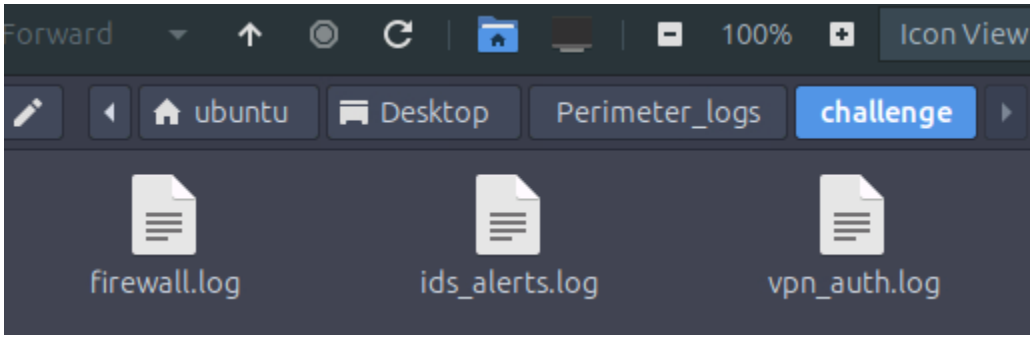
Incident Scenario

Initech Corp, a mid-sized financial services company, has recently deployed a new firewall and intrusion detection system (IDS) to monitor its network perimeter. Over the past month, security analysts have noticed abnormal traffic patterns, but the SOC team has been overwhelmed and missed deeper analysis.

As a new security analyst, you have been tasked with reviewing one month of perimeter logs to determine what techniques the adversary used, and whether they succeeded in breaching the perimeter.

- **Firewall Logs:**`firewall.log`
- **WAF Logs:**`ids_alerts.log`
- **VPN Logs:**`vpn_auth.log`



Network Assets

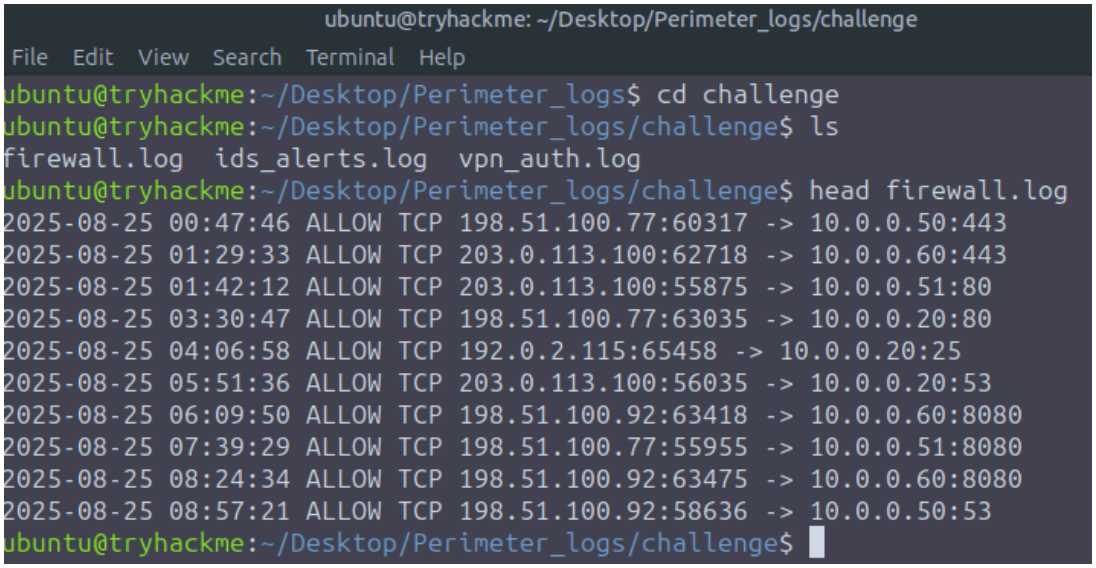
The Network of Initech Corp contains the following assets. We can use that as a reference.

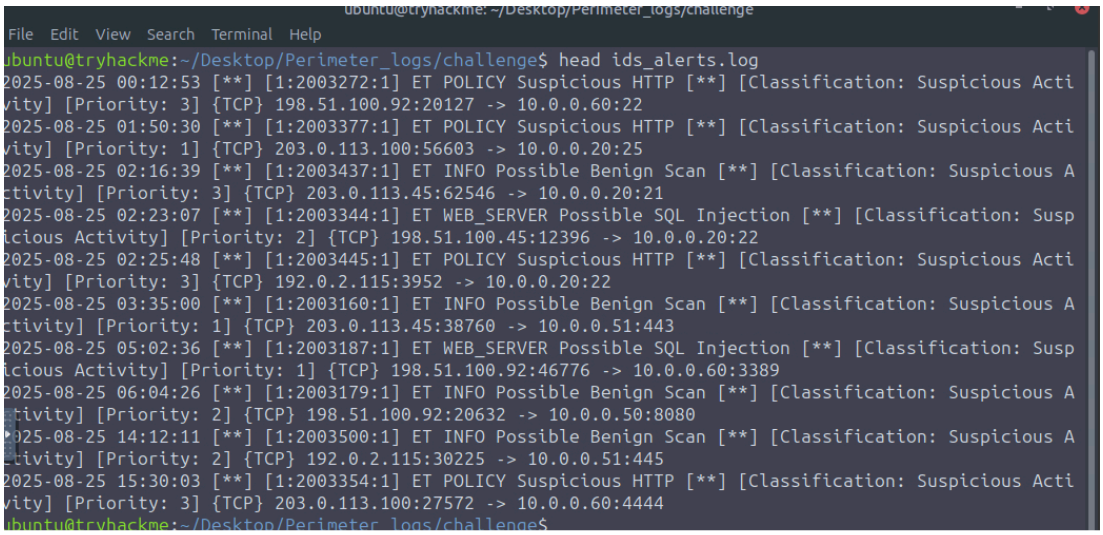
IP	Hostname	Role	OS	Team	Criticality
10.0.0.20	FINANCE-SRV1	File/Finance Server (SMB)	Windows Server	Finance IT	High
10.0.0.50	VPN-GW	VPN Gateway	Linux	NetOps	Critical
10.0.0.51	APP-WEB-01	Internal Web/App	Linux	Apps Team	High
10.0.0.60	WORKSTATION-60	Employee Workstation	Windows 10	Sales	Medium
10.8.0.23	VPN-CLIENT-ATTK	VPN Assigned Client (Ephemeral)	N/A	N/A	Critical
10.0.1.10	DMZ-WEB	DMZ Web Server	Linux	NetOps	Medium

