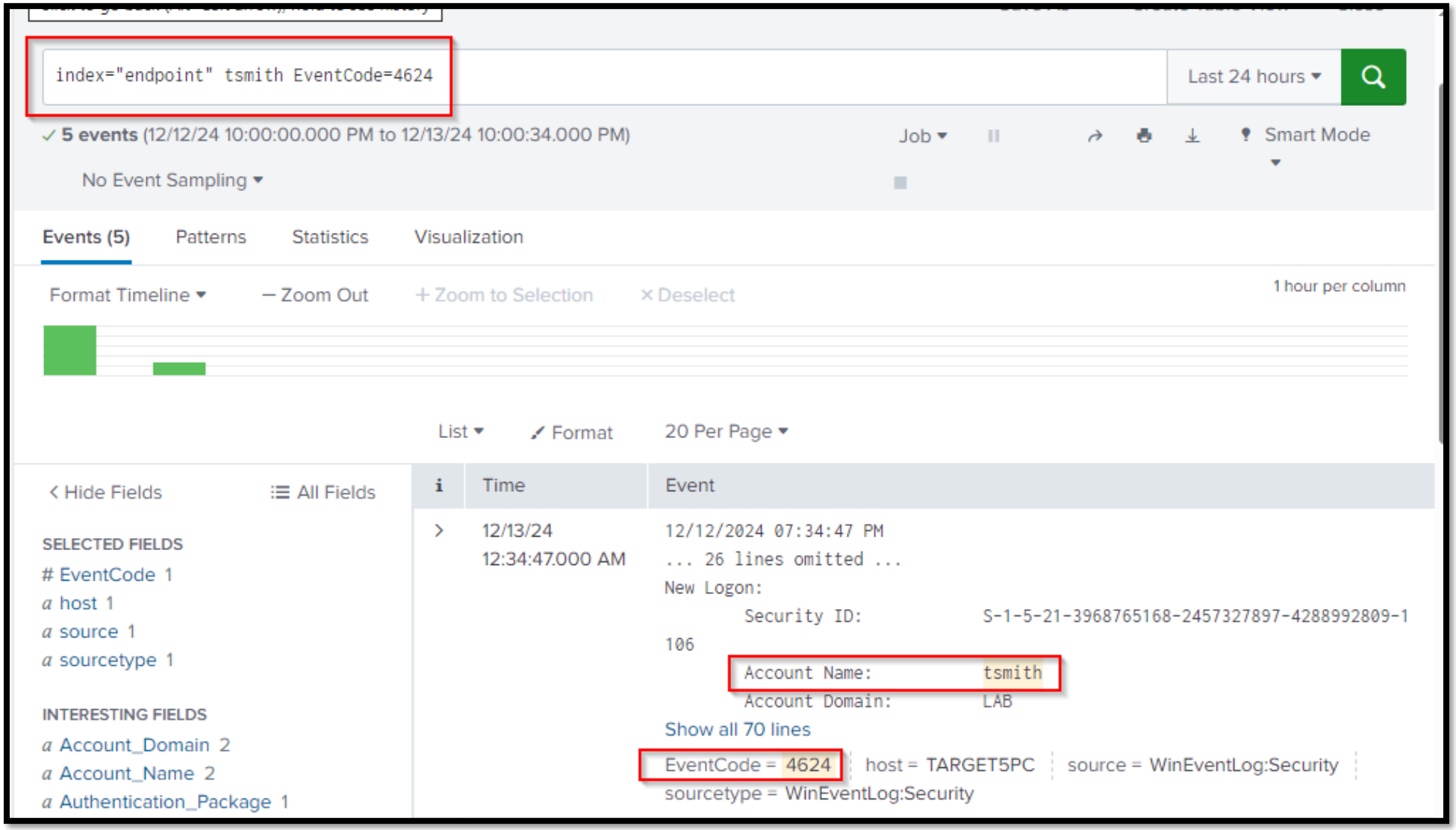
4625: An account failed to log on

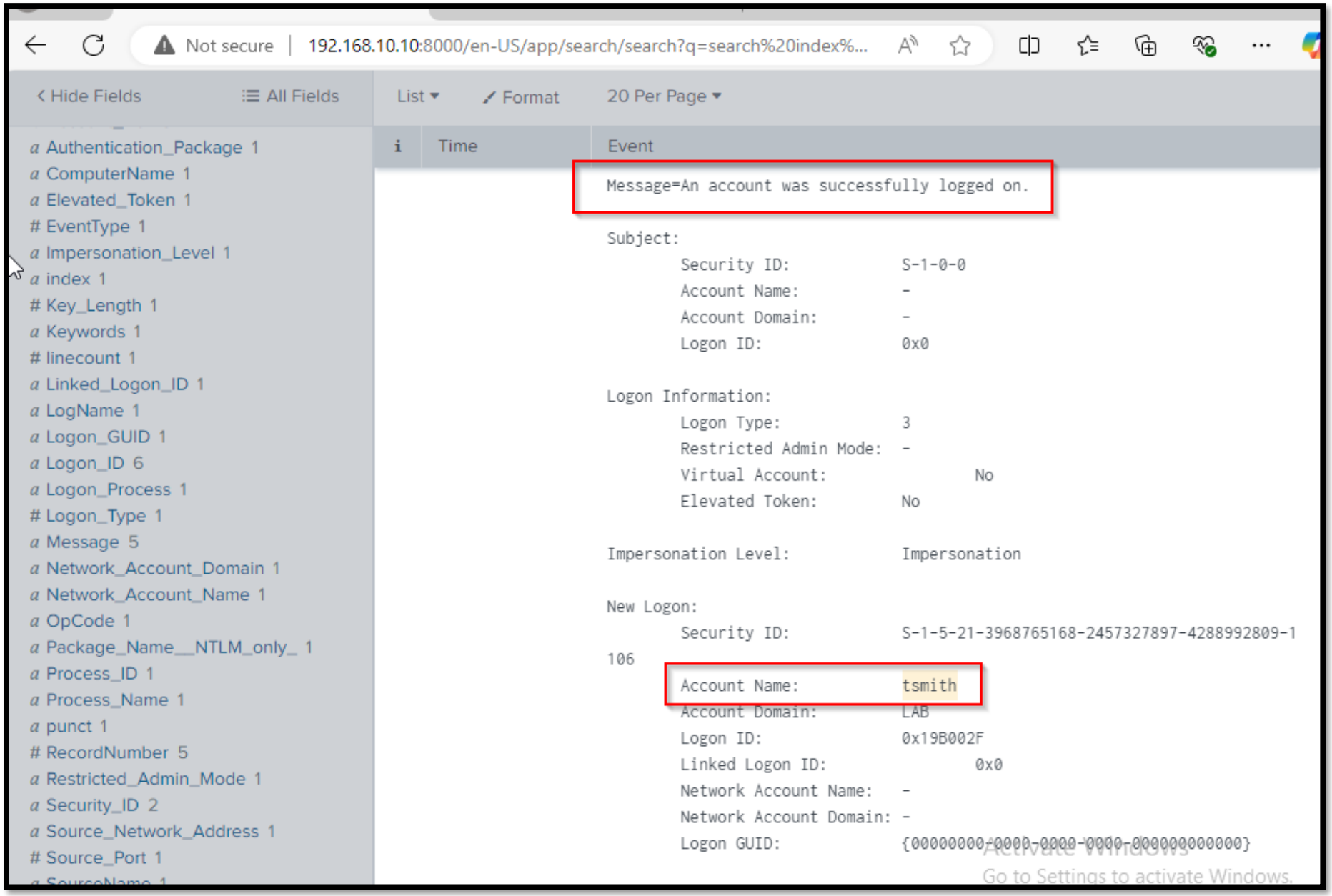
