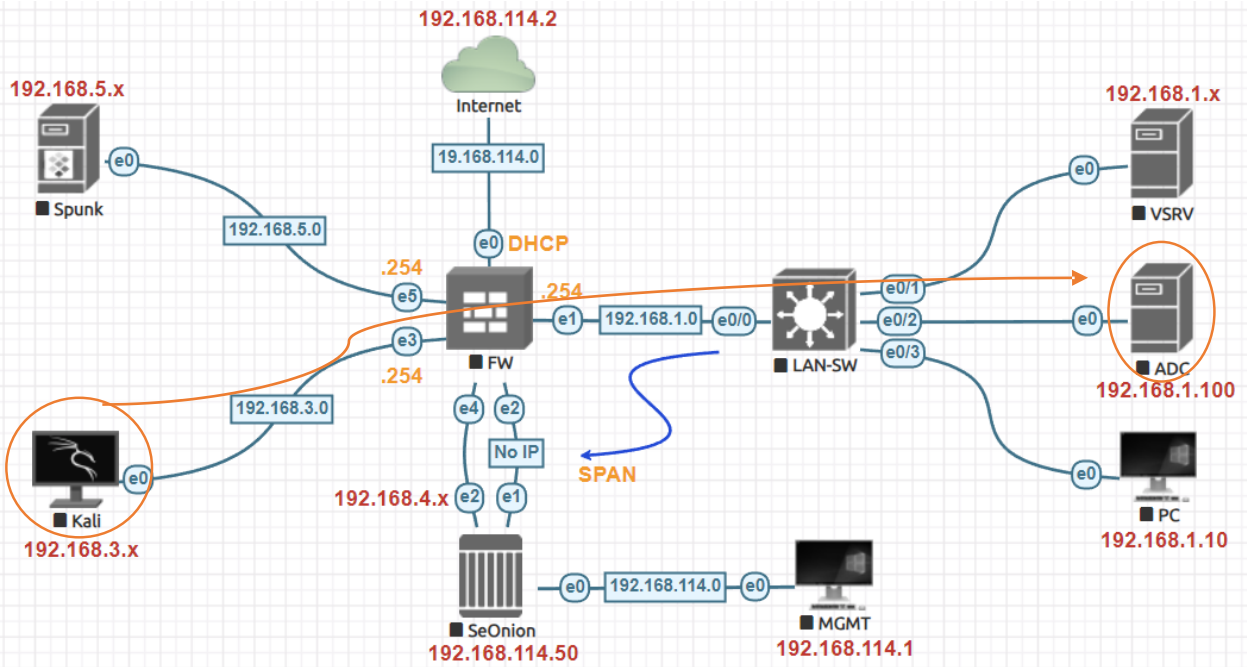
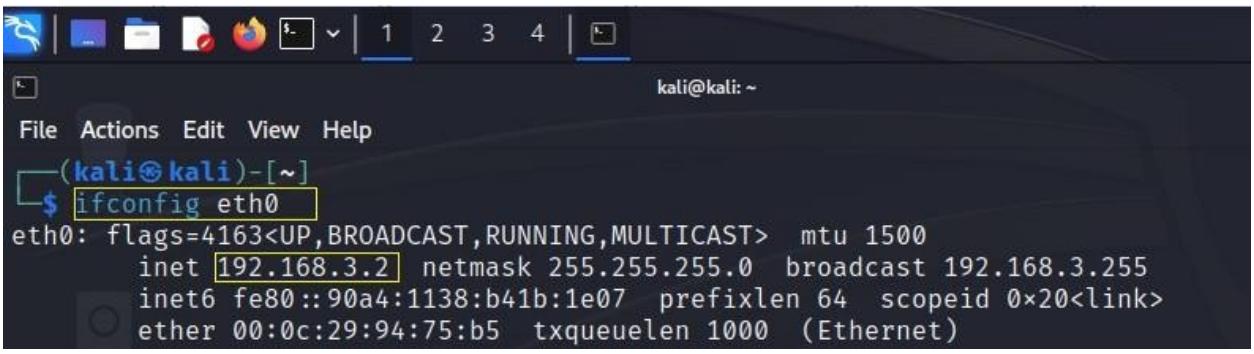
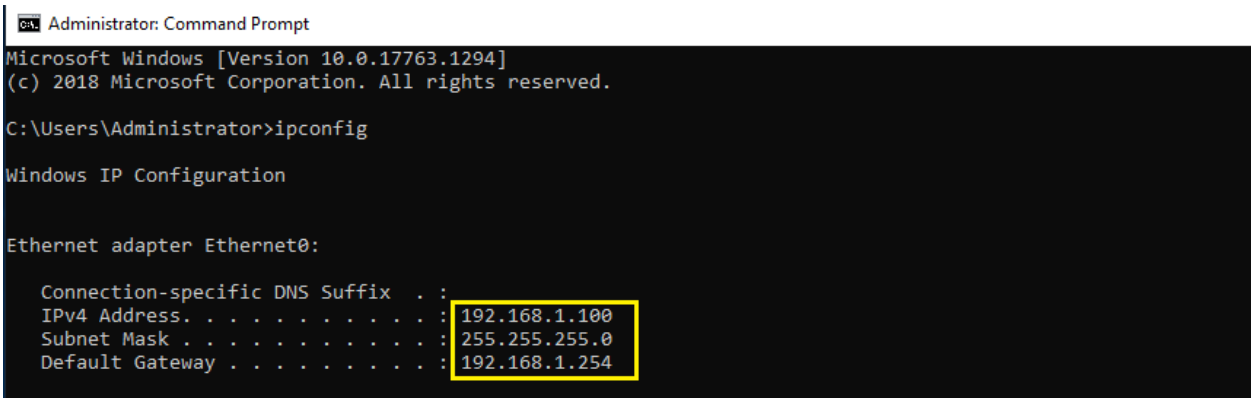
Active Direcotry Monitoring:



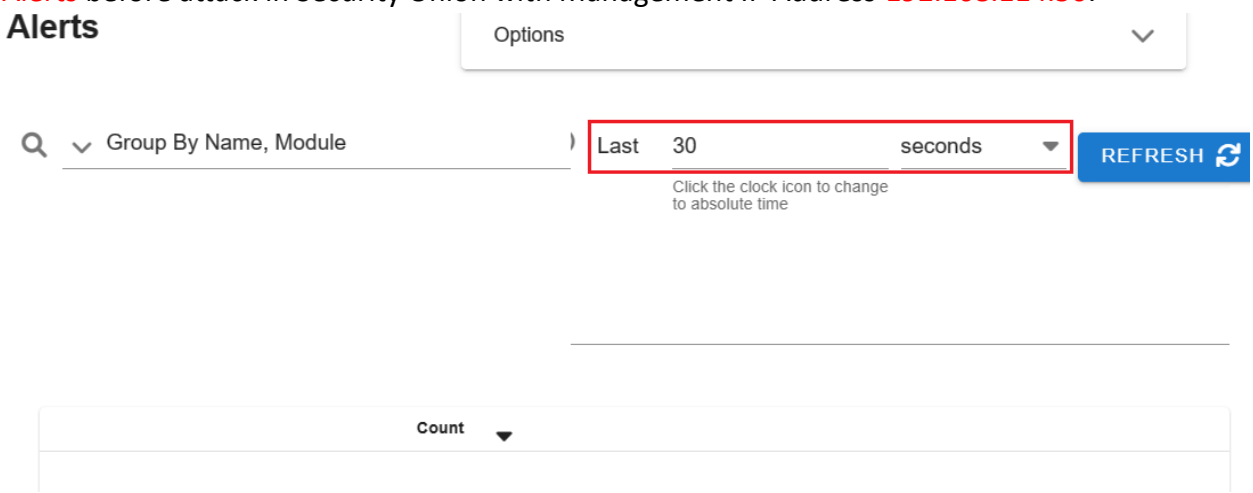
Kali Linux Attacker IP Address in the time of Attack 192.168.3.2.