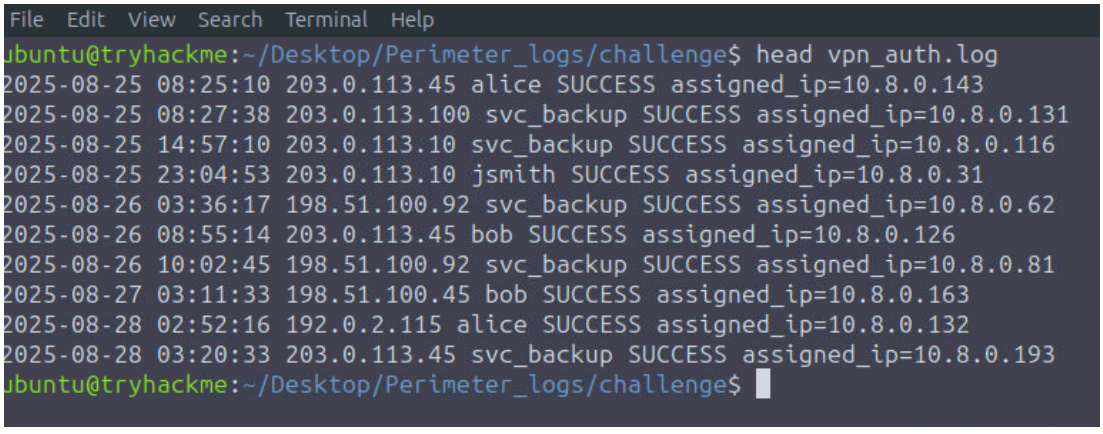
Investigating the Logs

There are two ways to investigate the logs: manually using command-line tools or using Splunk. Instructions on how to access the Splunk instance are mentioned at the end.

Method 1: Manual Log Analysis


ubuntu@tryhackme: ~/Desktop/Perimeter_logs/challenge
File Edit View Search Terminal Help
ubuntu@tryhackme:~/Desktop/Perimeter_logs$ cd challenge
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$ ls
firewall.log ids_alerts.log vpn_auth.log
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$ head firewall.log
2025-08-25 00:47:46 ALLOW TCP 198.51.100.77:60317 -> 10.0.0.50:443
2025-08-25 01:29:33 ALLOW TCP 203.0.113.100:62718 -> 10.0.0.60:443
2025-08-25 01:42:12 ALLOW TCP 203.0.113.100:55875 -> 10.0.0.51:80
2025-08-25 03:30:47 ALLOW TCP 198.51.100.77:63035 -> 10.0.0.20:80
2025-08-25 04:06:58 ALLOW TCP 192.0.2.115:65458 -> 10.0.0.20:25
2025-08-25 05:51:36 ALLOW TCP 203.0.113.100:56035 -> 10.0.0.20:53
2025-08-25 06:09:50 ALLOW TCP 198.51.100.92:63418 -> 10.0.0.60:8080
2025-08-25 07:39:29 ALLOW TCP 198.51.100.77:55955 -> 10.0.0.51:8080
2025-08-25 08:24:34 ALLOW TCP 198.51.100.92:63475 -> 10.0.0.60:8080
2025-08-25 08:57:21 ALLOW TCP 198.51.100.92:58636 -> 10.0.0.50:53
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$

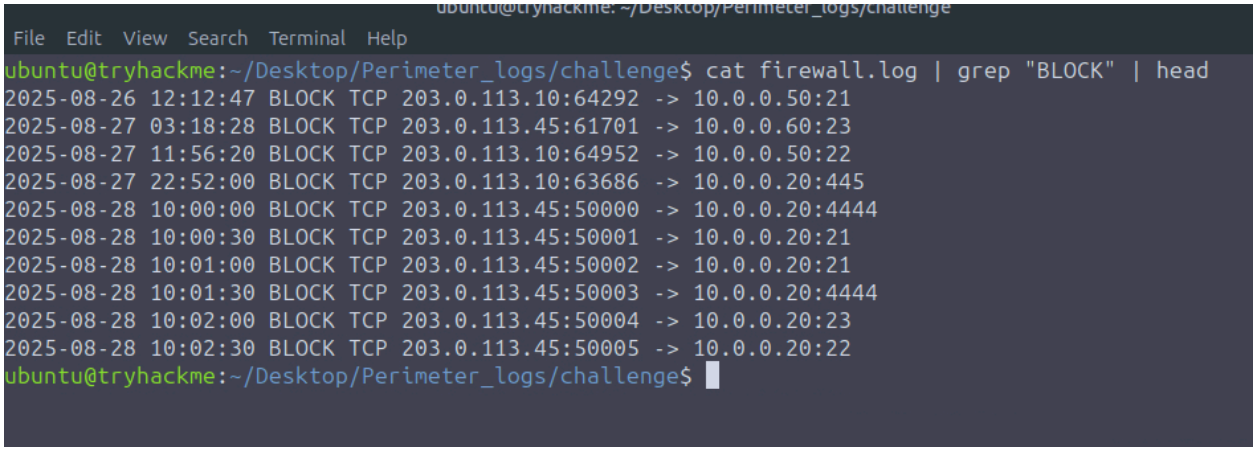

File Edit View Search Terminal Help
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$ head ids_alerts.log
2025-08-25 00:12:53 [**] [1:2003272:1] ET POLICY Suspicious HTTP [**] [Classification: Suspicious Acti
vity] [Priority: 3] {TCP} 198.51.100.92:20127 -> 10.0.0.60:22
2025-08-25 01:50:30 [**] [1:2003377:1] ET POLICY Suspicious HTTP [**] [Classification: Suspicious Acti
vity] [Priority: 1] {TCP} 203.0.113.100:56603 -> 10.0.0.20:25
2025-08-25 02:16:39 [**] [1:2003437:1] ET INFO Possible Benign Scan [**] [Classification: Suspicious A
ctivity] [Priority: 3] {TCP} 203.0.113.45:62546 -> 10.0.0.20:21
2025-08-25 02:23:07 [**] [1:2003344:1] ET WEB_SERVER Possible SQL Injection [**] [Classification: Susp
icious Activity] [Priority: 2] {TCP} 198.51.100.45:12396 -> 10.0.0.20:22
2025-08-25 02:25:48 [**] [1:2003445:1] ET POLICY Suspicious HTTP [**] [Classification: Suspicious Acti
vity] [Priority: 3] {TCP} 192.0.2.115:3952 -> 10.0.0.20:22
2025-08-25 03:35:00 [**] [1:2003160:1] ET INFO Possible Benign Scan [**] [Classification: Suspicious A
ctivity] [Priority: 1] {TCP} 203.0.113.45:38760 -> 10.0.0.51:443
2025-08-25 05:02:36 [**] [1:2003187:1] ET WEB_SERVER Possible SQL Injection [**] [Classification: Susp
icious Activity] [Priority: 1] {TCP} 198.51.100.92:46776 -> 10.0.0.60:3389
2025-08-25 06:04:26 [**] [1:2003179:1] ET INFO Possible Benign Scan [**] [Classification: Suspicious A
ctivity] [Priority: 2] {TCP} 198.51.100.92:20632 -> 10.0.0.50:8080
2025-08-25 14:12:11 [**] [1:2003500:1] ET INFO Possible Benign Scan [**] [Classification: Suspicious A
ctivity] [Priority: 2] {TCP} 192.0.2.115:30225 -> 10.0.0.51:445
2025-08-25 15:30:03 [**] [1:2003354:1] ET POLICY Suspicious HTTP [**] [Classification: Suspicious Acti
vity] [Priority: 3] {TCP} 203.0.113.100:27572 -> 10.0.0.60:4444
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$