On this page

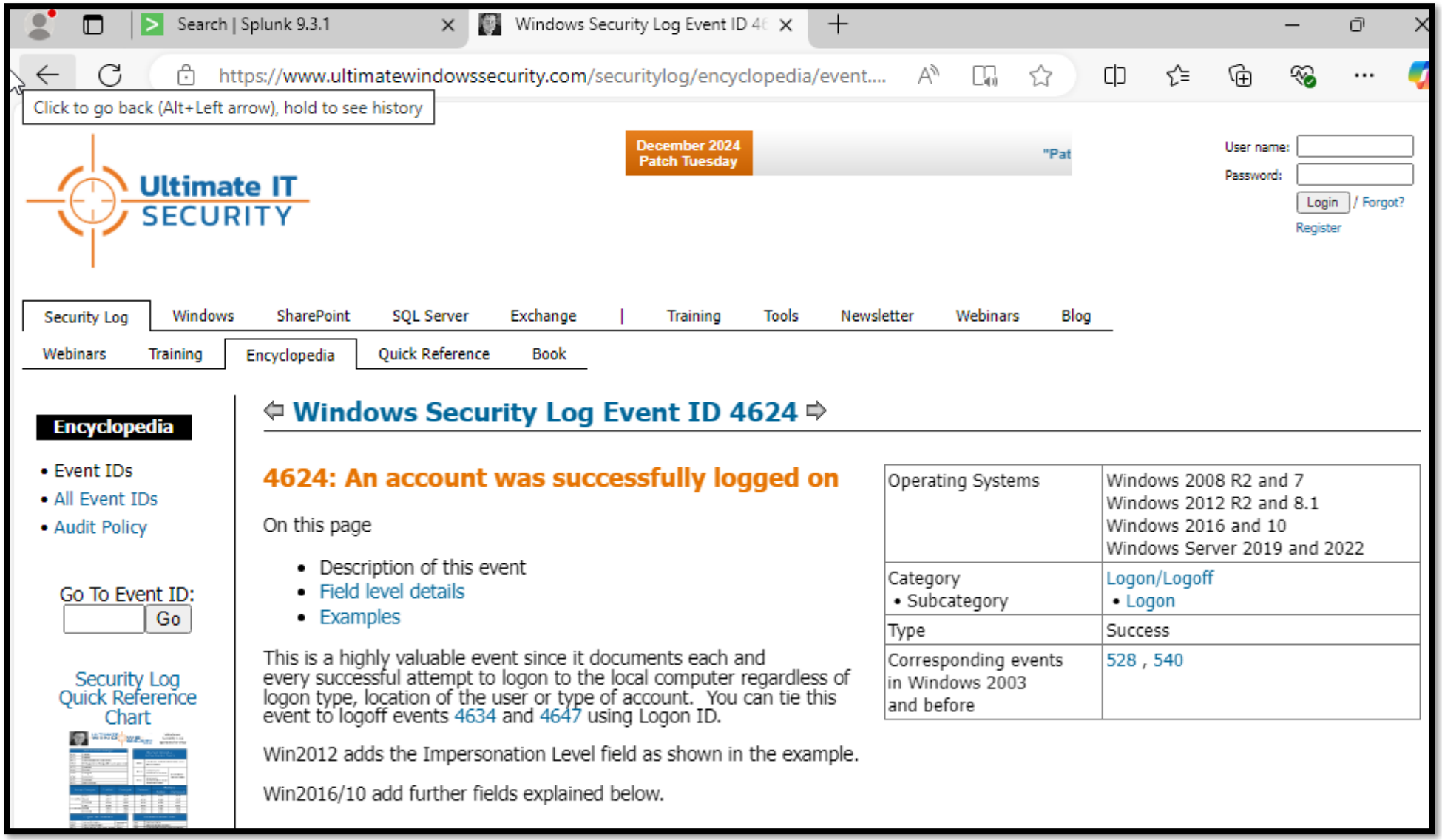
This is a useful event because it documents each and every failed attempt to logon to the local computer regardless of logon type, location of the user or type of account.