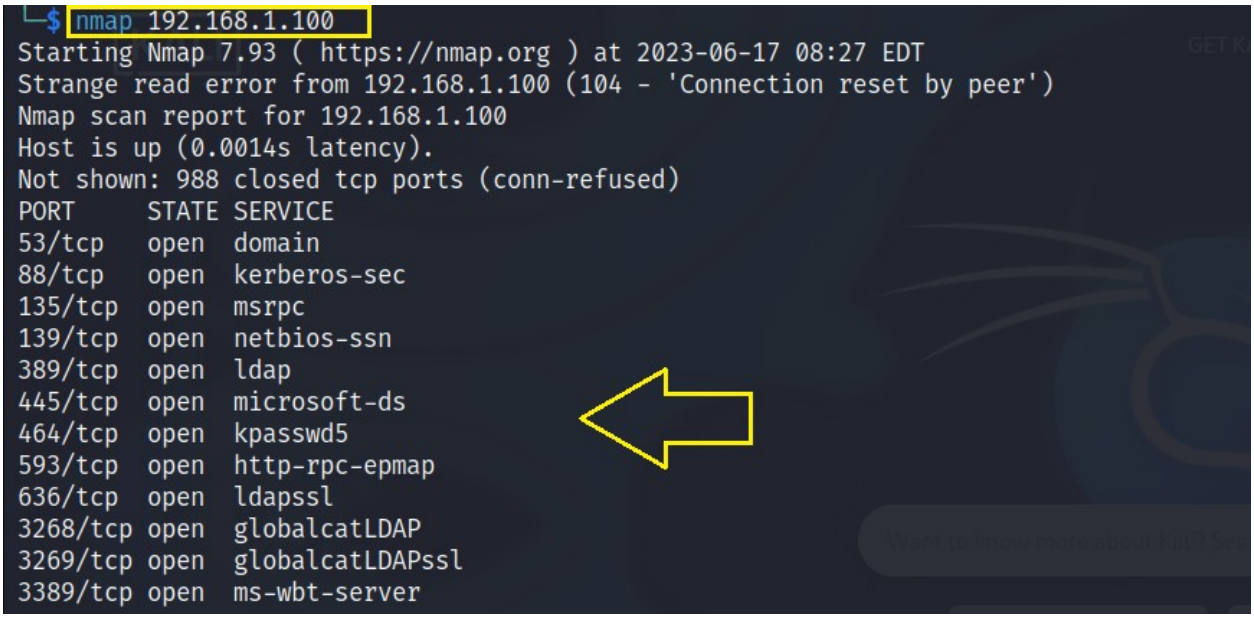
Microsoft Windows Server 2019 in the LAN IP Address 192.168.1.100.



Alerts before attack in Security Onion with Management IP Address 192.168.114.50.



Let's perform scanning attack from Kali Linux on Windows Server 2019 192.168.1.100.



```
└─$ nmap 192.168.1.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-17 08:27 EDT
Strange read error from 192.168.1.100 (104 - 'Connection reset by peer')
Nmap scan report for 192.168.1.100
Host is up (0.0014s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
```

Let's navigate back to Security Onion Alerts to see the attack.

		Count	rule.name	event.module
		1	ET SCAN Potential VNC Scan 5800-5820	suricata
		1	ET SCAN Potential VNC Scan 5900-5920	suricata
		1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata
		1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata
		1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata
		1	ET SCAN Suspicious inbound to mySQL port 3306	suricata

2023-06-17 15:27:49.325 +03:00	ET SCAN Potential VNC Scan 5800-5820	medium	

@timestamp	2023-06-17T12:27:49.325Z
destination.ip	192.168.1.100
destination.port	5815
ecs.version	8.0.0
event.category	network
event.dataset	alert
event.ingested	2023-06-17T12:27:57.845Z
event.module	suricata

Navigate to Dashboard filter by Suricata to see more specific logs related to the attack.

Timestamp	source.ip	source.port	destination.ip	destination.por
2023-06-17 15:27:50.605 +03:00	192.168.3.2	38080	192.168.1.100	1521
2023-06-17 15:27:50.603 +03:00	192.168.3.2	47462	192.168.1.100	5902
2023-06-17 15:27:50.435 +03:00	192.168.3.2	50376	192.168.1.100	5432
2023-06-17 15:27:49.325 +03:00	192.168.3.2	54084	192.168.1.100	5815
2023-06-17 15:27:48.120 +03:00	192.168.3.2	60842	192.168.1.100	1433
2023-06-17 15:27:48.112 +03:00	192.168.3.2	34168	192.168.1.100	3306

Count	destination.port
1	1433
1	1521
1	3306
1	5432
1	5815
1	5902

Rows per page: 10 1-6 of 6

Let's perform Kerberos attack from Kali Linux to Windows Server 2019 192.168.1.100

```
└─$ ./kerbrute_linux_amd64 userenum --dc 192.168.1.100 -d test.local users.txt

Version: v1.0.3 (9dad6e1) - 06/17/23 - Ronnie Flathers @ropnop

2023/06/17 08:34:31 >  Using KDC(s):
2023/06/17 08:34:31 >   192.168.1.100:88

2023/06/17 08:34:31 >  [+] VALID USERNAME:       hr1@test.local
2023/06/17 08:34:31 >  [+] VALID USERNAME:       it1@test.local
2023/06/17 08:34:31 >  [+] VALID USERNAME:       sal1@test.local
2023/06/17 08:34:31 >  [+] VALID USERNAME:       ad1@test.local
2023/06/17 08:34:31 >  [+] VALID USERNAME:       Afton.Gizela@test.local
2023/06/17 08:34:31 >  [+] VALID USERNAME:       Arda.Daniella@test.local
```