File Edit View Search Terminal Help
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$ head vpn_auth.log
2025-08-25 08:25:10 203.0.113.45 alice SUCCESS assigned_ip=10.8.0.143
2025-08-25 08:27:38 203.0.113.100 svc_backup SUCCESS assigned_ip=10.8.0.131
2025-08-25 14:57:10 203.0.113.10 svc_backup SUCCESS assigned_ip=10.8.0.116
2025-08-25 23:04:53 203.0.113.10 jsmith SUCCESS assigned_ip=10.8.0.31
2025-08-26 03:36:17 198.51.100.92 svc_backup SUCCESS assigned_ip=10.8.0.62
2025-08-26 08:55:14 203.0.113.45 bob SUCCESS assigned_ip=10.8.0.126
2025-08-26 10:02:45 198.51.100.92 svc_backup SUCCESS assigned_ip=10.8.0.81
2025-08-27 03:11:33 198.51.100.45 bob SUCCESS assigned_ip=10.8.0.163
2025-08-28 02:52:16 192.0.2.115 alice SUCCESS assigned_ip=10.8.0.132
2025-08-28 03:20:33 203.0.113.45 svc_backup SUCCESS assigned_ip=10.8.0.193
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$

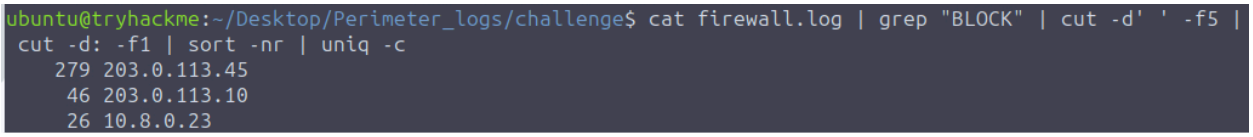
Reconnaissance attempt:

Let's begin our analysis by analyzing the blocked requests in the firewall logs, as shown below:

Examining the blocked requests indicates that an external IP has been found probing against internal IPs using various ports .



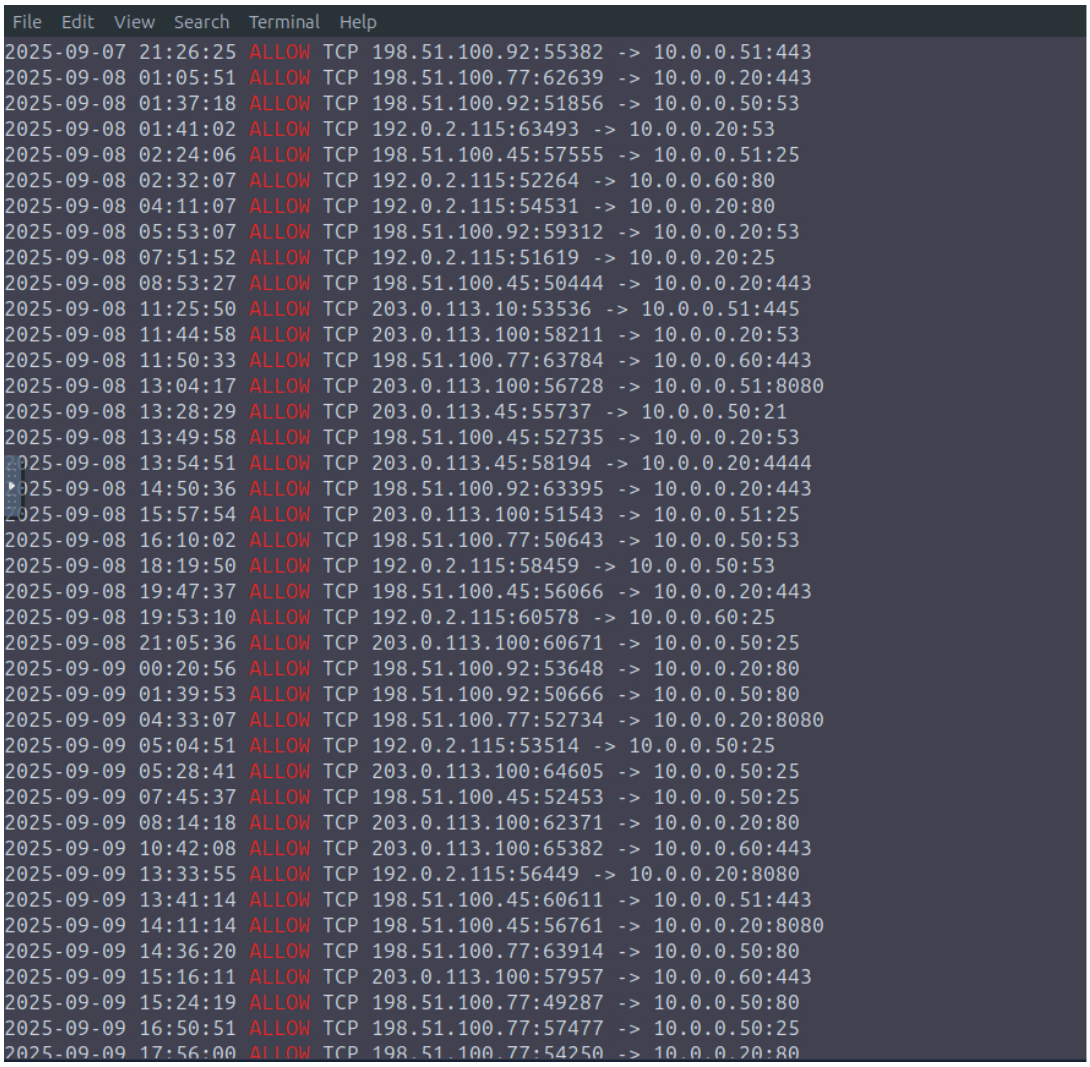
I have identified a suspicious IP, which we can use to pivot



By now, it is confirmed that, that attacker has successfully gained the initial access and got hold on to an internal IP address. Let's filter through the firewall logs and see if we can find the footprints of any lateral movement from the compromised host IP **REDACTED**.

It seems that the attacker was able to gain access to the internal network through exploitation.