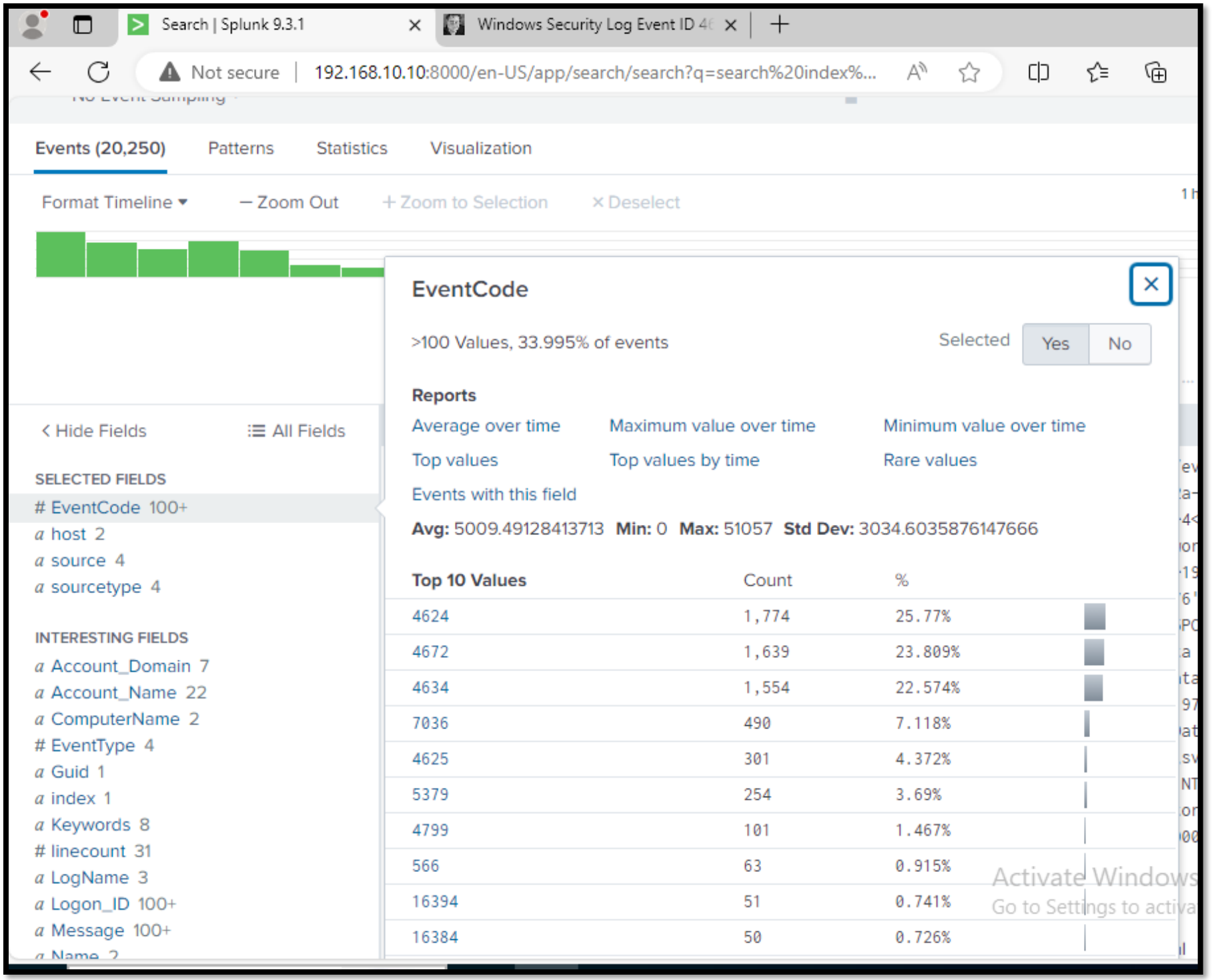
Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022
Category • Subcategory	Logon/Logoff • Logon
Type	Failure
Corresponding events in Windows 2003 and before	529 , 530 , 531 , 532 , 533 , 534 , 535 , 536 , 537 , 539

Free Security Log Resources by Randy


index="endpoint" tsmith EventCode=4624
Last 24 hours
5 events (12/12/24 10:00:00.000 PM to 12/13/24 10:00:34.000 PM)
Job
Smart Mode
No Event Sampling
Events (5)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
EventCode 1
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Account_Domain 2
a Account_Name 2
a Authentication_Package 1
Time
Event
12/13/24
12:34:47.000 AM
12/12/2024 07:34:47 PM
... 26 lines omitted ...