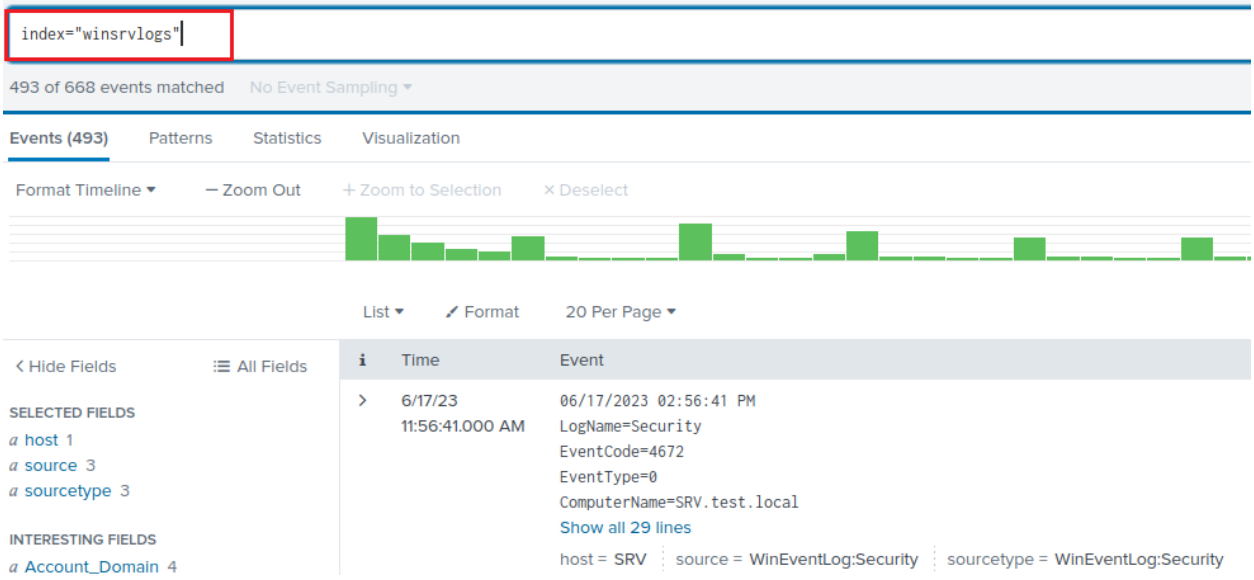
Navigate to Dashboard filter by Kerberos to see more details.

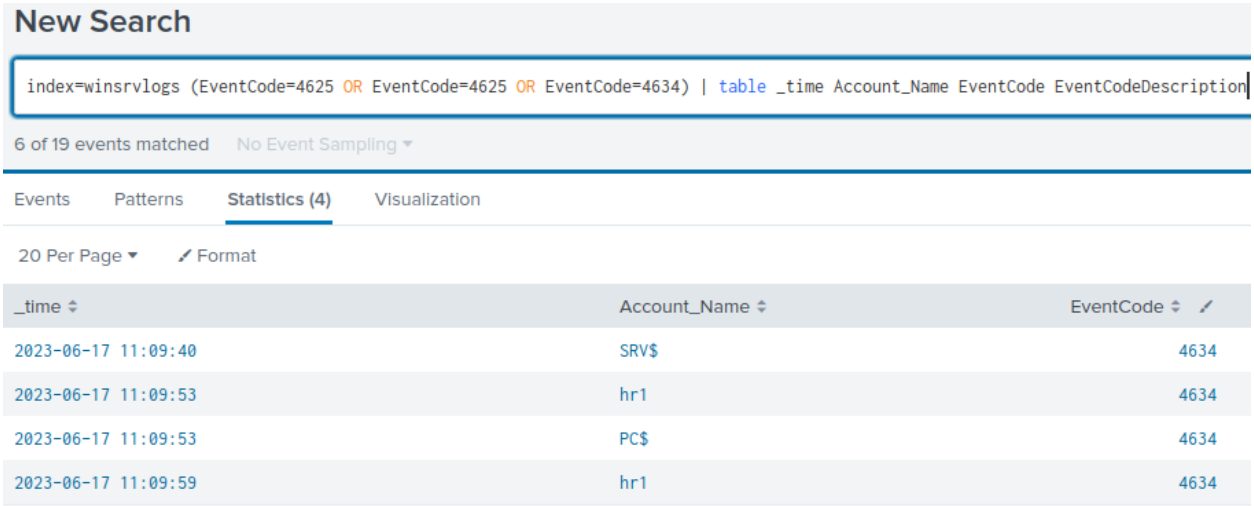
Count	event.dataset
4,370	access
1,293	conn
729	syscollector
419	elasticsearch.server
214	ossec
77	kerberos