`cat firewall.log | grep [REDACTED] | grep "ALLOW"`



We can clearly see that the suspicious IP has multiple failed VPN login attempts.

```
File  Edit  View  Search  Terminal  Help
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$ cat vpn_auth.log | grep FAIL | cut -d' ' -f3 | so
rt -nr | uniq -c
    118 203.0.113.45
      1 203.0.113.100
      1 198.51.100.92
      1 198.51.100.45
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$
```

the multiple login attempt was made against a certain user `svc_REDACTED`, followed by a success login, resulting in the attacker being assigned a local IP address.

```
File  Edit  View  Search  Terminal  Help
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$ cat vpn_auth.log | grep [REDACTED]
2025-08-25 08:25:10 203.0.113.45 alice SUCCESS assigned_ip=10.8.0.143
2025-08-25 08:27:38 203.0.113.100 svc_backup SUCCESS assigned_ip=10.8.0.131
2025-08-25 14:57:10 203.0.113.10 svc_backup SUCCESS assigned_ip=10.8.0.116
2025-08-25 23:04:53 203.0.113.10 jsmith SUCCESS assigned_ip=10.8.0.31
2025-08-26 03:36:17 198.51.100.92 svc_backup SUCCESS assigned_ip=10.8.0.62
2025-08-26 08:55:14 203.0.113.45 bob SUCCESS assigned_ip=10.8.0.126
2025-08-26 10:02:45 198.51.100.92 svc_backup SUCCESS assigned_ip=10.8.0.81
2025-08-27 03:11:33 198.51.100.45 bob SUCCESS assigned_ip=10.8.0.163
2025-08-28 02:52:16 192.0.2.115 alice SUCCESS assigned_ip=10.8.0.132
2025-08-28 03:20:33 203.0.113.45 svc_backup SUCCESS assigned_ip=10.8.0.193
2025-08-28 04:54:52 203.0.113.45 svc_backup SUCCESS assigned_ip=10.8.0.104
2025-08-28 09:32:18 198.51.100.92 alice SUCCESS assigned_ip=10.8.0.46
2025-08-28 20:29:44 198.51.100.45 bob SUCCESS assigned_ip=10.8.0.85
2025-08-28 20:59:06 192.0.2.115 alice SUCCESS assigned_ip=10.8.0.80
2025-08-29 08:11:44 198.51.100.45 jsmith FAIL
2025-08-29 21:02:21 203.0.113.45 jsmith SUCCESS assigned_ip=10.8.0.59
2025-08-30 14:46:31 203.0.113.100 bob SUCCESS assigned_ip=10.8.0.53
2025-08-30 23:25:10 203.0.113.45 bob SUCCESS assigned_ip=10.8.0.172
2025-08-31 00:32:09 192.0.2.115 bob SUCCESS assigned_ip=10.8.0.72
2025-08-31 10:52:34 192.0.2.115 bob SUCCESS assigned_ip=10.8.0.186
2025-08-31 12:25:56 192.0.2.115 svc_backup SUCCESS assigned_ip=10.8.0.20
2025-08-31 12:30:29 198.51.100.92 jsmith SUCCESS assigned_ip=10.8.0.38
2025-08-31 22:47:42 203.0.113.10 alice SUCCESS assigned_ip=10.8.0.32
2025-09-01 01:57:06 203.0.113.45 alice SUCCESS assigned_ip=10.8.0.89
2025-09-01 03:41:43 192.0.2.115 bob SUCCESS assigned_ip=10.8.0.179
2025-09-01 20:04:35 198.51.100.45 alice SUCCESS assigned_ip=10.8.0.174
2025-09-02 16:34:25 203.0.113.10 jsmith SUCCESS assigned_ip=10.8.0.86
2025-09-02 20:53:42 203.0.113.10 bob SUCCESS assigned_ip=10.8.0.114
2025-09-03 02:00:00 203.0.113.45 svc_backup FAIL
2025-09-03 02:00:10 203.0.113.45 svc_backup FAIL
2025-09-03 02:00:20 203.0.113.45 svc_backup FAIL
2025-09-03 02:00:30 203.0.113.45 svc_backup FAIL
2025-09-03 02:00:40 203.0.113.45 svc_backup FAIL
2025-09-03 02:00:50 203.0.113.45 svc_backup FAIL
2025-09-03 02:01:00 203.0.113.45 svc_backup FAIL
2025-09-03 02:01:10 203.0.113.45 svc_backup FAIL
2025-09-03 02:01:20 203.0.113.45 svc_backup FAIL
2025-09-03 02:01:30 203.0.113.45 svc_backup FAIL
```

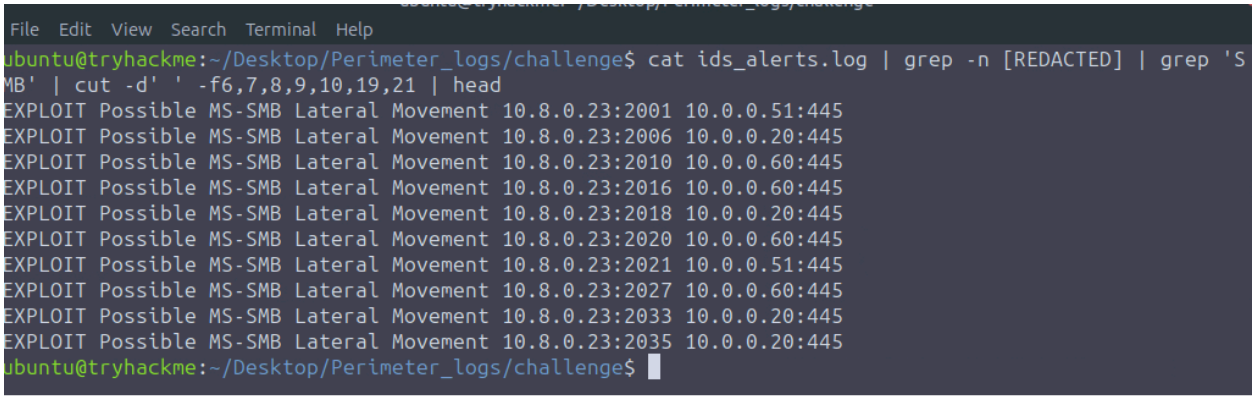
It is observed that, the compromised IP is probing internal machines `10.0.0.20/10.0.0.51/ 10.0.0.60` on various ports .

```
File  Edit  View  Search  Terminal  Help
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$ cat firewall.log | grep [REDACTED] | grep "ALLOW"
 | head
2025-08-25 00:47:46 ALLOW TCP 198.51.100.77:60317 -> 10.0.0.50:443
2025-08-25 01:29:33 ALLOW TCP 203.0.113.100:62718 -> 10.0.0.60:443
2025-08-25 01:42:12 ALLOW TCP 203.0.113.100:55875 -> 10.0.0.51:80
2025-08-25 03:30:47 ALLOW TCP 198.51.100.77:63035 -> 10.0.0.20:80
2025-08-25 04:06:58 ALLOW TCP 192.0.2.115:65458 -> 10.0.0.20:25
2025-08-25 05:51:36 ALLOW TCP 203.0.113.100:56035 -> 10.0.0.20:53
2025-08-25 06:09:50 ALLOW TCP 198.51.100.92:63418 -> 10.0.0.60:8080
2025-08-25 07:39:29 ALLOW TCP 198.51.100.77:55955 -> 10.0.0.51:8080
2025-08-25 08:24:34 ALLOW TCP 198.51.100.92:63475 -> 10.0.0.60:8080
2025-08-25 08:57:21 ALLOW TCP 198.51.100.92:58636 -> 10.0.0.50:53
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$
```