New Logon:
Security ID: S-1-5-21-3968765168-2457327897-4288992809-1106
Account Name: tsmith
Account Domain: LAB
Show all 70 lines
EventCode = 4624
host = TARGET5PC
source = WinEventLog:Security
sourcetype = WinEventLog:Security


Not secure
192.168.10.10:8000/en-US/app/search/search?q=search%20index%...
Hide Fields
All Fields
List
Format
20 Per Page
Authentication_Package 1
ComputerName 1
Elevated_Token 1
EventType 1
Impersonation_Level 1
index 1
Key_Length 1
Keywords 1
linecount 1
Linked_Logon_ID 1
LogName 1
Logon_GUID 1
Logon_ID 6
Logon_Process 1
Logon_Type 1
Message 5
Network_Account_Domain 1
Network_Account_Name 1
OpCode 1
Package_Name__NTLM_only_ 1
Process_ID 1
Process_Name 1
punct 1
RecordNumber 5
Restricted_Admin_Mode 1
Security_ID 2
Source_Network_Address 1
Source_Port 1
Time
Event
Message=An account was successfully logged on.
Subject:
Security ID: S-1-0-0
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Information:
Logon Type: 3
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: No
Impersonation Level: Impersonation
New Logon:
Security ID: S-1-5-21-3968765168-2457327897-4288992809-1106
Account Name: tsmith
Account Domain: LAB
Logon ID: 0x19B002F
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}
Activate Windows
Go to Settings to activate Windows.


Search | Splunk 9.3.1
Windows Security Log Event ID 4
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event....
Click to go back (Alt+Left arrow), hold to see history
Ultimate IT SECURITY
December 2024 Patch Tuesday
"Pat
User name:
Password:
Login / Forgot?
Register
Security Log
Windows
SharePoint
SQL Server
Exchange
Training
Tools
Newsletter
Webinars
Blog
Webinars
Training
Encyclopedia
Quick Reference
Book
Encyclopedia
Event IDs
All Event IDs
Audit Policy
Go To Event ID:
Go
Security Log Quick Reference Chart
Windows Security Log Event ID 4624
4624: An account was successfully logged on
On this page
Description of this event
Field level details
Examples
This is a highly valuable event since it documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. You can tie this event to logoff events 4634 and 4647 using Logon ID.
Win2012 adds the Impersonation Level field as shown in the example.
Win2016/10 add further fields explained below.
Operating Systems
Windows 2008 R2 and 7
Windows 2012 R2 and 8.1
Windows 2016 and 10
Windows Server 2019 and 2022
Category
• Subcategory
Logon/Logoff
• Logon
Type
Success
Corresponding events in Windows 2003 and before
528 , 540


Search | Splunk 9.3.1
Windows Security Log Event ID 4
Not secure
192.168.10.10:8000/en-US/app/search/search?q=search%20index%...
Events (20,250)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
Hide Fields
All Fields
SELECTED FIELDS
EventCode 100+
a host 2
a source 4
a sourcetype 4
INTERESTING FIELDS
a Account_Domain 7
a Account_Name 22
a ComputerName 2
EventType 4
a Guid 1
a index 1
a Keywords 8
linecount 31
a LogName 3
a Logon_ID 100+
a Message 100+
EventCode
>100 Values, 33.995% of events
Selected
Yes
No
Reports
Average over time
Maximum value over time
Minimum value over time
Top values
Top values by time
Rare values
Events with this field
Avg: 5009.49128413713 Min: 0 Max: 51057 Std Dev: 3034.6035876147666
Top 10 Values
Count
%
4624 1,774 25.77%
4672 1,639 23.809%
4634 1,554 22.574%
7036 490 7.118%
4625 301 4.372%
5379 254 3.69%
4799 101 1.467%
566 63 0.915%
16394 51 0.741%
16384 50 0.726%
Activate Windows
Go to Settings to activa