Count	event.module
4,503	kratos
1,450	zeek
971	ossec
419	elasticsearch
71	kibana
6	suricata

source.ip	source.port	destination.ip	destination.port	kerberos.client	kerberos.service
192.168.3.2	50841	192.168.1.100	88	ad1/TEST.LOCAL	krbtgt/TEST.LOCAL
192.168.3.2	36207	192.168.1.100	88	sal1/TEST.LOCAL	krbtgt/TEST.LOCAL
192.168.3.2	59085	192.168.1.100	88	hr1/TEST.LOCAL	krbtgt/TEST.LOCAL
192.168.3.2	46092	192.168.1.100	88	Berny.Lauren/TEST.LOCAL	krbtgt/TEST.LOCAL
192.168.3.2	45984	192.168.1.100	88	Albertine.Pier/TEST.LOCAL	krbtgt/TEST.LOCAL
192.168.3.2	51836	192.168.1.100	88	Alethea.Saraann/TEST.LOCAL	krbtgt/TEST.LOCAL
192.168.3.2	55760	192.168.1.100	88	Afton.Gizela/TEST.LOCAL	krbtgt/TEST.LOCAL

Monitor in Splunk:





New Search

```
index="winsrvlogs"  Account_Name="hr1"
```

6 of 7 events matched No Event Sampling

Events (6) Patterns Statistics Visualization

List Format 20 Per Page

Hide Fields All Fields

SELECTED FIELDS
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS
- Account_Domain 3

i	Time	Event
>	6/17/23 11:11:08.000 AM	06/17/2023 02:11:08 PM LogName=Security EventCode=4634 EventType=0 ComputerName=SRV.test.local Show all 22 lines host = SRV source = WinEventLog:Security sourcetype = WinEventLog:Security

New Search

```
fail* password
```

1 of 1 event matched No Event Sampling

Events (1) Patterns Statistics Visualization

List Format 20 Per Page

Hide Fields All Fields

SELECTED FIELDS
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS
- Account_Domain 1
- Account_Name 2

i	Time	Event
>	6/17/23 11:41:53.000 AM	06/17/2023 02:41:53 PM ... 24 lines omitted ... Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Show all 61 lines host = SRV source = WinEventLog:Security sourcetype = WinEventLog:Security

```
index="winsrvlogs"  Account_Name="hr1" | table _time Account_Name EventCode
```

31 of 37 events matched No Event Sampling

Events Patterns Statistics (31) Visualization

20 Per Page Format

_time	Account_Name
2023-06-17 11:11:08	hr1
2023-06-17 11:11:07	hr1
2023-06-17 11:11:07	hr1
2023-06-17 11:11:07	- hr1

```
index="winsrvlogs" TaskCategory="*" Account_Name="*" | table TaskCategory Account_Name
```

23 of 23 events matched No Event Sampling

Events Patterns **Statistics (11)** Visualization

20 Per Page Format

TaskCategory	Account_Name
Logon	- PC$
Logoff	SRV$
Kerberos Authentication Service	hr1
Kerberos Service Ticket Operations	hr1@TEST.LOCAL

New Search

```
index="winsrvlogs" Keywords="Audit Failure" | stats count by host
```

1 of 6 events matched No Event Sampling

Events Patterns **Statistics (1)** Visualization

20 Per Page Format

host	count
SRV	1

Data Summary

Hosts (1) **Sources (4)** Sourcetypes (4)

filter

Source	Count	Last Update
WinEventLog:Application	786	6/17/23 11:18:15.000 AM
WinEventLog:Security	15,625	6/17/23 12:08:13.000 PM
WinEventLog:Setup	24	6/14/23 2:30:36.000 PM
WinEventLog:System	3,748	6/17/23 12:02:17.000 PM