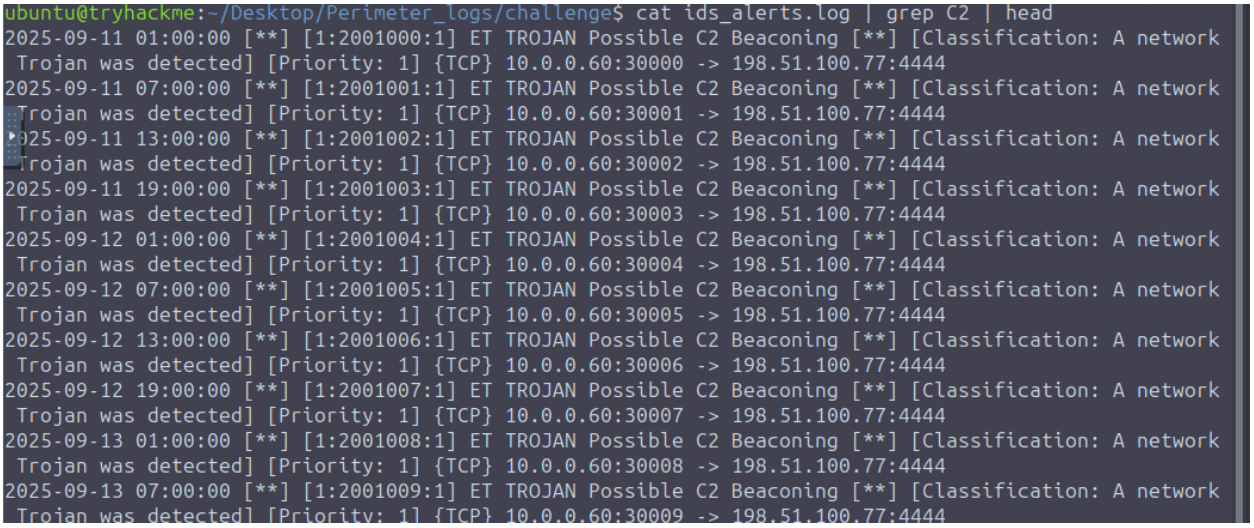
It seems, the compromised host is trying to exploit various vulnerabilities against the services mentioned above on those hosts. One of the IDS alerts indicates SMB exploit, which look interesting.

```
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$ cat ids_alerts.log | grep [REDACTED] | head
2025-08-25 00:12:53 [**] [1:2003272:1] ET POLICY Suspicious HTTP [**] [Classification: Suspicious Acti
vity] [Priority: 3] {TCP} 198.51.100.92:20127 -> 10.0.0.60:22
2025-08-25 01:50:30 [**] [1:2003377:1] ET POLICY Suspicious HTTP [**] [Classification: Suspicious Acti
vity] [Priority: 1] {TCP} 203.0.113.100:56603 -> 10.0.0.20:25
2025-08-25 02:16:39 [**] [1:2003437:1] ET INFO Possible Benign Scan [**] [Classification: Suspicious A
ctivity] [Priority: 3] {TCP} 203.0.113.45:62546 -> 10.0.0.20:21
2025-08-25 02:23:07 [**] [1:2003344:1] ET WEB_SERVER Possible SQL Injection [**] [Classification: Susp
icious Activity] [Priority: 2] {TCP} 198.51.100.45:12396 -> 10.0.0.20:22
2025-08-25 02:25:48 [**] [1:2003445:1] ET POLICY Suspicious HTTP [**] [Classification: Suspicious Acti
vity] [Priority: 3] {TCP} 192.0.2.115:3952 -> 10.0.0.20:22
2025-08-25 03:35:00 [**] [1:2003160:1] ET INFO Possible Benign Scan [**] [Classification: Suspicious A
ctivity] [Priority: 1] {TCP} 203.0.113.45:38760 -> 10.0.0.51:443
2025-08-25 05:02:36 [**] [1:2003187:1] ET WEB_SERVER Possible SQL Injection [**] [Classification: Susp
icious Activity] [Priority: 1] {TCP} 198.51.100.92:46776 -> 10.0.0.60:3389
2025-08-25 06:04:26 [**] [1:2003179:1] ET INFO Possible Benign Scan [**] [Classification: Suspicious A
ctivity] [Priority: 2] {TCP} 198.51.100.92:20632 -> 10.0.0.50:8080
2025-08-25 14:12:11 [**] [1:2003500:1] ET INFO Possible Benign Scan [**] [Classification: Suspicious A
ctivity] [Priority: 2] {TCP} 192.0.2.115:30225 -> 10.0.0.51:445
2025-08-25 15:30:03 [**] [1:2003354:1] ET POLICY Suspicious HTTP [**] [Classification: Suspicious Acti
vity] [Priority: 3] {TCP} 203.0.113.100:27572 -> 10.0.0.60:4444
ubuntu@tryhackme:~/Desktop/Perimeter_logs/challenge$
```

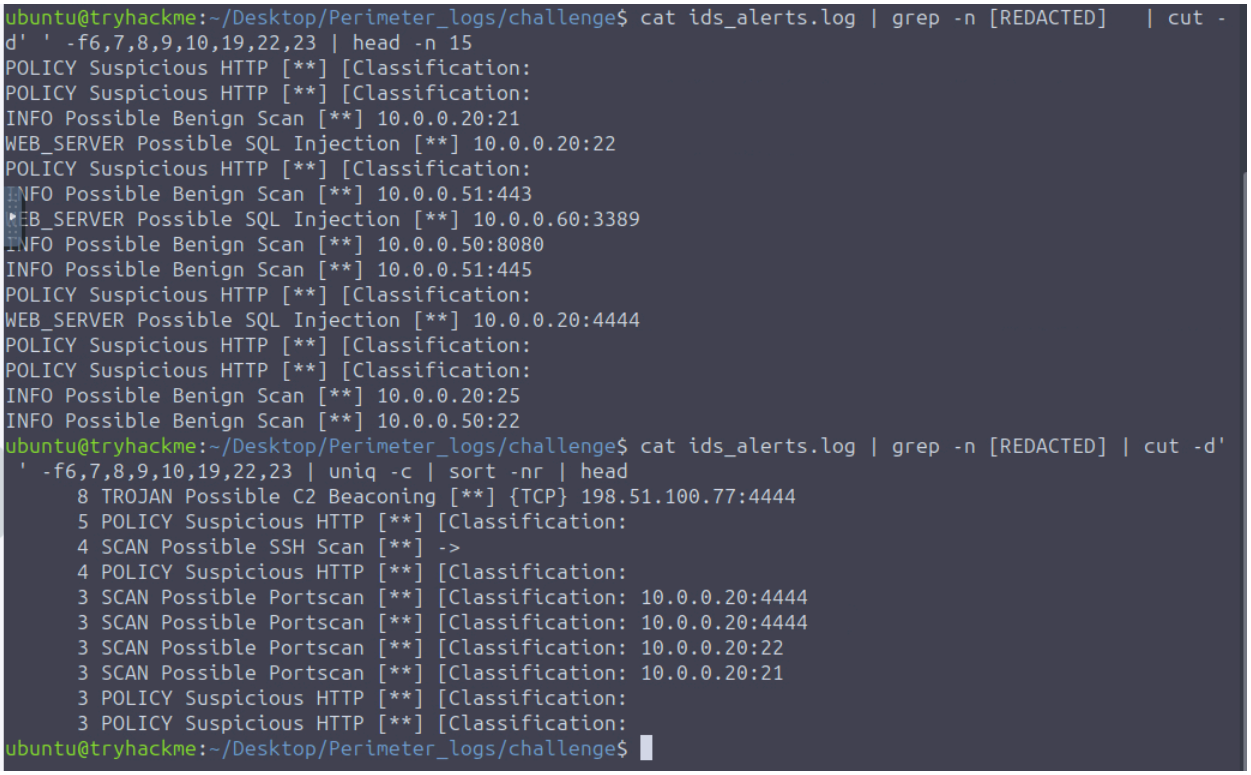
The results confirm that, the compromised host was able to exploit SMB service and was able to achieve lateral movement.



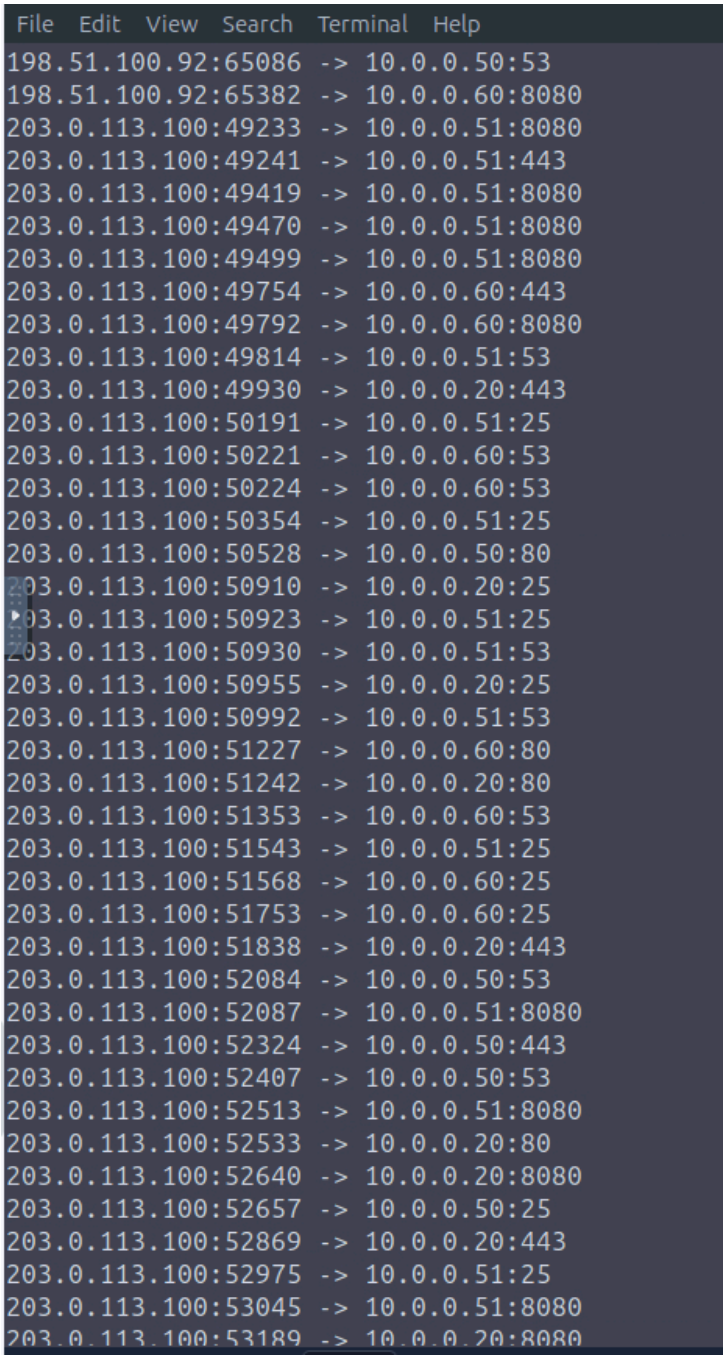
It clearly confims our suspicion against one of the internal compromised host.

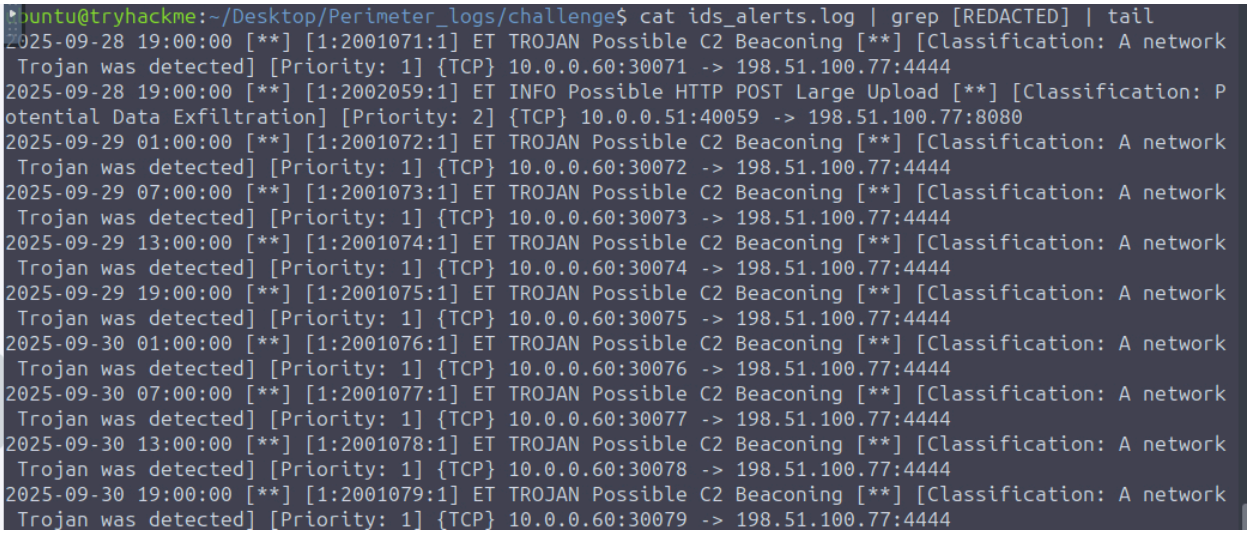


analysis clearly indicates that our internal network is fully compromised, and we now have the external IP address acting as a C2 server, recieving the C2 beacons from our compromised host.

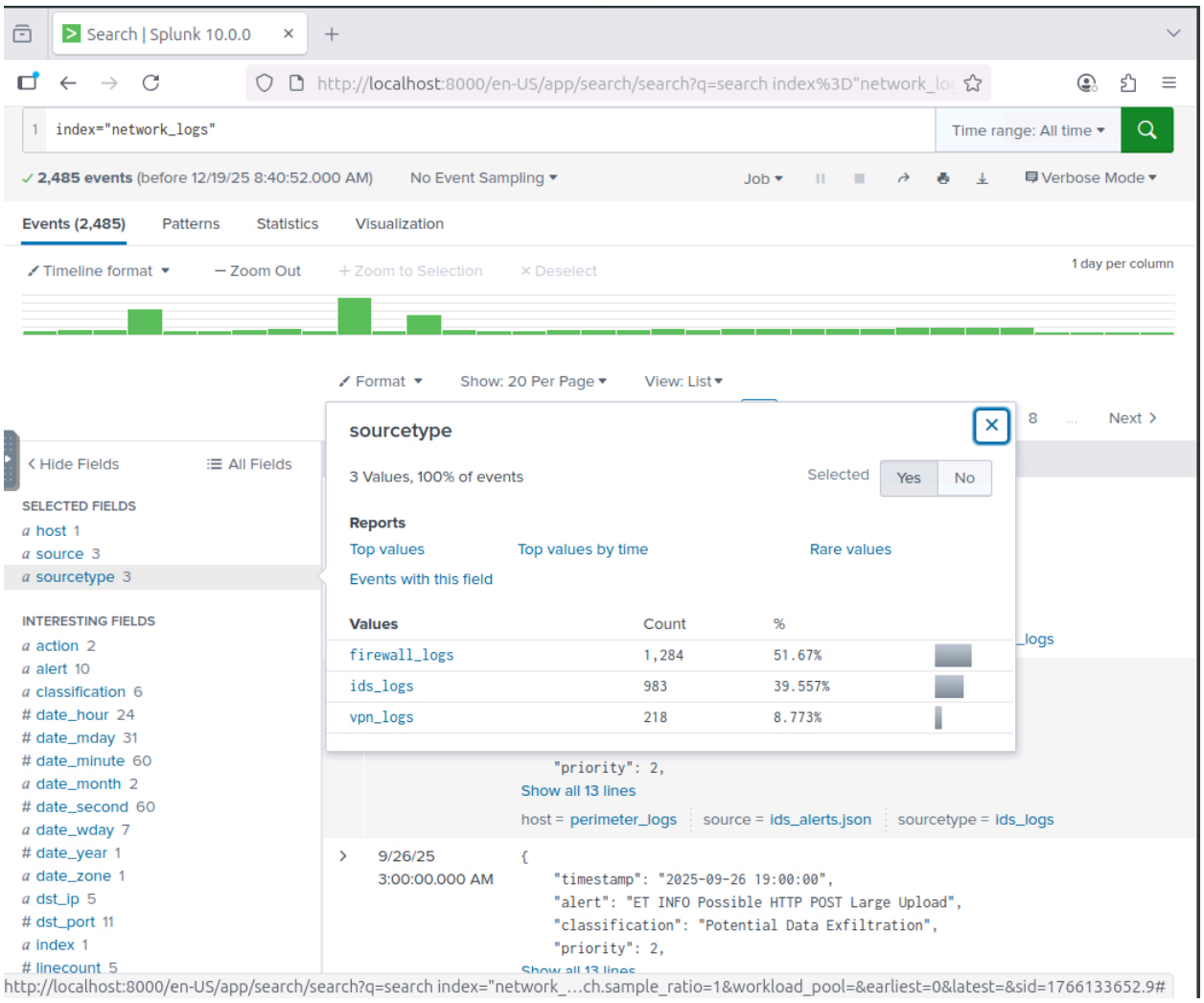


The output clearly shows, the compromised host REDACTED is sending extensive amound of traffic on external IP address. We can also filter on IDS logs, to see the alerts being triggered on these activities from the internal IP.

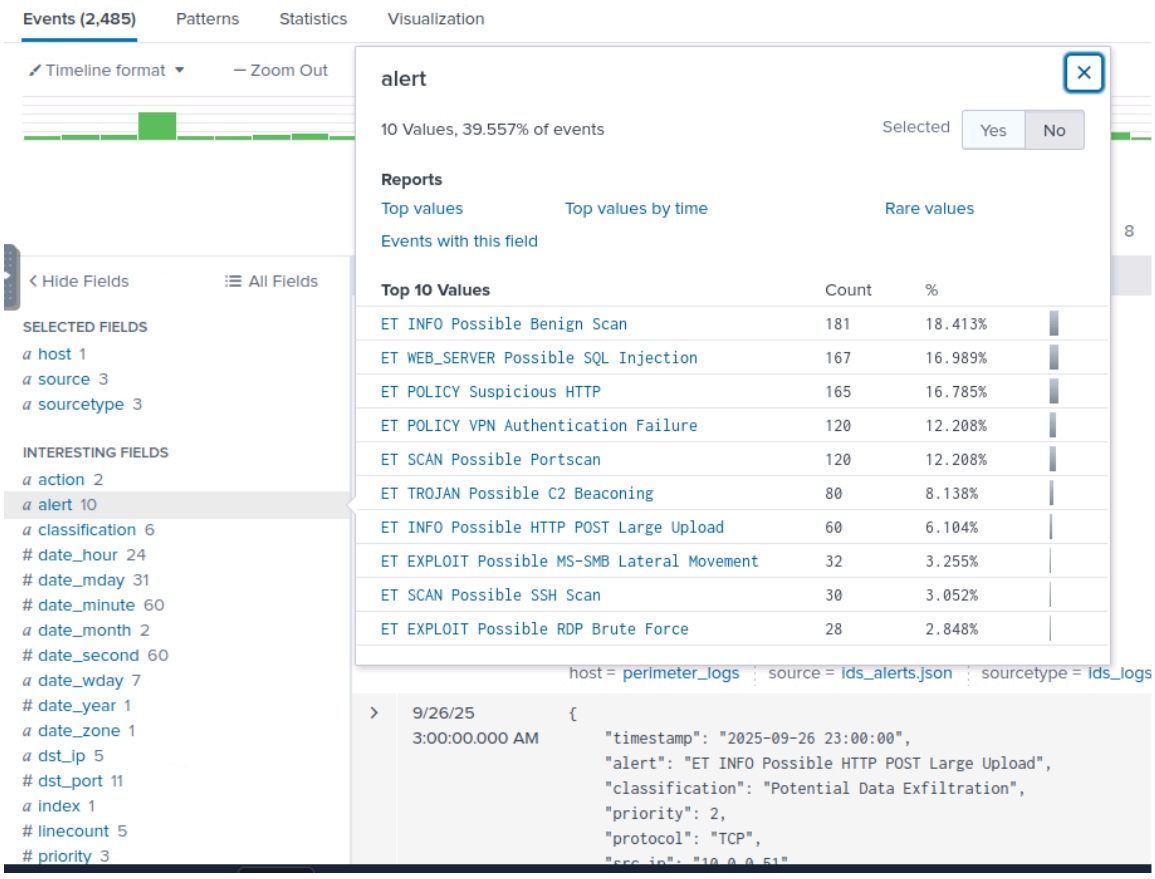



buntu@tryhackme:~/Desktop/Perimeter_logs/challenge$ cat ids_alerts.log | grep [REDACTED] | tail
2025-09-28 19:00:00 [**] [1:2001071:1] ET TROJAN Possible C2 Beaconing [**] [Classification: A network Trojan was detected] [Priority: 1] {TCP} 10.0.0.60:30071 -> 198.51.100.77:4444
2025-09-28 19:00:00 [**] [1:2002059:1] ET INFO Possible HTTP POST Large Upload [**] [Classification: Potential Data Exfiltration] [Priority: 2] {TCP} 10.0.0.51:40059 -> 198.51.100.77:8080
2025-09-29 01:00:00 [**] [1:2001072:1] ET TROJAN Possible C2 Beaconing [**] [Classification: A network Trojan was detected] [Priority: 1] {TCP} 10.0.0.60:30072 -> 198.51.100.77:4444
2025-09-29 07:00:00 [**] [1:2001073:1] ET TROJAN Possible C2 Beaconing [**] [Classification: A network Trojan was detected] [Priority: 1] {TCP} 10.0.0.60:30073 -> 198.51.100.77:4444
2025-09-29 13:00:00 [**] [1:2001074:1] ET TROJAN Possible C2 Beaconing [**] [Classification: A network Trojan was detected] [Priority: 1] {TCP} 10.0.0.60:30074 -> 198.51.100.77:4444
2025-09-29 19:00:00 [**] [1:2001075:1] ET TROJAN Possible C2 Beaconing [**] [Classification: A network Trojan was detected] [Priority: 1] {TCP} 10.0.0.60:30075 -> 198.51.100.77:4444
2025-09-30 01:00:00 [**] [1:2001076:1] ET TROJAN Possible C2 Beaconing [**] [Classification: A network Trojan was detected] [Priority: 1] {TCP} 10.0.0.60:30076 -> 198.51.100.77:4444
2025-09-30 07:00:00 [**] [1:2001077:1] ET TROJAN Possible C2 Beaconing [**] [Classification: A network Trojan was detected] [Priority: 1] {TCP} 10.0.0.60:30077 -> 198.51.100.77:4444
2025-09-30 13:00:00 [**] [1:2001078:1] ET TROJAN Possible C2 Beaconing [**] [Classification: A network Trojan was detected] [Priority: 1] {TCP} 10.0.0.60:30078 -> 198.51.100.77:4444
2025-09-30 19:00:00 [**] [1:2001079:1] ET TROJAN Possible C2 Beaconing [**] [Classification: A network Trojan was detected] [Priority: 1] {TCP} 10.0.0.60:30079 -> 198.51.100.77:4444

Method 2: Analyzing Logs via Splunk




9/26/25
3:00:00.000 AM
{ [-]
alert: ET INFO Possible HTTP POST Large Upload
bytes: 1898575
classification: Potential Data Exfiltration
dst_ip: 198.51.100.77
dst_port: 8080
priority: 2
protocol: TCP
sid: 2002049
src_ip: 10.0.0.51
src_port: 40049
timestamp: 2025-09-27 03:00:00
}
Show as raw text
host = perimeter_logs
source = ids_alerts.json
sourcetype = ids_logs


Events (2,485)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
alert
10 Values, 39.557% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Top 10 Values
Count
%
ET INFO Possible Benign Scan 181 18.413%
ET WEB_SERVER Possible SQL Injection 167 16.989%
ET POLICY Suspicious HTTP 165 16.785%
ET POLICY VPN Authentication Failure 120 12.208%
ET SCAN Possible Portscan 120 12.208%
ET TROJAN Possible C2 Beaconing 80 8.138%
ET INFO Possible HTTP POST Large Upload 60 6.104%
ET EXPLOIT Possible MS-SMB Lateral Movement 32 3.255%
ET SCAN Possible SSH Scan 30 3.052%
ET EXPLOIT Possible RDP Brute Force 28 2.848%
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 3
a sourcetype 3
INTERESTING FIELDS
a action 2
a alert 10
a classification 6
date_hour 24
date_mday 31
date_minute 60
a date_month 2
date_second 60
a date_wday 7
date_year 1
a date_zone 1
a dst_ip 5
dst_port 11
a index 1
# linecount 5
# priority 3
host = perimeter_logs
source = ids_alerts.json
sourcetype = ids_logs
9/26/25
3:00:00.000 AM
{
"timestamp": "2025-09-26 23:00:00",
"alert": "ET INFO Possible HTTP POST Large Upload",
"classification": "Potential Data Exfiltration",
"priority": 2,
"protocol": "TCP",

Answer the questions :

- **Examine the firewall logs. What external IP performed the most reconnaissance?**

  The answer:203.0.113.45

- **In the firewall log, Which internal host was targeted by scans?**

  The answer:10.0.0.20

- **Which username was targeted in VPN logs?**

  The answer:svc_backup

- **What internal IP was assigned after successful VPN login?**

  The answer:10.8.0.23

- **Which port was used for lateral SMB attempts?**

  The answer:445

- **In the IDS logs, which host beaconed to the C2?**

  The answer:10.0.0.60

- **During the investigation, which IP was observed to be associated with C2?**

  The answer:198.51.100.77

- **Which host showed the exfiltration attempts?**

  The answer:10.0.0.51